TOP ATTACKS AND BREACHES

- Microsoft disclosed that they detected an attack against their systems by Russian state-sponsored actor known as Midnight Blizzard (aka Nobelium). The threat actor used a password spray attack to compromise a legacy non-production test tenant account and then accessed very small percentage of Microsoft corporate email accounts and exfiltrated some emails and attached documents. The compromised accounts included members of Microsoft senior leadership team and employees in cybersecurity and legal functions.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Win.APT29; APT.Wins.Nobelium)*

- LockBit ransomware gang claimed responsibility for a cyber-attack on Foxsemicon Integrated Technology Inc. (FITI), one of Taiwan's biggest semiconductor manufacturers. The ransomware group allegedly exfiltrated five terabytes of customer data, yet Foxsemicon has not verified if any personal details of its customers or staff were compromised.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Wins.LockBit.ta*; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI, Ransomware_Linux_Lockbit)*

- Anna Jaques Hospital (AJH), which serves thousands of patients in Massachusetts and New Hampshire, has suffered a cyber-attack, which disrupted the electronic health records system and forced the hospital to divert ambulances on Christmas Day. Money Message ransomware group claimed responsibility for the attack, which allegedly resulted in the encryption of related 600GB of data.

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

- The municipality of Calvià in Spain has been a victim of a ransomware attack that resulted in a temporarily halt of all administrative processes. According to the city council, the threat actors have demanded around €10M of ransom, which will not be paid by the municipality.

- The National Bank of Angola, has acknowledged a cyber-attack that resulted in a minor impact on its infrastructure and data. Despite no group taking credit for the attack, researchers found out that an access to bank's systems was offered for sale in 2022 on a cybercriminal forum.

- Kansas State University (K-State) has confirmed a cyber-attack that impacted certain systems in the university's network environment, including VPN, K-State Today email system, and video content on platforms such as Canvas and Mediasite. The impacted systems were taken offline as a precaution.

VULNERABILITIES AND PATCHES

- VMware has addressed a critical vulnerability (CVE-2023-34063, CVSS score of 9.9) in VMware Aria Automation platform. The vulnerability enables an unauthorized access to remote workflows by authenticated attackers with low privileges and without user interaction. VMware has released patches for various affected versions, and there are no known exploitations of this vulnerability.
- Citrix warns of two zero-day vulnerabilities in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) that are being actively exploited in the wild. The first flaw (CVE-2023-6548, CVSS score of 5.5) could allow an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. The second flaw (CVE-2023-6549, CVSS score of 8.2) could allow an unauthenticated Denial of Service.
- Atlassian has patched a critical remote code execution (RCE) flaw (CVE-2023-22527, max CVSS score of 10.0), impacting Confluence Data Center and Confluence Server. A template injection vulnerability on out-of-date versions of Confluence Data Center and Server could allow an unauthenticated attacker to achieve RCE on an affected version.

THREAT INTELLIGENCE REPORTS

- Check Point Research analysis of cyber-attack data across various regions shows that throughout 2023, organizations around the world have each experienced over 60K attacks on average, 1158 attacks per organization per week. The Retail/Wholesale sectors witnessed a notable 22% spike in weekly attacks compared to 2022. Moreover, one out of every ten organizations worldwide was targeted by attempted ransomware attacks, marking a 33% increase from the previous year.
- Check Point Research has revealed an ongoing new and sophisticated NFT scam campaign targeting token holders of over 100 popular projects. The scam involves sending airdrops that appear to be from legitimate sources, such as the Ape NFT airdrop for APE token holders. These airdrops link to specially crafted websites designed to trick victims into connecting their wallets, thereby giving attackers full access to their funds.
- Microsoft has identified a sophisticated cyber campaign conducted by Mint Sandstorm (aka APT35, Charming Kitten) threat actor, linked to Iran's Islamic Revolutionary Guard Corps. Targeting high-profile individuals from Middle Eastern affairs at universities and research organizations, the campaign uses advanced social engineering and custom backdoors like MediaPl and MischiefTut.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Win.APT35; APT.Wins.APT35.ta.*; InfoStealer.Win.CharmingKitten)*