CVE-2016-4171 – Adobe Flash Zero-day used in targeted attacks

securelist.com/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/75082/

Incidents

Incidents

14 Jun 2016

minute read

Authors

 Costin Raiu

Earlier today, Adobe published the security advisory APSA16-03, which describes a critical vulnerability in Adobe Flash Player version 21.0.0.242 and earlier versions for Windows, Macintosh, Linux, and Chrome OS:

> Adobe is aware of a report that an exploit for CVE-2016-4171 exists in the wild, and is being used in limited, targeted attacks. Adobe will address this vulnerability in our monthly security update, which will be available as early as June 16. For the latest information, users may monitor the Adobe Product Security Incident Response Team blog.
>
> **Severity ratings**
>
> Adobe categorizes this as a critical vulnerability.
>
> **Acknowledgments**
>
> Adobe would like to thank Anton Ivanov and Costin Raiu of Kaspersky for reporting CVE-2016-4171 and for working with Adobe to help protect our customers.

A few of months ago, we deployed a new set of technologies into our products designed to identify and block zero day attacks. These technologies already proved its effectiveness earlier this year, when they caught an Adobe Flash zero day exploit, CVE-2016-1010. Earlier this month, we caught another zero-day Adobe Flash Player exploit deployed in targeted attacks.

We believe these attacks are launched by an APT Group we call “ScarCruft”.

ScarCruft is a relatively new APT group; victims have been observed in several countries, including Russia, Nepal, South Korea, China, India, Kuwait and Romania. The group has several ongoing operations utilizing multiple exploits — two for Adobe Flash and one for Microsoft Internet Explorer.

Currently, the group is engaged in two major operations: **Operation Daybreak** and **Operation Erebus**. The first of them, Operation Daybreak, appears to have been launched by ScarCruft in March 2016 and employs a previously unknown (0-day) Adobe Flash Player exploit, focusing on high profile victims. The other one, “Operation Erebus” employs an older exploit, for CVE-2016-4117 and leverages watering holes. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April.

We will publish more details about the attack once Adobe patches the vulnerability, which should be on June 16. Until then, we confirm that Microsoft EMET is effective at mitigating the attacks. Additionally, our products detect and block the exploit, as well as the malware used by the ScarCruft APT threat actor.

** More information about the ScarCruft APT and Operation Daybreak is available to customers of Kaspersky Intelligence Services. Contact: intelreports@kaspersky.com*

- Adobe Flash
- APT
- Vulnerabilities
- Zero-day vulnerabilities

Authors

 Costin Raiu

CVE-2016-4171 – Adobe Flash Zero-day used in targeted attacks

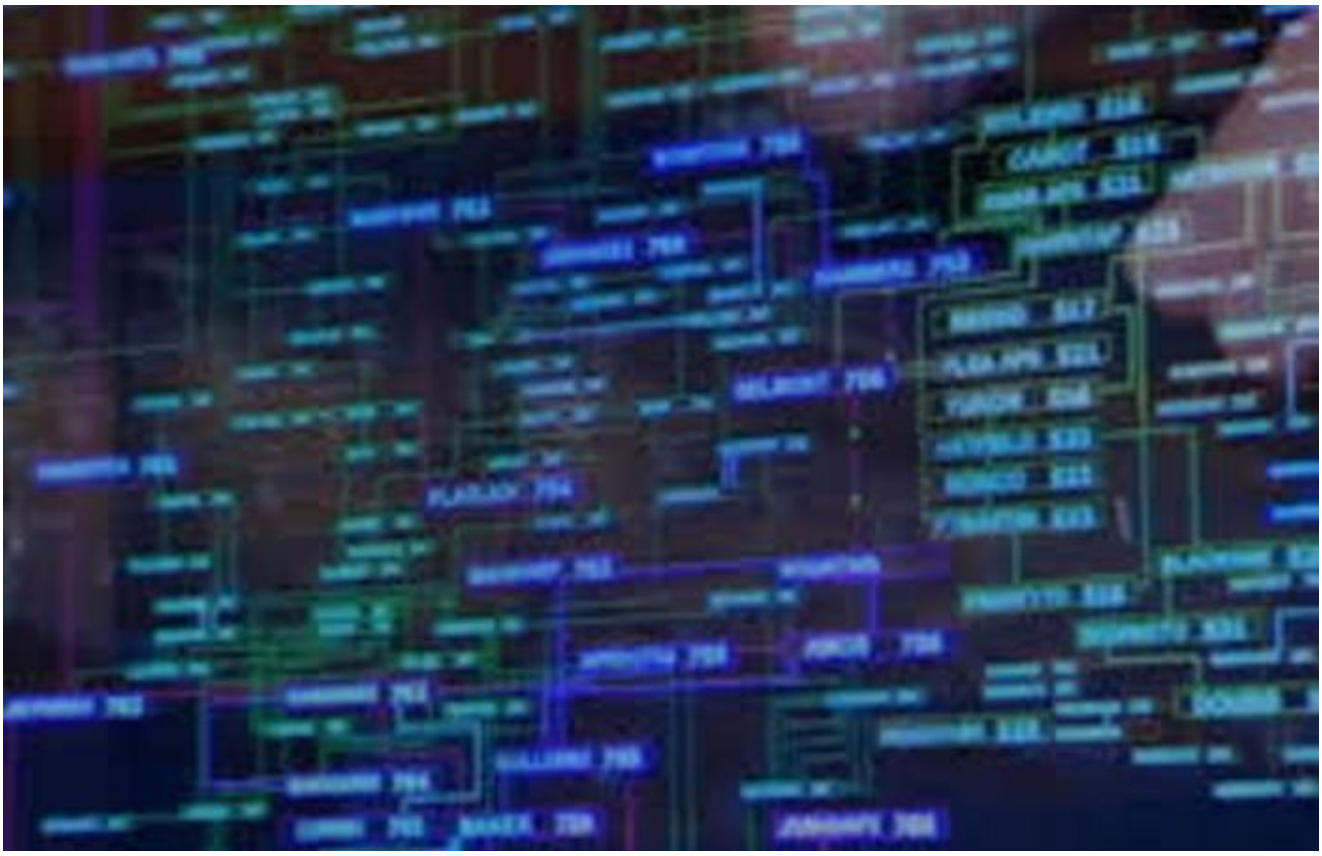
---

GReAT webinars

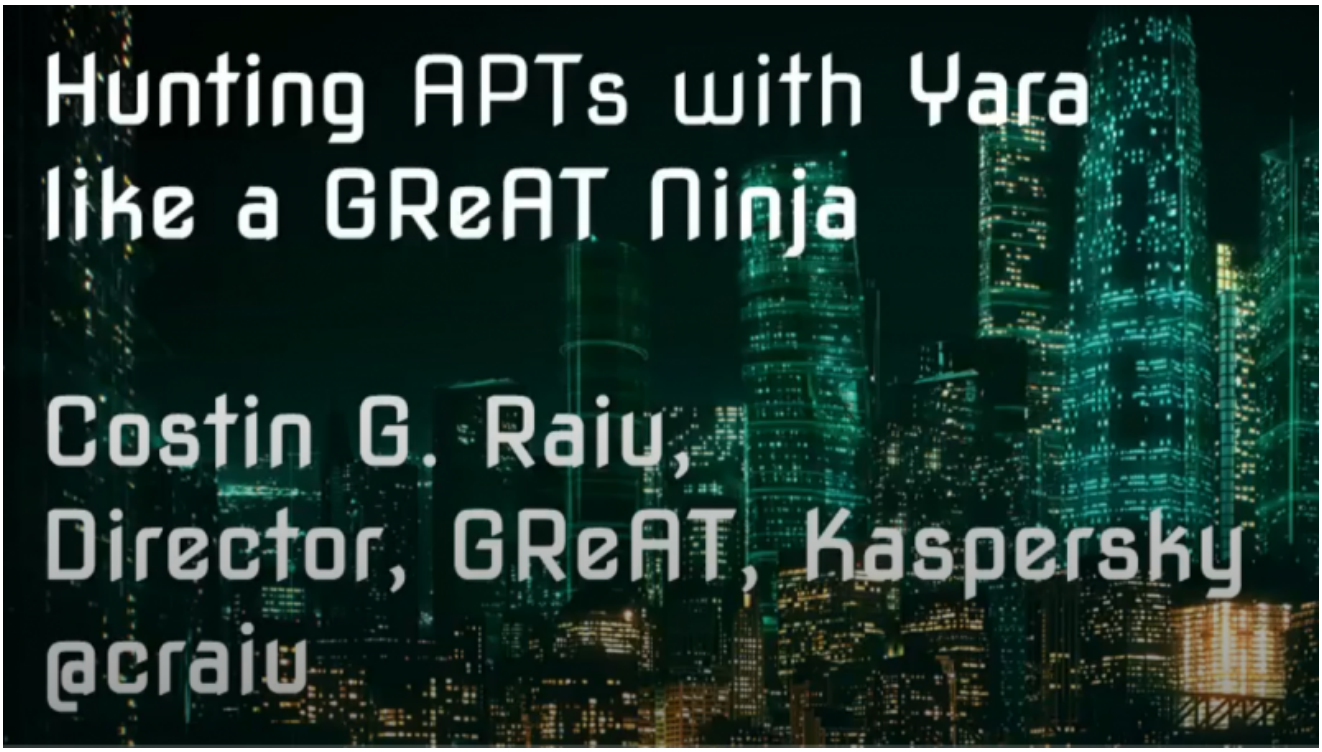
13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors



Looking at Big Threats Using Code Similarity. Part 1



YARA webinar follow up

Hunting APTs with YARA

Penquin's Moonlit Maze

From Shamoon to StoneDrill

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

-
-
-