30th October – Threat Intelligence Report

research.checkpoint.com/2023/30th-october-threat-intelligence-report/

October 30, 2023

For the latest discoveries in cyber research for the week of 30th October, please download our Threat_Intelligence Bulletin.

TOP ATTACKS AND BREACHES

> Stanford University has been a victim of cyber-attack that affected the systems of its Department of Public Safety (SUDPS). Akira ransomware gang claimed responsibility for the attack, which allegedly resulted in the exposure of 430GB of university's data.

Check Point Harmony End Point and Threat Emulation provides protection against this threat (Ransomware_Linux_Akira; Ransomware.Wins.Akira)

- Ukrainian hacktivists groups dubbed KibOrg and NLB in collaboration with the Ukraine Security Services (SBU) have breached the Russia's largest private bank Alfa-Bank. The threat actors claimed to have obtained the private information of more than 30M clients, including full names, dates of birth, account numbers, and phone numbers.
- The University of Michigan has disclosed a data breach that affected the personal information of an unverified amount of students, applicants, employees and others. The threat actors have gained access to the university servers between August 23-27, and have stolen Social Security numbers, driver's license numbers, government IDs, payment card numbers, as well as healthcare information.

- The University of Tokyo has experienced a data breach that impacted the personal information of students from the academic years of 2003 to 2022. The exposed data consists of more than 4K files containing addresses and grades, which were leaked as a result of malware infection that was distributed from a faculty member's email.
- The city of Philadelphia has confirmed a data breach that may have affected some individuals' private information. The threat actors accessed the city's email system for a period of two months, and potentially obtained sensitive healthcare data stored in the email accounts.
- Victorville city in California, has been a victim of a data breach that exposed the personal information of an unverified amount of individuals. The threat actors gained access to certain files within the city's network which include Social Security numbers, driver's license numbers, state ID card numbers, medical information, and health insurance policy numbers.
- The Clark County School District (CCSD) in Nevada has suffered a data breach occurred due to an unauthorized access to the district's email servers. The attackers accessed personal information related to a subset of students, parents, and employees. The data potentially includes student photos, addresses, student ID numbers, and email addresses. Security researchers found that SingularityMD threat group is behind the breach and have already begun to leak the data.

VULNERABILITIES AND PATCHES

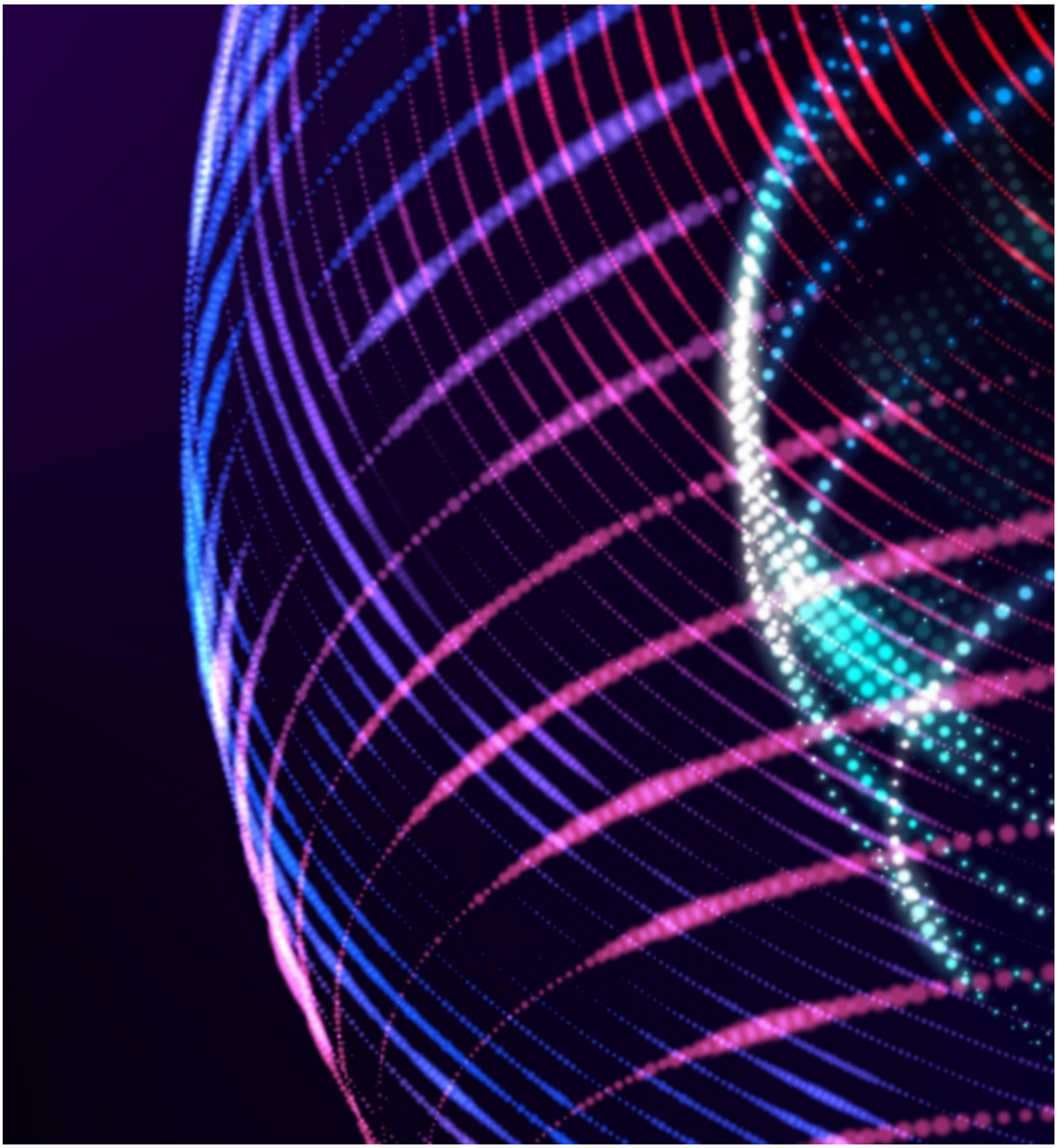
- Apple has released security patches for a variety of products, including iOS and iPadOS 17.1, macOS Sonoma 14.1, watchOS 10.1, and others. Among them is a high severity single kernel-level security flaw (CVE-2023-32434) that could be exploited to execute arbitrary code with kernel privileges.
- A medium severity vulnerability (CVE-2023-4372) in the LiteSpeed Cache plugin could allow attackers to inject malicious code into WordPress websites. The plugin is used by over 4M WordPress websites, making it a popular target for attackers.
- F5 has addressed security hotfixes for a critical unauthenticated RCE vulnerability (CVE-2023-46747) in the F5 BIG-IP configuration utility. The vulnerability can be exploited without authentication in low-complexity attacks, and could allow an attacker with remote access to the configuration utility to perform unauthenticated remote code execution.
- Researchers have observed a 0Auth vulnerability that can affect popular apps such as Grammarly, Vidio and Bukalapak. The vulnerability could allow an unauthorized access to users' accounts.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on a 3% uptick in average weekly global cyberattacks in first three quarters of 2023, compared to the corresponding period in the previous year. One in every 34 organizations globally encountered a ransomware attack attempt, marking a 4% increase compared to the same timeframe last year. Additionally, the global healthcare sector faced an average of 1613 attacks per week, indicating a substantial 11% year-over-year surge, and APAC was the most heavily attacked region with a substantial 15% YoY increase.
- Check Point shares cybersecurity predictions for 2024 that broadly fall into seven categories: Artificial Intelligence and Machine Learning; Cloud GPU farming; Supply chain and critical infrastructure attacks; cyber insurance; nation state attacks; weaponized deepfake technology and phishing attacks.
- Researchers revealed how attackers could leverage Hugging Face, the popular AI development and collaboration platform, to carry out an AI supply chain attack that could impact tens of thousands of developers and researchers. The attack could lead to remote code execution and hijacking of heavily used models and datasets from Hugging Face with over 100K downloads.
- Researchers share a deep technical dive into Cactus ransomware. The ransomware, which was discovered in March 2023, has been observed creating a mutex to improve infection, and maintaining persistence using a scheduled task named “Updates Check Task”.

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

GO UP
BACK TO ALL POSTS



SUBSCRIBE TO CYBER INTELLIGENCE REPORTS