CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The International Criminal Court (ICC) disclosed a sophisticated cyber-security incident in late June 2025, its second such event in recent years. The intrusion, which occurred in June 2025, was promptly detected and contained, and the full extent of the impact is under investigation.
- Australian airline Qantas suffered a cyber incident after attackers targeted an offshore call center and accessed a third-party customer service platform, affecting records of up to 6 million customers. Stolen data includes personal data and frequent flyer numbers. Qantas contained the incident, notified authorities and customers, enlisted forensic teams, and is enhancing support and security.
- Ingram Micro, an American distributor of information technology products and services, was hit by a ransomware attack that resulted in the shutdown of internal systems, including its website, online ordering platforms, the Xvantage distribution platform, and the Impulse license provisioning platform. The ransomware gang SafePay claimed responsibility for the attack.
- Spanish telecom provider Telefónica suffered a possible cyber-attack by a threat actor affiliated with the Hellcat ransomware gang. The threat actor claims to exfiltrate 106 GB of sensitive internal data, including more than 385,000 files. The data includes information related to employees and business clients tied to European and Latin American subsidiaries.
- Gloucester County, Virginia, fell victim of a ransomware attack that resulted in the theft of sensitive information belonging to 3,527 current and former government employees. The attack led to significant personal data exposure, including Social Security numbers, bank account details and medical information. The BlackSuit ransomware gang claimed responsibility for the incident after the county reportedly refused to negotiate a ransom.
- The Swiss health-promotion non-profit Radix confirmed it was hit by a ransomware attack, resulting in data theft and encryption. The group's clients include various federal administration offices, whose data was stolen and published on the dark web.
- German charity organization Welthungerhilfe was targeted by a ransomware-as-a-service group demanding 20 BTC ($2.1 million) for stolen data. The organization refused to pay, shut down affected systems, and engaged cybersecurity experts. Humanitarian operations remain unaffected while authorities investigate the incident.
- Columbia University has suffered a data breach that resulted in the theft of up to 460 gigabytes of sensitive information after a hacktivist with a political agenda accessed targeted IT systems. The stolen data reportedly includes at least 1.8 million Social Security numbers belonging to employees, applicants, students, and their family members.

VULNERABILITIES AND PATCHES

- Wordfence disclosed a High-severity vulnerability (CVE-2025-6463) in the Forminator WordPress plugin. Exploitation of unauthenticated arbitrary file deletion flaw could allows attackers to delete any file on the web server, including critical files like wp-config.php, potentially resulting in remote code execution and full site compromise.

- Citrix has published an advisory addressing two vulnerabilities in NetScaler ADC and NetScaler Gateway. CVE-2025-5349 is an Improper access control in the management interface, while CVE-2025-5777 is a memory over-read flaw due to insufficient input validation when configured as a Gateway. While no active exploitation has been confirmed, the severity and public exposure warrant urgent patching, as both flaws are considered critical and allow access to sensitive data.

  Check Point IPS provides protection against this threat *(Citrix NetScaler Out-of-Bounds Read (CVE-2025-5777))*

- Researchers have discovered a critical remote code execution vulnerability in Wing FTP Server (CVE-2025-47812). The flaw allows attackers to bypass authentication using a null-byte injection in the username, resulting in successful logins without valid credentials. The issue, found following anonymous access fuzzing, grants access to authenticated user privileges via the UID cookie

  Check Point IPS provides protection against this threat *(Wing FTP Server Remote Code Execution)*

THREAT INTELLIGENCE REPORTS

- Check Point Research have uncovered a surge in cybercrime activity targeting Amazon Prime Day 2025, with over 1,000 new domains resembling Amazon appearing in June—87% of which are flagged as malicious or suspicious. The fraudulent domains are designed to harvest login credentials via phishing pages that mimic legitimate Amazon sign-in portals, aimed to lure victims into entering personal information or payment details on fake websites.

- Researchers analyzed the “Scattered Spider” financially motivated cybercriminal group. The threat actor targets individuals rather than exploiting software vulnerabilities directly, employing social engineering and living-off-the-land techniques to penetrate organizations across telecom, gaming, transportation, and retail.

- The Hunters International ransomware group announced it is shutting down, providing free decryption tools to previous victims, though their effectiveness is questioned by incident responders. Researchers say that the group is transitioning to operate as an extortion-only platform known as World Leaks, with strong operational and code similarities to Hive ransomware.

- Researchers have discovered “RondoDox,” a sophisticated botnet that infects TBK DVRs and Four-Faith routers by exploiting CVE-2024-3721 and CVE-2024-12856. After gaining access, the malware covertly establishes persistence, disguises its traffic as gaming or VPN packets, downloads additional payloads via secure connections, and enables devices to launch distributed denial-of-service (DDoS) attacks.