TOP ATTACKS AND BREACHES

- Russian state-sponsored APT actor Sandworm made an attempt to hack into Ukraine's power grid with the Industroyer2 malware, aiming at taking down multiple infrastructure components. The malware forensic analysis has revealed that the attack had been planned at least two weeks prior to the assault.

- Hackers have been targeting Ukrainian government entities leveraging Zimbra exploits and phishing attacks using the IcedID malware, with the goal to perform cyberespionage after gaining internal networks access.

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

- German wind turbine company Nordex has been victim of a cyberattack claimed by the Conti ransomware gang. The attack, which occurred on March 30, shut down all the company's internal IT systems and disrupted their remote access to the turbines.

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

- Several senior European Union officials have been allegedly infected with the Israeli NSO group Pegasus spyware. It is not clear at this time who is at the origin of these attacks nor which information was compromised. The NSO has denied responsibility in a statement.

- OldGremlin threat actor, a ransomware operation with lower attack counts, has targeted Russian organizations with phishing campaigns starting at the end of March 2022. The group impersonated a senior Russian accountant and used a malicious document in a Dropbox that installs the new TinyFluff backdoor.

- North Korean state-sponsored APT group Lazarus has been linked to a recent theft of $625 million worth in Ethereum cryptocurrency in the Axie Infinity game.

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

- Ermenegildo Zegna, a luxury fashion brand in Italy, revealed it has been victim of a RansomExx ransomware attack. After refusing to pay the ransom, their data, including sensitive accounting materials, was published online.

VULNERABILITIES AND PATCHES

- Check Point Research identified a security flaw in Rarible, the NFT marketplace with over two million monthly active users. If exploited, the vulnerability would have enabled a threat actor to steal a user's NFTs and cryptocurrency wallets.
- Cisco has patched a critical authentication bypass in the Wireless Lan Controller (WLC) tracked CVE-2022-20695. The vulnerability could let a hacker gain administrator privileges by crafting their own credentials and eventually take over the targeted system.
- Google has issued an emergency Chrome update to fix a high severity type confusion vulnerability in the Chrome 8 JavaScript engine, CVE-2022-1364, currently exploited in the wild.
- One of the recently patched flaws in VMware Workspace ONE Access is now being exploited in the wild. The vulnerability tracked CVE-2022-22954 is a critical remote code execution flaw.

THREAT INTELLIGENCE REPORTS

- Check Point Research reveals that Emotet remains the most prevalent malware in March 2022, impacting 10% of organizations worldwide while Agent Tesla moves from fourth to second place after several mal-spam campaigns.

  Check Point Threat Emulation and Anti-Bot provide protection against these threats *(Trojan.Win32.Emotet)*

- Multiple law enforcement agencies from different countries, including the FBI and Europol, have taken down the RAIDForums in a joint operation. RAID has been one of the most popular hacking marketplaces to buy and sell stolen data from diverse cyber-attacks.
- Financially motivated cybercriminal group Karakurt has been found to have ties with the Conti ransomware gang as their data extortion arm.

  Check Point Threat Emulation and Harmony Endpoint provide protection against these threats
  (Ransomware.Win.Conti.F; Trojan.Win32.Karakurt.TC)

- Microsoft has successfully disrupted the ZLoader botnet gang, and took control of 65 of their domains that were leveraged to grow, control and communicate with the malware. ZLoader is a malware-as-a-service operation used to steal and extort money from their victims.

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

- CISA, FBI and NSA warn of nation-state threat actors leveraging custom-made malware dubbed PIPEDREAM to attack ICS/SCADA devices.