APT Exploits Microsoft Zerologon Bug: Targets Japanese Companies

By Elizabeth Montalbano

Published: 2020-11-19 · Archived: 2026-04-05 13:09:24 UTC

Threat actors mount year-long campaign of espionage, exfiltrating data, stealing credentials and installing backdoors on victims' networks.

China-backed APT Cicada joins the list of threat actors leveraging the Microsoft Zerologon bug to stage attacks against their targets. In this case, victims are large and well-known Japanese organizations and their subsidiaries, including locations in the United States.

Researchers observed a "large-scale attack campaign targeting multiple Japanese companies" across 17 regions and various industry sectors that engaged in a range of malicious activity, such as credential theft, data exfiltration and network reconnaissance. Attackers also installed the QuasarRAT open-source backdoor and novel Backdoor.Hartip tool to continue surveillance on victims' systems, according a recent report.

Due to some notable hallmark activity, the attacks appear to be the work of Cicada (aka APT10, Stone Panda, Cloud Hopper), a state-sponsored threat group which has links to the Chinese government, researchers at Broadcom's Symantec said.

"This campaign has been ongoing since at least mid-October 2019, right up to the beginning of October 2020, with the attack group active on the networks of some of its victims for close to a year," researchers wrote in a report posted online. "The campaign is very wide-ranging, with victims in a large number of regions worldwide."

A number of threat patterns and techniques observed in the campaign that link the activity to Cicada, including a third-stage DLL with an export named "F**kYouAnti;" a third-stage DLL using CppHostCLR technique to inject and execute the .NET loader assembly; .NET Loader obfuscation using ConfuserEx v1.0.0; and the delivery of QuasarRAT as the final payload.

Researchers observed attackers leveraging Zerologon, or CVE-2020-1472, a Microsoft zero-day elevation-of-privilege vulnerability first disclosed and patched on Aug. 11. The flaw—which stems from the Netlogon Remote Protocol available on Windows domain controllers–allows attackers to spoof a domain controller account and then use it to steal domain credentials, take over the domain and completely compromise all Active Directory identity services.

"Among machines compromised during this attack campaign were domain controllers and file servers, and there was evidence of files being exfiltrated from some of the compromised machines," researchers observed.

Zerologon has been a thorn in the side of Microsoft for some time, with multiple APTs and other attackers taking advantage of unpatched systems. Last month Microsoft warned that the Iranian group MERCURY APT has been actively exploiting the flaw, while the Ryuk ransomware gang used it to deliver a lightning-fast attack that moved from initial phish to full domain-wide encryption in just five hours.

Given the length of the campaign discovered, Cicada may well be one of the earliest APT groups to take advantage of Zerologon. The group is known for attacking targets in Japan as well as MSPs with living-off-the-land tools and custom malware. In the latter category, the latest campaign uses Backdoor.Hartip, which researchers said is a brand new tool for the group.

In addition to Zerologon, attackers also extensively used DLL side-loading in the campaign, a common tactic of APT groups that "occurs when attackers are able to replace a legitimate library with a malicious one, allowing them to load malware into legitimate processes," researchers said. In fact, suspicious activity surrounding DLL side-loading is what tipped Symantec researchers off to campaign when it triggered an alert in Symantec's Cloud Analytics tool, they said.

"Attackers use DLL side-loading to try and hide their activity by making it look legitimate, and it also helps them avoid detection by security software," according to the report.

Other tools attackers leveraged in the campaign included: RAR archiving, which can transfer files to staging servers before exfiltration; WMIExec, used for lateral movement and to execute commands remotely; Certutil, a command-line utility that can be exploited to decode information, download files and install browser root certificates; and PowerShell, an environment in the Windows OS that's often abused by threat actors. The campaign also used legitimate cloud file-hosting service for exfiltration, researchers said.
