TOP ATTACKS AND BREACHES

- US-based communications company Twilio has disclosed a new data breach that occurred on June 2022 allegedly by the same threat actors behind the August hack. The hackers have used voice phishing to trick a Twilio employee into handling over their credentials, which the hackers then used to access customer information.

- Cuba ransomware is targeting Ukrainian Government agencies via phishing emails that impersonate the Press Service of the General Staff of the Armed Forces of Ukraine in an attempt to make recipients click on attached links and download the payload.

  Check Point Harmony Endpoint and Threat Emulation provides protection against this threat (Ransomware.Wins.Cuba.)*

- Quantum ransomware gang has taken responsibility for a data breach at Australian Clinical Labs (ACL) that took place in February 2022. The threat actors were able to steal and leak data including medical records, full names, and credit card numbers.

- Hive ransomware gang has claimed responsibility for a cyberattack reported by Indian Power Company Tata Power earlier this month. The threat actors have allegedly leaked stolen data and posted it on their Tor site. The data allegedly includes personally identifiable information, National ID numbers, Tax account numbers, etc.

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

- Vice Society hacking group is targeting the education sector across the United States and worldwide using multiple ransomware families, such as BlackCat, Zeppelin, as well as their own payload dubbed RedAlert.

  Check Point Threat Emulation provides protection against this threat (Trojan.Wins.ViceSociety.)*

- LockBit has launched an attack against Australian property management company SSKB, and claimed to have stolen 200GB of confidential data including construction projects, financial files of customers, correspondences, etc.

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

- The Largest copper manufacturer in Europe – Aurubis - has been the victim of a cyberattack that targeted its IT systems and forced the company to shut down many of its sites' systems.

VULNERABILITIES AND PATCHES

- OpenSSL, used widely for secure communications, gave heads-up for a critical vulnerability in versions 3.0 and above that will be published on Tuesday, November 1st.
- Google has provided an urgent security update to fix a currently exploited high severity zero-day vulnerability tracked CVE-2022-3723 in Chrome V8, that could lead to out-of-bounds memory access and arbitrary code execution.
- The US Cybersecurity and Infrastructure Security Agency (CISA) has warned of two actively exploited vulnerabilities in the Cisco AnyConnect Secure Mobility Client for Windows. Tracked as CVE-2020-3433 and CVE-2020-3153, these flaws would let a threat actor perform DLL hijacking and run arbitrary commands on the affected machine with SYSTEM privileges.

  Check Point IPS provides protection against this threat *(Cisco AnyConnect Secure Mobility Client Privilege Escalation (CVE-2020-3153))*
- VMware has released security updates to address a critical remote code execution vulnerability tracked as CVE-2021-39144 in VMware Cloud Foundation.
- ConnectWise has released security updates to address a critical vulnerability in the ConnectWise Recover and R1Soft Server Backup Manager that would allow threat actors to infect thousands of vulnerable R1Soft servers exposed to the internet with ransomware.

THREAT INTELLIGENCE REPORTS

- Check Point Research published a technical analysis of the RC4 encryption algorithm, providing a detailed explanation of the its vulnerabilities.
- Check Point Research highlights the brands that are most frequently imitated by threat actors in their attempts to steal personal or payment data. CPR found that the number one, DHL, relates to 22% of all phishing attacks globally, followed by Microsoft with 16% and LinkedIn with 11%.
- Check Point Research found that global attacks increased by 28% in the third quarter of 2022, with education/research as the most attacked industry overall, and the healthcare sector the most targeted industry in ransomware attacks.
- Threat actors are using the Raspberry Robin worm as an access-as-a-service malware in order to deploy other payloads such as IcedID, Bumblebee, Clop ransomware, etc.
- Security Researchers have uncovered a new campaign of Sharkbot and Vultur banking Trojans distributed through apps in Google Play Store. The apps have accumulated more than 130K downloads.