APT37 (Reaper): The Overlooked North Korean Actor

fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html

Threat Research

FireEye

Feb 20, 2018

2 mins read

Advanced Persistent Threats (APTs)

Threat Research

Malware

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).

Our analysis of APT37's recent activity reveals that the group's operations are expanding in scope and sophistication, with a toolset that includes access to zero-day vulnerabilities and wiper malware. 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.

Read our report, *APT37 (Reaper): The Overlooked North Korean Actor*, to learn more about our assessment that this threat actor is working on behalf of the North Korean government, as well as various other details about their operations:

- **Targeting:** Primarily South Korea – though also Japan, Vietnam and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.
- **Initial Infection Tactics:** Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyber espionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately.
- **Exploited Vulnerabilities:** Frequent exploitation of vulnerabilities in Hangul Word Processor (HWP), as well as Adobe Flash. The group has demonstrated access to zero-day vulnerabilities (CVE-2018-0802), and the ability to incorporate them into operations.
- **Command and Control Infrastructure:** Compromised servers, messaging platforms, and cloud service providers to avoid detection. The group has shown increasing sophistication by improving their operational security over time.
- **Malware:** A diverse suite of malware for initial intrusion and exfiltration. Along with custom malware used for espionage purposes, APT37 also has access to destructive malware.

More information on this threat actor is found in our report, *APT37 (Reaper): The Overlooked North Korean Actor*. You can also register for our upcoming webinar for additional insights into this group.

Download Now