December 5 - 11, 2022

Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The company that holds the World Cup broadcasting rights for sub-Saharan Africa has suffered a series of cyberattacks since the beginning of the tournament, targeting one of its decoding servers.

- The New York-based Metropolitan Opera has been a victim of a cyberattack that shut down their website, call center and box office, limiting purchases and ability to provide exchanges and refunds.

- Amnesty International's Canadian branch has been a victim of data breach, allegedly performed by Chines state-sponsored group known as APT27. The threat actors used a vulnerability affecting password management company Zoho (tracked as CVE-2021-40539).

  Check Point IPS provides protection against this threat (VERN_Zoho ManageEngine ADSelfService Plus Authentication Bypass (CVE-2021-40539))

- Russia state-sponsored hacking group TAG-53 (aka Blue Callisto), has been linked to phishing and credential-harvesting operations targeting multiple organizations. Nine suspected malicious domains have been referenced to potential victims, one of them contains a spoofed Microsoft login page masquerading as Global Ordnance, a legitimate US military weapons and hardware supplier.

  Check Point Harmony Endpoint provides protection against this threat (Gen.Win.Reg.Callisto.AntiVmVirtualBox; Gen.Win.Reg.Callisto.Sandboxie)

- China-linked state-sponsored group Mustang Panda has been using the Russia-Ukraine conflict in a recent phishing campaign, collecting sensitive data from entities in Europe and the Asia Pacific.

  Check Point Threat Emulation provides protection against this threat (APT.Win.MustangPanda; Trojan.Wins.MustangPanda)

- CERT-UA has analyzed a phishing attack against the Railway Transport Organization of Ukraine, by attack group UAC-0140. Phishing emails allegedly included information on the Iranian Shahed-136 drones, eventually leading to the DolphinCape malware.

- A new wiper named Fantasy has been observed used by Agrius Iranian APT group to execute a supply-chain attack abusing an Israeli software suite used in the diamond industry. The wiper, based on Agrius's previous wiper Apostle, functions as a data wiper and does not attempt to masquerade as ransomware.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Apostle)

- China-linked cyber espionage APT group BackdoorDiplomacy has been exploiting ProxyShell on Exchange servers, in a campaign against telecom companies in the Middle East which started in August 2021.

VULNERABILITIES AND PATCHES

- Google has released security updates for Android, fixing four critical-severity vulnerabilities (tracked as CVE-2022-20472, CVE-2022-20473, CVE-2022-20411 and CVE-2022-20498), including an RCE flaw exploitable via Bluetooth. The update addresses more than 45 vulnerabilities in core Android components, and another 36 vulnerabilities impacting third-party components.
- An Internet Explorer zero-day vulnerability (tracked as CVE-2022-41128) was actively exploited by North Korean state-sponsored group APT 37 (ScarCruft). The exploit was embedded in a malicious docx, referencing a recent tragic incident in Itaewon, South Korea, where 158 people were killed in a crowd crush during Halloween celebrations.

  Check Point IPS provides protection against this threat *(Microsoft Windows Scripting Languages Type Confusion (CVE-2022-41128))*
- Cisco has disclosed a high-severity vulnerability (tracked as CVE-2022-20968) affecting the latest generation of its IP phones. Successful exploitation could cause a stack overflow, resulting in possible remote code execution and denial of service (DoS) attacks.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed the activity of cyber-espionage group Cloud Atlas. Since its discovery in 2014, the group has launched multiple, highly targeted attacks on critical infrastructure across geographical zones and political conflicts, however its scope has narrowed significantly in the last year, with a clear focus on Russia, Belarus and conflicted areas in Ukraine and Moldova.

  Check Point Threat Emulation and Harmony Email and Office provide protection against this threat
- The U.S. Department of Health and Human Services (HHS) has released a warning about Royal ransomware that targets the Healthcare and Public Healthcare sector. Royal ransomware is a financial motivated gang that steal data using double-extortion attacks, first observed in September 2022.
- Researchers have identified a Deathstalker malware that uses a new Janicab variant. The malware was used by threat actors to target law firms and financial institutions in the Middle East throughout 2020. Recently, it was used in a campaign against travel agencies in the Middle East and Europe.
- Iranian nation-state group Nemesis Kitten (aka DEV-0270, PHOSPHORUS) is using Drokbk malware, leveraging GitHub as a "dead drop resolver" to hide its C2 communication.
- Researchers have discovered a novel Go-based botnet called "Zerobot" that exploits multiple vulnerabilities in IoT devices. The botnet attacks different protocols and can self-propagate. It communicates with its command-and-control server using the WebSocket protocol.