TOP ATTACKS AND BREACHES

- Check Point Research revealed a yearlong campaign targeting German companies, focused on German car dealerships and manufacturers. Threat actors used a vast infrastructure designed to mimic existing German companies and leveraged phishing emails, with a combination of ISO\HTA payloads that, if opened, would infect victims with various info stealing malware.

  Check Point Harmony Endpoint, Anti-Virus, Anti-Bot and Threat emulation provide protection against these threats. *(InfoStealer.Azorult; RAT.Win.BitRat; InfoStealer.Win.Raccoon)*

- Costa Rica has declared a State of Emergency following a devastating ransomware attack by the Conti gang. The attack affected many governmental organizations, including The Finance Ministry, The Costa Rican Social Security Fund, and The Ministry of Science, Innovation, Technology, and Telecommunications. An estimated $200 million was lost due to disruptions related to the tax and customs platforms.

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

- Lincoln College, a 157-year-old institution in Illinois, has announced it will indefinitely close after a significant ransomware attack that occurred in December 2021 took a toll on the school operations.

- Pro-Ukraine hacktivists have defaced the Russian TV online schedule with anti-war slogans like “blood is on your hands” and accused the Russian government of spreading propaganda on Russia’s national Victory day.

- CERT Ukraine has warned of an email phishing campaign leveraging “chemical attacks” themed lures to induce victims into opening malicious XLS documents. After enabling the content, it infects the user with the Jester Stealer info stealing malware.

- CERT Italy has revealed that governmental websites have recently been targeted with distributed denial-of-service attacks (DDoS), making the servers unable to respond for users. The attacks were claimed by the Pro-Russia hacktivist group Killnet.

- Iranian APT34 group (aka Oilrig) has been targeting a Jordanian diplomat with custom-crafted tools in new cyber espionage campaign, using spear phishing methods.

VULNERABILITIES AND PATCHES

- CISA requested federal agencies to immediately patch the now actively exploited F5 BIG-IP critical flaw tracked CVE-2022-1388. The vulnerability concerns the BIG-IP iControl REST authentication component and could let an unauthenticated remote hacker execute commands on vulnerable devices.

  Check Point IPS provides protection against this threat *(F5 BIG-IP Authentication Bypass (CVE-2022-1388))*

- Microsoft has issued updates addressing a vulnerability in Azure Synapse and Azure Data Factory pipelines. Tracked CVE-2022-29972 (aka SynLapse) the vulnerability could be leveraged to execute commands remotely across Integration Runtime infrastructure.

- SonicWall recommends users to patch several vulnerabilities (CVE-2022-22282, CVE-2022-1701 and CVE-2022-1702) affecting its Secure Mobile Access (SMA) products, which could lead to authorization bypass and compromise vulnerable appliances.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports that in April, Emotet was yet again the most prevalent malware, followed by Formbook. This month also saw Spring4Shell make headlines; CPR expects its impact to grow in the coming months.

  Check Point IPS provides protection against this threat *(Spring Core Remote Code Execution (CVE-2022-22965))*

- Check Point Research provides a five-year perspective on the cyber trends and events that have shaped the ransomware ecosystem, from the WannaCry attack into what it has become today.

- The European Union and the United States have formally attributed and condemned the cyberattack that targeted the KA-SAT network satellite (operated by the commercial communications company Viasat in Ukraine) on February 24, just an hour before Ukraine's invasion, to the Russian Federation. The modems were hit with the AcidRain wiper malware.

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

- Security researchers have identified a new remote access Trojan called Nerbian RAT that spreads via email phishing campaigns impersonating the World Health Organization (WHO) with "Covid 19" themed attachments, aimed at industries in Italy, Spain, and the United Kingdom. The RAT includes sophisticated evasion techniques, and can log keystrokes, screen capture, and steal information.

- CISA and other international cyber authorities have released a joint advisory warning of possible threats aimed at managed service provides (MSP) and their clients.