

Vidar

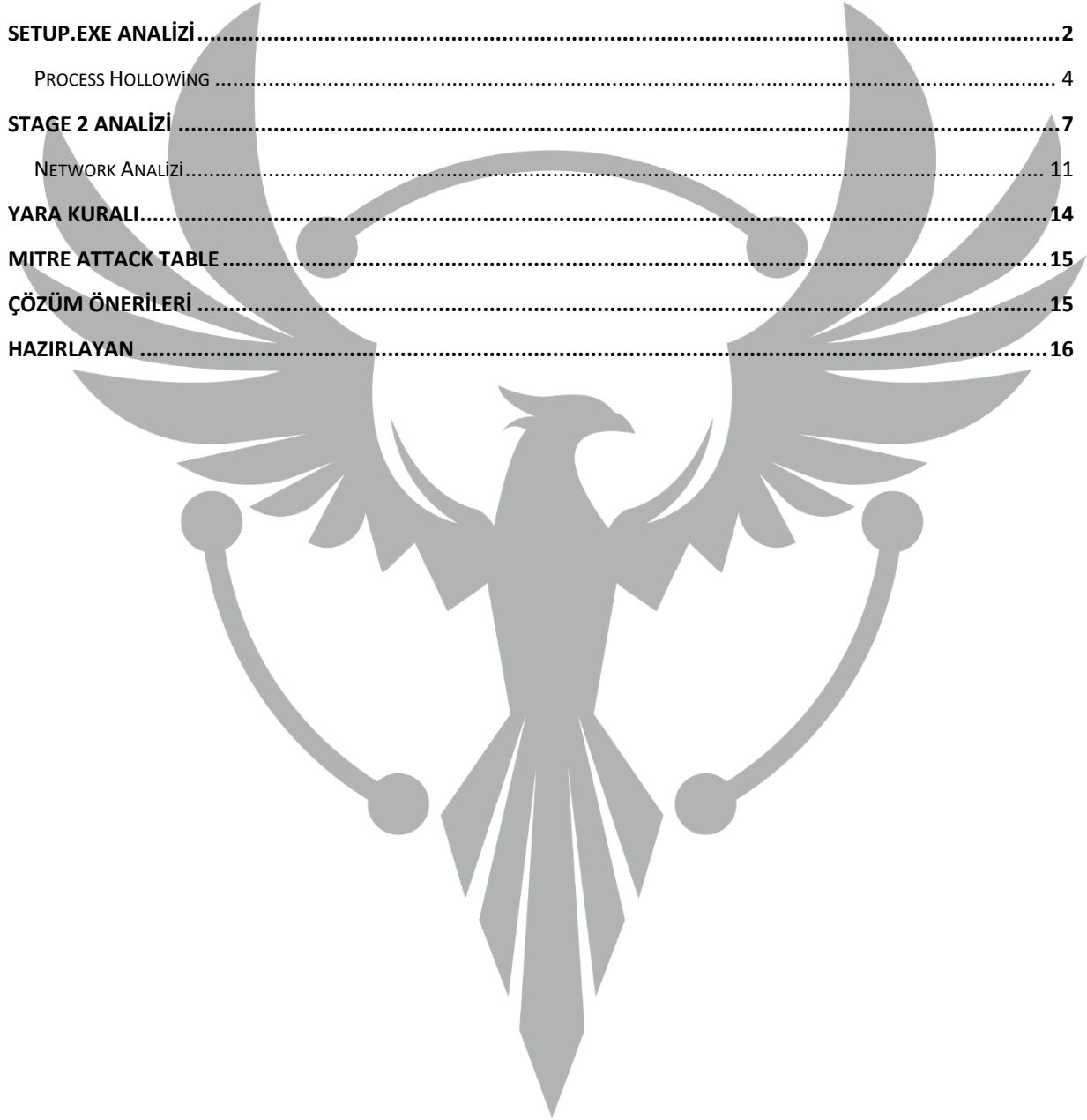
TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN BAKIŞ	1
SETUP.EXE ANALİZİ	2
PROCESS HOLLOWING	4
STAGE 2 ANALİZİ	7
NETWORK ANALİZİ	11
YARA KURALI	14
MITRE ATTACK TABLE	15
ÇÖZÜM ÖNERİLERİ	15
HAZIRLAYAN	16



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	8f0d2909498e32a88ea7a3873958edd5456e0d9d3e766ce7c8bcc3 03f67d8984
Dosya Türü	PE32 / EXE

```
004010FD 55          push ebp
004010FE 8BEC       mov  ebp,esp
004010F3 83EC       sub  esp,1C
004010F6 C745 EC 00410160  mov  dword ptr [ebp-14],vldar.410160
004010FD 8B45 E4    mov  eax,dword ptr [ebp-10]
00401100 50          push  eax
00401101 8B4D F0    mov  ecx,dword ptr [ebp-10]
00401104 51          push  ecx
00401105 FF15 LC014100  call dword ptr [kernel32.GetModuleHandleA]
00401108 C745 E8 70014100  mov  dword ptr [ebp-18],vldar.410170
00401112 8B55 E8    mov  ecx,dword ptr [ebp-18]
00401115 52          push  ecx
00401116 FF15 0A004100  call dword ptr [kernel32.GetModuleHandleA]
0040111F C745 F4 00000000  mov  dword ptr [ebp-10],0
00401126 8B45 EC    mov  eax,dword ptr [ebp-14]
00401129 50          push  eax
0040112A 8B4D FC    mov  ecx,dword ptr [ebp-14]
0040112D 51          push  ecx
0040112E FF15 00004100  call dword ptr [kernel32.GetProcAddress]
00401134 A3 00147000  mov  dword ptr [470180],eax
00401139 8D55 F4    lea  edx,dword ptr [ebp-8]
0040113C 52          push  edx
0040113D 6A 40     push  40
0040113F 8B4D 0C    mov  ecx,dword ptr [ebp-4]
00401142 50          push  ecx
00401143 8B4D 08    mov  ecx,dword ptr [ebp-8]
00401146 51          push  ecx
00401147 FF15 80014700  call dword ptr [470180]
0040114F 3302     xor  eax,eax
00401150 3302     xor  ecx,ecx
```

Şekil 1- API Çözülmesi

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- Çözümlemiş dosya

Zararlının çalışma anında çözümlediği “MZ” başlıklı dosya bulunmuştur.

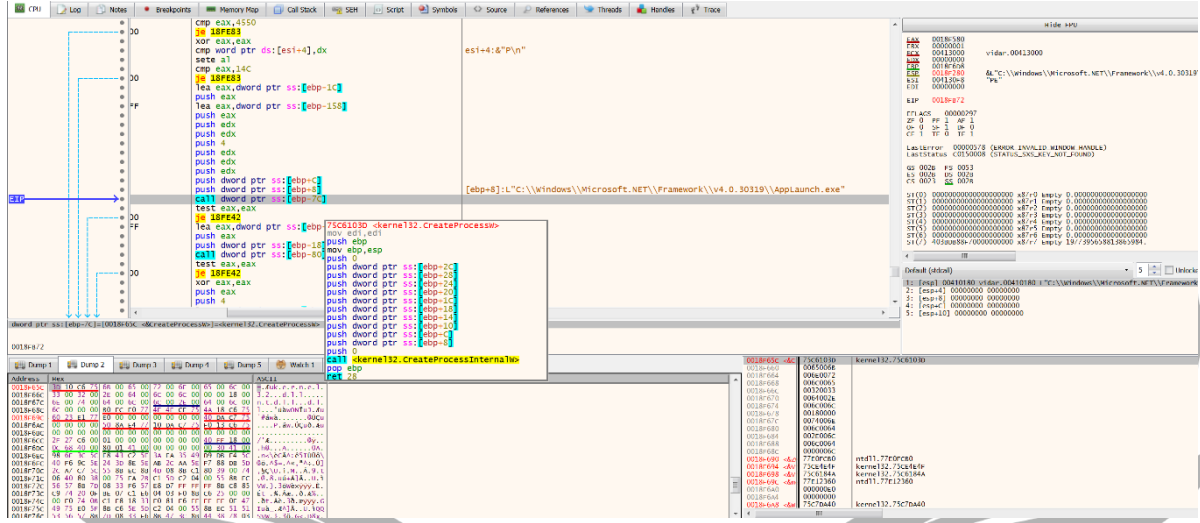
```

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



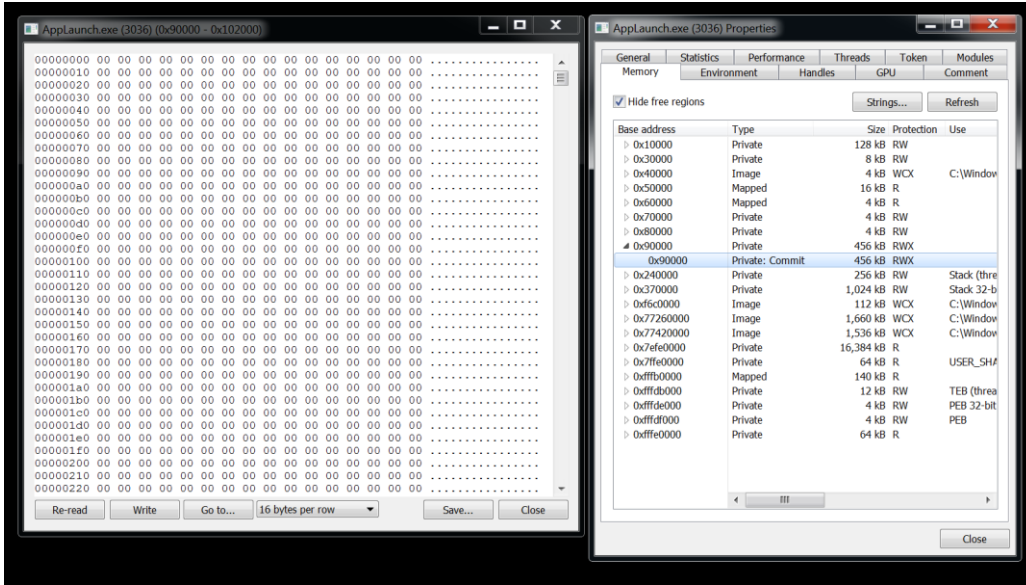
Şekil 4- CreateProcess API'si ile bir process başlatıldığı görülmekte.

Zararlı, “CreateProcess” API’ini kullanarak “suspend” durumda bir process oluşturmaktadır. Bu processin tam yolunun “C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe” olduğu görülmektedir.

explorer.exe	2756	0.01		87.65 MB	ice
vm vmtoolsd.exe	2848	0.09	1.2 kB/s	29.36 MB	ice
chrome.exe	2540	0.14	1.14 kB/s	123.64 MB	ice
Everything.exe	4024			15.85 MB	ice
x32dbg.exe	2984	0.35	36 B/s	54.69 MB	ice
VIDAR.exe	3296	0.01		1.04 MB	ice
AppLaunch.exe	3000			408 kB	ice
ProcessHacker.exe	2224	0.61		15.07 MB	ice

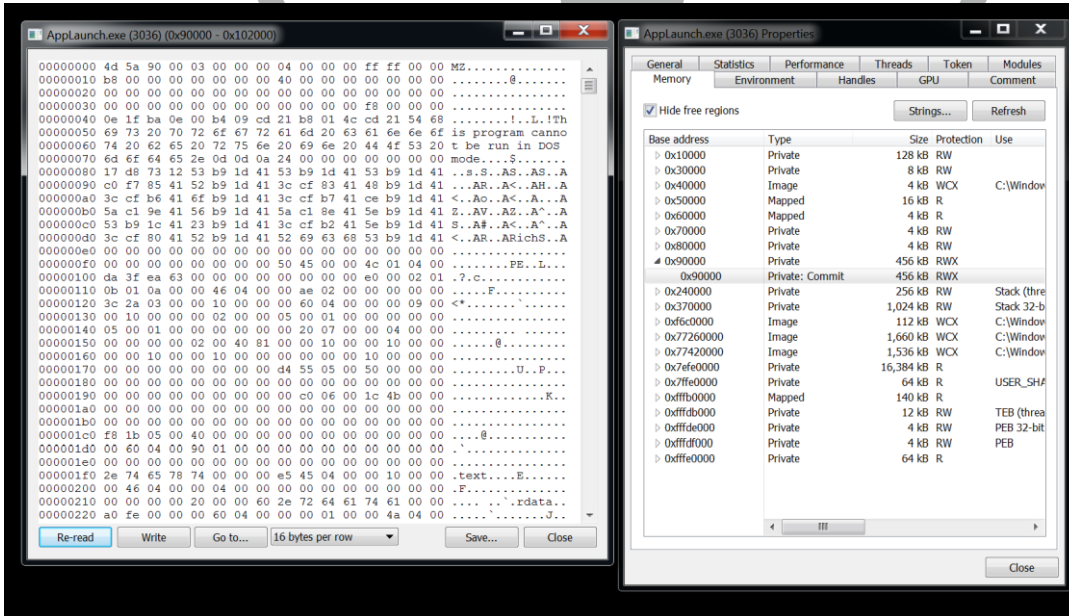
Şekil 5- AppLaunch.exe

Zararının, “VirtualAllocEx” API’sini kullanarak “suspend” durumda oluşturduğu processte 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

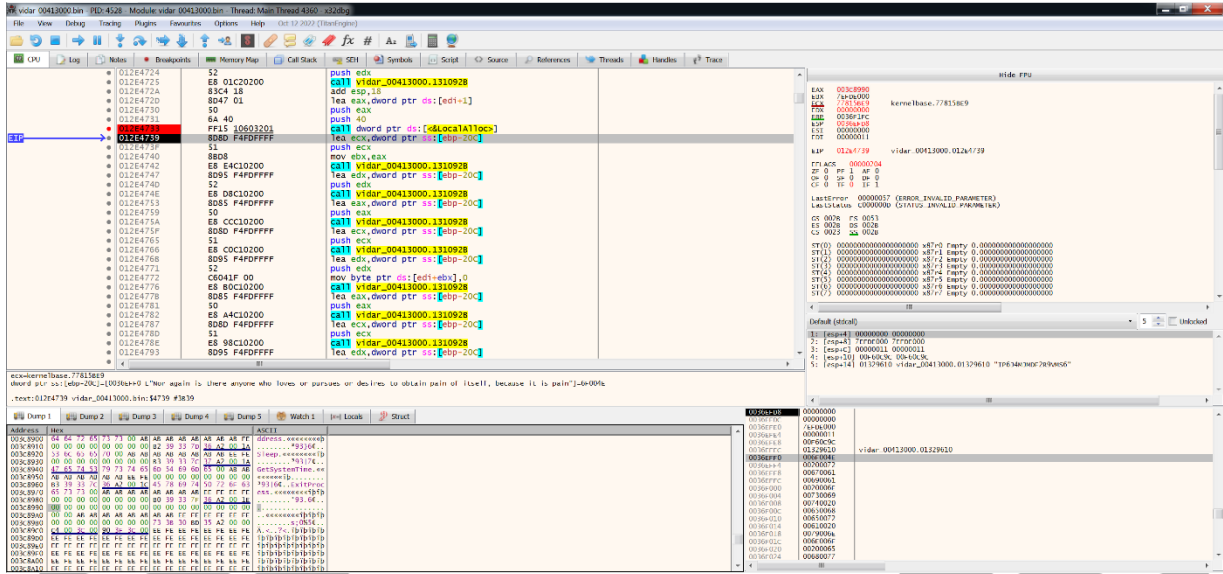
Adı	-
MD5	c404e69187afab5fd694570220660576
SHA256	279fff770c6678a1839799bd83aa9ace0c78380b9f93bd4b4a689c2453826
Dosya Türü	PE32 / EXE

Şekil 9- Şifrelenmiş metinlerin çözülmesi

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.

Zararının kullanacağı çözümlenen stringler bu yöntemi kullanarak çözümlenmiştir.

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



Şekil 10- LocalAlloc API'sinin kullanılması

Çözülenmiş string ifadelerin “LocalAlloc” kullanarak ayrılan bellek alanına yazıldığı görülmektedir.

<pre> cmp dword ptr ds:[ebx+4],40 jb vidar_00413000.12E48F8 mov eax,dword ptr ds:[ebx] push 40 push eax push esi call vidar_00413000.130EEED mov ecx,5A4D </pre>	40: 'e'	<pre> eax: "\\Microsoft\\Edge\\User Data\\" eax: "\\Microsoft\\Edge\\User Data\\" </pre>
<pre> cmp dword ptr ds:[ebx+4],40 jb vidar_00413000.12E48F8 mov eax,dword ptr ds:[ebx] push 40 push eax push esi call vidar_00413000.130EEED mov ecx,5A4D </pre>	40: 'g'	<pre> eax: "\\opera Software\\opera Stable\\" eax: "\\opera Software\\opera Stable\\" </pre>
<pre> cmp dword ptr ds:[ebx+4],40 jb vidar_00413000.12E48F8 mov eax,dword ptr ds:[ebx] push 40 push eax push esi call vidar_00413000.130EEED mov ecx,5A4D </pre>	40: 'g'	<pre> eax: "\\AppData\\Roaming\\FileZilla\\recentservers.xml" eax: "\\AppData\\Roaming\\FileZilla\\recentservers.xml" </pre>
<pre> cmp dword ptr ds:[ebx+4],40 jb vidar_00413000.12E48F8 mov eax,dword ptr ds:[ebx] push 40 push eax push esi call vidar_00413000.130EEED mov ecx,5A4D </pre>	40: 'g'	<pre> eax: "\\soft\\Discord\\discord_tokens.txt" eax: "\\soft\\Discord\\discord_tokens.txt" </pre>
<pre> cmp dword ptr ds:[ebx+4],40 jb vidar_00413000.12E48F8 mov eax,dword ptr ds:[ebx] push 40 push eax push esi call vidar_00413000.130EEED mov ecx,5A4D </pre>	40: 'g'	<pre> eax: "\\BraveSoftware\\Brave-Browser\\User Data\\" eax: "\\BraveSoftware\\Brave-Browser\\User Data\\" </pre>

Şekil 11- Bilgi toplamak için kullanılan bazı tarayıcı dizinleri

Zararlı hassas verileri elde etmek için izin 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

```

cmp dword ptr ds:[ebx+4],40
jb vidar_00413000.12E48F8
mov eax,dword ptr ds:[ebx]
push 40
push eax
push esi
call vidar_00413000.130EEE0
mov ecx,5A4D
40:'@'
eax:"BinanceChainWallet"
eax:"BinanceChainWallet"

cmp dword ptr ds:[ebx+4],40
jb vidar_00413000.12E48F8
mov eax,dword ptr ds:[ebx]
push 40
push eax
push esi
call vidar_00413000.130EEE0
mov ecx,5A4D
40:'@'
eax:"Coinbase"
eax:"Coinbase"

cmp dword ptr ds:[ebx+4],40
jb vidar_00413000.12E48F8
mov eax,dword ptr ds:[ebx]
push 40
push eax
push esi
call vidar_00413000.130EEE0
mov ecx,5A4D
40:'@'
eax:"Mathwallet"
eax:"Mathwallet"

```

Şekil 12- Bilgi toplamak için kullanılan bazı cüzdan isimleri

EQUALWallet	BitAppWallet	iWallet
Wombat	MewCx	GuildWallet
RoninWallet	NeoLine	CloverWallet
LiquidityWallet	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
Eternal	Hashpack	OKX Web3 Wallet
Exodus Web3 Wallet	Trust Wallet	Tronium
Braavos	Enkrypt	Finnie

Tablo 2-Crypto Cüzdanlar

Zararlıının 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

Zararlıının sistem bilgilerini topladığı gözlemlenmiştir.

Şekil 13-MachineGuid bilgisinin alınması

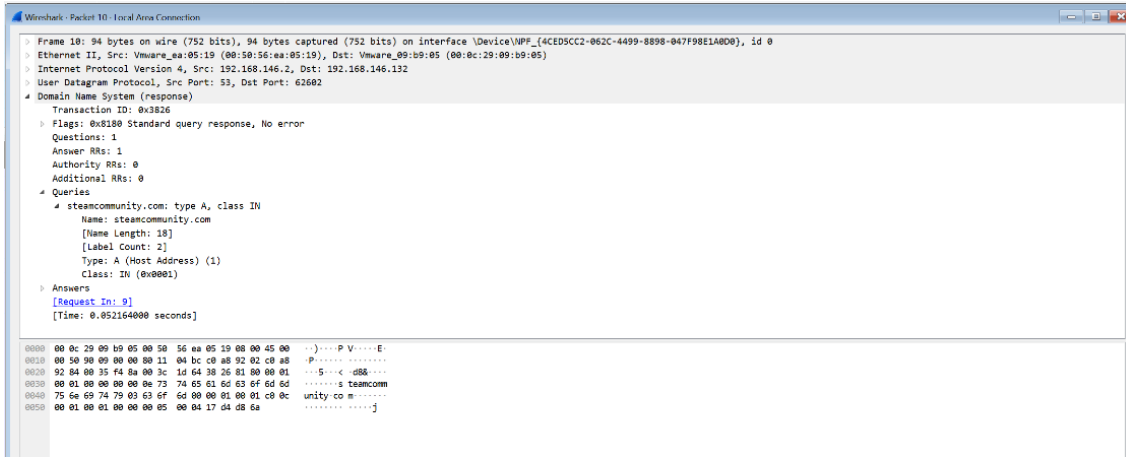
Şekil 14-GetSystemInfo API’nin kullanılması

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

Şekil 15-GetCurrentHwProfileA API’nin kullanılması

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

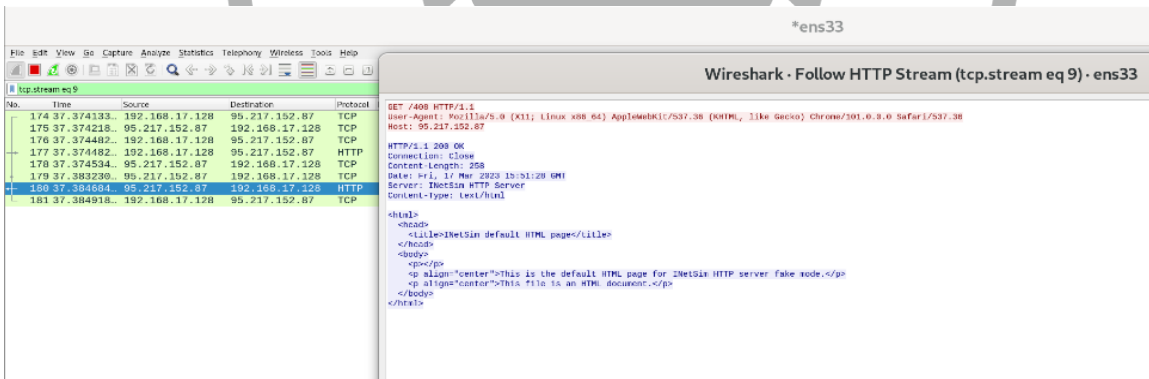
Network Analizi



```
Wireshark - Paket 10 - Local Area Connection
> Frame 10: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{4CED5CC2-862C-4499-8898-047F98E1A800}, id 0
> Ethernet II, Src: VMware_aa:09:19 (00:50:56:aa:09:19), Dst: VMware_00:09:05 (00:0c:29:09:09:05)
> Internet Protocol Version 4, Src: 192.168.146.2, Dst: 192.168.146.132
> User Datagram Protocol, Src Port: 53, Dst Port: 62692
* Domain Name System (response)
  Transaction ID: 0x3826
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  * Queries
  * steamcommunity.com: type A, class IN
    Name: steamcommunity.com
    [Name Length: 18]
    [Label Count: 2]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
  * Answers
  [Request In: 9]
  [Time: 0.052164000 seconds]

0000  00 0c 29 09 09 05 00 56 56 aa 09 19 00 00 45 00  ..P.V....E
0010  00 50 09 00 00 00 11 04 bc c8 a8 92 02 c8 a8  ..P.....
0020  92 04 00 35 f4 8a 00 3c 1d 64 38 26 81 00 00 01  ..S...c86...
0030  00 01 00 00 00 00 0e 73 74 65 61 60 63 6f 6d 6d  ..t...eamcomm
0040  75 6e 69 74 79 03 63 6f 6d 00 00 01 00 01 c8 0c  unity.co...
0050  00 01 00 01 00 00 00 00 00 04 17 04 08 8a  ..j
```

Şekil 16-DNS isteği



```
Wireshark - Follow HTTP Stream (tcp.stream eq 9) - ens33
GET /408 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/501.0.3.0 Safari/537.36
Host: 95.217.152.87

HTTP/1.1 200 OK
Connection: close
Content-Length: 258
Date: Wed, 11 Nov 2020 19:31:28 GMT
Server: IketSın HTTP Server
Content-type: text/html

<html>
<head>
<title>IketSın default HTML pages</title>
</head>
<body>
<p align="center">This is the default HTML page for IketSın HTTP server fake node.</p>
<p align="center">This file is an HTML document.</p>
</body>
</html>
```

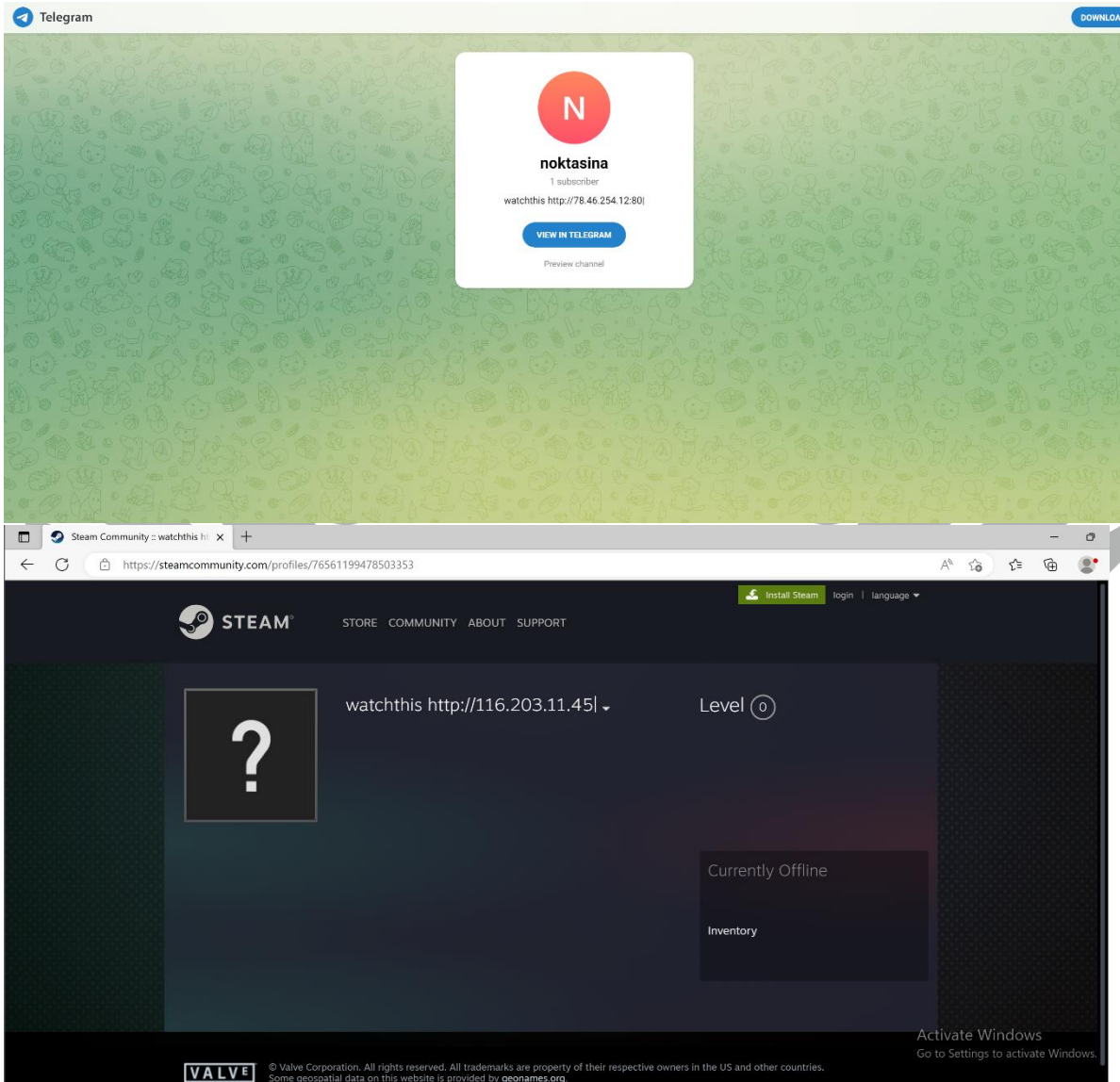
Şekil 17- HTTP GET isteği

```
00401000 .push 7CF
00401001 .lea ecx,dword ptr ss:[ebp-8E0]
00401002 .push ecx
00401003 .push esi
00401004 .call dword ptr ds:[!InternetReadFile]
00401005 .test eax,eax
00401006 .je vidar_00413000.12F2655
00401007 .nop
00401008 .mov eax,dword ptr ss:[ebp-9F0]
00401009 .test eax,eax
0040100A .je vidar_00413000.12F2655
0040100B .lea edx,dword ptr ss:[ebp-9A4]
0040100C .mov byte ptr ss:[ebp+eax-8E0],0
0040100D .push edx
0040100E .lea eax,dword ptr ss:[ebp-8FC]
0040100F .push eax
00401010 .lea ebx,dword ptr ss:[ebp-8E0]
00401011 .call !vidar_00413000.mayconcatz
00401012 .add esp,8
00401013 .mov edi,eax
00401014 .lea esi,dword ptr ss:[ebp-9A4]
00401015 .mov hvte ntr,sc:[ehh-4] 19
00401016 .
```

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/epon.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 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>