Waterbear malware used in attack wave against government agencies

zdnet.com/article/waterbear-malware-used-in-attack-wave-against-government-agencies/

Home Innovation Security

The loader has been launched against a number of Taiwanese government entities.

Written by Charlie Osborne, Contributor on Oct. 8, 2020

-
-
-
-
-

Researchers have spotted a fresh Waterbear campaign in which Taiwanese government agencies have been targeted in sophisticated attacks.

Security

- My Instagram account was hacked, and two-factor authentication didn't help
- The 5 best browsers for privacy: Secure web browsing
- Stop doing these 10 things that let hackers in, says FBI and NSA
- What is a cybersecurity degree?
- How to delete yourself from search results and hide your identity online

According to CyCraft researchers, the attacks took place in April 2020, but in an interesting twist, the threat group responsible leveraged malware already present on compromised servers -- due to past attacks -- in order to deploy malware.

Waterbear has previously been associated with BlackTech, an advanced cyberattack group that generally attacks technology companies and government entities across Taiwan, Japan, and Hong Kong.

Trend Micro researchers say the modular malware is primarily "used for lateral movement, decrypting and triggering payloads with its loader component." Last year, Waterbear captured interest in the cybersecurity industry after implementing API hooking to hide its activities by abusing security products.

See also: Black Hat: Hackers are using skeleton keys to target chip vendors

In the latest wave, CyCraft says a vulnerability was exploited in a common and trusted data loss prevention (DLP) tool in order to load Waterbear. The job was made easier as malware leftover from previous attacks on the same targets had not been fully eradicated.

The attackers have been tracked in attempts to use stolen credentials to access a target network. In some examples, endpoints were still compromised from past attacks, and this was leveraged to access the victim's internal network and covertly establish a connection to the group's command-and-control (C2) server.

A vulnerability in the DLP tool was then used to perform DLL hijacking. As the software failed to verify the integrity of DLLs it was loading, the malicious file was launched with a high level of privilege.

This DLL then injected shellcode into various Windows system services, allowing the Waterbear loader to deploy additional malicious packages.

Another interesting facet of the loader is the "resurrection" of a decade-old antivirus evasion technique, according to the researchers.

Known as "Heaven's Gate," the misdirection technique is used to trick Microsoft Windows operating systems into executing 64-bit code, even when declared as a 32-bit process. This, in turn, can be used to bypass security engines and to inject shellcode.

CNET: Privacy push could banish some annoying website popups and online tracking

"Just as 64-bit and 32-bit programs are quite different, so are analysis mechanisms. Malware equipped with Heaven's Gate contains both 64-bit and 32-bit parts," the team says. "Therefore, some monitor/analysis systems will only apply 32-bit analysis and will fail the 64-bit part; thus, this approach will break some monitor/analysis mechanisms."

To scupper analysis attempts, the Waterbear loader will also use RC4 encryption on its main payload and "pad contents [and memory] from Kernel32.dll in front of and behind shellcode." The size of the malware's binary was also inflated in an attempt to bypass file-based scanners.

TechRepublic: Cybersecurity Awareness Month: How to protect your kids from identity theft

In August, the CyCraft team told virtual attendees of Black Hat USA that a Chinese advanced persistent threat (APT) group has been striking the systems of Taiwanese chip manufacturers.

Sensitive corporate information and property including semiconductor designs, source code, and software development kits (SDKs) have been stolen in "precise and well-coordinated attacks" over 2018 and 2019. At least seven separate vendors have fallen prey to the group.

The biggest hacks, data breaches of 2020 (so far)

Previous and related coverage

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0