Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- An unaffiliated threat actor has been initialing a phishing campaign targeting government entities in Europe and the U.S, exploiting the recently disclosed Microsoft Office "Follina" vulnerability, tracked CVE-2022-30190.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190); Exploit.Win.Follina)*

- Microsoft disabled a coordinated malicious activity between Lebanon-based and Iran-linked threat actors, targeting and compromising Israeli organizations. The offensive activity abused OneDrive cloud storage platform for data exfiltration and command and control. Microsoft claims to have suspended more than 20 malicious OneDrive applications created by the attackers.

- Costa Rica's public health service was attacked by Hive ransomware, which shut off their computer systems. The Hive ransomware group demanded $5 million in Bitcoin to unlock the infected servers. This attack can be related to the Conti ransomware attacks on this and other government-related entities.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat

- Iranian government-sponsored hackers planned to attack Boston Children's Hospital and disrupt services last summer, the FBI claims. Affiliation and motive remain unclear.

- Chinese-speaking APT dubbed LuoYu has been using an information stealer malware called WinDealer as a tool in sophisticated attacks. The malware, delivered through automatic updates of legitimate applications, allows attackers to search and transmit data from affected Windows systems, install backdoors to maintain persistence, manipulate files, propagate and run arbitrary commands.

- Post U.S. sanctions, Evil Corp group continues to distance themselves from known tools, now by using LockBit ransomware. This is to evade the OFAC regulations and insure the victims' ransom payment.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat

- FluBot, the notorious mobile malware threat that spreads globally mainly via SMS-based phishing, has been taken down in a joint law enforcement operation – Europol announced.

  Check Point Harmony Mobile provides protection against this threat

VULNERABILITIES AND PATCHES

- Researchers revealed a zero-day vulnerability in Microsoft Office that might enable remote code execution on a victim's machine. The vulnerability, dubbed "Follina", uses the remote template feature in Word to retrieve an HTML File from a remote server, and can execute a PowerShell by using an ms-msdt MSProtocol URI scheme.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190); Exploit.Win.Follina)*

- Check Point Research found a vulnerability within the UNISOC chip firmware used in Android mobile phones, which can allow a remote attacker to disrupt the device's radio communication through a malformed packet.

  Check Point Harmony Mobile provides protection against this threat

- A Critical vulnerability affecting Atlassian Confluence and Data Center servers (CVE-2022-26134), exploited in the wild, has been patched. Successful exploitation could allow remote attackers to create new admin accounts, execute commands, and take over the server.

  Check Point IPS provides protection against this threat (Atlassian Confluence Remote Code Execution (CVE-2022-26134))

- GitLab issues a patch for a critical account takeover vulnerability (tracked CVE-2022-1680); a security flaw that could allow a malicious actor to invite arbitrary users through their username and email, change credentials and ultimately take over accounts.

THREAT INTELLIGENCE REPORTS

- Check Point Research analyzed the current version of the Xloader infostealer, known for its techniques of hiding its C&C servers among tens of thousands of decoys. Over the past year, two new versions have been released in which the authors of the malware further improved these techniques and experimented with probability theory, making C&C server discovery even more difficult.

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

- Researchers analyzing the leaked chats of the Conti ransomware operation have discovered that Conti developers had created proof-of-concept (PoC) code that exploited Intel firmware. Even though the Conti operation may have shut down, Conti engineers moved to other malware operations where they can develop new, unknown exploits in firmware.

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

- Researchers developed a proof-of-concept of a ransomware for IoT (R4IoT) devices that targets IT and OT networks.