Mustang Panda Group Targets Philippines Amid Tensions in the South China Sea

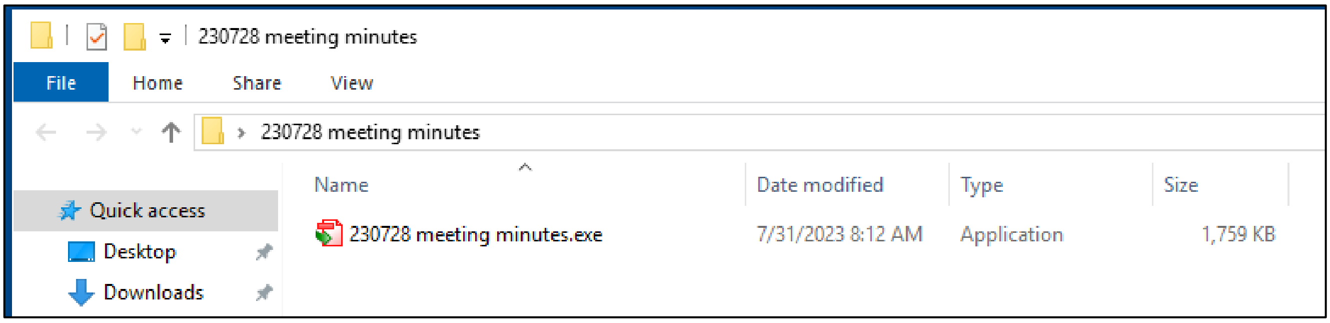
Introduction

The relationship between China and the Philippines has experienced significant strain in recent months. Early in August, a Chinese Coast Guard ship fired its water cannon at a Philippine vessel carrying supplies to the contested Second Thomas Shoal in the Spratly Islands. In response, the Philippines has announced plans for joint patrols with the United States and naval exercises with Australia. Additionally, it has been reported that the Philippine Coast Guard has ended communication with its Chinese counterparts and removed Chinese barriers erected near the disputed Scarborough Shoal.

Concurrently with these real-world events, research shows Mustang Panda had three cyber espionage campaigns in August. These campaigns are believed to have targeted entities in the South Pacific, including the Philippine government. The campaigns utilized legitimate software such as Solid PDF Creator and SmadavProtect, an Indonesian antivirus solution, to execute malicious files onto target systems. The threat actors also devised a clever approach of cloaking the malware's command and control communications to mimic legitimate Microsoft traffic.

Mustang Panda is a Chinese advanced persistent threat (APT) group that has been operating since at least 2012. The group is believed to be affiliated with the Chinese government and has been linked to a number of cyberespionage campaigns targeting government entities, nonprofits, and other organizations in North America, Europe, and Asia.

On August 1, 2023, it was observed that a Mustang Panda malware package was hosted for download on Google Drive. The threat actors had disguised the malware package as a ZIP file named *230728 meeting minutes.zip*. When unsuspecting victims extracted the archive, they were presented with the view 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 File

Upon opening the extracted folder, victims are presented with an application named "*20230728 meeting minutes.exe*" bearing a PDF icon. This file is a renamed copy of the legitimate Solid PDF Creator software. However, unbeknownst to the victims, the folder also contains a hidden file named "*SolidPDFCreator.dll*."

Executing the seemingly harmless "*20230728 meeting minutes.exe*" triggers the side-loading of the malicious DLL residing in the same folder. Once loaded, the malicious DLL communicates with 45.121.146[.]113 to establish a command-and-control (C2) connection.

Our assessment indicates that an entity affiliated with the Philippine government encountered this initial malware package as early as August 1, 2023.

The third campaign, created on August 16, 2023, mirrors the structure of the first campaign. However, the ZIP and EXE filenames differ, with the third campaign using "*Labour Statement.zip*" instead of "*230728 meeting minutes.zip*" from the first instance.

Upon extracting the ZIP file's contents, victims encounter two files. The first file, "*Labour Statement.exe*," is a harmless copy of the Solid PDF Creator software. The second file, identified as "*SolidPDFCreator.dll*," harbors malicious intent.

Executing the seemingly innocuous "*Labour Statement.exe*" triggers loading the malicious DLL residing in the same folder. Subsequently, the malicious DLL establishes a connection with 45.121.146[.]113, mirroring the command-and-control (C2) communication pattern observed in the previous two campaigns.

Indicators of Compromise

Value	Type
bebde82e636e27aa91e2e60c6768f30beb590871ea3a3e8fb6aedbd9f5c154c5	Sha256
24c6449a9e234b07772db8fdb944457a23eecbd6fbb95bc0b1398399de798584	Sha256
ba7c456f229adc4bd75bfb876814b4deaf6768ffe95a03021aead03e55e92c7c	Sha256
969b4b9c889fbec39fae365ff4d7e5b1064dad94030a691e5b9c8479fc63289c	Sha256
3597563aebb80b4bf183947e658768d279a77f24b661b05267c51d02cb32f1c9	Sha256
d57304415240d7c08b2fbada718a5c0597c3ef67c765e1daf4516ee4b4bdc768	Sha256
54be4a5e76bdca2012db45b1c5a8d1a9345839b91cc2984ca80ae2377ca48f51	Sha256
2b05a04cd97d7547c8c1ac0c39810d00b18ba3375b8feac78a82a2f9a314a596	Sha256
45.121.146[.]113	IP Address
hxxps://drive.google[.]com/uc?id=1QLIQXP-s42TtZsONsKLAAtOr4Pdxljcu	URL

Conclusion

Throughout August, Mustang Panda operatives orchestrated at least three cyber espionage campaigns directed at entities within the South Pacific region. Our assessment indicates that at least one of these campaigns specifically targeted the Philippine government, and the perpetrators successfully infiltrated a government agency for five days in August.

Mustang Panda consistently proves its effectiveness in carrying out persistent cyber espionage operations, establishing itself as one of the most active Chinese advanced persistent threats (APT) groups. These operations target a diverse range of entities worldwide that align with the geopolitical interests of the Chinese government. We strongly urge organizations to utilize our findings to inform the implementation of protective measures to counter this threat group.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

USA – TX

Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

JAPAN

Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
hiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.