TOP ATTACKS AND BREACHES

- Check Point Research reported how the Conti ransom group has taken cybercrime to a new, geopolitical level. They intervene in the internal politics of Costa Rica, the relationship between Costa Rica and the US, and basically moved the ransomware gangs to a new business stage of country extortion.

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

- Austrian federal state Carinthia has been attacked by the BlackCat ransomware gang, allegedly encrypting thousands of workstations. The notorious ransomware gang is demanding a $5 million ransom to unlock the encrypted computers.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.BlackCat)

- Russian state-sponsored hacking group, Turla, has been launching a reconnaissance campaign against the Austrian Economic Chamber, a NATO platform, and the Baltic Defense College.

  Check Point Threat Emulation, Anti-Virus and Anti-Bot provide protection against this threat

- Indian airline SpiceJet has been the victim of a ransomware attack that resulted in delayed flight departures and underlying system failures. The company announced that the attack is also delaying its financial results announcement.

- An undetected APT group is targeting Russian government agencies with phishing emails disguising into Windows security updates to install a RAT. It is believed that the group is operating from China.

- Clop ransomware is back after shutting down their operation for several months, and 21 new victims were added to their data leak site within a single month. Clop's most targeted sector was the industrial sector, with 45% of Clop ransomware attacks hitting industrial organizations and 27% targeting tech companies.

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

- Threat actors launched a credential stuffing attack against General Motors that resulted in the leakage of customers' information. The threat actors used the stolen information to redeem reward points for gift cards.

VULNERABILITIES AND PATCHES

- Security researchers discovered critical flaws in the Open Automation Software Platform (tracked as CVE-2022-26833 and CVE-2022-26082) which threat actors may exploit to execute remote code and to gain unauthorized access to sensitive information.
- VMware released security updates following a recent vulnerability (tracked as CVE-2022-22972) affecting Workspace ONE access, VMware Identity manager, and vRealize automation.

  Check Point IPS provides protection against this threat (VMware Authentication Bypass (CVE-2022-22972))
- Zyxel has published a security advisory following multiple vulnerabilities that were recently disclosed affecting a wide range of firewall, AP, and AP controller products, Tracked as CVE-2022-0734, CVE-2022-26531, and CVE-2022-26532.
- Mozilla has released security updates for multiple products to address zero-day vulnerabilities (CVE-2022-1802 and CVE-2022-1529) exploited during the Pwn2Own Vancouver 2022 hacking contest. The vulnerabilities, if exploited, could lead to JavaScript code execution on devices running vulnerable versions of Firefox.

THREAT INTELLIGENCE REPORTS

- A new ransomware dubbed “Cheers” targeting VMware ESXi servers has been identified, used for used a double-extortion attacks. All currently known samples operate on Linux OS.
- A new version of the Android banking Trojan called ERMAC has been released. Version 2.0 has increased the number of applications targeted from 378 to 467, covering a much wider range of apps to steal credentials and crypto-wallets.

  Check Point Harmony Mobile provides protection against this threat (RAT.AndroidOS.Ermac)
- The new ChromeLoader malware is seeing an increase in detections this month, following a relatively stable volume since the start of the year. The malware's operators perceive financial gains through a system of marketing affiliation by redirecting user traffic to advertising sites.

  Check Point Threat Emulation and Anti-virus provide protection against this threat (Trojan.Win.ChromeLoader)
- An unknown threat actor targeted security researchers using fake windows proof-of-concept exploits that infected devices with the Cobalt Strike backdoor. Attackers exploited recently patched Windows RCE vulnerabilities tracked as CVE-2022-24500 and CVE-2022-26809.

  Check Point Threat Emulation and IPS provide protection against these threats (Trojan.Win32.Cobalt Strike Beacon; Microsoft RPC Remote Code Execution (CVE-2022-26809))