June 29 – July 5, 2020

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Roblox, a multiplayer game platform, has suffered a data breach in which more than 1,800 user profiles were defaced with messages in support of Donald Trump's reelection campaign, and their avatars' clothes were changed to look like the President's. The Roblox credentials were publised on Pastebin and social media.

- MongoDB databases have been hit by ransomware attacks using GDPR as extortion leverage. The attacker used an automated script to wipe all content and left a note demanding a bitcoin ransom equivalent to $140, to be paid within two days. The attack hit 23,000 databases, almost 50% of the databases exposed online without a password.

- Xerox Corporation, based in the US and present in at least 160 countries, has suffered a Maze ransomware attack. The attackers threaten to publish over 100GB of company data.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Maze)*

- EvilQuest, a macOS ransomware is now also stealing key logs and cryptocurrency wallets. It is being spread through a fake Google Software Update package and through pirated versions of different software.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.OSX.EvilQuest)*

- FakeSpy Android infostealer is spreading via an SMS phishing campaign associated with the Roaming Mantis threat group. The malware, which is disguised as legitimate global postal-service apps, steals SMS messages, financial data, and more from the victims' devices.

  Check Point SandBlast Mobile provides protection against this threat

- A new variant of Try2Cry ransomware implements wormable capabilities to infect other Windows systems using USB flash drives and Windows shortcuts (LNK files).

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Try2Cry)*

VULNERABILITIES AND PATCHES

- Check Point researchers have found that Apache Guacamole, a popular infrastructure for remote work, is vulnerable to several critical Reverse RDP vulnerabilities.

  Check Point IPS blade provides protection against this threat (Apache Guacamole Remote Code Execution)

- F5 has released a security advisory to address a remote code execution (RCE) vulnerability (CVE-2020-5902) in the BIG-IP Traffic Management User Interface (TMUI). An attacker could exploit this vulnerability to take control of an affected system.

  Check Point IPS blade provides protection against this threat (F5 BIG-IP Remote Code Execution (CVE-2020-5902))

- Mozilla has released security updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. An attacker could exploit some of these vulnerabilities to take control of an affected system.

- Netgear has released security patches to address ten vulnerabilities affecting nearly 80 of its product, including issues discovered at the Pwn2Own contest.

- Microsoft has released two out-of-band emergency security updates through Windows app store addressing two remote code execution (RCE) vulnerabilities in its Windows Codecs (CVE-2020-1425, CVE-2020-1457).

- Samba Team has released security updates to address vulnerabilities in multiple versions of Samba. An attacker could exploit some of these vulnerabilities to take control of an affected system.

THREAT INTELLIGENCE REPORTS

- Researchers have discovered almost 250,000 sets of personally identifiable information of users from the UK, Australia, South Africa, the US, Singapore and other countries exposed in a multi-stage bitcoin scam.

- The University of Delhi has suffered from a data breach in its admit card download portal, which is a part of the official University website, causing the exposure of personal details of all student.

- Fitness firm V Shred has exposes 606GB worth of sensitive customer data. The breach occurred due to a misconfigured Amazon Web Service (AW). The data included personally identifiable information (PII) of 100,000 customers and trainers, including before and after body images, health condition and more.

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