Virus Bulletin 2019: Japanese Attacks Highlight Savvy APT Strategy

Author:
Tara Seals

October 2, 2019 / 12:47 pm

2 minute read

Write a comment

Share this article:

Multiyear campaigns stretching back to at least 2014 have been seen using zero-days in region-specific software.

LONDON — Three separate, multi-year APT campaigns targeting region-specific software showcase a savvy technique of leveraging zero-day vulnerabilities in niche software in order to infect victims with malware.

According to researchers at JPCERT in Japan, speaking at Virus Bulletin 2019, both the APT17 and Bronze Butler threat groups have carried out ongoing campaigns that use the same techniques, swapping out exploits as new exploits are developed. The targets of the attacks are generally Japanese government agencies and vertical organizations, including education organizations, researchers said, with the most recent malicious activity seen in April 2019.

According to JPCERT researchers Tomoaki Tani and Shusei Tomonaga, the regional software targeted by the APTs includes Sanshiro (a spreadsheet application similar to Microsoft Excel, which was discontinued in 2014 but still used across Japan); Ichitaro (a word processing, software similar to Microsoft Word); and SkySea Client View (an enterprise asset-management tool).

When it comes to Sanshiro, major campaigns from APT17 leveraged a zero-day exploit for an arbitrary code execution vulnerability (CVE-2014-0810), spread in malicious documents attached to spearphishing emails. It began its routine when the user opened the software; and the endgame was the delivery of the PlugX remote access trojan (RAT).

"This exploit was shared in several campaigns, and perhaps the actor was the same in all of them," said Tani, speaking in a Wednesday session at Virus Bulletin 2019. "Further analysis showed that PlugX was used in other attacks, with each sample resolving to the same command-and-control server address."

A similar effort targeted Ichitaro, which was used in a multi-year campaign starting in 2014 dubbed Blue Termite. It affected more than 100 organizations across Japan; here, another zero-day code-execution exploit (CVE-2014-7247) was used in spearphishing campaigns to spread a triumvirate of malware: PlugX and two bots, Emdivi and Agtid. The bots can upload and download files from the victim's computer.

JPCERT also observed attacks likely carried out by an APT called Bronze Butler, making use of the SkySea Client View software, which is an asset-management software. It contains a vulnerability (CVE-2016-7836) that was exploited as a zero-day campaign in 2016 – and it was seen continuing through February 2019. It was used to execute the NodeRAT multiplatform backdoor malware, which is written in JavaScript and runs on Node.js; and the Wali downloader application.

This attack is linked, researchers suspect, to an April 2019 effort targeting a vulnerability in the Virus Buster Corporate Edition from Trend Micro, which is popular in Japan.

In all cases, the campaigns were aimed at infiltrating target networks, moving laterally and stealing data, in classic APT fashion.

The takeaway from the research is that APT groups are actively targeting niche attack surfaces in hopes of flying under the radar of defenders. While these particular attacks occurred in Japan, the same approach would prove effective elsewhere, according to Tani.

"Targeted attacks against Japanese organizations exploited three different vulnerabilities in software that's used only in Japan," Tani concluded. "Nonetheless, these APT groups investigated this software and leveraged them for attacks. Unlike more popular software, it is often the case that countermeasures against vulnerabilities in such regional attacks are not well-prepared. Attackers understand this and aim for such weak points."

What are the top cyber security issues associated with privileged account access and credential governance? Experts from Thycotic will discuss during our upcoming free Threatpost webinar, "Hackers and Security Pros: Where They Agree & Disagree When It

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 15, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

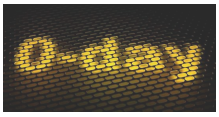
The Case for Cyber-Risk Prospectuses
December 24, 2019 1

Write a comment

Share this article:

Government Hacks Vulnerabilities

SUGGESTED ARTICLES



Microsoft Zero-Day Actively Exploited, Patch Forthcoming

CVE-2020-0674 is a critical flaw for most Internet Explorer versions, allowing remote code execution and complete takeover.

January 21, 2020 4

News Wrap: Hotel Robot Hacks, FTC Stalkerware Crackdown

From hacking hotel room robots to crackdowns on stalkerware apps, Threatpost editors break down this week's top news stories.

October 25, 2019

Bedside Hotel Robot Hacked to Stream In-Room Video

An unsecured NFC tag opens a door to trivial exploitation of robots inside Japanese hotels.

October 23, 2019

DISCUSSION

Leave A Comment

Write a reply...

Your name Your email

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

Send Comment

I'm not a robot reCAPTCHA Privacy - Terms

This site uses Akismet to reduce spam. Learn how your comment data is processed.