Check Point SOFTWARE TECHNOLOGIES LTD.

Jan 18 - 24, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The CHwapi hospital in Belgium has been hit by BitLocker, encrypting 40 of its servers and 100 TB of data. The attack caused the hospital to redirect patients and delay surgical procedures.

  Check Point SandBlast Agent provides protection against this threat

- Cybersecurity firm SonicWall has suffered an attack on its internal system by unknown threat actors exploiting a zero-day vulnerability in the company's secure mobile access VPN and its VPN client.

- Buyucoin, an Indian cryptocurrency exchange, has suffered a data breach by a threat actor named ShinyHunters, known for stealing and selling website databases. The leaked data includes email addresses, country, hashed passwords, mobile numbers and Google sign-in tokens for the exchange's 160,000 users.

- The Russian Federal Security Service (FSB) has issued a security warning to organizations in Russia regarding possible retaliatory cyberattacks by the USA after the SolarWinds breach.

- A new wave of DDoS ransom attacks has been spotted targeting a large number of companies, requesting payment in Bitcoin.

- The Taiwanese hardware vendor QNAP has warned costumers of a new variant of Dovecat, a crypto-mining malware that is targeting Network-Attached Storage devices exposed online and using weak passwords.

- Malwarebytes has reported they were targeted by nation state actors as part of the SolarWinds breach. Evidence suggests abuse of privileged access to Microsoft Office 365 and Azure environments to gain access to a limited subset of internal company emails, with no evidence of unauthorized access.

- Threat actors have leaked 2.28 million user records from MeetMindful dating site. The data includes real names, Facebook account tokens, email addresses, and geolocation information.

- Porn site MyFreeCams has suffered from a data breach, and 2 million of its user records including plain text passwords, email IDs, and MFC tokens are now being sold on hacker forums.

VULNERABILITIES AND PATCHES

- A vulnerability has been reported in Windows NT LAN Manager (CVE-2021-1678), allowing remote code execution via an NTLM relay.
- Amazon has addressed a number of flaws affecting the Kindle e-reader that could have allowed an attacker to take control of victims' devices.
- Drupal has released a security update to address a vulnerability (CVE-2020-36193) that resides in the pear Archive_Tar third-party library.
- Cisco has fixed multiple flaws in Cisco SD-WAN products that could allow an unauthenticated, remote attacker to execute attacks against the device (CVE-2021-1138, CVE-2021-1140, CVE-2021-1142).

THREAT INTELLIGENCE REPORTS

- Check Point Research has encountered several attacks that exploit vulnerabilities on Linux devices using a new malware variant, called FreakOut. The threat actor behind the attacks infected many devices and incorporated them into a botnet, which in turn could be used for DDoS attacks and crypto-mining.

  Check Point SandBlast, IPS and Anti-Bot provide protection against this threat

- Check Point Research in collaboration with Otario, has uncovered a large-scale phishing campaign where the attackers unintentionally left over a thousand stolen log-in credentials accessible to the public by a simple Google search.
- Check Point research has found a new malware loader by the North Korea-linked APT group Lazarus, reusing old doc file decoy and macros, and using VBS scheduled task for persistence.
- A new malware has been discovered in the SolarWinds investigation. Named RainDrop, the malware is a loader that delivers a Cobalt Strike payload. On a similar note, Microsoft has released a deep dive into the Solorigate second-stage activation from SUNBURST to TEARDROP and the recent RainDrop.

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

- Researchers have warned of a publicly available fully functional exploit that could be used to target SAP enterprise software, exploiting a vulnerability that stems from a missing authentication check in their solution manager (CVE-2020-6207). A patch to this vulnerability was released in March 2020.
- Research shows how Microsoft Remote Desktop Protocol (RDP) can be exploited to amplify distributed denial-of-service (DDoS attacks), with more than 14,000 servers vulnerable.