TOP ATTACKS AND BREACHES

- A callback phishing campaign has been observed targeting corporate networks while impersonating known cybersecurity companies – the emails mention an alleged threat in the target's network, asking them to call the company and let them in the network to investigate. Some suggest the operation is done by the Quantum ransomware gang, who employs several veterans from the Conti group.
- Security researchers revealed attempts to infect common Industrial Control Systems with Sality malware, through password recovery tools that exploit a vulnerability in Automation Direct's DirectLogic programmable logic controllers (tracked CVE-2022-2033).
- Researches have published a report covering the activity of several nation-state hacking groups routinely targeting, and masquerading as, journalists and media organizations.
- A new ransomware operation named "Lilith", a C/C++ console-based ransomware created for targeting 64-bit Windows systems, has been spotted using the common double-extortion tactic; listing its first victim - a large construction group based in South America.
- Mantis, a powerful new botnet and the operation behind the largest DDoS attack ever recorded, which peaked at 26 million requests-per-second from 5,067 devices (June 2022), has reportedly launched over 3,000 DDoS attacks against Cloudflare's customers in the past month.
- A sophisticated phishing attack against Uniswap (a popular decentralized cryptocurrency exchange) allowed threat actors to steal 8 million dollars' worth of Ethereum by redeeming all Uniswap v3 LP tokens in the victim's wallet.
- A new unsophisticated hacker group, active since March 2022 and dubbed "Luna Moth", relies on phishing attacks to deliver off-the-shelf tools (such as Atera and Splashtop) to steal data and demand ransom to keep it private, without encrypting the files.
- The new "Autolycos" malware that secretly subscribes Android users to premium services, and has been installed over 3 Million times, has been discovered in eight Android applications in Google Play Store.

  Check Point Harmony Mobile provides protection against this threat
- Researchers discovered a phishing kit targeting PayPal users, in attempt to steal full IDs from victims.

VULNERABILITIES AND PATCHES

- Microsoft has released patches for 84 security vulnerabilities, one of which being an actively exploited, high severity, elevation of privileges zero-day vulnerability in Windows' Client/Server Runtime Subsystem (CSRSS). This vulnerability, tracked as CVE-2022-22047, can allow malicious actors to gain SYSTEM privileges, and it has led CISA to ensure federal agencies patch it within three weeks.

  Check Point Harmony Endpoint, Threat Emulation and IPS provide protection against this threat *(Exploit.Win.CVE-2022-22047.*; Microsoft Windows Client/Server Runtime Subsystem Elevation of Privilege (CVE-2022-22047))*

- A Speculative Execution attack called Retbleed affects numerous older AMD and Intel microprocessors, and could be used to extract sensitive information (tracked CVE-2022-29900 and CVE-2022-29901).

- Researchers have uncovered a vulnerability in macOS (identified as CVE-2022-26706) that could help an attacker bypass sandbox restrictions and run code on the system.

- Some modern Honda car models have a vulnerable rolling code mechanism (CVE-2021-46145) as part of the keyfob subsystem, allowing to unlock cars or even start the engine remotely.

THREAT INTELLIGENCE REPORTS

- Check Point Research found that in June 2022, a new Android banking malware named MaliBot took third place as most prevalent mobile malware, following the takedown of FluBot at the end of May. Emotet is still the most prevalent malware overall, and Snake Keylogger comes in third after an increase in activity since appearing in eighth place last month.

- Researches shed light on the North-Korea-affiliated H0lyGh0st ransomware operation, which has been active targeting small and midsize businesses since June 2021, while staying in the margins of the arena.

  Check Point Anti-Virus provides protection against this threat *(H0lyGh0st.TC.*)*

- Qakbot malware (AKA Qbot) is adopting new methods with objective of improving their detection evasion, while transforming their delivery vectors, improving code obfuscation, multiplying layers in the attack chain, and using multiple URLs as well as unknown file extensions to deliver their payload.

  Check Point Harmony Endpoint, Threat Emulation and Anti-Bot provide protection against this threat *(Trojan.Wins.Qbot.*, qbot.TC.*, Banking.Win32.Qbot.TC.*, Trojan.Win32.Qakbot.TC.*)*

- Malicious actors have been targeting Elastix VoIP phones using Digium's software in a large-scale campaign, possibly exploiting RCE vulnerability in FreePBX module, tracked CVE-2021-45461.

- A large-scale financial motivated phishing campaign using adversary-in-the-middle (AiTM) sites has been attacking over 10 thousand organizations since September 2021, allowing to skip authentication on sites and to hijack the Office 365 authentication process, even if multi-factor authentication was enabled.