# KPMG Cyber Threat Intelligence Platform

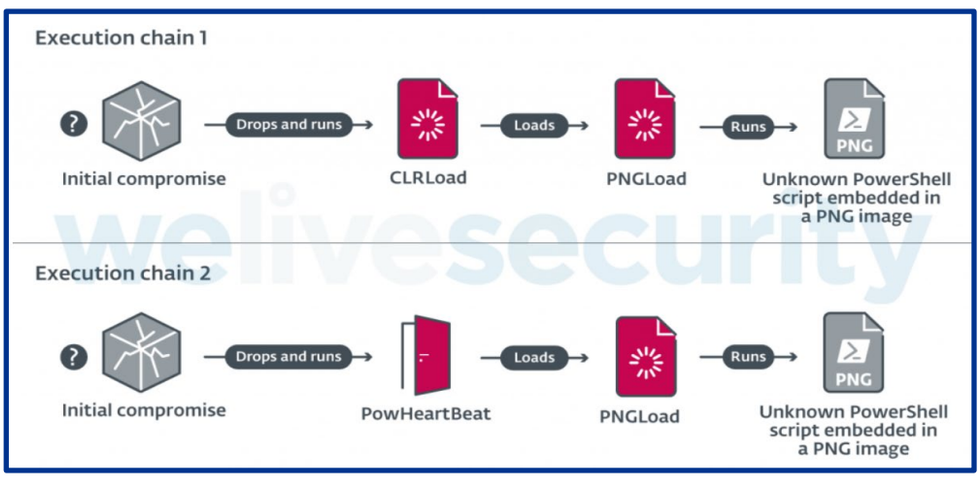
## Cyber Threat Notification | Worok Hacker targets government and critical organizations across Asia

**Tracker ID:** TN0914 **Date:** 19/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Middle East, Africa

### Background

Worok, a cyber espionage organisation, infiltrated numerous prominent businesses and regional governments in Asia, the Middle East, and Africa using secretive methods. It primarily targets businesses in the telecoms, banking, shipping, energy, and public, military, and governmental sectors. The Worok hackers were able to breach several victims in late 2020. Worok and another adversarial group known as TA428 have common tools and interests.

Between May 2021 and January 2022, the group's malicious operations took a significant hiatus before picking back up the following month. Information theft is in line with the group's objectives. ProxyShell exploits were used to gain an initial foothold on target networks until 2021 and 2022. Additional custom backdoors were then introduced for entrenched access.




In an identified campaign, the first-stage loader in Worok's malware arsenal is dubbed CLRLoad, and it is followed by the.NET-based steganographic loader PNGLoad, which can run an unidentified PowerShell script that is hidden inside a PNG image file. Infection chains in 2022 have now abandoned CLRLoad in favour of PowHeartBeat, a fully functional PowerShell implant that launches PNGLoad and communicates with a remote server via HTTP or ICMP to carry out associated file operations, transmit and receive files, and execute arbitrary commands.

A cyber espionage organisation called Worok compromises its targets using both custom-built tools and techniques that already exist. Although it's believed that the malware might be cloaked in legitimate, innocent-looking PNG pictures and therefore "hidden in plain sight" without drawing attention, it was unable to recover any of the final-stage PNG payloads.


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.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Worok Hacker targets government and critical organizations across Asia

**Tracker ID:** TN0914 **Date:** 19/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Middle East, Africa

### MITRE ATT&CK Tactics

Reconnaissance, Resource Development, Execution, Persistence, Defense Evasion, Credential Access, Collection, Command and Control, Discovery and Exfiltration.

### Indicators of Compromise

Please refer to the attached sheet for IOCs.

### Recommendations

- Immediately identify the vulnerable instances and apply the vendor-provided fixes as soon as possible.
- Collect and review relevant logs, data, and artifacts to ensure the threat is eradicated from the network and thwart residual issues that could enable follow-on exploitation.

### References


- Ravie Lakshmanan, Worok Hackers Target High-Profile Asian Companies and Governments, The Hacker News, 6th September 2022, External Link (thehackernews.com).
- Thibaut Passilly, Worok: The big picture, WeLiveSecurity, 6th September 2022, External Link (www.welivesecurity.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.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Worok Hacker targets government and critical organizations across Asia

**Tracker ID:** TN0914 **Date:** 19/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Middle East, Africa

*

| SHA-256 | Domain | IP |
|---|---|---|
| 30e61ff19add249449427dba73e153e7f91e00f0cd29ea765a13e31bb8063deb | airplane.travel-commercials[.]agency | 118.193.78[.]22 |
| 4f6ff43ef26d6314073cf81df10be9afd68a13c1edf70e6cc6527b876e41765c | central.suhypercloud[.]org | 118.193.78[.]57 |
| 88f21d6d6b5eee63c2d3287c2237fba2ebaaa7b60693088460da8580ea7476b2 | | 5.183.101[.]9 |
| 95ac61d4747dce9d788bbb014f1cc229b38466701536fb6bfb55ea982ecacd9c | | 45.77.36[.]243 |
| 354f0c12a6ee48a3134b239d17b19b7037f0a543b8175a1c5f3788c36a1bc8ca | | |
| 83256251c68865f3bfaaaa4e84af1a7cd86a03496bff6812af959c42935e0d3c | | |
| 6add19b9e897c9b6a28ff936fdd43a2767d431f1aafbfeae44eda62bbddbe1c2 | | |
| dc07499acbb66efeede1fe0ea3b58af7d21d576b4e6dd0ac2689d91d51e1db2a | | |
| 212cf693f1fe30a1a331bab46e967e33dba78f573783f3c3f825a69e5e1de1b7 | | |
| 1c640f819746b8487da061252bf273a5552da051f3ce7398d04a12f4afe1d68a | | |
| 048bf4763c9ee1720484083b7510f7b069e9a49d17d30b16896cae153923210f | | |
| 7e30f679770cdee8d9bc07aca3ab74de0ff3e8db6b553c5d73b316d263854606 | | |
| 32604f40d1466beb3595d071d03b62283d1c6995c844a07cd8a43ac1165f3c73 | | |
| abf4924189449f138e2c317801980bf678fcf41dc3439da1165b0e0bc0338b5e | | |
| f0cb38bcd7f0eb151d6b9e9d4dbb6f4d151d93027f857036fb50b265e56bc047 | | |
| abbba5b314358b9653d8239b2ba4e7f4b28fedacb96521367db0be5c1628d7aa | | |
| 867ab458f7dbba5d9c6e9e9f7e51b6ebdf3c5bf874ca5f5378f4e93562ab96c4 | | |
| 3829d52fd46a19aa899877b51674539250a2581bba737a2bd16310c5cf6eaeb7 | | |
| 8ef147f36126f5e2eb1999a39696f503f682b5ed430c78607f8ab00b20aafc97 | | |
| 14f2bc448bea41cb504db2bcf5705b524d172390e4b08dd17d3d7ca904fa7b36 | | |
| AD42DF1A28A6BA2C3FC03CE028E64DD1C26CB906EC437B0154EB82838E2EAB3A | | |
| C4C0038A7E40BE59DE36AFC4F97BA33501E1D7BA984C13C567CF1C8AA19A0569 | | |
| c85745dcec836ad94339a81adbe5350538cf7d55115139fb8ed67d6985bad3c1 | | |

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.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia