TOP ATTACKS AND BREACHES

- Check Point Research has released data on cyber attacks observed around the current Russia/Ukraine conflict. Cyber attacks on Ukraine's government and military sector surged by 196% in the first three days of combat. Cyber attacks on Russian organizations increased by 4%. Phishing emails in the East Slavic languages increased 7-fold.

- Check Point Research has spotted a new malware, Electron-bot, distributed through gaming applications on Microsoft's official store, with at least 5,000 victims, mostly in Sweden, Bulgaria, Russia, Bermuda and Spain. The malware can control social media accounts of its victims, including Facebook, Google and Sound Cloud. The malware can register new accounts, log in, comment on and "like" other posts.

  Check Point Harmony Endpoint provides protection against this threat

- Following an announcement by OpenSea about a contract migration they are planning, Check Point Research observed that hackers took advantage of the upgrade process and scammed NFT users, leading to theft of millions of dollars.

- A new data wiper called HermeticWiper has been targeting hundreds of computers in Ukraine. The malware appears to have been compiled in December 2021, which implies that the attack was premeditated for at least a couple of months.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Trojan.Win.KillDisc.A; Trojan.Win.HermeticWiper.A; Trojan.Wins.HermeticWiper.B)*

- Belarussian state-sponsored threat actor UNC1151 has been targeting private email accounts of Ukraine military forces and related individuals, luring them into clicking a link to verify their contact information.

- State-sponsored Iranian APT group MuddyWater is using a new malware in a cyber espionage campaign targeting government and commercial networks worldwide. Intrusion is facilitated with spear-phishing attacks to lure victims into downloading ZIP archives containing malicious Excel or PDF files.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat

- US based chipmaker Nvidia has been hit by a cyber-attack impacting their developer tools and email systems. It is claimed that the cyber criminals were hacked back, encrypting the data they had stolen.

- TiltedTemple APT group has been targeting US defense contractors with sophisticated SockDetour backdoor to maintain persistence. SockDetour can hijack network connections made to the pre-existing network socket and establishes an encrypted C2 channel with a remote hacker via the socket.

VULNERABILITIES AND PATCHES

- US Cybersecurity Infrastructure and Security Agency (CISA) has warned of 2 vulnerabilities in Zabbix IT monitoring tool that are actively exploited in the wild.

  Check Point IPS will provide protection against this threat in the next online package *(Zabbix Web Frontend Authentication Bypass (CVE-2022-23134); Zabbix Web Frontend Authentication Bypass (CVE-2022-23131))*

- A patch has been issued for a remote code execution flaw in Okta Advanced Server Access Client (CVE-2022-24295) that could let a remote hacker perform command injections via a specially crafted URL.

- Cisco has addressed four security vulnerabilities in new updates: CVE-2022-20650, a command injection flaw in the NX-API feature of Cisco NX-OS Software, CVE-2022-20623 & CVE-2022-20624, two DoS flaws in NX-OS, and CVE-2022-20625, another DoS vulnerability in the Cisco Discovery Protocol service.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed how the Eastern Europe conflict affects the dynamics of the cyberspace. Hacktivists, cybercriminals and white hat researchers are picking a clear side, emboldened to act on behalf of their choices. This includes building the Ukraine "IT army" of volunteers, Conti ransomware which threatens to attack those opposing Russia, and more.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win32.Conti)*

- The Russia affiliated Cyclops Blink malware that replaces VPNFilter code, has been deployed to compromise routers and will provide DDoS tools to attackers. The threat actor has been linked to Sandworm (aka Voodoo Bear), known to target Ukraine in the past.

  Check Point Threat Emulation provide protection against this threat *(Trojan.Wins.CyclopsBlink)*

- Operators of TrickBot malware have shut down their servers, after 2 months of inactivity. Some of its developers may have joined the Conti gang.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats

- Dridex malware are now delivering Entropy ransomware in recent attacks against different organizations. The attackers were relying on Cobalt Strike beacons as a means to infect more machine.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats

- Researchers have published details of Bvp47, a backdoor used by the Equation APT group, allegedly linked to the US National Security Agency (NSA). Bvp47 has been used on over 287 targets located in 45 countries, mainly China, Korea, Japan, Germany, Spain, India and Mexico.