Chinese APT Combines Fresh Hodur RAT with Complex Anti-Detection

By Nate Nelson

Published: 2022-03-24 · Archived: 2026-04-10 02:10:10 UTC

Mustang Panda's already sophisticated cyberespionage campaign has matured even further with the introduction of a brand-new PlugX RAT variant.

The Chinese advanced persistent threat (APT) Mustang Panda (a.k.a. Temp.Hex, HoneyMyte, TA416 or RedDelta) has upgraded its espionage campaign against diplomatic missions, research entities and internet service providers (ISPs) – largely in and around Southeast Asia.

For one thing, the APT has deployed a brand-new, customized variant of an old but powerful remote-access tool (RAT) called PlugX (aka Korplug), according to researchers from ESET. They named this latest variant "Hodur," after a blind Norse god known for slaying his thought-to-be-invulnerable half-brother Baldr.

Beyond that, Mustang Panda has developed a complex array of tactics, techniques and procedures (TTPs) to maximize the efficacy of its attacks.

ESET researchers noted, "Every stage of the deployment process utilizes anti-analysis techniques and control-flow obfuscation."

The cyberespionage campaign dates back to at least last August and is still ongoing, according to ESET, and is targeting mainly governments and NGOs. Most victims are located in East and Southeast Asia, but there are outliers in Europe (Greece, Cyprus, Russia) and Africa (South Africa, South Sudan).

The attacks begin with social-engineering emails or watering-hole attacks, researchers said.

"The compromise chain includes decoy documents that are frequently updated and relate to events in Europe [and the war in Ukraine]," noted the team, in a Wednesday posting. "One of the filenames related to this campaign is "Situation at the EU borders with Ukraine.exe."

Other phishing lures mention updated COVID-19 travel restrictions, an approved regional aid map for Greece, and a Regulation of the European Parliament and of the Council.

"The final lure is a real document available on the European Council's website," according to ESET. "This shows that the APT group behind this campaign is following current affairs and is able to successfully and swiftly react to them."

What is Hodur?

Hodur derives from PlugX, a RAT that "allows remote users to perform data theft or take control of the affected systems without permission or authorization. It can copy, move, rename, execute and delete files; log keystrokes; fingerprint the infected system; and more."

PlugX is one of the oldest malware families around, having existed in some form or another since 2008, with a rise in popularity in the mid-2010s. Malware that old won't cut it these days, which is why Mustang Panda has constantly iterated on it. Even just a few weeks ago, researchers from Proofpoint discovered an upgrade "changing its encoding method and expanding its configuration capabilities."

According to ESET, the new variant "mostly lines up with other Korplug variants, with some additional commands and characteristics." It for instance closely resembles another Norse-themed variant – Thor – discovered in 2020.

Sophisticated Attack Chain

Hodur itself is hardly the star of the show: Mustang Panda's campaign features literally dozens of TTPs designed to establish persistence, collect data and evade defenses.

As mentioned, the campaign begins simply, as the group uses current events to phish their targets. For example, last month, Proofpoint discovered it puppeteering a NATO diplomat's email address to send out .ZIP and .EXE files titled "Situation at the EU borders with Ukraine."

If a target falls for the bait, a legitimate, validly signed, executable vulnerable to DLL search-order hijacking, a malicious DLL, and an encrypted Hodur file are deployed on the target machine.

"The executable is abused to load the module, which then decrypts and executes the…RAT," explained researchers. "In some cases, a downloader is used first to deploy these files along with a decoy document."

Mustang Panda's campaigns then frequently use custom loaders for shared malware including Cobalt Strike, Poison Ivy, and now, Hodur. Then things get interesting. ESET analysts tallied a total of 44 MITRE ATT&CK techniques deployed in this campaign. Most interesting are the 13 different methods of obfuscating or otherwise evading cybersecurity tools and detection.

For example, the ESET blog noted that "directories created during the installation process are set as hidden system directories," and "file and directory names match expected values for the legitimate app that is abused by the loader."

And, the malware gaslights you because "scheduled tasks created for persistence use legitimate-looking names," and "when writing to a file, Korplug sets the file's timestamps to their previous values."

Who's Behind Mustang Panda?

Cybersecurity analysts have been tracking Mustang Panda since 2017, when they first started using Mongolian-themed phishing tactics to conduct espionage on targets in Southeast Asia. Still, there's much we don't know

about the group.

The depth and complexity of their TTPs puts Mustang Panda more in the company of state-sponsored groups than criminal ones. So “it is possible, though unproven, that they are state-sponsored or at least state-sanctioned,” wrote Mike Parkin, senior technical engineer at Vulcan Cyber, via email.

Historically, the group has kept to Southeast Asia, with one notable exception – the Vatican – in 2020. The vast majority of targets in ongoing campaigns have, indeed, been located in Mongolia and Vietnam, followed closely by Myanmar. However, as mentioned, the list also includes select entities in Europe and Africa, which muddies the picture a bit.

“The target distribution is interesting,” Parkin concluded. “There isn’t enough information publicly available here to determine the attacker’s ultimate agenda.”

Moving to the cloud? Discover emerging cloud-security threats along with solid advice for how to defend your assets with our FREE downloadable eBook, “Cloud Security: The Forecast for 2022.” We explore organizations’ top risks and challenges, best practices for defense, and advice for security success in such a dynamic computing environment, including handy checklists.
