Jan 3 – 9, 2022

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A series of attacks targeting Russia's Ministry of Foreign Affairs has been attributed to North Korean APT group Konni. Threat actors gained access by leveraging a socially engineered phishing campaign with New Year greetings and stealing credentials, aiming at collecting intelligence.

  Check Point Anti-Bot provides protection against this threat *(Trojan.Win32.KONNI))*

- Threat actors have been targeting the UK National Health Service (NHS) using the Log4Shell flaw to hack compromised VMWare Horizon servers, likely as a reconnaissance phase.

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

- The website management solution company for Education FinalSite has been hit by a ransomware attack that disrupted thousands of schools receiving their services across 115 different countries.

- Fertility Centers of Illinois (FCI), US-based fertility clinics, has reported a breach concerning the personal health information of 80.000 patients as well as the company's employees. The attacker used an administrative account to gain access to widespread highly sensitive data.

- The Florida based healthcare provider Broward Health has suffered a significant breach impacting over 1.3 million individuals, in which cyber criminals gained access to patients' medical information.

- American based pharmacy service Ravkoo has suffered a data breach after their AWS cloud portal used for prescriptions was compromised. The pharmacy notified tens of thousands of their clients that their personal information might have been exposed.

- FIN7 hackers have been sending malicious USB devices through the US postal services, hoping to infect organizations in the transportation, insurance and defense industries. Once plugged in, the device will execute a BadUSB attack and run PowerShell commands for further exploit.

  Check Point Harmony Endpoint provides protection against this threat

VULNERABILITIES AND PATCHES

- Experts have found a new vulnerability related to the Log4J flaw. The vulnerability, tracked CVE-2021-42392, was rated critical in the H2 Java database console and could lead to a Java code injection.
- VMWare has issued a patch for a heap-overflow vulnerability (CVE-2021-22045) that could lead to Arbitrary Code Execution. This patch concerns Workstation, Fusion and ESXi products. The company urges users to disable CD-ROM and DVD devices running on virtual machines as a successful exploit will require CD image.

THREAT INTELLIGENCE REPORTS

- Check Point Research has found a new Zloader campaign involving the MalSmoke threat group. The malware exploits Microsoft's digital signature verification, and leverages the Atera legitimate software to gain initial access, with the goal of stealing user credentials and private information.

  Check Point Threat Emulation, Anti-Bot and Anti-Virus provide protection against this threat (Trojan-Downloader.Win.Zloader; Downloader.Win32.Zloader)

- Threat actors have been exploiting Google Docs and the larger Google Workspace suite in a phishing campaign. The attack requires mentioning the end-user in a comment in a Google Doc, and then the threat actor can easily send malicious links that get right into the target's inbox.

  Check Point Harmony Email and Office provides protection against this threat

- New ransomware family dubbed Night Sky targets corporate networks and uses double-extortion technique after having successfully stolen data.
- The FBI warns of fraudsters targeting Americans who post their phone number online with Google Voice authentication scams.
- Threat actor dubbed Elephant Beetle has been stealing millions of dollars by patiently lurking and studying their victim's environment for months. The financially motivated group will then exploit known vulnerabilities and target compromised Java-based web servers. Victims are mostly in Latin America.

  Check Point IPS provides protection against this threat (Primetek Primefaces Weak Encryption Remote Code Execution; IBM WebSphere Application Server Commons-Collections Library Remote Code Execution)

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