KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification| ScanBox Framework used for Cyber Espionage by Chinese Threat Actors

Tracker ID: TN0904 **Date:** 06/Sep//2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Australia, Europe

Background

A Chinese nation-state threat group utilized a reconnaissance malware, ScanBox, to acquire details about its targets during a months-long cyber espionage campaign. The ScanBox exploitation framework was used to target victims who visit a malicious domain masquerading as a news website. Local and federal government agencies, news media outlets, and worldwide heavy industry producers with wind turbine fleets were among the targets. This current attack affected Australia, Malaysia, and Europe, as well as organizations conducting business in the Asia-Pacific area, with a particular emphasis on the South China Sea.

ScanBox is a JavaScript-based malware that has been used in attacks since 2014, allowing threat actors to profile their victims and deliver next-stage payloads to key targets. Along with HUI Loader, PlugX, and ShadowPad, it is rumored to be shared covertly by numerous Chinese hacker groups. APT10 (also known as Red Apollo or Stone Panda), APT27 (also known as Emissary Panda, Lucky Mouse, or Red Phoenix), and TA413 are some of the major threat actors who have previously been observed using ScanBox (aka Lucky Cat).

Indictments have publicly identified overlapping conduct with this threat actor as "APT40" and "Leviathan." APT40, a threat actor with espionage motivations based in China, has been active since 2013. In July 2021, the US government and its allies linked the adversarial group to China's Ministry of State Security (MSS). Between April 12 and June 15, the assaults employed phishing campaign waves to spread the ScanBox reconnaissance framework by impersonating Australian media businesses utilizing URLs impersonating Australian media companies. The subject lines of the phishing emails included words like "Sick Leave, User Research, and Cooperation Request."

In contrast to watering holes or strategic web breaches, which infect a real website known to be visited by the targeted with malicious JavaScript code, the APT40 activity uses an actor-controlled domain to deploy the malware. The threat actor would typically pose as a representative of the fictitious "Australian Morning News," sending out URLs to the malicious domain and demanding that targets view or share any published research information.

These attacks exploited malicious RTF files to launch a first-stage downloader, which later functioned as a conduit for receiving encoded versions of the Meterpreter shellcode. In March 2022, a European manufacturer of heavy machinery used in offshore wind projects in the Taiwan Strait was one of the victims of this campaign. Furthermore, the Copy-Paste compromises targeting government entities revealed by the Australian Cyber Security Centre (ACSC) in June 2020 have been linked to APT40. This is not the first time that APT40 has utilized fraudulent news websites to spread ScanBox. A 2018 phishing effort used news article URLs published on a rogue domain to trick victims into downloading malware. It's worth noting that from March 2021 to March 2022, a long-term phishing campaign linked to the same threat actor targeted Malaysian and Australian organizations, as well as foreign corporations interested in the South China Sea offshore energy projects.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | ScanBox Framework used for Cyber Espionage by Chinese Threat Actors

Tracker ID: TN0904 **Date:** 06/Sep//2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Australia, Europe

MITRE ATT&CK Tactics

Reconnaissance, Initial Access , Execution, Command and Control.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Ensure patches are applied for the Follina Bug, CVE-2022-30190, that restricts exploitation of RTF documents.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically
- Ensure secure handling of emails that come from outside sources and data acquired from the Internet.
- Implement employees training and awareness on the ongoing phishing campaigns and techniques.
- Avoid opening untrusted links and email attachments without first verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- Establish a data recovery strategy and routinely backup your files to a secure offsite place.
- Use strong passwords, change them frequently, and, when available, multi-factor authentication.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart threats.

References

- MICHAEL RAGGI AND SVEVA SCENARELLI, Rising Tide: Chasing the Currents of Espionage in the South China Sea , Cybereason, 30th August 2022, External Link (proofpoint.com)
- Ravie Lakshmanan, Chinese Hackers Used ScanBox Framework in Recent Cyber Espionage Attacks, 31st August 2022, External Link (thehackernews.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification| ScanBox Framework used for Cyber Espionage by Chinese Threat Actors

Tracker ID: TN0904 **Date:** 06/Sep//2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Australia, Europe

SHA-256 Hash	Domains	URL	IP	Email
7795936ed1bdb7a5756c1ff821b2dc8739966abbb00e3e0ae114ee728bf1cf1a	australianmorningnews[.]com	hxxp://australianmorningnews[.]com/?p=23	139.59.60[.]116:443	visitable.daishaju@gmail[.]com
4dedb022d3c43db6cddd87f250db4758bd88c967f98302d97879d9fc4fadd8a2	image[.]australianmorningnews[.]com	hxxp://australianmorningnews[.]com/?p=30	172.105.114[.]27:80	goodlandteactuator@gmail[.]com
5a1c689cddb036ca589f6f2e53d323109b94ce062a09fb5b7c5a2efedd7306bc	regionail[.]xyz	hxxp://australianmorningnews[.]com/?p=58		claire3bluntxq@gmail[.]com
cb981d04f21a97fdb46b101a882a3490e245760489f4122deb4a0ac951a8eaee	heraldsun[.]me	hxxp://australianmorningnews[.]com/?p=55		ascents.nestora2@gmail[.]com
3d37a977f36e8448b087f8e114fe2a1db175372d4b84902887808a6fb0c8028f	walmartsde[.]com	hxxp://australianmorningnews[.]com/?p=30		walknermohammad26@gmail[.]com
e8a919e0e02fecfe538a8698250ac3eaba969e2af2cc9d96fc86675a658e201e	theaustralian[.]in	hxxp://australianmorningnews[.]com/?p=23-<UserID>		entertainingemiliano20@gmail[.]com
0b9447cb00ae657365eb2b771f4f2c505e44ca96a0a062d54f3b8544215fc082		hxxp://asutralianmorningnews[.]com/?p=19-<UserID> (Actor Typo)		entertainingemiliano20@gmail[.]com
2f204f3b3abc97efc74b6fa016a874f9d4addb8ac70857267cc8e4feb9dbba26		hxxp://australianmorningnews[.]com/?p=23-<UserID>		osinskigeovannyxw@gmail[.]com
2a17927834995441c18d1b1b7ec9594eedfccaacca11e52401f83a82a982760e		hxxp://image[.]australianmorningnews[.]com/i/		brittanisoq@outlook[.]com
18db4296309da48665121899c62ed8fb10f4f8d22e44fd70d2f9ac8902896db1		hxxp://image[.]australianmorningnews[.]com/i/?cwhe18nc		charmainejuxtzk@outlook[.]com
F55c020d55d64d9188c916dcbece901bc6eb373ed572d349ff61758bd212857f		hxxp://image[.]australianmorningnews[.]com/i/v.php?m=b		gradyt18iheme@outlook[.]com
5681cf40c3f00c1a0dc89c05d983c0133cc6bf198bce59acfef788d25bcd9f69		hxxp://image[.]australianmorningnews[.]com/i/c.php?data=		dagny382cber@outlook[.]com
22df809c1f47cb8d685f9055ad478991387016f03efd302fdde225215494eb83		hxxp://image[.]australianmorningnews[.]com/i/k.php?data=		marikok2bedax@outlook[.]com
b7e435ccded277740d643309898d344268010808e0582f34ae07e879ac32cf1e		hxxp://image[.]australianmorningnews[.]com/i/p.php?data=		pearlykeap3l@outlook[.]com
3909ae9b64b281cca55fc2cd6d92a11b882d1a58e4c34a59a997a7cb65aba8ef		hxxp://image[.]australianmorningnews[.]com/i/v.php?m=a&data=		mattbotossd@outlook[.]com
54ad4c1853179a59d5e9c48b1cfa880c91c5bf390fcfb94e700259b3f8998cb3		hxxp://image[.]australianmorningnews[.]com/i/v.php?m=p&data=		thuang6102@gmail[.]com
c4471540b811f091124c166ab51d6d03b6757f71e29c61a0e360e5c64957fcdd		hxxp://image[.]australianmorningnews[.]com/i/v.php?m=plug		earlt1948@gmail[.]com
400be1d28d966ba8491f54237adad52ad4eea8a051f45f49774b92cbfdfcf1ea		hxxps://regionail[.]xyz/		amianggitaphill@yahoo[.]com
8033a52b327ad6635fc75f6c2c17b2cb4d56e1fd00081935541c0fb020e2582f		hxxps://regionail[.]xyz/austrade.au		zoezlb@gmail[.]com
a115051a02e4faa8eb06d3870af44560274847c099d8e2feb2ef8db8885edf5e		hxxps://magloball[.]com/nDo3SB		Daisha Manalo <visitable.daishaju@gmail[.]com>
57c8123dd505dadb640872f83cf0475871993e99fdb40d8b821a9120e3479f53		hxxps://theaustralian[.]in/europa.eeas		Blair Goodland <goodlandteactuator@gmail[.]com>
981c762ce305cd5221e8757bafa50a00fff8fbc92db5612b311c458d48c29793		hxxps://theaustralian[.]in/office		Claire Blunt <claire3bluntxq@gmail[.]com>
6d2b301e77839fff1c74425b37d02c3f3837ce50e856c21ae4cf7ababb04addc		hxxps://theaustralian[.]in/word		Nestor Pyles <ascents.nestora2@gmail[.]com>
13f593f217b4686d736bcfce3917964632e824cb0d054248b9ffcacc59b470d4		hxxp://172.105.114[.]27/v<victim identifier>		Mohammad Walkner <walknermohammad26@gmail[.]com>
c4f6fedb636f07e1e53eaef9f18334122cb9da4193c843b4d31311347290a78f		hxxp://walmartsde[.]com/UpdateConfig		Emiliano Regulus <entertainingemiliano20@gmail[.]com>
ab963bf7b1567190b8e5f48e7c88d53c02d7a3a57bd2294719595573a1f2b7c7				Emiliano Regulus <entertainingemiliano20@gmail[.]com>
e3f1519db0039e7423f49d92d43d549b152b534856a7efde1a7eda7a9276bb22				Geovanny Osinski <osinskigeovannyxw@gmail[.]com>
e1f34cb031bac517796c363c2b31366509bf1367599fd5583c6bc2b0314758bb				Brittani Silvestre <brittanisoq@outlook[.]com>
d357502511352995e9523c746131f8ed38457c38a77381c03dda1a1968abce42				Charmaine Jubinville <charmainejuxtzk@outlook[.]com>
55a5871b36109a38eed8aef943ccddf1ae9945f27f21b1c62210a810bb0f7196				Grady Iheme <gradyt18iheme@outlook[.]com>
98fbd5eb6ae126fda8e36e3602e6793c1f719ef3fdbf792689035104b39f14ac				Dagny Berdecia <dagny382cber@outlook[.]com>
7e1ab1b08eb4b69df11955c3dfe3050be467a374adb704a917ee1a69abcc58a5				Mariko Dax <marikok2bedax@outlook[.]com>
				Pearly Keasler <pearlykeap3l@outlook[.]com>
				Matt Botos <mattbotossd@outlook[.]com>
				ami phillips <amianggitaphill@yahoo[.]com>
				Tom Huang <thuang6102@gmail[.]com>
				Thomas Earl <earlt1948@gmail[.]com>
				zoe browne <zoezlb@gmail[.]com>
				suzannehhu316[@]outlook[.]com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia