Check Point
SOFTWARE TECHNOLOGIES LTD.

September 16 - 22, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Misconfigured Elasticsearch server holding personal information of more than 20 million Ecuadorian citizens has been found unsecured. The server, located in Miami and owned by the Ecuadorian company Novaestrat, exposes full PII (Personally identifiable information), marital status, education, financial info and more of probably every person in Ecuador. The local authorities arrested a Novaestrat executive as part of the case's investigation.

- Tens of millions of records from customers of two airline companies owned by Lion Air have been circulating on data exchange forums for at least a month. The info was stored in an Amazon bucket that was open on the web and included passenger and reservation IDs, physical addresses, phone numbers, email addresses, names, dates of birth, phone numbers, passport numbers and expiration dates.

- A Dubai-based company has lost over $50,000 in a phishing operation. A threat actor took over company email accounts, and emailed customers, asking them to wire funds to the hacker's overseas bank account.

- The Smominru botnet, which has been active since May 2017 and uses the EternalBlue exploit to infect Windows computers for cryptocurrency mining activity, is spreading rapidly, infecting over 90,000 new machines each month.

  Check Point IPS and Anti-Virus blades provides protection against this threat *(Microsoft Windows SMB Remote Code Execution (CVE-2017-0144); Trojan.Win32.SmominruCoinminer; botnet.Win32.Smominru)*

- Two international hotel chain websites have been compromised in a Magecart card skimming attack targeting Android and iOS users. The two hotel booking websites, owned by separate chains and serving 180 hotels, were injected with a JavaScript based card skimmer in an attack active since August 9th.

VULNERABILITIES AND PATCHES

- Google has released an urgent update for its Chrome web browser for Windows, Mac and Linux to address four use-after-free vulnerabilities, one of them being a critical vulnerability that allow remote hackers to take control of an affected system.
- Vulnerability in the AMD ATI Radeon video cards, recently discovered by researchers, could be exploited by attackers to escape VM environment and execute on the host. The vulnerability, tracked as CVE-2019-5049, has received a CVSS score of 9.0.
- Atlassian, provider of the Jira helpdesk request tracker, has released security updates to address critical vulnerabilities in Jira Service Desk and Jira Service Desk Data Center that could lead to information disclosure or even server-side remote code execution.

  Check Point IPS blade will protect against this threat in its next online package
- The popular password manager LastPass has released an update to fix a security bug, which could be used by attackers on malicious pages to extract users' credentials from previously visited sites. The vulnerability has not been seen exploited in the wild.
- In a recent survey researchers evaluated the security of 13 SOHO (small office/home office) routers and NAS devices (network attached storage) and found 125 CVEs exposing all devices to at least one web application vulnerability and allowing them to obtain root shells on 12 of the devices.

THREAT INTELLIGENCE REPORTS

- Australian intelligence has determined that China was responsible for the cyber-attack detected in February, aimed at its parliament and three largest political parties ahead of the May general elections. The report recommended keeping the findings secret in order to preserve trade relations with Beijing.
- As part of its ongoing investigation following the Cambridge Analytica scandal in the US 2016 presidential elections, Facebook has suspended and banned tens of thousands of apps on its platform. According to its announcement, the removed apps have inappropriately shared private data, made it publicly available or otherwise violated Facebook policies
- InnfiRAT, a new RAT malware targeting Windows OS, has been discovered by researchers. InnfiRAT provides attackers full control over compromised machines but has been specifically designed to look for Bitcoin and Litecoin cryptocurrency wallet information and grab browser cookies to steal stored usernames and passwords.

  Check Point SandBlast and Anti-Virus provide protection against this threat (Infostealer.Win32.InnfiRAT)