April 9 - 15, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Hacktivists have successfully defaced several popular YouTube music videos, including the most viewed video of all time, "Despacito". This activity is attributed to anti-Israeli cyber activity.

- Researchers have spotted a wide-spread scanning of IoT (Internet of Things) devices that is likely related to establishment of a new IoT botnet. The scans are arriving via Chinese IP addresses and are targeting network devices mostly in Brazil. Targeted devices are China-made routers and IP cameras, many of which are vulnerable to attacks using default username and passwords.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Weak Password Login Attempt Over Telnet; Botnet.Win32.Mirai.)*

- Coinsecure, an Indian cryptocurrency exchange, has suffered a security incident resulting in the theft of 438.318 Bitcoins from its systems (approximately $3.5M). According to the company's announcement, the incident took place while its CSO conducted some actions using the company's crypto-wallet.

- Security researchers have conducted a major sinkholing operation on the C&C infrastructure behind EITest. EITest is a Traffic Distribution System (TDS) that started its life in 2011 as a private TDS for an exploit kit named Glazunov. Since 2014 EITest has become rentable, with massive traffic volumes. According to the researchers behind the operation, EITest's author didn't try to reclaim it so far.

  Check Point IPS blade provides protection against this threat (EITest Exploit Kits Traffic Distribution System)

- Two new variants of Matrix ransomware were spotted in the wild. The new variants are installed via hacked Remote Desktop services.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Microsoft Windows Remote Desktop Protocol Scanning Attempt; Multiple RDP Initial Connection Requests; Trojan-Ransom.Win32.Matrix.)*

- The US National Cybersecurity and Communications Integration Center (NCCIC) has issued a warning on a growth in ransomware attacks across the world, including best practices for protection.

VULNERABILITIES AND PATCHES

- Microsoft has released its Patch Tuesday for April, includeing security updates for Internet Explorer, Microsoft Edge, Microsoft Windows, Microsoft Office and Microsoft Office Services and Web Apps, ChakraCore, Adobe Flash Player, Microsoft Malware Protection Engine and Microsoft Visual Studio.

  Check Point IPS blade provides protection against these threats (Microsoft Office Remote Code Execution, Microsoft Office Graphics Remote Code Execution, Microsoft JET Database Engine Remote Code Execution, Microsoft Excel Remote Code Execution, Microsoft Windows VBScript Engine Remote Code Execution)

- Adobe has released several security updates for Adobe PhoneGap Push plugin, Adobe Digital Editions, InDesign CC, ColdFusion, Adobe Experience Manager and Adobe Flash Player. The updates address 19 vulnerabilities, 6 of which are rated critical and may allow arbitrary code execution.

  Check Point IPS blade provides protection against this threat (Adobe Flash Player Use After Free, Adobe Flash Player Out-of-bounds read, Adobe Flash Player Heap Overflow)

- VMware has released a security advisory addressing vulnerabilities in vRealize Automation (vRA). One of the vulnerabilities is a cross-site scripting (XSS) vulnerability, and the other is a Missing renewal of session tokens vulnerability. Exploitation of these issues may lead to the compromise of the vRA user's workstation or to the hijacking of a valid vRA user's session.

- A critical vulnerability has been discovered in CyberArk's Enterprise Password Vault application, which may allow a remote attacker to perform unauthenticated remote code execution on a web server.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have published an in-depth technical report on Drupalgeddon 2, a highly critical vulnerability that was recently discovered in the Drupal content management system (CMS). In their report, the researchers have examined how the vulnerability may easily be exploited, thus putting organizations' resources at risk.

  Check Point IPS blade provides protection against this threat (Drupal Core Remote Code Execution (CVE-2018-7600))

- A new report describes the risks of social media questionnaires asking for historic details on users. According to the report, many questionnaires are asking users to share private and nostalgic details (first pet, first car, etc.), typically used as secret questions for online accounts security. Such details are highly useful for identity theft scams and other fraudulent actions.

- Academic researchers have developed a new malware that can exfiltrate data from air-gapped machines via power lines. The malware, dubbed PowerHammer, can control the power consumption of a system by intentionally regulating the CPU utilization. Data collected from the power lines of target machines is converted into computer actions.