Malware identificat în atacurile împotriva organizațiilor din Ucraina

Microsoft Threat Intelligence Center (MSTIC) a identificat o campanie malware ce vizează multiple organizații din Ucraina. Malware-ul a fost identificat pentru prima dată pe stațiile victimelor în data de 13 ianuarie 2022.

Investigațiile sunt în curs, dar până la momentul actual nu au fost identificate informații care să lege evenimentul de o grupare de hackeri cunoscută. De asemenea, MSTIC a identificat faptul că malware-ul a fost proiectat să lase impresia unui atac cu ransomware, dar în componența acestuia nu există mecanisme care să permită victimelor decriptarea datelor, imediat după ce suma de răscumpărare a fost achitată.

Analiza activității atacatorilor

Pe data de 13 ianuarie, Microsoft a identificat activități intruzive din Ucraina, ce păreau să fie activități de ștergere a MBR (Master Boot Records). În urma investigației, a fost descoperită o variantă de malware

Pasul 1: Modificarea Master Boot Record pentru afișarea unei note de răscumpărare false

Malware-ul se poate găsi în diferite directoare de pe stație, precum **C:\PrefLogs**, **C:\ProgramData**, **C:** și **C:\temp**, iar fișierul poartă de cele mai multe ori numele **stage1.exe**. Din analiza efectuată până în prezent, malware-ul rulează prin intermediul Impacket, modalitate utilizată de mulți actori pentru mișcare laterală și execuție comenzi.

Primul pas se execută atunci când dispozitivul primește comanda de *Shut Down*. Modificarea MBR este o metodă atipică hackerilor care operează atacuri ransomware. În realitate, nota de răscumpărare este doar o diversiune pentru a deruta victimele. Textul notei de răscumpărare poate fi observat mai jos:

Your hard drive has been corrupted.

In case you want to recover all hard drives

of your organization,

You should pay us $10k via bitcoin wallet

1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via

tox ID
8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65

with your organization name.

We will contact you to give further instructions.

Pasul 2: Malware care corupe fișierele

Stage2.exe este un dowloader pentru un malware utilizat la coruperea fișierelor. În momentul execuției, stage2.exe descarcă un malware găzduit pe un canal de Discord, prin intermediul unei secvențe de cod inclusă în malware. Acesta este clasificat ca fiind un "file corrupter" din cauza faptului câ în momentul execuției în memorie, acesta localizează multiple directoare de pe stație și corupe fișierele ce au următoarele extensii:

.3DM .3DS .7Z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2 .CGM .CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH .DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM .HTML .HWP .IBD .INC .INI .ISO .JAR .JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6 .LDF .LOG .MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .ODP .ODS .ODT .OGG .ONETOC2 .OST .OTG .OTP .OTS .OTT .P12 .PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5 .PHP6 .PHP7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS

.PPSM .PPSX .PPT .PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK .SLN .SNT .SQ3 .SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC .SXD .SXI .SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM .VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML .XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW .YML .ZIP

Dacă un fișier identificat are extensia de mai sus, malware-ul va suprascrie fișierul cu un număr fix de bytes (0xCC). După procesul de suprascriere, fișierul va primi o nouă extensie aleatorie (random four-byte extension).

Recomandări

MSTIC și celelate echipe de securitate din cadrul Microsoft lucrează pentru crearea și implementarea unor instrumente de detecție.

La momentul actual, Microsoft, a implementat măsuri pentru detecția noi familii malware denumită ***WhisperGate*** (DoS:Win32/WhisperGate.A!dha) în Microsoft Defender Antivirus și Microsoft Defender Endpoint.

Tehnicile utilizate de către acest actor și descrise în acest document pot fi atenuate urmând setul de recomandări de mai jos:

- Utilizarea IOC-urilor de la finalul documentului, în scopul identificării prezenței atacatorilor în infrastructura dumneavoastră;
- Revizuirea politicilor de acces la distanță, în special a conturilor care nu utilizează tehnologii de tipul autentificării multi-factor(MFA);
- Activarea multi-factor authentication (MFA) pentru a preveni utilizarea de către atacatori a unor seturi de credențiale compromise anterior;
- Activarea Controlled folder Access (CFA) în cazul în care utilizați Defender Endpoint, pentru a preveni modificările asupra MBR/VBR.

Indicatori de compromitere (IOCs)

Lista de mai jos cuprinde IOC-urile identificate în timpul investigației și se recomandă utilizarea acestora pentru a identifica dacă infrastructura a fost compromisă și pentru protecția împotriva viitoarelor atacuri:

Indicator	Type	Description
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA-256	Hash of destructive malware *stage1.exe*
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	SHA-256	Hash of *stage2.exe*
cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1	Command line	Example Impacket command line showing the execution of the destructive malware. The working directory has varied in observed intrusions.

Detecții

Microsoft 365 Defender

- DoS:Win32/WhisperGate.A!dha
- DoS:Win32/WhisperGate.C!.dha
- DoS:Win32/WhisperGate.H!dha
- DoS:Win32/WhisperGate.X!dha

Sursa: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/