December 21-27, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Lazarus group, an APT affiliated with North Korea, has targeted two healthcare entities – Ministry of Health and a pharmaceutical company involved in a COVID-19 vaccine development, probably in order to collect information about the advancements in the pandemic research.
- Microsoft software resellers have been leveraged by hackers to hack into Microsoft Office 365 customers, including security provider CrowdStrike, who was unsuccessfully attacked. Researchers suspect that the hacking group behind it is the same Russia-based group behind the SolarWinds supply-chain attack.
- New spam campaign has been delivering the Dridex banking Trojan using fake Amazon Gift Cards distributed via email. The email offers victims a link to a $100 gift certificate and features the original Amazon logo.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat *(Banking.Win32.Dridex; Trojan.Win32.Dridex)*
- Emotet has resumed its attack activities on Christmas eve, after a two-month break, in a campaign targeting over 100,000 users per day. The botnet has updated its payloads, improved detection evasion capabilities and changed its malicious macro document to disguise the payload installation flow.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Trojan.Win32.Emotet)*
- Livecoin, a Russian cryptocurrency exchange, has been breached on Christmas eve. Attackers managed to gain control over some of the exchange servers and modified the exchange rates.
- Following a breach to The Hospital Group, a UK cosmetic surgery chain, the REvil ransomware group has threatened to release celebrity before-and-after surgery photos, part of the 600 GB of stolen data.

  Check Point SandBlast Agent and Anti-Bot provide protection against this threat *(Ransomware.Win32.Sodinokibi)*
- Citrix has confirmed that some of its users have been suffering an ongoing Distributed Denial-of-Service (DDoS) attack affecting Citrix Application Delivery Controller (ADC). The attack uses the DTLS protocol as an amplification vector.

VULNERABILITIES AND PATCHES

- Two critical vulnerabilities have been found in the ThinOS operating system, affecting several versions of the Dell Wyse thin client, a simple machine optimized for remote connection. The flaws, assigned CVE-2020-29492 and CVE-2020-29491, allow access to the thin clients via FTP without the use of credentials.
- QNAP has published security updates to patch six high severity vulnerabilities affecting its Network-Attached Storage (NAS) devices running the operating systems QES, QTS and QuTS hero. Among these is a flaw assigned CVE-2020-2503 that allows a remote attacker to inject arbitrary code in File Station.
- Researchers have uncovered that a zero-day vulnerability in Windows print spooler API has been improperly patched. The privilege escalation bug, assigned CVE-2020-0986, allows an attacker to execute arbitrary code. No patch is in sight, and the flaw has already been exploited in the wild.

  Check Point IPS provides protection against this threat (Microsoft Windows Kernel Elevation of Privilege (CVE-2020-0986))

THREAT INTELLIGENCE REPORTS

- Check Point Research has performed an in-depth analysis of SUNBURST, the backdoor used in the renowned supply-chain attack leveraging the SolarWinds IT software, and its payloads, mainly the TEARDROP, a tailor-made malware dropper.

  Check Point Anti-Bot provides protection against this threat (Backdoor.Win32.Sunburst; Trojan.Win32.TearDrop)
- During the ongoing investigation of the SolarWinds supply-chain attack, a new backdoor called SUPERNOVA has been detected. Some researchers believe that the .NET web shell is the product of another APT group.
- The Pegasus spyware, offered for sale by known surveillance tech provider NSO Group, has been utilized by state operatives to hack and monitor some 36 Al Jazeera employees including journalists and producers. iOS devices were hacked via the Kismet exploit chain, which relies on a zero-click exploit in iMessage.
- The Department of Homeland Security warns US companies against cyber threats originating from China, mostly for the purpose of theft of intellectual property, confidential business information and private citizen data. It also recommends examining the use of equipment and data services developed by Chinese firms.
- Researchers have investigated the security state of smart doorbells and found that this entire device sector is highly vulnerable to attacks leveraging hardcoded credentials and authentication flaws, lacks security patches before shipment and suffers from critical security bugs.

For comments, please contact: TI-bulletin@checkpoint.com