New Mustang Panda hacking campaign targets diplomats, ISPs

bleepingcomputer.com/news/security/new-mustang-panda-hacking-campaign-targets-diplomats-isps/

Bill Toulas

By
Bill Toulas

- March 23, 2022
- 03:13 PM
- 0

Security analysts have uncovered a malicious campaign from China-linked threat actor Mustang Panda, which has been running for at least eight months with a new variant of the Korplug malware called Hodur and custom loaders.

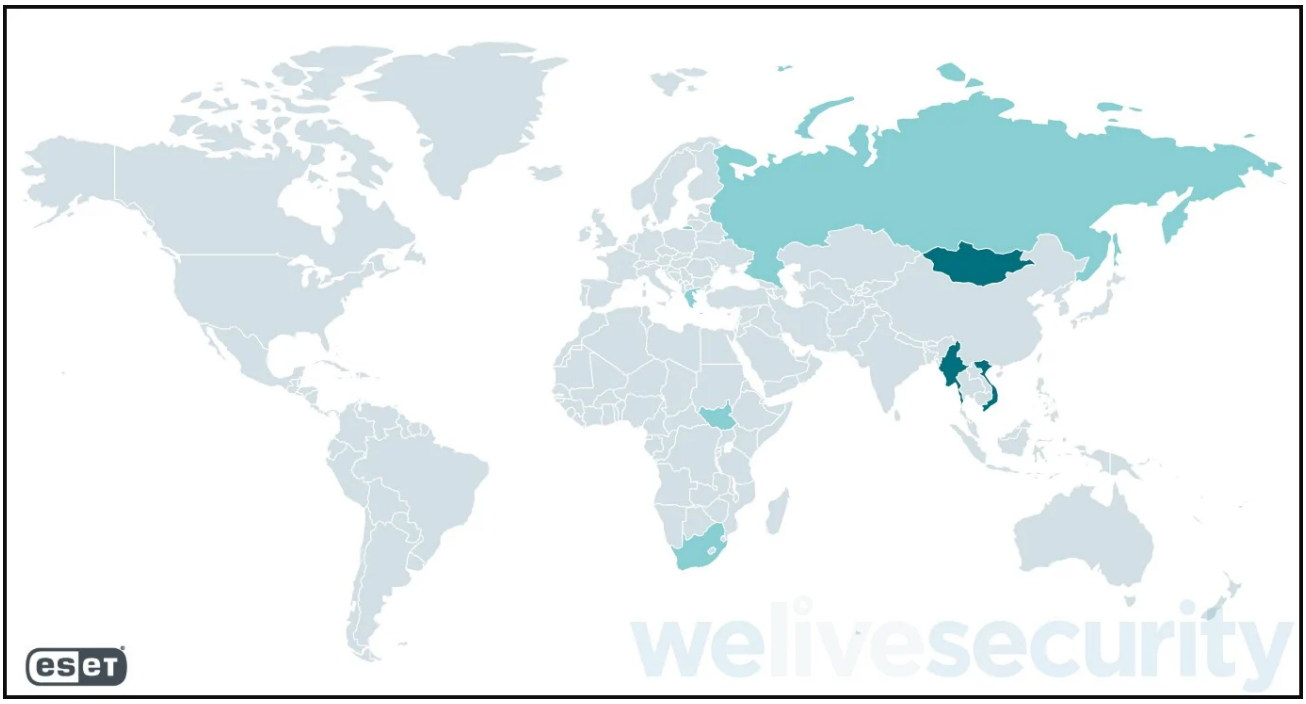
Also tracked as TA416, Mustang Panda is known to serve China-aligned interests and has been recently associated with phishing and espionage operations that targeted European diplomats.

Korplug is a custom malware used extensively but not exclusively by this particular threat actor, first exposed in a 2020 report that examined the activity of Chinese hackers against Australian targets.

In the latest known campaign, analyzed by cybersecurity company ESET, Mustang Panda focuses on European diplomats, ISPs (Internet Service Providers), and research institutes, using phishing lures with decoy documents.

Since August 2021, when this campaign is believed to have started, the hackers refreshed their lures several times, the latest ones being topics related to Russia's invasion of Ukraine, COVID-19 travel restrictions, or documents copied from the European Union Council's website.

The targeted countries in this campaign are Russia, Greece, Cyprus, South Africa, Vietnam, Mongolia, Myanmar, and South Sudan.



Mustang Panda targets heatmap *(ESET)*

Same targets, new tools

The targeting scope of Mustang Panda has remained largely unchanged in the past couple of years, so the threat group is mainly occupied with refreshing its lures and improving its toolset.

ESET reports having sampled elaborate custom loaders and new Korplug (Hodur) variants that still use DLL side-loading but now feature much heavier obfuscation and anti-analysis systems present across the entire infection chain.

The malicious module and the encrypted Korplug payload are downloaded along with the decoy document and a legitimate executable, combining their execution for DLL side-loading to evade detection.

Korplug's loading chain *(ESET)*

The custom DLL loader leverages the digitally-signed legitimate executable, in this case, a SmadAV file, and exploits a known vulnerability for side-loading.

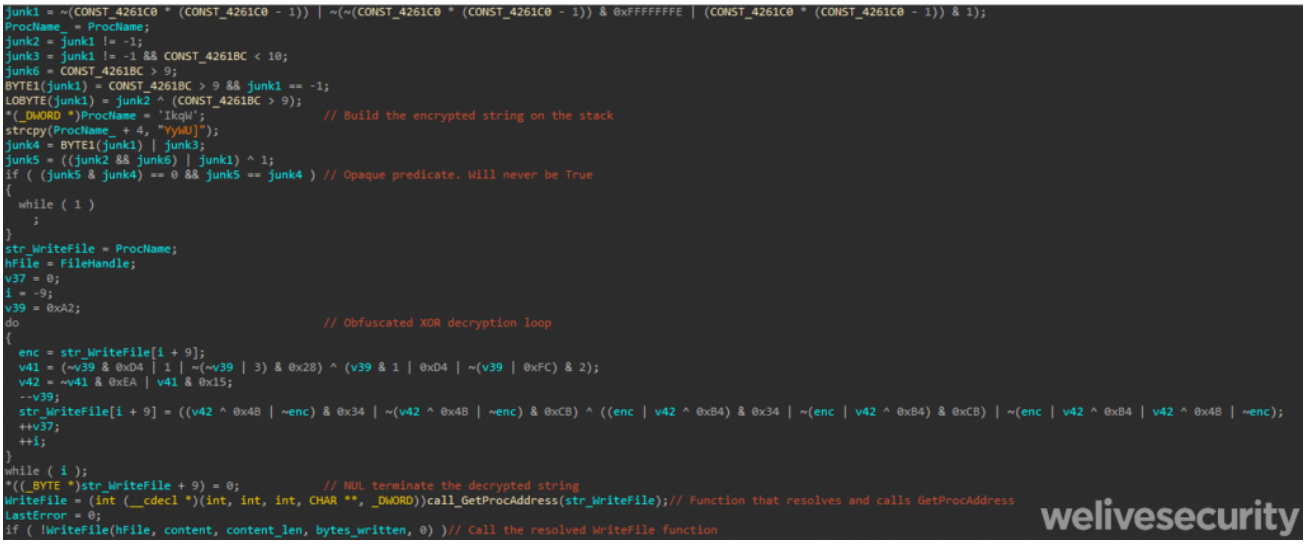
The multiple functions exported by the loader are bogus, except for one, which is the function that loads the new Korplug variant.

A new backdoor version

Korplug is a remote access trojan (RAT) whose functionality hasn't been thoroughly analyzed thus far, potentially because there are so many variants created by each APT using it.

The one used by Mustang Panda in this campaign is very similar to THOR, a PlugX variant discovered by Unit 42 researchers last year.

Korplug payloads are decrypted in memory, while only an encrypted form is ever written to the disk. Additionally, all strings are encrypted and Windows API function calls are obfuscated, while anti-execution measures also exist.



Windows API call obfuscation *(ESET)*

Persistence is achieved by adding a new registry entry to "Software\Microsoft\Windows\CurrentVersion\Run", while the newly created directories that host the malware components are marked as "hidden" and "system."

The additions of this new version are spotted on the RAT aspect of Korplug, where its authors have added more commands and features.

The commands supported by the first handler of the particular Korplug variant are the following:

- **Ping** – start listening for commands
- **GetSystemInfo** – gather and send system information
- **ListenThread** – start a new threat that listens for commands for the second handler
- **ResetConnection** – reset connection to C2
- **Uninstall** – delete added registry keys, remove all malware components and delete the created folders
- **Stop** – disable registry key and exit

The second handler listens to a different set of commands that concern the RAT's functionality and are thus more advanced than the first set, which is used for basic reconnaissance.

The list of this second group is extensive, but some indicative examples are commands to list drives and directories, read and write files, execute commands on a hidden desktop, and start an interactive remote cmd.exe session.

ESET believes Mustang Panda will continue to improve its toolset, making it more potent and stealthy, while special attention has to be paid to phishing emails that appear very realistic.

Being a Chinese actor that has shown signs of serving higher political espionage interests, its targeting scope should remain relatively stable.

Related Articles:

Chinese state-backed hackers now target Russian state officers

Hackers target Russian govt with fake Windows updates pushing RATs

New stealthy Nerbian RAT malware spotted in ongoing attacks

Emotet botnet switches to 64-bit modules, increases activity

Phishing campaign targets Russian govt dissidents with Cobalt Strike

- China
- Cyber-espionage
- Mustang Panda
- Phishing
- RAT
- ta416
- Trojan

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

You may also like: