October 30 – November 5, 2023

Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Boeing has acknowledged that a cyber-attack had affected its parts and distribution business, and that the company is working with law enforcement to investigate. Earlier this week, ransomware group LockBit has added Boeing to its victim page and claimed to have stolen large amounts of data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Lockbit, Ransomware_Linux_Lockbit)

- Allied Pilots Association (APA), a union representing more than 15,000 American Airlines pilots, has been suffering a ransomware attack that encrypted part of APA systems. Currently, it is not clear whether pilots' personal information was compromised in the attack.

- A ransomware attack on German IT provider Südwestfalen IT has caused widespread services disruption of more than 70 municipalities in Germany, as the firm shut down its servers to prevent the ransomware from spreading. The group behind the attack is not yet known.

- Long lasting distributed-denial-of-service (DDoS) attacks have affected the Singapore based Synapxe, which oversees almost fifty public healthcare institutions. The attacks, which lasted about 7 hours, resulted in disruptions to internet connectivity and prevented users from accessing the websites of healthcare organizations, including Singapore General Hospital.

- BlackCat (ALPHV) ransomware claims to have breached healthcare solutions provider Henry Schein and to have stolen 35TB of data, including payroll data and shareholder information. Despite disruption to some of its business operations, the company states its management software remains unaffected.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.BlackCat, Ransomware_Linux_BlackCat)

- The Toronto Public Library, Canada's largest public library system, was hit by a ransomware attack, forcing it to close all of its branches and suspend online services. The Black Basta ransomware gang is suspected to be responsible for the attack.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.BlackBasta)

- Ransomware group Daixin Team has begun leaking information exfiltrated from TransForm, a Canadian firm operating 5 hospitals in Ontario, Canada. The ransomware group claims to have stolen 5.6M record database which contains personal and medical information of the hospitals' patients.

VULNERABILITIES AND PATCHES

- Atlassian issued an urgent security advisory to address a critical vulnerability (CVE-2023-22518) in all versions of Confluence Data Center and Server. The company urges to immediately patch Internet-exposed Confluence instances as attackers can exploit this flaw and cause significant data loss.
- A vulnerability has been revealed in Apache ActiveMQ (CVE-2023-46604), which could allow remote code execution in unpatched versions. The flaw is being actively exploited by HelloKitty ransomware group to deploy ransomware on victim systems.

  Check Point IPS and Threat Emulation provide protection against this threat (Apache ActiveMQ Remote Code Execution (CVE-2023-46604), Ransomware.Wins.HelloKitty.ta)

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed an ongoing espionage campaign of Scarred Manticore - threat actor tied to the Iranian Ministry of Intelligence and Security (MOIS). The attacks rely on LIONTAIL, an advanced passive malware framework installed on Windows servers. The current campaign is targeting high-profile organizations in the Middle East, focusing on government, military, and telecommunications sectors.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Backdoor.WIN32.Liontail.A/B, APT.Wins.Liontail.C/D)

- Check Point Research released a recent review of the evolving cyber events in light of the Israel-Hamas war. The recent weeks revealed that pro-Palestinian hacktivist groups have broadened their scope beyond Israel, mainly targeting countries perceived as Israeli allies. These cyber operations aim to have informational and retaliatory effect, however, have limited reported damage. Notably, the target choice is set by the groups' previously established interests, in addition to evolving geopolitical events.
- Researchers have analyzed BiBi-Linux, a wiper that can completely wipe infected Linux systems and is targeting Israeli companies. Later findings have also revealed a Windows variant of the same malware. This group started attacking Israeli organizations with the beginning of the Israel-Hamas war.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware_Linux_Bibi, Ransomware.Win.BiBiWiper.A, Trojan.Wins.Generic.R, Trojan.Wins.IronSwords.ta.G)

- Researchers observed a new and upgraded variant of Kazuar, the stealthy and advanced .NET backdoor used by the Russia affiliated threat group Pensive Ursa (aka Turla, Uroburos). Kazuar malware is usually used as a second stage payload and exhibits robust code and string obfuscation and protection.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Trojan.Win.Kazuar.A)