Check Point
SOFTWARE TECHNOLOGIES LTD.

Nov 8 – 14, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research notes a 178% increase in the number of malicious shopping websites, compared to the rest of the year, spotting over 5300 different malicious websites per week ahead of the end of this year's e-shopping season.

- Check Point Research has analyzed the operations of threat actor MosesStaff following its multiple offensive campaigns against Israeli companies. The group's motive, purely political, is to cause damage by leaking stolen sensitive data while encrypting networks without asking for a ransom.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Wins.DCSrv.A; Ransomware.Win.MosesStaff.A; Ransomware.Win.MosesStaff.B; Ransomware.Win.MosesStaff.C)*

- Email servers of the FBI have been hacked and used to distribute spam emails to thousands of individuals and companies, warning that their network was compromised and data was stolen in a cyberattack.

- The North Korean state-sponsored hacking group Lazarus attempts to hack security researchers around the world with malicious executables hidden in a pirated version of the reverse engineering application IDA Pro, commonly used by malware analysts.

  Check Point Anti-Virus and Threat Emulation provides protection against this threat

- Researchers reveal that the Iranian state sponsored APT group Lyceum (aka HEXANE, Spilrin) has attacked Internet Service Providers and telecommunication service providers in the Middle East and Africa between July and October 2021, with a primary focus on computer network intrusion.

- Electronics retail giant MediaMarkt was victim of a Hive ransomware attack with an initial ransom demand of $240 million, dropping to $50 million after negotiations. The attack caused IT systems to shut down, and store operations were disrupted in Netherlands and Germany.

  Check Point Harmony Endpoint provides protection against this threat

- VoIP provider Telnyx has recently been targeted with distributed denial-of-service (DDoS) attacks, causing worldwide outages and disruptions around the world.
- South Korea residents with Android devices are being targeted by an ongoing spyware campaign called "PhoneSpy" masquerading as legitimate lifestyle apps, hiding in plain sight while exfiltrating data.
- The Clop ransomware gang (aka TA505 & FIN11) is exploiting a SolarWinds Serv-U FTP software vulnerability to breach organizations networks and ultimately encrypt their devices.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
- Costco Wholesale Corporation has sent notification to their customers warning that their payment card information may have been stolen while recently shopping at one of its stores.

VULNERABILITIES AND PATCHES

- The Australian Cyber Security Center warns of the active exploitation of vulnerability CVE-2021-42237, a remote code execution flaw in the Sitecore Experience Platform (Sitecore XP).
- Microsoft urges admins to immediately patch a high severity Exchange Server vulnerability, CVE-2021-42321, that may allow authenticated attackers to execute code remotely on vulnerable servers.
- Microsoft has patched an Excel zero-day vulnerability, CVE-2021-42292, exploited in the wild by threat actors. A patch for macOS users will be released soon.

  Check Point IPS provides protection against this threat (Microsoft Excel Security Feature Bypass (CVE-2021-42292))
- A free and unofficial patch is now available for a zero-day local privilege escalation flaw (CVE-2021-34484) in the Windows User Profile Service that could allow threat actors to gain SYSTEM privileges under certain conditions.

THREAT INTELLIGENCE REPORTS

- Check Point Research reveals that Trickbot is the most prevalent malware for the fifth time and a new vulnerability in Apache HTTP Server Directory Traversal is one of the most exploited vulnerabilities worldwide. Education and Research industries remain at the top of the target list for hackers.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Trojan-Banker.Win32.Trickbot)
- Romanian law enforcement authorities apprehended two individuals believed to be REvil ransomware affiliates (aka Sodinokibi) responsible for the attack against Kaseya MSP platform. The United States State department is issuing a bounty of up to $10 million for identifying or locating their operators.

  Check Point Harmony Endpoint and Anti-Bot provide protection against this threat (Trojan.Win32.Sodinokibi)

- Shatak group (aka TA551) has recently partnered with the TrickBot gang (aka ITG23, Wizard Spider) to distribute the Conti ransomware on compromised systems.

  Check Point Harmony Endpoint and Anti-Bot provide protection against this threat *(Ransomware.Win32.Conti; HEUR:Trojan-Ransom.Win32.Conti)*

- The Magniber ransomware gang is now exploiting two patched Internet Explorer vulnerabilities and malicious advertisements to infect users and encrypt their computers.

  Check Point IPS and Harmony Endpoint provide protection against this threat *(Microsoft Internet Explorer Memory Corruption (CVE-2021-26411); Microsoft Internet Explorer MSHTML Remote Code Execution (CVE-2021-40444))*

- A new botnet named BotenaGo, written in Golang, has been discovered by researchers, capable of using over 30 different vulnerabilities to attack millions of routers and IoT devices.

  Check Point IPS provides protection against this threat *(Draytek Vigor Command Injection (CVE-2020-8515); D-LINK Multiple Products Remote Code Execution (CVE-2015-2051); Netgear Multiple Products Command Injection (CVE-2016-1555); Netgear R7000 and R6400 cgi-bin Command Injection; Dasan GPON Router Authentication Bypass; Dasan GPON Router Remote Command Injection; XiongMai uc-httpd Buffer Overflow; Comtrend Command Injection (CVE-2020-10173) etc)*

- A new Android malware known as MasterFred is using fake Apps looking similar to Instagram, Netflix and Twitter to steal the credit card information of users.

  Check Point Harmony Mobile provides protection against this threat

For comments, please contact: TI-bulletin@checkpoint.com