CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Financial data systems of The Grand Palais which hosts Olympic events in France, were targeted by an undisclosed ransomware group. As part of the attack, also the financial systems of around 40 other French museums, including the Louvre and Grand Palais, were affected. The attack didn't affect the museum's operations nor the core Olympic systems.

- The city of Killeen, Texas, was hit by ransomware attack, disrupting essential services and exposing sensitive data. The attack was attributed to the BlackSuit ransomware group, a rebrand of a gang responsible for shutting down Dallas last year.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.BlackSuite, Ransomware.Wins.BlackSuit, Ransomware_Linux_BlackSuit)

- Sumter County Sheriff's Office confirmed it had suffered a ransomware attack. Rhysida ransomware group claimed responsibility for the attack, and allegedly exfiltrated data including passports, Social Security numbers, amongst other confidential data and documents.

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

- Michigan non-profit hospital network McLaren, was hit with a ransomware attack. The attack, attributed to INC ransom group, disrupted the network's IT and phone systems of 13 hospitals.

- 911 emergency services were disrupted in the region of Central Texas for a day, due to DDoS attack. Threat actors used a large amount of fake robocalls (automated phone calls) which crashed the 911 emergency phonelines, affecting call qualities or blocking the emergency from going through at all.

- Classroom management platform Mobile Guardian has announced that it had been affected by a cybersecurity breach. The attack has allowed an attacker to unenroll and wipe more than 13,000 iPad and Chromebook devices. Mobile Guardian has suspended its service due to the attack.

- A massive data breach of a scraping service, operated by background check company National Public Data (AKA Jerico Pictures), has exposed personal information of approximately 2.9 billion people. The stolen database was initially listed for sale by the USDoD threat actor for $3.5 million, was later partially leaked for free on the notorious BreachForums. It contains sensitive data such as names, addresses, dates of birth, and Social Security numbers.

- SOCRadar had reportedly have a flow which allowed cybercriminals to scrape database of 322 million emails from the cybersecurity firm. The threat actor who claimed to scrape the data, USDoD, alleged the data was compiled by SOCRadar from previous breaches and leaks. The claim is still not confirmed.

VULNERABILITIES AND PATCHES

- Microsoft reported 4 vulnerabilities discovered in OpenVPN, a popular open-source project which is integrated into many IP devices worldwide. The flaws (CVE-2024-27459, CVE-2024-24974, CVE-2024-27903, CVE-2024-1305) could allow attackers to gain local privilege escalation as well as remote code execution. OpenVPN has patched the vulnerabilities in its 2.6.10 version release.

- Google has patched a high-severity zero-day vulnerability (CVE-2024-36971) affecting Android devices. The Linux kernel flaw, seen actively exploited in the wild, allows attackers to remotely execute code on affected devices.

- Akamai researchers discovered vulnerabilities in Ivanti Connect Secure and FortiGate VPNs. The flaws (CVE-2024-37374, CVE-2024-37375) can allow a user initial access to and control over a compromised VPN server. Attackers can use this to manipulate VPN functionalities or intercept sensitive information like external authentication credentials. At the time the report was published, Ivanti have yet to release a patch and Fortinet decided not to fix the custom encryption key bypass.

- Cisco has released an advisory for critical vulnerabilities affecting the Web UI for its SPA300 and SPA500 IP Phones. The flaws (CVE-2024-20450, CVE-2024-20454) allow attackers arbitrary command executions as well as causing a denial-of-service condition. Cisco has announced that it is not planning to fix the vulnerabilities as the products have entered end-of-life.

THREAT INTELLIGENCE REPORTS

- Researchers warn of a large, ongoing Magniber ransomware campaign. The threat actors target home users rather than firms and appear to use trojanized software crack downloaders as an initial attack vector. The ransomware encrypts files on the device and appends a random 5-9 character extension, like .oaxysw or .oymtk, to encrypted file names. The ransom note demands $1,000-$5,000 from each victim.

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

- Researchers have identified a new attack vector that exploits the Windows Update process to downgrade software versions, allowing attackers to reintroduce vulnerabilities that have been patched. The downgrading process bypasses all verification steps, including integrity verification and Trusted Installer enforcement. Downgraded OS presents as fully updated and unable to install future updates, thus rendering the system vulnerable to attacks.

- The Chameleon Device-Takeover Trojan has resurfaced in new campaigns targeting Canada and Europe. The malware, affecting Android devices, now masquerades as a Customer Relationship Management (CRM) app. This campaign was seen targeting hospitality employees, particularly within a Canadian restaurant chain operating internationally. Once installed, Chameleon collects credentials via keylogging and fake login pages, posing significant risks to business banking accounts.