Chinese APT Bronze President Mounts Spy Campaign on Russian Military

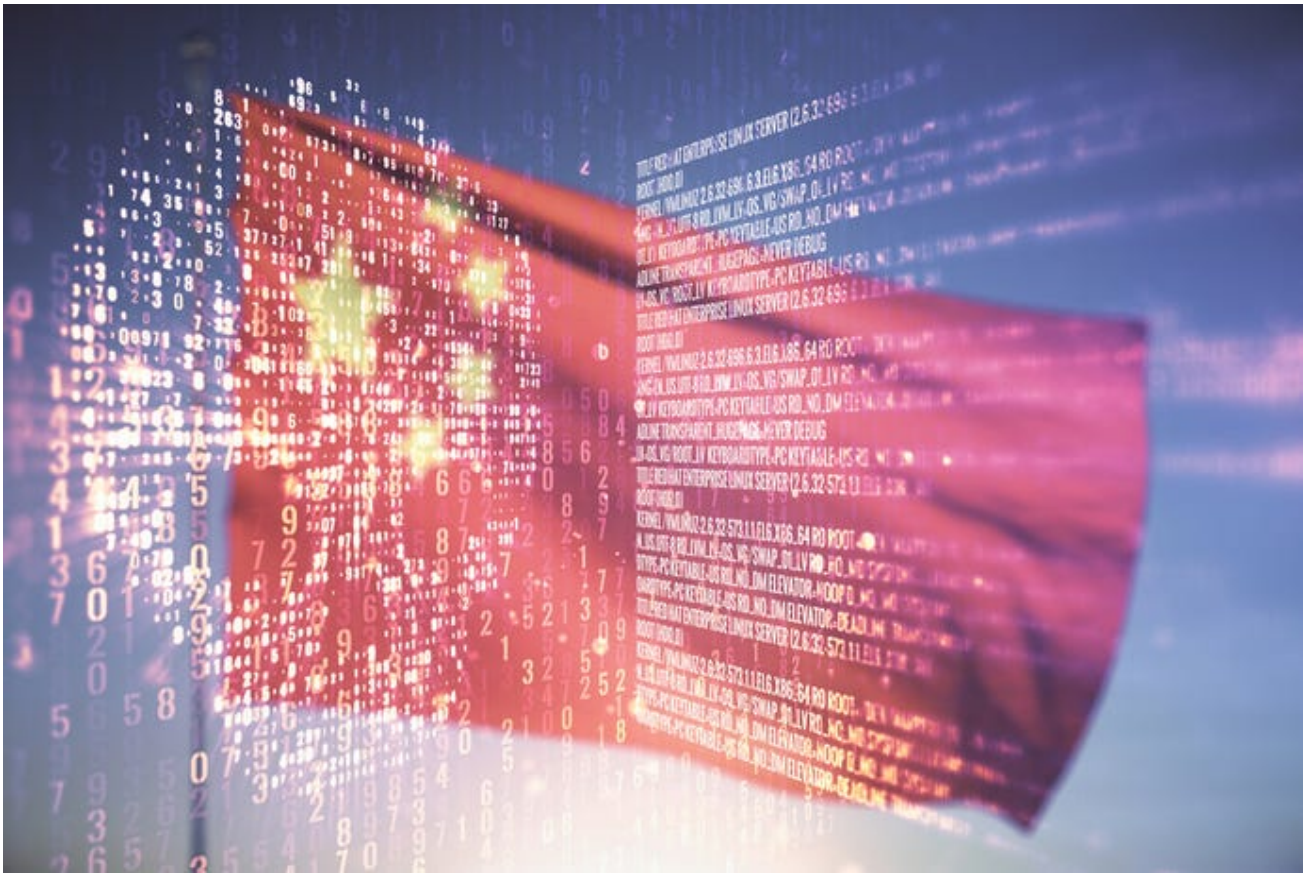
darkreading.com/threat-intelligence/chinese-apt-bronze-president-spy-campaign-russian-military

Jai Vijayan April 27, 2022

Threat Intelligence
4 MIN READ

NEWS
The war in Ukraine appears to have triggered a change in mission for the APT known as Bronze President (aka Mustang Panda).

Jai Vijayan
Contributing Writer, Dark Reading
April 27, 2022



Source: Pixels Hunter via Shutterstock

China's tacit support for Russia's war in Ukraine apparently doesn't preclude likely China-backed cyber actors from mounting espionage campaigns on the Russian military.

Researchers from Secureworks' Counter Threat Unit this week said they recently discovered malware that suggests the advanced persistent threat (APT) known as Bronze President (aka Mustang Panda) is now targeting Russian military personnel and officials. The security vendor described the effort as an example of how political changes can push countries into new territory for surreptitious information-gathering efforts, even against friends and allies.

Cyberespionage Campaign Delivers PlugX

According to the report, the heavily obfuscated malicious executable being used in the campaign is designed to appear as a Russian-language PDF document pertaining to Russia's 56th Blagoveshchenskiy Red Banner Border Guard Detachment (which is deployed near Russia's border with China). The file is designed so that default Windows settings do not display its .exe extension, Secureworks said.

Secureworks also explained that the executable file displays a decoy document written in English, though the filename itself is in Russian. The document appears to be legitimate and contains data pertaining to asylum applications and migratory pressure in the three countries that border Belarus — Poland, Lithuania, and Latvia. The content also includes commentary on European Union sanctions against Belarus for its role in the war in Ukraine.

When executed, the file downloads three additional files from a staging server. One of them is a legitimate signed file from Global Graphics Software, a UK-based firm. The file uses DLL search-order hijacking to import an updated version of PlugX, a remote-access Trojan (RAT) that has been previously associated with Bronze President.

"DLL search-order hijacking has been around for years," says Mike McLellan, director of intelligence at Secureworks. "It's a well-known technique by threat actors in which they maliciously use a legitimate executable file, often from a well-known vendor, together with a malicious library file (DLL), to load and execute an encrypted malware payload."

Threat actors use the technique because it ensures that the malicious payload file on a compromised system is never sitting around on disk in a manner that scanners and anti-malware can detect.

"This technique has been a staple of several China-nexus threat groups for many years," McLellan says.

As part of the attack chain, the threat actors have also included a ping command that adds a significant delay before executing the legitimate signed file, Secureworks said — a generic evasion technique to introduce a time lag while files are downloaded to the victim.

The staging server that Secureworks observed the threat actor using in the current campaign hosts a domain that Proofpoint earlier this year linked to a PlugX campaign against diplomatic entities in Europe. The security vendor determined that campaign to be

motivated by matters related to the war in Ukraine as well. The same domain has also been linked to Bronze President attacks in 2020 that Secureworks observed against the Vatican.

A New Set of Victims for Bronze Panda

Bronze President is a threat group that has been active since at least 2018, according to the researchers. Secureworks and others have assessed the group as being China-based and likely sponsored by — or operating with the knowledge of — the Chinese government. The group has been associated with numerous attacks on nongovernmental organizations and others, mostly in Asia but to some extent in other countries. Last year, for example, researchers from McAfee spotted the threat actor conducting a major cyber espionage operation targeting telecommunication companies in the US, Asia, and Europe.

The latest campaign represents a departure from the usual for the group, since it targets Russian entities, according to McLellan: "This is substantially different to what we have seen over the past two years where Bronze President has been about 90% focused on Myanmar and Vietnam. We believe they still have a mission in the Asia region, but this has been a bit of a departure for them."