TOP ATTACKS AND BREACHES

- Check Point Research has analyzed the Conti Ransomware gang's chat leaks and revealed insights on the group's Hi-tech company type of management, with physical offices, HR & finance departments and more. CPR published a detailed connection map exposing the organizational structure within the key members and affiliates of the group.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win32.Conti)*

- A variety of APT groups including Fancy Bear (aka APT28, Russia affiliated), Ghostwriter (aka UNC1151, Belarus affiliated) and Mustang Panda (aka TA416, China affiliated) have been targeting Ukraine, Poland and other European organizations with different phishing campaigns.

- State-sponsored APT41 group (aka Wicked Panda) affiliated with China has been successfully breaching into US government networks for the past 6 months by exploiting vulnerable web facing applications. Vulnerabilities included Log4Shell and a zero-day flaw in the USAHerds app tracked CVE-2021-44207.

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228))*

- Romanian gas station chain Rompetrol has been hit by Hive ransomware which forced the company to shut down their websites and the Fill&Go service of their stations for data protection. The Hive gang is demanding a $2 million ransom in exchange for a decryptor and not leaking the stolen data.

  Check Point Harmony Endpoint provides protection against this threat

- UK ferry operator Wightlink has been breached, affecting back-office IT systems and impacting data of some of its customers and employees.

- State-sponsored Iranian APT group MuddyWater has been linked to cyber-attacks targeting Turkey and Asian countries, using malicious documents to eventually infect the victims with Remote Access Trojans. Another campaign is active in the Arabian peninsula leveraging a malware dubbed "SloughRAT".

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Trojan.Win32.Muddywater)*

VULNERABILITIES AND PATCHES

- A privilege escalation flaw tracked as CVE-2022-0847 (also known as "Dirty Pipe") has been found and patched in Linux kernel versions 5.8 & above, and could be leveraged by a local threat actor to take control of a compromised system, read private messages and gain administrator privileges.
- Three critical security zero-day vulnerabilities dubbed "TLStorm" (tracked CVE-2022-22805, CVE-2022-22806, CVE-2022-0715), could let threat actors take control over APC Uninterruptible Power Supply (UPS) devices, leading to data loss, disruptions or even physical harm.
- Microsoft has patched a critical flaw in the Azure Automation service. Named "AutoWarp", this vulnerability could have given unauthorized access to other Azure customer data and take over control.

THREAT INTELLIGENCE REPORTS

- Check Point Research reveals in its top malware report for February 2022 that Emotet is again the most prevalent malware, impacting 5% of organizations worldwide, while TrickBot falls from second place into sixth. Several malware in the chart are currently leveraging the public interest around the Russia/Ukraine conflict for malicious email campaigns.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats

- Chinese affiliated APT group Mustang Panda (aka TA416) has been attacking European diplomats since at least mid-2020, and their most recent phishing campaign involves new lure themes exploiting the current geopolitical situation in Ukraine.
- Cybercriminals have found another way to exploit the Ukraine/Russia conflict by offering malware to cyber-operatives supporting Ukraine, asserting to be offensive tools to attack Russian targets when in fact once downloaded, the payload directly infects the receiver with different types of malware.
- A new variant of the Aberebot Android banking Trojan, dubbed "Escobar", includes a module for stealing Google Authenticator multi-factor authentication codes. The malware is being offered as a service on underground forums.
- BazarLoader malware is now being distributed through contact forms as opposed to common phishing emails and malicious documents.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat