September 16 - 22, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Medusa ransomware gang has claimed responsibility for an attack on the Providence Public School District (PPSD) in Rhode Island. The school district is still grappling with ongoing internet outages since September 11, impacting over 20,000 students across 37 schools. While the district has contacted law enforcement and federal agencies, it has not confirmed the ransomware claims and has not closed schools.
- American technology company Dell is investigating claims of a data breach after a hacker named "grep" leaked information allegedly belonging to over 10,000 Dell employees and partners. The leaked data includes employee names, unique identifiers, and internal details, with a sample shared for free on a hacking forum. Dell has acknowledged the claims and is currently investigating.
- Singaporean cryptocurrency platform BingX has confirmed a cyber-attack that resulted in the theft of more than $44M. The attack exploited vulnerabilities in BingX's hot wallet, leading to unauthorized network access. Despite the significant financial impact, BingX has pledged to cover all losses using its own capital.
- Pro-Ukraine hackers have claimed responsibility for a cyberattack on Russia's Osnovanie, the federal agency responsible for certifying digital signatures used by businesses and individuals. The attack defaced the agency's websites, displaying a message about using proceeds from the sale of compromised data to support Ukrainian military efforts. Although Osnovanie reported that its digital signature verification system remained intact, the incident disrupted its services across 60 regions. The agency has since suspended operations for investigation and its websites remain unavailable.
- Russian anti-virus company Dr.Web experienced a cyberattack over the weekend, leading the company to disconnect its servers and halt virus database updates. The breach, which began on September 14, was detected and contained, preventing any impact on Dr.Web’s customers. The company resumed virus updates after an investigation, using its security tools to isolate the threat.
- A ransomware attack on Radio Geretsried, a radio station in Germany, has disrupted its regular programming, forcing it to broadcast music from emergency backups. The attackers, believed to be from Russia, encrypted the station’s music files and are demanding a large ransom. The station’s team is working to recover what data they can and restore operations.
- Access Sports, a New Hampshire orthopedic service provider, has reported a data breach affecting over 88,000 individuals following a ransomware attack by the group Inc Ransom. Discovered on May 10, 2024, the breach revealed unauthorized access to sensitive data, including names, Social Security Numbers, financial information, and medical records.

VULNERABILITIES AND PATCHES

- Mozilla Foundation has issued an update to patch vulnerability CVE-2024-8897. The flaw allows an attacker to redirect users to a malicious site via an open redirect. This can result in address bar contents spoofing, pretending a malicious site to have the same URL as a trusted site.
- VMware has addressed two critical-severity vulnerabilities (CVE-2024-38812 and CVE-2024-38813), found in its vCenter Server and VMware Cloud Foundation products. These vulnerabilities could enable attackers to execute remote code and gain elevated privileges.
- StarkeBlog has released a technical analysis of a critical-severity vulnerability, CVE-2024-20439, affecting the Cisco Smart Licensing Utility. This vulnerability involves a hardcoded static password in the system's administrative account that is undocumented and static. An unauthenticated, remote attacker could exploit this by using the static credentials to log in with administrative privileges over the API of the Cisco Smart Licensing Utility application. Successful exploitation would grant the attacker full administrative access to the affected system.
- Horizon3 shared a technical analysis of CVE-2024-8190, a high-severity command injection vulnerability in Ivanti Cloud Service Appliance (CSA). The vulnerability allows remote authenticated attackers to execute arbitrary commands due to insufficient input validation, primarily affecting improperly configured dual-homed CSA devices.

  Check Point IPS provides protection against this threat (Ivanti Cloud Services Appliance Command Injection (CVE-2024-8190))

THREAT INTELLIGENCE REPORTS

- Check Point Research has identified a significant increase of 32% in cyberattacks targeting healthcare organizations, with a global average of 2,018 attacks per week per organization between January and September 2024. The APAC region leads in attack volume, while Europe saw the largest percentage increase. Ransomware is a major threat, with cybercriminals exploiting vulnerabilities, trading patient data, and using ransomware-as-a-service (RaaS) to launch attacks.
- Check Point has uncovered a new phishing campaign exploiting Google Apps Script macros to target organizations. The campaign involves around 360 emails in various languages, tricking recipients into clicking a deceptive link in the subject line, which leads to a fake Google Apps Script page. The phishing emails claim to provide account details for a false registration, posing risks such as data exposure, financial fraud, and operational disruption.
- Researchers reported on a cyber operation known as UNC1860, linked to Iran’s Ministry of Intelligence and Security (MOIS), which acts as an initial access broker for Iranian hackers targeting telecommunications and government organizations across the Middle East. The group has developed a suite of tools and passive backdoors that facilitate stealthy access to systems, enabling various operations from espionage to network attacks.