Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries

fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Breadcrumb

Threat Research

FireEye

Mar 16, 2018

5 mins read

Malware

Intrusions Focus on the Engineering and Maritime Sector

Since early 2018, FireEye (including our FireEye as a Service (FaaS), Mandiant Consulting, and iSIGHT Intelligence teams) has been tracking an ongoing wave of intrusions targeting engineering and maritime entities, especially those connected to South China Sea issues. The campaign is linked to a group of suspected Chinese cyber espionage actors we have tracked since 2013, dubbed TEMP.Periscope. The group has also been reported as "Leviathan" by other security firms.

The current campaign is a sharp escalation of detected activity since summer 2017. Like multiple other Chinese cyber espionage actors, TEMP.Periscope has recently re-emerged and has been observed conducting operations with a revised toolkit. Known targets of this group have been involved in the maritime industry, as well as engineering-focused entities, and include research institutes, academic organizations, and private firms in the United States. FireEye products have robust detection for the malware used in this campaign.

TEMP.Periscope Background

Active since at least 2013, TEMP.Periscope has primarily focused on maritime-related targets across multiple verticals, including engineering firms, shipping and transportation, manufacturing, defense, government offices, and research universities. However, the group has also targeted professional/consulting services, high-tech industry, healthcare, and media/publishing. Identified victims were mostly found in the United States, although organizations in Europe and at least one in Hong Kong have also been affected. TEMP.Periscope overlaps in targeting, as well as tactics, techniques, and procedures (TTPs), with TEMP.Jumper, a group that also overlaps significantly with public reporting on “NanHaiShu.”

TTPs and Malware Used

In their recent spike in activity, TEMP.Periscope has leveraged a relatively large library of malware shared with multiple other suspected Chinese groups. These tools include:

- AIRBREAK: a JavaScript-based backdoor also reported as “Orz” that retrieves commands from hidden strings in compromised webpages and actor controlled profiles on legitimate services.
- BADFLICK: a backdoor that is capable of modifying the file system, generating a reverse shell, and modifying its command and control (C2) configuration.
- PHOTO: a DLL backdoor also reported publicly as “Derusbi”, capable of obtaining directory, file, and drive listing; creating a reverse shell; performing screen captures; recording video and audio; listing, terminating, and creating processes; enumerating, starting, and deleting registry keys and values; logging keystrokes, returning usernames and passwords from protected storage; and renaming, deleting, copying, moving, reading, and writing to files.
- HOMEFRY: a 64-bit Windows password dumper/cracker that has previously been used in conjunction with AIRBREAK and BADFLICK backdoors. Some strings are obfuscated with XOR x56. The malware accepts up to two arguments at the command line: one to display cleartext credentials for each login session, and a second to display cleartext credentials, NTLM hashes, and malware version for each login session.
- LUNCHMONEY: an uploader that can exfiltrate files to Dropbox.
- MURKYTOP: a command-line reconnaissance tool. It can be used to execute files as a different user, move, and delete files locally, schedule remote AT jobs, perform host discovery on connected networks, scan for open ports on hosts in a connected network, and retrieve information about the OS, users, groups, and shares on remote hosts.
- China Chopper: a simple code injection webshell that executes Microsoft .NET code within HTTP POST commands. This allows the shell to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and any other action allowed by the .NET runtime.

The following are tools that TEMP.Periscope has leveraged in past operations and could use again, though these have not been seen in the current wave of activity:

- Beacon: a backdoor that is commercially available as part of the Cobalt Strike software platform, commonly used for pen-testing network environments. The malware supports several capabilities, such as injecting and executing arbitrary code, uploading and downloading files, and executing shell commands.
- BLACKCOFFEE: a backdoor that obfuscates its communications as normal traffic to legitimate websites such as Github and Microsoft's Technet portal. Used by APT17 and other Chinese cyber espionage operators.

Additional identifying TTPs include:

- Spear phishing, including the use of probably compromised email accounts.
- Lure documents using CVE-2017-11882 to drop malware.
- Stolen code signing certificates used to sign malware.
- Use of bitsadmin.exe to download additional tools.
- Use of PowerShell to download additional tools.
- Using C:\Windows\Debug and C:\Perflogs as staging directories.
- Leveraging Hyperhost VPS and Proton VPN exit nodes to access webshells on internet-facing systems.
- Using Windows Management Instrumentation (WMI) for persistence.
- Using Windows Shortcut files (.lnk) in the Startup folder that invoke the Windows Scripting Host (wscript.exe) to execute a Jscript backdoor for persistence.
- Receiving C2 instructions from user profiles created by the adversary on legitimate websites/forums such as Github and Microsoft's TechNet portal.

Implications

The current wave of identified intrusions is consistent with TEMP.Periscope and likely reflects a concerted effort to target sectors that may yield information that could provide an economic advantage, research and development data, intellectual property, or an edge in commercial negotiations.

As we continue to investigate this activity, we may identify additional data leading to greater analytical confidence linking the operation to TEMP.Periscope or other known threat actors, as well as previously unknown campaigns.

Indicators

File	*Hash*	*Description*
x.js	3fefa55daeb167931975c22df3eca20a	HOMEFRY, a 64-bit Windows password dumper/cracker
mt.exe	40528e368d323db0ac5c3f5e1efe4889	MURKYTOP, a command-line reconnaissance tool
com4.js	a68bf5fce22e7f1d6f999b7a580ae477	AIRBREAK, a JavaScript-based backdoor which retrieves commands from hidden strings in compromised webpages

Historical Indicators

File	*Hash*	*Description*
green.ddd	3eb6f85ac046a96204096ab65bbd3e7e	AIRBREAK, a JavaScript-based backdoor which retrieves commands from hidden strings in compromised webpages
BGij	6e843ef4856336fe3ef4ed27a4c792b1	Beacon, a commercially available backdoor
msresamn.ttf	a9e7539c1ebe857bae6efceefaa9dd16	PHOTO, also reported as Derusbi
1024-aa6a121f98330df2edee6c4391df21ff43a33604	bd9e4c82bf12c4e7a58221fc52fed705	BADFLICK, backdoor that is capable of modifying the file system, generating a reverse shell, and modifying its command-and-control configuration