TOP ATTACKS AND BREACHES

- Japanese optics giant Hoya Corporation has been a victim of a ransomware attack that impacted its major IT infrastructure and various business divisions. Hunters International ransomware gang claimed responsibility for the attack and demanded a ransom of $10M for alleged 1.7M stolen files.

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

- French football club Paris Saint-Germain (PSG) has been a victim of a cyber-attack that impacted its ticketing system before Wednesday's Champions League match. The compromised system held some of the fans sensitive data, including names, emails, phone numbers, last three digits of IBAN numbers and more.

- BlackSuit ransomware gang, a rebrand of the Royal ransomware group, has claimed responsibility for two cyberattacks on The East Central University (ECU) of Ada, Oklahoma, and the non-profit healthcare service provider Group Health Cooperative of South Central Wisconsin (GHC-SCW). The threat actors attacked and encrypted file servers that affected various ECU campus computers as well as GHC-SCW protected health information (PHI).

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.Royal.ta.; Ransomware.Win.Royal)*

- Medusa ransomware group has claimed responsibility for two cyberattacks on the American dermatology clinic Paducah Dermatology PLLC and Tarrant County Appraisal District (TAD), a government agency in Texas. The gang demanded a ransom of $100K BTC from each of the victims, for the deletion of alleged personal stolen data.

- AT&T has confirmed a data breach that exposed the personal information of approximately 51M former and current clients. The exposed database may include full names, home addresses, email addresses, phone numbers, social security numbers, AT&T account number and AT&T passcode.

- Mobile gadget and bag maker Targus has suffered a cyberattack that resulted in an unauthorized access to several file systems, and shut down some of its network as a precaution. The nature of the stolen data has not yet been confirmed.

- UK veterinary services provider CVS Group has experienced a cyberattack that affected personal information as a result of an unauthorized external access to its IT systems. CVS Group took its IT systems offline as a precaution, which impacted its operations.

VULNERABILITIES AND PATCHES

- Microsoft's April 2024 Patch Tuesday fixes 149 vulnerabilities, one of which is an EoP vulnerability in the Azure Kubernetes Service Confidential Containers (AKSCC) rated with critical severity (CVE-2024-29990), and two are actively exploited zero-days. The first one (CVE-2024-26234) is a proxy driver spoofing flaw, and the second (CVE-2024-29988) is a SmartScreen prompt security feature bypass flaw that enables attackers to bypass Microsoft Defender Smartscreen by opening a specially crafted file.

  Check Point IPS blade protects against this threat *(Microsoft Proxy Driver Spoofing (CVE-2024-26234))*

- Two critical vulnerabilities in D-Link NAS devices (CVE-2024-3272 and CVE-2024-3273) have been revealed under active exploitation. Initially reported by "netsecfish" and disclosed by D-Link, these vulnerabilities allow for hard-coded credentials exposure and command injection. With over 94,000 internet-exposed units, attacks predominantly originate from China.

  Check Point IPS provides protection against this threat *(D-Link DNS Command Injection (CVE-2024-3273))*

- Citrix released security updates to address two vulnerabilities in XenServer and Citrix Hypervisor (CVE-2024-2201 and CVE-2024-31142). Successful exploitation could allow malicious unprivileged code in a guest VM to infer the contents of memory belonging to its own or other VMs on the same host. A further issue (CVE-2023-46842) has been discovered that may allow malicious privileged code running in a guest VM to cause the host to crash.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released March 2024's Most Wanted Malware report, which highlights a new method of deploying Remcos RAT, bypassing common security measures to gain unauthorized access to victims' devices. Blackbasta enters the top three of the most prolific ransomware groups for the first time, and Communications sector jumps into third place in the most exploited industries.

- Check Point Research shares insights on global cyber security trends for Q1 2024. As part of the trends, a 28% increase in the average number of cyber-attacks per organization was observed, compared to the last quarter of 2023. The Africa region saw a notable 20% increase in cyber-attacks, as opposed to Latin America, which reported a 20% decrease. Additionally, the Hardware Vendor industry experienced a 37% increase in cyber-attacks, while the Education/Research, Government/Military, and Healthcare sectors remained the most targeted.

- Researchers provide in-depth analysis of two malware families used by Earth Hundun, which is a cyberespionage-motivated threat actor that has been active for several years in the APAC region, targeting the technology and government sectors. One of its main tools is Waterbear, known for its complexity using several evasion mechanisms to minimize the chance of detection and analysis.