VIRUT

TEKNİK ANALİZ RAPORU

ZAYOTEM
ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İÇİNDEKİLER

Ön Bakış

Virut, yaklaşık olarak 2006 yılından itibaren aktif ve çoğunlukla DDoS saldırıları için kullanılan bir botnet zararlısıdır. Zararlı USB, zafiyetli siteler veya diğer medyalardan bulaşabilmektedir. Symantec'e göre 2012 de Dünya genelinde ele geçirdiği bilgisayar sayısının 300,000'den fazla olduğu varsayılmaktadır. Analizi yapılmış olan sample Windows Serverlarını hedef almaktadır. Bu kötü amaçlı yazılım bulaşmış olduğu bilgisayarın;

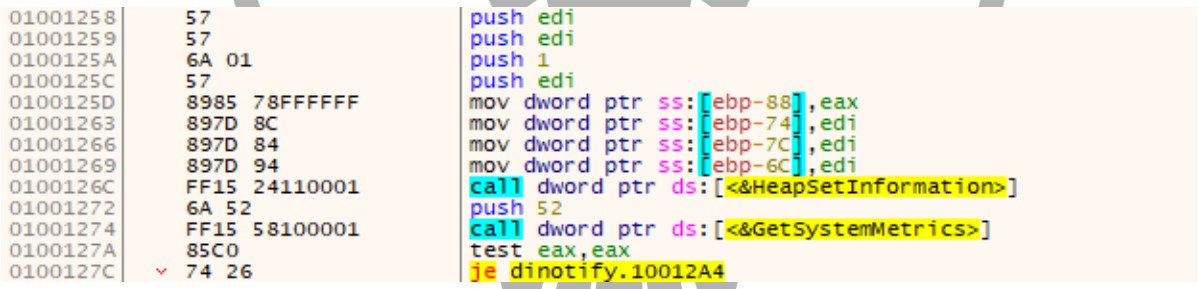
- Remote bağlantı kurarak uzaktan yönetilmesini,
- Network içerisinde yayılarak diğer cihazları enfekte etmesini hedeflemiştir.

DINOTIFY.EXE.exe Analizi

Adı	DINOTIFY.EXE.exe
MD5	19685224d240dc0eea1970b0e4840199
SHA256	6c2493a7d33d0e98fa11ca18e96e313aef8b89b3d6ae0e10c16523a38c871ce6
Dosya Türü	x32 Executable

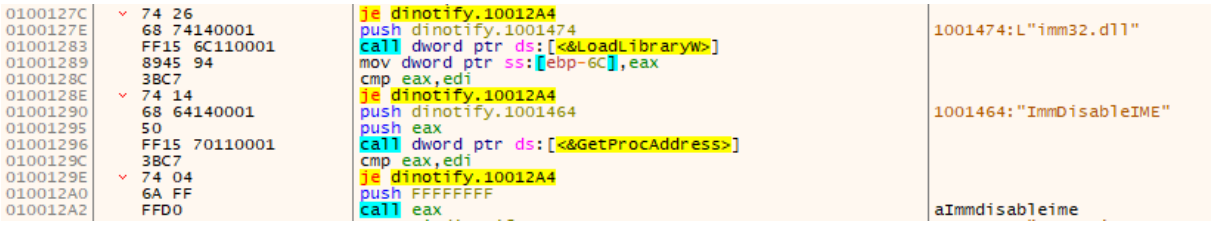
Dinamik Analiz

HeapSetInformation API HeapEnableTerminationOnCorruption parametresi ile çalıştırılarak hata anında program kapanmaya ayarlanmıştır. Ardından GetSystemMetrics API ile IMM/IME özelliklerinin açık olup olmadığını kontrol edilmektedir.



Şekil 1- HeapSetInformation / GetsystemMetrics API

IME(Input Method Editor) aktif olması durumunda imm32.dll içerisinden ImmDisableIME API ile IME kapatılmaktadır. IME standart ingilizce karakterler dışında başka bir dil kullanılmasını sağlar, kapatılması saldırganın Remote bağlantıyı ingilizce kullanacağı anlamına gelmektedir.



Şekil 2- ImmDisableIME

GetEnvironmentVariableW API ile alınan “UserInitLogonServer”, “UserInitLogonScript” ve “UserInitMprLogonScript” değerleri devamında SetEnvironmentVariableW API ile 0’a eşitlenmiştir.

```
010012A4    BE 3C140001     mov esi,dinotify.100143C                    100143C:L"UserInitLogonServer"
010012A9    56              push esi
010012AA    E8 38100000     call dinotify.10022E7
010012AF    68 14140001     push dinotify.1001414                       1001414:L"UserInitLogonScript"
010012B4    8945 88         mov dword ptr ss:[ebp-78],eax
010012B7    E8 2B100000     call dinotify.10022E7
010012BC    BB E4130001     mov ebx,dinotify.10013E4                    ebx:L"UserInitMprLogonScript",
010012C1    53              push ebx                                    ebx:L"UserInitMprLogonScript"
010012C2    8945 80         mov dword ptr ss:[ebp-80],eax
010012C5    E8 4A160000     call dinotify.1002914
010012CA    57              push edi
010012CB    56              push esi
010012CC    8B35 5C110001   mov esi,dword ptr ds:[<&SetEnvironmentVariableW>]
010012D2    8945 90         mov dword ptr ss:[ebp-70],eax
010012D5    FFD6            call esi
010012D7    57              push edi
010012D8    68 14140001     push dinotify.1001414                       1001414:L"UserInitLogonScript"
010012DD    FFD6            call esi
010012DF    57              push edi
010012E0    53              push ebx                                    ebx:L"UserInitMprLogonScript"
010012E1    FFD6            call esi
```

Şekil 3- SetEnvironmentVariables sıfırlandı.

“RunLogonScriptSync” HKEY_CURRENT_USER ve HKEY_LOCAL_MACHINE içerisindeki **“Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon”** keyinde ve HKEY_CURRENT_USER ve HKEY_LOCAL_MACHINE içerisindeki **“Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System”** keyinde RegQueryValueExW API ile sorgulanmıştır.

```
01002E05    8B35 24100001   mov esi,dword ptr ds:[<&RegOpenKeyExW>]      01001024:"0m6vp~6v`V6v"
01002E0B    57              push edi
01002E0C    8D45 FC         lea eax,dword ptr ss:[ebp-4]
01002E0F    50              push eax
01002E10    BF 19000200     mov edi,20019
01002E15    57              push edi
01002E16    6A 00           push 0
01002E18    68 48220001     push dinotify.1002248                       1002248:L"Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon"
01002E1D    68 01000080     push 80000001
01002E22    FFD6            call esi
01002E24    8B1D 20100001   mov ebx,dword ptr ds:[<&RegQueryValueExW>]   ebx:L"UserInitMprLogonScript"
01002E2A    85C0            test eax,eax
01002E2C    75 28           jne dinotify.1002E56
01002E2E    8D45 F8         lea eax,dword ptr ss:[ebp-8]
01002E31    50              push eax
01002E32    8D45 F4         lea eax,dword ptr ss:[ebp-C]
01002E35    50              push eax
01002E36    8D45 F0         lea eax,dword ptr ss:[ebp-10]
01002E39    50              push eax
01002E3A    6A 00           push 0
01002E3C    68 F82E0001     push dinotify.1002EF8                       1002EF8:L"RunLogonScriptSync"
```

Şekil 4- RunLogonScriptSync

Zararlı GetSystemMetrics API SM_REMOTESESSION parametresi ile Terminal Servisinin client session mı yoksa console session mı olduğunu kontrol etmektedir.

```
01002941    8945 FC         mov dword ptr ss:[ebp-4],eax
01002944    68 00100000     push 1000
01002949    FF15 58100001   call dword ptr ds:[<&GetSystemMetrics>]
0100294F    85C0            test eax,eax
01002951    0F85 3E090000   jne dinotify.1003295
```

Şekil 5- GetSystemMetrics

Client session değeri dönmesi sonucu “ctfmon.exe /n” değerini “HKEY_CURRENT_USER Software\\Microsoft\\Windows\\CurrentVersion\\Runonce” içerisine kaydeder. Bu sayede Bilgisayar tekrar başlatıldığında program sorunsuz çalışmaktadır. "ctfmon.exe” aktif pencereyi izler ve alternatif kullanıcı inputlarını sağlar, bu yüzden zararlı yapacağı bazı faaliyetler için “ctfmon.exe”ye ihtiyaç duyar çalışmadığı zaman ise hata almaktadır.

```
push ebx
mov esi,dinotify.100347C
lea edi,dword ptr ss:[ebp-40]
rep movsd
mov esi,dword ptr ds:[<&RegCreateKeyExW>]
push dinotify.1003418
mov edi,80000001
push edi
call esi
test eax,eax
```

```
100347C:L"ctfmon.exe /n"

1003418:L"Software\\Microsoft\\Windows\\CurrentVersion\\Runonce"
```

Şekil 6- ctfmon.exe Runonce içerisine kaydedilmiştir.

“HKEY_LOCAL_MACHINE System\\CurrentControlSet\\Control\\Terminal Server” içerisinden RegQueryValueExW ile değeri alınan **"TSAppCompat”** zararlının içerisinde bulunduğu makinenin Remote Admin modunda mı yoksa Application Server modunda mı olduğunu öğrenir. Sonra DwmpStartupViaUserInit ile Desktop Window Manager User Init yoluyla çalıştırılır.

```
push eax
push 1
push esi
push dinotify.10029F8
push 80000002
call dword ptr ds:[<&RegOpenKeyExW>]
test eax,eax
jne dinotify.10029CF
lea eax,dword ptr ss:[ebp-C]
push eax
lea eax,dword ptr ss:[ebp-4]
push eax
lea eax,dword ptr ss:[ebp-10]
push eax
push esi
push dinotify.10029E0
push dword ptr ss:[ebp-8]
mov dword ptr ss:[ebp-4],esi
mov dword ptr ss:[ebp-C],4
call dword ptr ds:[<&RegQueryValueExW>]
test eax,eax
je dinotify.1003498
push dword ptr ss:[ebp-8]
call dword ptr ds:[<&RegCloseKey>]
mov dword ptr ds:[1006080],esi
mov eax,dword ptr ds:[10064A4]
pop esi
leave
ret
```

```
10029F8:L"System\\CurrentControlSet\\Control\\Terminal Server"

10029E0:L"TSAppCompat"
```

Şekil 7- TSAppcompat

“HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo” altındaki önce taranıp sonra keyler RegDeleteTreeW API ile silinerek RegCreateKeyExW API ile ilk key içerisi boş olarak geri oluşturulmaktadır.

```
01002F41    57              push edi
01002F42    FFB0 D4010000   push dword ptr ds:[eax+1D4]
01002F48    8D85 64FFFFFF   lea eax,dword ptr ss:[ebp-9C]
01002F4E    68 C82F0001     push dinotify.1002FC8                    1002FC8:L"Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\SessionInfo\\%d"
01002F53    6A 4B           push 4B
01002F55    50              push eax
01002F56    33FF            xor edi,edi
01002F58    E8 F4000000     call dinotify.1003051
01002F5D    83C4 10         add esp,10
01002F60    85C0            test eax,eax
01002F62    7C 52           jl dinotify.1002FB6
01002F64    56              push esi
01002F65    8D85 64FFFFFF   lea eax,dword ptr ss:[ebp-9C]
01002F6B    50              push eax
01002F6C    BE 01000080     mov esi,80000001
01002F71    56              push esi
01002F72    FF15 18100001   call dword ptr ds:[<&RegDeleteTreeW>]
01002F78    8D85 60FFFFFF   lea eax,dword ptr ss:[ebp-A0]
01002F7E    50              push eax
01002F7F    8D85 5CFFFFFF   lea eax,dword ptr ss:[ebp-A4]
01002F85    50              push eax
01002F86    57              push edi
01002F87    6A 02           push 2
01002F89    6A 01           push 1
01002F8B    57              push edi
01002F8C    57              push edi
01002F8D    8D85 64FFFFFF   lea eax,dword ptr ss:[ebp-9C]
01002F93    50              push eax
01002F94    56              push esi
01002F95    FF15 14100001   call dword ptr ds:[<&RegCreateKeyExW>]
01002F9B    5E              pop esi
01002F9C    85C0            test eax,eax
01002F9E    75 16           jne dinotify.1002FB6
01002FA0    FFB5 5CFFFFFF   push dword ptr ss:[ebp-A4]
01002FA6    FF15 28100001   call dword ptr ds:[<&RegCloseKey>]
```

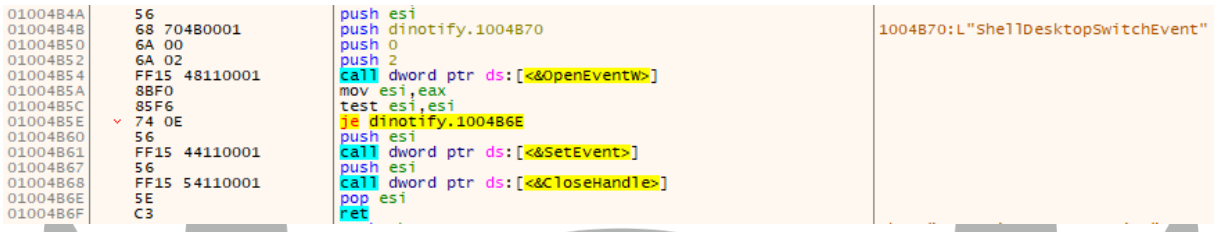
Şekil 8- SessionInfo keyi içerisindeki dosyalar silindi.

“HKLM\system\currentcontrolset\control\safeboot\option” keyinden UseAlternateShell ve AlternateShell değerleri kontrol edilir, en azından bir Shell’in bulunması sonraki eylem için önemli aksi takdirde zararlı bazı işlemleri tamamlayamaz.

```
01003DAA    8D85 B8F5FFFF       lea eax,dword ptr ss:[ebp-A48]
01003DB0    50                  push eax
01003DB1    53                  push ebx
01003DB2    68 FC430001         push dinotify.10043FC                    10043FC:L"UseAlternateShell"
01003DB7    FFB5 C8F5FFFF       push dword ptr ss:[ebp-A38]
01003DBD    C785 C0F5FFFF 040000( mov dword ptr ss:[ebp-A40],4
01003DC7    FF15 20100001       call dword ptr ds:[<&RegQueryValueExW>]
01003DCD    FFB5 C8F5FFFF       push dword ptr ss:[ebp-A38]
01003DD3    FF15 28100001       call dword ptr ds:[<&RegCloseKey>]
01003DD9    399D CCF5FFFF       cmp dword ptr ss:[ebp-A34],ebx
01003DDF    0F84 6DE8FFFF       je dinotify.1002652
01003DE5    8D85 C8F5FFFF       lea eax,dword ptr ss:[ebp-A38]
01003DEB    50                  push eax
01003DEC    68 19000200         push 20019
01003DF1    53                  push ebx
01003DF2    68 A8430001         push dinotify.10043A8                    10043A8:L"system\\currentcontrolset\\control\\safeboot"
01003DF7    57                  push edi
01003DF8    FFD6                call esi
01003DFA    85C0                test eax,eax
01003DFC    75 55               jne dinotify.1003E53
01003DFE    8D85 C0F5FFFF       lea eax,dword ptr ss:[ebp-A40]
01003E04    50                  push eax
01003E05    8D85 E0F5FFFF       lea eax,dword ptr ss:[ebp-A20]
01003E0B    50                  push eax
01003E0C    8D85 B8F5FFFF       lea eax,dword ptr ss:[ebp-A48]
01003E12    50                  push eax
01003E13    53                  push ebx
01003E14    68 84430001         push dinotify.1004384                    1004384:L"AlternateShell"
01003E19    FFB5 C8F5FFFF       push dword ptr ss:[ebp-A38]
01003E1F    C785 C0F5FFFF 080200( mov dword ptr ss:[ebp-A40],208
01003E29    FF15 20100001       call dword ptr ds:[<&RegQueryValueExW>]
```

Şekil 9- Shell kontrol

Zararlı remote bağlantı kurmadan önce OpenEventW API ile ShellDesktopSwitchEvent çalıştırarak Masaüstünü değiştirmekte ve yakalanmaktan kaçınmaktadır.

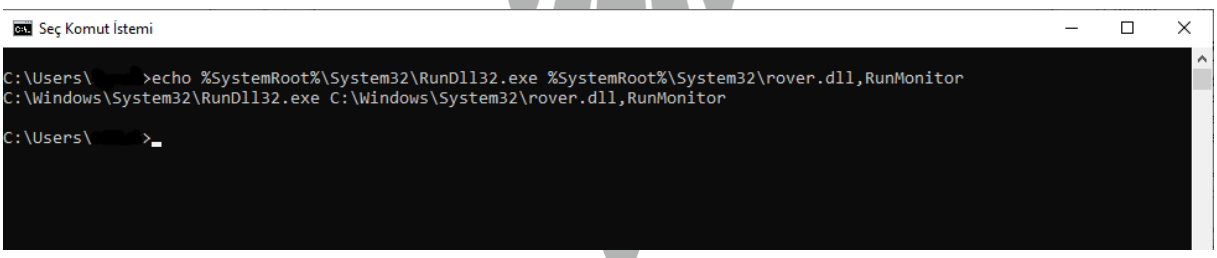


Şekil 10-OpenEventW(ShellDesktopSwitchEvent) ile Masaüstü değiştirildi.

"ts_remoteprograms.chm::/html/d69deee5-8457-4327-92b0-f0c6c8c826ef.htm" adresine CreateWindowExW API yardımıyla pencere oluşturmaktadır. Daha sonra bu fonskiyonu CreateThread ile çalıştırarak Botnet bağlantısını kurmaktadır.

Şekil 11- Remote Desktop

SetEnvironmentvariable API ile "C:\Windows" değeri "%SystemRoot%" ile değiştirilmektedir. Bu durumda %SystemRoot% olarak yazılan komutlar aslında "C:\Windows" işaret etmektedir.



Şekil 12- Gizlenen komut.

%SystemRoot%\System32\RunDll32.exe %SystemRoot%\System32\rover.dll,RunMonitor C:\Windows\ System32\RunDll32.exe C:\Windows\System32\rover.dll,RunMonitor

“\HKCR\CLSID\{16d12736-7a9e-4765-bec6-f301d679caaa}” keyi bulunuyorsa “C:\Windows\System32\RunDll32.exe C:\Windows\System32\rover.dll,RunMonitor” komutu çalıştırılır ve görüntü elde edilir. OpenEventW RasAutodialNewLogonUser parametresiyle çalıştırılarak yeni kullanıcı girişi yapılmaktadır.

```
push esi                                        1002174:L"RasAutodialNewLogonUser"
push dinotify.1002174
push ebx
push 100002
call dword ptr ds:[<&OpenEventW>]
mov esi,eax
cmp esi,ebx
jne dinotify.1003282
```

Şekil 13-OpenEventW kullanılark Uzak kullanıcı bağlandı.

“HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows\\System” keyinde bulunan Allow-LogonScript-NetbiosDisabled değeri kontrol edilir olumsuz koşulda işlem logon scriptleri çalıştırılamayacağı için işlem atlanır.

```
0100382D   50              push eax
0100382E   68 19000200     push 20019
01003833   57              push edi
01003834   68 C83B0001     push dinotify.1003BC8                1003BC8:L"SOFTWARE\\Policies\\Microsoft\\Windows\\System"
01003839   68 02000080     push 80000002
0100383E   FF15 24100001   call dword ptr ds:[<&RegOpenKeyExW>]
01003844   85C0            test eax,eax
01003846   75 2B           jne dinotify.1003873
01003848   8D45 D0         lea eax,dword ptr ss:[ebp-30]
0100384B   50              push eax
0100384C   8D45 E4         lea eax,dword ptr ss:[ebp-1C]
0100384F   50              push eax
01003850   8D45 CC         lea eax,dword ptr ss:[ebp-34]
01003853   50              push eax
01003854   57              push edi
01003855   68 803B0001     push dinotify.1003B80                1003B80:L"Allow-LogonScript-NetbiosDisabled"
0100385A   FF75 D4         push dword ptr ss:[ebp-2C]
0100385D   C745 D0 04000000 mov dword ptr ss:[ebp-30],4
01003864   FF15 20100001   call dword ptr ds:[<&RegQueryValueExW>]
0100386A   FF75 D4         push dword ptr ss:[ebp-2C]
0100386D   FF15 28100001   call dword ptr ds:[<&RegCloseKey>]
01003873   837D E4 01      cmp dword ptr ss:[ebp-1C],1
01003877   0F85 DC010000   jne dinotify.1003A59
```

Şekil 14- Allow-LogonScript-NetbiosDisabled değeri kontrol edilir.

ldap_initW API ile 185(TCP/UDP) Remote Port'unu kullanarak LDAP server başlatmaktadır. ldap_get_optionW ve ldap_set_optionW'la ayarları düzenleyerek ldap_connect ile bağlantı kurulmaktadır. ldap_bind_sW API bir clienti LDAP server'a authanticate etmektedir. Bu sayede zararlı networkte bulunan diğer cihazlara da bulaşmaktadır.

```
.text:0100399C push    eax             ; invalue
.text:0100399D push    4               ; option
.text:0100399F push    [ebp+ld]        ; ld
.text:010039A2 mov     [ebp+invalue], 1Eh
.text:010039A9 call    esi ; ldap_set_optionW ; Indirect Call Near Pr
.text:010039AB add     esp, 0Ch        ; Add
.text:010039AE test    eax, eax        ; Logical Compare
.text:010039B0 jnz     loc_1003A59     ; Jump if Not Zero (ZF=0)
```

```
.text:010039B6 mov     eax, [ebp+invalue]
.text:010039B9 mov     [ebp+timeout.tv_sec], eax
.text:010039BC lea     eax, [ebp+timeout] ; Load Effective Address
.text:010039BF push    eax             ; timeout
.text:010039C0 push    [ebp+ld]        ; ld
.text:010039C3 mov     [ebp+timeout.tv_usec], edi
.text:010039C6 call    ds:ldap_connect ; Indirect Call Near Procedure
.text:010039CC pop     ecx
.text:010039CD pop     ecx
.text:010039CE test    eax, eax        ; Logical Compare
.text:010039D0 jnz     loc_1003A59     ; Jump if Not Zero (ZF=0)
```

```
.text:010039D6 push    486h            ; method
.text:010039DB push    edi             ; cred
.text:010039DC push    edi             ; dn
.text:010039DD push    [ebp+ld]        ; ld
.text:010039E0 call    ds:ldap_bind_sW ; Indirect Call Near Procedure
.text:010039E6 add     esp, 10h        ; Add
.text:010039E9 test    eax, eax        ; Logical Compare
.text:010039EB jnz     short loc_1003A59 ; Jump if Not Zero (ZF=0)
```

Şekil 15-LDAP Connect

YARA Kuralı

```
rule dinotify

{

strings:

        $vnt1 = { BB F0 11 00 01 53 89 45 08 50 BF 00 00 10 00 57 FF D6 } //ShellReadyEvent

        $vnt2 = { 56 68 74 21 00 01 53 68 02 00 10 00 FF 15 48 11 00 01 } //RasAutodialNewLogonUser

        $vnt3 = { 56 68 70 4B 00 01 6A 00 6A 02 FF 15 48 11 00 01 } //ShellDesktopSwitchEven



        $imm1 = { 68 74 14 00 01 FF 15 6C 11 00 01 } //Load imm32.dll

        $imm2 = { 68 64 14 00 01 50 FF 15 70 11 00 01 3B C7 } //ImmDisableIME

        $ts1 = { 68 54 45 00 01 FF 15 6C 11 00 01 } //Load tsappcmp.dll

        $ts2 = { 68 3C 45 00 01 53 FF 15 70 11 00 01 3B C7 } //TermsrvCheckNewInIFiles

        $rm = { 68 10 42 00 01 68 10 40 00 00 53 56 53 53 E8 78 0A 00 00 } //rmt_chm

        $ldap1 = { 68 85 01 00 00 56 FF 15 34 60 00 01 } //ldap_initW

        $ldap2 = { 50 BE 92 00 00 00 56 FF 75 F8 FF 15 38 60 00 01 } //ldap_get_optionW
```

```
        $ldap3 = { 50 56 FF 75 F8 8B 35 30 60 00 01 FF D6 }
//ldap_set_optionW

        $ldap4 = { 50 FF 75 F8 89 7D C8 FF 15 40 60 00 01 }
//ldap_connect

        $ldap5 = { 68 86 04 00 00 57 57 FF 75 F8 FF 15 3C 60 00 01 }
//ldap_bind_sW

        $ldap6 = { FF 75 F8 FF 15 44 60 00 01 } //ldap_unbind_s

condition:

        all of them or

        2 of ($vnt*) and 3 of ($ldap*) or

        $rm and $ldap4 and $imm1 and $ts2 or

        all of ($ldap*) and all of ($vnt*) or

        all of ($ts*) and $rm and any of ($vnt*)

}
```

MITRE ATTACK TABLE

Initial Access	Persistence	Privilege Escalation	Discovery	Defense Evasion	C&C
Hardware Additions (T1200)	**Logon Script (Windows)** (T1037.001)	**Domain Accounts** (T1078.002)	**Group Policy Discovery** (T1615)	**Sandbox Evasion: System Checks** (T1497.001)	**Remote Desktop Protocol** (T1021.001)

Çözüm Önerileri

1. Bilinmeyen USB belleklerin kullanımından kaçınılmalıdır.
2. Bilinmeyen link ve sitelerden uzak durulmalıdır.
3. Güncel bir Anti-Virüs programı kullanılmalıdır.
4. Şirket içi cihazların haberleşmesi güvenli hale getirilmelidir.
5. Kullanılan uygulamalar lisanlı ve güncel olmalıdır.
6. İşletim sistemi güncellemeleri geciktirilmemelidir.

HAZIRLAYAN

Emre TÜRKYILMAZ

https://www.linkedin.com/in/emre-türkyılmaz