ScarCruft APT Group Used Latest Flash Zero Day in Two Dozen Attacks

By Michael Mimoso

Published: 2016-06-17 · Archived: 2026-04-05 14:34:11 UTC

The ScarCruft APT gang has made use of a Flash zero day patched Thursday by Adobe to attack more than two dozen high-profile targets in Russia and Asia primarily.

Adobe on Thursday patched a zero-day vulnerability in Flash Player that has been used in targeted attacks carried out by a new APT group operating primarily against high-profile victims in Russia and Asia.

Researchers at Kaspersky Lab privately disclosed the flaw to Adobe after exploits against the zero-day were used in March by the ScarCruft APT gang in what Kaspersky Lab is calling Operation Daybreak.

Researchers said the group has a number of operations under way and that it has two Flash exploits and another against Microsoft's Internet Explorer at its disposal. Kaspersky speculates that this group could also be behind another zero-day, CVE-2016-0147, a vulnerability in Microsoft XML Core Services that was patched in April.

In a report from Kaspersky Lab, researchers said the vulnerability is in Flash code that parses ExecPolicy metadata. ScarCruft's exploit implements read/write operations at a particular address in memory that can allow for full remote code execution. Full details are explained in the Kaspersky Lab report published today.

The attack happens in stages starting with shellcode downloading and executing a malicious DLL that loads in Flash and also includes a technique designed to bypass antivirus detection using the Windows DDE component, or Dynamic Data Exchange, a protocol that facilitates data transfers between applications.

Kaspersky researchers said this part of the attack makes "clever" use of Windows DDE.

"The main idea here is that if you create a LNK to an executable or command, then use the ShowGroup method, the program will be executed," Kaspersky Lab said in its report. "This is an undocumented behavior in Microsoft Windows."

Kaspersky's research indicates there have been more than two dozen Operation Daybreak victims to date, including an Asian law enforcement agency, a large Asian trading company, an American mobile advertising company and individuals affiliated with the International Association of Athletics Federations (IAAF), some of which were compromised in the past few days.

Attacks start with spear-phishing emails that include a link to a website hosting an exploit kit associated with ScarCruft and used in other attacks. The exploit kit eventually redirects victims' browsers to a server in Poland controlled by the attackers.

“The ScarCruft APT group is a relatively new player and managed to stay under the radar for some time,” researchers wrote. “In general, their work is very professional and focused. Their tools and techniques are well above the average.”

Another set of attacks called Operation Erebus leverages another Flash exploit, CVE-2016-4117, and relies on watering hole attacks as a means of propagation. Watering hole attacks involved compromising a site frequented by the target and serving exploits to site visitors that redirects to malware, often spy tools.

Adobe has implemented a number of mitigations in Flash that defend against memory-based attacks in particular that also make zero days incrementally difficult. While Adobe and outside researchers continue to find and patch critical issues in Flash Player, publicly attacks against unknown Flash flaws are much less frequent.

“Nowadays, in-the-wild Flash Player exploits are becoming rare. This is because in most cases they need to be coupled with a Sandbox bypass exploit, which makes them rather tricky. Additionally, Adobe has been doing a great job at implementing new mitigations to make exploitation of Flash Player more and more difficult,” Kaspersky researchers wrote. “Nevertheless, resourceful threat actors such as ScarCruft will probably continue to deploy zero-day exploits against their high profile targets.”

Google Project Zero team researcher Natalie Silvanovich said that efforts by Adobe to introduce new exploit mitigations into the Flash Player code base have slowed down exploit development and made it more difficult for researchers looking for bugs.

During the Infiltrate Conference in Miami in April, Silvanovich said during a presentation that, for example, use-after-free bugs are more difficult to exploit and that other classes of vulnerabilities such as redefinition bugs may be going away. She added that information garnered from the Hacking Team data breach last summer was also important to her work. “The Hacking Team dump was an unprecedented source of information on how Flash exploits work in the wild,” she said during her talk.

Thursday’s Flash Player update patched 36 vulnerabilities in total including the zero day CVE-2016-4171. Desktop versions 21.0.0.242 and earlier on Windows and Mac machines are affected and users should upgrade to 22.0.0.192.

The majority of the vulnerabilities patched today are memory corruption flaws. The update also takes care of type-confusion, use-after-free, buffer overflow and directory search path vulnerabilities as well a same-origin policy bypass flaw that exposes machines to information disclosure attacks.
