March 4 - 10, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A new InfoStealer campaign has been discovered by Check Point researchers, targeting Windows servers in Asia-Pacific countries. The InfoStealer uses familiar techniques to run malicious content on infected machines and conceals its behavior to evade Anti-Virus detection.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan-downloader.Win.Squiblydoo.A)*

- Hundreds of popular Israeli websites were compromised in a targeted cyber-attack after attackers tampered with DNS records of a popular accessibility plugin. The compromised plugin, which was accessible via multiple popular websites, delivered ransomware disguised as a Flash Player update.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.JCry)*

- The software company Citrix has suffered a security breach. The company reported that an international cybercrime group has gained access to its internal network, and stole business documents.

- Over 2 billion records have been exposed online after an unprotected server was found by security experts. The exposed databases, totaling over 196GB of data, belong to the email validation company Verifications.io.

- Security researchers have discovered a new exploit kit delivering various banking Trojans through malvertising. The new kit, dubbed “Spelevo”, was observed exploiting a use-after-free vulnerability in Flash Player from 2018.

  Check Point Anti-Virus blade provides protection against this threat *(Banking.Win32.Spelevo)*

- A new campaign has been uncovered, infecting machines with StealthWorker brute-force malware in an attempt to compromise e-commerce websites. The campaign currently targets the Magento, phpMyAdmin and cPanel platforms.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Downloader.Win32.StealthWorker)*

VULNERABILITIES AND PATCHES

- Check Point researchers have discovered a critical use-after-free bug in PXE servers of Windows Deployment Services that may allow a remote attacker to execute arbitrary code in all Windows servers.

  Check Point IPS blade provides protection against this threat *(Microsoft Windows Deployment Services TFTP Server Code Execution (CVE-2018-8476))*

- A use-after-free vulnerability has been discovered in Chrome browsers that may allow remote attackers to execute arbitrary code and gain control of compromised hosts. The vulnerability, dubbed CVE-2019-5786, resides in the FileReader component of the browser and is currently being exploited in the wild.

- Critical flaws have been found in smart car alarm systems which may allow remote attackers to hijack the vehicle, taking control over the car engine, the locking mechanism.

- A new privilege escalation vulnerability on Windows 7 has been found. The vulnerability affects Windows win32k.sys kernel driver and has yet to be patched.

- A critical flaw in macOS has been disclosed, which allows an attacker to gain privileges to perform malicious actions on a mounted filesystem without the victim knowing.

- Cisco has released security updates addressing over 24 serious vulnerabilities in their Nexus switches, including denial-of-service (DoS), privilege escalation and arbitrary code execution vulnerabilities.

- Multiple bugs have been found in visitor-management systems including data leakage, program hijacking, obtaining admin credentials and even breaking out of the visitor kiosk environment.

THREAT INTELLIGENCE REPORTS

- A recent study has discovered that SSL and TLS certificates can be acquired from dark web marketplaces. Prices vary from $260 to $2,000 and offers include fake certificates from well-reputed authorities.

- A new backdoor has been spotted in the wild, leveraging GitHub and Slack for C&C communication. The new malware, dubbed “SLUB”, was exploiting VBScript engine vulnerability from 2018 to propagate.

  Check Point Anti-Virus blade provides protection against this threat *(Backdoor.Win32.SLUB)*

- A recent report reveals hundreds of Docker hosts are infected with Monero cryptocurrency mining as a result of unprotected remote public API ports.

  Check Point CloudGuard and IPS provide protection against this threat *(runc Container Escape (CVE-2019-5736))*

- Over 1.6 million home networks have been found vulnerable to remote attacks, as home devices such as printers and routers are running outdated versions of the Universal Plug and Play service, which enables automatic discovery and communication with other devices via network protocols.