KillDisk Variant Hits Latin American Financial Groups

January 15, 2018

Content added to Folio

Cyber Threats

Trend Micro Research came across a new variant of the disk-wiping KillDisk targeting financial organizations in Latin America. Initial analysis reveals that it may be a component of another payload, or part of a bigger attack.

By: Gilbert Sison, Rheniel Ramos, Jay Yaneza, Alfredo Oliveira January 15, 2018 Read time: (words)

Updated as of January 15, 11:58 PM PDT to clarify that the new variant of KillDisk we found does not have a ransom note.

We came across a new variant of the disk-wiping KillDisk targeting financial organizations in Latin America. Trend Micro detects it as TROJ_KILLDISK.IUB. Trend Micro™ Deep Discovery™ proactively blocks any intrusions or attacks associated with this threat. Initial analysis (which is still ongoing) reveals that it may be a component of another payload, or part of a bigger attack. We are still analyzing this new KillDisk variant and we will update this post as we uncover more details about this threat.

KillDisk, along with the multipurpose, cyberespionage-related BlackEnergy, was used in cyberattacks in late December 2015 against Ukraine's energy sector as well as its banking, rail, and mining industries. The malware has since metamorphosed into a threat used for digital extortion, affecting Windows and Linux platforms. The note accompanying the ransomware versions, like in the case of Petya, was a ruse: Because KillDisk also overwrites and deletes files (and don't store the encryption keys on disk or online), recovering the scrambled files was out of the question. The new variant we found, however, does not include a ransom note.

Figure 1. KillDisk's infection chain

How is it dropped in the system?

This KillDisk variant looks like it is intentionally dropped by another process/attacker. Its file path is hardcoded in the malware (*c:\windows\dimens.exe*), which means that it is tightly coupled with its installer or is a part of a bigger package.

Figure 2. The new KillDisk variant's parameter to shut down the affected machine

KillDisk also has a self-destruct process, although it isn't really deleting itself. It renames its file to *c:\windows\0123456789* while running. This string is hardcoded in the sample we analyzed. It expects its file path to *be c:\windows\dimens.exe* (also hardcoded). Accordingly, if disk forensics is performed and *dimens.exe* is searched, the file that will be retrieved will be the newly created file with 0x00 byte content.

How does it delete files?

This new KillDisk variant goes through all logical drives (fixed and removable) starting from drive *b:*. If the logical drive contains the system directory, the files and folders in the following directories and subdirectories are exempted from deletion:

- WINNT
- Users
- Windows
- Program Files
- Program Files (x86)
- ProgramData
- Recovery (case-sensitive check)
- $Recycle.Bin

- System Volume Information
- old
- PerfLogs
-

Before a file is deleted, it is first randomly renamed. KillDisk will overwrite the first 0x2800 bytes of the file and another block that’s 0x2800-bytes big with 0x00.

Figure 3. Code snippets showing how KillDisk overwrites then deletes files

How does it wipe the disk?

The malware attempts to wipe \\.\PhysicalDrive0 to \\.\PhysicalDrive4. It reads the Master Boot Record (MBR) of every device it successfully opens and proceeds to overwrite the first 0x20 sectors of the device with “0x00”. It uses the information from the MBR to do further damage to the partitions it lists. If the partition it finds is not an extended one, it overwrites the first 0x10 and last sectors of the actual volume. If it finds an extended partition, it will overwrite the Extended Boot Record (EBR) along with the two extra partitions it points to.

Figure 4. Code snippets showing how KillDisk reads/scans the MBR (top, center), and overwrites the EBR (bottom)

What happens after the MBR, files, and folders are overwritten and/or deleted?

KillDisk has a numeric parameter that denotes the number of minutes (15 being the default) it will wait before it shuts down the affected machine. To try to reboot the machine, it will try to terminate these processes:

- Client/server run-time subsystem (csrss.exe)
- Windows Start-Up Application (wininit.exe)
- Windows Logon Application (winlogon.exe)
- Local Security Authority Subsystem Service (lsass.exe)

This is done most likely to force a reboot or dupe the user into restarting the machine. Terminating csrss.exe and wininit.exe, for instance, will cause a blue screen of death (BSOD). Terminating winlogon.exe will prompt the user to log in again, while terminating lsass.exe will cause a reboot. KillDisk also uses the *ExitWindowsEx* function to forcefully restart the machine.

Figure 5. Code showing KillDisk forcefully rebooting the system

What can organizations do?

KillDisk’s destructive capabilities, and how it could be just a part of a bigger attack, highlight the significance of defense in depth: securing the perimeters — from gateways, endpoints, and networks to servers — to further reduce the attack surface. Here are some best practices for organizations.

- Keep the system and its applications updated/patched to deter attackers from exploiting security gaps; consider virtual patching for legacy systems.
- Regularly back up data and ensure its integrity.
- Enforce the principle of least privilege. Network segmentation and data categorization help prevent lateral movement and further exposure.
- Deploy security mechanisms such as application control/whitelisting and behavior monitoring, which can block suspicious programs from running and thwart anomalous system modifications.
- Proactively monitor the system and network; enable and employ firewalls as well as intrusion prevention and detection systems.
- Implement a managed incident response policy that will drive proactive remediation strategies; further strengthen the organization’s security posture by cultivating a cybersecurity-aware workplace.

Trend Micro™ XGen™ security provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It features high-fidelity machine learning to secure
the gateway and endpoint data and applications, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen protects against today’s purpose-built threats that bypass traditional controls and exploit known, unknown, or undisclosed vulnerabilities. Smart, optimized, and connected, XGen powers Trend Micro’s suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Related Hash (SHA-256):

> 8a81a1d0fae933862b51f63064069aa5af3854763f5edc29c997964de5e284e5
> — TROJ_KILLDISK.IUB

sXpIBdPeKzI9PC2p0SWMpUSM2NSxWzPyXTMLlbXmYa0R20xk