Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The video streaming service Vevo, owned by Universal Music Group, Sony Music Entertainment, Abu Dhabi Media, Warner Music Group, and Alphabet Inc., has suffered a security breach caused by the OurMine threat group. About 3TB of data, including internal documents, were posted online and eventually removed at Vevo's request. The breach started with a compromised Vevo employee account on Okta, a single-sign-in app for workplaces.

- A large voter database, containing personal details of nearly 600,000 U.S voters, had been publicly available online. The records, which appear to include all registered voters in the state of Alaska, are part of TargetSmart's national voter file. Apart from personal details, some of the records contain highly personal information such as household income, descendant ages and even topics of interest on which the voter could be lobbied.

- Researchers have revealed a new LinkedIn phishing scam, targeting Gmail, Yahoo and AoL users, in which links to a compromised website are sent in private messages or InMail. The links send the victims to fake email entry pages asking for user name, passwords and phone numbers.

- Following the Equifax data-breach, the company announced that the Chief Information Officer and Chief Security Officer had departed their positions. Following the breach, Visa and Mastercard are reportedly taking measures to prevent misuse of the 200,000 credit cards leaked in the breach.

  Check Point IPS blade provides protection against this threat *(Apache Struts2 Content-Type Remote Code Execution; Apache Struts 2 Content-Disposition Remote Code Execution)*

- Researchers have revealed that about 15,000 Elasticsearch servers are unsecured, with 4,000 of them hosting the Point-of-Sale malware Alina and JackPoS. 99 percent of the compromised servers were hosted on Amazon Web Services' platform.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Nmap Scripting Engine Scanner Over HTTP Request; Trojan.Win32.Alina.*; Operator.Jackpos*)*

VULNERABILITIES AND PATCHES

- Security researchers have discovered vulnerabilities in Bluetooth components of over 5.3 billion devices. The vulnerabilities, codenamed "Blueborne" impact Bluetooth implementations in Android, iOS, Microsoft and Linux, and can allow attackers to take over devices and execute malicious code, or to run Man-in-the-Middle attacks and intercept Bluetooth communications. Patches will soon be released.

- In the September release of its security bulletin, Microsoft has addressed 82 bugs and vulnerabilities, including a zero-day remote code execution vulnerability that affects the .NET Framework (CVE-2017-8759), which according to researchers was leveraged in the distribution process of the FINSPY malware, possibly as part of a nation-state campaign against a Russian-speaking target.

  Check Point SandBlast and IPS blades provide protection against this threat *(Microsoft .NET Framework Remote Code Execution (CVE 2017 8759))*

- Adobe has released its September security bulletin, including two critical memory corruption bugs, a critical XML parsing flaw and others, in Adobe Flash Player, Adobe ColdFusion, and Adobe RoboHelp.

  Check Point IPS blade provides protection against this threat *(Adobe Flash Player Memory Corruption (APSB17-28: CVE-2017-11281); Adobe Flash Player Memory Corruption (APSB17-28: CVE-2017-11282))*

THREAT INTELLIGENCE REPORTS

- Check Point Researchers have spotted a malware targeting Android users dubbed "ExpensiveWall", spread via malicious apps. The malware is packed, thus able to evade Google Play's protections.

  Check Point SandBlast Mobile and Anti-Bot blades provide protection against this threat (Trojan.AndroidOS.ExpensiveWall)

- Check Point Researchers have found a new method for malware to bypass common security solutions. This technique, dubbed Bashware, leverages a new Windows 10 feature which enables users to run Linux features on Windows and may enable attackers to run malicious code undetected.

  Check Point SandBlast Agent provides protection against this threat

- Researchers have found a new remote access Trojan (RAT) which utilizes Gmail to connect with its C&C. The malware, dubbed Kedi, spreads by spear-phishing techniques and can be used to steal information. Uniquely, it can use HTML to contact its C&C, as well as DNS and HTTPs.

- Security researchers have found a new version of "Windows has been banned" ransomware in the wild. Upon booting, the malware presents victims with a screen claiming their OS has been banned by Microsoft due to a violation of the company's terms of use, demanding $50 in Bitcoin to restore the PC.

  Check Point Anti-Bot blade provides protection against this threat *(RogueSoftware.Win32.TechSupport.*)*