August 13 – 19, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have revealed a wave of Ursnif malspam campaign targeting Italy and operating from well-known Italian web email services. The campaign includes VBE file (encoded VBS) called "SCANSIONE.vbe" that is delivered via ZIP attachments in emails with the subject suggesting different documents in Italian.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Ursnif)

- Apple's internal systems have been hacked by an Australian 16-year old schoolboy numerous times over the course of more than a year. The young attacker has managed to download 90GB of secure files including highly secure authorized keys for logging into customer accounts.

- Hundreds of Instagram's accounts have been hijacked in a targeted attack attributed to Russian attackers. The attackers have modified personal information of the accounts, including the account names, profile pictures, passwords, email addresses, and Facebook accounts associated with the Instagram accounts.

- Cosmos Bank, India's second-largest cooperative bank, has fallen victim to a major ATM heist, with $13.5 million stolen out of it in three days. The attackers used cloned versions of the bank's debit cards, and compromised the bank's SWIFT inter-banking system, in order to conduct large-scale transactions and withdrawals.

- Security researchers have identified a new modular downloader dubbed 'Marap', being used in current targeted attacks against financial institutions. Marap is capable of downloading other modules and payloads, performing reconnaissance through a systems-fingerprinting module, as well as avoiding analysis and detection.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Marap; Marap)

VULNERABILITIES AND PATCHES

- Microsoft has released its Patch Tuesday for August, addressing 60 vulnerabilities in Microsoft Windows, Edge Browser, Internet Explorer, Office, ChakraCore, .NET Framework, Exchange Server, Microsoft SQL Server and Visual Studio; 2 of which had already been exploited in the wild at the time of the release.

  Check Point IPS blade provides protection against this threat *(Microsoft Word Remote Code Execution (CVE-2018-8414); Microsoft Graphics Remote Code Execution (CVE-2018-8344); Microsoft LNK Remote Code Execution (CVE-2018-8345))*

- Adobe has released its Patch Tuesday for August, addressing 11 vulnerabilities, including two arbitrary code execution vulnerabilities rated as critical affecting Adobe Acrobat and Reader software.

  Check Point IPS blade provides protection against this threat *(Adobe Flash Player Out-of-bounds read (CVE-2018-12824); Adobe Flash Player Security bypass (CVE-2018-12825); Adobe Flash Player Out-of-bounds read (APSB18-25: CVE-2018-12826); Adobe Flash Player Out-of-bounds read (APSB18-25: CVE-2018-12827))*

- Linux kernel maintainers have released security patches addressing two DOS vulnerabilities tracked as 'SegmentSmack' and 'FragmentSmack'. The vulnerabilities reside the Linux kernel's TCP stack, and may be exploited to cause a significant resource usage in Linux-based systems and lead to their reboot.

  Check Point provides protection against this threat

THREAT INTELLIGENCE REPORTS

- A new technique dubbed 'PhishPoint' allows attackers to bypass the protection mechanism implanted by Microsoft Office 365 and steal victims' credentials. The attack includes phishing emails containing a link to a SharePoint file which redirects the victim to a spoofed Office 365 login screen.

- A proof-of-concept for a new exploitation technique allows remote attackers to leverage critical unserialization vulnerabilities in PHP programming language to take full control over a web server. The exploits affect major content management systems (CMS), including WordPress and Typo3.

  Check Point IPS blade provides protection against this threat *(WordPress Core Phar Insecure Deserialization)*

- A potential distributed attack against urban water services has been disclosed. A potential attacker may leverage vulnerabilities found in smart irrigation systems left connected to the Internet, and use them to create an IoT botnet, increasing water consumption and causing a mass water crisis.

- A new version of AZORult Trojan has been spotted in the wild being used in campaign targeting devices globally. The campaign includes phishing emails containing a downloader which delivers the main malware with 2 payloads embedded in it. The first payload is AZORult info stealer, targeting local accounts, browsers, saved credentials and more, and the second is Aurora Ransomware.

  Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan.Win32.AZORult; Trojan.Win32. Aurora)*