BleachGap Revamped

V labs.k7computing.com/index.php/bleachgap-revamped/

By Gaurav Yadav

August 25, 2022



BleachGap ransomware was first reported in Feb 2021 by a researcher named <u>Petrovic</u> on Twitter. This **ransomware variant** that we have analysed was reported on <u>Twitter</u> in June 2022. This variant got us curious to get into the nuances of it because it was tagged as a **stealer and all the code was compiled in a single executable thereby not needing any supporting**.bat or PowerShell scripts to execute, most probably done for evasion and to be less noisy in comparison to the variant found in 2021, which needed the supporting .bat and .exe that it dropped for execution.Though there are not many cases reported in the wild, this blog has been written to let the cyber community know that threat actors are modifying the attack techniques of this malware for a possible major attack that might be planned in the future. Lets now get into the details.

Why a Stealer?

When this ransomware executes, the first step is to get the username and generate a **Unique ID (UID)** and **Password** for that particular victim. By the first look, it seems it is stealing the password from the user but after multiple executions we identified that the password is different every time and after reversing the sample we found that the ransomware is using a function (shown in Figure 1) to randomly generate the UID and the same function is being called again to generate the password which is always 32 byte long.



Figure 1: Function used to generate random ID and Pass

After generating the UID and Password, it gets the Username of the current user using the environment variable. It first moves the encoded bytes to memory which are already hardcoded in the executable and then decodes those to the '**username**' and then uses it as an argument to get environment variable data related to the username as shown in Figure 2.

	0F9C992 34 61 0F9C994 8885 7DFFFFF 0F9C99A 8885 7DFFFFF 0F9C9A0 04 06 0F9C9A2 34 60 0F9C9A4 8885 7EFFFFF 0F9C9A4 8885 7EFFFFF 0F9C980 04 07 0F9C980 C445 80 00 19SC980 5305 0F9C980 5305 0F9C980 5305 0F9C980 8885 7EFFFFF 0F9C980 8885 7EFFFFFF 0F9C980 8885 7EFFFFFF 0F9C980 8885 7EFFFFFF 0F9C980 8885 7EFFFFFF	<pre>xor a1,61 mov byte ptr ss:[ebp-83],a1 mov eax,dword ptr ss:[ebp-86] add a1,6 xor a1,60 mov byte ptr ss:[ebp-82],a1 mov eax,dword ptr ss:[ebp-86] add a1,7 mov byte ptr ss:[ebp-80],0 xor edx,edx mov dx,byte ptr ss:[ebp-84],a1 mov a1,byte ptr ss:[ebp-86] xor byte ptr s</pre>	Moving encode	d bytes to memory
	019/02/000 8A8415 78FFFFF 019/02/07 8880 74FFFFFF 019/02/000 02CA 019/02/000 32C8 019/02/01 888C15 78FFFFFF 019/02/02/88 42 019/02/02/88 42 019/02/88	<pre>mov al,byte ptr sst[ebp+edx ss] mov ecx,dword ptr sst[ebp+edx add cl,d] xor cl,al mov byte ptr sst[ebp+edx-88],cl inc edx cmp edx,8 [b malware.F9C9D0] fea eax,dword ptr sst[ebp-88]</pre>		ecode encoded bytes to sername')
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	6736371 C019 00 00 079C9F8 50 079C9F9 E8 67A21100 079C9F8 88B0 079C376 88B0 079C376 88B0 079C376 88B0 079C310 C738 48FEFFFF 00000C 079C419 C738 52FFFFF 00000C 079C419 C788 52FFFFF 00 079C419 C788 54FEFFFF 00 079C423 C688 48FEFFFF 00 079C424 C688 48FEFFFF 00 079C49 C788 50 070C48 50	<pre>reak, used bp: ss.gebp=ss</pre>		get envirnoment variable username
xt:00F9C9D0 malware.exe:	BEF738 "zct`}uxs"]=7A 'z' \$5C9D0 #5BDD0	🖗 Watch 1 🛛 Izealis 🎾 Struct		
I ess Hex I ess Hex IEF734 00F 00 00 7A 63 IEF744 00 00 00 00 00 00 IEF754 04 01 00 00 A F7 IEF764 BC F7 BE 00 74 64 IEF774 0A 53 C3 74 55 63 IEF754 0A 00 00 00 00 A0 IEF754 0A 00 00 00 20 DA	74 60 7D 75 78 73 0 00 0 0 0 0	Encode	d bytes in memory	

Figure 2: Getting username using environment variables

Instead of hardcoding the useful strings into executables directly, so as to evade detection, this ransomware has used a similar method of moving encoded strings into memory and then decoding them at runtime for different purposes. We will see similar method being used later in this ransomware. After getting the Username, it forms a huge string using the same method of decoding the encoded bytes which includes UID, Password, Username as shown in Figure 3.

ress	ASCII	
1518 1558	00	
15D 161 165	<pre>@om.ord¥x.]!{"content":"**Su per duper good and jealous software**\n UID: NVFUJXey3ast71F2Wj k9\n Pass: Chdq00p5zvLxBAbngJ251w3LrcJRbsP7\n Username:</pre>	
169	.0.°.0.°.0.°.0.°.0.°.0.°.«««««««•¥x!	

Figure 3: Large

decoded string

After further analysis we learn that this ransomware sends the large decoded string shown in Figure 3 as a Post request to the Discord Webhook API which has been highlighted in Figure 4 and 5.

OOF9785 OOF9785 OOF9784 O	<pre>lea eax.dword prr ssiebp-LC4 push dword prr ssiebp-LC4 push dword prr ssiebp-LC4 push dword prr ssiebp-LC4 push dword prr ssiebp-LC4 push eax.dword prr ssiebp-LC4 mov eax.dword prr ssiebp-LC4 push eax push eax inder prossiebp-LC4 push eax mov dword prr ssiebp-LC4 push eax mov dword prr ssiebp-LC4 mov dword pre ssiebp-LC4 mo</pre>	<pre>[ebp+18]:"{\"content\":\"**Super duper good and function to send api webhookreqest Post request body as argument to function</pre>	51(1) 00000000000000000000000000000000000	rr2 Empty 0.0000000000000 (r3 Empty 0.000000000000 (r5 Empty 0.000000000000 (r5 Empty 0.0000000000000 (s\"**Super duper good at
Still Still <th< th=""><th></th><th>scord api</th><th>0085F284 00043 0085F285 00005 0085F285 00005 0085F290 0085F 0085F290 0085 0085F290 00050 0085F290 00050 0085F290 00050 0085F240 0085F 0085F240 0085F</th><th><pre>F30C "POST" Gaos "(\"Content\":\"==5 0008 Gaos "(\"Content\":\"==5 0000 0000 0000 0000 0000 0000 0000</pre></th></th<>		scord api	0085F284 00043 0085F285 00005 0085F285 00005 0085F290 0085F 0085F290 0085 0085F290 00050 0085F290 00050 0085F290 00050 0085F240 0085F 0085F240 0085F	<pre>F30C "POST" Gaos "(\"Content\":\"==5 0008 Gaos "(\"Content\":\"==5 0000 0000 0000 0000 0000 0000 0000</pre>

Figure 4: Post request to Discord API

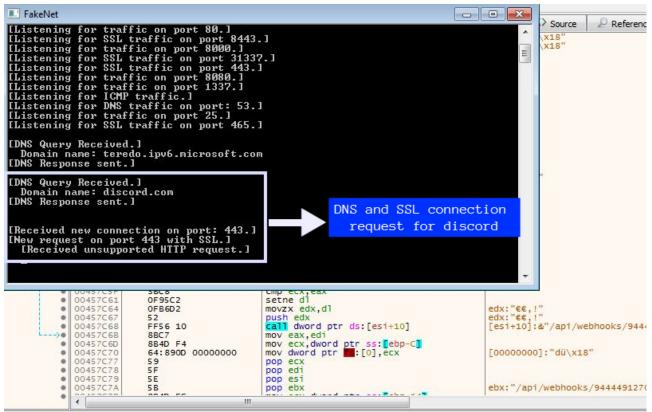


Figure 5: Fakenet output for DNS and SSL connection

Disabling Tools to Work

After sending information to the Discord API, the ransomware tries to disable tools like command prompt (CMD), Task Manager and Registry Editor so that the user is not able to make changes and stop the ransomware execution. Disabling the mentioned tools happens with the help of the registry. Ransomware first copies the encoded registry key into memory and then decodes the key using XOR loop and then does the same for key value and then calls the function **RegCreateKey** using the decoded key and value as arguments. Figure 6 shows the encoded registry key.

0	0045DC65	B9 E0146100	mov ecx,malware.6114E0	6114E0:&"C:\\Users										
:	0045DC6A 0045DC6F	E8 SCECFFFF	call malware.45C8D0											
	0045DC74	C68424 1C010000 5D	mov byte ptr ss:[esp+11C],5D	5D: '1'										
	0045DC7C	C68424 1D010000 79	mov byte ntr ss: [esp+110] 79											
•	0045DC84	C68424 1E010000 70	mov byte ptr ss: esp+11E,/0	79:'ý' 70:'p'										
	0045DC8C 0045DC94	C68424 1F010000 7E C68424 20010000 81	mov byte ptr ss:[esp+11F],7E	7E: '~'										
	0045DC94	C68424 20010000 81	mov byte ptr ss:[esp+120],81 mov byte ptr ss:[esp+121],68	6B: 'k'										
	0045DCA4	C68424 22010000 7C	mov byte ptr ss: [esp+122],7C	7C: '] '										
•	0045DCAC	C68424 23010000 6F	mov byte ptr ss:[esp+123],6F	6F: '0'										
	0045DCB4 0045DCBC	C68424 24010000 66 C68424 25010000 57	mov byte ptr ss: esp+124,66 mov byte ptr ss: esp+125,57	66:'f' 57:'W'										
	0045DCC4	C68424 26010000 73	mov byte ptr ss: [esp+126],73	73:'s'										
•	0045DCCC	C68424 27010000 6D	mov byte ptr ss:[esp+127],6D	6D: 'm'										
	0045DCD4 0045DCDC	C68424 28010000 7C C68424 29010000 79	mov byte ptr ss:[esp+128],7C mov byte ptr ss:[esp+129],79	7C:' ' 79:'y'										
	0045DCE4	C68424 24010000 7D	mov byte ptr ss:[esp+129],79 mov byte ptr ss:[esp+12A],7D	7D:'}}'										
	0045DCEC	C68424 2B010000 79		79: 'y'										
	0045DCF4	C68424 2C010000 70	mov byte ptr ss: esp+128,79 mov byte ptr ss: esp+12C,70 mov byte ptr ss: esp+12D,7E	70: 'p'										
	0045DCFC 0045DD04	C68424 2D010000 7E C68424 2E010000 66	mov byte ptr ss: esp+12D,7E mov byte ptr ss: esp+12E,66	7E:'~' 66:'f'										
	0045DD0C	C68424 2F010000 61	mov byte ptr ss: esp+12F1.61	61: 'a'										
•	0045DD14	C68424 30010000 73	mov byte ptr ss: esp+1301.73	73:'5'										
	0045DD1C	C68424 31010000 78	mov byte ptr ss: esp+131,78	78: 'X'										
	0045DD24 0045DD2C	C68424 32010000 6E C68424 33010000 79	mov byte ptr ss:[esp+132],6E mov byte ptr ss:[esp+133],79	6E:'n' 79:'y'										
	0045DD34	C68424 34010000 81	mov byte ptr ss: esp+134,81											
•	0045DD3C	C68424 35010000 7D	mov byte ptr ss:[esp+134],81 mov byte ptr ss:[esp+135],7D	7D:'}}' 66:'f'										
	0045DD44 0045DD4C	C68424 36010000 66 C68424 37010000 4D	mov byte ptr ss: esp+136,66	66:'f' 4D:'M'										
	0045DD54	C68424 38010000 7F	mov byte ptr ss: esp+137,4D mov byte ptr ss: esp+138,7F											
0	0045DD5C	C68424 39010000 7C	mov byte ptr ss:[esp+139],7C	7C: ' '										
•	0045DD64	C68424 3A010000 7C	mov byte ptr ss: esp+13A,7C	7C: ' '										
	0045DD6C 0045DD74	C68424 3B010000 6F C68424 3C010000 78	mov byte ptr ss: esp+138,6F mov byte ptr ss: esp+13C,78	6F:'0' 78:'x'										
	0045DD7C	C68424 3D010000 7E	mov byte ptr ss: esp+13D,7E	751										
	0045DD84	C68424 3E010000 60	mov byte ptr ss: esp+13E,60	60: 1										
	0045DD8C 0045DD94	C68424 3F010000 6F C68424 40010000 7C	mov byte ptr ss: esp+13F,6F mov byte ptr ss: esp+140,7C	6F:'0' 7C:' '										
	0045DD9C	C68424 41010000 7D	mov byte ptr ss:[esp+141],7D	7D:'}}'										
•	0045DDA4	C68424 42010000 73	mov byte ptr ss: esp+142,73	73:'5'										
:	0045DDAC 0045DDB4	C68424 43010000 79 C68424 44010000 78	mov byte ptr ss: esp+143,79	79: 'y' 78: 'x'										
	0045DDBC	C68424 45010000 66	mov byte ptr ss: esp+144,78 mov byte ptr ss: esp+145,66	66: 'f'										
•	0045DDC4	C68424 46010000 5A	mov byte ptr ss: esp+146,5A	5A: 'Z'										
	0045DDCC 0045DDD4	C68424 47010000 79 C68424 48010000 76	mov byte ptr ss: esp+147,79 mov byte ptr ss: esp+148,76	79: 'y' 76: 'y'										
	0045DDD4	C60424 45010000 75		73. 5										
	0045DDE4	C68424 4A010000 6D	mov byte ptr SS: esp+14A,6D	6D:'m'										
•	0045DDE4	C68424 4A010000 6D	mov byte ptr ss: esp+14A1,6D	6D:'m'										
•	0045DDE4	C68424 4A010000 6D	mov byte ptr ss: esp+14A1,6D mov byte ptr ss: esp+14A1,6D sted!!!! Encoded Regsitry key	6D:'m'										
byte ptr ss:[esp+14	0045DDE4 004EDDEC (4]=[0018FDC	C68424 4A010000 6D C68424 48010000 72 III A "les was been encryp	mov byte ptr ss: esp+14A1,6D	GD: 'm'										
byte ptr ss:[esp+14 6D 'm'	004500E4	C68424 4A010000 6D C68424 4B010000 73 III A "les was been encryp DE4 #5D1E4	being stored in memory	GD: 'm'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv	004500E4	C68424 4A010000 6D C68424 4B010000 73 III A "les was been encryp DE4 #5D1E4	<pre>prov byte ptr ss: esp+14A1,6D pted!!!! being stored in memory</pre>	6D: 'm' 77. 'e'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Ump 1 Ump Address	0045DDE4 0045DDE4 4A]=[0018FDC vare.exe:\$5D 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	C68424 4A010000 6D C68424 4B010000 73 III A "les was been encryp DE4 #5D1E4	mov byte ptr ss: esp+14A , 60 mov byte ptr ss: esp+14A , 60 sted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct Zyvs1 s was been encry	6D: 'm' 72. 's'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv .text:0045DDE4 malv .text:0045DDE4 malv .text:0045DDE4 malv .text:0045DDE4 malv .text:0045DDE4 malv	00450054 00450052 (↓ (↓ (↓ (↓) (↓) (↓) (↓) (↓) (C68424 4A010000 6D C68424 4B010000 73 III A "les was been encryp DE4 #5D1E4 p 3 000 Dump 4 000 Dur Sxny.}fM. 0x~`0 }syxfz	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted:::: Encoded Regsitry key being stored in memory mp 5 @ Watch 1 [x=]Locals 2 Struct Syvs] s was been encry ecurely with our	6D: 'm' 77. 'e'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD5 Dyp~.k[ofi 0018FD1 decryptor	0045DDE4 0045DDE4 (A) (A) (A) (A) (A) (A) (A) (A)	C68424 4A010000 6D C68424 48010000 73 III A "les was been encryp DE4 #5D1E4 p 3 J Dump 4 J Dum xny.}fM. ox~`o }syxf2 us an email to P2DqZHW	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted::::: Encoded Regsitry key being stored in memory mp 5 Watch 1	6D: 'm' 777 'e' C C C C C C C C										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD5 Dyp~.k[of) 0018FE1C decryptor 0018FE1C or to P2D0	0045DDE4 AA]=[0018FDC var e. exe: \$5D 0 2 ↓ Dum V5m y}yp~fas Send DTJ6L16H1q7a	C68424 4A010000 6D (68424 48010000 73 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dump xny.}fM. ox~`o }syxf2 us an email to P2DqZHW a@mail.a1.wtf) to recov	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted::::: Encoded Regsitry key being stored in memory mp 5 Watch 1	6D: 'm' 77 'c'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD5 Dyp~.k[ofi 0018FD1 decryptor	CO450014 On450014 On450014 A =[0018FDC var e. exe: \$50 2 @@ Dum Vsm y}yp~fas Send D136L16H1q72 led Regis Ov450000	C68424 4A010000 6D C68424 4A010000 6D III A "les was been encryp DE4 #5D1E4 p 3 U Dump 4 U Dur cxny.}fM.[ox~`o]}syxf2 us an email to P2Dq2HW a@mail.a1.wtf) to recov try key C68424 4F010000 5D	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 reading stored in memory being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct currely with our g28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+14F1, 50	6D: 'm' 77 'c'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv uppoump1 uppoump1 Address 0018FD5 uppo.k[off 0018FEC or to P200 Figure 6: Encod	0045DDE4 AA]=[0018FDC var e. exe: \$5D 0 2 ↓ Dum V5m y}yp~fas Send DTJ6L16H1q7a	C68424 4A010000 6D C68424 4B010000 6D III III III III III III III I	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 @ Watch 1 [x=]Locals 2 Struct yvs1 s was been encry ecurely with our g28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+14r, 50 mov byte ptr ss: esp+150, 83	6D: 'm' 72. 's' C C C C C C C C C C C C C C C C C C										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv U Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FD1 Dump* 0018FE1C decryptor 0018FE5C or to P2D0 Figure 6: Encod	00450034 00450034 (1) (4) (4) (4) (4) (4) (4) (4) (4	C68424 4A010000 6D C68424 4B010000 6D III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dum avny.}fM.[]ox~`o]}syxf2 us an email to P2Dq2HW a@mail.a1.wtf) to recov c68424 50010000 8D C68424 50010000 83 C68424 51010000 7D	mov byte ptr ss: esp+14A1, 60 mov byte ptr ss: esp+14A1, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals Struct gyvs] s was been encry ecurely with our gg28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 local structure for the st	6D: 'm' 772 'e' 6D: 'm' 772 'e' 6D: 'b' 6D: 'b' 7D: 'b' 7D: 'b' 7E: 'b' 7E: 'b'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv uppoump1 uppoump1 Address 0018FD5 uppo.k[off 0018FEC or to P200 Figure 6: Encod	00450034 00450034 (1) (4) (4) (4) (4) (4) (4) (4) (4	C68424 4A010000 6D C68424 4B010000 6D III III III III III III III I	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct yvs1 s was been encry ecurely with our g28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 7D ptr ss: esp+151, 7E ptr ss: esp+153, 6F	6D: 'm' 72. 'c' C C C C C C C C C C C C C C C C C C										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv U Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FD1 Dump* 0018FE1C decryptor 0018FE5C or to P2D0 Figure 6: Encod	00450034 00450034 (1) (4) (4) (4) (4) (4) (4) (4) (4	C68424 4A010000 6D C68424 4B010000 6D III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur axny.}fM.[]ox~`o]}syxf2 us an email to P2Dq2HW a@mail.a1.wtf) to recov c68424 50010000 8D C68424 50010000 83 C68424 51010000 7D	mov byte ptr ss: esp+14A1, 60 mov byte ptr ss: esp+14A1, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals Struct gyvs] s was been encry ecurely with our gg28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 local structure for the st	6D: 'm' 772 'e' 6D: 'm' 772 'e' 6D: 'b' 6D: 'b' 7D: 'b' 7D: 'b' 7E: 'b' 7E: 'b'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv U Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FD1 Dump* 0018FE1C decryptor 0018FE5C or to P2D0 Figure 6: Encod	Constant of the second s	C68424 4A010000 6D C68424 4B010000 6D III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur exny.}fM. ox~`o }syxfz us an email to P2Dq2HW amail.ai.wtf) to recov try key C68424 50010000 5D C68424 50010000 7D ry key Decoding C68424 55010000 00	mov byte ptr ss: esp+14A ,60 mov byte ptr ss: esp+14A ,60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct yvs1 s was been encry ecurely with our 1028A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+150 ,83 mov byte ptr ss: esp+151 ,70 ptr ss: esp+152 ,7E ptr ss: esp+153 ,6F mov byte ptr ss: esp+154 ,77 mov byte ptr ss: esp+155 ,0	6D: 'm' 72. 'c' 6D: 'J 7D: 'J 7D: 'J 7D: 'J 7D: 'J 7E: 'c' 6F; 'o'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FE1C decryptor 0018FE1C decryptor 0018FE1C decryptor	A)=[0018FDC AA]=[0018FDC var e. exe: \$5D 2	C68424 4A010000 6D C68424 4B010000 6D III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur exny.}fM. ox~`o }syxf2 us an email to P2Dq2HM a@mail.al.wtf) to recov C68424 50010000 5D C68424 50010000 5D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D	mov byte ptr ss: esp+14A1, 60 mov byte ptr ss: esp+14A1, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals Struct yvs] s was been encry ecurely with our Ig28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 72 ptr ss: esp+151, 70 ptr ss: esp+152, 72 ptr ss: esp+153, 6F mov byte ptr ss: esp+154, 77 mov byte ptr ss: esp+155, 0 xor ecx,ecx nop dword ptr ds:[eax],eax	6D: 'm' 72. 'c' 6D: 'J 7D: 'J 7D: 'J 7D: 'J 7D: 'J 7E: 'c' 6F; 'o'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FE1C decryptor 0018FE1C decryptor 0018FE1C decryptor	Vare.exe:\$50 2 U Dum Vare.exe:\$50 2 U Dum Vsm y}yp~fas send 0136L16H1q72 Ved Regist 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E35 00450E48 00450E48 00450E48 00450E48	C68424 4A010000 6D C68424 4B010000 6D III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~`o }syxfz us an email to P2DqZHW a@mail.a1.wtf) to recov try key C68424 50010000 5D C68424 50010000 7D c68424 50010000 7D c68424 50010000 00 33C9 061F00 8A840C 1C010000	mov byte ptr ss: esp+14A ,60 mov byte ptr ss: esp+14A ,60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct yvs] s was been encry ecurely with our 1028A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+150 ,83 mov byte ptr ss: esp+151 ,70 ptr ss: esp+152 ,76 ptr ss: esp+152 ,66 mov byte ptr ss: esp+154 ,77 mov byte ptr ss: esp+154 ,77 mov byte ptr ss: esp+155 ,0 xor ecx,ecx nop dword ptr ds:[eax],eax mov al,byte ptr ss: esp+ecx+11C]	6D: 'm' 72. 'c' 6D: 'J 7D: 'J 7D: 'J 7D: 'J 7D: 'J 7E: 'c' 6F; 'o'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FE1C decryptor 0018FE1C decryptor 0018FE1C decryptor	A)=[0018FDC AA]=[0018FDC Var e. exe: \$5D 2	C68424 4A010000 6D C68424 4A010000 6D W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dum xny.}fM.[]ox~`o]}syxf2 us an email to P2DqZHW Remail.a1.wtf) to recov C68424 50010000 83 C68424 50010000 83 C68424 50010000 83 C68424 50010000 83 C68424 50010000 00 33C9 OFIF00 8A840C 1C010000 2C 0A	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 ptr ss: esp+152, 72 ptr ss: esp+152, 72 ptr ss: esp+152, 75 mov byte ptr ss: esp+152, 75 ptr ss: esp+152, 75 mov byte ptr ss: esp	6D: 'm' 72. 'c' 6D: 'J 7D: 'J 7D: 'J 7D: 'J 7D: 'J 7E: 'c' 6F; 'o'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod	Construction	C68424 4A010000 6D C68424 4B010000 6D W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~`o }syxfz us an email to P2DqZHM amail.ai.wtf) to recov try key C68424 5010000 5D C68424 5010000 7D C68424 5010000 7D C68424 5010000 7D C68424 5010000 7D C68424 5010000 00 33C9 OF1F00 8A840C 1C010000 2C 0A 88840C 1C010000 41	mov byte ptr ss: esp+144, 60 mov byte ptr ss: esp+146, 72 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct yvs] s was been encry ecurely with our Mg28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+151, 7D ptr ss: esp+152, 7E mov byte ptr ss: esp+154, 77 mov byte ptr ss: esp+ex+11C], al inc ecx	6D: 'm' 72. 'c' 72. 'c' 6D: 'J 7D: 'J 7D: 'J 7E: 'c' 6F: 'c' 77: 'w'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod	A A A A A A A A A A	C68424 4A010000 6D (68424 4A010000 6D (68424 4B010000 72 W (A "les was been encryp (DE4 #5D1E4 p 3 Dump 4 Dum (SXNY.}fM.[]0x~`0]}syxf2 Us an email to P2DqZHW (SAMA) to recove (SAMA)	mov byte ptr ss: esp+144, 60 mov byte ptr ss: esp+146, 77 being stored in memory mp 5 Watch 1 [x=]Locals Struct yvs] s was been encry ecurely with our 10288265z@postheo.de (yvs] s was been encry ecurely with our 102882652@postheo.de (yvs] s was been encry ecurely with our 102882652@postheo.de (yvs] s was been encry ecurely with our 102882652@postheo.de (yvs] s was been encry 102882652@postheo.de (yvs] s was been encry 102882652@postheo.de (yvs] s was been encry 102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@postheo.de (102882652@pos	60: 'm' 72: 'c' 60: 'm' 60: 'm' 60: 'a' 60: 'a' 70: '} 70: '} 70: '} 70: '} 70: '} 70: '} 70: '} 70: '} 70: 'a' 77: 'w' 39: '9'										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod	A A A A A A A A A A	C68424 4A010000 6D C68424 4B010000 6D W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~`o }syxfz us an email to P2DqZHM amail.ai.wtf) to recov try key C68424 5010000 5D C68424 5010000 7D C68424 5010000 7D C68424 5010000 7D C68424 5010000 7D C68424 5010000 00 33C9 OF1F00 8A840C 1C010000 2C 0A 88840C 1C010000 41	mov byte ptr ss: esp+144, 60 mov byte ptr ss: esp+146, 72 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct yvs] s was been encry ecurely with our Mg28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+151, 7D ptr ss: esp+152, 7E mov byte ptr ss: esp+154, 77 mov byte ptr ss: esp+ex+11C], al inc ecx	6D: 'm' 772 'c' 772 'c' C C C C C C C C C C C C C C C C C C										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FEC or to P2D0 Figure 6: Encod	004500344 004500344 004500344 00450034 02 02 03 0450034 0450034 0450034 0450034 00450344 00450344	C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 (C6424 4E010000 72 (DE4 #5D1E4 p 3 Dump 4 Dum (DE4 #5D1E4 p 3 Dump 4 Dum (C6424 #5D10000 8D (C6424 50010000 00 (C6424 500000 00 (C6424 5000000 00 (C6424 5000000 00 (C6424 500000 00 (C6424 5000000 00 (C6424 5000000 00 (C6424 50000000000000000 (C6424 500000000000000000000000000000000000	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals Struct yvs] s was been encry ecurely with our 1028A2652@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 ptr ss: esp+152, 72 ptr ss: esp+153, 6F mov byte ptr ss: esp+153, 0 xor ecx, ecx mov al, byte ptr ss: [esp+154], 70 sub al, A mov byte ptr ss: [esp+ecx+11C], al inc ecx cmp ecx, 39]b malware. 45DE50 sub esp.18	60: 'm' 72: 'c' 60: 'm' 60: 'm' 60: 'a' 60: 'a' 70: '} 70: '} 70: '} 70: '} 70: '} 70: '} 70: '} 70: '} 70: 'a' 77: 'w' 39: '9'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FEC or to P2D0 Figure 6: Encod	00450034 00450034 00450034 1 4A]=[0018FDC vare.exe:\$50 2 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E15 00450E16 00450E16 00450E50 0045	C68424 4A010000 6D C68424 4B010000 6D W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~`o }syxfz us an email to P2DqZHM amail.al.wtf) to recov try key C68424 50010000 5D C68424 50010000 7D C68424 50000000 7D C68424 50	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals 2 Struct yvs] s was been encry ecurely with our Mg28A265z@postheo.de (/er your filesYou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E Noop byte ptr ss: esp+151,7D ptr ss: esp+152,7E Noop byte ptr ss: esp+154,77 mov byte ptr ss: esp+154,77 mov byte ptr ss: esp+154,77 mov byte ptr ss: [esp+ex+11C] sub al,A mov byte ptr ss: [esp+ex+11C],al inc ecx cmp ecx,39 jb malware.45DE50 sub eso.18	60: 'm' 72: 'c' 72: 'c' 60: 'J 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J 77: 'w'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FEC or to P2D0 Figure 6: Encod	00450034 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004 0045004	C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 (C6424 550164 p 3 Dump 4 Dum (C6424 550164 p 3 Dump 4 Dum (C6424 55010000 83 C68424 5001000 83 C68424 50010000 83 C68424 51010000 83 C68424 51010000 83 C68424 55010000 83 C68424 55010000 00 (C6424 5500000 00 (C6424 55000000 00 (C6424	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals Struct yvs] s was been encry ecurely with our 1028A2652@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 ptr ss: esp+152, 72 ptr ss: esp+153, 6F mov byte ptr ss: esp+153, 0 xor ecx, ecx mov al, byte ptr ss: [esp+154], 70 sub al, A mov byte ptr ss: [esp+ecx+11C], al inc ecx cmp ecx, 39]b malware. 45DE50 sub esp.18	60: 'm' 72: 'c' 72: 'c' 60: 'J 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J} 70: 'J 77: 'w'										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.kloft 0018FEC decryptor 0018FEC or to P2D0 Figure 6: Encod	00450034 A Image: A Imag	C68424 4A010000 6D (C6424 4B010000 6D (C6424 4B010000 72 W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur exny.}fM.[]ox~`o]}syxf2 us an email to P2Dq2HW agmail.a1.wtf) to recov try key C68424 50010000 83 C68424 51010000 83 C68424 51010000 7D C68424 51010000 7D C68424 55010000 00 33C9 0F1F00 8A840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 41 83F9 39 72 EA 835C 18 805424 51010000 88844 W	mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 [x=]Locals Struct yvs] s was been encry ecurely with our 1028A2652@postheo.de (/er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 ptr ss: esp+152, 72 ptr ss: esp+153, 6F mov byte ptr ss: esp+153, 0 xor ecx, ecx mov al, byte ptr ss: [esp+154], 70 sub al, A mov byte ptr ss: [esp+ecx+11C], al inc ecx cmp ecx, 39]b malware. 45DE50 sub esp.18	6D: 'm' 72: 'c' 72: 'c' 6C C C C C C C C C C C C C C C C C C C										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FEC or to P200 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw	00450034 00450034 00450034 4A] = [0018FDC var e. exe: \$500 02 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E30 00450E31 00450E50 00450E50 00450E61 00450E61 00450E61 00450E70 0450E70 0450E70	C68424 4A010000 6D C68424 4B010000 6D W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~`o }syxf2 us an email to P2Dq2HM admail.al.wtf) to recov try key C68424 5010000 83 C68424 5010000 83 C68424 51010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 83 C68424 5100000 83 C68424 51000000000000000000000000000000000000	<pre>mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 ptr being stored in memory mp5 Watch 1 [x=]Locals Struct yvs1 s was been encry ecurely with our g28A265z@postheo.de (//r your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 ptr ss: esp+152, 72 ptr ss: esp+153, 66 mov byte ptr ss: esp+154, 77 mov byte ptr ss: esp+154, 77</pre>	6D: 'm' 72: 'c' 72: 'c' 6C C C C C C C C C C C C C C C C C C C										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Dyp~.k[off 0018FEC or to P200 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw Dump 1 Dump	00450034 00450034 00450034 4A] = [0018FDC var e. exe: \$500 02 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E14 00450E30 00450E31 00450E50 00450E50 00450E61 00450E61 00450E61 00450E70 0450E70 0450E70	C68424 4A010000 6D C68424 4B010000 6D W A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~`o }syxf2 us an email to P2Dq2HM admail.al.wtf) to recov try key C68424 5010000 83 C68424 5010000 83 C68424 51010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 83 C68424 5100000 83 C68424 51000000000000000000000000000000000000	<pre>mov byte ptr ss: esp+14A, 60 mov byte ptr ss: esp+14A, 60 ptroverse ptr</pre>	GD: 'm' 772''c' CC CC CC CC CC CC CC CC CC CC CC CC CC										
byte ptr ss:[esp+14 6D 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD9 Uyp~.k off 0018FEC or to P2D0 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw U Dump 1 U Dump Address roots	00450034 00450034 00450034 00450034 02 0018FDC 02 0018FDC 02 0018FDC 02 0018FDC 03 0136116H1q72 0450E14 00450E14 00450E34 00450E35 00450E34 00450E50 00450E50 00450E50 <t< td=""><td>C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 III A "les was been encryp DE4 #5D1E4 p 3 J Dump 4 J Dum Dump 4 J Dum (C68424 #5D10000 83 C68424 50010000 83 C68424 50010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 00 33C9 OF1F00 8A840C 1C010000 2 C0A 88840C 1C010000 2 C0A 88840C 1C010000 41 83F9 39 72 EA 83EC 18 805C24 54010000 8804 III III III III III III III I</td><td>mov byte ptr ss: esp:14A, 60 mov byte ptr ss: esp:14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 @ Watch 1 [x=]Locals @ Struct cyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/ er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 pcf ss: esp+152, 77 ptr mov byte ptr ss: esp+153, 65 mov byte ptr ss: esp+154, 77 mov byte ptr ss: esp+152, 72 mov byte ptr ss: esp+152, 162 mov dive ptr ss: esp+152, 162 mov dive ptr ss: esp+ex+110 mov dive ptr ss: esp+154, 163 inc ex ex ex mov di</td><td>GD: 'm' 772''c' CC CC CC CC CC CC CC CC CC CC CC CC CC</td></t<>	C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 III A "les was been encryp DE4 #5D1E4 p 3 J Dump 4 J Dum Dump 4 J Dum (C68424 #5D10000 83 C68424 50010000 83 C68424 50010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 00 33C9 OF1F00 8A840C 1C010000 2 C0A 88840C 1C010000 2 C0A 88840C 1C010000 41 83F9 39 72 EA 83EC 18 805C24 54010000 8804 III III III III III III III I	mov byte ptr ss: esp:14A, 60 mov byte ptr ss: esp:14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 @ Watch 1 [x=]Locals @ Struct cyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/ er your filesYou mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+150, 83 mov byte ptr ss: esp+151, 70 pcf ss: esp+152, 77 ptr mov byte ptr ss: esp+153, 65 mov byte ptr ss: esp+154, 77 mov byte ptr ss: esp+152, 72 mov byte ptr ss: esp+152, 162 mov dive ptr ss: esp+152, 162 mov dive ptr ss: esp+ex+110 mov dive ptr ss: esp+154, 163 inc ex ex ex mov di	GD: 'm' 772''c' CC CC CC CC CC CC CC CC CC CC CC CC CC										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD0 Typk[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw Dump 1 Dump 1 Dump Address Software/M	004500341 A Image: A <tr td=""> <!--</td--><td>C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 III A "les was been encryp DE4 #5D1E4 p 3 J Dump 4 J Dum Dump 4 J Dum (C68424 #5D10000 83 C68424 50010000 83 C68424 50010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 00 33C9 OF1F00 8A840C 1C010000 2 C0A 88840C 1C010000 2 C0A 88840C 1C010000 41 83F9 39 72 EA 83EC 18 805C24 54010000 8804 III III III III III III III I</td><td>mov byte ptr ss: esp:14A, 60 mov byte ptr ss: esp:14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 Ix=lLocals 2 Struct yvs1 s was been encry ecurely with our g28A2652@postheo.de (mov byte ptr ss: esp:150, 83 mov byte ptr ss: esp:151, 70 mov byte ptr ss: esp:152, 72 mov byte ptr ss: esp:153, 6F mov byte ptr ss: esp:155, 0 xor ecx,ecx nov byte ptr nov di, byte ptr ss: [esp+155], 0 xor ecx,ecx nov al, byte ptr ss: [esp+155], 0 xor ecx,ecx mov al, byte ptr ss: [esp+ecx+11C], al inc ecx,doword ptr ss: [esp+154], mov ecx,ecx mov byte ptr ss: esp+ecx+11C], al inc ecx,ecx <tr< td=""><td>60: 'm' 772: 'c' 772: 'j' 50: j 70: 'j' 75: 'o' 77: 'w' 39: '9' Software\Microsoft\Wi 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018</td></tr<></td></tr> <tr><td>byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD9 Dyp~.k[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw U Dump 1 U Dump Address South 0018FD9 Dump 1 U Dump Address South 0018FD9 Dump 1 U Dump</td><td>00450034 00450034 00450034 4A] = [0018FDC var e. exe: \$500 02 00450E14 00450E30 00450E50 00450E61 00450E61 00450E62 00450E63 00450E64 00450E50 00450E61 00450E63 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E67 00450E67 00450E67 00450E67 00450E67 00450E67 00450E70 4</td><td>C68424 4A010000 6D (C6424 4B010000 6D (C6424 4B010000 72 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dum Exny.}fM. ox~`o }syxfz us an email to P2Dq2HW agmail.a1.wtf) to recov try key C68424 50010000 5D C68424 50010000 7D C68424 50010000 7D C68424 50010000 7D C68424 50010000 7D C68424 50010000 00 33C9 OFIF00 8A840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 885C 18 005C24 54010000 8894 III III E66 #5D266 3 UD Dump 4 UD Dump hdows\CurrentVersion\P0</td><td>mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]</td><td>60:'m' 772''c' 50: j 70: 'j) 70: 'j) 70: 'j) 77: 'w' 39: '9' Software\Microsoft\wi 0018 0018 0018 0018 0018 0018</td></tr> <tr><td>byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Jypk off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod .text:0045DE66 malw Dump 1 Dump Address .text:0045DE66 malw Dump 1 Dump</td><td>00450034 00450034 00450034 4 1 4 1 02 1 02 1 02 1 03 04 05 04 05 06 07 06 07 06 07 06 07 06 07 07 08 09 00450 <!--</td--><td>C68424 4A010000 6D (58424 4B010000 6D (58424 4B010000 73 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~'o }syxfz us an email to P2DqZHW amail.ai.wtf) to recov itry key C68424 50010000 8J C68424 50010000 7D C68424 500000 7D C68424 5000000 7D C68424 70 7</td><td>mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]</td><td>60:'m' 772''c' C C C C C C C C C C C C C C C C C C</td></td></tr>	C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 III A "les was been encryp DE4 #5D1E4 p 3 J Dump 4 J Dum Dump 4 J Dum (C68424 #5D10000 83 C68424 50010000 83 C68424 50010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 00 33C9 OF1F00 8A840C 1C010000 2 C0A 88840C 1C010000 2 C0A 88840C 1C010000 41 83F9 39 72 EA 83EC 18 805C24 54010000 8804 III III III III III III III I	mov byte ptr ss: esp:14A, 60 mov byte ptr ss: esp:14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 Ix=lLocals 2 Struct yvs1 s was been encry ecurely with our g28A2652@postheo.de (mov byte ptr ss: esp:150, 83 mov byte ptr ss: esp:151, 70 mov byte ptr ss: esp:152, 72 mov byte ptr ss: esp:153, 6F mov byte ptr ss: esp:155, 0 xor ecx,ecx nov byte ptr nov di, byte ptr ss: [esp+155], 0 xor ecx,ecx nov al, byte ptr ss: [esp+155], 0 xor ecx,ecx mov al, byte ptr ss: [esp+ecx+11C], al inc ecx,doword ptr ss: [esp+154], mov ecx,ecx mov byte ptr ss: esp+ecx+11C], al inc ecx,ecx <tr< td=""><td>60: 'm' 772: 'c' 772: 'j' 50: j 70: 'j' 75: 'o' 77: 'w' 39: '9' Software\Microsoft\Wi 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018</td></tr<>	60: 'm' 772: 'c' 772: 'j' 50: j 70: 'j' 75: 'o' 77: 'w' 39: '9' Software\Microsoft\Wi 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018	byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD9 Dyp~.k[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw U Dump 1 U Dump Address South 0018FD9 Dump 1 U Dump Address South 0018FD9 Dump 1 U Dump	00450034 00450034 00450034 4A] = [0018FDC var e. exe: \$500 02 00450E14 00450E30 00450E50 00450E61 00450E61 00450E62 00450E63 00450E64 00450E50 00450E61 00450E63 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E67 00450E67 00450E67 00450E67 00450E67 00450E67 00450E70 4	C68424 4A010000 6D (C6424 4B010000 6D (C6424 4B010000 72 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dum Exny.}fM. ox~`o }syxfz us an email to P2Dq2HW agmail.a1.wtf) to recov try key C68424 50010000 5D C68424 50010000 7D C68424 50010000 7D C68424 50010000 7D C68424 50010000 7D C68424 50010000 00 33C9 OFIF00 8A840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 885C 18 005C24 54010000 8894 III III E66 #5D266 3 UD Dump 4 UD Dump hdows\CurrentVersion\P0	mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]	60:'m' 772''c' 50: j 70: 'j) 70: 'j) 70: 'j) 77: 'w' 39: '9' Software\Microsoft\wi 0018 0018 0018 0018 0018 0018	byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Jypk off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod .text:0045DE66 malw Dump 1 Dump Address .text:0045DE66 malw Dump 1 Dump	00450034 00450034 00450034 4 1 4 1 02 1 02 1 02 1 03 04 05 04 05 06 07 06 07 06 07 06 07 06 07 07 08 09 00450 </td <td>C68424 4A010000 6D (58424 4B010000 6D (58424 4B010000 73 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~'o }syxfz us an email to P2DqZHW amail.ai.wtf) to recov itry key C68424 50010000 8J C68424 50010000 7D C68424 500000 7D C68424 5000000 7D C68424 70 7</td> <td>mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]</td> <td>60:'m' 772''c' C C C C C C C C C C C C C C C C C C</td>	C68424 4A010000 6D (58424 4B010000 6D (58424 4B010000 73 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~'o }syxfz us an email to P2DqZHW amail.ai.wtf) to recov itry key C68424 50010000 8J C68424 50010000 7D C68424 500000 7D C68424 5000000 7D C68424 70 7	mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]	60:'m' 772''c' C C C C C C C C C C C C C C C C C C
C68424 4A010000 6D (C6424 4E010000 6D (C6424 4E010000 72 III A "les was been encryp DE4 #5D1E4 p 3 J Dump 4 J Dum Dump 4 J Dum (C68424 #5D10000 83 C68424 50010000 83 C68424 50010000 83 C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 7D C68424 51010000 00 33C9 OF1F00 8A840C 1C010000 2 C0A 88840C 1C010000 2 C0A 88840C 1C010000 41 83F9 39 72 EA 83EC 18 805C24 54010000 8804 III III III III III III III I	mov byte ptr ss: esp:14A, 60 mov byte ptr ss: esp:14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 Ix=lLocals 2 Struct yvs1 s was been encry ecurely with our g28A2652@postheo.de (mov byte ptr ss: esp:150, 83 mov byte ptr ss: esp:151, 70 mov byte ptr ss: esp:152, 72 mov byte ptr ss: esp:153, 6F mov byte ptr ss: esp:155, 0 xor ecx,ecx nov byte ptr nov di, byte ptr ss: [esp+155], 0 xor ecx,ecx nov al, byte ptr ss: [esp+155], 0 xor ecx,ecx mov al, byte ptr ss: [esp+ecx+11C], al inc ecx,doword ptr ss: [esp+154], mov ecx,ecx mov byte ptr ss: esp+ecx+11C], al inc ecx,ecx <tr< td=""><td>60: 'm' 772: 'c' 772: 'j' 50: j 70: 'j' 75: 'o' 77: 'w' 39: '9' Software\Microsoft\Wi 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018</td></tr<>	60: 'm' 772: 'c' 772: 'j' 50: j 70: 'j' 75: 'o' 77: 'w' 39: '9' Software\Microsoft\Wi 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018 0018												
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv U Dump 1 U Dump Address 0018FD9 Dyp~.k[off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod esp=0018FC80 .text:0045DE66 malw U Dump 1 U Dump Address South 0018FD9 Dump 1 U Dump Address South 0018FD9 Dump 1 U Dump	00450034 00450034 00450034 4A] = [0018FDC var e. exe: \$500 02 00450E14 00450E30 00450E50 00450E61 00450E61 00450E62 00450E63 00450E64 00450E50 00450E61 00450E63 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E64 00450E65 00450E67 00450E67 00450E67 00450E67 00450E67 00450E67 00450E70 4	C68424 4A010000 6D (C6424 4B010000 6D (C6424 4B010000 72 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dum Exny.}fM. ox~`o }syxfz us an email to P2Dq2HW agmail.a1.wtf) to recov try key C68424 50010000 5D C68424 50010000 7D C68424 50010000 7D C68424 50010000 7D C68424 50010000 7D C68424 50010000 00 33C9 OFIF00 8A840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 88840C 1C010000 2C 0A 885C 18 005C24 54010000 8894 III III E66 #5D266 3 UD Dump 4 UD Dump hdows\CurrentVersion\P0	mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]	60:'m' 772''c' 50: j 70: 'j) 70: 'j) 70: 'j) 77: 'w' 39: '9' Software\Microsoft\wi 0018 0018 0018 0018 0018 0018										
byte ptr ss:[esp+14 GD 'm' .text:0045DDE4 malv Dump 1 Dump Address 0018FD9 Jypk off 0018FEC decryptor 0018FEC or to P200 Figure 6: Encod Figure 6: Encod .text:0045DE66 malw Dump 1 Dump Address .text:0045DE66 malw Dump 1 Dump	00450034 00450034 00450034 4 1 4 1 02 1 02 1 02 1 03 04 05 04 05 06 07 06 07 06 07 06 07 06 07 07 08 09 00450 </td <td>C68424 4A010000 6D (58424 4B010000 6D (58424 4B010000 73 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~'o }syxfz us an email to P2DqZHW amail.ai.wtf) to recov itry key C68424 50010000 8J C68424 50010000 7D C68424 500000 7D C68424 5000000 7D C68424 70 7</td> <td>mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]</td> <td>60:'m' 772''c' C C C C C C C C C C C C C C C C C C</td>	C68424 4A010000 6D (58424 4B010000 6D (58424 4B010000 73 III A "les was been encryp DE4 #5D1E4 p 3 Dump 4 Dur sxny.}fM. ox~'o }syxfz us an email to P2DqZHW amail.ai.wtf) to recov itry key C68424 50010000 8J C68424 50010000 7D C68424 500000 7D C68424 5000000 7D C68424 70 7	mov byte ptr ss: esp+14A, 60 pted!!!! Encoded Regsitry key being stored in memory mp 5 Watch 1 rs=lLocals Struct gyvs1 s was been encry ecurely with our ig28A265z@postheo.de (/er your filesyou mov byte ptr ss: esp+151,7D ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E ptr ss: esp+152,7E iov byte ptr ss: [esp+152,7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7D ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],7E ptr ss: [esp+152],6F inv byte ptr ss: [esp+152],7E ptr sss: [esp+152],7E ptr ss: [esp+152],7E ptr sss: [esp+152]	60:'m' 772''c' C C C C C C C C C C C C C C C C C C										

Figure 7: Decoding encoded registry key

8:38:3 Imalware.exe 8:38:3 Imalware.exe 8:38:4 Imalware.exe	1224 KegCreateKey 1224 RegSetValue 1224 RegCreateKey	HKLU\Software\Microsoft\Windows\Lurre HKCU\Software\Microsoft\Windows\Curre HKCU\Software\Policies\Microsoft\Windo	ntVersion\Policies\System\DisableTa ws\System	iskmgr	SUCCESS SUCCESS SUCCESS	Desired Access: A Type: REG_DWO Desired Access: A
8:38:4 Imalware.exe	1224 RegSetValue	HKCU\Software\Policies\Microsoft\Windo		Registry	keys gett	ing created
8:39:2 Imalware.exe	1224 RegCreateKey			shown by	procmon	
8:39:2 I malware.exe 8:39:2 I malware.exe	1224 RegSetValue 1224 RegCreateKey	HKCU\Software\Microsoft\Windows\Curre HKCU\Software\Microsoft\Windows\Curre		Shown by	SUCCESS	Desired Access: A
8:39:2 malware exe	1224 RegSetValue	HKCU/Software/Microsoft/Windows/Curre HKCU/Software/Microsoft/Windows/Curre		anistry Tools	SUCCESS	Type: REG DWO
o.oo.c				gally room	0000200	1)20.1120_0110
C:\Windows\system32	2\cmd.exe					
Microsoft Windows	[Version 6.1.7601] ation. All rights reserved	*			
			E			
The command promp	t has been disable	d by your administrator.				try editor
Press any key to	continue			got	disabled	
. 이번 이 이번 10년 19일 17일 18일 17일 19일 19일 19일						
		😢 Registry Editor	23			
		Registry editing has been disal	oled by your administrator.	6		
						4
		•		0018FC68	650FC34	•
		W		0018FC6C 0	018FD48 "Docur	ments"
		W	ОК	0018FC6C 0 0018FC70 0 0018FC74 0	0018FD48 "Docum 0027B4C0 "C:\\ 00000010	ments" Users\\K7User\\'
		0		0018FC6C 0018FC70 0	0018FD48 "Docur 0027B4C0 "C:\\ 00000010 0018FD48 "Docur	
		a		0018FC6C 0 0018FC70 0 0018FC74 0 0018FC78 0	0018FD48 "Docu 002784C0 "C:\\\ 00000010 0018FD48 "Docu 00000009	ments" Users\\K7User\\'
				0018FC6C 0 0018FC70 0 0018FC74 0 0018FC78 0 0018FC76 0	0018FD48 "Docu 002784C0 "C:\\\ 00000010 0018FD48 "Docu 00000009	ments" Users\\K7User\\'
				0018FC6C 0 0018FC70 0 0018FC74 0 0018FC78 0 0018FC78 0 0018FC70 0	0018FD48 "Docui 002784C0 "C:\\0 00000010 0018FD48 "Docui 00000009 00000000	ments" Users\\K7User\\'
				OOLBFCGC OOLBFC70 OOLBFC70 OOLBFC78 OOL	0018FD48 "Docu 002784C0 00000010 0018FD48 "C:\\1 00000000 00000000 "C:\\1 "Docu 000000000	ments" Users\\K7User\\'
00 CE 10 00 33 00	20124 00 10 43 00 00	00.02 ++21+21/310c+1++		0018FC70 0018FC74 0018FC74 0018FC74 0018FC780 0018FC780 0018FC780 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC74 0008FC74	0018FD48 "Docu 002784C0 "C:\\ 00000010 0018FD48 "Docu 00000000 " 00000000 " 00000000 "	ments" Users\\K7User\\'
5 23 FF 74 24 10 53 53 5 23 FF 74 24 10 53 53	E8 82 72 08 00 85 C0 85 P5 06 75 F 74	00 00 1.Art.51 0.100.11.1 75 04 u#97.58.rAu. 24 18 [7	OK	OOLBFCGC OOLBFC70 OOLBFC70 OOLBFC78 OOL	0018FD48 "Docu 002784C0 "C:\\ 00000010 0018FD48 "Docu 00000000 " 00000000 " 00000000 "	ments" Users\\K7User\\'
8 64 6C 03 00 5B 50	6A 00 6A 00 E8 E8 F7	75 04 u#9t5.5e.rAu 24 18 [A.y356] 00 00 ed[Pj]Not able 1	OK	0018FC70 0018FC74 0018FC74 0018FC74 0018FC780 0018FC780 0018FC780 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC80 0018FC74 0008FC74	0018FD48 "Docur 002784C0 "C:\\ 00000010 0018FD48 "Docur 00000000 000000000 stacked side by side	ments" Users\\K7User\\'
8 64 6C 03 00 5B 50 B F8 57 E8 BD 6D 03 0 00 00 BA 80 00 E8	6A 00 6A 00 E8 E8 F7 00 EB F8 8B FF 64 8B	00 00 edl[P].]Not able 1 00 00 .øwe½meø	<u>Ок</u>	OOLBECCO OOL	0018FD48 "Docum 002784C0 "C:\\ 00000010 0018FD48 "Docum 00000000 000000000 stacked stacked side by side top	ments" Users\\K7User\\'

Figure 8: Tools getting disabled

After disabling the tools, the ransomware decodes the different folder names which includes Desktop, Documents, Downloads, Pictures, Music ,Public and adds it to the string **C:\Users\%username%** so that it can enumerate these folders first and encrypt the files stored inside.

. 0	045EB6E 045EB72	8D8C24 30020000	lea ecx, dword ptr ss: esp+20		LastStatus 00000000 (STATUS_SUCCESS)
	045EB79	E8 A2D10000	call <malware.add_strings></malware.add_strings>	C:\User\%user%\ + Desktop	GS 002B FS 0053
. 01	045EB7E	C68424 C8000000 49	mov byte ptr ss:[esp+C8],49	49: 'I'	ES 0028 DS 0028
. 01	045EB86	33C9	xor ecx.ecx	ecx: "You need to send your ID to send y	CS 0023 SS 0028
	045EB88	C68424 C9000000 74	mov byte ptr ss:[esp+C9],74	74: 't'	CS 0025 22 0026
. 01	045EB90	C68424 CA000000 68	mov byte ptr ss: esp+CA1.68	68: 'h'	
e 01	045EB98	C68424 CB000000 7A	mov byte ptr ss: esp+CB .7A	7A: 'z'	ST(0) FFFF5312199A1BA09C24 x87r0 Empty inval
	045E8A0	C68424 CC000000 72	mov byte ptr ss: esp+CC ,72	72: 'r'	ST(1) FFFFDD2073044B5154FC x87r1 Empty qnan
	045EBA8	C68424 CD000000 6A	mov byte ptr ss: esp+CD1.6A	6A: '1'	ST(2) FFFF68CF1237FDA49268 x87r2 Empty inval
	045EBB0	C68424 CE000000 73	mov byte ptr ss: esp+CE1,73	6A:'j' 73:'s'	ST(3) FFFF06E264760DDCF590 x87r3 Empty inval-
	045EB88	C68424 CF000000 79	mov byte ptr ss: esp+CF ,79	79: 19	
	045EBC0	C68424 D0000000 78	mov byte ptr ss: esp+D01,78	78: "x" Ar	guments for add_strings function
	045E8C8	C68424 D1000000 00	mov byte ptr ss: esp+D1 .0	1080 U.S. 10	SI(6) FFFF/51881C13/8056FD X8/P6 EMPTY INVAL
	045EBD0		mov al, byte ptr ss:[esp+C8]		ST(6) FFFF/S1001C15/0050FD X0/10 Empty Hivat
	045EBD7	66:0F1F8400 00000000	nop word ptr ds:[eax+eax],ax		4 III +
	045EBE0		mov al.byte ptr ss:[esp+ecx+C8]		
	045EBE7	2C 05	sub al,5		perault (stocar) * 5 + unit clo
	045EBE9		mov byte ptr ss:[esp+ecx+C8],a]		1: [esp] 3650FC34
	045EBF0	41	inc ecx	ery: "You need to send your TD to send y	2: [esp+4] 0018FCD8 "Desktop"
	A +FRAFA		THE CEX	ecx: "You need to send your ID to send y	3: [esp+8] 0027B4C0 "C:\\Users\\
· · · · ·		III.		the second se	4: [esp+C] 00000010
strings	and the second se				5: [esp+10] 0018FCD8 "Desktop"

Figure 9: Function adding folder names after decoding

After getting all the folder names, the ransomware starts to enumerate them using **FindFirstFileExW** and **FindNextFileW** and then uses **ReadFile** to read the existing file into a buffer for encryption.



Figure 10: Using FindFirstFileExW

7DD754ED 9	ň	nop			P		
200754EE 8	BFF	mov edi,edi		FindNextFileW	0000001 028CF98	Amount for	- FiedNewtFileW
P 700754F3 50	BEC	mov ebp,esp pop ebp			018F674		FindNextFileW
700754F4 × E	B 05 0	<pre>pop ebp jmp <jmp.&findnextfi nop</jmp.&findnextfi </pre>	1ew>		018F5E4	&"èø\x18" "6XG	T
7DD754F7 9 7DD754F8 9 7DD754F8 9 7DD754F9 9	D	nop nop			018F658 018F674	&L"C:\\Users\\	\\Desktop\\ALL TOOLS*"
# 700754FA 9	0 F25 <u>3C0AD77D</u>	jmp dword ptr ds:[<4	FindNextFilew>]	JMP.&FindNextFilew	DD754EE	<kernel32.findn< td=""><td>extFileW></td></kernel32.findn<>	extFileW>
Figure 11: U	-	NextFileW			0010010/		
	00585EA6	50		pusn eax			
	 00585EA7 00585EAA 	8845 F4 50		push eax			1
	00585EAB	FF75 EC		push dword ptr ss	:[ebp-14]		
	• 00585EAE	FF75 E8	000	push dword ptr ss call dword ptr ds	ebp-18		
	00585EB7	FF15 58705 85C0	900	test eax,eax	:[<&ReadF110	e>1	
	• 00585EB9	✓ 74 5A		je malware.585F15			
	 00585EBB 00585EBE 	8B4D 10 394D E4		mov ecx, dword ptr	ss: ebp+10		
	-0 00585EC1	× 77 52		ia malware, 585E15	Sector Sector Sector		
	• 00585EC3	037D E4		add edi,dword ptr	ss: ebp-1		
	→● 00585EC6 ● 00585EC9	8845 F8 8855 F0		mov eax, dword ptr mov edx, dword ptr	ss ebp-8	👕 Usin	g ReadFile
	• 00585ECC	880485 <u>887</u>		mov eax, dword ptr	ds:[eax*4+	617FB8	_
EIP	00585ED3	807C02 28	00	cmp byte ptr ds:[edx+eax+28]	,0	
	00585EDA	807D FF 02		jge malware.585E8 cmp byte ptr ss:	ebp-11.2		
1	00585EDE	× 74 17		je malware.585EF7			
	 00585EE0 00585EE2 	D1E9 51		shr ecx,1 push ecx			
	• 00585EE3	FF75 OC		push dword ptr ss	:[ebp+C]		
	 00585EE6 00585EE7 	57		push edi	. Taha dal		
	 00585EE7 00585EEA 	FF75 EC 53		push dword ptr ss push ebx	:Leop-14]		
	•	EA ECENEER			1	1	
dword ntr ss: F							
	ebn-14]=[021]	EE9AC "Èè "]=00	1975969				
	ebp-14]=[021	FF9AC "Èè,"]=00	082E8C8				
		FF9AC "Èè,"]=OC :\$185EAB #1852A					
.text:00585EAB	malware.exe	\$185EAB #1852A	АВ	mp 5 🛛 🏘 Watch 1	[x=] Lo als	Struct	Q
.text:00585EAB	malware.exe		AB	an and all a second second second second	[x=] Lo als	Struct	0.
.text:00585EAB	malware.exe	\$185EAB #1852A Dump 3 Image: Constraint of the second sec	NB 4 000 Du	ASCII 00 00 L	A	Struct	^ Ö
.text:00585EAB	malware.exe	\$185EAB #1852A Dump 3 Ump Dum 02 00 00 00 00 08 00 20 00 00	AB	ASCII 00 00 L FB 80F	A ×4û.	2 Struct	
.text:00585EAB	malware.exe	\$185EAB #1852A Dump 3 Image: Constraint of the second sec	AB 1000 CO 00 000 D7 34 501 58 70 000 O1 00	ASCII 00 00 L. FB 80 F6 80 A10.×4û.A10. 00 00 A10.×.	A ×4û. ×pö.		
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 9B 00 D6 01 D7 34 D6 01 00 73 00 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 FB 80 C0 31 D 08 00 00 00 00 00 00 00 00 00	AB 1000 C0 00 000 D7 34 501 58 70 1000 22 01	ASCII 00 00 L FB 80F F6 80 Å1Ö.×4ù.À1Ö. 00 00 Å1Ö.×	À ×4û. ×pö.		stored in
.text:00585EAB	malware, exe Dump 2 00 00 01 14 00 46 98 00 D6 01 D7 34 D6 01 00 78 00 00 00 00 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 08 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 54 BA 2D 10	AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F	ASCII 00 00 L FB 80 A.F F6 80 A10.×4û.A10. 00 00 A10.× 4 <u>C 00</u> 6F 6C 1ÀT°	А ×4û. хрб. тоо]	File	stored in
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 9B 00 D6 01 D7 34 D6 01 00 78 00 00 00 00 38 00 08 00 24 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 08 00 20 00 00 08 00 20 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 EF 00 00	AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F 8 53 4D 57 0 0 00 20 00	ASCII AS	A x4û. xpö. Tool MWAT	File buf:	stored in fer after
.text:00585EAB	malware, exe Dump 2 00 00 01 14 00 60 98 00 06 01 D7 34 D6 01 00 78 00 00 00 00 00 00 00 00 38 00 08 00 2A 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 08 00 00 00 00 08 00 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 EF BE 44 69 55 00 00 00 00 00 00 00 00 00 00	AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F 8 53 4D 57 0 0 00 20 00 0 00 54 00	ASCII 00 00 L FB 80 A.Ö.×40.A1Ö. 00 00 A1Ö.×. 4C 00 6F 6C 1ÅT° C5 54 s.8ī¥HS 00 00 °-☆i∧. 6F 00	A x4û. xpö. Tool T.O.	File buf:	stored in fer after adFile
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 98 00 D6 01 D7 34 D6 01 00 73 00 00 00 00 38 00 08 00 2A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 76 80 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 EF BE 48 69 55 00 00 00 00 00 00 00 00 00 01 14 00 70 10 00 15 04 50 45	AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 22 01 0 00 54 6F 8 53 4D 57 0 00 54 00 0 00 54 00 0 00 54 00 0 00 54 55	ASCII 00 00 L FB 80F F6 80 A1Ö.x4û.A1Ö. 00 00 A1Ö.x. 4C 00 6F 6C 1ÅT° 55 54 s.8ï¥HS 00 00 °-"1Å 6F 00 00 00 o.l.sp. 7E 31ÅTMAPKS	A ×4û. Xpö. ".L. Tool MwAT T.o. 1 T.v.	File buf:	stored in fer after adFile
.text:00585EAB	malware, exe Dump 2 00 00 01 14 00 60 98 00 06 01 D7 34 D6 01 00 78 00 00 00 00 00 00 00 00 38 00 08 00 2A 00 00 00 00 00 00 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 00 00 00 08 00 00 00 00 08 00 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 10 54 48 54 00 08 00 00	AB 0 00 C0 00 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F 8 53 4D 57 0 0 00 20 00 0 00 31 00 5 53 54 55 4 00 EF BE 6	ASCII 00 00 L	A X40. Xpö. Tool MWÅT T.o. 1 STU~1 1%ÅT	File buf:	stored in fer after adFile
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 98 00 D6 01 D7 34 D6 01 00 78 00 00 00 00 00 00 00 00 24 00 00 00 24 00	\$185EAB #1852A Dump 3 ### Dum 02 00 00 00 08 00 20 00 00 08 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 04 00 F B 44 69 5E 00	AB p 4 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 22 01 0 00 54 6F 0 00 20 00 0 00 54 6F 0 00 20 00 0 00 54 00 0 00 00 00 0 00 54 00 0 00 00 00 0 00 00 00 0 00	ASCII 00 00 L	A X40. Xpö. Tool MWÅT T.o. 1 STU~1 1%ÅT	File buf:	stored in fer after after after
.text:00585EAB	ma]ware.exe Dump 2 00 00 01 14 00 60 98 00 06 01 D7 34 D6 01 07 78 00 00 00 00 00 00 00 00 2A 00 00 00 00 00 00 00 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 08 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 23 00 74 00 76	AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F 8 53 4D 57 0 0 00 31 00 0 00 31 00 5 53 54 55 1 00 EF BE 0 3 A7 00 00 0 00 00 00	ASCII 00 00 L	A x4û. xpö. Tool MWÀT TU~1 i‰AT d.i.	File buf:	stored in fer after
.text:00585EAB	malware.exe Dump 2 Image: Constraint of the second s	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 02 00 00 00 08 02 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 04 00 04 00 00 00 04 00 04 00 00 2A 00 00 00 00 00 00 2A 00 00 00 00 00 00 53 00 74 00 07 22 00 22 00 22 00 10 75	AB mp 4 U Du 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 22 01 0 00 54 6F 0 00 20 00 0 00 54 6F 0 00 20 00 0 00 54 6F 0 00 20 00 0 00 54 55 1 00 EF BE 0 00 EF BE 0 00 00 00 0 00 00 00 0 00 4 00 0 00 00 00 0	ASCII 00 00 L	A ×4û. ×pô. Tool Tuol Tuol 	File buf:	stored in 500000000000000000000000000000000000
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 98 00 D6 01 D7 34 D6 01 07 34 00 00 00 00 38 00 08 00 24 00 00 00 00 00 00 00 00 00 00	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 78 80 C0 31 D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2A 00 00 00 00 00 52 00 20 27 00 28 00 00 00 00 20 26 00 00 12 00 26 00 00 00 12 00 26 00 00 00 12 <t< td=""><td>AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F 8 53 4D 57 0 0 00 31 00 0 00 31 00 5 53 54 55 1 00 EF BE 0 3 A7 00 00 0 00 00 00</td><td>ASCII 00 00 L</td><td>A x4û. xpö. Tool MWAT T.0. 1 TU~1 i%AT d.i. 4 2x</td><td>File buf:</td><td>stored in fer after adFile</td></t<>	AB 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 01 00 0 00 22 01 0 00 54 6F 8 53 4D 57 0 0 00 31 00 0 00 31 00 5 53 54 55 1 00 EF BE 0 3 A7 00 00 0 00 00 00	ASCII 00 00 L	A x4û. xpö. Tool MWAT T.0. 1 TU~1 i%AT d.i. 4 2x	File buf:	stored in fer after adFile
.text:00585EAB	malware.exe Dump 2 Image: Constraint of the second s	\$185EAB #1852A Dump 3 #1000 02 00 00 00 08 00 20 00 00 08 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 E B 48 00 00 00 00	AB AD AD AD AD AD AD AD AD AD AD	ASCII 00 00 L	A x4û. xpô. Tool MWÅT TUol TUol 	File buf:	stored in 500000000000000000000000000000000000
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 98 00 D6 01 D7 34 D6 01 00 78 00 00 00 00 00 00 00 00 00 00 00 0	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 78 80 C0 31 D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2A 00 00 00 00 00 2E 00 12 00 24 00 00 2A 00 00 00 00 00 00 2A 00 00 00 00 00	AB D 00 C0 00 00 D7 34 5 01 58 70 00 01 00 00 22 01 0 00 54 6F 5 3 4D 57 0 00 54 6F 5 3 4D 57 0 00 54 00 0 00 54 55 1 00 EF BE 0 00 64 00 5 3 54 55 1 00 EF BE 0 0 64 00 5 0 54 55 1 00 EF BE 0 0 0 0 0 00 0 0 0 0 0 00 0 0 0 0 0	ASCII 00 00 L	A x4û. xpô. Tool MWÅT TUol TUol 	File buf:	stored in fer after adFile
.text:00585EAB	malware.exe Dump 2 00 00 01 14 00 46 98 00 D6 01 D7 34 D6 01 00 78 00 00 00 00 00 00 00 00 00 00 00 0	\$185EAB #1852A Dump 3 Image: Dum 02 00 00 00 08 00 20 00 00 08 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 E B 48 00 01 40 77 10 00 41 50 48 00 00 00 00 00 24 00 00 00 00 25 00 20 00 00 26 03 20 02 42 48 00 00 00 00 24 00 00 00 00 20 00 11 10 48 48 00 00 00 <	AB mp 4 U Du 0 00 C0 00 0 00 D7 34 5 01 58 70 0 00 22 01 0 00 54 6F 0 00 54 6F 0 00 54 6F 0 00 54 00 0 00 20 00 0 00 54 00 0 00 54 00 0 00 54 00 0 00 20 00 0 00 54 00 0 00 20 00 0 00 54 00 0 00 54 00 0 00 20 00 0 00 54 00 0 00 54 00 0 00 00 00 0 00 54 00 0 00 54 00 0 00 00 00 0 00 00 00 0 00 64 00 0 00 00 00 0 00 00 00 0 00 00 00 0 00 00 00 0 00 00 00 0 00 00 00 00 0 00 00 00 00 0 00 00 00 00 00 00 00 00 00 00 00 00 0	ASCII 00 00 L	A x4û. xpö. Tool MWÀT STU~1 i‰AT 	File buf:	stored in fer after adFile
.text:00585EAB	malware.exe Dump 2 Image: Constraint of the second s	\$185EAB #1852A Dump 3 Imposition 02 00 00 00 08 00 20 00 00 78 80 C0 31 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 00 74 00 00 00 53 00 74 00 75 76 00 00 00	AB p 4 0 00 C0 00 00 D7 34 5 01 58 70 0 00 20 00 0 00 54 6F 5 3 4D 57 0 00 54 6F 3 53 4D 57 0 00 54 00 0 00 64 00 0 00 00 00 0 00 00 00 0 00 00 00 0 00 00 00 0 00 00 00 00 0 00 00 00 00 00 00 00 00 00 00 00 00 0	ASCII 00 00 FB 80 FG 80 AIO.x 00 00 AIO.x 4C 00 AIO.x 4C 00 AIO.x AIO.x 4C 00 6F 6C 1ATM.x ASC AIO.x AGO AIO.x AGO Construction AIO.x AGO Construction AIO.x AGO Construction AIO.X AIO.X <tr td=""></tr>	A x4û. xpö. Tool MWÀT STU~1 i‰AT 	File buf:	stored in fer after adFile
.text:00585EAB	malware.exe 00 00 01 14 00 46 98 00 06 01 D7 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	\$185EAB #1852A Dump 3 Imposition 02 00 00 00 08 00 20 00 00 78 80 C0 31 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 00 74 00 00 00 53 00 74 00 75 76 00 00 00	AB pp 4 0 00 CO 00 0 00 D7 34 5 01 58 70 0 00 22 01 0 00 22 01 0 00 24 00 0 00 24 00 0 00 24 00 0 00 34 00 5 00 64 00 5 53 54 55 1 00 EF BE 0 00 254 55 1 00 EF BE 0 00 40 00 5 00 64 00 0 00 00 00 00 0 00 1C 00 0 00 1C 00	ASCII 00 00 L	A x4û. xpö. Tool MWÀT STU~1 i‰AT 	File buf:	stored in fer after adFile

Figure 12: Using **ReadFile** to read **ApkStudio.exe.Ink**

Encrypting Files

When analysing the sample after ReadFile we observed that the sample doesn't use any common encryption related Windows APIs like **CryptAcquireContextA**,

CryptReleaseContext, CryptGenKey, CryptExportKey, etc. On further digging, we found that the whole encryption routine is implemented inside the ransomware. We identified this when a hardware breakpoint on the randomly generated password (described at the start of the blog) was hit after the ReadFile API. There were some calculations happening with the password and some bytes were also present in the .rdata section.

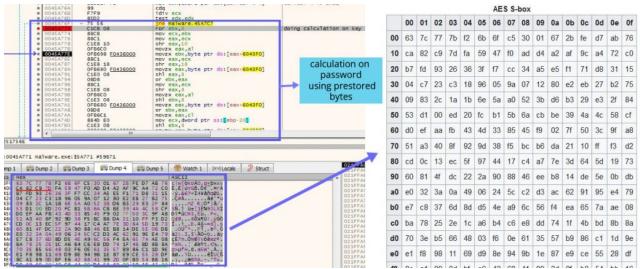


Figure 13: Using AES S-block for key expansion

After checking those prestored bytes we identified that it is an S-Block used in the AES Algorithm during the Key Expansion phase. So ransomware is using the AES algorithm to encrypt the files using the password (key) that was randomly generated and sent to discord webhook. On further analysis, we got the functions which were responsible for encrypting the file bytes and writing it to the memory 16 bytes at a time as in Figure 14 and Figure 15.

	0045 0045 0045 0045	AC1D 8 AC23 8 AC26 8 AC29 7 AC29 7 AC29 7 AC29 7	BD6 8 E3FCFFFF 8845 BC 33C6 10 33EF 01 75 E5 30 10 III III 8 #54018	add esi, sub edi,	ware.45A9 dword ptr 10 1 are.45AC1	ss: ebp-44	Function 16 byt	edx:L"o-5.2.4-x writing some st n encrypting es at a tim storing it memory	uff to memoe g file e and	
np 1 s He	Dump 2	Dump 3	Dump 4	imp 5 🛞	Watch 1	[x=] Locals	2 Struct		021FFAD 021FFAE	0 0081D268
F8 AB 08 58 18 00 28 00 38 00	AB AB AB EE 24 79 17 57 00 00 00 00 00 00 00 00 00 00 00 E0	FE EE FE C9 00 18 00 00 00 00 00 00 B3 59 00	00 00 00 00 AB AB 00 00 00 00 00 00 00 00 00 00 00 03 D2 AB AB AB AB AB AB AB AB 58 24 79 14 54 C9 00	00 00 ««««« <u>81 00</u> [\$y AB AB 00 1C 00 00	«îþîþ. .WE .X\$y. .a*y. .««««««««	sò «««« TÉ			021FFAE 021FFAF 021FFAF 021FFAF 021FFAF	4 0081FDE0 8 021FFB34 C FFFFD488 0 00004C5 4 0081D268 8 0081FDE0 C 0000005 0 0000000
73 42 83 87 93 26 43 D4 E3 3F3 D3 BA E3 60 03 72 13 60 013 72 23 72 23 72 23 72 23 72 23 72 24 25 26 26 26 26 26 26 26 26 26 26 26 26 26	26 F6 C0 35 98 01 7F 87 82 00 AD 3F 84 17 B3 E6 01 62 58 62 50 E9 38 B4 8F CD 96 7C FD 53 6F 80 F1 18 36 A0 F1 18 36 A0 F1 72 91 AC 10 FE DE C7 7D F2 BD 79 70 72 8D 79	E3 88 42 3F AF CA 89 31 08 AB FD B4 A7 A2 30 58 23 45 A9 37 AE 1C 08 C3 45 A9 37 AE 1C 08 C3 45 A9 37 AE 11 08 C3 45 A9 37 AE 13 18 EA 80 03 89 F3 E9 28 71 99 CD	A0 F1 A3 69 EE D7 82 DA 7C 1E BF C2 0A 58 21 B8 5E 51 75 F6 68 72 6C 3D 20 98 DE 68 D1 E4 D1 05 83 FB 08 4E E0 A6 6C AD 89 0E E1 8E 88 40 13 24 99 D2 C5 E9 57 57 C6 AC 5A 12 EA 08 65 F7 C C0 A6 58 E7 95 CC 02 A6 85 B0 66 3F 7F 86 EE B0 66 3F 7F 86 EE 82 84 85 50 85 82 84 85 50 86 85 85 50 86 85 85 50 86 85 85 50 86 85 50 86 50 86 85 50 86 50 8	79 3A 8&0 23 16 F6 7D 0 96 71 0 96 71 0 90 72 0 90 71 0 90 71 0 90 71 0 90 71 0 90 71 0 91 7 92 74 r 82 74 r 82 74 r 82 74 r 81 26 H±6F 12 72 6 ±8Å 70 84 2}0	Àsā.B.Ú . .??L.uöhr *æ≪ý .Ph Xb§¢oÑ.û Xb§¢oÑ.û Xb§¢oÑ (£ØÂ G.û.X.ÔÅê G.û.A.Z. bÇ.êo.ÌÀ PʰµðKS &/óé+°f?. %yq.Ifó%(¿Ay: ^Q#. Näö} .N7, q ē° ë° ¢I ;∨*Ä çt	Encz	rypted file in memory	021FF80 021FF80 021FF80 021FF81 021FF81 021FF81 021FF82 021FF82 021FF82	4 021FFB1C 8 005838AD 007E0000 0 0083D9C0 0 0083D9C0 0 0083DAB0 8 0083DAB0 0 021FFB3C 0 021FFB3C 0 021FFE3C 0 0000000 0 021FFE80 4 00458389 8 0081FDE0 0 0081FDE0 0 0081F738

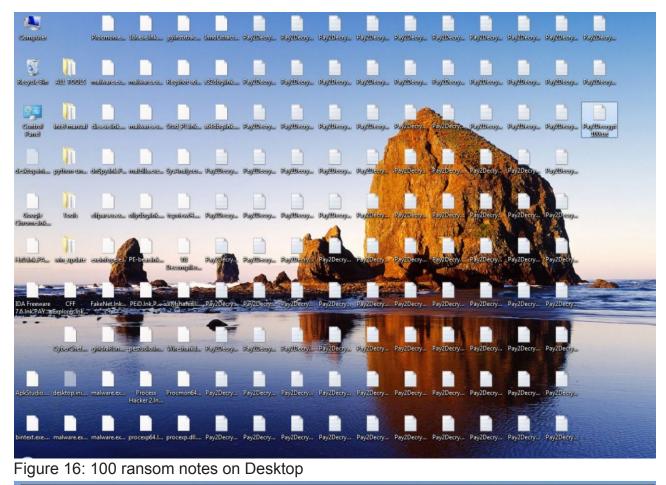
Figure 14: ApkStudio.exe.Ink File getting encrypted

ApkStudio.exe.Ink.PAY2DECRYPTRLDIAMG4XPqfVNQ9jMzvsA0

												-					
Offset(h)	00	01	02	03	04	0.5	06	07	08	09	0A	0B	00	0D	0E	0F	Decoded text
00000000	AE	C2	AE	07	02	81	65	39	AO	F1	A3	69	EE	D7	BD	DO	SÂ⊗e9 ñ£iî×₩Đ
00000010	42	26	F6	CO	35	E3	88	42	82	DA	7C	1E	BF	C2	79	ЗA	B&öÀ5ã^B,Ú .¿Ây:
00000020	87	9B	01	7F	87	3F	AF	CA	OA	5B	21	B8	5E	51	23	16	‡>‡? [−] Ê.[!,^Q#.
00000030	26	82	00	AD	3F	89	31	0B	75	F6	68	72	6C	3D	2A	E6	&,?%1.uöhrl=*æ
00000040	D4	84	17	B3	E6	AB	FD	B4	20	9B	DE	68	D1	E4	F6	7D	Ô".³æ≪ý′ >ÞhÑäö}
00000050	ЗF	01	62	58	62	A7	A2	30	D1	05	83	FB	08	4E	37	2C	?.bXb§¢0Ñ.fû.N7,
00000060	F3	50	E9	38	B 4	58	23	45	EO	A6	6C	AD	89	OE	96	71	óPé8′X#Eà¦l.‰q
00000070	BA	BF	CD	96	7C	A9	37	AE	E1	8E	B 8	4D	13	24	2E	BO	°¿Í- ©7®áŽ,M.Ş.°
00000080	C8	FD	53	6F	80	10	0B	C9	D8	C4	19	04	EB	AE	90	7E	ÈýSo€ÉØÄ뮜~
00000090	60	F1	18	36	AD	FA	7F	BD	99	D2	C5	E9	57	57	02	80	`ñ.6.ú.⊁™ÒÅéWW.€
000000A0	7C	F1	72	91	AC	4A	D3	16	C6	AC	5A	12	EA	08	8C	CF	ñr`¬JÓ.ƬZ.ê.ŒÏ
00000B0	72	10	FE	DE	C7	13	1B	EA	6F	7F	CC	CO	A6	56	B2	C4	r.þÞÇêo.ÌÀ¦V*Ä
00000000	48	B1	36	50	C8	80	03	B9	B5	FO	4B	53	E7	9D	81	26	H±6PÈ€.¹µðKSç&
00000D0	C9	E6	C3	C6	2F	F3	E9	2B	BO	66	3F	7F	B6	EE	12	CE	ÉæÃÆ/óé+°f?.¶î.Î
000000E0	32	7D	F2	BD	79	71	99	CD	A3	F3	BE	28	4B	59	FO	B4	2}ò¾yq™Í£ó¾(KYð′
000000F0	20	20	20	22	10	62	20	07	22	TO	70	00	22	07	22	01	©°."HaÙ>Òù∣™⊊-,.
00000100	22	C8	F4	2F	B 5	6D	E7	61	CF	6D	FE	D8	E9	10	1D	04	"Èô/µmçaÏmþØé
00000110	02	9A	4E	A4	FE	AA	D5	29	32	40	E8	A1	E9	4D	97	00	.šN¤þ°Õ)2@è;éM−.
00000120	EO	OD	FB	36	04	72	51	86	01	3D	08	8B	7E	B 5	F6	54	à.û6.rQt.=.<~µöT
	23.3	1000	1.5			01		-		-				-			

Figure 15: Encrypted File **ApkStudio.exe.Ink**

Ransomware creates a new file with the same name and writes the encrypted bytes into that file and then renames the file with the extension **PAY2DECRYPT+UID**. After encrypting the files, it puts 100 ransom notes on the Desktop. This ransomware encrypts executables as well. It changes its own name to encrypted file extension but the file remains as-is and not encrypted.



Pay2Decrypt100.bt - Notepad File Edit Format View Help Ocops! Your files was been encrypted!!!!!!. You can recover your files securely with our decryptor. Send us an email to P2Dq2HMg28A2652@postheo.de (or to P2D0TJ6L16H1q7a@mail.al.wtf) to recover your files Ask for Hynn and he will send his wallet (thank you Hynn) and the pay amount, this may vary from 0.0002 to 0.2 BTC Hynn will rate your case (being friendly increases your chance to send you the decryptor free!) and then he will send you more information. You need to send your ID to send you the correct personalized decryptor. ID: IAMG4XPqfVNQ9jMzvsA0

Figure 17: Ransom Note

We at K7 Labs provide detection for BleachGap ransomware and all the latest threats. Users are advised to use a reliable security product such as **"K7 Total Security"** and keep it up-to-date to safeguard their devices.

Indicators of Compromise (IOCs)

File Name	Hash	Detection Name
ransomito.exe	bfe289c6f91ffcda97c207f3c1c525a9	Riskware (00584baa1)

References

https://www.goggleheadedhacker.com/blog/post/reversing-crypto-functions-aes

https://twitter.com/Finch39487976/status/1533126802159304705

https://www.reversingsecurity.com/blog/pay2decrypt-bleachgap-analysis