April 1 – 7, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Georgia Institute of Technology has confirmed a data breach that exposed personal information of 1.3 million current and former faculty members, students, staff and student applicants. Exploiting a vulnerability in its web app, an unauthorized entity gained access to the university's central database.

- Last week Facebook was recorded asking users to share their email passwords. It has now been published that more than half a billion records of its users have been found exposed on unprotected Amazon cloud servers. Exposed datasets were collected and insecurely stored online by third-party Facebook app developers.

- A month after 2 million customer payment cards were offered for sale online, Earl Enterprises, an American hospitality firm , announced that criminals had hacked and stolen payment card details of dozens of its restaurants' customers over a period of 10 months. Affected restaurants include Planet Hollywood, Earl of Sandwich and others.

- The phone of Amazon chief, Jeff Bezos, has been hacked by Saudi Arabian authorities interested in access to his personal data. The findings come after Mr. Bezos accused the National Enquirer's parent company American Media Inc. (AMI) of blackmail.

- New York state capital Albany has been hit with a ransomware attack. This follows the March 1st Jackson County ransomware in which $400,000 had been paid, the March 18th attack on Orange County and this week's attack on Genesee County Michigan. Details of the specific type of malware used in Albany and whether ransom has been paid are yet unknown.

- German pharmaceuticals giant, Bayer, confirmed it had been attacked by the Winnti malware, a backdoor tool associated with Chinese hacking groups. The company recently removed the malware after it had been monitoring it for over a year stating there was no evidence of data outflow.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Backdoor.Win32.Winnti; Winnti.TC)

VULNERABILITIES AND PATCHES

- Check Point researchers have revealed that a security app, pre-installed on more than 150 million devices manufactured by Xiaomi, China's biggest and world's 4th largest smartphone company, was suffering from multiple vulnerabilities that could have allowed remote hackers to compromise Xiaomi smartphones.

  Check Point SandBlast Mobile customers are protected from this threat

- VMware has released security updates addressing security vulnerabilities, some of which had been exposed during the Pwn2Own 2019 hacking contest, when a team escaped a VMware workstation virtual machine and executed code on the underlying host operating system.
- Debian released security updates that fix multiple vulnerabilities with Thunderbird mail client, twig and dovecot Packages that could lead to DOS, information disclosure and Arbitrary Code Execution.
- Dropbox has uncovered 264 vulnerabilities, paying out $319,300 in bounties, after a one-day bug hunt in Singapore that brought together hackers from 10 nations around the world.

THREAT INTELLIGENCE REPORTS

- New families of credit card skimming code have been reveled in an analysis of JS sniffers. Researchers reported of a growing trend of JS-Sniffers being rented to cybercriminal in underground forums.

  Check Point SandBlast provides protection against these threats

- A recently published report has found that FIN6 cybercrime group, previously known for compromising Point-of-Sale (PoS) systems, has added ransomware to its portfolio and is currently using LockerGoga and Ryuk encryption malwares.
- 26,000 Kibana instances have been reported unprotected on the internet, many of them running outdated Kibana versions thus exposing Elasticsearch databases and systems to cyber-attacks. Banks, hospitals and universities are amongst the exposed enterprises.
- Still running older versions, estimates are that over 2 million Apache HTTP servers are exposed to a critical privilege escalation vulnerability (CVE-2019-0211) which had been recently patched by Apache.

For comments, please contact: TI-bulletin@checkpoint.com