CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Supply chain software provider Blue Yonder was hit by a ransomware attack, disrupting services for clients like Starbucks and UK grocery chains Morrisons and Sainsbury's. The incident affected operations such as employee scheduling and payroll processing. Blue Yonder is collaborating with cybersecurity firms to recover and has informed affected customers.

- Uganda's central bank experienced a cyberattack resulting in the unauthorized transfer of approximately 62 billion Ugandan shillings (around $16.8 million). Whilst the state-owned newspaper 'New Vision' reported that the attack was carried out by a Southeast Asian hacking group identified as "Waste", who allegedly directed portions of the stolen funds to accounts in Japan, independent sources report that insiders within the bank may have been involved with the hackers. Authorities said they have managed to recover over half of the misappropriated money.

- The city of Hoboken, New Jersey, was forced to close its offices temporarily following a ransomware attack. The incident disrupted municipal operations, including public access to essential services. City officials have not confirmed whether any sensitive data was compromised and are working with cybersecurity experts to investigate the breach and restore affected systems.

- Wirral University Teaching Hospital NHS Trust in the UK faced a cyberattack that led to IT system outages, forcing staff to use manual processes and causing delays in patient services. Some scheduled procedures were postponed as cybersecurity experts are working to restore operations.

- Great Plains Regional Medical Center in Oklahoma suffered a ransomware attack in September, compromising data of over 130,000 individuals. The breach involved personal and medical information, including Social Security numbers. The hospital secured its systems, initiated an investigation with cybersecurity experts, and began notifying affected patients.

- International Game Technology (IGT), a global gaming technology provider, experienced a cyberattack. The company took certain systems offline to protect its network and is working with cybersecurity experts to investigate and restore affected services.

- Italian football club Bologna FC confirmed a ransomware attack, claimed by the RansomHub group, resulting in the theft of company sponsorship contracts and personal information of players and staff. The RansomHub group threatened that it will publish all medical, personal and confidential data of the club's players, as the club's management presumably refused to pay the ransom fee.

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

VULNERABILITIES AND PATCHES

- Researchers have detected active exploitation of a critical vulnerability in the file-sharing application ProjectSend (CVE-2024-11680). This flaw allows attackers remote and unauthenticated access to modify configurations, create accounts, upload webshells and embed malicious JavaScript. While a patch for the vulnerability has been available for a year, 99% of ProjectSend instances have not been patched, and are now being exploited.

  Check Point IPS provides protection against this threat *(ProjectSend Authentication Bypass (CVE-2024-11680))*

- WordFence identified a critical vulnerability (CVE-2024-8672) in the WordPress Widget Options plugin, affecting over 100,000 websites. This flaw allows contributors with access to execute arbitrary code via poorly filtered inputs in the plugin's display logic feature. The vulnerability was patched in the recent update.

- Jenkins has published a security advisory addressing vulnerabilities in its products. Two of the vulnerabilities addressed are classified as high severity: CVE-2024-47855 which allowed denial of service in Jenkins core, and CVE-2024-54003, a stored cross-site scripting vulnerability affecting Simple Queue Plugin.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a novel method by which cybercriminals exploit the Godot Engine—a popular open-source game development platform—to execute malicious GDScript code. This technique enables attackers to deliver malware across multiple platforms, including Windows, macOS, Linux, Android, and iOS, while evading detection by most antivirus solutions. Malicious loader, dubbed "GodLoader", which is using this technique has been active since at least June 2024, and is believed to have already infected over 17,000 machines. The distribution of the malware was facilitated through the "Stargazers Ghost Network," a GitHub-based malware-as-a-service operation that leverages numerous repositories and stargazers to lend legitimacy to the malicious content.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Technique.win.GDscript., Dropper.Win.Godot.*)*

- Researchers reported that China-linked APT group, Salt Typhoon, has been targeting Southeast Asian telecommunications firms with a sophisticated new backdoor named GhostSpider. The group exploits web vulnerabilities for initial access and uses legitimate tools for lateral movement, and the malware's modular design allows independent updates, complicating detection and analysis.

- Researchers found that Russia-linked group RomCom has exploited two zero-day vulnerabilities in Firefox and Windows to target victims in Europe and North America. The flaws, CVE-2024-9680 in Firefox and CVE-2024-49039 in Windows Task Scheduler, were chained to achieve remote code execution without user interaction. Victims were redirected to malicious websites, leading to the deployment of the RomCom backdoor for further payloads and command execution.