KillDisk Variant Hits Latin American Finance Industry

blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-latin-american-financial-organizations-again/

June 7, 2018

In January, we saw a variant of the disk-wiping KillDisk malware hitting several financial institutions in Latin America. One of these attacks was related to a foiled heist on the organization's system connected to the Society for Worldwide Interbank Financial Telecommunication's (SWIFT) network.

Last May, we uncovered a master boot record (MBR)-wiping malware in the same region. One of the affected organizations was a bank whose systems were rendered inoperable for several days, thereby disrupting operations for almost a week and limiting services to customers. Our analysis indicates that the attack was used only as a distraction — the end goal was to access the systems connected to the bank's local SWIFT network.

The telltale sign was a problem related to the affected machine's boot sector. Based on the error message it displayed after our tests, we were able to ascertain that this was another — possibly new — variant of KillDisk. This kind of notification is common in systems affected by MBR-wiping threats and not in other malware types such as ransomware, which some people initially believed to be the culprit. Trend Micro products detect this threat as TROJ_KILLMBR.EE and TROJ_KILLDISK.IUE.

The nature of this payload alone makes it difficult to determine if the attack was motivated by an opportunistic cybercriminal campaign or part of a coordinated attack like the previous attacks we observed last January.

 *Figure 1. Error screen after the boot sector is overwritten*

Initial analysis

We were able to source a sample that may be the malware involved in the May 2018 attacks. We ran it, and it broke the boot sector as expected (see Figure 1). An initial analysis of the file revealed it was created using Nullsoft Scriptable Install System (NSIS), an open-source application used to create setup programs. The actor behind this threat used the application and purposely named it “MBR Killer.” Although the sample was protected by VMProtect (a virtualization protector used to defend against reverse engineering), we were still able to verify that it has a routine that wipes the first sector of the machine’s physical disk, as shown in Figure 2. We haven’t found any other new or notable routines in the sample we have. There is no evident command-and-control (C&C) infrastructure or communication, or ransomware-like routines coded into the sample. There are no indications of network-related behavior in this malware.

 *Figure 2. The malware named “MBR Killer” (highlighted, top) and a code snippet showing its routine of wiping the disk’s first sector (bottom)*

 *Figure 3. How the malware carries out its MBR-wiping routine*

How the malware wipes the affected machine’s disk

The malware was designed to wipe all the physical hard disks it can find in the infected system. Here’s a summary of how it performs its MBR-wiping routine:

1. It uses the application programming interface (API) *CreateFileA* to \\.*PHYSICALDRIVE0* to retrieve the handle of the hard disk.
2. It overwrites the first sector of the disk (512 bytes) with "0x00". The first sector is the disk’s MBR.
3. It will try to perform the routines above (steps 1-2) on \\.*PHYSICALDRIVE1*, \\.*PHYSICALDRIVE2*, \\.*PHYSICALDRIVE3*, and so on, as long as a hard disk is available.
4. It will then force the machine to shut down via the API *ExitWindows*.

When calling the APIs, the main executable will drop the component file *%User Temp%/ns{5 random characters}.tmp/System.dll.* The main executable will then load the dynamic-link library (DLL) file, which has the export function “Call” used to call for the APIs.

Mitigation and best practices

The destructive capabilities of this malware, which can render the affected machine inoperable, underscore the significance of defense in depth: arraying security to cover each layer of the organization's IT infrastructure, from gateways and endpoints to networks and servers. Here are some best practices that organizations can adopt to defend against this kind of threat:

- ***Identify and address security gaps.*** Regularly patch and update networks, systems, and programs/applications to remove exploitable vulnerabilities. Create strict patch management policies and consider virtual patching, especially for legacy systems. Regularly back up data and safeguard its integrity.
- ***Secure mission-critical infrastructure.*** Secure the infrastructure used to store and manage personal and corporate data. For financial institutions, SWIFT has a Customer Security Programme that provides mandatory and advisory controls for their local SWIFT infrastructure. Some of these include virtual patching, vulnerability scanning, application control, and integrity monitoring of SWIFT-related applications.
- ***Enforce the principle of least privilege.*** Restrict access to mission-critical data. Network segmentation limits user or program access to the network; data categorization organizes data by importance to minimize further exposure to threats or breaches. Restrict access to and use of tools reserved for system administrators (for example, PowerShell, command-line tools) to prevent them from being abused. Disable outdated and unneeded system or application components.
- ***Proactively monitor online premises.*** Deploy additional security mechanisms to further hinder attackers. Firewalls and intrusion detection and prevention systems help against network-based attacks, while application control and behavior monitoring prevent the execution of suspicious and unwanted files or malicious routines. URL categorization also helps prevent access to malware-hosting sites.
- ***Foster a culture of cybersecurity.*** Many threats rely on social engineering to succeed. Awareness of the telltale signs of spam and phishing emails, for instance, significantly helps thwart email-based threats.
- ***Create a proactive incident response strategy.*** Complement defensive measures with incident response strategies that provide actionable threat intelligence and insights to help IT and information security teams actively hunt for, detect, analyze, correlate, and respond to threats.

Trend Micro Solutions

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.

Indicators of Compromise (IOCs)

Related Hashes (SHA-256):

- a3f2c60aa5af9d903a31ec3c1d02eeeb895c02fcf3094a049a3bdf3aa3d714c8 — TROJ_KILLMBR.EE
- 1a09b182c63207aa6988b064ec0ee811c173724c33cf6dfe36437427a5c23446 — TROJ_KILLDISK.IUE

Malware

In January, we saw a variant of the disk-wiping KillDisk malware hitting several financial institutions in Latin America. Last May, we uncovered a master boot record (MBR)-wiping malware in the same region.

By: Fernando Merces, Byron Gelera, Martin Co June 07, 2018 Read time: (words)

Content added to Folio