TEMP.Periscope cyber espionage group targets Engineering and Maritime Industries

By Frank Crast / March 20, 2018 / Cybercrime, Cybersecurity Attacks / Cyberesionage, FireEye, Leviathan, South China, TEMP.Periscope, Windows, WMI

A suspected Chinese-linked cyber espionage campaign dubbed **Temp.Periscope** has been targeting engineering and maritime industries. FireEye has observed a spike in the campaign activity since early 2018 and has tracked the activity since 2013.

According to FireEye, the bad actors have sharply escalated attacks this year on engineering and maritime industries connected to South China issues. The group also goes by name "**Leviathan**" as identified by other security firms.

Temp.Periscope uses a revised toolkit with a relatively large library of malware shared with multiple other suspected Chinese groups. A number of malicious tools have been used to include: AIRBREAK, BADFLICK, PHOTO, HOMEFRY, LUNCHMONEY, MURKYTOP and China Chopper.

A few of the tactics, techniques, and procedures (TTPs) include targeted spear phishing campaigns that use compromised emails accounts as well as exploitation of an MS Office memory corruption vulnerability (CVE-2017-

Search...

Categories
Select Category

Archives
Select Month

Most Recent Posts
WinWAR and Openfire vulnerabilities exploited in the wild
August 26, 2023
Microsoft Visual Studio, .NET

11882) to drop malware on target systems. The vulnerability was patched last November.

The campaign also takes advantage of bitsadmin.exe and Powershell tools to download additional malicious tools, as well as use of Windows Management Instrumentation (WMI) for persistence.

The current TEMP.Periscope activity "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," FireEye said in the report.

← Previous Post

Next Post →

vulnerability (CVE-2023-38180) under attack in the wild

Top 12 Most Routinely Exploited vulnerabilities in 2022 August 18, 2023

Microsoft August 2023 Security Updates Fixes 74 Vulnerabilities (6 Critical severity) August 9, 2023

Apple patches zero-day vulnerabilities in iOS 16.6, macOS Ventura 13.5, and other products July 26, 2023

Critical MOVEit vulnerabilities exploited in the wild July 16, 2023

Microsoft July 2023 Security Updates Fixes 132 Vulnerabilities (9 Critical, 6 zero-days) July 13, 2023

Mozilla Releases Firefox 115 With Fixes For 3 High Severity Vulnerabilities July 9, 2023

Apple patches zero-day vulnerabilities in iOS 16.5.1, macOS Ventura 13.4.1, and other products June 22, 2023