Defined: TEMP.Hermit North Korean Cyber Espionage Activity

Fusion (FS) | Cyber Espionage (CE)

October 08, 2018 11:12:00 AM, 17-00009537, Version: 4

Executive Summary

- TEMP.Hermit is a cluster of sophisticated and well-resourced North Korean activity that uses custom backdoors and strategic web compromises.
- TEMP.Hermit has used zero-day vulnerabilities; and engages in data destruction, theft, and manipulation.
- Though early TEMP.Hermit operations primarily targeted entities on the Korean Peninsula, current operations show expansion to include targets worldwide and suggest financial motivations to benefit the North Korean regime.

Threat Detail

New Version Details

Version 4, Oct. 4, 2018: Significant changes and updates to split off activity that has been attributed to a threat group now tracked as APT38 (18-00016353).

Version 3, May 23, 2018: Added information regarding the SMOOTHRIDE Flash loader and the RAWHIDE downloader.

Threat Detail

TEMP.Hermit is a cluster of cyber espionage activity that has been active since at least 2013. While the group primarily targets entities in South Korea, TEMP.Hermit has also targeted entities linked to North Korean affairs worldwide. As such, we believe that the group's primary mission includes the collection of strategic intelligence against countries that would benefit North Korean interests and dissident activity deemed a threat to the regime.

- TEMP.Hermit primarily targets government, defense, and financial institutions on the Korean Peninsula.
- In July 2017, U.S. aerospace defense contractors were targeted by the group with Terminal High Altitude Area Defense (THAAD)-themed lures. Some of the lures specifically targeted individuals holding U.S. Top Secret/Sensitive Compartmented Information (TS/SCI) and Secret security clearances.
- In 2015, two U.S. universities were compromised by CAKETEARS. The universities were likely targeted due to their relationships with North Korean defector awareness groups.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

Links to Financially Motivated Activity

TEMP.Hermit has been linked, with varying degrees of confidence, to multiple instances of cyber activity undertaken for financial gain, rather than information advantage. These include global SWIFT-fraud operations attributed to APT38, WANNACRY ransomware attacks, and targeting of bitcoin exchanges in South Korea. Criminal activities, including counterfeiting and drug smuggling, have long been a part of North Korea's efforts to evade sanctions and fund the regime. These cyber operations are the latest manifestation of this effort.

- TEMP.Hermit is believed to share significant development resources with APT38, a North Korean regime-sponsored group that conducts complex bank heist operations. A primary reason that these groups are frequently lumped together in public reporting is because they share malware code and functionality across multiple distinct regime-backed operations.
- Code shared between the WANNACRY malware and TEMP.Hermit tool MACKTRUCK suggests a link between TEMP.Hermit and the ransomware activity.
- In May 2017, PEACHPIT was leveraged in a spear-phishing operation against digital currency companies in South Korea.

Attribution and Scope

We believe that activity attributed to TEMP.Hermit is conducted on behalf of North Korea; however, this group's reliance on compromised infrastructure hinders analysis efforts. We characterize TEMP.Hermit activity by consistent targeting and tactics, techniques, and procedures (TTPs) along with code shared between malware in a way that indicates a shared codebase. Multiple scenarios could explain the observed evidence, but we are currently unable to attribute to that level of granularity. We believe that TEMP.Hermit broadly aligns with the publicly reported group "Lazarus"; however, we do not attribute all activity reported as "Lazarus" to TEMP.Hermit. Some TEMP.Hermit activity has also been publicly referred to as "Hidden Cobra" by the U.S. Department of Homeland Security. We attribute TEMP.Hermit's activity to North Korea due to multiple factors, including Korean-language artifacts in malware and a targeting focus on South Korea.

- U.S. Department of Justice (DOJ) allegations against Park Jin Hyok, a North Korean programmer, provide significant details linking TEMP.Hermit-attributed operations to the North Korean regime (18-00014948). The complaint published in September 2018 includes IP addresses, multiple overlapping email and social media accounts, and links between TEMP.Hermit operations and known North Korean front organizations.
- Multiple pieces of TEMP.Hermit malware have had Korean-language artifacts, indicating that the programmers were likely Korean-language speakers (15-00012308). In addition, TEMP.Hermit operations have focused on South Korea, including destructive attacks.
- A shared codebase could be drawn on by multiple actor groups with different missions. These operational subgroups within TEMP.Hermit, have been theorized by Kaspersky Labs here. The use of certain malware only for one type of goal supports this theory; however, other malware used by TEMP.Hermit has been used for multiple missions, complicating the assessment.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- The code overlaps could also be the result of bureaucratic separation between developers and operators. It is possible that one organization develops a codebase with modules or example code with defined functionality. A separate operational organization could then take the code that corresponds with the desired functionality and compile it themselves. In this case, the variance would be explained by inconsistencies between individual actors.

Tactics, Techniques, and Procedures (TTPs)

TEMP.Hermit typically leverages target-specific spear-phishing lures to trick the user into downloading malware, but it has demonstrated the capability to leverage watering hole tactics as well. The group historically targets South Korean organizations and individuals. Additionally, TEMP.Hermit attempts to obfuscate its activities on victims' machines.

- TEMP.Hermit specifically targets machines running Korean-language operating systems, relying heavily on vulnerabilities to Hangul Word Processor (HWP), software that is prevalent across public and private sectors in South Korea.
- TEMP.Hermit leveraged a strategic web compromise to distribute VOLGMER (HANGMAN) malware in 2016.
- The group deploys malware that runs anti-emulation checks and uses encoded API names to limit malware analysis.

Observed Targets

Countries

Observed Targets (Countries)	
South Korea	United States
	Switzerland

Table 1: Observed targets (countries)

Industries

Observed Targets (Industries)		
Aerospace and Defense	Energy	Financial
High-Tech	Telecommunications	Media
Government	Transportation	Education
Retail		

Table 2: Observed targets (industries)

Vulnerabilities

To date, the following vulnerabilities have been leveraged in TEMP.Hermit operations.

CVE	Description
	Microsoft Office 2010 SP2, Office 2013 SP1, and Office 2016 allow a remote code execution vulnerability

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

CVE-2017-0262	when the software fails to properly handle objects in memory, known as "Office Remote Code Execution Vulnerability."
CVE-2016-4117	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2016-1019	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial-of-service (DoS) or possibly execute arbitrary code via unspecified vectors.
CVE-2015-8651	Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK and Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-6585	Vulnerability in Hangul Word Processor that allows remote users to execute arbitrary code via a crafted heap spray, and by leveraging a "type confusion" via an HWPX file containing a crafted para text tag.

Table 3: Vulnerabilities exploited by TEMP.Hermit

MALWARE

We believe that the malware found in Table 4 is unique to TEMP.Hermit.

TEMP.Hermit malware	
VOLGMER (HANGMAN)	PEACECOFFEE
PEACHPIT	CAKETEARS
MACKTRUCK	MONKEYCHERRY
FALLCHILL	

Table 4: TEMP.Hermit malware

VOLGMER

VOLGMER (publicly referred to as HANGMAN) is almost certainly used only in cyber espionage operations against South Korean targets based on its use of an HWP exploit and its configuration to run only on Korean computers.

- VOLGMER attempts to evade network detection and can download, upload, and delete files; execute commands; list directories; and terminate processes.
- In 2015, FireEye reported on VOLGMER exploiting a zero-day vulnerability affecting CVE-2015-6585. The widespread use of the HWP software in South Korean organizations, including government, opens these organizations to compromises by VOLGMER.
- Before the first observation of VOLGMER using the HWP exploit, MS Office macros were used to drop the payload. Although the exploits differed, the lure documents

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

continued to exclusively target South Korean entities. These lures were written in Korean and masqueraded as South Korean government or company documents. In one case, a lure sent to a South Korean government agency was disguised as a resume.
- Security vendors reported on VOLGMER in late 2014, linking the malware with the DESTOVER malware used in the Sony breach.
- According to public reports, an early version of the VOLGMER Trojan shared a command and control (C&C) server with DESTOVER.
- VOLGMER was linked to the 2013 Jokra campaign against South Korean media and financial institutions through functional similarities and the C&C infrastructure.

PEACHPIT

FireEye iSIGHT Intelligence first identified PEACHPIT, a VOLGMER variant in November 2015, being used against the South Korean Atomic Energy Research Institute. Like VOLGMER, PEACHPIT can gather a victim's system data, download, upload and execute files, and update the service registry key. While PEACHPIT uses the VOLGMER loader, the PEACHPIT variant drops COMPCONF.DLL (MD5: c89b2b22d7374abd857ebdfb6656a405) instead of INSs.DLL (MD5: eb9db98914207815d763e2e5cfbe96b9) used by VOLGMER.

- Past targeting indicates a high likelihood that PEACHPIT mainly targets South Korean organizations. However, the vulnerabilities leveraged by PEACHPIT are not unique to South Korean systems and are likely able to affect non-South Korean organizations.
- In May 2017, PEACHPIT was observed using lure documents targeting virtual currency services using a spear-phishing campaign. The documents exploited the CVE-2017-0262 vulnerability to drop PEACHPIT on the targeted machine.
- In 2016, FireEye iSIGHT Intelligence observed PEACHPIT operating with a new C&C infrastructure, likely because of expanding operations against South Korean targets.
- The earliest observed deployment leveraged an invitation to the South Korean 2015 Aerospace Weapons Seminar through a spear-phishing campaign. PEACHPIT, like VOLGMER, exploited the CVE-2015-6585 HWP vulnerability.
- PEACHPIT was observed again in the second quarter of 2015, targeting individuals associated with a South Korean think tank and an organization operating in public administration.

MACKTRUCK

MACKTRUCK is a backdoor that attempts to hide itself from detection and analysis by using encoded API names and running anti-emulation checks. According to 2016 FireEye iSIGHT Intelligence reporting, MACKTRUCK has been observed only in a small number of cases. The malware is configured to allow it to run only after a specific date or on a particular system. If the targeted system does not meet the requirements, MACKTRUCK will exit the system.

- NESTEGG was observed only on machines previously infected with MACKTRUCK and was used in the SWIFT manipulation attacks in Southeast Asia. As both malware families have only been observed in a small number of cases, it is unlikely that their overlap is coincidental.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- Based on observed operations, the MACKTRUCK backdoor is likely used when targeting financial institutions for SWIFT fraud. However, MACKTRUCK could be leveraged against organizations across different sectors.

FALLCHILL

FALLCHILL is a malware tool linked to TEMP.Hermit based on code overlap with MACKTRUCK and PEACHPIT malware. They share similar loading of library functions and the command to create a process and redirect output to a temp file. FALLCHILL is a threat to organizations in the public and private sector, as it has been leveraged against organizations in varying industries.

- Like VOLGMER and PEACHPIT, FALLCHILL gathers intelligence for a later operation.
- FALLCHILL can run on 32-bit and 64-bit systems, giving operators greater access to newer machines.
- In late 2016, TEMP.Hermit deployed the FALLCHILL backdoor against telecommunication companies and financial institutions.
- Unlike previous TEMP.Hermit malware, FALLCHILL was seen operating in a Northern European country, in addition to Asia. This is likely an indication of the group's recent expansion of operations beyond East Asia.

PEACECOFFEE

PEACECOFFEE is a backdoor dropped via spear-phishing lures that can collect system information, manipulate processes, list audio and video files, and download, upload, and execute files. Based on previous observations and the dropper using a Korean-language popup, PEACECOFFEE is primarily a threat to South Korean organizations in the retail and high-tech sectors. However, it is possible for PEACECOFFEE to be leveraged against other sectors in South Korea.

- PEACECOFFEE was leveraged in targeting retail companies by sending a decoy MS Word document disguised as a resume in an email.
- South Korean high-tech industries were sent emails containing computer animated videos and a JPEG and PPT file highlighting 10Kw charging modules. Each email contained a self-extracting RAR that dropped PEACECOFFEE onto the victim's system.
- PEACECOFFEE targeted systems running Windows 7 or later versions. If the infected machine ran a version before Windows 7, PEACECOFFEE would not execute.

CAKETEARS

TEMP.Hermit was observed using CAKETEARS to establish backdoors in at least two U.S. universities; a South Korea-based telecommunications organization; and a Switzerland-based company in the media, business services, and transportation sectors. As such, CAKETEARS can likely be leveraged across multiple industries operating globally by TEMP.Hermit to gain access to sensitive information that can be exploited for later operations.

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- CAKETEARS will only execute if the machine has a Korean locale OS, the system is up for more than six minutes, and the machine operates on Windows XP or a more recent version.
- CAKETEARS is a tool used to collect system information; list, download, and execute files; and communicate with C&C infrastructure.

MONKEYCHERRY

MONKEYCHERRY is an embedded macro that automatically executes if macros are enabled. After execution, it decodes, drops, and executes the FALLCHILL backdoor.

- TEMP.Hermit leveraged MONKEYCHERRY and FALLCHILL against U.S. defense contractors that supply South Korea with tactical systems in July 2017.
- The decoy documents were job descriptions or U.S. Government proposals tailored for the contractors. Some of these documents noted the need for individuals to hold a U.S. Top Secret/SCI or Secret security clearance.

Outlook

TEMP.Hermit will likely remain a persistent threat to public and private sector organizations on the Korean Peninsula. Further, the group will likely continue to rely on vulnerabilities to HWP documents based on the software's prevalence in South Korea. Given observed targeting and the group's recent use of MONKEYCHERRY and FALLCHILL, we believe TEMP.Hermit's operations are conducted in support of tactical and strategic directives that support North Korean interests. In particular, government and defense organizations are likely at a heightened risk of targeting due to political conflicts concerning North Korea's missile program and South Korea's THAAD deployment plans.

Please rate this product by taking a short four question survey

First Version Publish Date

September 07, 2017 10:01:00 AM

Threat Intelligence Tags

Motivation

- Military/Security/Diplomatic

Affected System

- Users/Application and Software

Source Geography

- North Korea

Affected Industry

- Aerospace & Defense

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- Industrial Engineering
- Financial Services
- Automobile & Parts
- Media
- Government - Subnational
- Telecommunications
- Industrial Support Services
- Retail
- Electronic & Electrical Equipment
- Electricity
- Education
- Technology
- General Industrials
- Government - National
- Travel & Leisure
- Industrial Transportation

Intended Effect

- Military Advantage
- Political Advantage

Tactics, Techniques And Procedures(TTPs)

- Network Reconnaissance
- Malware Propagation and Deployment
- Fraud
- Exploit Development

Target Geography

- South Korea
- United States
- Switzerland

Actor

- Hermit

Targeted Information

- Government Information
- IT Information
- Credentials

Malware Family

- HANGMAN
- PEACHPIT
- PEACECOFFEE
- MACKTRUCK

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

- FALLCHILL
- MONKEYCHERRY
- CAKETEARS

Common Vulnerabilities and Exposures

CVE ID:	CVE-2017-0262(NVD Description)External Link CVE-2016-4117(NVD Description)External Link CVE-2016-1019(NVD Description)External Link CVE-2015-8651(NVD Description)External Link CVE-2015-6585(NVD Description)External Link

Version Information

Version:1.0, September 07, 2017 10:01:00 AM
Defined: TEMP.Hermit North Korean Cyber Espionage Activity

Version:2.0, May 22, 2018 03:03:00 PM
Defined: TEMP.Hermit North Korean Cyber Espionage Activity

Version:3.0, May 29, 2018 08:09:00 AM
Defined: TEMP.Hermit North Korean Cyber Espionage Activity

Version:4.0, October 08, 2018 11:12:00 AM
Defined: TEMP.Hermit North Korean Cyber Espionage Activity

Confidential and Proprietary / Copyright © 2020 FireEye, Inc. All rights reserved.

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: https://intelligence.fireeye.com/reports/17-00009537

© 2020, FireEye, Inc. All rights reserved.