Check Point
SOFTWARE TECHNOLOGIES LTD.

February 8-14, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russian Internet and e-Commerce giant Yandex has suffered a breach that led to the exposure of almost 5,000 customer accounts. The breach was enabled by a system admin that sold unauthorized access to customer mailboxes.
- Threat actors have gained access to the industrial control system at a US drinking water treatment facility and leveraged the software to sabotage the water treatment process and increase the amount of sodium hydroxide. According to the FBI, the attackers' vector of access is still unknown.
- UAE government agencies have been targeted by a campaign most likely carried out by the Iranian espionage group Static Kitten. The campaign features phishing emails using Israeli geopolitics and Ministry of Foreign Affairs references.
- CD Projekt Red, a Poland-based video game developer, has disclosed that it suffered a ransomware attack in which source code for several games, some of them unreleased yet, has been stolen. Although the attackers have threatened to sell the stolen data, the company refused to pay the ransom.
- Researchers have uncovered two Android spyware, dubbed Hornbill and SunBird, most likely distributed by the Confucius APT, a state-sponsored group that promotes Indian agenda and targets mainly Pakistani and other South Asian targets.
- Discount Car and Truck Rentals, a popular Canadian company, has been hit by the DarkSide ransomware, resulting in disruptions to the company's rental service portal and possibly in the theft of some 120GB of data.

  Check Point SandBlast and Anti-Virus provide protection against this threat (Ransomware.Linux.DarkSide)
- Singaporean Telecom giant Singtel has fallen victim to an attack originating from a security flaw in a third-party file-transfer appliance. An Australian medical research institution has also suffered a similar attack. The software leveraged for the attack is Accellion, a legacy file-transfer platform.

VULNERABILITIES AND PATCHES

- Microsoft has patched some 56 vulnerabilities, among them three critical flaws that might lead to remote code execution. The flaws reside in the .NET 5 and .NET Core applications, and exploit takes place when parsing certain types of graphics files on systems running MacOS or Linux. A local privilege escalation flaw in Windows 10 and Windows Server, assigned CVE-2021-1732, was patched as well, and had already been exploited in the wild.

  Check Point IPS provides protection against this threat *(Microsoft Win32k Elevation of Privilege (CVE-2021-1732))*

- New Command Injection vulnerability has been discovered in D-Link DAP-1860 firmware Wi-Fi extenders. The flaw, assigned CVE-2020-27864, allows unauthenticated network-adjacent attackers to execute arbitrary code on vulnerable firmware versions.

- Adobe has addressed security vulnerabilities in Adobe Acrobat, Reader, Illustrator, Photoshop and more. The flaw assigned CVE-2021-21017 is a heap-based buffer overflow zero-day vulnerability in Adobe Acrobat and Reader and is already being exploited in the wild.

  Check Point IPS provides protection against this threat *(Adobe Acrobat and Reader Heap-based Buffer Overflow (APSB21-09: CVE-2021-21017))*

- SAP has released updates addressing 7 security flaws, among them a critical remote code execution vulnerability assigned CVE-2021-21477 in SAP Commerce and several critical flaws in SAP Business Warehouse.

- CISA has released some 23 security advisories warning against attack vectors and exploitable flaws in industrial control systems, including a vulnerability in Wibu-Systems AG's CodeMeter.

THREAT INTELLIGENCE REPORTS

- Researchers have developed a novel supply-chain attack technique and used it to access 35 high-profile organizations including Netflix, Apple, PayPal and Tesla. Called dependency confusion, the technique relies on the fact that software could include components from both private and public sources.

- A report reviews supply-chain risks to US election systems, focusing on how hardware and software components can provide potential backdoors.

- Journalists have published a long-term investigation concluding that Chinese intelligence services have planted backdoors in chips sold by California-based hardware maker Super Micro Computer Inc. that were later distributed across military networks and global technology companies.