TOP ATTACKS AND BREACHES

- Check Point Research uncovered a malicious campaign dubbed "DangerousSavanna" targeting multiple major financial groups in French-speaking Africa for the past two years. Threat actors used spear-phishing as the initial infection method, sending malicious attachments by emails to financial services employees in Ivory Coast, Morocco, Cameroon, Senegal, and Togo.

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

- North Korean APT group Lazarus (aka APT28) was found to be targeting energy providers across the globe, including in the US, Canada and Japan, in an espionage campaign exploiting the log4shell vulnerability on VMware Horizon as initial access.

  Check Point IPS and Threat Emulation provide protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44228)); APT.Win.Lazarus)*

- Multiple cyberattacks linked to Iran have been disrupting Albania's government systems since July, forcing them to shut down some online services. In response, Albania's government halted its diplomatic ties with Iran, ordering staff to leave within 24 hours. The latest attack which occurred over the weekend, allegedly by the same actor, targeted the Albanian Police's computer system, forcing officials to take its TIMS system, used for immigration data tracking, offline.

- A cyber-attack targeting the Portuguese Armed Forces General Staff Agency (EMGFA) resulted in the theft of classified NATO documents which are now available to purchase on the Dark Web.

- Los Angeles Unified School District (LAUSD), one of the largest district in the US, has been victim of a ransomware attack which disrupted access to IT systems. The attack was claimed by the Vice Society ransomware gang, known for its double extortion schemes.

- InterContinental Hotels Group PLC (IHG) announced it was victim of a cyber-attack in which hackers were able to access the company's systems, disrupting IHG booking channels and other applications.

- The outdoor clothing company The North Face has announced it was targeted by a credential stuffing attack earlier in August and notified its customers of possible compromised accounts. Hackers possibly accessed purchase history information, addresses, phone number, date of birth and more.

- Iranian state-affiliated APT group Nemesis Kitten has been leveraging vulnerabilities and living-off-the-land tools to encrypt victims' systems, demanding thousands of dollars in exchange for decryption keys.

VULNERABILITIES AND PATCHES

- CISA has added 12 additional vulnerabilities to its catalog including two D-Link security flaws: CVE-2022-28958 and CVE-2022-26258, which are currently being leveraged by the Moobot botnet. These flaws could let a threat actor execute code remotely and take over the compromised devices. US Federal Agencies have three weeks to patch their systems.

  Check Point IPS provides protection against this threat *(D-Link DIR-820L Command Injection (CVE-2022-26258))*

- Taiwanese NAS provider QNAP warns that DeadBolt ransomware is attacking its users, exploiting a flaw in the Photo Station application to encrypt QNAP NAS connected to the internet. QNAP consequently patched the vulnerability and recommends its users to not directly connect NAS devices to the internet.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Wins.deadbolt)*

- A zero-day vulnerability in WordPress plugin BackupBuddy is currently being exploited, with around 5 million attempts so far. This flaw, tracked CVE-2022-31474, could let an unauthenticated hacker download and view any arbitrary file content on a server that can be read by the WordPress installation.

  Check Point IPS provides protection against this threat *(WordPress BackupBuddy Plugin Arbitrary File Read (CVE-2022-31474))*

- HP has released an advisory warning of new severe vulnerability in HP Support Assistant. Tracked CVE-2022-38395 it could enable threat actors to escalate privileges when Fusion launches the HP Performance Tune-up on compromised devices.

THREAT INTELLIGENCE REPORTS

- A new multistage Linux malware dubbed Shikitega has been reported, enabling threat actors to gain full control over Linux endpoints and IoTs devices, as well as drop a persistent cryptocurrency miner.

- The ex-Conti ransomware gang's Cobalt Strike infrastructure, now used by several other ransomware groups, has been victim of Distributed-Denial-of-Service (DDoS) attacks associated with anti-war messages, disrupting their operation.

- Members of the Conti Ransomware gang appear to now be part of UAC-0098, an initial access broker group that has been known to take part in ransomware operations leveraging banking malware. The financially motivated threat actor has recently been shifting its purpose by targeting Ukrainian entities, including governmental as well as European non-profit organizations.

- CISA, the FBI and the Multi-State Information Sharing & Analysis Center have released a joint alert regarding the Vice Society ransomware gang disproportionately targeting the Education sector.