Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Several Taiwanese government websites were temporarily taken down in a denial of service attack, as Speaker of the US House of Representatives Pelosi visited Taiwan, a visit strongly opposed by China.
- Over 35,000 Github repositories were cloned in an attempted Supply Chain attack. The cloned projects were edited to include malicious code, in hope that programs would use the cloned versions and become infected. Github has removed the malicious versions of the projects from its library following the discovery of this threat.
- The British National Health Service (NHS) has suffered major services outage, as its managed service provider, Advanced, was hit by a cyberattack.
- Researchers have discovered a new remote access Trojan, dubbed WoodyRAT, which has primarily been targeting Russian entities for the past year. WoodyRAT has sophisticated capabilities, and is suspected to be distributed by either Chinese or North Korean actors.

  Check Point Anti-Virus provides protection against this threat *(Woody.TC.*, RAT.Win32.Woody.TC.*)*
- Attacks targeting various Cryptocurrency/Blockchain platforms have been observed in the past week. In one incident, a security flaw in Crypto-bridge firm Nomad's service allowed nearly $200 million to be stolen, while another attack targeting the Solana platform saw thousands of digital wallets drained. In a third case, the DeBridge Finance Blockchain firm has successfully thwarted an attack likely initiated by the North-Korean APT group Lazarus, who has previously stolen over $600 million from Blockchain gaming firm Axie Infinity earlier this year.
- Semikron, a German manufacturer of power modules and systems, has been targeted by the LV ransomware group. In a statement, Semikron confirmed that an attack caused partial encryption of files, and that the hacker group claim to have exfiltrated data.

  Check Point Harmony Endpoint provides protection against this threat
- Online survey firm QuestionPro was being extorted, after a database containing 22 million of its users has been obtained by malicious actors. The database was eventually leaked online.

VULNERABILITIES AND PATCHES

- VMware has published a security advisory addressing a critical vulnerability in several of its products. The authentication bypass vulnerability allows attackers to gain Administrator privileges without authentication.
- Patches were released by multiple router device manufacturers in the past week, as a large trove of vulnerabilities were discovered in Draytek routers, as well as F5 and Cisco devices.
- The Department of Homeland Security warns of critical vulnerabilities in the American Emergency Alert System, which is used to broadcast emergency warnings from the authorities to the media. Successful exploitation could potentially allow attackers to send fake alerts, block authentic ones, and even lock out legitimate actors from the system.

THREAT INTELLIGENCE REPORTS

- Check Point has released the 2022 Mid-Year Attack Trends report, which analyses how cyberattacks have become firmly entrenched as a state-level weapon, including the new ransomware method of 'Country Extortion' and the increased disruption to the everyday lives of citizens. The report details the impact the war in Ukraine has had on the cyber landscape for companies across all sectors, and provides up-to-date statistics, advice and predictions for the remainder of 2022.
- US CISA, with the cooperation of its Australian counterpart, has published a report detailing the top malware strains of 2021. According to the report, the most prominent families are AgentTelsa, AZORult, Formbook, Ursnif and Lokibot.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats
- Researchers warn of increasing popularity of the 'Dark Utilities' platform, which offers C&C-servers-as-a-service for its customers. Threat groups have been observed to be using this service, which is capable of targeting multiple operating systems, to avoid having to create and maintain their own C&C server infrastructure.
- A report detailing the activity of new ransomware family SolidBit has been released. SolidBit, written in the Rust programming language, has been distributing its payloads by utilizing fraudulent files, which masquerade as tools for gamers and social media users.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.TouchTrapFiles.A)*
- Research shed light on the Genesis marketplace, an invitation-only platform that gains initial access to hosts in various networks. Genesis then sells access to the compromised machines to malicious actors who exploit the initial access in order to further infect the victim with their payloads.