November 23-29, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has analyzed a new global campaign that distributed Bandook, a 13-year old backdoor Trojan. Previous campaigns utilizing the malware were attributed to the Kazakh and the Lebanese governments. The current campaign targets multiple sectors and locations, hinting that the malware is part of an infrastructure offered for hire.

  Check Point SandBlast Agent provides protection against this threat (APT_Bandook; Backdoor.Win32.APT_Bandook)

- Baltimore County Public Schools has suffered a ransomware attack, possibly by Ryuk, disrupting its student virtual learning. The district, which serves 115,000 students, has been forced to call-off its virtual classes for a week.

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

- Rand McNally, a Chicago-based provider of technology for consumer electronics, commercial transportation and education, has been hit by an attack that crippled its network functionality, and took down the management platform of its electronic logging devices (ELD) used by truck drivers to log driving hours.

- Sophos, a UK-based cyber security vendor, has notified its customers that it has suffered a data breach due to misconfiguration. Accessed information includes customers' full names, email addresses and phone numbers.

- The Conti ransomware group has attacked the Industrial Internet-of-Things (IIoT) chip maker Advantech, demanding a 14 million USD ransom for the decryption and erasure of the stolen files. A 3GB archive, containing 2% of the stolen data, has already been published on Conti's designated leak website.

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

- US Fertility, the largest fertility clinic network in the US with 55 locations, has disclosed that it has been the victim of a ransomware attack, in which protected patient information may have been stolen, in addition to names, addresses, social security number and more.

VULNERABILITIES AND PATCHES

- Drupal, an open-source web content management framework, has issued an emergency update to address two critical flaws assigned CVE-2020-28948 and CVE-2020-28949. The vulnerabilities allow arbitrary PHP code execution on some versions of Drupal CMS.
- Critical flaw has been discovered in Real-Time Automation (RTA) 499ES EtherNet/IP (ENIP) Adapter Source Code Stack, a product for factory floor applications. Tracked as CVE-2020-25159, the flaw could be exploited by a remote attacker to hack the industrial control systems.
- VMware has released a temporary patch to address a critical command injection vulnerability in several products. Assigned CVE-2020-4006, the flaw enables an attacker to take control of an affected system.
- Administrative tools provider cPanel & WebHost Manager (WHM) has addressed a security flaw that could have allowed remote attackers to bypass two-factor authentication protection mechanism using valid account credentials.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a new mobile malware dubbed 'WAPDropper', which consists of a dropper module and a premium dialer module that subscribes the victims to legitimate premium services, in this campaign - telecommunication providers in Thailand and Malaysia, to manipulate money transactions.

  Check Point SandBlast Mobile provides protection against this threat

- Researchers have published a warning against a massive phishing campaign leveraging the popularity of virtual Thanksgiving dinner meetings to distribute phishing emails impersonating Zoom meeting invitations.
- A series of critical security flaws has been revealed by researchers, following an investigation of up-to-date implementations of DNS Cache Poisoning Attacks. These flaws leverage network side channels that exist in all operating systems, enabling an attacker to inject a malicious DNS record into a DNS cache.
- Fake modpacks for Minecraft, a successful sandbox-based video game with over 126 million monthly active users, have been distributed by attackers via Google Play, leading to more then 1 million infections of Android devices. The applications display heavy advertisements.
- Two applications by Chinese tech giant Baidu, Baidu Search Box and Baidu Maps, have been removed from Google Play Store after it has been discovered that they were leaking data, thus violating user privacy. The apps were downloaded by over 6 million US users.