June 07-14, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Audi and Volkswagen have experienced data breaches that affected 3.3 million customers. Between August 2019 and May 2021, unsecured data was left exposed on the internet by a mutual vendor. During that time, an unauthorized threat actor accesses the data.
- Researchers have observed a new wave of DDoS extortion by Fancy Lazarus, a threat group that is known for masquerading as various APT groups since 2016. The group is asking for a 2 BTC ransom (around $75,000) if companies want to avoid a severe DDoS attack.
- The FBI has warned critical infrastructure sectors regarding scammers impersonating construction companies and committing business email compromise (BEC) attacks. There have been hundreds of thousands to millions in losses since the campaign began in March 2021.

Check Point Harmony Mail provides protection against such threats

- Researchers have uncovered Siloscape, the first malware to target Windows containers to compromise Kubernetes clusters. Its main purpose is to open a backdoor into poorly configured Kubernetes clusters in order to run malicious containers.
- Researchers have discovered a 1.2 terabytes database of stolen data. The database contains 26 million login credentials, 1.1 million unique email addresses, more than 2 billion browser cookies, autofill data, and payment information extracted by malware that has yet to be identified.
- Slilpp, the largest online marketplace for stolen login credentials, was taken-down in a multinational operation led by the US Department of Justice. The US, German, Dutch, and Romanian law enforcement agencies have seized Slilpp's marketplace infrastructure and domain names.
- Threat actors have stolen roughly 780 GB of data, including games, source code, and debug tools, from EA games. According to the hackers, they have access to all EA's services and are selling them at a cost of $28 million.

VULNERABILITIES AND PATCHES

- Check Point Research recently disclosed four vulnerabilities in Microsoft Office's MSGraph component. The flaw has existed for several years and can be exploited to run code on a target machine. The vulnerability could be triggered once the victim opens a malicious Office file. The flaws were patched by Microsoft.
- Intel has released a patch that addresses 73 security vulnerabilities. The Intel Virtualization Technology for Directed I/0 products, the BIOS firmware for some Intel processors, and the Intel Security Library are among the products affected by high severity vulnerabilities.
- Microsoft's Patch Tuesday fixes 50 vulnerabilities, including seven zero-day flaws, six of which have been exploited before. The PuzzleMaker threat actors exploited two zero-days to gain remote code execution in Windows. Microsoft also released new cumulative updates for all supported versions of Windows.

  Check Point IPS blade provides protection against this threat *(Google Chrome Remote Code Execution (CVE-2021-21220), Microsoft Windows NTFS Elevation of Privilege (CVE-2021-31956))*

- Researchers discovered the Polkit privilege escalation vulnerability (CVE-2021-3560). This bug allows a threat actor to get a root shell by exploiting an authentication bypass vulnerability in the Polkit auth system service installed by default on many modern Linux distributions. A fix was released for this bug.
- Researchers have uncovered multiple vulnerabilities in Samsung mobile devices that allow malicious apps to steal victims' photos, videos and contacts and change settings, without any user consent or notice.
- Adobe has patched 41 vulnerabilities in ten of its products, including Adobe Acrobat, Reader, and Photoshop. There were no known actively exploited zero-day vulnerabilities among the flaws.

THREAT INTELLIGENCE REPORTS

- Check Point has released its Most Wanted Malware index for May 2021. Dridex has dropped from the index after being the topmost prominent malware globally, while Trickbot, a modular botnet and banking Trojan, rose to first place.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Trojan-Banker.Win32.Trickbot; Banking.Win32.Dridex)*

- Interpol has taken down thousands of online marketplaces that posed as pharmacies and sold fake drugs and medicine, half of which were fake and unauthorized COVID-19 tests. As part of this operation, Interpol and regulatory authorities from 92 countries took down 113,020 web links.
- Researchers have linked the Gelsemium threat group to the NoxPlayer Android emulator attack, called Operation NightScout, which targeted gamers from September 2020 to January 2021. The group used spear phishing emails with document attachments exploiting CVE-2012-0158 to deliver several malware.

  Check Point IPS blade provides protection against this threat *(Microsoft MSCOMCTL.OCX ActiveX Control Remote Code Execution)*