May 6 - 12, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The city of Baltimore has been hit by a cyber-attack, resulting in infection of the city's technology systems with an unknown ransomware. The ransomware apparently continued to spread throughout the network, forcing also the unaffected servers to shut down as a precaution.

- Binance, one of the largest cryptocurrency exchanges in the world, has suffered a security breach resulting in the loss of nearly $41 million in Bitcoin. The attackers used a variety of intrusion techniques and managed to obtain access to a Bitcoin wallet belonging to the company as well as API keys and two-factor authentication codes.

- An ongoing credit-card hacking campaign has been stealing payment information from more than 100 e-commerce websites using an injection of malicious JavaScripts into the targeted shopping websites. All affected websites are running Magento e-commerce CMS software.

- The hacking groups LulZSec and Anonymous Italy have been involved in a recent cyber-attack hitting the Italian Ministry of Environment in which they managed to steal data belonging to 30,000 Roman lawyers. The stolen data, which also contained information belonging to the Mayor of Rome, was later published and archived online.

- A Russian hacking group is offering for sale access to networks of Anti-Virus companies and the source code of their software. The group, called Fxmsp, claimed to breach the networks of at least three vendors, obtain long-term access and steal 30 terabytes of data which they are offering for sale.

- An unprotected MongoDB database has exposed over 275 million records of Indian citizens. The exposed data included names, emails, mobile phone numbers, education details, professional info and current salaries. Despite the massive amounts of information, the database could not be linked to a specific owner.

VULNERABILITIES AND PATCHES

- Security researchers have revealed a flaw in Alpine Linux Docker Images that may allow attackers and unauthorized users to gain root access, as it is pre-defined with a NULL password. The flaw had been patched in 2015 but the fix was inadvertently removed few weeks later during regression tests.

- A use-after-free vulnerability has been discovered in SQLite 3, which may result in remote code execution. The vulnerability, tracked as CVE-2019-5018, could be triggered by an especially crafter SQL command sent to the targeted server.

  Check Point IPS blade will provide protection against this threat in its next online package

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered the activity of an Indonesian hacking group called "PlaNETWORK" that claims to be an innocent IT consultancy group. The research reveals the various hacking tools published and used by the group as well as several hacking incidents they conducted.

- A report has revealed that a Chinese-linked APT group called Buckeye was using the NSA-linked zero-day exploits and tools nearly a year before Shadow Brokers leaked them on the internet. The researchers suggest that Buckeye may have captured the code from an NSA attack on their own computers.

  Check Point Anti-Bot blade provides protection against this threat *(Backdoor.Win32.Pirpi.C)*

- A new malware, dubbed ElectricFish, has been uncovered by the U.S Department of Homeland Security and the FBI. The malware is utilized for traffic tunneling out of compromised computer systems and was linked to the North Korean-linked APT group Lazarus.

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

- Security researchers have reported the resurfacing of the Retefe banking Trojan in the wild. The new variant spreads through spam messages with zipped JavaScript and weaponized Word documents.

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

- The Russia-linked APT group Turla has been targeting large organizations using a new backdoor to hijack Microsoft Exchange mail servers. The backdoor, dubbed LightNeuron, can be used to access and modify e-mails passing through the compromised exchange server, as well as compose new messages.

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

- A code bug in one of the most widespread IoT botnets, Mirai, has been discovered. The bug, apparently existing in many of Mirai's variants, can cause its C&C server to temporarily shut down until reset manually by its operator.