January 11-17, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The European Medicines Agency (EMA), responsible for the approval of medicine for the European Union, has been hacked, leading to the exposure of third-party documents related to the Covid-19 vaccines online.
- The Scottish Environment Protection Agency (SEPA), a public regulator with 1,200 employees, has suffered a ransomware attack by the Conti ransomware. The attackers have managed to steal company data and have begun leaking information online.

  Check Point SandBlast Agent and Anti-Virus provide protection against this threat *(Ransomware.Win32.Conti)*
- Threat actors have compromised a certificate issued by Mimecast, an email security provider, used to authenticate the connection to the company's designated Microsoft Office 365 products. The attack allows the actors to intercept the connection and hijack sent and received email messages.
- Espionage group Charming Kitten, linked to the Iranian government, has launched a phishing campaign targeting mobile devices, leveraging Christmas holidays theme and distributing emails and text messages.
- One of Germany's largest newspaper publishers, Funke Media Group, has been attacked by ransomware, impacting over 6,000 laptops and thousands of additional machines. The attack halted the activities at the company's editorial offices and several printing houses.
- Researchers have uncovered an attack operation dubbed 'Spalax' that began on 2020. The campaign targets Colombian entities, mostly related to the government, energy and metallurgical sectors.
- A new Android malware is masquerading as a Pakistani chat application, stealing users' personal data.

  Check Point SandBlast Mobile provides protection against this threat
- CISA has released a warning against attacks targeting organizational cloud services. The attacks use phishing as the main attack vector and leverage poor configuration and security practices, as well as the hybrid work format integrating organizational and home devices.

VULNERABILITIES AND PATCHES

- Dell has released a patch to address multiple vulnerabilities, among them a remediation for the flaw assigned CVE-2020-29493, a critical SQL injection vulnerability in the DELL EMC Avamar Server allowing a remote, unauthenticated attacker to execute SQL commands on the backend database.
- Adobe has addressed multiple security vulnerabilities in Adobe Photoshop, Illustrator, Animate and more. Among them is a critical heap-based Buffer Overflow vulnerability in Adobe Photoshop assigned CVE-2021-21006. The flaw could lead to arbitrary code execution.
- Microsoft has patched 83 security vulnerabilities, 10 of them rated critical. The flaw assigned CVE-2021-1647 is a critical remote code execution in Microsoft Defender, which resides in the Microsoft Malware Protection Engine. The flaw may have already been exploited in the wild.

  Check Point IPS provides protection against these threats (Microsoft Defender Remote Code Execution (CVE-2021-1647); etc)
- Two critical vulnerabilities have been discovered in Orbit Fox, a WordPress plugin. Both flaws, a privilege-escalation vulnerability and a stored XSS bug, impact over 40,000 users and can be exploited to inject malicious code into vulnerable websites.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a sophisticated network of Android mobile malware development on the darknet, operated by a threat actor called 'Triangulum'. Since early 2020, the actor has been offering for sale on underground forums a new MRAT called 'Rogue', composed of open-source and darknet tools.

  Check Point SandBlast Mobile provides protection against this threat
- Check Point Research has released a quarterly review of the brands most leveraged for phishing attacks. Microsoft leads the chart with 43% of phishing attempts globally, followed by DHL (18%) and LinkedIn (6%).

  Check Point Anti-Phishing provides protection against this threat
- Attackers have developed a technique to leverage the Windows Finger command to download and install a malicious payload into victim machines. The Finger command allows a local user to retrieve information about users of a remote machine.
- Jocker's Stash, the largest dark web marketplace for stolen credit cards and credentials, has announced that it will soon be shut down, following a decrease in the amount of credentials published on the portal.
- Researchers suspect ties between the Sunburst backdoor, distributed as part of the SolarWinds supply-chain attack, and a backdoor linked to Turla APT, a group affiliated with Russia, due to overlapping features.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat (Backdoor.Win32.SUNBURST; Trojan.Win32.TearDrop)