TOP ATTACKS AND BREACHES

- Stanford University experienced a data breach in which files containing Economics Ph.D. program admission information were leaked. Personal and health information of 897 applicants might have been exposed.
- Dish Network, a major American TV and satellite broadcast provider, had been experiencing an unexplained outage with its websites and apps. Shortly after, the company's employees detected suspicious activity on their desktops and reported it as a cyberattack.
- Canadian telecom TELUS is investigating a potential data breach after a threat actor allegedly stole employee data and source code and shared samples online. So far, no corporate or retail customer data has been reported stolen.
- Dole Food Company, a major American producer and distributor of fresh fruits and vegetables, has confirmed a ransomware attack that disrupted its operations. The company is assessing the situation to determine the extent of the incident, while also notifying law enforcement authorities.
- Russian state hackers have breached multiple government websites in Ukraine by exploiting backdoors that were planted as early as December 2021. CERT-UA, the Computer Emergency Response Team of Ukraine, identified the attacks after finding a web shell on one of the compromised sites. This web shell allowed the hackers, who go by the names UAC-0056, Ember Bear, or Lorec53, to install more malware.
- An ongoing malware campaign targets YouTube and Facebook users, infecting their computers with a new information stealer dubbed S1deload that will hijack their social media accounts and use their devices to mine for cryptocurrency.
- The founders of Forsage, a decentralized finance (DeFi) investment platform, have been indicted for running a $340 million Ponzi and pyramid scheme.
- Hydrochasma, a new cybercriminal group, targets COVID-19 research labs and shipping firms. The group make use of open-source tools and "living off the land" tactics to steal intelligence and evade detection. Researchers have been tracking them since October 2022, but attribution is proving difficult.

VULNERABILITIES AND PATCHES

- VMware has released patches to address a critical security vulnerability (tracked as CVE-2023-20858, CVSS score of 9.1), affecting its Carbon Black App Control product.
- Proof of Concept for CVE-2023-21839 in the Oracle WebLogic Server product has been released. This vulnerability would allow for unauthenticated attacker to gain network access via T3, IIOP.
- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) updated its Known Exploited Vulnerabilities catalog with three security flaws that are currently being actively exploited. The list includes a code execution vulnerability in IBM Aspera Faspex (CVE-2022-47986, CVSS score: 9.8) and two vulnerabilities in Mitel MiVoice Connect, including a code injection vulnerability (CVE-2022-41223, CVSS score: 6.8) and a command injection vulnerability (CVE-2022-40765, CVSS score: 6.8).

THREAT INTELLIGENCE REPORTS

- One year into the Russia-Ukraine war, Check Point Research marks September 2022 as a turning point, as weekly cyber-attacks against Ukraine decreased by 44%, while cyber-attacks against some NATO countries increased by nearly 57%. Further analysis of this year lists wipers and hacktivism as key trends.
- Dariy Pankov, a Russian citizen accused of creating and selling the NLBrute password-cracking tool, was extradited from Georgia to the US after his arrest in October 2022. Pankov, also known as dpxaker, is charged with access device fraud and computer fraud, carrying a maximum sentence of 47 years in federal prison.
- Researchers have found a new threat actor using an evasive Discord campaign to target government entities. PureCrypter downloader and a compromised non-profit organization's domain are used to deliver various malware types, including Redline Stealer and Philadelphia Ransomware.
- As OpenAI introduced of a paid ChatGPT tier called ChatGPT Plus, threat actors are now offering so called free access to the platform, luring users to download malicious apps or visit phishing websites.
- Dutch police has arrested three men aged 18 to 21 for ransomware activity. The suspects are accused of extorting small and large organizations in multiple countries and making €2.5 million in the process.
- HardBit ransomware has evolved to version 2.0 and its operators are now manipulating insurance policies to maximize ransom payments. The attackers persuade victims to reveal their insurance details, allowing them to tailor their ransom demands to ensure the costs are fully covered.

  Check Point Threat Emulation provides protection against this threat *(Virus.Wins.Neshta.M; Trojan.Wins.Imphash.P)*