Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Nissan has revealed that the Akira ransomware attack from December 2023 has compromised the personal information of approximately 100K individuals in Australia and New Zealand. The data concerns customers, dealers and some of the employees. The breach resulted in unauthorized access to Nissan's local IT servers, with up to 10% of affected individuals having government identification documents compromised, including Medicare cards, driver's licenses, passports, etc.

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

- France's unemployment agency has disclosed that information of 43 million people has been leaked due a cyber-attack on the agency. According to reports, information of every person who has been registered on the agency in the past 20 years has been exfiltrated.

- U.S. based TV streaming service Roku has confirmed that over 15K user-accounts were breached via a credential stuffing attack and then used for fraudulent hardware purchases. The stolen accounts were sold for as little as $0.50 each, exploiting stored credit card information for illegal transactions.

- The LockBit ransomware gang claimed responsibility for a cyberattack on the South African Government Pensions Administration Agency in February 2024. This incident disrupted the organization's operations and affected pension payments.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.LockBit.ta; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI, Ransomware_Linux_Lockbit)*

- Birmingham, Alabama, is grappling with a network outage affecting government services for over a week, attributed to a cyberattack. The city is manually processing transactions, causing delays in services like license renewals and new business applications.

- MarineMax, a leading boat seller, reported a cyberattack after an unauthorized access was detected in its information environment. Immediate containment measures caused some business disruptions, but operations continued, with no sensitive data compromised.

- The International Monetary Fund (IMF) disclosed an investigation into a cyber security incident detected on February 16, impacting 11 IMF email accounts, excluding those of top officials. Immediate actions re-secured the compromised accounts, with ongoing investigations to prevent further breaches.

VULNERABILITIES AND PATCHES

- Microsoft's March 2024 Patch Tuesday disclosed 60 vulnerabilities, including two critical issues within Windows Hyper-V that could allow an adversary to compromise a host machine from a virtual machine environment. Two highlighted vulnerabilities are a denial-of-service vulnerability (CVE-2024-21408) and a remote code execution flaw (CVE-2024-21407). Another significant vulnerability (CVE-2024-21334) concerns Open Management Infrastructure, allowing unauthenticated internet-based exploitation.
- Adobe fixed vulnerabilities in multiple products, including Critical vulnerabilities in ColdFusion, Bridge, and Lightroom. Critical vulnerabilities in Adobe Bridge have also been addressed, including arbitrary code execution vulnerabilities (CVE-2024-20756, CVE-2024-20755, and CVE-2024-20752).
- Fortinet addressed a critical SQL injection vulnerability (CVE-2023-48788) in its FortiClient Enterprise Management Server software. This flaw could allow unauthenticated attackers to execute code with SYSTEM privileges on affected servers without user interaction. Fortinet has patched the vulnerability affecting specific versions of FortiClient EMS.
- Researchers report on security flaws in the plugin platform for ChatGPT, which could allow an attacker to gain access to sensitive content. Attackers can send links to ChatGPT chats that have custom plugins enabled, which can be used to send any information back to the attacker.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released its February 2024's Most Wanted Malware report. It highlighted a new campaign with FakeUpdates, also known as SocGolish, targeting and compromising WordPress websites with hacked admin accounts. CPR also highlights Play ransomware's entrance to the top three of most active ransomware groups, while education remains the most attacked sector worldwide.
- Check Point Harmony Email researchers highlight the emergence of phishing attacks leveraging Venmo, a popular payment app, where threat actors send fake payment notifications with scam phone numbers attached. These emails appear legitimate, passing SPF and DKIM checks, making them harder to detect.
- Researchers have identified a new ransomware gang named "Donex," employing a capable Windows-based encryptor targeting various business sectors. Its encryptor features include local and network file encryption, event log clearance, and the use of common Windows service APIs and system commands.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Wins.DoNex.ta.A)
- Researchers have spotted malicious campaigns targeting Chinese users with trojanized Notepad++ and VNote versions via search engine malvertising. The Linux and macOS-targeted apps carry backdoors for unauthorized remote access, resembling the Geacon project connected to CobaltStrike and BeaconTool.