December 14-20, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Additional companies have been breached in the high-profile SolarWinds supply chain attack exposed last week. In addition to several US government agencies, Microsoft has confirmed that it was compromised, but states that no customer information or production services were accessed. The nation-state actors have also hacked Cox Communications, a digital cable and internet provider, and the networks of the US National Nuclear Security Administration agency.

  Check Point Anti-Virus and Anti-Bot blades provides protection against this threat (Backdoor.Win32.Sunburst)

- Two public school districts in Montana and Mississippi, one of them serving 7,000 students, have suffered an attack by the DoppelPaymer ransomware. Financial information wasn't affected, but a server containing student information was accessed.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.Doppelpaymer)

- Researchers have uncovered some 45 million medical imaging files left exposed on over 2,100 insecure internet-facing servers. The data belongs to healthcare facilities worldwide and includes x-rays and CT scans, as well as protected patient information.

- Threat actors have stolen millions of dollars from financial institutions in Europe and the US by leveraging mobile emulators, virtualization software mimicking mobile devices and spoofing legitimate financial accounts. Over 16,000 accounts have been compromised.

- Symrise, flavor and fragrant developer with products used by Nestle, Coca-Cola, and Unilever, has been hit by the Clop ransomware, resulting in the theft of 500 GB of data. The ransomware operators have released a data sample on their official data leak website.

  Check Point SandBlast Agent provides protection against this threat

©2020 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

- The Vietnam Government Certification Authority (VGCA) has been the victim of a supply-chain attack. The attackers embedded a backdoor into software installers available for download on the agency's website to compromise its application users.

VULNERABILITIES AND PATCHES

- HPE has disclosed a critical zero-day vulnerability affecting the latest version of its proprietary HPE Systems Insight Manager (SIM). The bug, assigned CVE-2020-7200, could allow an unprivileged attacker remote code execution.
- Researchers have released an in-depth analysis of five vulnerabilities in D-Link's DSL-2888A router, following the recently-released security patch. The flaws enable a local network or malicious Wi-Fi user to obtain access to the router's web interface and plaintext credentials and execute system commands.
- Bouncy Castle, a popular open-source cryptography library, has reported a severe vulnerability that could allow an attacker to access an administrator account. The flaw, assigned CVE-2020-28052, is the result of a cryptographic weakness in the password checking process.
- Apple has addressed eleven security vulnerabilities in its iOS and iPadOS mobile operating systems. The update features a fix for a flaw that could be leveraged by an attacker to execute arbitrary code via a malicious font file based two vulnerabilities assigned CVE-2020-27943 and CVE-2020-27944.
- Several vulnerabilities have been discovered in Medtronic's MyCareLink Smart 25000 Patient Reader product, a platform that gathers and transmits data from implanted cardiac devices. The vulnerabilities could be exploited by attackers to gain control over a paired cardiac device.

THREAT INTELLIGENCE REPORTS

- The NSA has released a warning against two attack techniques that might allow threat actors to bypass authentication mechanisms and obtain access to cloud resources and by that, collect credentials and establish persistent access.
- Researchers have demonstrated that sensitive information could be exfiltrated from an air-gapped machine, physically insolated from insecure networks, via a new technique relying on Wi-Fi signals transmitting the data and a custom malware, without the use of Wi-Fi hardware.
- Gitpaste-12, a recently-discovered Linux cryptomining worm, has been distributed in a new wave of attacks targeting IoT devices and web applications and exploiting some 31 vulnerabilities. The malware infrastructure is hosted on legitimate services such as such as GitHub and Pastebin.