TOP ATTACKS AND BREACHES

- Large companies including Microsoft, Okta, NVIDIA, Samsung & Ubisoft have been breached by the Lapsus$ hacking group. This cyber gang is best known for publishing sensitive information stolen from major technology companies and governments. How the gang managed to breach these targets is not yet clear to the public. In recent developments, the UK police announced having arrested 7 teenagers, aged 16 to 21 years old, suspected of being behind the hacks.

- French organizations in the construction, real estate and government sectors were targeted using an open-source package installer Chocolatey to deliver the Serpent backdoor. Threat actors leveraged a resume themed subject and a macro-enabled document claiming to include GDPR information, as well as steganography - a cartoon image used to install the backdoor.

- Chinese-speaking APT group Scarab has been targeting Ukraine since the beginning of the conflict with a campaign leveraging the HeaderTip malware. Their campaign generally involves phishing emails with socially engineered lure documents containing the payload.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransom.Win32.Scarab; Technique.Win.MalScript.la.B)

- One of Russia's largest meat producers Miratorg Agribusiness Holding has suffered a major cyberattack. Threat actors used Windows BitLocker to encrypt the victim's IT systems in full volumes and demanded a ransom. The attack resulted in distribution disruptions for several days.

- A Chinese APT actor has been linked to a new campaign dubbed "Operation Dragon Castling" which has been targeting gambling companies in Southeast Asia, mostly Taiwan, the Philippines, and Hong Kong. Attackers' TTPs involve leveraging a remote code execution vulnerability in WPS Office tracked CVE-2022-24934. These attacks were not yet linked to a known group.

- Researchers have found a malicious Android application called "Craftsart Cartoon Photo Tools" that was installed by over 100,000 users. The application infects its victim with Android Trojan called Facestealer to eventually steal Facebook credentials while communicating with a domain registered in Russia.

  Check Point Harmony Mobile provides protection against this threat *(Trojan.Win32.Facestealer)*

- Morgan Stanley customer accounts have been breached in social engineered attacks, which were the result of Vishing schemes. Hackers successfully transferred money to their own bank accounts.

VULNERABILITIES AND PATCHES

- Google has released an emergency update to patch a high-severity zero-day vulnerability in Chrome that is actively exploited in the wild. Tracked CVE-2022-1096, it is a type confusion vulnerability in the V8 JavaScript engine and could allow a threat actor to perform out-of-bounds memory access.
- Sophos has fixed a critical vulnerability tracked CVE-2022-1040 in its Firewall. The flaw is an authentication bypass in the user portal and webadmin areas of Sophos Firewall versions 18.5 MR3 and earlier. If exploited it could allow attackers to bypass authentication and execute arbitrary code.
- VMware has patched two critical security vulnerabilities in Carbon Black App Control Platform. CVE-2022-22951, an OS command injection flaw could be leveraged to execute commands on the server and CVE-2022-952, a file upload flaw that could let a hacker execute code on the affected Windows instance.
- CISA has added 66 flaws to its known vulnerabilities catalog, which have been exploited in cyberattacks against organizations.
- Select Honda and Acura car models are vulnerable to "replay attacks" that can let a nearby malicious actor unlock the car and start the engine, by capturing the RF signals sent from the key to the car and resending them to take control from a short distance.

THREAT INTELLIGENCE REPORTS

- Check Point Research found that cyberattacks from Chinese IP addresses on NATO countries jumped by 116%, and 72% worldwide. While these attacks weren't attributed to specific threat actors, this trend indicates that hackers are increasingly using Chinese IPs as a resource to launch cyberattacks amid the Russia-Ukraine conflict.
- Researchers have found that two state-sponsored North-Korean threat actors have been exploiting a remote code execution flaw in Chrome, tracked CVE-2022-0609. The campaigns targeted US organizations, IT, cryptocurrency and the fintech sector.

  Check Point IPS provides protection against this threat (Google Chrome Use After Free (CVE-2022-0609))
- Chinese APT group Mustang Panda (aka TA416) has introduced a new variant to their ongoing espionage campaign's toolset against diplomats, research sector and ISPs in Southeast Asia. The new custom loader dubbed Hodur is a Korplug variant with whom it shares similar RAT functionalities.
- The US Government has issued a warning to companies against potential cyberattacks from Russia in response to the economic sanctions recently enforced by western countries.
- The FBI reports that 649 critical infrastructures were hit by Ransomware attacks in 2021.