EINPRESSWIRE

ESET Research discovers new China-aligned APT group CeranaKeeper, which targeted the Thai government

DUBAI, DUBAI, UNITED ARAB EMIRATES, October 7, 2024 /EINPresswire.com/ -- ESET researchers have discovered several targeted campaigns against governmental institutions in Thailand, starting in 2023, where massive amounts of data have been exfiltrated. The campaigns misused legitimate file-sharing services such as Dropbox, PixelDrain, GitHub, and OneDrive in the process. Based on the findings, ESET researchers decided to track this activity cluster as the work of a separate threat actor, which ESET named CeranaKeeper. The numerous occurrences of the string “bectrl” in the code of the group’s tools inspired the name: a wordplay between the word beekeeper and the bee species Apis Cerana, or the Asian honeybee. ESET presented its findings about CeranaKeeper and the compromise in Thailand at the 2024 Virus Bulletin conference.

The threat actor behind the attacks on the Thai government, CeranaKeeper, seems particularly relentless, as the plethora of tools and techniques used by the group keeps evolving at a rapid rate. The operators write and rewrite their toolset as needed and react rather quickly to avoid detection. This group’s goal is to harvest as many files as possible and it develops specific components to that end. CeranaKeeper uses cloud and file-sharing services for exfiltration and probably relies on the fact that traffic to these popular services would mostly seem legitimate and harder to block when identified.
CeranaKeeper has been active since at least the beginning of 2022, mainly targeting governmental entities in Asia such as Thailand, Myanmar, the Philippines, Japan, and Taiwan.

The Thai attacks leveraged revamped versions of components previously attributed by other researchers to the China-aligned APT group Mustang Panda, and later, a new set of tools that abuse service providers such as Pastebin, Dropbox, OneDrive, and GitHub to execute commands on compromised computers and exfiltrate sensitive documents. However, the review of the tactics, techniques and procedures, code, and infrastructure discrepancies leads ESET to believe that tracking CeranaKeeper and MustangPanda as two separate entities is necessary. Both China-aligned groups could be sharing information and a subset of tools in a common interest or through the same third party.

“Despite some resemblances in their activities like similar side-loading targets and archive format, ESET observed distinct organizational and technical differences between the two groups, such as differences in their toolsets, infrastructure, operational practices, and campaigns. We also noted differences in the way the two groups accomplish similar tasks,” explains ESET researcher Romain Dumont, who discovered CeranaKeeper.

CeranaKeeper is likely using the publicly documented toolset called “bespoke stagers” (or TONESHELL), which heavily relies on a side-loading technique, and uses a specific sequence of commands to exfiltrate files from a compromised network. In their operations, CeranaKeeper deploys components known to be unique to the group and are deployed in their operations. Furthermore, the group left some metadata in its code that provided ESET with insight into its development process, further solidifying our attribution to CeranaKeeper.

After gaining privileged access, the attackers installed the TONESHELL backdoor, deployed a tool to dump credentials, and used a legitimate Avast driver and a custom application to disable security products on the machine. From this compromised server, they used a remote administration console to deploy and execute their backdoor on other computers in the network. The group deployed a new BAT script across the network, extending their reach to other machines by exploiting the domain controller to gain Domain Admin privileges.

In the attack against the Thai government, the attackers found and selected a couple of compromised computers of sufficient interest to deploy previously undocumented, custom tools. These support tools were used not only to facilitate the exfiltration of documents to public storage services but also to act as alternative backdoors. One notable technique the group uses is GitHub’s pull request and issue comment features to create a stealthy reverse shell, leveraging GitHub, a popular online platform for sharing and collaborating on code, as a C&C server.

For a more detailed analysis and technical breakdown of CeranaKeeper’s tools, check out the latest ESET Research white paper “CeranaKeeper: A relentless, shape-shifting group targeting Thailand” on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET

ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/749586271