April 3 – 9, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Taiwanese computing hardware giant MSI has suffered a ransomware attack by the recently-founded group Money Message. The group has demanded $4M in ransom, and claims to have stolen source code and databases as part of 1.5TB of information exfiltrated from the company.

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

- A ransomware attack has affected New Jersey Camden County's police department. According to reports, while the attack has been going on since the middle of March, the department has not yet managed to repair its systems. Meanwhile, criminal investigation files have been locked and are inaccessible.

- Russian hacktivist group NoName057(16) has targeted Finland government websites, in what they claim is a response for Finland joining NATO this week. Among the websites targeted with denial of service attacks were the Finnish parliament websites, as well as the website of exiting Prime Minister Sanna Marin.

- After initially releasing 10GB of data stolen from the city of Oakland, California, in a ransomware attack, the PLAY ransomware group has leaked additional 600GB of information stolen in the attack. The city has confirmed that this batch of data contains personal information of some Oakland residents, in addition to employees' personal information that was leaked previously.

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

- ACRO, the UK's Criminal Records Office, has stated that the issues that have been affecting its service since January are caused by a cyber security incident. The office's website has been inactive since the end of March, after online applications were shut down previously. ACRO has instructed users to contact it for service via email.

- Swiss German-language newspaper NZZ has reduced the volume of its publication over the Easter holiday, after its systems have been affected by a ransomware attack.

- Various Muslim-affiliated hacktivist groups have launched "OpIsrael", targeting Israeli websites with DDoS during the past week. Among the targets hit by Anonymous Sudan, were Israeli government subdomains, as well as websites of universities, hospitals, media journals, airports and Israeli companies.

VULNERABILITIES AND PATCHES

- Apple has released an emergency security patch for macOS Ventura. The patch addresses two critical vulnerabilities (CVE-2023-28205 and CVE-2023-28206), which allowed attackers arbitrary code execution on iPhones. The vulnerabilities were discovered after already being exploited in the wild.
- Researchers have found a series of vulnerabilities affecting the products of Nexx, an IoT smart-device firm. The vulnerabilities could allow an attacker to remotely access and control users' garage-door, alarm and smart-plug devices.
- VM2, a popular JavaScript library used for sandboxing, has released version 3.9.15 to address a critical sandbox escape vulnerability. The vulnerability (CVE-2023-29017), allows to the attacker to bypass the sandbox and execute arbitrary code on the host machine running the sandbox.
- Cisco has published security advisories regarding vulnerabilities affecting several of its products. Successful exploitation of the vulnerabilities could allow attackers remote code execution or command injection on vulnerable devices.

THREAT INTELLIGENCE REPORTS

- Check Point Research discovered a new strain of ransomware dubbed Rorschach, which was deployed via DLL sideloading of a legitimate, signed security product. This ransomware is highly customizable with technically unique features previously unseen in ransomware, and is one of the fastest ransomware observed, by the speed of encryption.

  Check Point Harmony Endpoint provides protection against this threat.
- Check Point Research highlights the growing underground market selling flight points, hotel rewards and stolen credential of airline accounts. The research shows dedicated brute forcing tools used to steal such accounts and special underground "travel agents" selling discounted flights and hotel reservations using stolen airline and hotel accounts.
- Genesis market, one of the biggest underground markets for stolen credentials and device fingerprints was taken down in a coordinated operation of 17 countries, called Cookie Monster. As part of the operation, 119 users of the platform were arrested.
- An analysis of the new version of the Typhon Reborn malware has been published. The malware, an infostealer widely available for sale on underground forums, has added detection evasion and anti-virtual machine capabilities. Due to its relatively cheap price, researchers estimate that Typhon Reborn will increase in popularity with attack actors in upcoming months.

  Check Point Threat Emulation provides protection against this threat (Infostealer.Win.PasswordStealer.A)