# Attacks Leveraging Adobe Zero-Day (CVE-2018-4878) – Threat Attribution, Attack Scenario and Recommendations

fireeye.com/blog/threat-research/2018/02/attacks-leveraging-adobe-zero-day.html

## Threat Research Blog

February 03, 2018 | by FireEye
Vulnerability
0day
Zero-day
On Jan. 31, KISA (KrCERT) published an advisory about an Adobe Flash zero-day vulnerability (CVE-2018-4878) being exploited in the wild. On Feb. 1, Adobe issued an advisory confirming the vulnerability exists in Adobe Flash Player 28.0.0.137 and earlier versions, and that successful exploitation could potentially allow an attacker to take control of the affected system.

FireEye began investigating the vulnerability following the release of the initial advisory from KISA.

### Threat Attribution

We assess that the actors employing this latest Flash zero-day are a suspected North Korean group we track as TEMP.Reaper. We have observed TEMP.Reaper operators directly interacting with their command and control infrastructure from IP addresses assigned to the STAR-KP network in Pyongyang. The STAR-KP network is operated as a joint venture between the North Korean Government's Post and Telecommunications Corporation and Thailand-based Loxley Pacific. Historically, the majority of their targeting has been focused on the South Korean government, military, and defense industrial base; however, they have expanded to other international targets in the last year. They have taken interest in subject matter of direct importance to the Democratic People's Republic of Korea (DPRK) such as Korean unification efforts and North Korean defectors.

In the past year, FireEye iSIGHT Intelligence has discovered newly developed wiper malware being deployed by TEMP.Reaper, which we detect as RUHAPPY. While we have observed other suspected North Korean threat groups such as TEMP.Hermit employ wiper malware in disruptive attacks, we have not thus far observed TEMP.Reaper use their wiper malware actively against any targets.

## Attack Scenario

Analysis of the exploit chain is ongoing, but available information points to the Flash zero-day being distributed in a malicious document or spreadsheet with an embedded SWF file. Upon opening and successful exploitation, a decryption key for an encrypted embedded payload would be downloaded from compromised third party websites hosted in South Korea. Preliminary analysis indicates that the vulnerability was likely used to distribute the previously observed DOGCALL malware to South Korean victims.

## Recommendations

Adobe stated that it plans to release a fix for this issue the week of Feb. 5, 2018. Until then, we recommended that customers use extreme caution, especially when visiting South Korean sites, and avoid opening suspicious documents, especially Excel spreadsheets. Due to the publication of the vulnerability prior to patch availability, it is likely that additional criminal and nation state groups will attempt to exploit the vulnerability in the near term.

## FireEye Solutions Detections

FireEye Email Security, Endpoint Security with Exploit Guard enabled, and Network Security products will detect the malicious document natively. Email Security and Network Security customers who have enabled the riskware feature may see additional alerts based on suspicious content embedded in malicious documents. Customers can find more information in our FireEye Customer Communities post.

Previous Post
Next Post