September 9 - 15, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The Port of Seattle has confirmed that the Rhysida ransomware group was responsible for a cyberattack in August 2024, which affected its critical systems, including Seattle-Tacoma International Airport. The ransomware attack caused major service disruptions, including outages in check-in systems, baggage handling, and the Port's website. The Port declined to pay the ransom.

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

- Fortinet cybersecurity firm confirmed a data breach involving 440GB of files stolen from its Microsoft SharePoint server by a threat actor active on a popular cybercrime forum. While the event did not include data encryption or access to the company's corporate network, attempts to extort a ransom from Fortinet were made and the company refused payment. Reportedly the breach involved a small amount of customer data stored on a third-party cloud-based shared file drive.

- The Highline Public Schools in Washington state experienced a significant disruption due to a cyber-attack that led to the closure of facilities and cancellation of activities. The incident, which has not been claimed by any group, involves ongoing investigations with federal and state law enforcement involvement to address the unauthorized network activities impacting critical systems.

- Several French retail companies, including Boulanger and Cultura, confirmed that customer data was stolen in a cyberattack by a threat actor active on a popular cybercrime forum. The stolen data includes customer names, addresses, and contact details but no banking information. Cultura has since reported they've located and patched the vulnerability exploited in the attack.

- Kadokawa, a Japanese media company involved in manga, anime, and video games, is dealing with an additional data leak following an alleged BlackSuit ransomware attack that occurred in June. BlackSuit has now leaked sensitive company data, including contracts and employee information.

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

- The BlackSuit ransomware gang has claimed responsibility for an attack on Charles Darwin School, resulting in the theft of sensitive student data. The group has reportedly stolen confidential information, including student personal records.

- The Free Russia Foundation, a U.S.-based nonprofit, is investigating a data breach linked to the Kremlin-linked hacker group Coldriver. Thousands of emails and documents were exposed online, likely including sensitive strategic and financial data. The breach aims to intimidate and suppress pro-democracy advocates, aligning with ongoing Russian government cyber-espionage efforts.

## VULNERABILITIES AND PATCHES

- Microsoft's September 2024 Patch Tuesday has addressed 79 vulnerabilities, including four zero-days, of which three actively exploited in the wild. Two of the critical/high vulnerabilities, a Windows Update remote code execution flaw (CVE-2024-43491) and a privilege escalation vulnerability in Windows Installer (CVE-2024-38014), were highlighted as priorities for patching. The update also resolves multiple elevation of privilege and remote code execution flaws across several Windows components and Microsoft products.

- Ivanti has released fixes for a critical Remote Code Execution (RCE) vulnerability (CVE-2024-29847) in its Endpoint Manager (EPM) software, an enterprise endpoint management solution that allows for centralized management of devices within an organization. The flaw is caused by improper deserialization of untrusted data. A PoC has since been shared, increasing potential risk.

- Ivanti has confirmed the active exploitation of a high-severity vulnerability (CVE-2024-8190) in its Cloud Services Appliance (CSA), which allows remote code execution. This flaw affects CSA versions 4.6 through command injection and has prompted CISA to add it to its Known Exploited Vulnerabilities catalog, requiring patches by federal agencies by October 4.

- A privilege escalation vulnerability (CVE-2024-8253) exists in the Post Grid and Gutenberg Blocks WordPress plugin, affecting over 40,000 sites. The vulnerability, now patched, allows authenticated users with minimal permissions to escalate their privileges to administrator.

## THREAT INTELLIGENCE REPORTS

- Check Point Research have identified a cyber campaign by Iranian threat actors using malware named Veaty and Spearal to target Iraqi government networks. Techniques used include a passive IIS backdoor, DNS tunneling, and C2 communication via compromised email accounts, suggesting ties to the APT34 group, linked to the Iranian MOIS. The campaign likely employs social engineering for initial infection and sophisticated C2 infrastructure.

  *Check Point Threat Emulation and Harmony Endpoint provide protection against this threat*
  *(APT.Wins.Oilrig.ta.B/C/D/E, APT.Win.OilRig.F, APT.Win.OilRig.WA.G, APT.Win.OilRig.H)*

- Check Point has released its Global Threat Index for August 2024 discussing top ransomware, malware and exploited vulnerabilities. The report reveals that RansomHub has reached the top of the ransomware families, and that Meow ransomware marked a notable rise through innovative extortion tactics. At the top of the malware families list, FakeUpdates is the most prevalent with an impact of 8% worldwide organizations, followed by Androxgh0st and Phorpiex.

- Researchers have detected a resurgence of Operation Crimson Palace, a Chinese state-sponsored cyberespionage campaign targeting governmental and public service organizations in Southeast Asia. This operation utilizes a new keylogger named "TattleTale" and leverages compromised networks as command-and-control relay points to expand its espionage activities in the region.