


3rd October – Threat Intelligence Report

 research.checkpoint.com/2022/3rd-october-threat-intelligence-report/

October 3, 2022



For the latest discoveries in cyber research for the week of 3rd October, please download our [Threat Intelligence Bulletin](#).

Top Attacks and Breaches

Check Point Research identified an ongoing, mobile malware campaign that has consistently targeted Uyghurs for at least the past seven years. Attributed to the actor Scarlet Mimic, the malware campaign was disguised in multiple baits such as books, pictures, and even an audio version of the Quran.

Check Point Harmony Mobile provides protection against this threat

- Hactivist groups around the world have taken aim at the Iranian regime, as protests throughout the country continue. The groups have been leaking information relating to Iranian government officials, and offering support to the protesters in sharing information and evading censorship.
- Mexico's government has suffered a large-scale hack, with more than 6TB of data being leaked. Included in the leaked data is sensitive information, such as the president's medical condition. The hactivist group 'Guacamaya' has assumed responsibility for the hack. The group is notorious in the Latin American region, and has previously targeted the governments/militaries of Chile, Peru, Colombia, and El Salvador.

- Personal information of 10 million Australians has been stolen in a breach of telecom company Optus. The data includes sensitive information, such as passport and healthcare details. While the hackers initially demanded a 1M USD ransom, they later retracted their demand due to the high attention drawn to the hack and the law enforcement operation initiated to identify the attackers.
- Following September's ransomware attack on Los Angeles Unified School District, the 2nd largest school district in the United States, the school district now declared they refuse to pay the ransom. Vice Society, the group behind the attack, started leaking data stolen during the attack.

Check Point Threat Emulation, Anti-Virus and Harmony Endpoint provide protection against this threat (Ransomware.Win32.Vice.; Trojan.Win.ViceSociety.*)*

- Luxury hotel chain Shangri-La has notified customers of a security breach, resulting in guest information from eight of the chain's hotels in Southeast Asia being stolen.
- American IT firm NJVC has been breached by ransomware group BlackCat. Among the firm's customers is the United States Department of Defense.

Check Point Anti-Virus, Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.BlackCat; Ransomware_Linux_BlackCat)

A potential LinkedIn social engineering campaign has been discovered, in which threat actors created a network of fraudulent profiles of CISO executives in fortune 500 companies.

Vulnerabilities and Patches

2 zero-day vulnerabilities in Microsoft Exchange have been disclosed, after already being exploited in the wild. The vulnerabilities allow an authenticated user to gain remote code execution capability on exchange servers, and have similarities to the notorious 2021 ProxyShell vulnerabilities. While Microsoft has acknowledged the vulnerabilities (CVE-2022-41040 and CVE-2022-41082) and offered steps for detection and mitigation, an official patch is yet to be released.

Check Point Threat Emulation, Harmony Endpoint and IPS provide protection against this threat (Exploit.Wins.ProxyShell.; Exploit.Win.ProxyShell; Microsoft Exchange Server Remote Code Execution (CVE-2022-41082); Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); Microsoft Exchange Server Security Feature Authentication Bypass (CVE-2021-31207))*

- A critical vulnerability affecting popular mobile messaging platform WhatsApp has been discovered. The integer overflow vulnerability could allow an attacker to gain remote code execution capability against the target via video call. WhatsApp has released a security update addressing this threat.

- Multiple vulnerabilities and security flaws were found in popular end-to-end encryption library Matrix. Matrix has published a patch addressing some of the security flaws.

Threat Intelligence Reports

- Check Point Research published a report studying the rising trend of state-mobilized Hacktivism. While in the past Hacktivist groups tended not to affiliate themselves with national interests, groups nowadays take part in state-directed efforts, driven by geopolitical conflicts.
- Intelligence reports detailing the recent activities of the North Korean APT groups ZINC and Lazarus suggest the groups have been spying on companies of various fields, mostly located in Europe and Asia.

Check Point Threat Emulation provides protection against this threat (APT.Win.Lazarus.; Backdoor.Wins.Lazarus.*)*

- A new botnet malware dubbed 'Chaos' is written by Chinese threat actors, has sophisticated post-infection capabilities, and has been used to conduct DDoS attacks on targets in various fields.
- Researchers have compiled a report on the techniques used by the Witchetty group. The groups has been employing spyware tools targeting governments in the Middle East.

Check Point Anti-Virus provides protection against this threat (Spyware.Win32.Witchetty.)*

- A study of the Brazilian cyber gang Prilex shows that the group, notorious in Brazil for their malware targeting ATMs and credit-card cloning, has lately been focusing on developing Point of Sale malware.
- The American Internal Revenue Service (IRS) has warned Americans of a significant increase in Phishing scams distributed via SMS during the past few weeks.

[GO UP](#)

[BACK TO ALL POSTS](#)