August 5 - 11, 2019

YOUR CHECK POINT

# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- AT&T employees have been bribed to unlock more than 2 million mobile devices and plant malware on the company's internal network. The malware allowed the threat actor to gather the telco's confidential and proprietary data and to remotely process unauthorized unlock requests.

- GermanWiper, suspected to be a variant of Sodinokibi ransomware, has been found targeting German organizations via spam phishing emails. Once infected a system, GermanWiper deletes files, rather than encrypts them, while misleading victims to think paying the ransom would get them the files back.

  *Check Point Anti-Virus blade protects against this threat* *(Ransomware.Win32.GermanWiper)*

- Security researchers have uncovered that Machete, a cyber espionage group focusing on Latin American countries and mainly on Venezuelan government entities, has stolen gigabytes of confidential documents including files used by geographic information systems (GIS) software.

  *Check Point Anti-Virus and Anti-Bot blades protect against this threat* *(Spyware.Win32.Machete)*

- New Clicker Trojan has been found installed on more than 33 Android applications with over 100 million installations. The Trojan allows attackers to preform multiple malicious activities including displaying advertisements or subscribing users to expensive premium services.

  *Check Point SandBlast Mobile provides protection against this threat*

- The American insurance giant "State Farm" has fallen victim to a credential-stuffing attack, putting its 83 million costumers' online accounts at risk.

- Security researchers have revealed that the infamous LokiBot infostealer has introduced new upgraded and sophisticated capabilities including updated persistence mechanism and the ability to hide its source code within image files on infected machine. It is currently being spread in a phishing email campaign.

  *Check Point SandBlast and Anti-Bot blades protect against this threat* *(Trojan.Win32.LokiBot; Botnet.Win32.LokiBot)*

## VULNERABILITIES AND PATCHES

- Check Point researchers have revealed several vulnerabilities in the picture transfer protocol (PTP) used in Canon DSLR digital cameras, which allow attackers to completely take over the camera via WiFi or USB and deploy any kind of malware strain on it.

  *Check Point IPS blade protects against this threat (DSLR Cameras PTP/IP Multiple Buffer Overflow Vulnerabilities)*

- A new variant of the Spectre vulnerability has been found, affecting all modern Intel CPUs and some AMD processors leveraging speculative execution for high performance. The vulnerability may allow local attackers to access sensitive information stored in the operating system privileged kernel memory.

- A zero-day privilege escalation vulnerability has been discovered in Steam game client for Windows, exposing over 100 million users and allowing attackers with limited permissions to run arbitrary code on administrative privileges.

- New critical vulnerabilities have been discovered in Qualcomm's chips and Linux kernel driver, exposing millions of Android devices to cyber attacks. When chained together, the vulnerabilities may allow a remote attacker to take complete control over targeted Android devices within their Wi-Fi range.

- A new unpatched zero-day vulnerability has been discovered in the KDE software desktop environment for Linux. The vulnerability may allow attackers using maliciously crafted .desktop and .directory files to run arbitrary code on a user's computer without needing the victim to open them.

## THREAT INTELLIGENCE REPORTS

- Check Point researchers have discovered that SQLite database can be abused by attackers to execute malicious code in other apps, including Apple's, by exploiting memory corruptions issues in the SQLite engine.

  *Check Point IPS blade protects against this threat (SQLite fts3_tokenizer Untrusted Pointer Remote Code Execution (CVE-2019-8602))*

- Check Point researchers have demonstrated three potential attack methods leveraging the vulnerabilities they had discovered in WhatsApp. The vulnerabilities allow attackers to intercept and manipulate WhatsApp conversations and potentially spread misinformation from allegedly trusted sources.

- A new strain of Clipsa malware has been spotted in the wild, capable of scanning the Internet to locate vulnerable WordPress sites and launch brute-force attacks on them. Clipsa info stealer is also capable of stealing administrator credentials and cryptocurrency transfers, and installing a cryptocurrency miner.

  *Check Point Anti-Virus and Anti-Bot blades protect against this threat (Infostealer.Win32. Clipsa)*