Check Point
SOFTWARE TECHNOLOGIES LTD.

September 25 - October 1, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- SHEIN fashion retailer has suffered a major data breach affecting about 6.5 million users. Threat actors have managed to access customers' personal information, including email addresses and encrypted passwords of customers who visited the online store.

- Security researchers have discovered a Monero Cryptomining campaign leveraging Kodi Media Player add-ons for distribution. The multi-stage malware distributed in this campaign is able to compromise both Windows and Linux platforms, has anti-analysis abilities, and already targeted over 5,000 victims.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.KodiMIner; Trojan.Linux.KodiMiner)

- Facebook has been hacked and data of 50 million users has been exposed. Threat actors have exploited a zero-day vulnerability in the "View as" features to steal access tokens of the users and take over their accounts.

- The Port of San Diego has suffered a ransomware-based attack, a few days after the Port of Barcelona was hit by a cyber-attack as well. The attack has impacted the processing of park permits and record requests, along with other operations.

- Security researchers have identified a new sophisticated malware called 'LoJax', used as part of the first UEFI (Unified Extensible Firmware Interface) rootkit. The LoJax UEFI rootkit is used by the infamous Russia-linked Fancy Bear group in current targeted attacks against governments in the Balkans, and in Central and Eastern Europe. It allows attackers to achieve persistence on the targeted devices and survives a complete hard-drive wipe.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.LoJax)

VULNERABILITIES AND PATCHES

- The Bitcoin Core team has released a security patch for a critical DDoS attack vulnerability in the Bitcoin Core wallet software. The vulnerability may allow attackers to crash Bitcoin Core nodes, and in a worst scenario to take down the entire blockchain system by coordinating an attack through Bitcoin miners.
- A new integer overflow vulnerability has been spotted in Linux Kernel dubbed 'Mutagen Astronomy', affecting Red Hat, CentOS, and Debian Distributions. The vulnerability may allow an unauthorized attacker to gain superuser access to the targeted system.
- Cisco has released a security patch addressing 25 vulnerabilities, 14 of which are rated as critical and most of which are denial-of-service flows affecting components in its IOS and IOS XE Software products.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have identified a new online builder, dubbed 'Gazorp', designed for building binaries of the Azorult infostealer which harvests passwords, credit card information, cryptocurrency-related data and more. Gazorp is hosted on the Dark Web and is offered there for free, allowing any threat actor to create fresh Azorult samples.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.Azorult)

- Security researches have revealed that s new version of the infamous IoT botnet 'Hide N Sick' (HNS) is targeting Android devices. HNS botnet exploits the Android Debug Bridge, allowing the attackers to execute any command in administrator privileges remotely.
- Security researchers have discovered a highly sophisticated IoT botnet dubbed 'Torii', targeting a wide range of architectures, including ARM, MIPS, x86, x64, PowerPC, and SuperH. Torii infects devices that have Telnet exposed and protected by weak credentials, and steals data from the compromised devices.
- New dangerous capabilities have been spotted in the VPNFilter, the highly sophisticated multi-stage IoT botnet attributed to the Russia-linked Fancy Bear group. The new capabilities include networks mapping, compromising endpoints connected to infected devices, obfuscating and encrypting malicious traffic, building a network of proxies that may be used to hide the source of malicious traffic, and more.

  Check Point IPS Anti-Bot and Anti-Virus blades provide protection against this threat (IOT.Linux.VPNFilter; Netgear WNDR4700 Router Authentication Bypass (CVE 2013 3071); VPNFilter Client Malicious Self-Signed Certificate; Netgear DGN Unauthenticated Command Execution; NETGEAR DGN2200 Remote Code Execution (CVE-2017-5521); Trojan.UNIX.VPNFilter.)*

- The fifth version of GandCrab Ransomware has been spotted in the wild, leveraging the Task Scheduler ALPC vulnerability to gain System privileges on infected devices.

  Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan-Ransom.Win32.GandCrab)