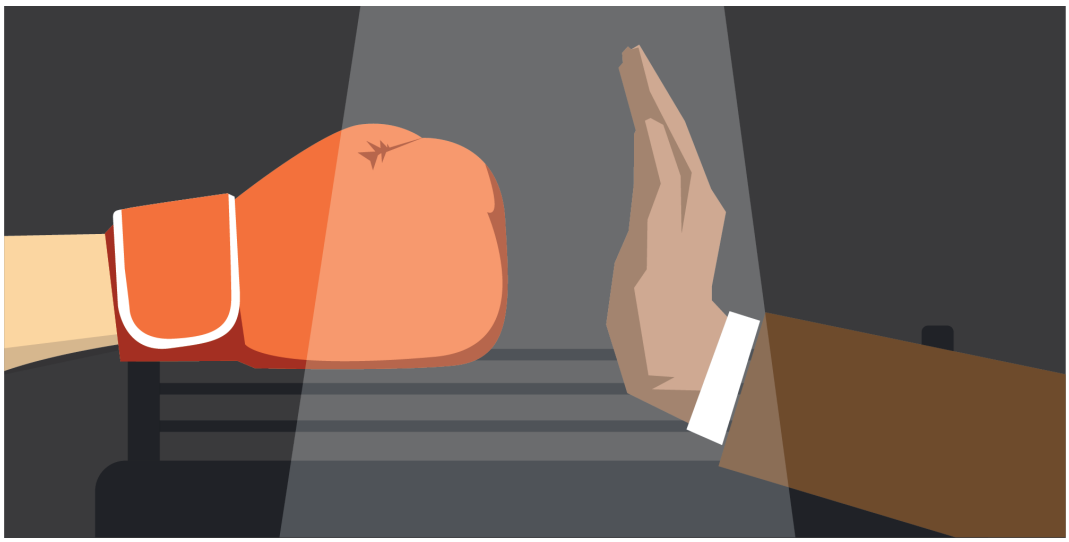
Unit 42 Researchers Discover Multiple Espionage Operations Targeting Southeast Asian Government

Lior Rochberger, Tom Fakterman, Robert Falcone ⋮⋮ 9/22/2023

By Lior Rochberger, Tom Fakterman and Robert Falcone

September 22, 2023 at 6:00 AM

Category: Government



This post is also available in: 日本語 (Japanese)

Executive Summary

In early 2023, Unit 42 researchers began investigating a series of espionage attacks that targeted a government in Southeast Asia. These attacks focused on different governmental entities in the same country, including critical infrastructure, public healthcare institutions, public financial administrators and ministries.

This appeared at first glance to be the activity of a single threat actor. Careful analysis, however, revealed the attacks to have been carried out by separate threat actors whose activities group into three distinct clusters. While this activity occurred around the same time and in some instances even simultaneously on the same victims' machines, each cluster is characterized by distinct tools, modus operandi and infrastructure.

The techniques and tools observed during the attacks, along with the persistent long-term surveillance efforts made by the different attackers, suggest the work of advanced persistent threats (APTs). In our analysis, we were able to attribute the three clusters to known APT groups with different levels of confidence.

The Unit 42 system for defining and tracking threat adversaries provides a framework for grouping similar behaviors, tools, infrastructure and tradecraft, and then assigning names to the resulting clusters. When we applied this framework to the attacks we observed, we broke the clusters down as follows:

- The activity observed in the first cluster (tracked as CL-STA-0044) is attributed with moderate-high confidence to the well-known Stately Taurus group (aka Mustang Panda), a group believed by the security community to be affiliated with Chinese interests. Read more about the activity observed in this cluster in "Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda."
- The activity observed in the second cluster (tracked as CL-STA-0045) is attributed with a moderate level of confidence to the Alloy Taurus group (aka GALLIUM). This group is also believed to be operating on behalf of Chinese state interests. Read more about the activity observed in this cluster in "Persistent Attempts at Cyberespionage Against Southeast Asian Government Target Have Links to Alloy Taurus."

- Lastly, the activity observed in the third cluster (tracked as CL-STA-0046) is attributed with a moderate level of confidence to the Gelsemium group, which so far has not been formally attributed to any specific state. Read more about the activity observed in this cluster in "Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Government."

This research offers a glimpse into the intricate and clandestine world of nation-state cyberespionage, in which multiple critical government entities of one country were compromised.

Palo Alto Networks Cortex XDR and XSIAM customers receive protections through WildFire, Behavioral Threat Protection, Local Analysis, Analytics and multiple other security modules that can help detect and block various threats including targeted APT attacks.

Organizations can engage the Unit 42 Incident Response team for specific assistance with this threat and others.

Related Unit 42 Topics **Government**, APTs

Table of Contents

Background

While conducting threat hunting operations in late 2022, Unit 42 researchers discovered activity targeting a government in Southeast Asia. Initially, we found malicious activities in one compromised environment that belonged to a government entity. Through careful examination of the forensic evidence, including the tactics, techniques and procedures (TTPs) as well as infrastructure, we were able to identify three distinct clusters of activity.

You can find the descriptions for the individual clusters in the following reports:

- Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda
- Persistent Attempts at Cyberespionage Against Southeast Asian Government Target Have Links to Alloy Taurus
- Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Government

The diagram in Figure 1 provides a comprehensive visual overview of the overall observed activities, prior to the breakdown by clusters of activity. It includes the TTPs employed by the threat actors and the affected machines within the environment.

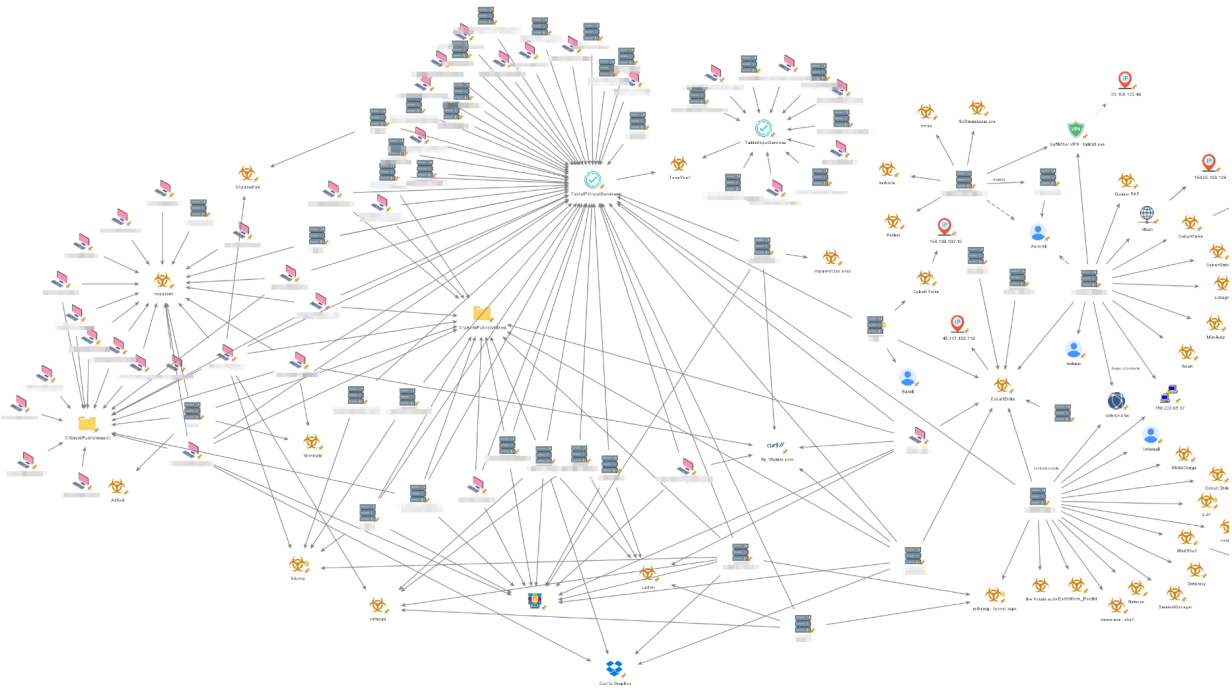


Figure 1. Maltego graph of the artifacts observed in the initial compromised environment.

Each cluster had its own unique characteristics, which allowed us to define each one separately. The clustering and attribution process we used was based on the Diamond model of attribution, allowing for a comprehensive understanding of the threat landscape.

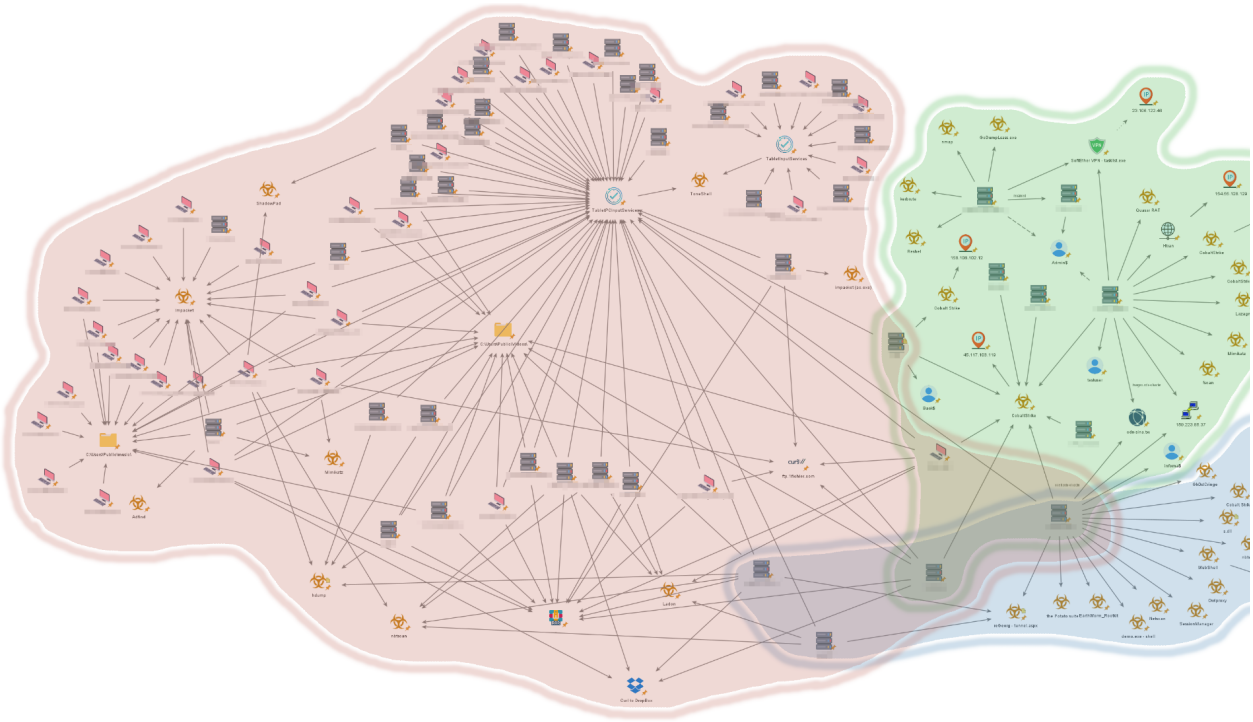


Figure 2. Maltego graph of the three clusters identified in the initial compromised environment.

As the investigation progressed, we found further overlapping activity in additional environments. All of these environments were determined to belong to governmental entities for the same government in Southeast Asia.

Bird's Eye View of Each Cluster's Activity

The following section provides an overview of the main findings in each of the clusters.

CL-STA-0044 (Approximately Q1 2021-Q3 2023)

The activity observed in this cluster is attributed with moderate-high confidence to the APT group Stately Taurus. Analysis of the activity suggests that the attackers conducted a cyberespionage operation that focused on gathering intelligence as well as stealing sensitive documents and information, while maintaining a persistent and clandestine foothold.

The attackers used two main backdoors. The first one was an undocumented variant of the ToneShell backdoor. The second backdoor was ShadowPad, a complex and modular backdoor known to be exclusively used by Chinese APT groups.

The attackers also used a range of known hacking tools, such as the following:

- LadonGo
- Impacket
- China Chopper web shells
- Scanning and credential dumping tools

A full analysis of CL-STA-0044 activity, TTPs and IoCs can be found in "Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda."

CL-STA-0045 (Q1 2022-Q3 2023)

The activity observed in this cluster is attributed with a moderate level of confidence to the Alloy Taurus APT group. Analysis of the activity shows that the attackers were mainly focused on the following activities:

- Establishing long-term persistence
- Reconnaissance missions
- Obtaining and maintaining access through a variety of activities
    - Various backdoors
    - Web shells
    - Prolific credential-gathering activities

The attackers attempted to remain under the radar by using uncommon techniques and by circumventing several security products.

The main tools observed in this cluster included two previously unknown backdoors, Zapoa and ReShell, first identified by Unit 42 researchers. Moreover, the attackers also used known malware and hacking tools such as the following:

- GhostCringe remote access Trojan (RAT)
- Quasar RAT
- Cobalt Strike
- Kerbrute brute forcing tool
- China Chopper web shell

A full analysis of CL-STA-0045 activity, TTPs and IoCs can be found in "Persistent Attempts at Cyberespionage Against Southeast Asian Government Target Have Links to Alloy Taurus."

CL-STA-0046 (Q3 2022-Q4 2022)

The activity observed in this cluster is attributed with a moderate level of confidence to the Gelsemium APT group. Analysis of the activity shows that the attackers mainly focused on reconnaissance and maintaining access activities, specifically targeting vulnerable IIS servers.

The two main, unique types of malware used in this cluster were OwlProxy and SessionManager. The combination of these distinct tools has only been observed in past attacks that other researchers have attributed to Gelsemium.

In addition, the attackers used more common tools such as the following:

- Cobalt Strike
- Meterpreter
- Earthworm
- Spoolfool

A full analysis of CL-STA-0046 activity, TTPs and IoCs can be found in "Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Government."

Conclusion

The investigation we conducted revealed that what initially appeared as a single attack orchestrated by a solitary threat actor was not so simple. It unfolded into a complex operation of multiple infiltrations carried out across three distinct clusters of activity.

Distinguishing one activity from another is a complicated task and can, in many cases, lead to wrong clustering and misattributions. This investigation highlights the importance of paying attention to details and carefully examining artifacts and data.

The revelation of these clusters dating back to the beginning of 2021 and spanning into the present year, provides a glimpse into the relentlessness of advanced persistent threats. By attributing each cluster to previously known APT groups — Stately Taurus, Alloy Taurus and Gelsemium — our investigation underlines the importance of vigilance in safeguarding the digital landscape against these experienced adversaries whose techniques are always evolving.

It's clear that our ability to overcome challenges posed by these threat actors relies on the foundations of proactive defense and multilayer protection systems being constantly updated for new techniques.

Palo Alto Networks Cortex XDR and XSIAM customers receive protections through WildFire, Behavioral Threat Protection, Local Analysis, Analytics and multiple other security modules that can help detect and block various threats including targeted APT attacks.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.