Threat Spotlight: Follow the Bad Rabbit

blog.talosintelligence.com/2017/10/bad-rabbit.html

Note: This blog post discusses active research by Talos into a new threat. This information should be considered preliminary and will be updated as research continues.

Update 2017-10-26 16:10 EDT: *added additional information regarding the links between Nyetya and BadRabbit*

Update 2017-10-26 09:20 EDT: *added additional information regarding the EternalRomance exploit*

Update 2017-10-25: *added additional information regarding encryption and propagation methods*

On October 24, 2017, Cisco Talos was alerted to a widescale ransomware campaign affecting organizations across eastern Europe and Russia. As was the case in previous situations, we quickly mobilized to assess the situation and ensure that customers remain protected from this and other threats as they emerge across the threat landscape.

There have been several large scale ransomware campaigns over the last several months. This appears to have some similarities to Nyetya in that it is also based on Petya ransomware. Major portions of the code appear to have been rewritten. The distribution does not appear to have the sophistication of the supply chain attacks we have seen recently.

Distribution

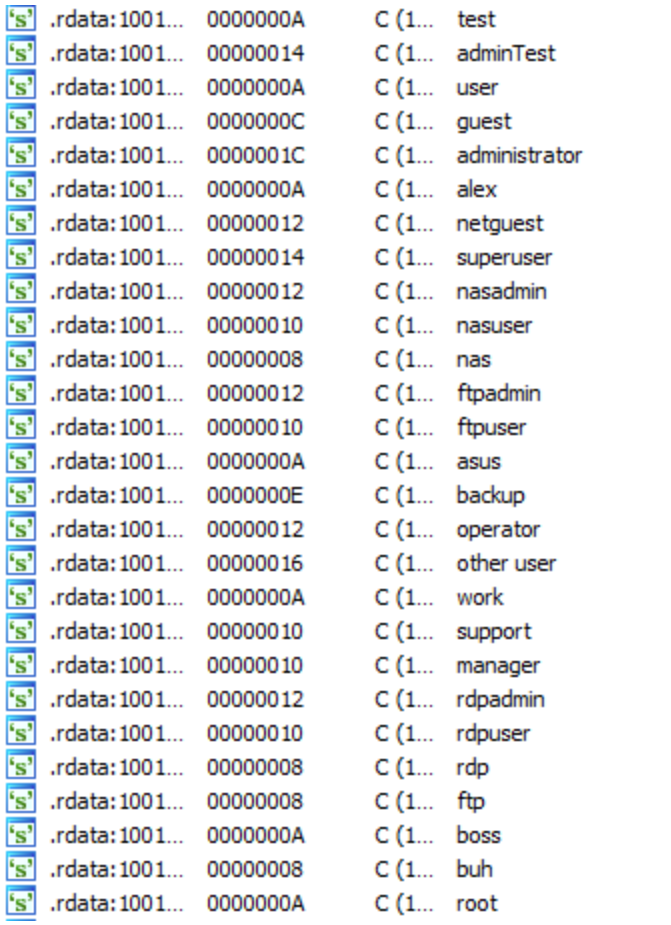
Talos assesses with high confidence that a fake Flash Player update is being delivered via a drive-by-download and compromising systems. The sites that were seen redirecting to BadRabbit were a variety of sites that are based in Russia, Bulgaria, and Turkey.

When users visited one of the compromised websites, they were redirected to 1dnscontrol[.]com, the site which was hosting the malicious file. Before the actual malicious file was downloaded a POST request was observed to a static IP address (185.149.120[.]3). This request was found to be posting to a static path of "/scholasgoogle" and provided the user agent, referring site, cookie, and domain name of the session. After the POST the dropper was downloaded from two different paths from 1dnscontrol[.]com, /index.php and /flash_install.php. Despite two paths being utilized only a single file was downloaded. Based

on current information, the malware appears to have been active for approximately six hours before the server 1dnscontrol[.]com was taken down. The initial download was observed around 2017-10-24 08:22 UTC.

The dropper (630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da) requires a user to facilitate the infection and does not use any exploit to compromise the system directly. This dropper contains the BadRabbit ransomware. Once installed there is an SMB component used for lateral movement and further infection. This appears to use a combination of an included list of weak credentials and a version of mimikatz similar to that which was used in Nyetya. Below is a list of the username/password combinations that we have observed. Note there is overlap with the 1995 cult classic "Hackers".

.rdata:1001...	00000008	C (1...	god
.rdata:1001...	00000008	C (1...	sex
.rdata:1001...	0000000E	C (1...	secret
.rdata:1001...	0000000A	C (1...	love
.rdata:1001...	00000008	C (1...	321
.rdata:1001...	0000000E	C (1...	123321
.rdata:1001...	0000000A	C (1...	uiop
.rdata:1001...	0000000A	C (1...	zxcv
.rdata:1001...	0000000E	C (1...	zxc321
.rdata:1001...	0000000E	C (1...	zxc123
.rdata:1001...	00000008	C (1...	zxc
.rdata:1001...	00000014	C (1...	qwerty123
.rdata:1001...	0000000E	C (1...	qwerty
.rdata:1001...	0000000C	C (1...	qwert
.rdata:1001...	0000000A	C (1...	qwer
.rdata:1001...	0000000E	C (1...	qwe321
.rdata:1001...	0000000E	C (1...	qwe123
.rdata:1001...	00000008	C (1...	qwe
.rdata:1001...	00000008	C (1...	777
.rdata:1001...	0000000C	C (1...	77777
.rdata:1001...	0000000C	C (1...	55555
.rdata:1001...	0000000E	C (1...	111111
.rdata:1001...	00000012	C (1...	password
.rdata:1001...	00000010	C (1...	test123
.rdata:1001...	00000020	C (1...	admin123Test123
.rdata:1001...	00000012	C (1...	Admin123
.rdata:1001...	00000010	C (1...	user123
.rdata:1001...	00000010	C (1...	User123
.rdata:1001...	00000012	C (1...	guest123
.rdata:1001...	00000012	C (1...	Guest123
.rdata:1001...	00000022	C (1...	administrator123
.rdata:1001...	00000022	C (1...	Administrator123
.rdata:1001...	00000016	C (1...	1234567890
.rdata:1001...	00000014	C (1...	123456789
.rdata:1001...	00000012	C (1...	12345678
.rdata:1001...	00000010	C (1...	1234567
.rdata:1001...	0000000E	C (1...	123456
.rdata:1001...	0000000C	C (1...	12345
.rdata:1001...	0000000A	C (1...	1234
.rdata:1001...	00000008	C (1...	123



Observed Password List

Despite initial reports, we currently have no evidence that the EternalBlue exploit is being leveraged. However, we identified the usage of the EternalRomance exploit to propagate in the network. This exploit takes advantage of a vulnerability described in the Microsoft MS17-010 security bulletin. The vulnerability was also exploited during the Nyetya campaign. Our research continues and we will update as we learn more.

Technical Details

The malware contains a dropper which is responsible for extracting and executing the worm payload. This payload contains additional binaries stored in the resources (compressed with zlib):

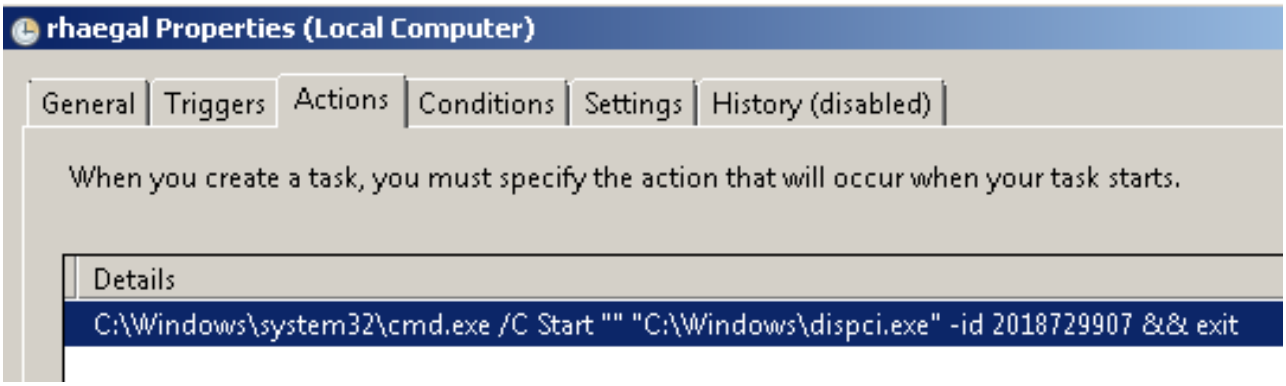
- legitimate binaries associated with DiskCryptor (2 drivers x86/x64 and 1 client);
- 2 mimikatz-like binaries (x86/x64) similar to the sample seen during Nyetya. A popular open source tool used for recovery of user credentials from computer memory using several different techniques.

It drops files into the C:\Windows\ directory. The mimikatz-like binaries are executed using the same technique that was leveraged in the Nyetya campaign. The communication

between the payload and the stealer will be performed by a named pipe, for example:

```
C:\WINDOWS\561D.tmp \\.\pipe\{C1F0BF2D-8C17-4550-AF5A-65A22C61739C}
```

The malware then uses RunDLL32.exe to execute the malware and continue the malicious operations. The malware then creates a scheduled task with the parameters shown in the screenshot below:

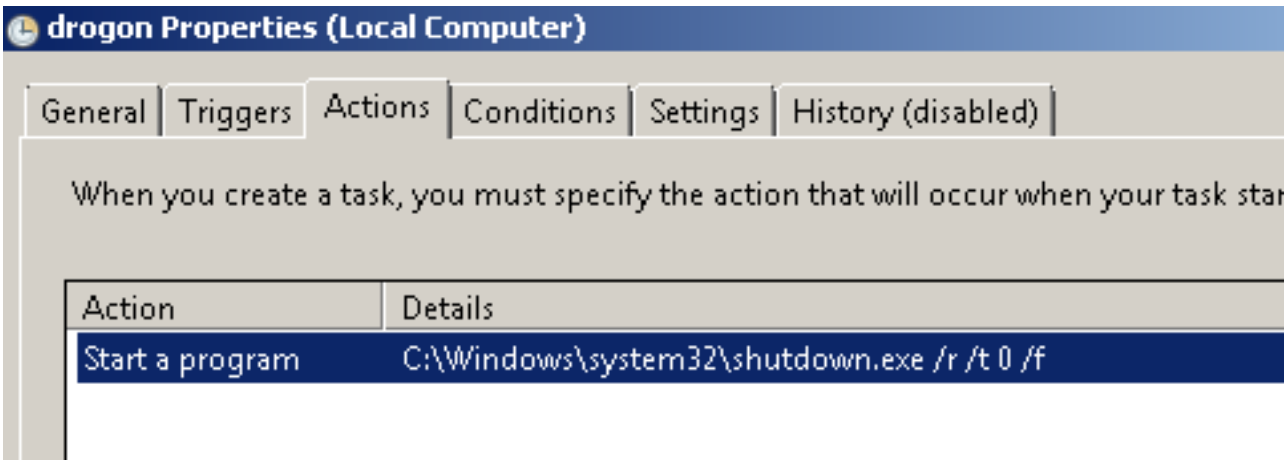


Encryption is performed with 2 techniques:

- Full disk encryption with DiskCryptor (an open source disk encryption solution)
- Individual file encryption

Here is the list of the targeted extensions: .3ds .7z .accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .hpp .hxx .iso .java .jfif .jpe .jpeg .jpg .js .kdbx .key .mail .mdb .msg .nrg .odc .odf .odg .odi .odm .odp .ods .odt .ora .ost .ova .ovf .p12 .p7b .p7c .pdf .pem .pfx .php .pmf .png .ppt .pptx .ps1 .pst .pvi .py .pyc .pyw .qcow .qcow2 .rar .rb .rtf .scm .sln .sql .tar .tib .tif .tiff .vb .vbox .vbs .vcb .vdi .vfd .vhd .vhdx .vmc .vmdk .vmsd .vmtm .vmx .vsdx .vsv .work .xls .xlsx .xml .xvd .zip

In addition to the aforementioned scheduled task, the malware creates a second scheduled task that is responsible for rebooting the system. This second task does not occur instantaneously but is scheduled to occur later.



If the names for these scheduled tasks look familiar they appear to be a reference to Game of Thrones, specifically they match the names of the dragons.

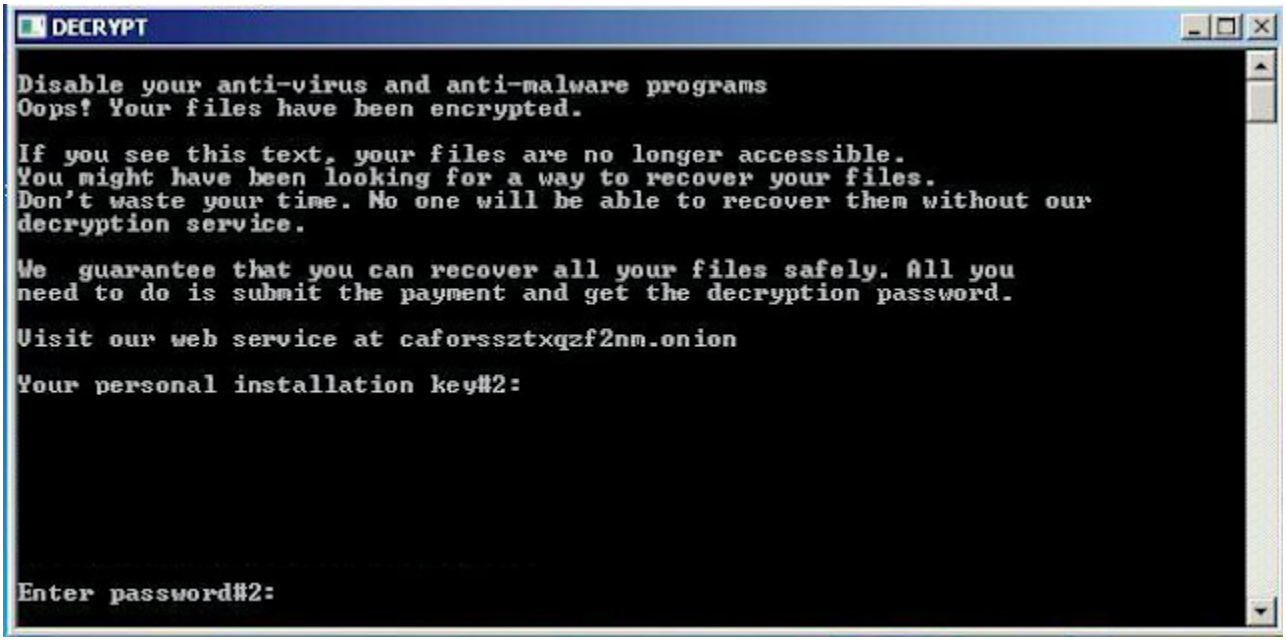
Then the malware propagates itself in the network, the technique to enumerate the network systems is exactly the same than Nyetya. It is performed by Microsoft Windows legitimate features, via:

- SVCCTL: the remote service management
- SMB2
- SMB
- NTLMSSP authentication brute force
- WMI

And an exploit:

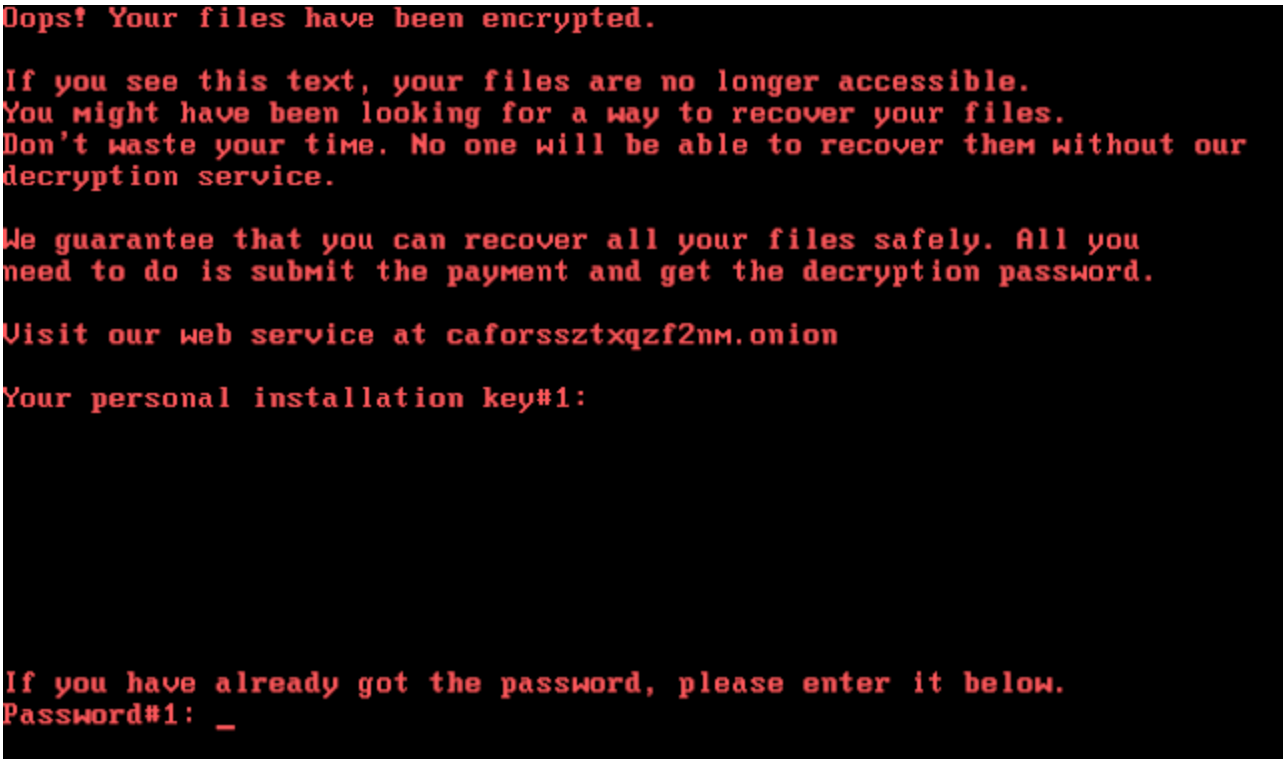
EternalRomance

The malware also creates a file on the infected user's desktop called DECRYPT. Executing this file causes the following ransom note to be displayed to victims.

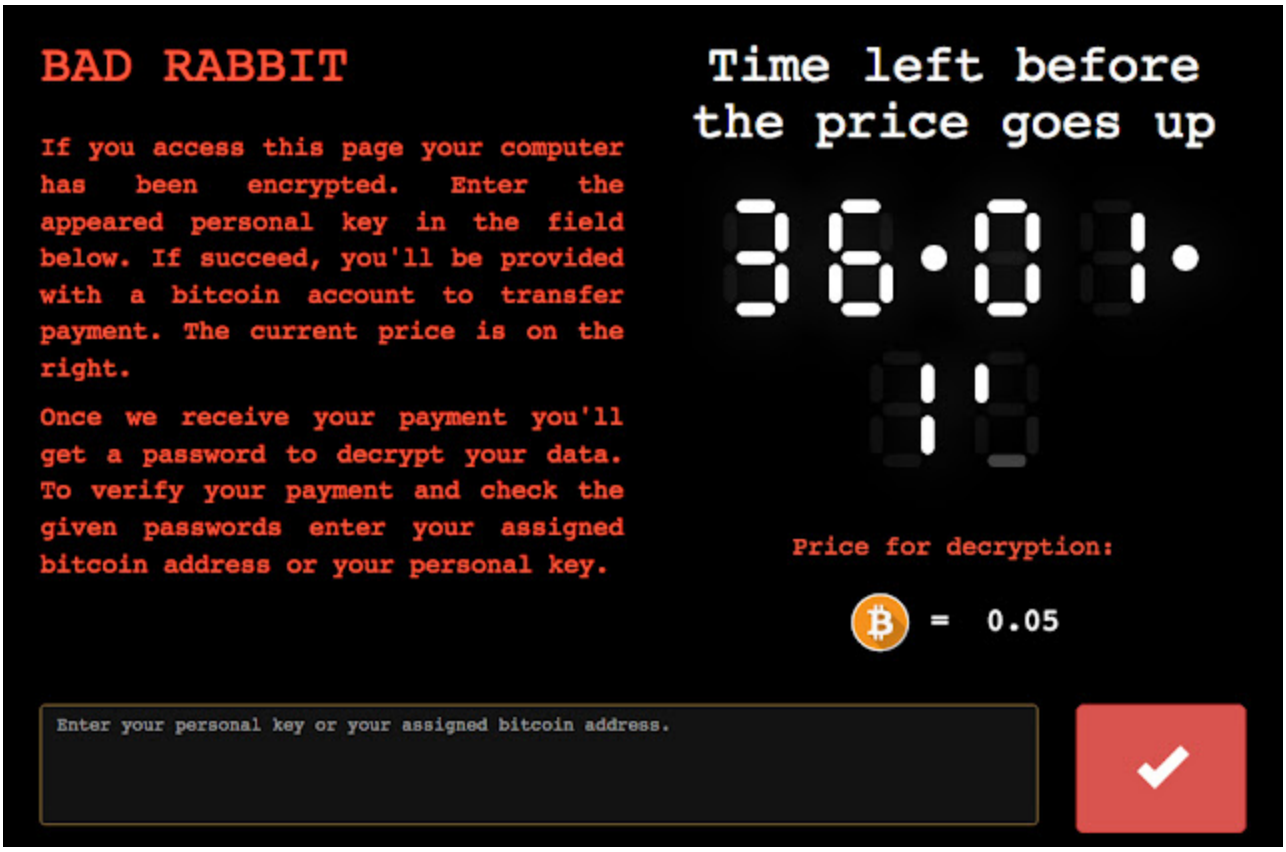


To demonstrate how quickly these sorts of threats can propagate globally, the below graphic reflects the DNS related activity associated with one of the domains that were being used to distribute the fake Adobe Flash update that was used to drop the malware on victims' systems.

The malware modifies the Master Boot Record (MBR) of the infected system's hard drive to redirect the boot process into the malware authors code for the purposes of displaying a ransom note. The ransom note that is displayed following the system reboot is below, and is very similar to the ransom notes displayed by other ransomware variants, namely Petya, that we have observed in other notable attacks this year.



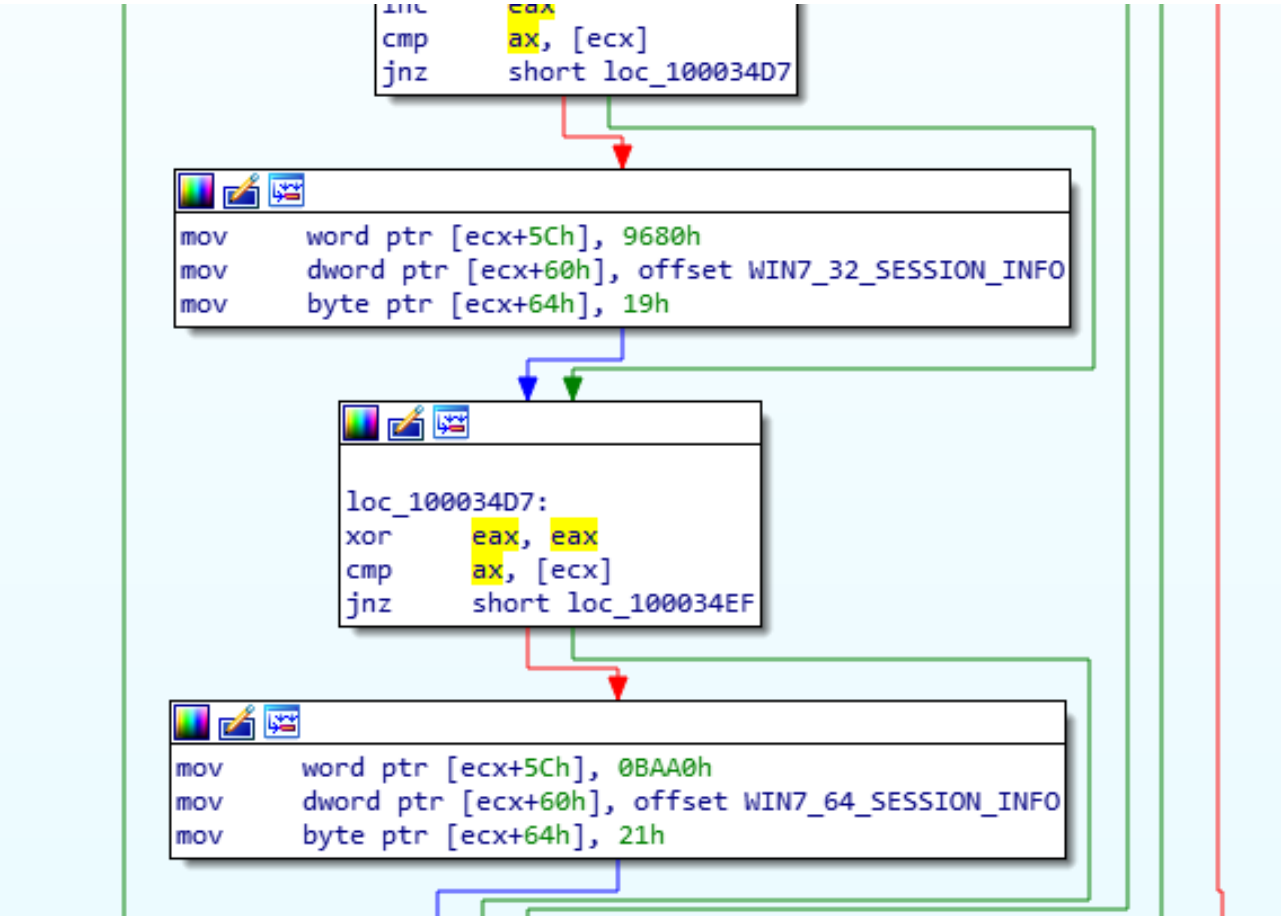
This is the payment page from the Tor site:



EternalRomance Exploit

Cisco Talos has identified an exploit in the BadRabbit sample. It is very similar to the publicly available Python implementation of the EternalRomance exploit that is also exploited by Nyetya. However, the BadRabbit exploit implementation is different than the one in Nyetya, although it is still largely based on the EternalRomance exploit published in the ShadowBrokers leak.

The following screenshot shows that BadRabbit is building modified security context structures for various operating system versions:



The structures are obfuscated using an NOT operation. For example, here is the original value of WIN7_32_SESSION_INFO in the sample:

```
"\xD5\xFD\xE3\xFF\xFE\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFF\xFD\xFF\xFF\xFF\xFF\
```

Once decoded, the value of the buffer is:

```
“2a\x02\x1c\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x00\x00\x00\x0
```

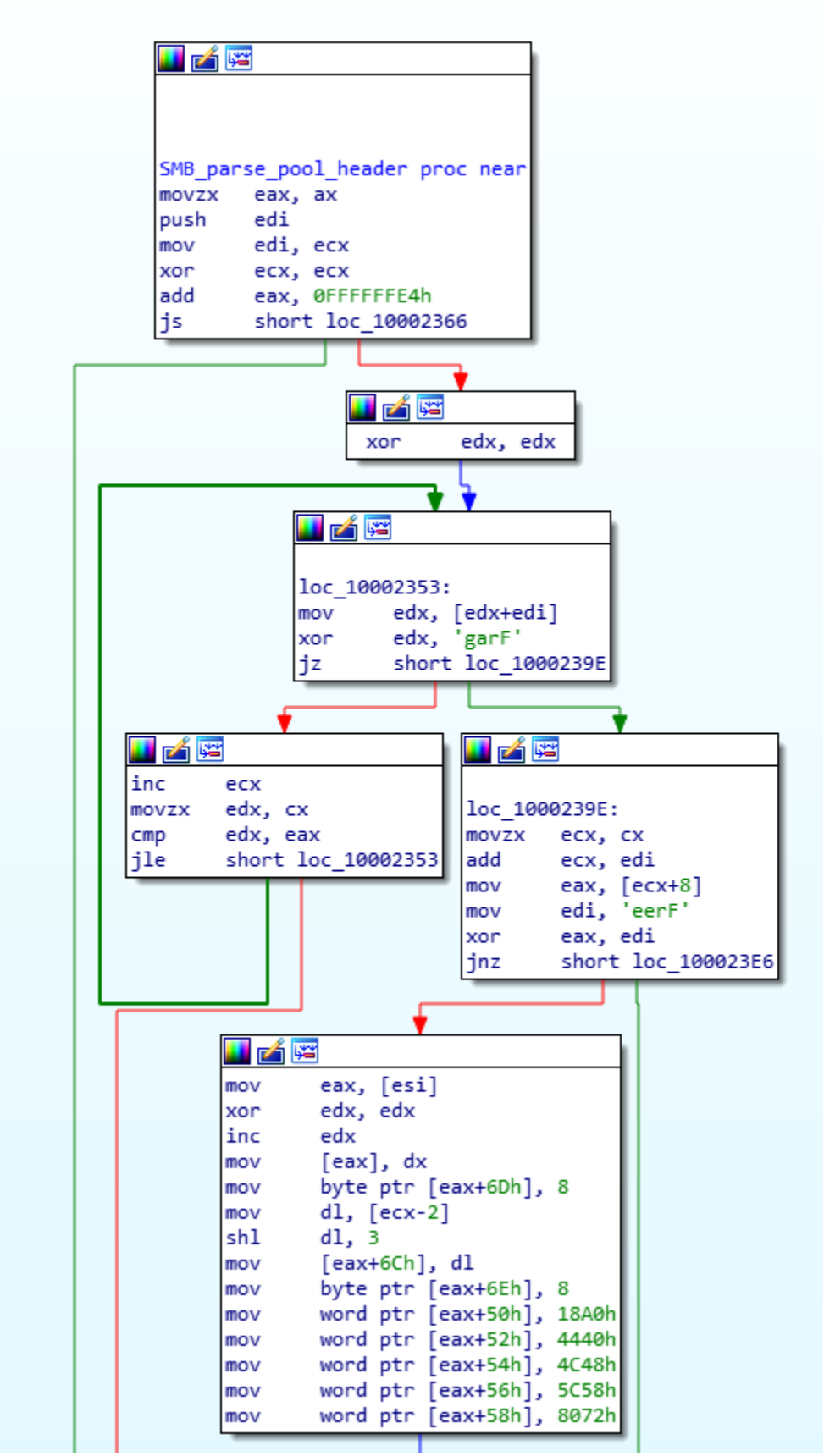
After updating the endian byte order and formatting to match a field in the WIN7_32_SESSION_INFO structure, the value is

```
0x001C022A, 0x00000001, 0x00000000, 0x00000000, 0x00000002, 0x00000000, 0x00000001
```

The extracted value matches the FAKE_SECCTX data in the publicly available EternalRomance exploit mentioned earlier:

```
109  WIN7_32_SESSION_INFO = {
110          'SESSION_SECCTX_OFFSET': 0x80,
111          'SESSION_ISNULL_OFFSET': 0x96,
112          'FAKE_SECCTX': pack('<IIIIIIB', 0x1c022a, 1, 0, 0, 2, 0, 1),
113          'SECCTX_SIZE': 0x1c,
114  }
```

The sample then parses an SMB response containing the kernel leak of the Frag pool structure:



Once again, the BadRabbit code matches the leak_frag_size() function in the public exploit.

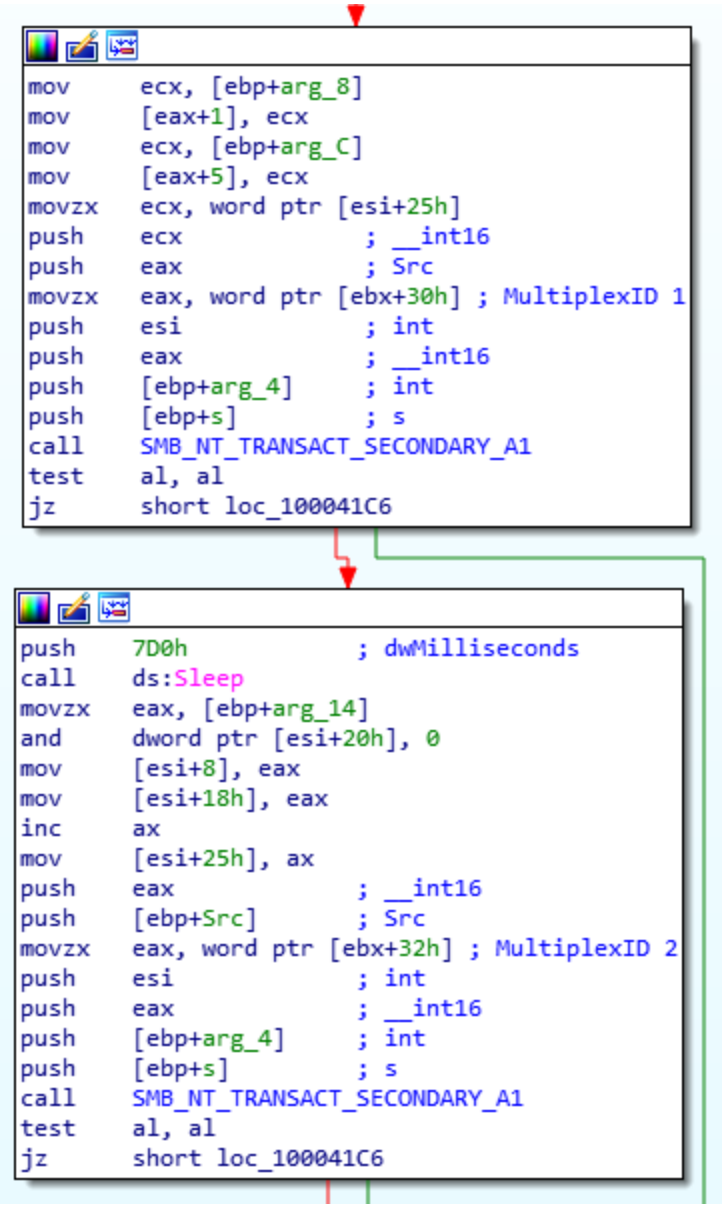
The sample also checks the NT status code on an NT_Trans request after attempting to modify the data in another Transaction structure:

```
call    q_SMB_NT_TRANSACT_A0
push    edi             ; lpMem
push    8               ; dwFlags
mov     [ebp+var_4], eax
call    ebx ; GetProcessHeap
push    eax             ; hHeap
call    ds:HeapFree
cmp     [ebp+var_4], 10002h ; NT_STATUS Invalied SMB if transaction modified
mov     [ebp+var_4], 0BADF00Dh
jz      kernel_write_success
```

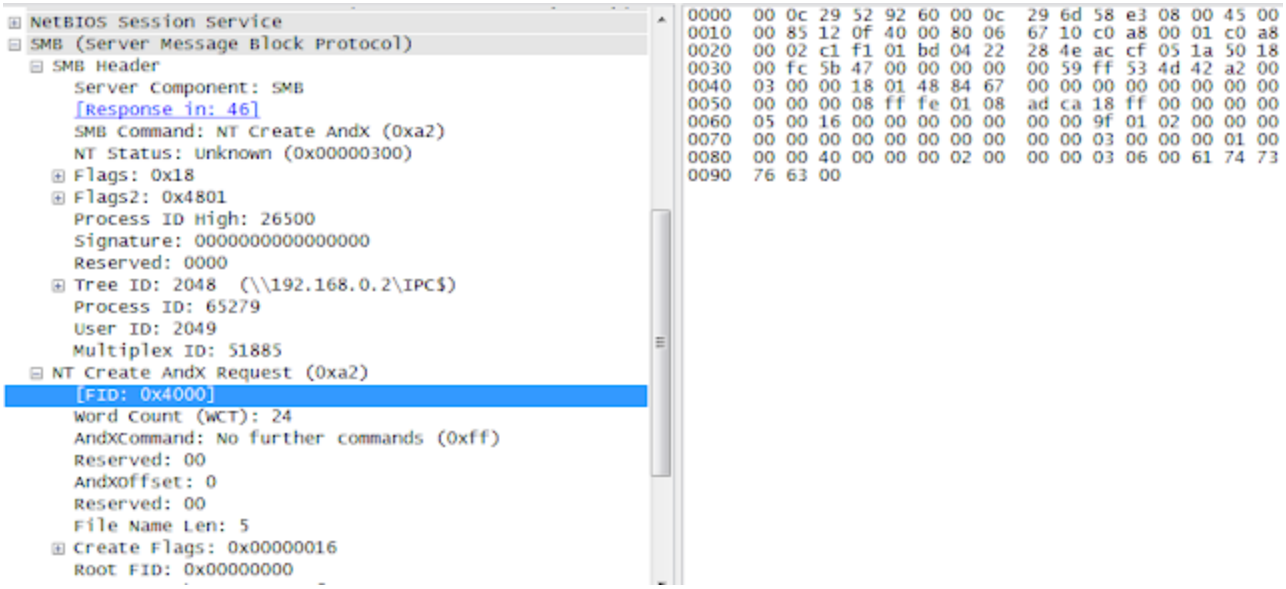
The same action is performed in the public exploit:

```
544         recvPkt = conn.send_nt_trans(5, mid=special_mid, param=pack('<HH', fid, 0), data='')
545         if recvPkt.getNTStatus() != 0x10002:  # invalid SMB
546                 print('unexpected return status: 0x{:x}'.format(recvPkt.getNTStatus()))
547                 print('!!! Write to wrong place !!!')
548                 print('the target might be crashed')
549                 return False
```

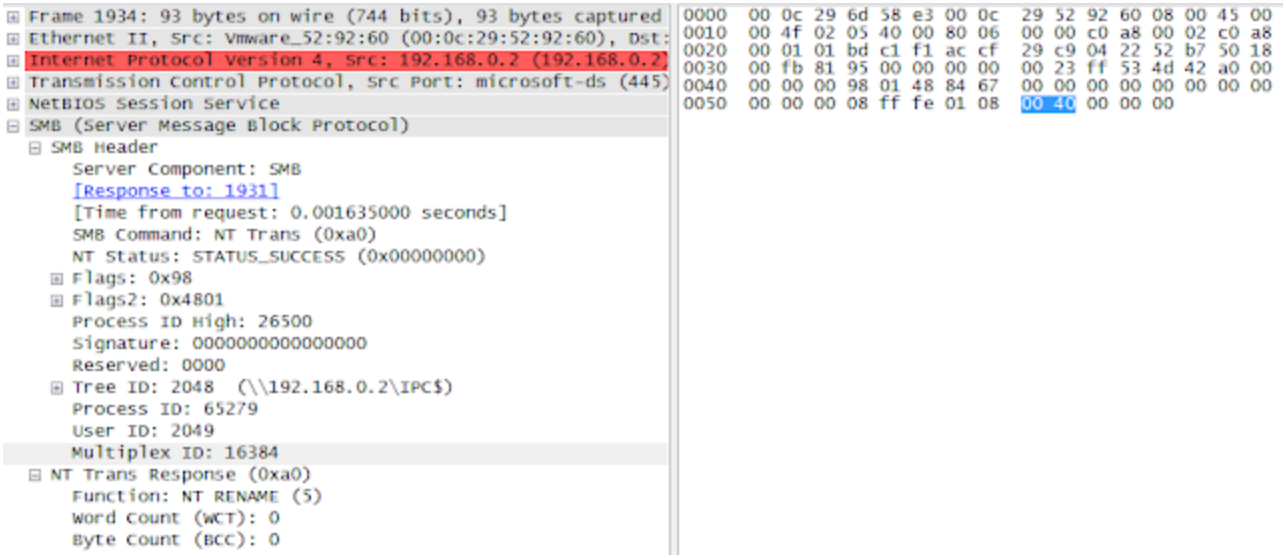
After the NT Trans check, the sample sends multiple NT_TRANSACT_SECONDARY commands using different MultiplexID values.



The equivalent is also performed by the public exploit Python script implementation in the function write_data(). Finally, we can confirm the findings of the static analysis by looking at the traffic generated by a pcap capture.



The sample first gets a FileID of 0x4000 and then the same value is used as a MultiplexID in an NT_Trans request:



Once again, this demonstrates a type confusion attempt similar to the one attempted by the EternalRomance exploit (the “Matched Pairs” technique). It matches the following Python code:

```
479   def exploit_matched_pairs(conn, pipe_name, info):
480           # for Windows 7/2008 R2 and later
481
482           tid = conn.tree_connect_andx('\\\\'+conn.get_remote_host()+'\\'+'IPC$')
483           conn.set_default_tid(tid)
484           # fid for first open is always 0x4000. We can open named pipe multiple times to get other fids.
485           fid = conn.nt_create_andx(tid, pipe_name)
486
487           info.update(leak_frag_size(conn, tid, fid))
488           # add os and arch specific exploit info
489           info.update(OS_ARCH_INFO[info['os']][info['arch']])
```

With all this in mind, we can be fairly confident that BadRabbit includes an EternalRomance implementation used to overwrite a kernel's session security context to enable it to launch remote services, while in Nyetya it was used to install the DoublePulsar backdoor. Both actions are possible due to the fact that EternalRomance allows the attacker to read/write arbitrary data into the kernel memory space.

Links Between Nyetya and BadRabbit

We assess with high confidence:

- that BadRabbit is built on the same core codebase as Nyetya.
- that the build tool chain for BadRabbit is highly similar to the build tool chain for Nyetya.

The evasion techniques present in the modifications to the DoublePulsar backdoor in Nyetya and EternalRomance in BadRabbit demonstrate similar, advanced, levels of understanding of the exploits involved, the network detections in place at the time of deployment, and general Windows kernel exploitation.

The shared codebase was modified for the BadRabbit build. Instead of leveraging PSEXEC, the remote file placement and remote Windows Service management was directly implemented. A second export was added to the dll that allows the remote execution to restart itself in a new rundll32 process, possibly to avoid having the parent process be clearly started as a service. The SMB implementation that Nyetya contained for leveraging SMB exploits has been replaced with an entirely different SMB implementation as well as a different exploitation technique. The post-reboot drive encryption with Petya has been replaced with drive encryption with the open source DiskCryptor.

Unmodified functionality from Nyetya includes the self-relocation of the malicious dll, process and thread token manipulations, network peer identification, and thread-safe collections for managing credentials and target information. Lightly modified functionality which demonstrates source level modifications are found in the flow of the malicious entrypoint, the interaction with the embedded and modified mimikatz, and in aspects of the system initialization and bitflag based feature control.

While these links are not absolute proof, based on these findings Talos assesses with low confidence that the authors of Nyetya and BadRabbit are the same.

Conclusion

This is yet another example of how effective ransomware can be delivered leveraging secondary propagation methods such as SMB to proliferate. In this example the initial vector wasn't a sophisticated supply chain attack. Instead it was a basic drive-by-download

leveraging compromised websites. This is quickly becoming the new normal for the threat landscape. Threats spreading quickly, for a short window, to inflict maximum damage. Ransomware is the threat of choice for both its monetary gain as well as destructive nature. As long as there is money to be made or destruction to be had these threats are going to continue.

This threat also amplifies another key area that needs to be addressed, user education. In this attack the user needs to facilitate the initial infection. If a user doesn't help the process along by installing the flash update it would be benign and not wreak the devastation it has across the region. Once a user facilitates the initial infection the malware leverages existing methods, such as SMB, to propagate around the network without user interaction.

Coverage

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	N/A
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such as NGFW, NGIPS, and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Email has not been identified as an attack vector at this time. The malware, if transferred across these systems on your networks, will be blocked.

Indicators of Compromise

Hashes (SHA256)

Dropper:

630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

Payload:

- 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93 C:\Windows\dispci.exe (diskcryptor client)
- 682ADCB55FE4649F7B22505A54A9DBC454B4090FC2BB84AF7DB5B0908F3B7806 C:\Windows\cscc.dat (x32 diskcryptor drv)
- 0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6 C:\Windows\cscc.dat (x64 diskcryptor drv)
- 579FD8A0385482FB4C789561A30B09F25671E86422F40EF5CCA2036B28F99648 C:\Windows\infpub.dat
- 2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035 (mimikatz-like x86)
- 301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c (mimikatz-like x64)

Scheduled Tasks names

- viserion_
- rhaegal
- drogon

Domains

Distribution domain:

1dnscontrol[.]com

Distribution Paths:

- /flash_install.php
- /index.php

Intermediary Server:

185.149.120[.]3

Referrer Sites:

- Argumentiru[.]com
- Fontanka[.]ru
- Adblibri[.]ro
- Spbvoditel[.]ru
- Grupovo[.]bg
- www.sinematurk[.]com

Hidden service:

caforssztxqzf2nm[.]onion