H E A D Q U A R T E R S
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

Ghost Emperor hacking group uses Demodex rootkit to attack Asia

A previously unknown but highly skilled cyberespionage group is using sophisticated malware to attack government and private entities in South East Asia through a long-running campaign that targets systems running the latest versions of Microsoft's Windows 10.

The hacking group, dubbed *GhostEmperor* uses a multi-stage malware framework designed to give the attackers remote control over the targeted servers. At the same time, they leverage a rootkit, named *Demodex*, as a backdoor into the servers.

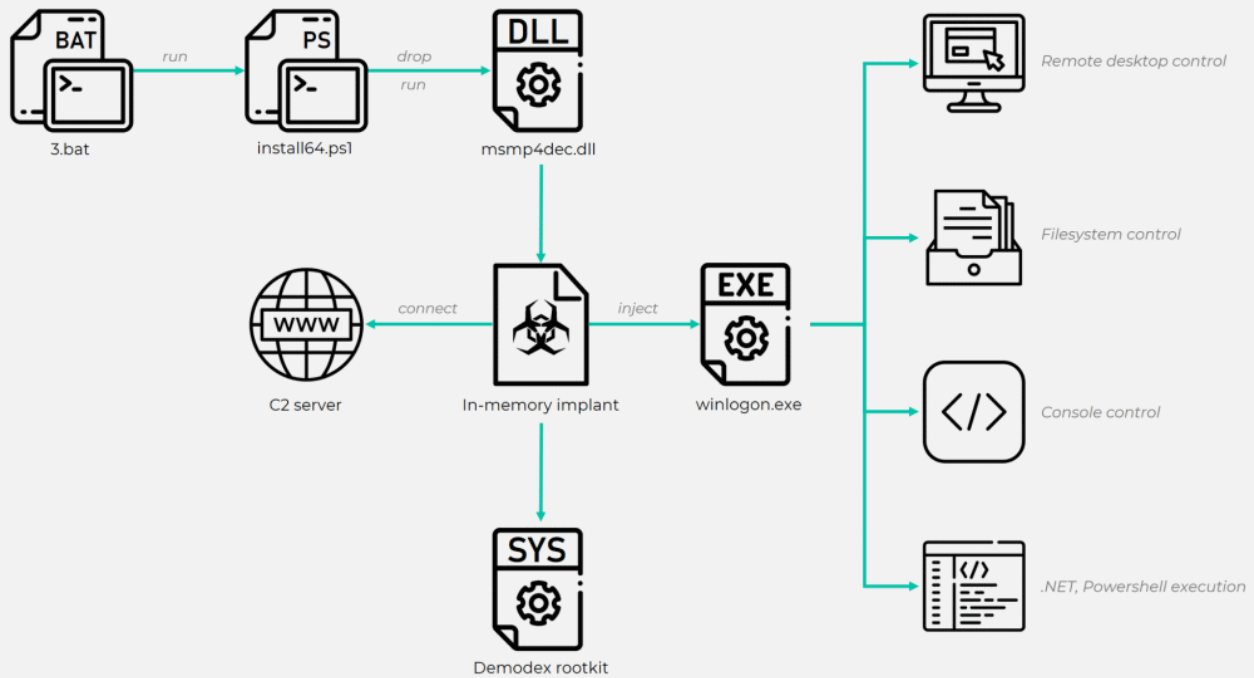
This rootkit's primary goal is to hide malware artifacts (including files, registry keys, and network traffic) to evade detection by both forensic investigators and security products.

According to Kaspersky researchers, they have surmised that the toolset has been in use since at least July 2020

Attack Vectors

The entry point for the hacks were public-facing servers. Kaspersky believes the group used exploits for *Apache*, *Oracle*, *Microsoft Exchange servers*, and the *ProxyLogon* to breach a target's perimeter network and then pivot to more sensitive systems inside the victim's network.

According to a technical report [PDF] released, *GhostEmperor* used an assortment of different scripts and tools to deploy backdoors inside a victim's network.



GhostEmperor infection chain (Kaspersky)

The *Demodex* rootkit is used to hide the malware's artifacts from investigators and security products. It includes an undocumented loading scheme involving the kernel mode component of an open-source project named *Cheat Engine* - a memory scanner and debugger that has been used to help users evade detection, which bypasses the *Windows PatchGuard* security feature.

Researchers said the rootkit was extremely advanced and allowed the group to maintain access to the victim's device even after OS reinstalls and even on systems running recent versions of the Windows 10 OS. It was said that the advanced toolset is unique and Kaspersky researchers see no similarity to already known threat actors.

Skilled hacking group with a focus on high-profile targets

GhostEmperor operators showed that they are "accomplished in their craft" and with a significant set of skills highlighted through the use of both sophisticated and uncommon anti-analysis and anti-forensic techniques.

While the vast majority of their attacks were focused on telecom firms and government organizations from South East Asia (e.g., Malaysia, Thailand, Vietnam, Indonesia), the researchers also observed targeting of other geopolitical areas, including countries like Egypt, Ethiopia, and Afghanistan.

"We observed that the underlying actor managed to remain under the radar for months, all the while demonstrating a finesse when it came to developing the malicious toolkit, a profound understanding of an investigator's mindset and the ability to counter forensic analysis in various ways," Kaspersky concluded.

The attackers conducted the required level of research to make the rootkit fully functional on Windows 10, allowing it to load through documented features of a third-party signed and benign driver.

However, the rootkit still needs to be taken into account as a TTP during investigations and that advanced threat actors, such as the one behind *GhostEmperor*, are willing to continue making use of them in future campaigns.

It was also determined that the campaign is being run by an unknown Chinese-speaking threat actor because of the use of open-source tools like *Ladon* and *Mimikat_ssp*, which they said are popular with cybercriminals from the region. There also were other indicators, including version information found within the resource section of second-stage loader binaries that included a legal trademark field with a Chinese character.

Mitigation

Given that the common entry points were public-facing servers with known vulnerabilities, organizations should make sure to undergo inventories of all public-facing assets as often as possible and ensure they're patched.

Organizations should also audit their configured services and monitor event logs for the creation and modification of services to detect the creation of the service loading the legitimate – but unexpected – Cheat Engine driver, which is pivotal to the infection chain.

References:

https://www.esecurityplanet.com/threats/chinese-attackers-use-new-rootkit-against-windows-10/

https://thehackernews.com/2021/10/chinese-hackers-used-new-rootkit-to-spy.html

https://www.bleepingcomputer.com/news/security/ghostemperor-hackers-use-new-windows-10-rootkit-in-attacks/

https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/30094337/GhostEmperor_technical-details_PDF_eng.pdf