Check Point
SOFTWARE TECHNOLOGIES LTD.

Dec 27 – Jan 2, 2022

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Vietnamese trading platform ONUS was victim of a ransomware attack leveraging the Log4j flaw on its payment system. Cyber criminals demanded a $5 million ransom in a double extortion scheme. ONUS refused to pay, so threat actors published for sale records of 2 million ONUS costumers.

  Check Point IPS provides protection against this threat (Apache Log4j Remote Code Execution (CVE-2021-44228))

- Photography Company Shutterfly was victim of a Conti ransomware attack. Four thousands devices were encrypted as well as 120 VMware ESXI servers. The stolen data includes legal agreements, bank account information, login credentials, spreadsheets and customer credit cards info.

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

- QNAP network-attached storage (NAS) devices are being hit with eCh0raix ransomware (aka QNAPcrypt) in a current wave of attacks. While the initial infection vector is unknown, hackers aim at encrypting pictures and documents before extorting the victims.

  Check Point Anti-Virus provides protection against this threat (Ransomware.Win32.Ech0raix)

- T-Mobile was victim of a data breach. Although affecting less customers than the previous breach in August, the latest attack may have resulted in SIM swapping for several phone owners, in addition to the compromise of phone call data, including call logs.

- PulseTV e-commerce website has disclosed a data breach affecting 200,000 customers. The company announced that names, addresses, emails and credit card details were compromised.

- BlackTech advanced persistent threat group that specializes in cyber espionage campaigns has been targeting Japanese organizations with new malware dubbed “Flagpro” for network reconnaissance. Their techniques include socially engineered phishing emails carrying a compressed file containing Excel documents with malicious macros.

  Check Point Threat Emulation and Threat Extraction provide protection against this threat

VULNERABILITIES AND PATCHES

- Apache has released version 2.17.1 of Log4j to address an arbitrary code execution flaw tracked as CVE-2021-44832, with a lower severity than the original Log4Shell (CVE-2021-44228).

  Check Point IPS provides protection against this threat *(Apache Log4j Remote Code Execution (CVE-2021-44832))*

- Microsoft has fixed a flaw that caused disruptions to mail delivery on on-premise Exchange servers, triggered as the year changed to 2022. The bug was a result of MS Exchange checking the version of its antivirus engine, which is now larger than its maximum storage, causing the engine to crash.

- Researchers have revealed 6 unpatched vulnerabilities in the Netgear Nighthawk R6700v3 router version 1.0.4.120, which could let an attacker take control of the device. Users were advised to change their credentials.

THREAT INTELLIGENCE REPORTS

- More than four years after the Shadow Brokers' Lost In Translation leak, Check Point Research shares new insights on DoubleFeature, the logging component leveraged inside DanderSpritz, Equation Group's post-exploitation framework.

- Apple AirTags are suspected to be used to track and steal cars. These heists appear to be the work of sophisticated groups who have the resources to reprogram car keys as they are located. High-end car models are the primary choice for these scheme.

- Vice Society ransomware gang has claimed responsibility for UK Spar wholesaler James Hall & Co. early December and is also being linked to a recent attack on the Norwegian media company Amedia AS, which forced the company to shut off some of its presses.

- AvosLocker ransomware operators provided a free decryptor and apologized after realizing they hit a US police department. The gang places the responsibility on their affiliates who seem to have locked the network without the operators' prior review.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Win32.AvosLocker)*

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