OFFENTLIG BRIEF

Viktigt att veta om de ökade digitala riskerna efter cyberattackerna i Ukraina

April, 2022

conscia

SAMMANFATTNING

Under de pågående striderna har vi kunnat spåra utvecklingen av nya målinriktade och skräddarsydda skadliga programvaror (HermeticWiper och Whisper Gate) i forum på Darkweb. Nu rapporterar flera välkända källor om samma underrättelser. Teknisk analys av dessa skadliga programvaror visar på deras destruktiva kapacitet. För närvarande är den primära avsikten och användningen fortfarande begränsad till cyberkrigföring riktad mot Ukraina. Men de kommer utan tvekan att innebära en risk för organisationer i hela världen när de används av fler aktörer.

När den här bloggen publiceras har vår SOC (Security Operations Center) ännu inte upptäckt någon ökning i cyberattacker som använder funktioner som har utvecklats specifikt för det här cyberkriget. Det är också förväntat så här tidigt i kriget eftersom motståndare inte vill ge säkerhetsspecialister möjligheten att följa hur den skadliga programvaran utvecklas.

Det är dock ytterst viktigt att känna till dessa hot och vara väl förberedd. När den här skadliga programvaran har nått sina militära mål kommer de snabbt att spridas till kommersiella marknader eller ännu tidigare riktas mot västerländska organisationer som upplevs stöda Ukraina.

Den här artikeln ger en detaljerad analys av kända skadliga programvaror som används i cyberkrigföring och riktlinjer för att upptäcka, mitigera och svara på dessa.

ÖVERSIKT ÖVER BERÖRDA APT:er

Eftersom APT-grupper ofta sponsras av länder som deltar i kriget är det väntat att de involveras i kriget. Idag behöver det knappt sägas att militära krig följs av sina motsvarigheter i cybervärlden.

Som ett led i processen av att samla in hotunderrättelser om pågående operationer i Ukrainakriget tittade vi på existerande kunskap och kända kunskapsbaser över kända ryska Advanced Persistent Threat-grupper (APT-grupper). Det här är statssponsrade hotaktörer som sannolikt kommer att involveras i det pågående kriget, och som är viktiga att känna till.

*Table 1 – Ryska APT:er som sannolikt är involverade i cyberattackerna mot Ukraina och deras kända aktivitet**

#	Sandworm Team	Gamaredon	Turla	APT28	APT29
Avdelning	Rysslands militära-underrättelse-tjänst (GRU)	Rysslands-baserad	Ryska federationens säkerhets-tjänst (FSB)	Rysslands militära underrättelse-tjänst (GRU)	FSB /Ryska federationens yttre underrättelse-tjänst (SVR)
Aktivitet	Attacker	Mål: organisationer och företag i Ukraina	Spionage	Spionage	Spionage

**Källa:* https://attack.mitre.org/groups/

KÄNDA TTP:er FRÅN RYSKA APT:er

Nu när vi känner till ryska APT:er som sannolikt kommer att delta i cyberkrigföringen i Ukraina går vi vidare med att titta på taktik, teknik och tillvägagångssätt. Till det utnyttjade vi MITRE ATT&CK Navigator.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution
Search Victim-Owned Websites			System Services	External Remote Services
			User Execution	Hijack Execution Flow
			Windows Management Instrumentation	Implant Internal Image
				Modify Authentication Process
				Office Application Startup
				Pre-OS Boot
				Scheduled Task/Job
				Server Software Component
				Traffic Signaling
				Valid Accounts

Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services
Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing
Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer
Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking
Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services
Domain Policy Modification	Deploy Container	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media
Escape to Host	Direct Volume Access	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools
Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content
Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material
Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	File and Directory Discovery	
Process Injection	File and Directory Permissions Modification	Steal Application Access Token	Group Policy Discovery	
Scheduled Task/Job	Hide Artifacts	Steal or Forge Kerberos Tickets	Network Service Scanning	
Valid Accounts	Hijack Execution Flow	Steal Web Session Cookie	Network Share Discovery	
	Impair Defenses	Two-Factor Authentication Interception	Network Sniffing	
	Indicator Removal on Host	Unsecured Credentials	Password Policy Discovery	
	Indirect Command Execution		Peripheral Device Discovery	
	Masquerading		Permission Groups Discovery	
	Modify Authentication Process		Process Discovery	
	Modify Cloud Compute Infrastructure		Query Registry	
	Modify Registry		Remote System Discovery	
	Modify System Image		Software Discovery	
	Network Boundary Bridging		System Information Discovery	
	Obfuscated Files or Information		System Location Discovery	
	Pre-OS Boot		System Network Configuration Discovery	
	Process Injection		System Network Connections Discovery	
	Reflective Code Loading		System Owner/User Discovery	
	Rogue Domain Controller		System Service Discovery	
	Rootkit		System Time Discovery	
	Signed Binary Proxy Execution		Virtualization/Sandbox Evasion	
	Signed Script Proxy Execution			
	Subvert Trust Controls			
	Template Injection			
	Traffic Signaling			
	Trusted Developer Utilities Proxy Execution			
	Unused/Unsupported Cloud Regions			
	Use Alternate Authentication Material			
	Valid Accounts			
	Virtualization/Sandbox Evasion			
	Weaken Encryption			
	XSL Script Processing			

Collection	Command and Control	Exfiltration	Impact
Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Data from Local System	Non-Application Layer Protocol		Network Denial of Service
Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
Data from Removable Media	Protocol Tunneling		Service Stop
Data Staged	Proxy		System Shutdown/Reboot
Email Collection	Remote Access Software		
Input Capture	Traffic Signaling		
Screen Capture	Web Service		
Video Capture			

Figur 1 – Ryska APT taktiker och tekniker (gulmarkerade) utifrån MITRE ATT&CK-ramverket

Ovanstående figur skapades med hjälp av MITRE ATT&CK Navigator. Vi filtrerade bort APT:erna som nämns i **tabell 1 - Ryska APT:er som sannolikt är inblandade i cyberattacker mot Ukraina och deras kända aktiviteter*.** Den sammanfattar de stora mängder tekniker som hotaktörerna använder.

Vad kan du göra med den här datan?

Genom att känna till en potentiell fiende kan du samla underrättelser om fienden och förbereda ditt försvar därefter. Men vi kan inte utgå från att varje APT kommer att delta i kriget, och även om de gör det måste vi veta vilka cyberattacker som kommer från vilka hotaktörer, så att vi vet säkert vilka som är inblandade.

Genom att känna till vilka APT:er som deltar kan vi:

1. Skapa specifika regler som upptäcker potentiella cyberattacker från de här aktörerna.
2. Utveckla skräddarsydda uppdrag som proaktivt potentiella intrång från en given aktör.

3. Förbereda lindrande åtgärder och stärka cyberförsvaret med höjd säkerhetsutformning.

Dessutom används MITRE ATT&CK numera som en referensmodell för många säkerhetsprodukter (främst EDR) för att visa deras förmåga inom hotdetektering. Så du kan använda den här informationen för att verifiera att dina säkerhetsprodukter hanterar de här teknikerna.

VAD HAR VI SETT HITILLS

Cyberattacker i samband med Ukrainakrisen har pågått åtminstone sedan januari 2022. Men vidare undersökning avslöjar att försök gjordes redan i slutet av 2021 för att testa den skadliga programvaran och cyberattacker. Vårt Threat Intelligence-team övervakade de här aktiviteterna som började långsamt för att sedan öka i snabb takt när kriget bröt ut.

Här följer en lista på cyberattacker mot ukrainska tillgångar under kriget:

- Destruktiv skadlig programvara: WhisperGate och HermeticWiper
- Spionage (CISA-varning AA22-047A)
- DDoS mot infrastruktur för regering, militär, finanssektorn och IT-branschen
- Förstörda webbplatser
- Desinformation genom olika medier
- Leverantörsattacker (Kitsoft)
- Fildumpar på Darkweb

Teknikerna som används i ovanstående cyberattacker kan matchas med MITRE ATT&CK-teknikerna i figur 1. Utifrån den här informationen är vi övertygade om att attackerna utfördes av några av APT-grupperna i tabell 1. Så länge det saknas officiell tillskrivning eller någon uppenbar ”signatur” går det inte att säga säkert exakt vilken APT som ligger bakom attackerna. Men om syftet är att stärka vårt cyberförsvar är underrättelserna mer än tillräckliga.

Vi kommer att ge ytterligare teknisk analys av WhisperGate och HermeticWiper, eftersom det här är de destruktiva skadliga programvarianterna som används i det pågående cyberkriget och sannolikt kommer att användas i efterdyningarna eller mot länder som stödjer Ukraina.

TEKNISK ANALYS AV STÖRRE HOT

I den tekniska analysen av de främsta hoten fokuserar vi på de två skadliga programvaror som är utvecklade specifikt för det pågående kriget i Ukraina. De här analyserna är på en hög nivå och ger en bra överblick över hur skadlig programvara beter sig. Syftet är inte att ge djup förståelse för den skadlig programvaran, utan snarare relevant information som går att använda i din organisation.

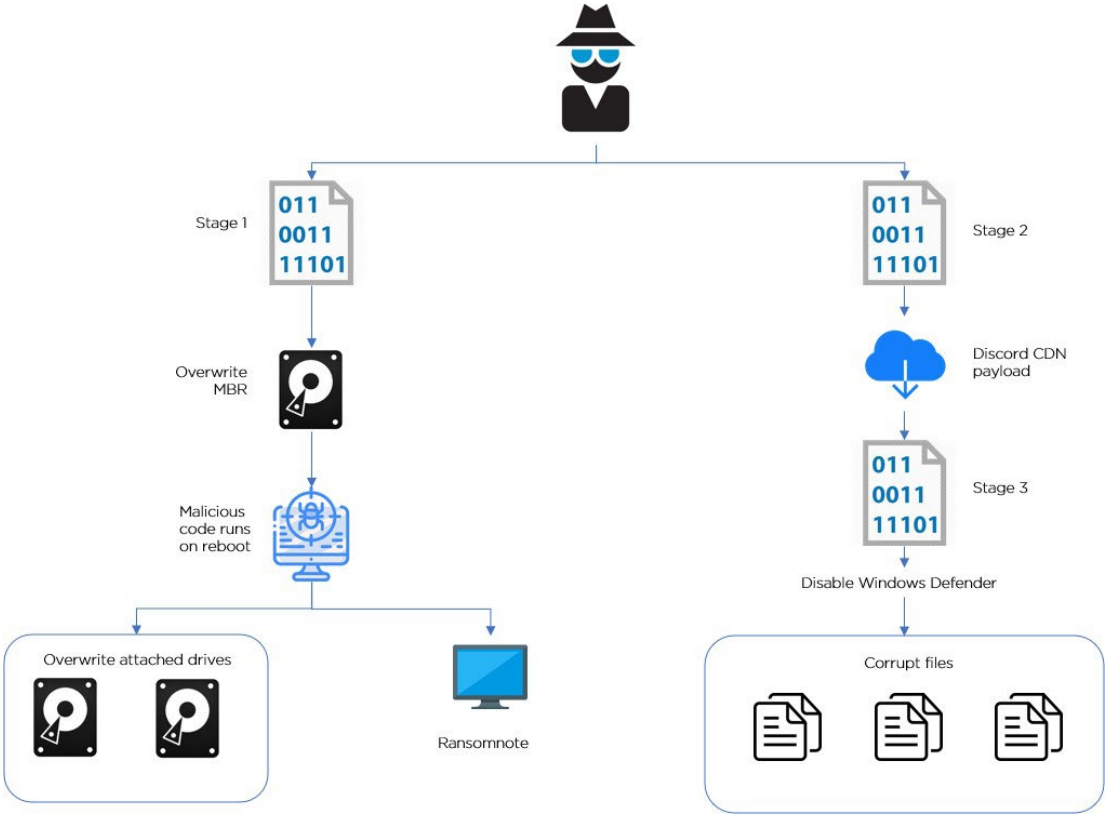
WhisperGate

WhisperGate är en ny skadlig programvara som används i en pågående operation riktad mot flera industrier i Ukraina. Huvudsyftet med programmet är att förstöra offrets Master Boot Record (MBR) och skada filer på anslutna lagringsenheter. Målet nås genom tre steg:

1. Skriv över MBR med ett utpressningsmeddelande
2. Ladda ner ytterligare nyttolast Discord CDN som en JPG-bilaga, vilket leder till steg 3
3. Initierar processen att förstöra alla filer som matchar en lista med 191 filändelser

I det sista steget används tung kodobfuskering för att undvika upptäckt och analys av skadlig programvara. WhisperGates effektivitet i att radera och korrumpera filer är så pass bra att filer och enheter inte längre går att återställa eller använda.

Det finns inte någon officiell hänvisning till vilken hotaktörsgrupp som ligger bakom verksamheten. Men vi märker tydligt att den skadliga programvaran riktas mot ukrainska organisationer. Det antyder att hotaktören som ligger bakom den sponsras av Ryssland.



Figur 2 – WhisperGates arbetsflöde (baserat på analys av Recorded Future)

HermeticWiper

HermeticWipers primära mål är att skriva över Master Boot Record (MBR) och att korrumpera NTFS- och FAT-filsystem i partitionstabellen. Vi kunde se att den skadliga programvaran är digitalt signerad av *Hermetica Digital Ltd,* vilket gör den svårare att upptäcka. Wiper utnyttjar *EaseUS Partition Managers* drivrutin "empntdrv.sys" för att komma åt fysiska enheter direkt och även för att hämta partitionsinformation. Den inaktiverar WoW64 File System Redirection om offret kör 64-bitars operativsystem eftersom detta stoppar 64-bitars system från att ladda in 32-bitars Kernel drivers från katalogen SySWoW64\drivers. Istället tvingas de att använda system32\drivers, där den skadliga programvaran ersätter Kernel drivern.

Därefter listar den skadliga programvaran ett antal fysiska enheter och korrumperar de första 512 bytes:en i MBR. Efter raderingen initierar HermeticWiper en systemavstängning. Enligt aktuella rapporter från ESET släpptes den skadliga programvaran via standard (domänpolicy) GPO, vilket indikerar att motståndare vanligtvis tar kontroll över domänkontrollanter innan HermeticWiper körs.

RecordedFutures Insikt Group menar att utpressningsprogrammet PartyTicket är associerat med HermeticWiper. Deras analys visar att utpressningsmeddelandet har flera stavfel och grammatiska fel. Det är därför troligtvis inte utvecklat av en kriminell utpressningsgrupp. Dessutom skiljer sig listan över filändelser som utpressningsprogrammet försöker kryptera från den som används i andra utpressningsattacker. Den här listan innehåller filändelser som

.dll och .exe, vilka är filer som ofta behövs för systemdrift. Därför är det sannolikt en destruktiv skadlig programvara och inte ett legitimt utpressningsprogram.

MITIGERING – ALLMÄNNA RIKTLINJER

Det här avsnittet behandlar de tre huvudkategorierna: initial åtkomst, förebygga och upptäcka. Ingen av de här skadliga programvarorna aktiveras förrän de körs på offrets dator. För att det ska hända måste motståndare på något sätt plantera skadlig programvara på datorerna. Det är därför bättre att fokusera på den initiala vektorn fram till leverans. Vi kommer också att fokusera på förmågan att upptäcka och förebygga baserat på underrättelser i den tekniska analysen. Det här är praktiska mitigerande åtgärder som också används av vårt eget Conscia Cyberdefense-team.

Initial åtkomst

I de här fallen var ingången oftast genom Microsoft Exchange Server och en Apache Tomcat-server. Vi rekommenderar att du säkerställer att sådana här servrar i dina nätverk har alla uppdateringar och programfixar installerade. Det finns dock flera ingångar som den här typen av kapabla motståndare kan använda och anpassa. I det här sammanhanget bör du följa de allmänna riktlinjer som följer och titta på CISA:s AA22-057A-varning för ytterligare information.

Förebyggande åtgärder

Eftersom HermeticWiper utnyttjar EaseUS Partition Managers drivrutin, rekommenderar vi att du tar bort det här verktyget om du har det installerat och det inte är nödvändigt för din verksamhet.

WhisperGates steg 2-körning försöker ladda ner ytterligare nyttolast från Discord CDN. Om din organisation inte använder Discord rekommenderar vi att du blockerar inkommande nätverk från Discord CDN i dina brandväggar (eller om du vill vara riktigt specifik: *https://cdn[.]discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg*).

Upptäckt

För båda skadliga programvarorna gäller att du måste förlita dig på ett EDR-verktyg (eller något med liknande funktioner) för att upptäcka dem.

Till en början tillhandahåller vi riktlinjer för att upptäcka WhisperGate. Eftersom det är en attack i tre steg kommer vi även undersöka möjligheten till upptäckt i varje steg.

WhisperGate Detektering under steg 1

Detektera följande sträng på kommandoprompten:

cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$\ [TIMESTAMP] 2>&1 Även om detta enkelt kan ändras så är det fortfarande ett av de enklaste sätten att detektera tidigt under körningen i steg 1.

WhisperGate Detektering under steg 2

- Detektera följande PowerShell-kommandokörning:

  ```
  powershell -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
  ```

  Ovan Base64-kodade sträng avkodas till "Start-Sleep -s 10". WhisperGate kör det här kommandot två gånger för att undvika AV-detektering.

- Detektera nätverksanslutningar till:

  https[:]//cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg

- Detektera om fil skapas / ändringar som inkluderar filnamn:

  Tbopbh.jpg

WhisperGate Detektering under steg 3

Steg 3 extraherar två GZIP-packade resurser som kallas AdvancedRun och Waqybg.

- AdvancedRun kommer att försöka stoppa Windows Defender Service genom att köra VBS-skriptet Nmddfrqqrbyjeygggda.vbs i Temp-mappen. Scriptet kör följande kommando som går att använda vid detektering:

  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” Set-MpPreference -ExclusionPath ‘C:\’

Det här kommandot angav C:\ som en undantagsmapp.

- Därefter försöker det stoppa Windows Defender-tjänsten med AdvancedRun.exe och ta bort dess katalog. Detektera följande processkörningar:

  ```
  C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe
  ” /EXEFilename “C:\Windows\System32\sc.exe” /WindowState
  0 /CommandLine “stop WinDefend” /StartDirectory “” /RunAs

  8 /Run
  ```

```
C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe
" /EXEFilename
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.ex
e" /WindowState 0 /CommandLine "rmdir
'C:\ProgramData\Microsoft\Windows Defender' -Recurse"

/StartDirectory "" /RunAs 8 /Run
```

- Slutligen kör den skadliga programvaran ping-kommandot och raderar sig själv. Detektera följande körningar i kommandoprompten:

```
cmd.exe /min /C ping 111.111.111.111

-n 5 -w 10 > Nul & Del /f /q \"[Filepath]\"
```

Om den skadliga programvaran har körts hälsas offret med följande meddelande utpressningsmeddelande:

"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
8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1E D23054C057ECED5496F65

with your organization name.

We will contact you to give further instructions."

HermeticWiper Detektering

Det bästa sättet att detektera HermeticWiper är att övervaka specifika sökvägar, modifiering av behörighet och modifiering av systemkontroller. Du kan även detektera utfärdaren av den digitala signaturen för binära filer som matchade *Hermetica Digital Ltd.*

Sökvägar

Detektera åtkomst till sökvägar som inkluderar följande strängar:

- `EPMNTDRV`
- `PhysicalDrive`

Systemkontroller

Övervaka ändringar i följande systemkontroller:

- `SYSTEM\\CurrentControlSet\\Control\\CrashControl`
- `CrashDumpEnabled`

Behörigheter

Övervaka ändringar i följande behörigheter:

- `SeLoadDriverPrivilege`
- `SeBackupPrivilege`

Som vi nämnt så verkar HermeticWiper åtföljas av utpressningsprogrammet PartyTicket. Vi rekommenderar att du övervakar följande strängar och filändringar:

- `403forBiden`
- `wHiteHouse`
- `main.voteFor403`
- `main.n1hk9`

Strängsppecifikt utpressingsmeddelande:

- `"Thank you for your vote!"`
- `"photoes"`

HermeticWiper Decryptor

Om du ändå blir utsatt för intrång och dina data krypteras så tillhandahåller Avast ett gratis dekrypteringsprogram för PartyTicket som kan laddas ner och köras för att återskapa filer. När det här dokumentet skrevs så är dekrypteringen effektiv. Men det kan förändras längre fram när motståndare börjar anpassa utpressningsprogrammets kod.

Generella riktlinjer

Det här är slutligen ett bra tillfälle att verifiera att de viktigaste förebyggande motåtgärderna är optimalt distribuerade:

- Kontrollera att alla dina fjärråtkomster till organisationens nätverk kräver flerfaktorsautentisering (MFA).
- Säkerställ att all privilegierad och administrativ åtkomst kräver MFA.
- Säkerställ att programvaran du använder är uppdaterad, särskilt programvara som exponeras för internet (exponerad serverprogramvara, webbläsare).
- Se till att använda bästa praxis utifrån SBM, till exempel programfixar för kända SMB-svagheter. Inaktivera även SMB v1 på alla system eftersom det ofta utnyttjasill att sprida skadlig programvara i miljöer.
- Utvärdera svagheter på dina exponerade tillgångar för att hitta saknade programfixar och kritiska felkonfigurationer.

- Säkerställ att dina användare är uppmärksamma på phising och annan typ av social manipulation som gör er sårbara för intrång.
- Kontrollera din säkerhetskopieringsstrategi, distribution, säkerhetskopieringsplatser (inklusive utanför offline), plan för att återskapa i kritiska fall och rutiner så fort som möjligt.
- Om ni använder OT så bör ni undersöka dess kopplingar till externa system och övervaka intern OT-aktivitet.
- Se till att det finns en uppdaterad åtgärdsplan för incidenter med korrekta kontaktuppgifter.

Slutsats

Just nu finns det två större destruktiva skadliga program som dykt upp under den senaste månaden. Båda verkar ha kopplingar till kriget i Ukraina eftersom tidpunkterna stämmer överens och TTP:erna liknar tidigare cyberattacker från ryska statliga hotaktörer. Vi förväntar oss att mer skadlig programvara utvecklas med det primära målet att orsaka störningar och förstöra data för att ge endera sida fördel i cyberkriget. Men när konflikten väl är löst tror vi att dessa skadliga verktyg blir tillgängliga för försäljning/användning för att rikta in sig på andra offer som inte är relaterade till det pågående kriget.

Var uppmärksam på att hotbilder och risker kan förändras.