February 22-28, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The biochemical systems at an Oxford university research lab currently studying the Covid-19 pandemic has been breached. Clinical research was not affected by the incident. Breached systems include machines used to prepare biochemical samples, and hackers are currently attempting to sell their access to those machines.
- Twitter has permanently suspended multiple accounts found to be part of four disinformation campaign networks, most likely operated by state-sponsored actors associated with Iran, Russia and Armenia. The Iranian infrastructure was previously used to disrupt the 2020 US presidential campaign discourse.
- Gmail accounts of global pro-Tibet organizations have been targeted by the Chinese APT TA413, an espionage group known for its operations against civil dissidents. The campaign leverages a customized malicious Mozilla Firefox browser extension to gain control over the victims' Gmail accounts.
- Npower, a British gas and energy supplier, has shut down its mobile application following a data breach that leveraged the application to steal sensitive customer information, via a credential stuffing attack.
- Bombardier, a Canadian plane manufacturer, has admitted it has suffered a data breach leading to the exposure of employee, customer and supplier information after some of the stolen data was leaked online by the attackers.
- Cybercrime group dubbed 'Hotarus Corp' has breached Ecuador's Ministry of Finance, as well as the country's largest private bank, Banco Pichincha. The group claims they have stolen data from the bank's network, and have recently posted online some 6,500 records, allegedly taken from the Ministry of Finance.
- American Telecom provider T-Mobile has disclosed it has suffered a breach, after multiple customers have fallen victim to SIM swapping attacks, in which a hacker ports the victim's number using social engineering to gain control over their account. Personal information and identification information were stolen.

VULNERABILITIES AND PATCHES

- VMWare has alerted its customers that a newly discovered critical vulnerability in its vCenter Server product, a management software for VMware vSphere environments, might allow an attacker to execute commands with elevated privileges. The flaw was assigned CVE-2021-21972. The flaw has already been exploited in the wild, as attackers have been observed scanning the web for vulnerable servers.

  Check Point IPS provides protection against this threat (VMware vSphere Client Remote Code Execution (CVE-2021-21972))

- Microsoft has patched a critical remote code execution vulnerability in Windows. The flaw, assigned CVE-2021-24093, is found in a Windows graphics component and impacts multiple Windows 10 and Windows Server versions.

- Critical authentication bypass vulnerability has been discovered in Rockwell Automation's Programmable Logic Controllers (PLCs). The flaw, assigned CVE-2021-22681, could enable an unauthenticated attacker to bypass verification mechanisms, connect to Logix controllers and modify their configuration.

- Cisco has released a security update to address three critical flaws affecting its ACI Multi-Site Orchestrator (MSO), Application Services Engine and NX-OS software, as well as other vulnerabilities. The most severe flaw is a remote bypass authentication assigned CVE-2021-1388, that affects an MSO's API endpoint.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released the annual Security Report for 2021. The report provides malware distribution and vulnerability exploit statistics for 2020, covers the biggest cyber incidents and reviews attack trends observed during the past year, including a rise in attacks against the healthcare sector, double extortion attacks and more.

- Several large-scale ransomware operations targeting mainly big corporations have recently shifted their focus from Windows OS machines to VMware ESXi Servers, and developed custom variants of their ransomware, capable of running on Linux OS machines.

  Check Point SandBlast and Anti-Virus provide protection against these threats (Ransomware.Win32.DarkSide; Ransomware.Linux.DarkSide; Trojan.Win32.Ransomexx)

- Researchers have investigated a campaign by the North Korean APT Lazarus that leveraged the ThreatNeedle malware family to target defense industry entities. The campaign uses Covid-19 themes in spear-phishing emails in addition to tailored personal information.

- New variant of the Ryuk ransomware has been observed in the wild. The new version implements self-replication capabilities within a local network among Windows-based machines.

  Check Point SandBlast and SandBlast Agent provide protection against this threat (Ransomware.Win32.Ryuk)