Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific

Unit 42 ⁝⁝ 11/17/2023

By Unit 42

November 17, 2023 at 3:00 AM

Category: Malware

Tags: Advanced URL Filtering, Advanced WildFire, APT, C2, China, Cloud-Delivered Security Services, Cortex XDR, Cortex XSIAM, Cortex XSOAR, DNS security, Machine Learning, next-generation firewall, Stately Taurus, threat prevention, WildFire

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

Executive Summary

Tensions between China and the Philippines have risen sharply over the past several months. In early August, a Chinese Coast Guard vessel fired its water cannon at a Philippine vessel that was performing a resupply mission to the disputed Second Thomas Shoal in the Spratly Islands. Since then, the Philippines has announced joint patrols with the United States, and naval exercises with Australia. It has been reported that the Philippine Coast Guard has both terminated a hotline established with their Chinese counterparts and acted to remove Chinese barriers placed near the disputed Scarborough Shoal.

Coinciding with these real-world events, Unit 42 researchers observed three Stately Taurus campaigns during the month of August. These campaigns are assessed to have targeted entities in the South Pacific including the Philippines government. The campaigns leveraged legitimate software including Solid PDF Creator and SmadavProtect (an Indonesian-based antivirus solution) to sideload malicious files. Threat authors also creatively configured the malware to impersonate legitimate Microsoft traffic for command and control (C2) connections.

Stately Taurus (aka Mustang Panda, Bronze President, Red Delta, Luminous Moth, Earth Preta and Camaro Dragon) has been operating since at least 2012. It is assessed to be a Chinese advanced persistent threat (APT) group that routinely conducts cyberespionage campaigns. This group has historically targeted government entities and nonprofits, as well as religious and other non-governmental organizations across North America, Europe and Asia.

Palo Alto Networks customers receive protection from the threats described in this article through Cortex XDR and WildFire malware analysis.

Related Unit 42 Topics **China**, APT, Stately Taurus

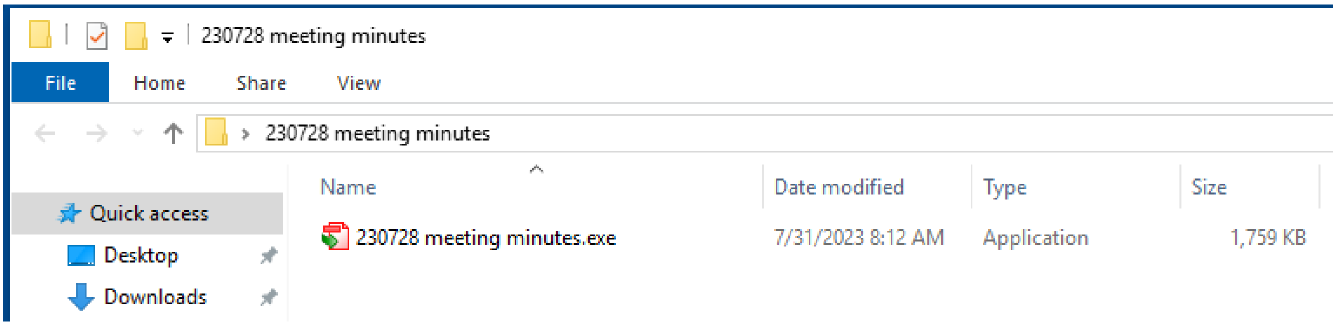
Table of Contents

Campaigns

Unit 42 observed three Stately Taurus campaigns during the month of August.

Campaign 1

The first campaign was observed on Aug. 1, 2023, when we identified a Stately Taurus malware package that was hosted for download on Google Drive. Threat operators configured this malware package as a ZIP file named 230728 meeting minutes.zip. Upon extracting this archive, unsuspecting victims are presented with the view shown in Figure 1.



Name	Date modified	Type	Size
230728 meeting minutes.exe	7/31/2023 8:12 AM	Application	1,759 KB

Figure 1. ZIP archive contents.

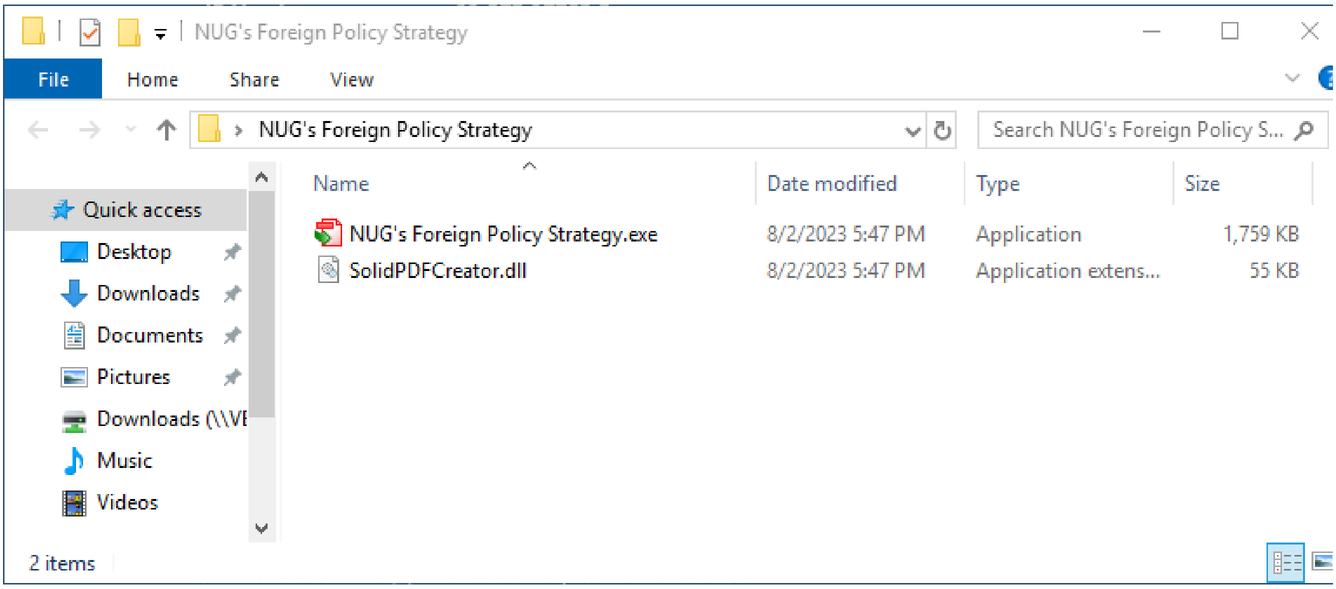
By default, victims are presented with a visible application (20230728 meeting minutes.exe) that contains a PDF icon. This file is in fact a legitimate copy of Solid PDF Creator software that has been renamed. However, what victims don’t see is that this folder contains a second hidden file named SolidPDFCreator.dll.

Any attempt to execute the legitimate Solid PDF Creator software will result in the side-loading of the malicious DLL contained in the same folder. Once loaded, the malicious DLL then establishes a connection with 45.121.146[.]113 to facilitate C2.

We assess that an entity associated with the Philippines government saw this first malware package as early as Aug. 1, 2023.

Campaign 2

We subsequently identified a second Stately Taurus malware campaign on Aug. 3, 2023. This malware package was configured as a ZIP file named NUG's Foreign Policy Strategy.zip. In this case, the acronym "NUG" is believed to be a reference to the National Unity Government of Myanmar. Upon extracting this archive, victims are presented with a view that is similar to the first campaign, which is shown in Figure 2.



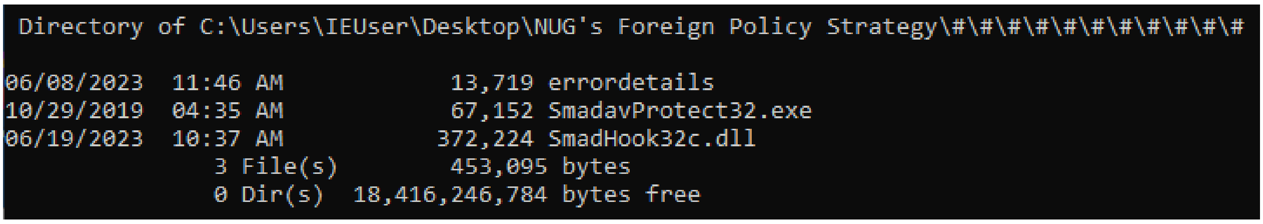
Name	Date modified	Type	Size
NUG's Foreign Policy Strategy.exe	8/2/2023 5:47 PM	Application	1,759 KB
SolidPDFCreator.dll	8/2/2023 5:47 PM	Application extens...	55 KB

Figure 2. ZIP archive contents.

Here we see a legitimate copy of Solid PDF Creator software that has been renamed as NUG's Foreign Policy Strategy.exe. We also see the hidden SolidPDFCreator.dll file that is side-loaded when the application is launched. However, what is deceiving about this sample is that this ZIP file also contains additional files hidden in the path:

NUG's Foreign Policy Strategy\#\#\#\#\#\#\#\#\#\#\#\

After traversing 11 folders named #, we identified three additional files, shown in Figure 3.



```
 Directory of C:\Users\IEUser\Desktop\NUG's Foreign Policy Strategy\#\#\#\#\#\#\#\#\#\#\#

06/08/2023  11:46 AM            13,719 errordetails
10/29/2019  04:35 AM            67,152 SmadavProtect32.exe
06/19/2023  10:37 AM           372,224 SmadHook32c.dll
               3 File(s)        453,095 bytes
               0 Dir(s)  18,416,246,784 bytes free
```

Figure 3. Contents of # folder.

In terms of process flow, upon executing the visible NUG's Foreign Policy Strategy.exe binary, the threat side-loads SolidPDFCreator.dll. This DLL then copies these three files (errordetails, SmadavProtect32.exe and Smadhook32c.dll) to the victim's home directory and establishes a registry key (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\AHealthDB) to call SmadavProtect32.exe when a user logs on.

SmadavProtect32.exe is a legitimate and benign copy of an Indonesian antivirus program called SmadAV. Upon login, SmadavProtect32.exe will load the malicious DLL (SmadHook32c.dll) and then the malware (errordetails) contained in the same folder. Once running, the malware is configured to call home to 45.121.146[.]113 for C2.

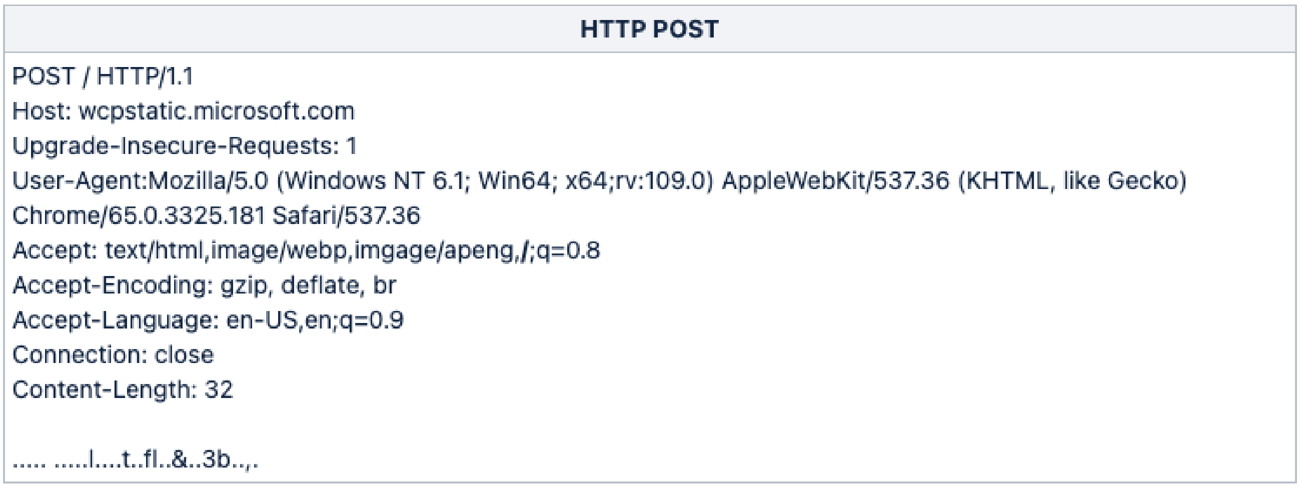
Campaign 3

The third campaign is structurally identical to the first campaign, and it was created on Aug. 16, 2023. However, the ZIP and EXE filenames use Labour Statement.zip instead of 230728 meeting minutes from the first example.

Upon extracting the contents of the ZIP file, victims are presented with two files. The first file, called Labour Statement.exe, is a benign copy of Solid PDF Creator software. The second file is a malicious DLL named SolidPDFCreator.dll. Following execution of the application, the malicious DLL is loaded, and it establishes a connection to 45.121.146[.]113 for C2 consistent with the previous two campaigns.

C2 Infrastructure

The IP address 45.121.146[.]113 was first associated with Stately Taurus during a series of campaigns launched in June 2023. We assess that the actors continued to leverage this infrastructure throughout the month of August 2023. However, one interesting aspect of the C2 activity is that the actors attempted to disguise it as legitimate Microsoft traffic, as shown in Figure 4.



HTTP POST

```
POST / HTTP/1.1
Host: wcpstatic.microsoft.com
Upgrade-Insecure-Requests: 1
User-Agent:Mozilla/5.0 (Windows NT 6.1; Win64; x64;rv:109.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.181 Safari/537.36
Accept: text/html,image/webp,imgage/apeng,/;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 32

..... .....l....t..fl..&..3b..,.
```

Figure 4. Malware POST statement.

Specifically, in the POST statements the malware sets the host field to wcpstatic.microsoft[.]com despite the traffic being directed to an IP address in Malaysia that has no relation to any legitimate Microsoft services.

Additionally, in monitoring traffic associated with the C2 server, we identified multiple connections between Aug. 10 and Aug. 15, 2023, originating from Philippines government infrastructure. Given traffic to the known malicious C2 server, we assess a Philippines government entity was likely compromised during these campaigns, at least for the five-day period in August 2023.

Conclusion

During the month of August, Stately Taurus actors launched at least three campaigns targeting entities in the South Pacific. We assess that at least one of these campaigns directly targeted the Philippines government and that the actors were successful in their attempts to compromise a government entity for five days in August.

Stately Taurus continues to demonstrate its ability to conduct persistent cyberespionage operations as one of the most active Chinese APTs. These operations target a variety of entities globally that align with geopolitical topics of interest to the Chinese government. We encourage organizations to leverage our findings to inform the deployment of protective measures to defend against this threat group.

Protection Recommendations

To defend against the threats described in this blog, Palo Alto Networks recommends organizations employ the following capabilities:

- Network Security: Delivered through a Next-Generation Firewall (NGFW) configured with machine learning-enabled, and best-in-class, cloud-delivered security services. This includes, for example, threat prevention, URL filtering, DNS security and a malware prevention engine capable of identifying and blocking malicious samples and infrastructure.
- Endpoint Security: Delivered through an XDR solution that can identify malicious code through the use of advanced machine learning and behavioral analytics. This solution should be configured to act on and block threats in real time as they are identified.
- Security Automation: Delivered through an XSOAR or XSIAM solution capable of providing SOC analysts with a comprehensive understanding of the threat derived by stitching together data obtained from endpoints, network, cloud and identity systems.

Protections and Mitigations

Palo Alto Networks customers receive protection from the threats discussed above through the following products:

- Advanced WildFire cloud-delivered malware analysis service accurately identifies the malware described in this blog as malicious.
- Cortex XDR prevents the execution of known malware and also prevents the execution on unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings 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.

Indicators of Compromise

Stately Taurus Samples

- bebde82e636e27aa91e2e60c6768f30beb590871ea3a3e8fb6aedbd9f5c154c5
- 24c6449a9e234b07772db8fdb944457a23eecbd6fbb95bc0b1398399de798584
- ba7c456f229adc4bd75bfb876814b4deaf6768ffe95a03021aead03e55e92c7c
- 969b4b9c889fbec39fae365ff4d7e5b1064dad94030a691e5b9c8479fc63289c
- 3597563aebb80b4bf183947e658768d279a77f24b661b05267c51d02cb32f1c9
- d57304415240d7c08b2fbada718a5c0597c3ef67c765e1daf4516ee4b4bdc768
- 54be4a5e76bdca2012db45b1c5a8d1a9345839b91cc2984ca80ae2377ca48f51
- 2b05a04cd97d7547c8c1ac0c39810d00b18ba3375b8feac78a82a2f9a314a596

Infrastructure

- 45.121.146[.]113
- hxxps://drive.google[.]com/uc?id=1QLIQXP-s42TtZsONsKLAAtOr4Pdxljcu