October 31 – November 6, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Two European automotive companies were hit by ransomware - The German multinational group Continental was hit by LockBit ransomware gang and the breached data has been published on Lockbit's leak site. Italian company Landi Renzo was breached by Hive.

  Check Point Harmony Endpoint, Anti-Bot and Threat Emulation provide protection against these threats (Ransomware.Win.Lockbit; Ransomware.Hive.A; Ransomware.Wins.Hive.ta.B)

- OPERA1ER threat group has stolen at least $11 million over the course of four years from banks and telecommunication service providers in Africa, using evolving TTPs and off-the-shelf hacking tools.

- IT Army of Ukraine claim to have gained access to Russia's Central Bank. They published 27K of the leaked files, containing personal, legal, and financial data.

- German company Aurubis, the second largest copper producer globally, has been hit by a cyberattack forcing it to shut down some of its IT systems.

- Researchers have spotted new TTPs used by the Chinese threat group APT10 in their operations against high-interest Japanese targets, as they install a new version of the LODEINFO malware.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Win32.LODEINFO.)*

- Dropbox was victim of a phishing attack, in which threat actors successfully accessed company code stored in GitHub. Customer data and payment information was not accessed.

- A cyber-attack stopped train service of DBS - the largest train operating company in Denmark, after the Danish company Supeo, which provides enterprise asset management solutions to railway companies, was breached at end of October.

- Threat group DDoSecrets released a batch of almost 20,000 records from a hack of Innwa Bank owned by the Myanmar Economic Corporation (MEC), giving insight into the secretive bank, which is under US, UK and EU sanctions.

- A total of four malicious applications available in Google Play, with already over 1 million installs, are leading users to phishing sites that steal sensitive information or generate 'pay-per-click' chain.

  Check Point Harmony Mobile provides protection against this threat

VULNERABILITIES AND PATCHES

- OpenSSL has patched two high-severity security flaws (CVE-2022-3602 and CVE-2022-3786) in its open-source cryptographic library used to encrypt communication channels and HTTPS connections. Both vulnerabilities affect OpenSSL version 3.0.0 and later and have been patched in OpenSSL 3.0.7.

  Check Point IPS provides protection against this threat (OpenSSL Buffer Overflow (CVE-2022-3602))

- Fortinet disclosed an improper access control vulnerability in FortiOS (tracked CVE-2022-38380) that may allow a remote authenticated read-only user to modify the interface settings via the API.
- Researchers revealed a critical authentication bypass vulnerability in Jupyter Notebooks for Microsoft Azure Cosmos DB, which could have allowed attackers to achieve remote code execution on containers.
- Researchers have found vulnerabilities in Apache Batik default security controls that could lead to server-side request forgery and RCE through remote class loading.

THREAT INTELLIGENCE REPORTS

- After nearly a four-month break, the Emotet malware operation is active and back to spamming email addresses worldwide, using stolen email reply chains to distribute malicious Excel attachments. Emotet now also tricks victims into enabling macros by asking to move the file to a trusted folder.

  Check Point Harmony Endpoint, Threat Emulation and IPS provide protection against this threat (Trojan.Wins.Emotet.; Worm.Win.Emotet.*; Emotet Exploit Kit Landing Page; Emotet Maldoc Download Page; Dropper.Win.GenDrop.la.E)*

- Researchers have linked the Black Basta ransomware operation to the financially motivated hacking group FIN7, AKA "Carbanak", as its developers authored evasion tools used exclusively by Black Basta, and as the two share certain indicators of compromise and specific TTPs.

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

- A new technical analysis of the ChromeLoader malware has been published, demonstrating how it infects the browser in order to later download malicious Chrome extensions.
- Researches dived into the TTPs of the notorious Qakbot malware (also known as QBot, QuakBot or Pinkslipbot) infection, with in-depth details of different functionalities and collaborations with Black Basta ransomware group.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (qbot.TC.; Trojan.Wins.Qbot.*; Trojan.Win32.Qakbot.*; Banker.Win.Qbot.*; Ransomware.Win.BlackBasta.*)*