Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research reports on cyber criminals' and hacktivists' increased activity leveraging Telegram amid the Russia-Ukraine war. Anti-Russian cyber-attack groups have been growing, while others claiming to fundraise for Ukraine are suspected to be fraudulent.
- Ukraine "IT army" consisting of cyber-operatives and volunteers worldwide has claimed attacks taking down multiple Russian and Belarusian key websites, including the Kremlin's official site.
- After the HermeticWiper (aka FoxBlade, KillDisc) attacks on Ukrainian targets, a new data wiper called IsaacWiper was found to be deployed against a Ukraine government network.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats *(Trojan.Win.KillDisc; Trojan.Win.HermeticWiper; Trojan.Wins.IsaacWiper)*
- Non-governmental organizations and multiple charities providing humanitarian aid in Ukraine have been targeted in an effort to spread confusion and disrupt operations supplying medicine, food and clothing to those directly affected by the conflict.
- Ransomware gang Lapsus$, which took responsibility for last week's breach on the giant chip firm NVIDIA, claims it has now managed to breach the Korean manufacturer Samsung, and published 190GB of sensitive data online.
- As part of the NVIDIA leak by the Lapsus$ ransomware gang were 2 stolen code signing certificates used by to sign their drivers and executables. Attackers have already started using these certificates to sign malware, hoping to evade security solutions.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Trojan.Wins.NvidiaLeakedCert.A)*
- US insurance broker AON is investigating a cyber-attack that has impacted part of their systems.
- Swedish camera company Axis has had to shut down all its public-facing internet services after a cyber-attack targeted its IT systems.
- Japanese car manufacturer Toyota has halted their operations and productions in its plants across Japan after one of its plastic component suppliers Kojima Press Industries suffered a cyber-attack.

VULNERABILITIES AND PATCHES

- Researchers have shared details on the now patched severe design flaws in the Samsung Galaxy encryption hardware feature affecting 100M devices. Tracked CVE-2021-25444 & CVE-2021-25490, these vulnerabilities affect Samsung Galaxy S1, S20 models and S8, S9 & S10 devices.
- CISA has enriched its catalog of known exploited vulnerabilities with 95 new flaws based on evidence of ongoing exploitations.

  Check Point IPS provides protection against 47 of these vulnerabilities and we continue expanding our coverage
- CISA warns of a highly severe vulnerabilities in Schneider and GE Digital's SCADA software. Tracked CVE-2022-22722, CVE-2022-22723 & CVE-2022-22725, these flaws could lead to disclosure of device credentials, denial-of-service, device reboot, or let a hacker gain control of the relay.

THREAT INTELLIGENCE REPORTS

- Check Point Research warns of disinformation surrounding hacktivists' multiple campaigns supporting both Russia and Ukraine: while there have been numerous attack claims, many of these "successes" remain either questionable or impossible to verify.
- Research shows 75% of the infusion pumps in healthcare organizations are vulnerable to known flaws.
- A new espionage tool, Daxin, has been used by China-affiliated threat actors in campaigns targeting governments, as well as telecom, transportation and manufacturing enterprises.

  Check Point Anti-Virus provide protection against this threat (Trojan.Win32.Malware.TC.daxin)
- Conti Ransomware internal chats have been leaked, allegedly by a Ukrainian researcher, a few days after the group's pledge to retaliate cyber-attacks on Russian targets. The file dump contains 13 months of conversations providing insights on their modus operandi, tools, internal management and more.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win32.Conti)
- The Russian government has released a list of 17,576 IP addresses and 166 domains that have allegedly been targeting its infrastructures with distributed denial-of-service (DDoS) attacks. The list includes CIA, FBI and several media outlets domains.
- The Log4Shell flaws are still exploited by threat actors to deploy various malware payloads, but mostly for DDoS botnets and planting cryptominers.

  Check Point IPS provides protection against this threat (Apache Log4j Remote Code Execution (CVE-2021-44228))