Ranzy Locker

Teknik Analiz Raporu

İçindekiler

Giriş

Ranzy Locker olarak bilinen zararlı yazılım ThunderX ransomware ailesine aittir. Bilgisayarınızda bulunan tüm önemli dosyaları şifreler.

Ranzy Locker zararlı yazılımı ilk olarak 21 Ekim 2020 tarihinde görülmüştür. Kurban bilgisayara bulaştığında önemli dosyaları şifreler ve şifrelerin çözülmesi karşılığında fidye talep eder. Talep işlemini dosyaları şifreledikten sonra oluşturduğu readme.txt dosyasının içerisinde bulunan, bulaştığı sisteme ait anahtar üzerinden proton mail adresi ile iletişime geçerek gerçekleştirmektedir.

Kötü amaçlı yazılımı genellikle Windows sistemleri hedeflemektedir.

Özet

Deleteme.exe birçok uygulamanın anlık görüntülerini ve bu uygulamaların bilgilerini almaktadır. Bu uygulamaların listesi detaylı analiz bölümünde ayrıntılı olarak listelenmiştir.

Çeşitli anti-debug yöntemleri uygulayarak zararlıyı analiz edilemeyecek duruma getirmeye çalışmakta ve analistin işini zorlaştırmaya çalışmaktadır.

Geri dönüşüm kutusunda bulunan verileri ve eğer varsa sistem yedeklemelerini silmektedir.

Sistemde kaç diskin tanımlı olduğu bilgisini ve adaptör bilgilerini almaktadır.

Son olarak kurban bilgisayarda bulunan tüm önemli verileri şifreleyerek fidye talebinde bulunmaktadır.

deleteme.exe Analizi

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

Dosya Adı	**Exe dosyası**
MD5	84e8bf44a339c6c2a51aedb17b52e83e
SHA-1	6681ac4c02f2b2696590eebad5f8e94cf1723678
SHA-256	0db6f0721b23aba59852382dad8042be26832c7bb182d79f4734e17da3bcd5ee

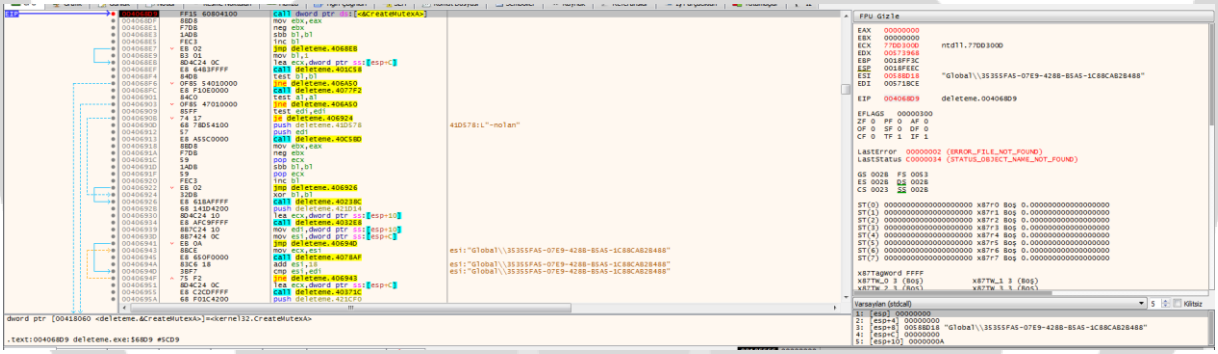
Portable Executable tipinde 32 bit bir exe dosyası olduğu anlaşılmaktadır.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .└...┘...ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.......
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	08	01	00	00	............◘ ..
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	♫ °♫.´.Í!¸ LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.......
00000080	E1	6C	A8	3C	A5	0D	C6	6F	A5	0D	C6	6F	A5	0D	C6	6F	ál¨<¥.Æc¥.Æc¥.Æo
00000090	FE	65	C5	6E	AF	0D	C6	6F	FE	65	C3	6E	30	0D	C6	6F	şeÅn¯.Æoşeãn0.Æo
000000A0	FE	65	C2	6E	B7	0D	C6	6F	6E	62	C2	6E	B4	0D	C6	6F	şeân·.ÆonbÂn´.Æo
000000B0	6E	62	C5	6E	B0	0D	C6	6F	6E	62	C3	6E	8F	0D	C6	6F	nbÅn°.ÆonbÃn .Æo
000000C0	FE	65	C7	6E	B0	0D	C6	6F	A5	0D	C7	6F	2E	0D	C6	6F	şeÇn°.Æc¥.Ço..Æo
000000D0	23	7D	CF	6E	AF	0D	C6	6F	23	7D	39	6F	A4	0D	C6	6F	#}Ïn¯.Æo#}9o¤.Æo
000000E0	A5	0D	51	6F	A4	0D	C6	6F	23	7D	C4	6E	A4	0D	C6	6F	¥.Qo¤.Æo#}Än¤.Æo
000000F0	52	69	63	68	A5	0D	C6	6F	00	00	00	00	00	00	00	00	Rich¥.Æo........
00000100	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	........PE..L.┘.

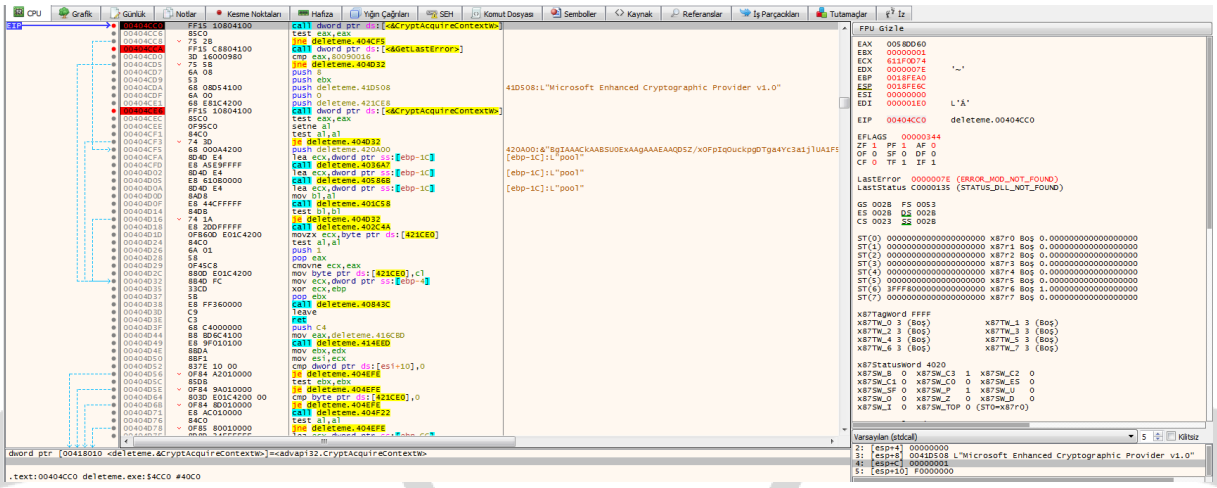
```
0018FE2C 00000004
0018FE30 00000000
0018FE34 0018FE60
0018FE38 0040E103 return to deleteme.0040E103 from deleteme.0040E8EF
0018FE3C 00000004
0018FE40 0018FEE8
0018FE44 0018FE98 "43"
0018FE48 00000000
0018FE4C 0040C0B5 return to deleteme.0040C0B5 from deleteme.0040E0E6
0018FE50 00401F36 return to deleteme.00401F36 from deleteme.0040C0B0
0018FE54 0018FEE8
0018FE58 00420BF8 &"433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572"
0018FE5C 0018FE98 "43"
0018FE60 0018FEC0
0018FE64 004060B1 return to deleteme.004060B1 from deleteme.00401F29
0018FE68 0018FE98 "43"
0018FE6C 19E5D7E3
0018FE70 00000036
0018FE74 00421D38 deleteme.00421D38
```

“433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572” şeklinde bir ASCII bulunuyor.

Bu ASCII’nin anlamı “C:\Program Files\Microsoft SQL Server”. Burada zararlı yazılım SQL veritabanı sunucularını kontrol etmektedir.



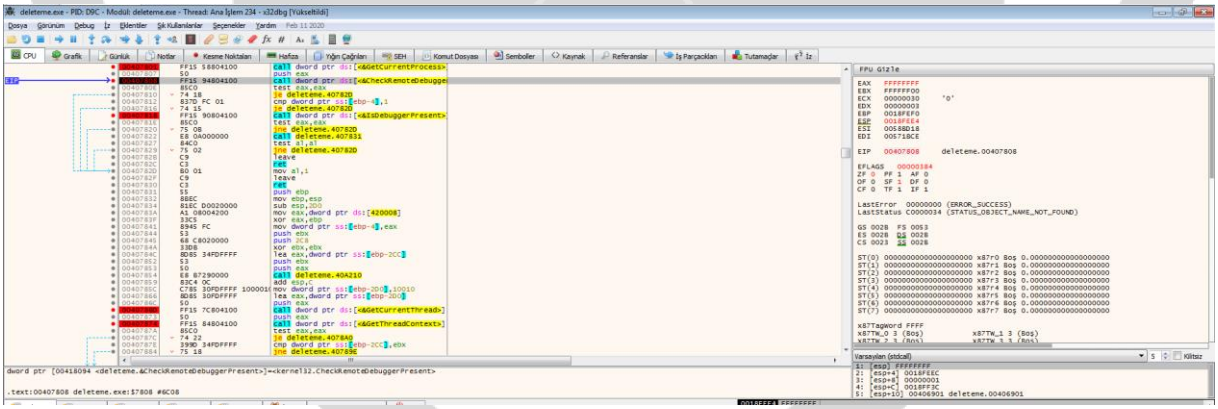
“Global\35355FA5-07E9-428B-B5A5-1C88CAB2B488” isminde bir mutex nesnesi oluşturma ve bu nesneyi açmaktadır.



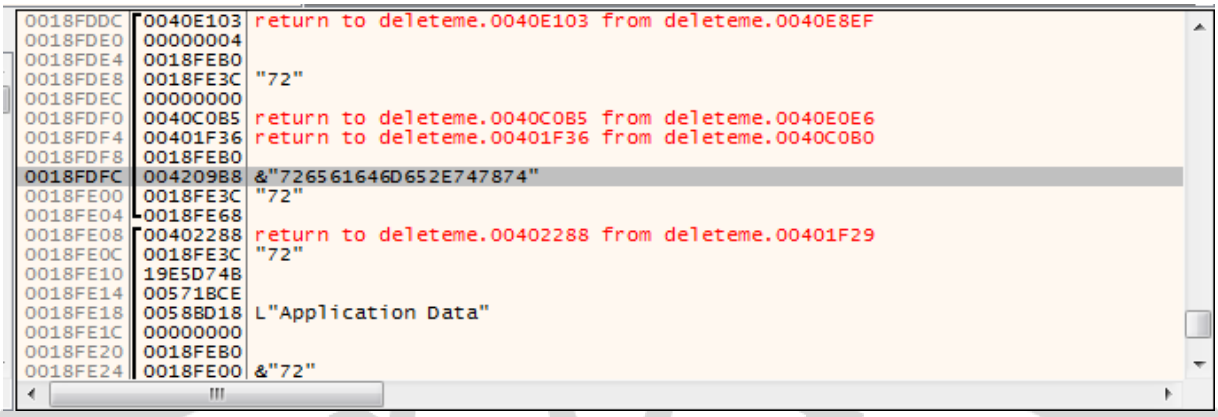
“BgIAAACkAABSU0ExAAgAAAEAAQD5Z/x0FpIqOuckpgDTga4Yc3a1jlUA1F5Af5uw61G8EK/RFWT2qgi2kgvWG6V8AfsGbBBGTrFInJz8lzb6qkudvlxXCuK+CEAIyWC60S4BQN++zwdzJtYtYEfLRpp5WVkrM39cFn3rohIXO7SgIzAADVzo1OoFjbAV8/NhcNWQBssIyHs+LttfEPJ61KljmW0aS1hJhvbh2A+kekJf48lgXMP04wFarlDHmDPFjfJTJ4Zo2bwvkfpgiwhcEsSGeeSJ108mCqnKbOeGvizxaDPkwOY5rOBknvZXHxZswqOvruRSUT4PJOjBuBRhgEPblffy4qYej3JNtzteYDkCVCSY”

Yukarıda verilen encode edilmiş bir veri ile karşılaşılmaktadır. Bu veri decode edildiğinde şifreleme sisteminin RSA-1 olduğu anlaşılmaktadır.

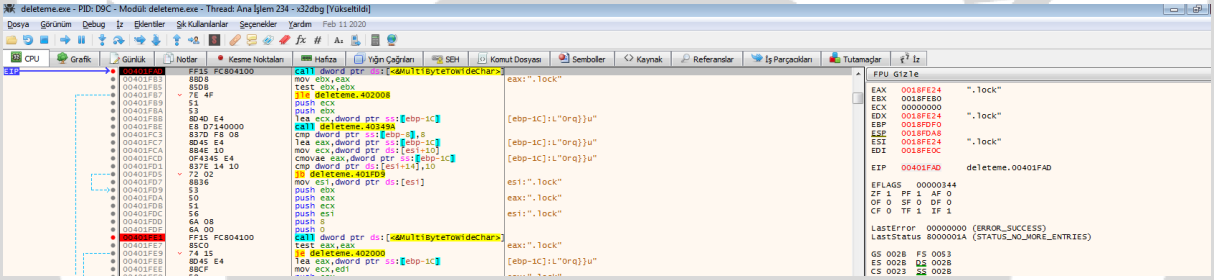
Daha sonra şifreleme işlemlerini gerçekleştirir.



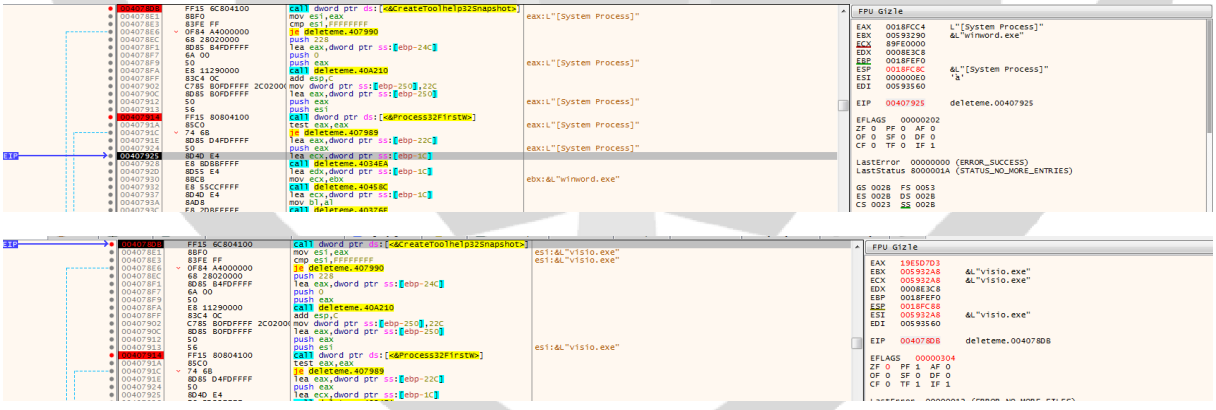
Zararlı çeşitli anti-debug yöntemleri uygulamaktadır. Fotoğrafta verilen örnekte CheckRemoteDebuggerPresent API’ı ile anti-debug işlemi yapılmaktadır.



ASCII ile encode halde bulunan “726561646D652E747874” şeklinde string decode edildiğinde “readme.txt” belgesinin oluşturulduğu gözlemlenmekte ve bu belgenin, analizin devamında yer alan fidye talep belgesi olduğu anlaşılmaktadır.



Ransomware şifrelediği dosyaların uzantılarını “.lock” olarak değiştirmektedir.



Zararlı yazılım sistemde çalışan processlerin ve bazı uygulamaların anlık görüntülerini almakta ve çalışıp çalışmadığını kontrol etmektedir. Bu dosyalar aşağıda listelenmiştir;

winword.exe	visio.exe	ensvc.exe	mysql_opt.exe
occsd.exe	thabat.exe	ocomm.exe	outlook.exe
mysqld.exe	sqlagent.exe	sqlservr.exe	infopath.exe
sqlbrowser.exe	thunderbird.exe	msftesql.exe	wordpad.exe
synctime.exe	agntsvc.exe	dbsnmp.exe	mydesktopservice.exe
ocautoupds.exe	thebat64.exe	sqbcoreservice.exe	isqlplussvc.exe
oracle.exe	tbirdconfig.exe	mysqld-nt.exe	

Bu uygulamalar çeşitli SQL sunucuları, e-mail istemcileri, not defterleri ve Oracle'a ait bazı yazılımları içermektedir.

GetTickCount API'ı ile anti debug uygulamaktadır.

Bazı WMI sorguları yürütülmektedir. Bu sorgular aşağıda listelenmiştir;

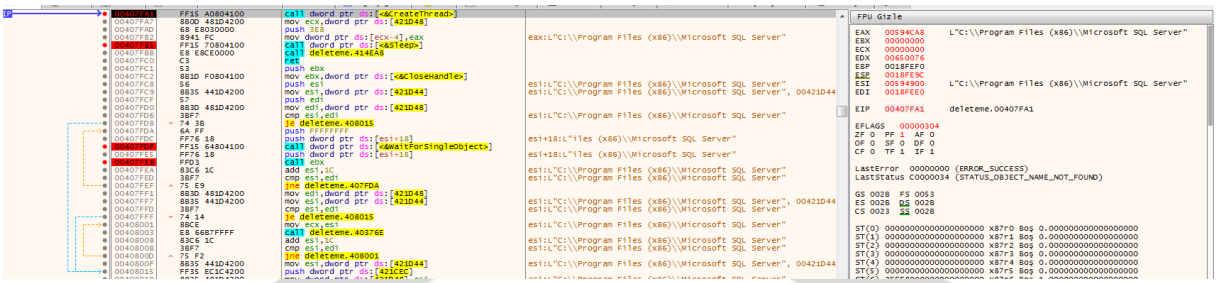
vmickvpexchange	vmicquestinterface	vmicshutdow	vmicheartbeat
MSSQLFDLauncher	MSSQLSERVER	SQLBrowser	SQLSERVERAGENT
SQLWriter	MSSQL	WRSVC	ekrn

OpenSCManagerW ile Services Control Manager'a bağlanır ve Open ServicesW API'ı ile yukarıdaki listede verilen vmickvpexchange hizmetini başlatır.

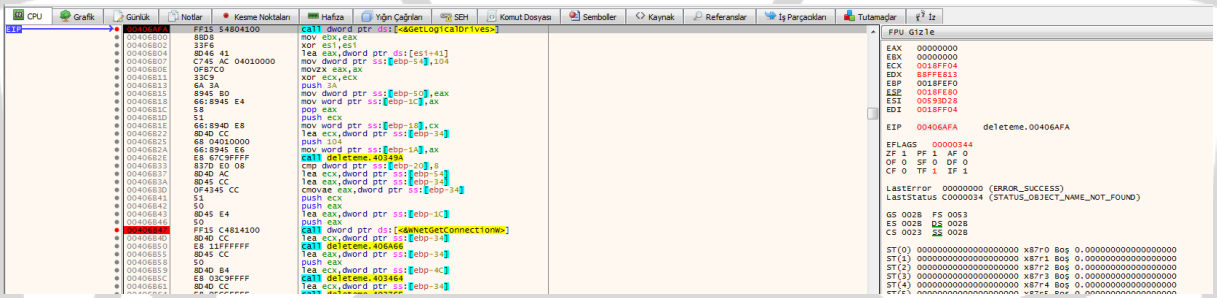
Vmickvpexchange hizmeti, sanal makine ile fiziksel bilgisayarda çalışan işletim sistemi arasında veri alışverişi için bir mekanizma sağlar.

Zararlı Yazılım çeşitli komutlar yürüterek dosyalar şifrelendikten sonra, verilerin kurtarılmasını imkânsız hale getirmeye çalışmaktadır. Bu komutları ASCII olarak encode halde tutmakta ve tek tek özümleyerek decode etmektedir. Yürüttüğü tüm komutlar aşağıda listelenmiştir;

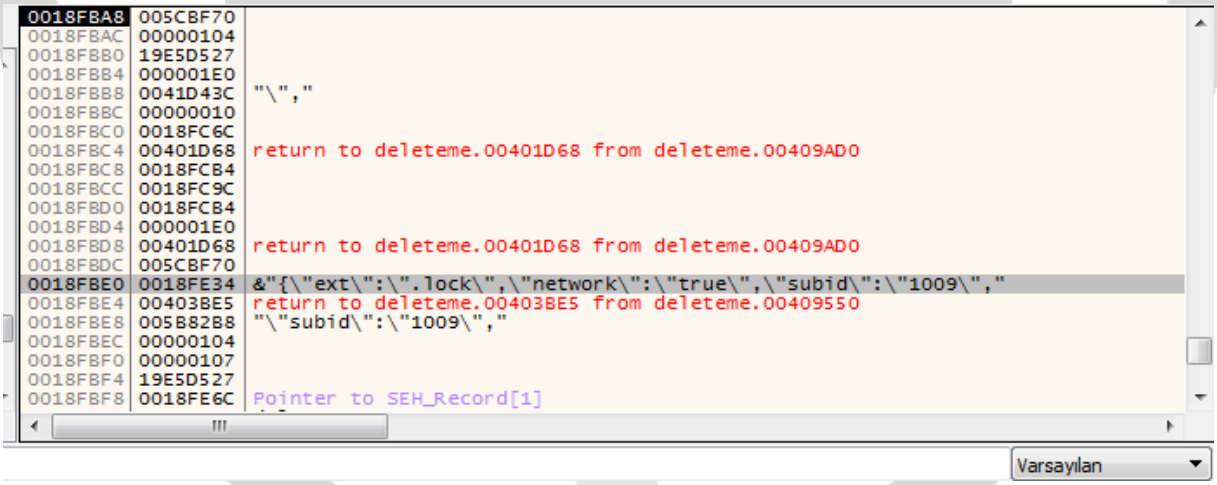
Komut	Yaptığı İşlem
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest	En eski sistem yedeklemelerinin tamamını siler.
wmic.exe SHADOWCOPY /nointeractiv	Tüm Shadow Copy'leri siler.
wbadmin DELETE SYSTEMSTATEBACKUP	Tüm sistem yedeklemelerini siler.
bcdedit.exe /set {default} recoveryenabled No	Windows kurtarmayı ve onarmayı devre dışı bırakır.
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures	Windows kurtarmayı deaktif hale getirir. Bir hata oluşması durumunda bilgisayarı normal şekilde önyüklemeye çalışacaktır.
vssadmin.exe Delete Shadows /All /Quiet	Tüm Shadow Copy'leri siler.



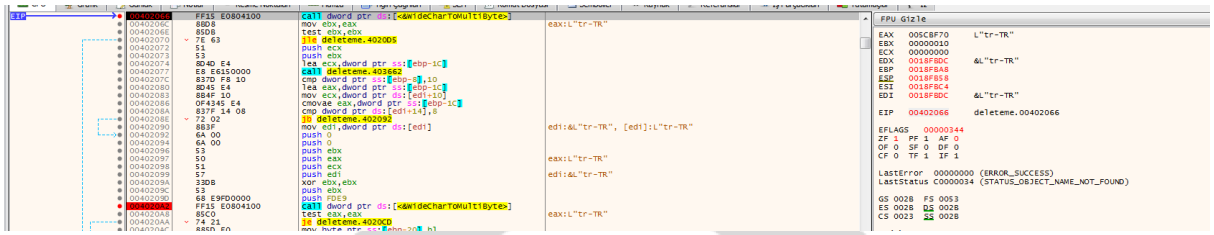
Thread oluşturmaktadır.



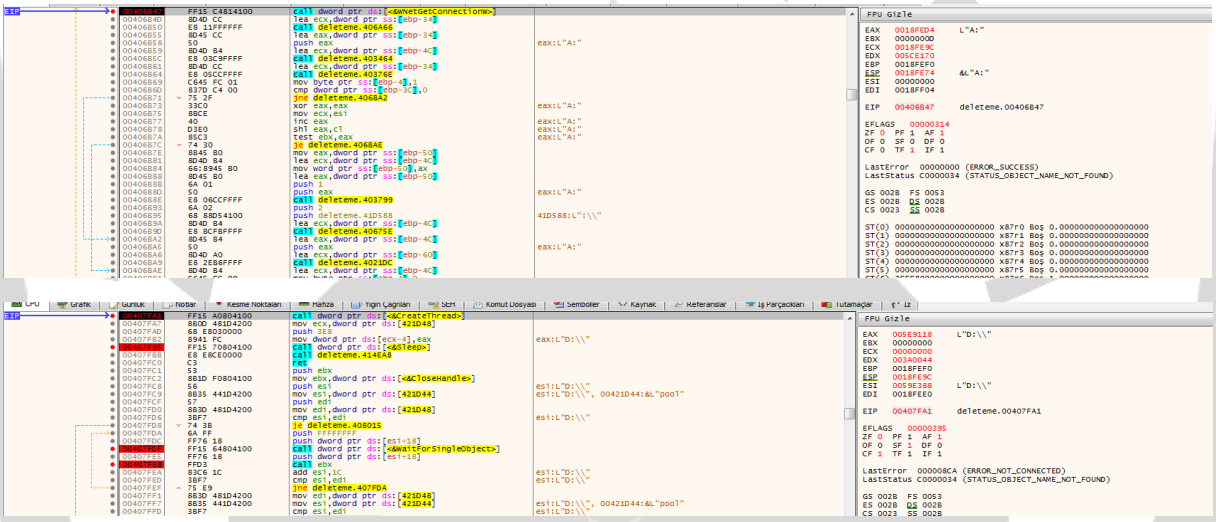
Sistemde kaç diskin tanımlı olduğunu kontrol eder.



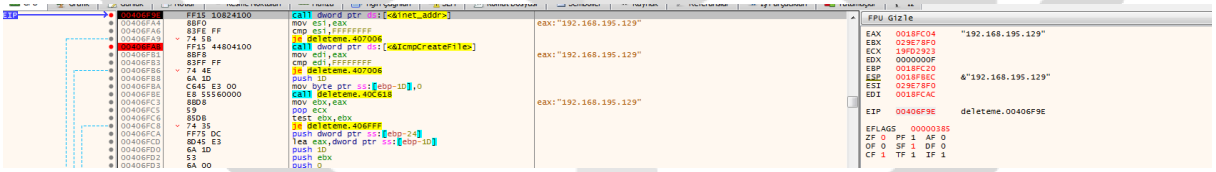
ASCII olarak encode halde tutulan veriler decode edildiğinde "ext":" , "network":" , "subid":" , "lang":" , {PATTERN_ID} , {UID} gibi verileri almakta olduğu tespit edilmiştir.



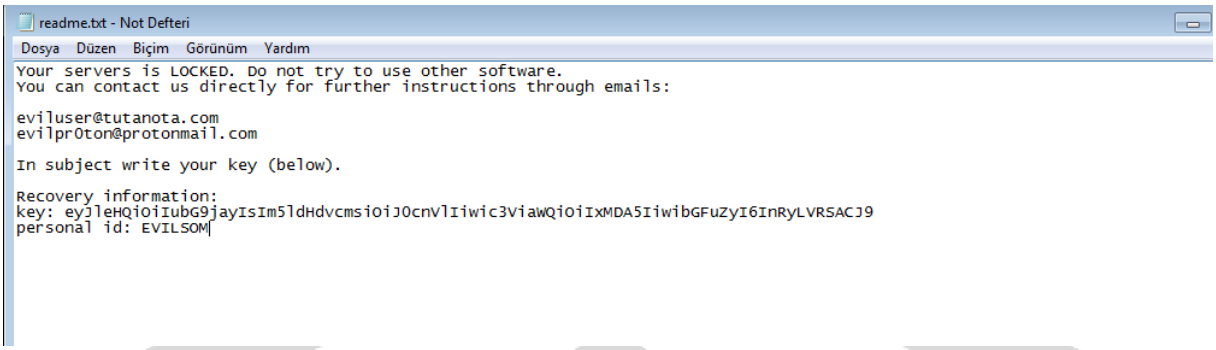
Zararlı, sistem dilini almaktadır.



Sistemde bulunan yerel diskleri kontrol etmektedir.



Sistemin local IP adresini almaktadır.



Dosyaları şifreleme işlemi bittikten sonra readme.txt dosyasını oluşturmakta, bu dosyanın içerisinde kurban bilgisayara özel bir anahtar tanımlamakta daha sonra şifrelediği dosyaları kurtarması için yine bu dosyanın içerisinde bulunan protonmail adresi ile iletişime geçilmesi gerektiğini belirtmektedir.

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.

Yara Kuralı

```
import  "hash"

rule Ranzy_Locker

{

meta:

author = "ZAYOTEM-TAHA HİCRET"

description = "RanzyLocker"

first_date = "21.10.2020"

report_date = "05.08.2021"

file_name = "deleteme.exe"

strings:

$s1 = "476C6F62616C5C33353335354641352D303745392D343238422D423541352D31433838434141423242343838"

$s2 = "776D69632E6578652053484144 4F57434F5059202F6E6F696E746572616374697665"

$s3 ="776261646D696E2044454C4554452053595354454D53544154454241434B5550"

$s4 ="776261646D696E2044454C4554452053595354454D53544154454241434B5550202D64656C6574654F6C64657374"

$s5 ="626364656469742E657865202F736574207B64656661756C747D207265636F76657279656E61626C6564204E6F"

$s6
="626364656469742E657865202F736574207B64656661756C747D20626F6F7473746174747573706F6C6963792069676E6F7265616C6C6661696C75726573"

$s7 ="76737361646D696E2E6578652044656C6574652053686861646F7773202F416C6C202F5175696574"

$s8 ="433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572"

$s9 ="534F4654574152455C4D6963726F736F66745C45524944"

condition:

hash.md5(0, filesize) == "84e8bf44a339c6c2a51aedb17b52e83e"

or

all

of

them

}
```

Hazırlayan

Taha HİCRET

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