Vidar

TEKNİK ANALİZ RAPORU

ZAYOTEM
ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

Ön Bakış

Vidar zararlı yazılımı, ilk kez 2018 yılında güvenlik uzmanları tarafından keşfedildi. Bu kötü amaçlı yazılım, finansal bilgi hırsızlığı yapmak amacıyla tasarlanmıştır ve diğer benzer zararlı yazılımlar gibi, kullanıcıların bilgisayarlarına bulaşarak bilgi çalmak için çalışır.

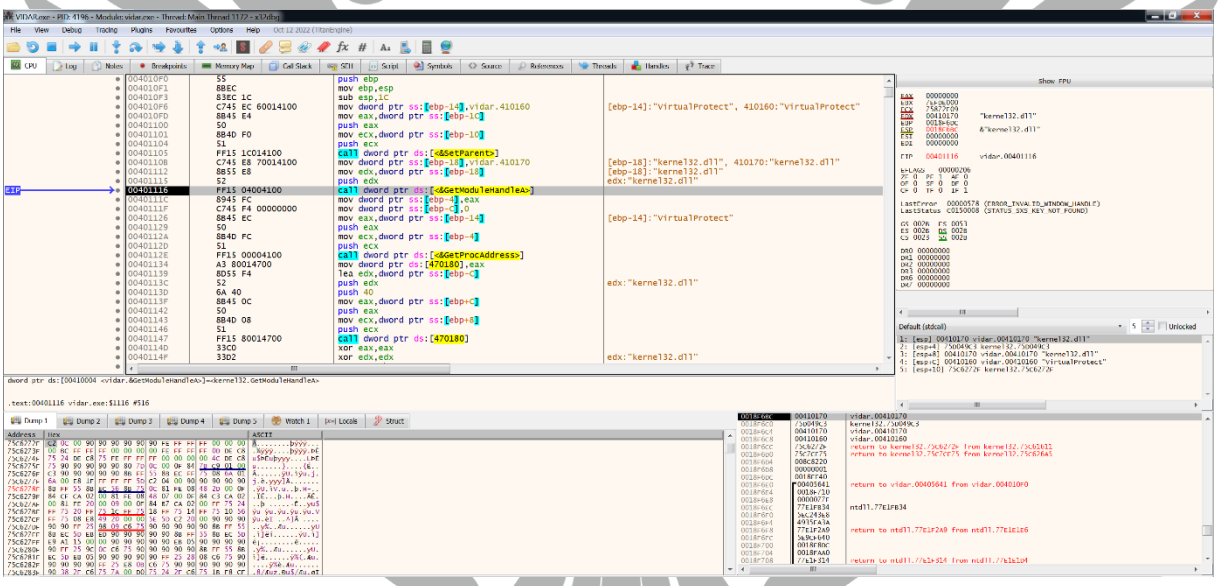
Vidar, özellikle finansal hedefleri olan kullanıcıları hedefleyen bir yazılımdır ve ödeme bilgilerinin yanı sıra, banka hesap bilgileri, para transferleri ve diğer finansal işlemler gibi önemli bilgileri de çalmayı hedefler. Bunun için kripto cüzdanlar ve internet tarayıcısı geçmişini kaydederek, hedeflenen bilgisayardaki tüm kişisel bilgileri toplamaya çalışır.

Dağıtım yöntemleri olarak spam e-postaları, sahte yazılım güncellemeleri, kötü amaçlı web siteleri ve çevrimiçi reklamlar gibi yöntemleri kullanabilir. Vidar'ın farklı sürümleri olduğu bilinmektedir ve her sürümü farklı özellikler gösterebilmektedir.

Vidar zararlı yazılımı, keşfedildiği tarihten bu yana, farklı sürümleriyle birlikte birçok bilgisayara bulaşmış ve finansal bilgi hırsızlığı yaparak birçok kullanıcının zarar görmesine neden olmuştur.

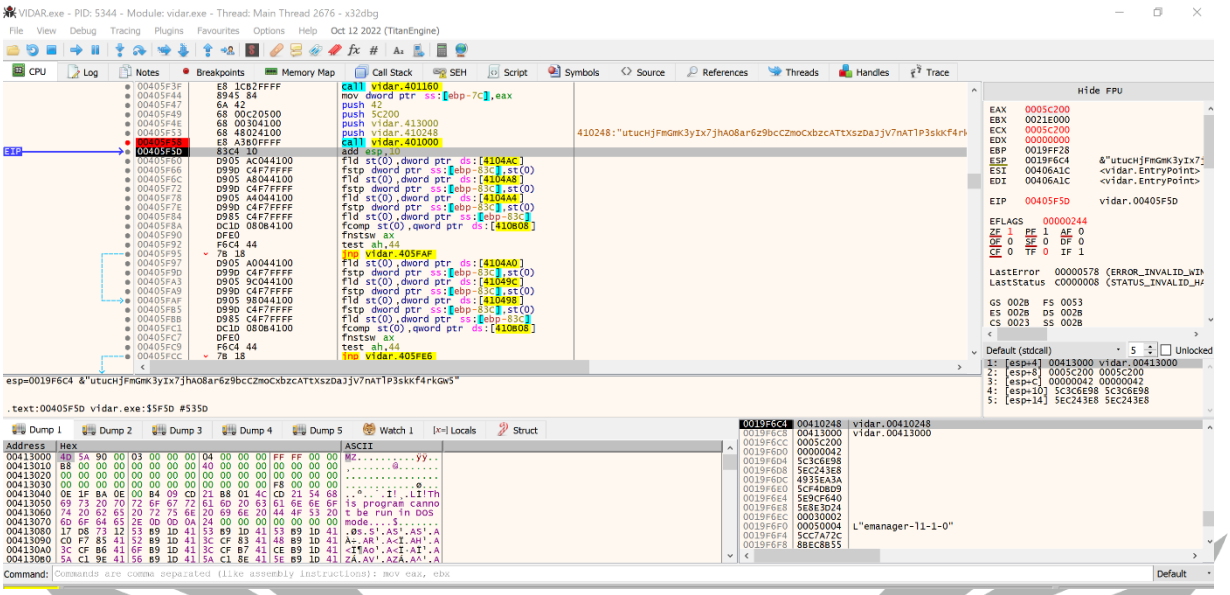
Setup.exe Analizi

Adı	Setup.exe
MD5	dcd26511183f2d7eb30678661a88b765
SHA256	8f0d2909498e32a88ea7a3873958edd5456e0d9d3e766ce7c8bcc303f67d8984
Dosya Türü	PE32 / EXE



Şekil 1- API Çözümlemesi

Zararlı, **GetModuleHandle** ve **GetProcAddress** API'leri ile yaptığı API çözümlemesi sonucunda **VirtualProtect** API'sini kullanarak belirtilen sanal bellek alanında yürütme, salt okunur veya okuma/yazma erişimini etkinleştirmiştir.



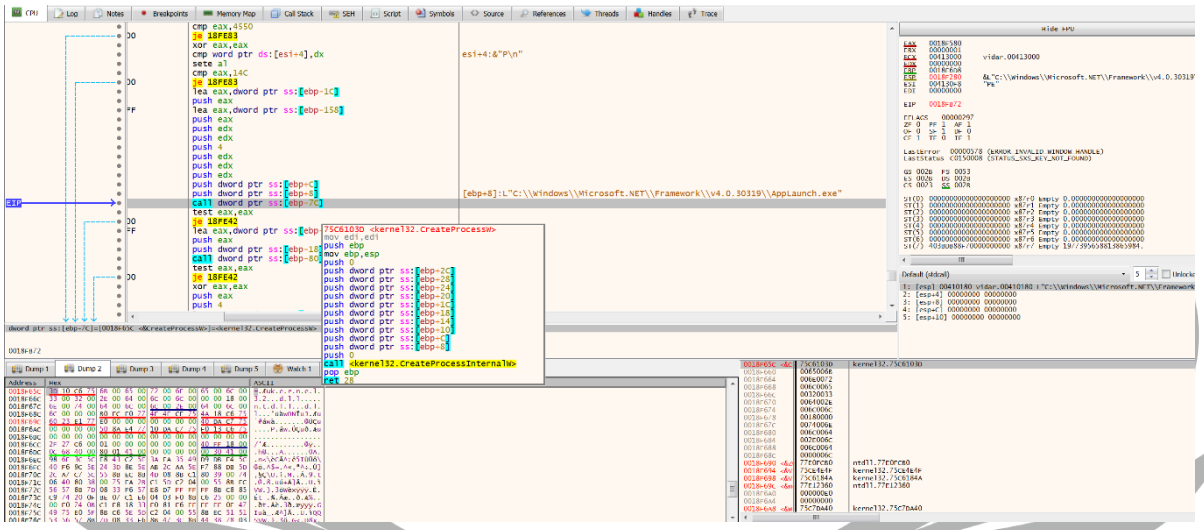
Şekil 2- Çözümlenmiş dosya

Zararlının çalışma anında çözümlediği **“MZ”** başlıklı dosya bulunmuştur.

```
1  unsigned int __cdecl sub_401000(int a1, int a2, unsigned int a3)
2  {
3    unsigned int result; // eax
4    char v4; // [esp+7h] [ebp-5h]
5    unsigned int i; // [esp+8h] [ebp-4h]
6
7    for ( i = 0; i < a3; ++i )
8    {
9      SetActiveWindow(hWnd);
10     v4 = (36 * *(_BYTE *)(a1 + (int)i % 60)) & 0x70 ^ *(_BYTE *)(i + a2);
11     *(_BYTE *)(i + a2) = 2 * v4;
12     *(_BYTE *)(i + a2) -= v4;
13     result = i + 1;
14   }
15   return result;
16 }
```

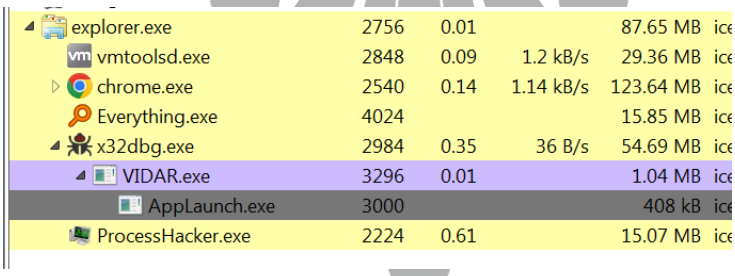
Şekil 3- Çözümleme algoritması

Process Hollowing



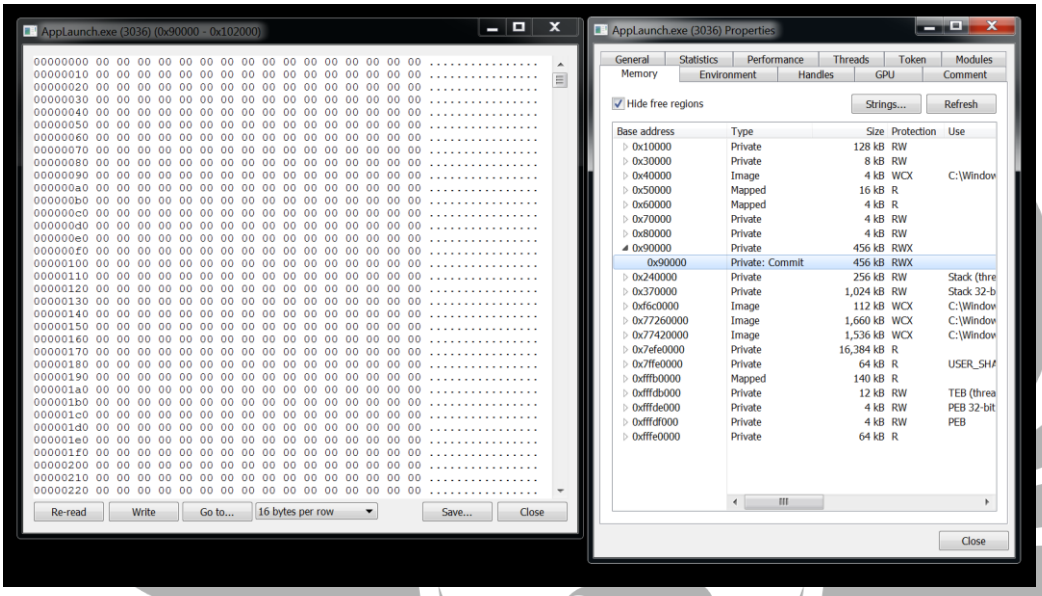
Şekil 4- CreateProcess API'si ile bir process başlatıldığı görülmekte.

Zararlı, **"CreateProcess"** API'ını kullanarak "suspend" durumda bir process oluşturmaktadır. Bu processin tam yolunun "**C:\\Windows\\Microsoft.NET\\Framework\\v4.0.3019\\AppLaunch.exe**" olduğu görülmektedir.



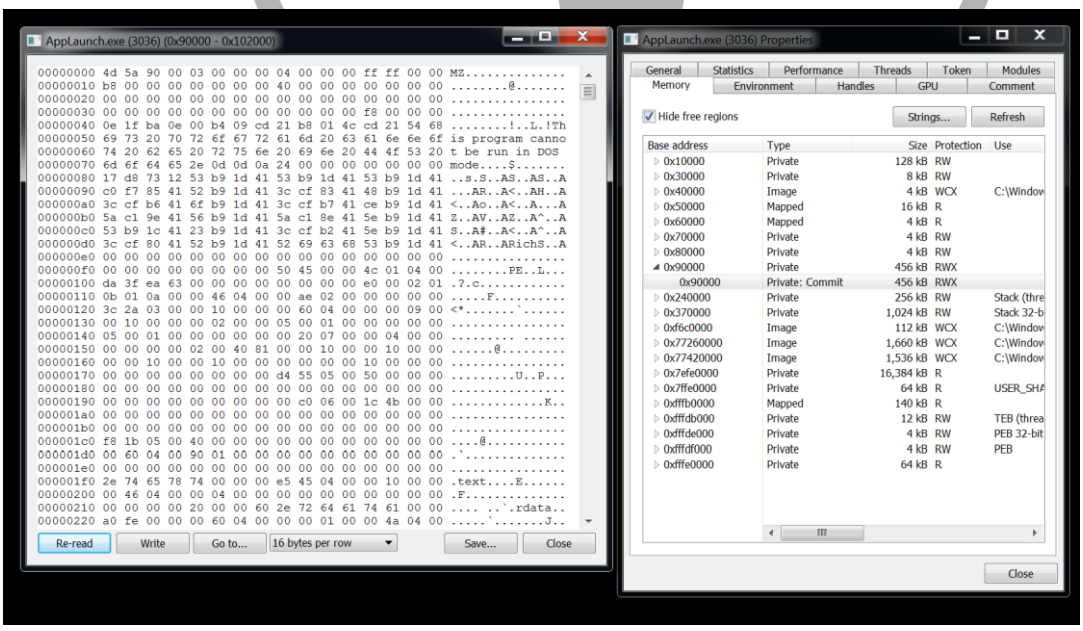
Şekil 5- AppLaunch.exe

Zararlının, **“VirtualAllocEx”** API’sini kullanarak “suspend” durumda oluşturduğu processde bellek alanı ayırdığı görülmektedir.

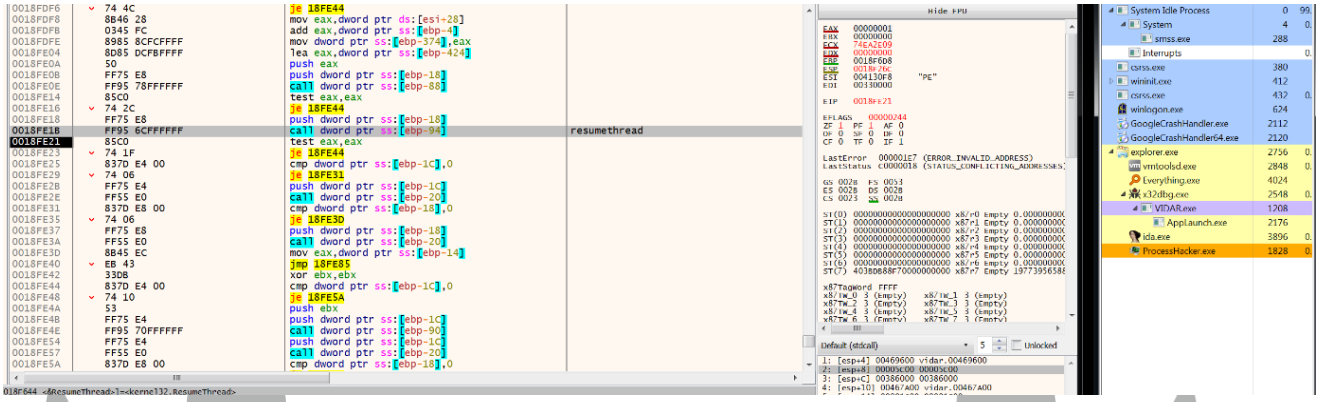


Şekil 6- Ayrılan bellek alanı

Bu bellek alanına çözümlediği çalıştırılabilir dosyayı, **“WriteProcessMemory”** API’sini kullanarak yazdığı görülmektedir.



Şekil 7- WriteProcessMemory API’si sonrası bellek alanı

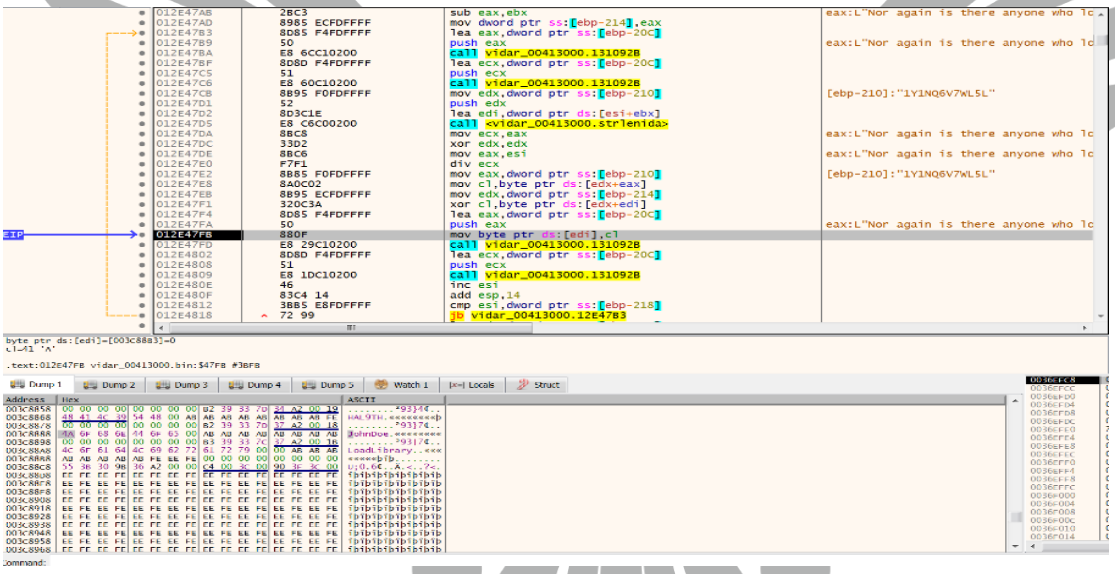


Şekil 8- ResumeThread API'sinin kullanılması

Yazma işlemi bittikten sonra **"ResumeThread"** API'si ile suspend durumdaki process aktif hale gelerek çalışmaya başlamaktadır.

Stage 2 Analizi

Adı	-
MD5	c404e69187afab5fd694570220660576
SHA256	279fff770c6678a1839799bd83aa9ace0c78380b9f93bd4b4a689c245382b4e6
Dosya Türü	PE32 / EXE

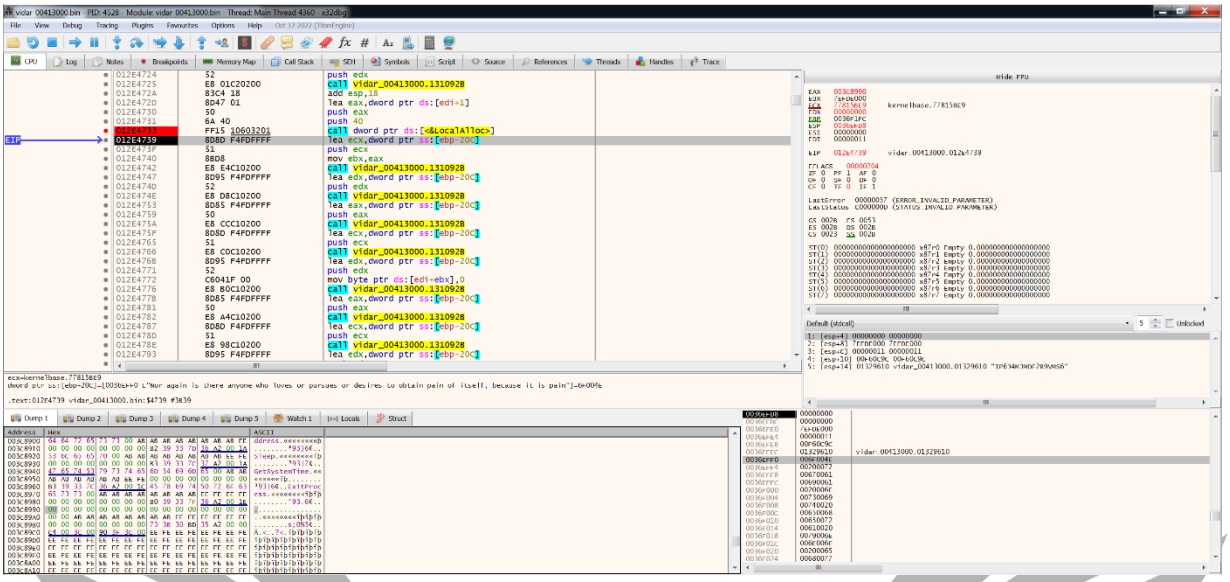


Şekil 9- Şifrelenmiş metinlerin çözümlenmesi

Zararlı şifreleme algoritması kullanarak baz aldığı **“Nor again is there anyone who loves or pursues or desires to obtain pain of itself, because it is pain"** stringini ve her şifreli stringi çözümlemek için kullanacağı benzersiz bir anahtar kullanmaktadır.

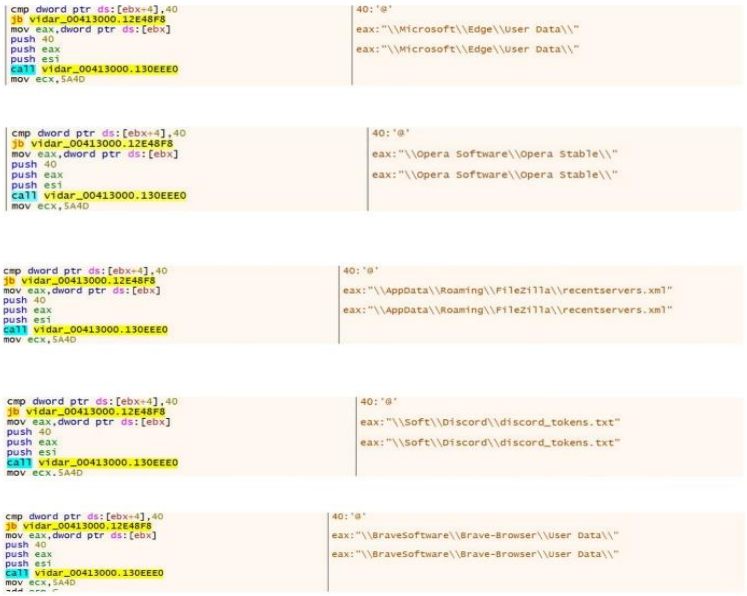
Zararlının kullanacağı çözümlenen stringler bu yöntemi kullanarak çözümlenmiştir.

Örneklerine Tablo-1 ve Tablo-2’de yer verilmiştir.



Şekil 10- LocalAlloc API'sinin kullanılması

Çözümlenmiş string ifadelerin **"LocalAlloc"** kullanarak ayrılan bellek alanına yazıldığı görülmektedir.

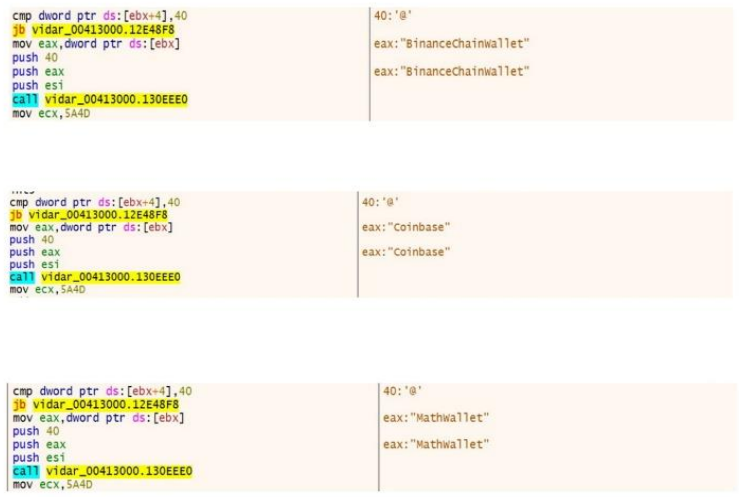


Şekil 11- Bilgi toplamak için kullanılan bazı tarayıcı dizinleri

Zararlı hassas verileri elde etmek için dizin taraması yapmaktadır. Tarama yaptığı dizinlere Tablo-1'de yer verilmiştir.

MicrosoftEdge\\Cookies	\\AppData\\Roaming\\FileZilla\\recentservers.xml
\\Mozilla\\Firefox\\Profiles\\	\\Moonchild Productions\\Pale Moon\\Profiles\\
\\Google\\Chrome\\User Data\\	\\Chromium\\User Data\\
\\Amigo\\User Data\\	\\Torch\\User Data\\
\\Comodo\\Dragon\\User Data\\	\\Epic Privacy Browser\\User Data\\
\\Vivaldi\\User Data\\	\\CocCoc\\Browser\\User Data\\
\\CentBrowser\\User Data\\	\\TorBro\\Profile\\
\\Chedot\\User Data\\	\\7Star\\7Star\\User Data\\
\\Microsoft\\Edge\\User Data\\	\\360Browser\\Browser\\User Data\\
\Tencent\\QQBrowser\\User Data\\	\\Opera Software\\Opera Stable\\
\\Opera Software\\Opera GX Stable\\	

Tablo 1-Tarayıcı dizinleri



Şekil 12- Bilgi toplamak için kullanılan bazı cüzdan isimleri

EQUALWallet	BitAppWallet	iWallet
Wombat	MewCx	GuildWallet
RoninWallet	NeoLine	CloverWallet
LiqualityWallet	Terra_Station	Keplr
AuroWallet	PolymeshWallet	ICONex
KardiaChain	EVER Wallet	Rabby
Harmony	Coin98	Ledger Live
Bitwarden	Leap Terra	Martian Wallet
Petra Wallet	Pontem Wallet	Gero Wallet
Eternl	Hashpack	OKX Web3 Wallet
Exodus Web3 Wallet	Trust Wallet	Tronium
Braavos	Enkrypt	Finnie

Tablo 2-Crypto Cüzdanlar

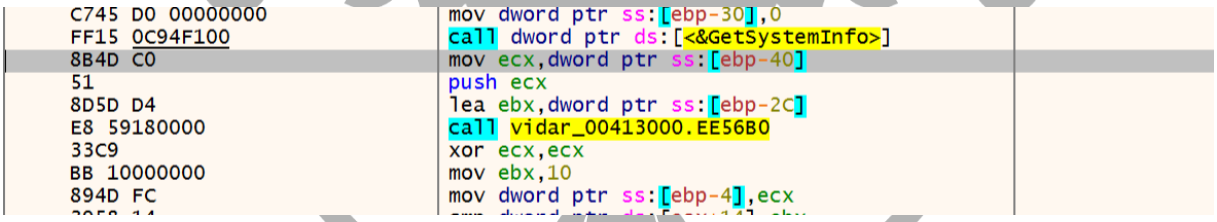
Zararlının hassas verileri elde etmek için “şifre yöneticisi” uygulamalarını hedef aldığı gözlemlenmiştir. Bunlara Tablo-3’te yer verilmektedir.

KeePass Tusk	Trezor Password Manager
KeePassXC-Browser	Microsoft AutoFill

Tablo 3-Şifre Yöneticileri

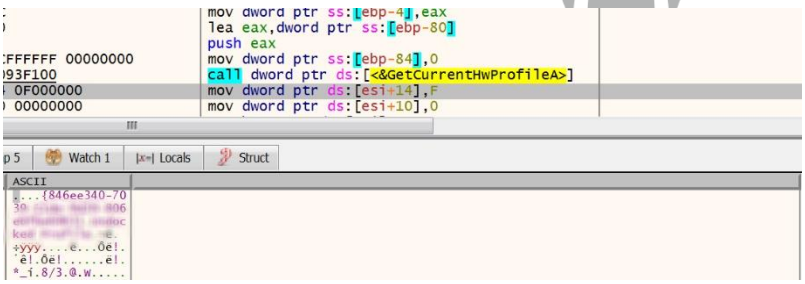
Zararlının sistem bilgilerini topladığı gözlemlenmiştir.

Şekil 13-MachineGuid bilgisinin alınması



Şekil 14-GetSystemInfo API’nın kullanılması

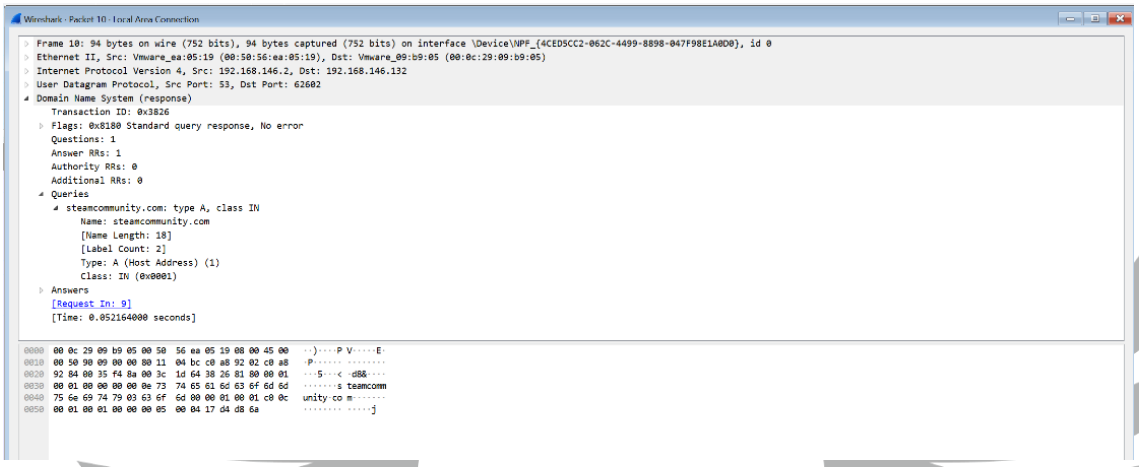
Zararlı **“GetSystemInfo”** API’si sayesinde işlemci mimarisi, işlemci türü, işlemci sayısı gibi sistem bilgilerini edinmektedir.



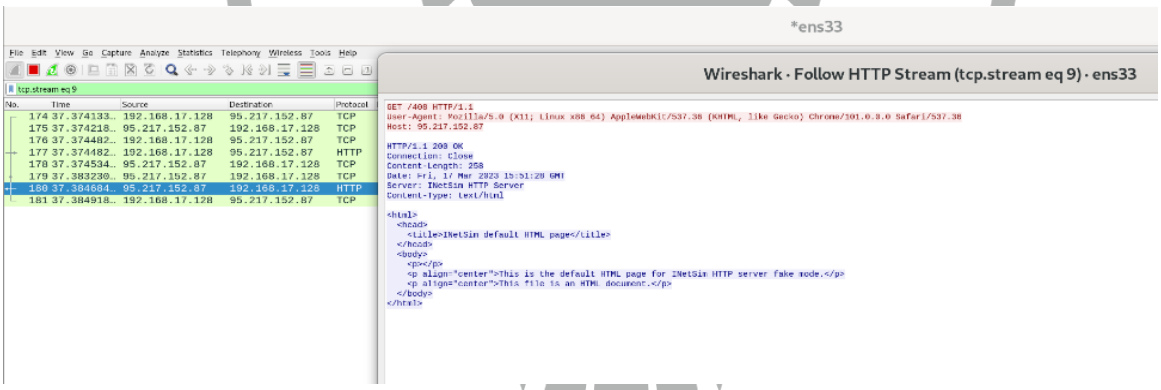
Şekil 15-GetCurrentHwProfileA API’nın kullanılması

“GetCurrentHwProfileA” API’si kullanılarak local bilgisayarın donanım profili hakkında bilgi toplanmaktadır.

Network Analizi



Şekil 16-DNS isteği

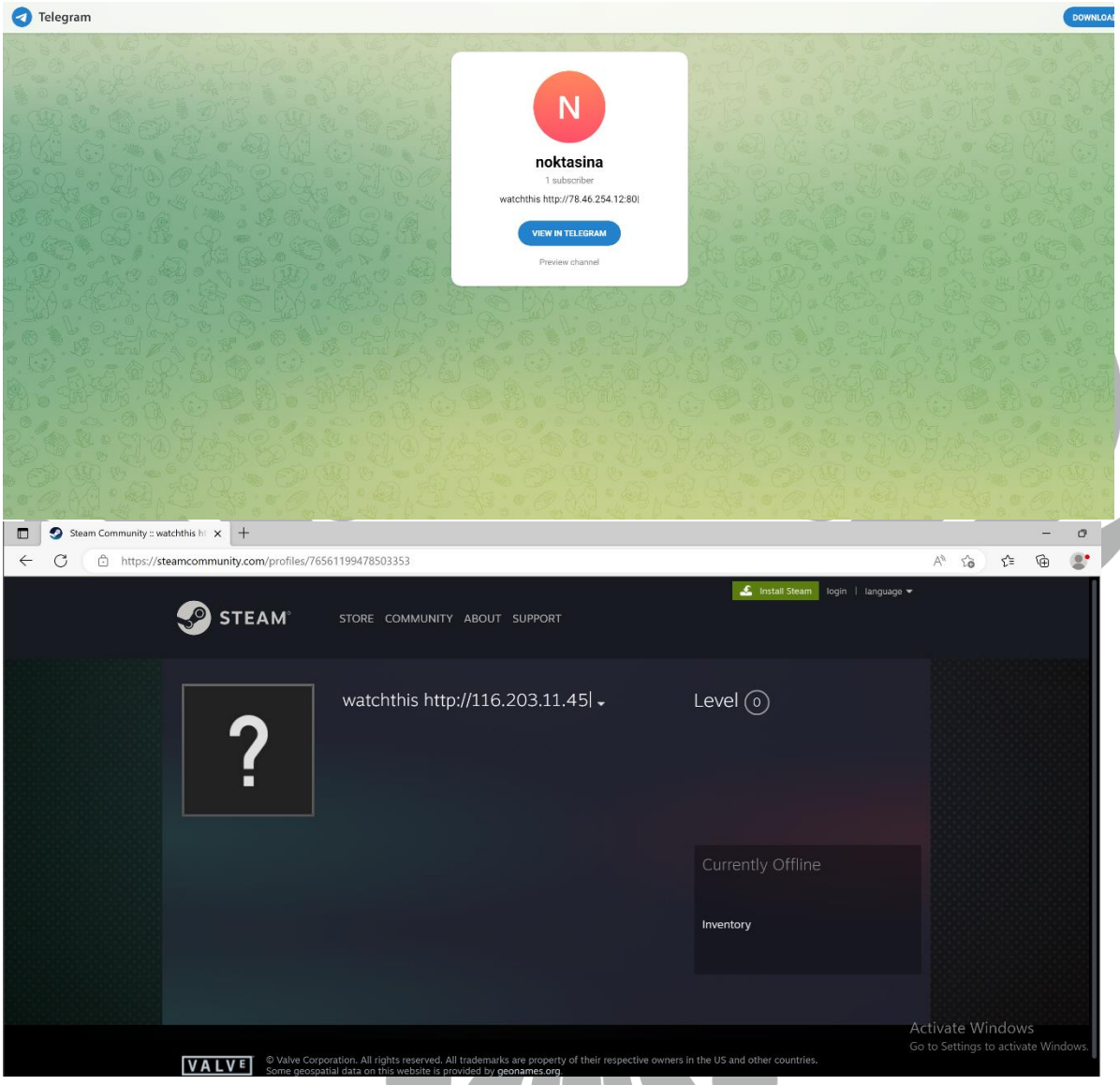


Şekil 17- HTTP GET isteği

Şekil 18-InternetReadFile API'sinin kullanılması

Zararlı dönen isteğin içeriğini "**InternetReadFile"** API'sini kullanarak okumaktadır.

C2 sunucuları kapalı olduğundan dolayı gönderilen istek başarısız olmaktadır.



Şekil 19-C2 servers

http://116[.]203[.]11[.]45/408	https://steamcommunity.com/profiles/76561199478503353
http://95[.]217[.]152[.]87:80	https://t.me/noktasina
http://95[.]217[.]152[.]87:80/epson.zip	

Tablo 3-URLs

YARA Kuralı

```
import "hash"

rule vidar_rule {

    meta:

        description = "This is a YARA rule"

        author = "Dilara Behar"

    strings:

        $watchthis = "watchthis"

        $epson_zip = "epson.zip"

        $caf_racer = "A caf\\? racer is a genre of sport motorcycles that originated among British motorcycle enthusiasts of the early 1960s in London"

        $user_agent = "Mozilla\\/5\\.0 \\(X11\\; Linux x86\\_64\\) AppleWebKit\\/537\\.36 \\(KHTML\\, like Gecko\\) Chrome\\/101\\.0\\.0\\.0 Safari\\/537\\.36"

  $st="https:\\/\\/steamcommunity\\.com\\/profiles\\/76561199478503353"

  $update_zip="update.zip"

condition:


  hash.md5(0, filesize) == "dcd26511183f2d7eb30678661a88b765" or
   any of them
}
```

MITRE ATTACK TABLE

Reconnaissance	Execution	Discovery	Privilege Escalation	Defense Evasion	Credential Access	C&C	Collection
	T1106-Native API	T1083- File and Directory Discovery	T1055- Process Hollowing	T1055- Process Hollowing		T1573 - Encrypted Channel	T1005- Data from Local System
		T1087- Account Discovery				T1071- Application Layer Protocol	
		T1082- System Information Discovery					

Çözüm Önerileri

1. Antivirüs yazılımı kullanmak, zararlı yazılımların tespiti ve kaldırılması için en etkili yöntemlerden biridir. Antivirüs yazılımı, bilgisayarınıza indirdiğiniz veya açtığınız dosyaları ve web sitelerini tarayarak zararlı yazılımları tespit edebilir. İkinci çözüm önerisi
2. İşletim sistemi ve diğer yazılımlarınızın güncellemelerini düzenli olarak yaparak, bilgisayarınızın güvenliğini sağlayabilirsiniz. Güncellemeler, çeşitli güvenlik açıklarının kapatılmasına yardımcı olur.
3. Dosya indirmeleri yaparken güvenilir kaynaklardan indirmeye özen gösterin. Bilinmeyen veya şüpheli kaynaklardan indirilen dosyaların içinde zararlı yazılımlar olabilir.

HAZIRLAYAN

Dilara BEHAR

https://www.linkedin.com/in/dilara-behar-0530b3195