Check Point
SOFTWARE TECHNOLOGIES LTD.

February 24 – March 1, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- An unprotected ElasticSearch database belonging to the sport retailer Decathlon in Spain has been discovered, exposing over 123 million records of employee and customer data. The archive, over 9GB in size, contains unencrypted employee and admin passwords, customer emails and more.
- The operators behind Sodinokibi ransomware claim that they have in possession 70,000 financial and work documents as well as 60,000 customer data records belonging to the US fashion house Kenneth Cole. The operators published a part of the data, threatening to release all of it if the fashion house refuses to pay ransom.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Sodinokibi)*
- A misconfigured web server belonging to the marketing company Straffic has been found, exposing 49 million email addresses, phone numbers and postal addresses of their users.
- Bretagne Télécom, a French cloud services company, has been hit by a DoppelPaymer ransomware attack during January 2020. The attackers successfully exploited the then-unpatched vulnerability in Citrix (CVE-2019-19781), and managed to encrypt 148 machines. The attackers stole some data during the attack, and published samples of it in DopplePaymer's recently-launched data leak website.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Doppelpaymer)*
- Hackers are sharing SQL databases from unsecured Amazon S3 buckets. The shared information from the SQL dumps contains at least 36,000 emails and logins from the affected websites.
- An electric utility department in Massachusetts has been hit by a ransomware attack, which took down some of its online resources. Supply of electricity and customer information was not impacted.
- Clearview AI, the facial recognition startup, has suffered a security breach that allowed unknown hackers to gain unauthorized access to a list of all of its customers, as well as number of users and searchers they conducted.

VULNERABILITIES AND PATCHES

- Multiple Zyxel Network-Attached Storage (NAS) devices are affected by a critical vulnerability that may allow unauthorized attackers to execute code on vulnerable devices. The vulnerability is due to insufficient sanitization of a username parameter in one of the device's CGI. Zyxel patched the flaw.

  Check Point IPS blade provides protection against this threat *(ZyXEL NAS Command Injection (CVE-2020-9054))*

- Over 1 billion devices are potentially affected by a flaw discovered in popular Broadcom and Cypress WiFi chips, which are integrated in various devices, from mobile phones, laptops and IoT. Exploitation of the bug may allow partial decryption of user communication via wireless network packets.

- Google has released a critical software update for Chrome to address a number of critical vulnerabilities; one of them, tracked as CVE-2020-6418, is actively exploited in the wild.

  Check Point IPS blade provides protection against this threat *(Google Chrome Type Confusion (CVE-2020-6418))*

- A critical vulnerability has been found in OpenSMTPD servers that may allow attackers to gain full control over email servers running OpenBSD or Linux OS. Attackers may use this flaw to execute arbitrary commands on the vulnerable servers with privileges of either root or non-root user.

- Threat actors are launching a hacking campaign exploiting a zero-day cross-site scripting vulnerability in WordPress plugin Flexible Checkout Fields. These attacks may allow the attackers to create themselves admin accounts and take over the vulnerable servers.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released a malware evasion encyclopedia, listing and categorizing known methods malware detect virtualized environments to evade analysis. The different categories include technique details, code examples, signatures to track attempts to apply these techniques and more.

- Hackers are actively scanning for Microsoft Exchange servers vulnerable to CVE-2020-0688, a remote code execution flaw that was patched by Microsoft two weeks ago. To exploit the flaw, attackers must find an internet-accessible, unpatched server and log in to it using credential stuffing.

  Check Point IPS blade will provide protection against this threat in its next online package *(Microsoft Exchange Server Remote Code Execution (CVE-2020-0688))*

- A new backdoor malware dubbed Mozart uses DNS packets to communicate with its C&C server in an attempt to evade detection. The backdoor, which arrives to a target system through phishing emails, uses the TXT records feature in DNS packets to store commands and data from the infected system.

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