APT37 (REAPER)

The Overlooked North Korean Actor

SPECIAL REPORT

CONTENTS

INTRODUCTION

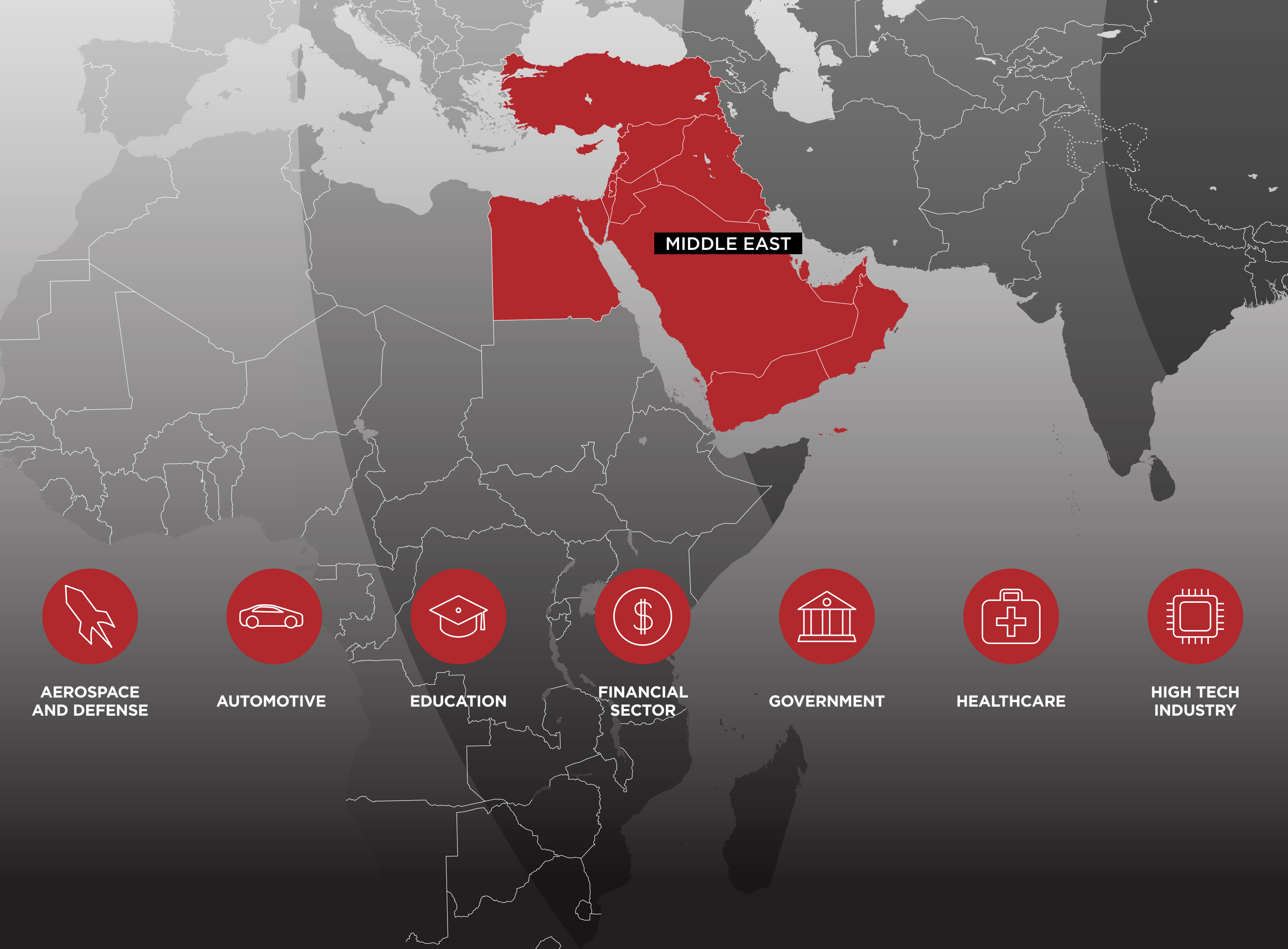
On Feb. 2, 2018, we published a blog detailing the use of an Adobe Flash zero-day vulnerability (CVE-2018-4878) by a suspected North Korean cyber espionage group that we now track as APT37 (Reaper). Recent examination of this group's activities by FireEye iSIGHT Intelligence reveals APT37 has expanded its operations in both scope and sophistication. APT37's toolset, which includes access to zero-day vulnerabilities and wiper malware, combined with heightened tensions in Northeast Asia and North Korea's penchant for norm breaking, means this group should be taken seriously.

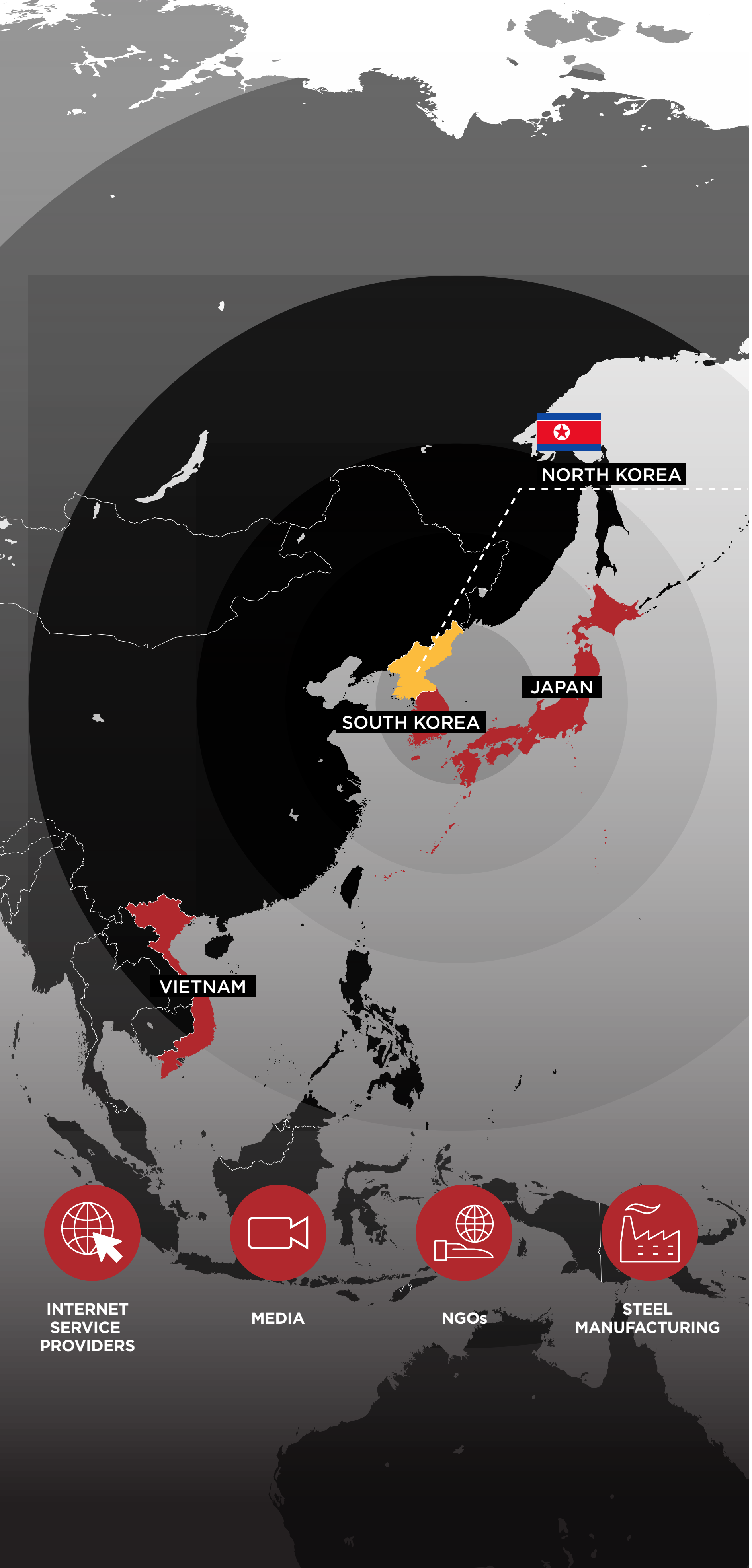
We assess with high confidence that this activity is carried out on behalf of the North Korean government given malware development artifacts and targeting that aligns with North Korean state interests. FireEye iSIGHT Intelligence believes that APT37 is aligned with the activity publicly reported as Scarcruft and Group123.

Targeting and Mission

APT37 has likely been active since at least 2012 and focuses on targeting the public and private sectors primarily in South Korea. In 2017, APT37 expanded its targeting beyond the Korean peninsula to include Japan, Vietnam and the Middle East, and to a wider range of industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive and healthcare entities (Fig. 1).

Figure 1. APT37 Targeting Scope.

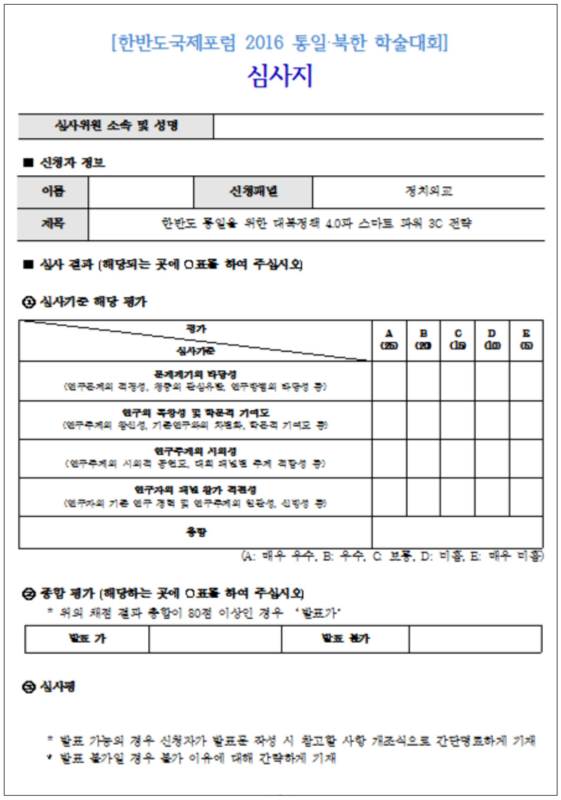




We judge that APT37's primary mission is covert intelligence gathering in support of North Korea's strategic military, political and economic interests. This is based on consistent targeting of South Korean public and private entities and social engineering. APT37's recently expanded targeting scope also appears to have direct relevance to North Korea's strategic interests.

From 2014 to 2017, APT37 targeting concentrated primarily on the South Korean government, military, defense industrial base, and media sector. Lure materials (Fig. 2) typically leveraged the Korean language and featured themes such as Korean peninsula reunification or sanctions.

Figure 2. "2016 Korean Reunification Conference Form" (MD5:183be2035d5a546670d2b9deeca4eb59).



[한반도국제포럼 2016 통일·북한 학술대회]

심사지

심사위원 소속 및 성명	

■ 신청자 정보

이름		신청패널	정치외교
제목	한반도 통일을 위한 대북정책 4.0과 스마트 파워 3C 전략		

■ 심사 결과 (해당되는 곳에 O표를 하여 주십시오)

① 심사기준 해당 평가

평가 심사기준	A (25)	B (20)	C (15)	D (10)	E (5)
문제제기의 타당성 (연구문제의 적정성, 청중의 관심유발, 연구방법의 타당성 등)					
연구의 독창성 및 학문적 기여도 (연구주제의 참신성, 기존연구와의 차별화, 학문적 기여도 등)					
연구주제의 시의성 (연구주제의 시의적 중요도, 대회 의제별 주제 적합성 등)					
연구자의 회의 참가 적격성 (연구자의 기존 연구 경력 및 연구주제의 일관성, 신뢰성 등)					
총합					

(A: 매우 우수, B: 우수, C: 보통, D: 미흡, E: 매우 미흡)

② 종합 평가 (해당하는 곳에 O표를 하여 주십시오)

* 위의 채점 결과 총합이 80점 이상인 경우 '발표가'

발표 가		발표 불가	

③ 심사평

* 발표 가능의 경우 신청자가 발표문 작성 시 참고할 사항 개조식으로 간단명료하게 기재
* 발표 불가일 경우 불가 이유에 대해 간략하게 기재

In 2017, APT37 targeted a Middle Eastern company that entered into a joint venture with the North Korean government to provide telecommunications service to the country (read on for a case study). At that time, other targets included individuals involved in international affairs and trade issues, the general director of a Vietnamese international trading and transport company, and possibly individuals working with Olympics organizations assisting in securing resources for athletes.

North Korean defector and human rights-related targeting provides further evidence that APT37 conducts operations aligned with the interests of North Korea.

APT37 targeted a research fellow, advisory member, and journalist associated with different North Korean human rights issues and strategic organizations. It also targeted an entity in Japan associated with the United Nations missions on sanctions and human rights. APT37 distributed SLOWDRIFT malware using a lure referencing the Korea Global Forum against academic and strategic institutions located in South Korea. Notably, the email was sent from a compromised South Korean institute that conducts studies on North Korea. The string “durihana,” which is also the name of a Christian missionary organization that works with North Korean defectors, was included in an APT37 weaponized document sent to an individual who works with a North Korean human rights organization.

CASE STUDY:

Targeting of Middle Eastern Organization with Business ties to North Korea

We believe a Middle Eastern organization was targeted by APT37 because it had been involved with a North Korean company and a business deal went bad. This firm was targeted shortly after media reports of this schism had gone public. The targeting effort may have been an attempt by the North Korean government to gather information on a former business partner. The operation exemplifies APT37’s tactics, techniques and procedures (TTPs), and reflects the advanced capabilities of this espionage group.

In May 2017, APT37 used a bank liquidation letter as a spear phishing lure against a board member of a Middle Eastern financial company. The specially crafted email included an attachment containing exploit code for CVE-2017-0199, a vulnerability in Microsoft Office that had been disclosed just a month earlier. Once opened, the malicious document communicated with a compromised website, most likely to surreptitiously download and install a backdoor called SHUTTERSPEED (MD5: 7c2ebfc7960aac6f8d58b37e3f092a9c). The tool would enable APT37 to collect system information, take screenshots and download additional malicious files to the victim computer.

Initial Infection Vectors

In addition to the aforementioned spear phishing tactics, APT37 leverages a variety of methods to deliver malware. These include strategic web compromises typical of targeted cyber espionage operations, as well as the use of torrent file-sharing sites to distribute malware more indiscriminately.

Numerous campaigns have employed social engineering tactics tailored specifically to desired targets. Lures and websites of particular interest to South Korean organizations (e.g. reunification) are regularly leveraged in campaigns. Multiple South Korean websites were abused in strategic web compromises to deliver newer variants of KARAE and POORAIM malware. Identified sites included South Korean conservative media and a news site for North Korean refugees and defectors. In one instance, APT37 weaponized a video downloader application with KARAE malware that was indiscriminately distributed to South Korean victims through torrent websites.

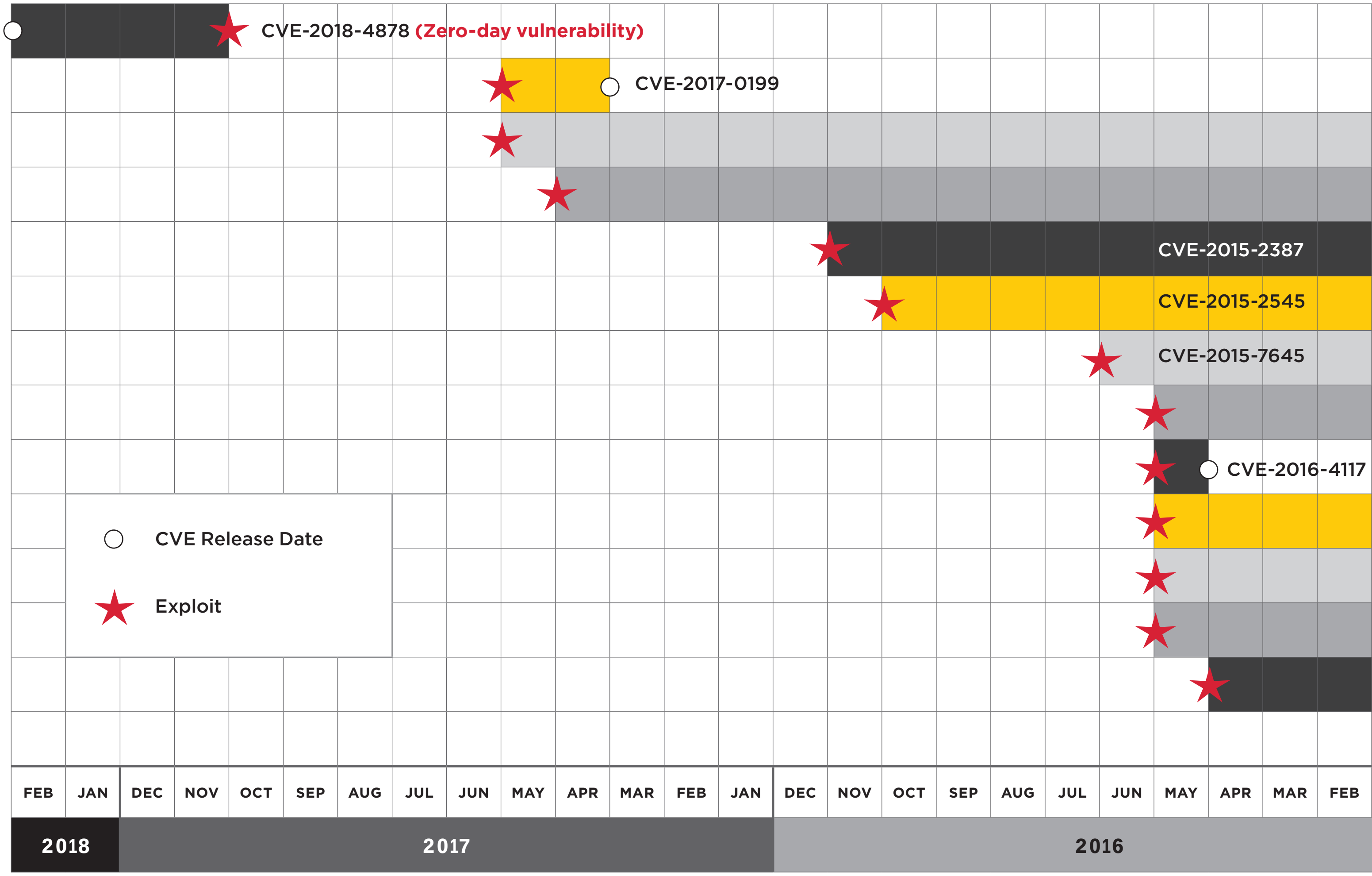


Figure 3. Timeline of CVE Release Dates vs. Dates of APT37 CVE Exploitation.

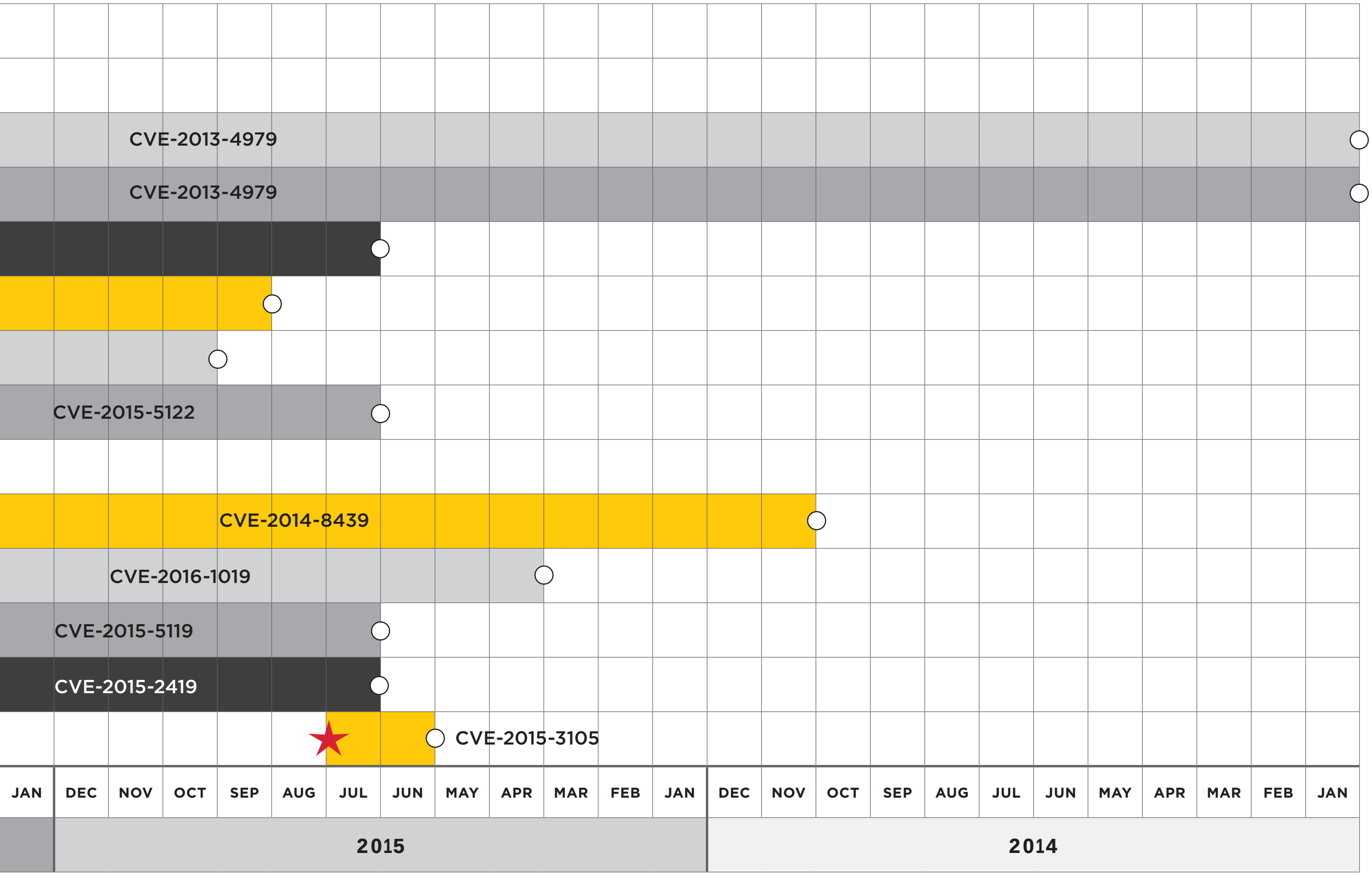
Exploited Vulnerabilities

APT37 frequently exploits vulnerabilities in Hangul Word Processor (HWP) due to the software's prevalence in South Korea. Further, the group recently demonstrated access to zero-day vulnerabilities (CVE-2018-0802) and has the flexibility to quickly incorporate recently publicized vulnerabilities into spear phishing and strategic web compromise operations. These capabilities suggest a high operational tempo and specialized expertise.

APT37 has repeatedly deployed exploits, especially in Flash, quickly after vulnerabilities are initially publicized (see Table 1). CVE-2016-4117, CVE-2016-1019 and CVE-2015-3043 were all exploited by APT37 in this way. FireEye iSIGHT Intelligence confirmed that since at least November 2017, APT37 exploited a zero-day Adobe Flash vulnerability, CVE-2018-4878, to distribute DOGCALL malware to South Korean victims.

While use and discovery of zero-day exploits over the past several years has expanded beyond a nation-state dominated environment to include commercial vendors of cyber espionage capabilities and sophisticated financially motivated actors, access to zero-day exploits remains a factor in distinguishing sophisticated or well-resourced actors.

Figure 3 details the vulnerabilities exploited by APT37, comparing the time of exploitation to the time the CVE was released.



Command and Control Infrastructure

APT37 uses a variety of techniques for command and control. They leverage compromised servers, messaging platforms and cloud service providers to avoid detection. The group often relies on compromised sites to host second stage malware payloads. Over time, APT37 has changed the email providers to set up command and control accounts in a possible attempt to cover their tracks and cause misdirection. These tactics have been refined over the years as APT37 evolves to evade network defenders.

APT37 has used various legitimate platforms as command and control for its malware tools. While some early campaigns leveraged POORAIM, which abused AOL Instant Messenger, newer activity deploys DOGCALL, which uses cloud storage APIs such as pCloud and Dropbox.

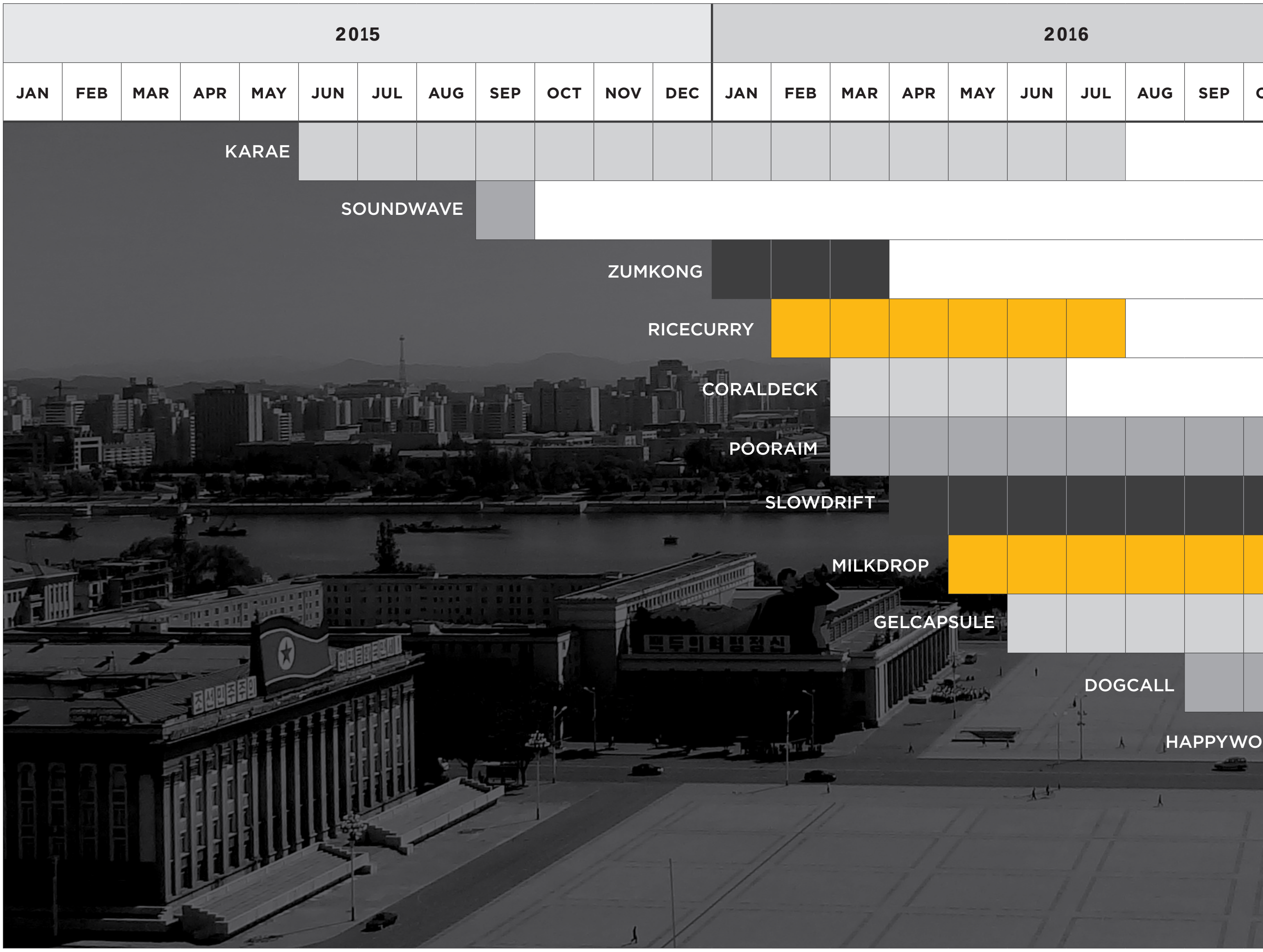
APT37 relies on compromised websites to host second stage malware. Small websites focused on subjects such as aromatherapy and scuba diving have been leveraged, and were most likely compromised opportunistically and made to host malicious payloads.

APT37 has improved its operational security over time. For example, early 2015 use of SLOWDRIFT involved credentials associated with Korea related mail servers such as “Daum.net”. Later, in 2015 and early 2016, APT37 pivoted to different email providers such as Gmail and “hmamail.com” in an attempt to anonymize activity. Then from mid-2016 onward, APT37 began using @yandex.com and @ india.com email accounts -- possibly an attempt to cause misattribution.

Malware

APT37 employs a diverse suite of malware for initial intrusion and exfiltration. Their malware is characterized by a focus on stealing information from victims, with many set up to automatically exfiltrate data of interest. Figure 4 shows APT37's malware usage over time. A full breakdown of the malware we associate with APT37, along with how it is detected by FireEye devices, is available in the Appendix.

Along with custom malware used for espionage purposes, APT37 also has access to destructive malware. In April 2017, APT37 targeted South Korean military and government organizations with the DOGCALL backdoor and RUHAPPY wiper malware. Although the wiper capability was not used in the identified instance, RUHAPPY can overwrite a machine's Master Boot Record (MBR), causing the system to fail to boot into preconfigured partitions.



It is possible that APT37's distribution of KARAE malware via torrent websites could assist in creating and maintaining botnets for future distributed denial-of-service (DDoS) attacks, or for other activity such as financially motivated campaigns or disruptive operations. Disruptive and destructive cyber threat activity, including the use of wiper malware, public leaks of proprietary materials by false hacktivist personas, DDoS attacks and electronic warfare tactics such as GPS signal jamming is consistent with past behavior by other North Korean actors.

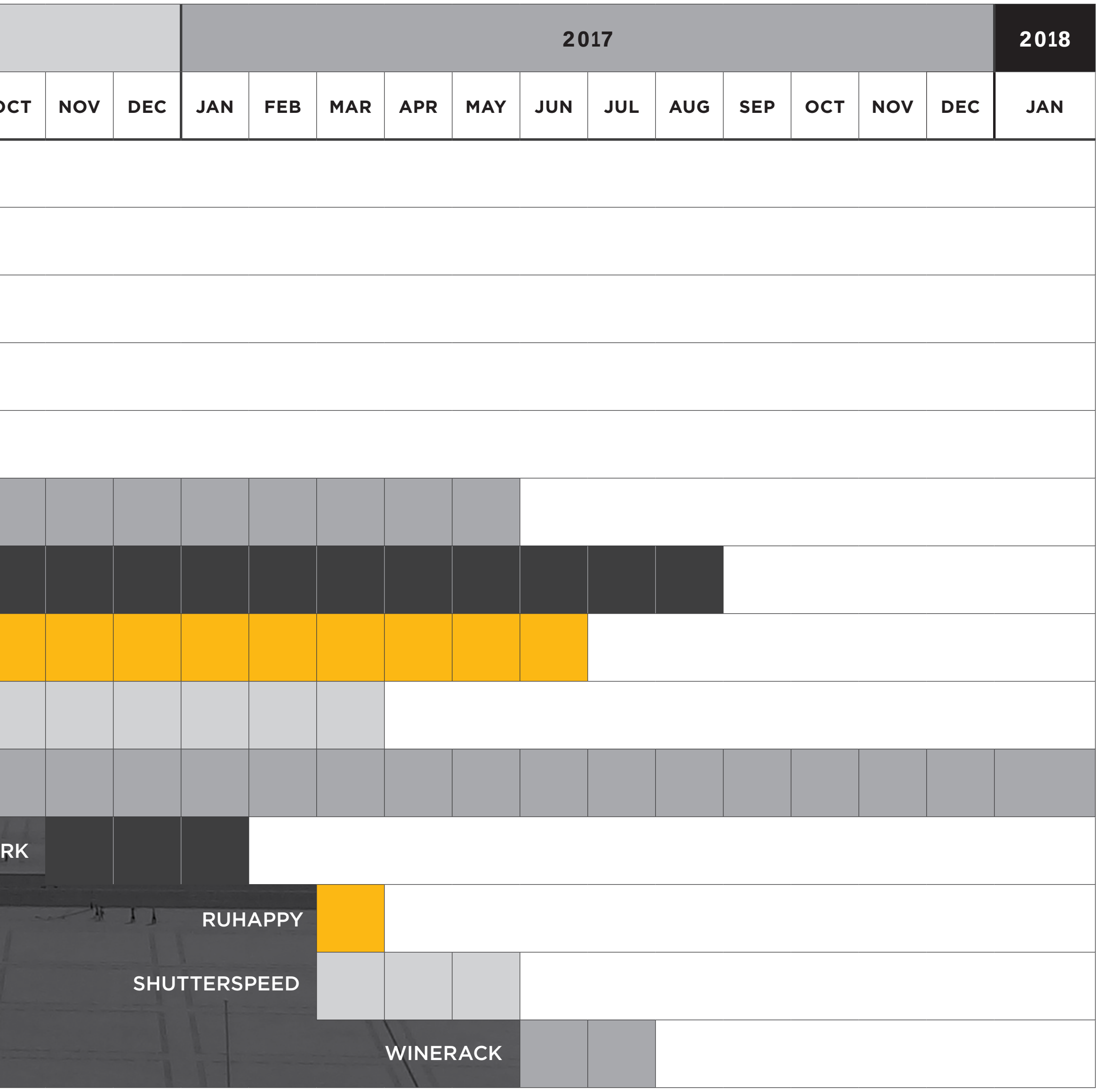


Figure 4.
Timeline of APT37 Malware Use
By First and Last Observed Compile Times.

Attribution

We assess with high confidence that APT37 acts in support of the North Korean government and is primarily based in North Korea. This assessment is based on multiple factors, including APT37's targeting profile, insight into the group's malware development and probable links to a North Korean individual believed to be the developer of several of APT37's proprietary malware families:

- An individual we believe to be the developer behind several APT37 malware payloads inadvertently disclosed personal data showing that the actor was operating from an IP address and access point associated with North Korea.
- The compilation times of APT37 malware is consistent with a developer operating in the North Korea time zone (UTC +8:30) and follows what is believed to be a typical North Korean workday (Fig. 5). The majority of malware compilation times occurred between 10:00 a.m. and 7:00 p.m., with a dip around noon. Additional activity occurred late into the evening. This is consistent with media reporting of extremely long hours for North Korean workers.
- The majority of APT37 activity continues to target South Korea, North Korean defectors, and organizations and individuals involved in Korean Peninsula reunification efforts. Similarly, APT37 targeting of a Middle Eastern company in 2017 is also consistent with North Korean objectives given the entity's extensive relationships inside North Korea.

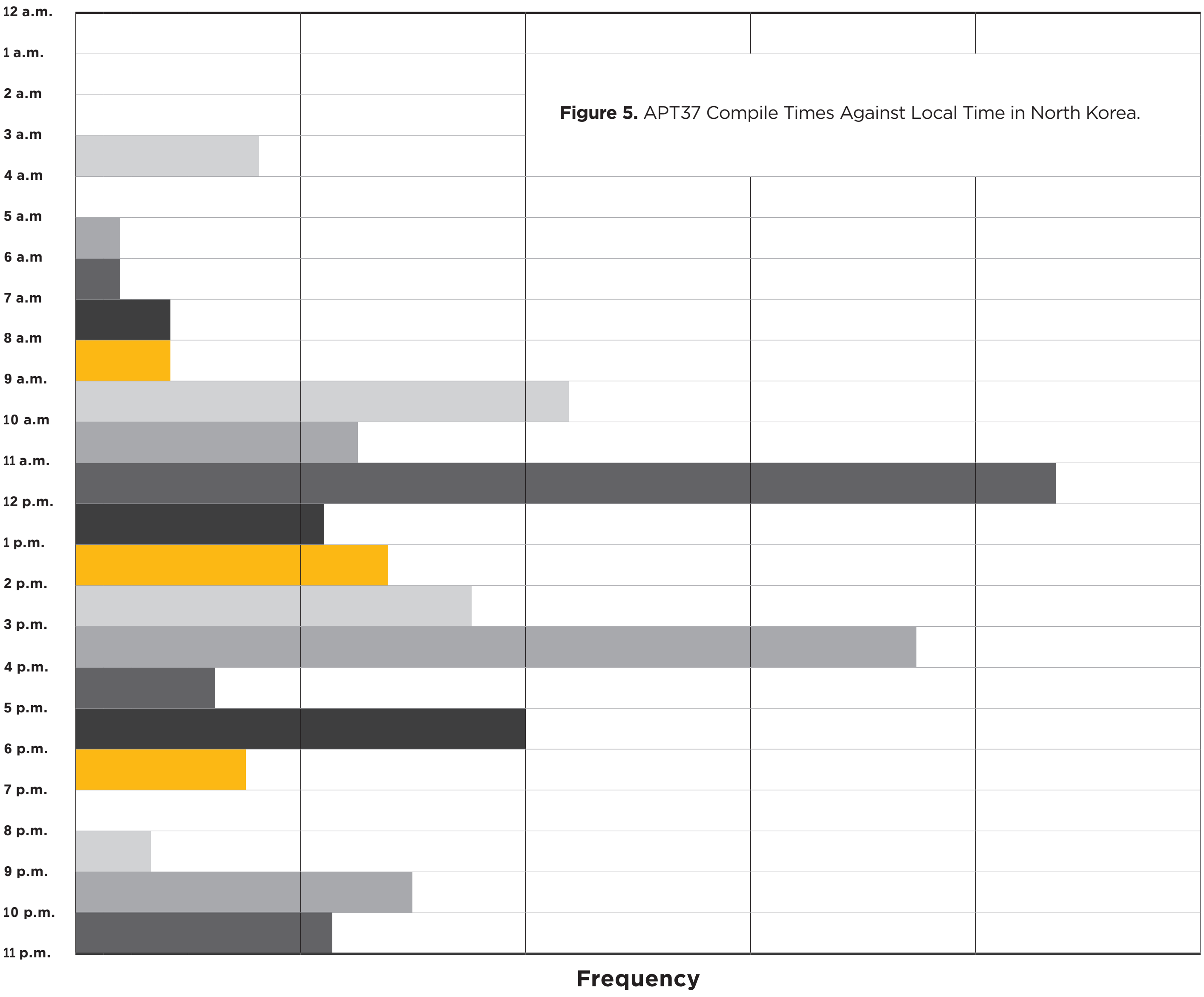


Figure 5. APT37 Compile Times Against Local Time in North Korea.

Outlook and Implications

North Korea has repeatedly demonstrated a willingness to leverage its cyber capabilities for a variety of purposes, undeterred by notional redlines and international norms. Though they have primarily tapped other tracked suspected North Korean teams to carry out the most aggressive actions, APT37 is an additional tool available to the regime, perhaps even desirable for its relative obscurity. We anticipate APT37 will be leveraged more and more in previously unfamiliar roles and regions, especially as pressure mounts on their sponsor.

The slow transformation of regional actors into global threats is well established. Minor incidents in Ukraine, the Middle East and South Korea have heralded the threats, which are now impossible to ignore. In some cases, the global economy connects organizations to aggressive regional actors. In other cases, a growing mandate draws the actor on to the international stage. Ignored, these threats enjoy the benefit of surprise, allowing them to extract significant losses on their victims, many of whom have never previously heard of the actor.

Appendix: Malware Used by APT37

Malware	Description	Detected as
CORALDECK	CORALDECK is an exfiltration tool that searches for specified files and exfiltrates them in password protected archives using hardcoded HTTP POST headers. CORALDECK has been observed dropping and using Winrar to exfiltrate data in password protected RAR files as well as WinImage and zip archives.	APT.InfoStealer.Win.CORALDECK FE_APT_InfoStealer_Win_CORALDECK_1
DOGCALL	DOGCALL is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex. DOGCALL was used to target South Korean Government and military organizations in March and April 2017. The malware is typically dropped using an HWP exploit in a lure document. The wiper tool, RUHAPPY, was found on some of the systems targeted by DOGCALL. While DOGCALL is primarily an espionage tool, RUHAPPY is a destructive wiper tool meant to render systems inoperable.	FE_APT_RAT_DOGCALL FE_APT_Backdoor_Win32_DOGCALL_1 APT.Backdoor.Win.DOGCALL
GELCAPSULE	GELCAPSULE is a downloader traditionally dropped or downloaded by an exploit document. GELCAPSULE has been observed downloading SLOWDRIFT to victim systems.	FE_APT_Downloader_Win32_GELCAPSULE_1
HAPPYWORK	HAPPYWORK is a malicious downloader that can download and execute a second-stage payload, collect system information, and beacon it to the command and control domains. The collected system information includes: computer name, user name, system manufacturer via registry, IsDebuggerPresent state, and execution path. In November 2016, HAPPYWORK targeted government and financial targets in South Korea.	FE_APT_Downloader_HAPPYWORK FE_APT_Exploit_HWP_Happy Downloader.APT.HAPPYWORK
KARAE	Karae backdoors are typically used as first-stage malware after an initial compromise. The backdoors can collect system information, upload and download files, and may be used to retrieve a second-stage payload. The malware uses public cloud-based storage providers for command and control. In March 2016, KARAE malware was distributed through torrent file-sharing websites for South Korean users. During this campaign, the malware used a YouTube video downloader application as a lure.	FE_APT_Backdoor_Karae_enc FE_APT_Backdoor_Karae Backdoor.APT.Karae

Malware	Description	Detected as
MILKDROP	MILKDROP is a launcher that sets a persistence registry key and launches a backdoor.	FE_Trojan_Win32_MILKDROP_1
POORAIM	POORAIM malware is designed with basic backdoor functionality and leverages AOL Instant Messenger for command and control communications. POORAIM includes the following capabilities: System information enumeration, File browsing, manipulation and exfiltration, Process enumeration, Screen capture, File execution, Exfiltration of browser favorites, and battery status. Exfiltrated data is sent via files over AIM. POORAIM has been involved in campaigns against South Korean media organizations and sites relating to North Korean refugees and defectors since early 2014. Compromised sites have acted as watering holes to deliver newer variants of POORAIM.	Backdoor.APT.POORAIM
RICECURRY	RICECURRY is a Javascript based profiler used to fingerprint a victim's web browser and deliver malicious code in return. Browser, operating system, and Adobe Flash version are detected by RICECURRY, which may be a modified version of PluginDetect.	Exploit.APT.RICECURRY
RUHAPPY	RUHAPPY is a destructive wiper tool seen on systems targeted by DOGCALL. It attempts to overwrite the MBR, causing the system not to boot. When victims' systems attempt to boot, the string "Are you Happy?" is displayed. The malware is believed to be tied to the developers of DOGCALL and HAPPYWORK based on similar PDB paths in all three.	FE_APT_Trojan_Win32_RUHAPPY_1
SHUTTERSPEED	SHUTTERSPEED is a backdoor that can collect system information, acquire screenshots, and download/execute an arbitrary executable. SHUTTERSPEED typically requires an argument at runtime in order to execute fully. Observed arguments used by SHUTTERSPEED include: 'help', 'console', and 'sample'. The spear phishing email messages contained documents exploiting RTF vulnerability CVE-2017-0199. Many of the compromised domains in the command and control infrastructure are linked to South Korean companies. Most of these domains host a fake webpage pertinent to targets.	FE_APT_Backdoor_SHUTTERSPEED APT.Backdoor.SHUTTERSPEED APT.Backdoor.SHUTTERSPEED

Malware	Description	Detected as
SLOWDRIFT	SLOWDRIFT is a launcher that communicates via cloud based infrastructure. It sends system information to the attacker command and control and then downloads and executes additional payloads. Lure documents distributing SLOWDRIFT were not tailored for specific victims, suggesting that TEMP.Reaper is attempting to widen its target base across multiple industries and in the private sector. SLOWDRIFT was seen being deployed against academic and strategic targets in South Korea using lure emails with documents leveraging the HWP exploit. Recent SLOWDRIFT samples were uncovered in June 2017 with lure documents pertaining to cyber crime prevention and news stories. These documents were last updated by the same actor who developed KARAE, POORAIM and ZUMKONG.	FE_APT_Downloader_Win_SLOWDRIFT_1 FE_APT_Downloader_Win_SLOWDRIFT_2 APT.Downloader.SLOWDRIFT
SOUNDWAVE	SOUNDWAVE is a windows based audio capturing utility. Via command line it accepts the -l switch (for listen probably), captures microphone input for 100 minutes, writing the data out to a log file in this format: C:\Temp\HncDownload\YYYYMMDDHHMMSS.log.	FE_APT_HackTool_Win32_SOUNDWAVE_1
ZUMKONG	ZUMKONG is a credential stealer capable of harvesting usernames and passwords stored by Internet Explorer and Chrome browsers. Stolen credentials are emailed to the attacker via HTTP POST requests to mail[.]zmail[.]ru.	FE_APT_Trojan_Zumkong Trojan.APT.Zumkong
WINERACK	WINERACK is backdoor whose primary features include user and host information gathering, process creation and termination, filesystem and registry manipulation, as well as the creation of a reverse shell that utilizes statically-linked Wine cmd.exe code to emulate Windows command prompt commands. Other capabilities include the enumeration of files, directories, services, active windows and processes.	FE_APT_Backdoor_WINERACK Backdoor.APT.WINERACK

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
877 FIREEYE (347.3393)
info@FireEye.com

www.FireEye.com