TOP ATTACKS AND BREACHES

- Following ransomware gang INC claim about an attack on Xerox, the company's subsidiary, Xerox Business Solution (XBS), confirmed having suffered a cyber-attack. Xerox spokesperson said that although personal data from XBS may have been compromised, the attack was contained and did not affect any Xerox corporate systems, data, or operations.

- The Victoria court system in Australia has been compromised by a cyber-attack, most likely perpetrated by Russian ransomware gang Qilin. Reportedly, hackers were able to gain access to two-months' worth of the court system's audio-visual archive; this means data from testimonies and hearings, including highly sensitive materials, was stolen and could now be leaked.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Wins.Qilin)*

- A major Swedish supermarket chain, Coop, was hit by a cyber-attack during the Christmas holiday. The attack rendered the company's card payment services unavailable and caused problems to the Coop website. The Cactus ransomware gang claimed responsibility for the attack.

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

- Beckley, West Virginia, was hit by a cyber-attack, with city officials working to investigate and mitigate the incident's impact on their computer network. Details about the incident, including the involvement of ransomware or the identity of the threat actor, are yet to be disclosed.

- Mandiant, had its X (formerly Twitter) account hacked and hijacked by cryptocurrency scammers. The attackers modified the Mandiant account to impersonate the Phantom crypto wallet, and posted links to a Phantom phishing website, luring victims in by claiming to award them with free token – only to then drain their wallets.

- American Health management solutions provider, HealthEC LLC, suffered a major data breach, affecting the data of approximately 4.5 million people. Compromised personal information includes names, addresses, DOB, SSN, medical and billing information, health insurance details and more.

- Hackers have disrupted Orange Spain users' internet connectivity. The threat actor known as Snow on X (formerly Twitter), claimed responsibility for the company's breached RIPE account. The attacker hijacked the Border Gateway Protocol (BGP) and misconfigured the routing to IP addresses, known as BGP hijacking. Orange Spain said no customer data was compromised.

VULNERABILITIES AND PATCHES

- Ivanti patched a critical Remote Code Execution vulnerability in its Endpoint Management Software (EMS). Tracked as CVE-2023-39336, the security flaw allows an attacker with access to the victim's internal network to leverage SQL injection to execute arbitrary SQL queries and retrieve output without need for authentication. The Ivanti EMS helps manage devices running a wide range of platforms, including Windows, macOS and more.

- Juniper has issued a security advisory addressing multiple vulnerabilities in Juniper Secure Analytics (Affected platforms: JSA Series Virtual Appliance). If exploited, threat actor could exploit these vulnerabilities to gain control of the affected system. Two critical flaws are included in the advisory, Remote Code Execution vulnerability (CVE-2023-46604), and SQL injection vulnerability (CVE-2023-40787), both ranked at 9.8 CVSS.

THREAT INTELLIGENCE REPORTS

- Researchers detected a new attack method, in which victims of ransomware groups are approached by threat actors for follow-on extortion attempts. A victim of the ransomware gang Akira was approached by a cybercriminal that claimed to have access to servers where the exfiltrated data was stored. A similar case was observed in an organization compromised by Royal Ransomware; the so-called Ethical Side Group (ESG) who presented itself as legitimate security researchers, offered to hack the group's servers to remove the organization's stolen data. The payment demands were minimal, and both cases presented many similarity points, including offering proof of access to the stolen data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Royal, Ransomware.Win.Akira.A; Trojan.Win.Krap.gl.D)*

- Researchers have uncovered a new macOS backdoor named SpectralBlur. The malware is attributed to North Korean threat actors, displaying capabilities such as file upload and download, shell execution, and configuration updates. SpectralBlur signifies an escalating trend of North Korea-linked operations targeting macOS, particularly within the cryptocurrency and blockchain sectors.

- Researchers uncovered a phishing campaign targeting Ukrainian government entities with malicious documents disguised as Israel Defense Forces (IDF) consultancy job offers, that actually contain the RemcosRAT, a well-known surveillance and control malware often used in cyber-espionage operations. The attack is attributed to Russia-linked APT UAC-0050.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(RAT.Win.Remcos)*