BIZCOMMUNITY

No environment is immune to cyber attacks

Check Point Software Technologies, a provider of cybersecurity solutions globally, released its "Cyber Attack Trends: 2019 Mid-Year Report", revealing that no environment is immune to cyber attacks.

Threat actors continue to develop new toolsets and techniques, targeting corporate assets stored on cloud infrastructure, individuals' mobile devices, trusted third-party supplier applications and even popular mail platforms:

- **Mobile banking**: With over 50% increase in attacks when compared to 2018, banking malware has evolved to become a very common mobile threat.

  Today, banking malware is capable of stealing payment data, credentials and funds from victims' bank accounts, and new versions of this malware are ready for massive distribution by anyone that's willing to pay.

Source: pixabay.com

- **Software supply chain attacks**: Threat actors are extending their attack vectors such as focusing on the supply chain.

In software supply chain attacks, the threat actor typically instils a malicious code into legitimate software, by modifying and infecting one of the building blocks the software relies upon.

- **Email**: Email scammers have started to employ various evasion techniques designed to bypass security solutions and anti-spam filters such as encoded emails, images of the message embedded in the email body, as well as complex underlying code which mixes plain text letters with HTML characters.

  Additional methods allowing scammers to remain under the radar of Anti-Spam filters and reaching targets' inbox include social engineering techniques, as well as varying and personalizing email content.

- **Cloud**: The growing popularity of public cloud environments has led to an increase in cyber attacks targeting enormous resources and sensitive data residing within these platforms. The lack of security practices such as misconfiguration and poor management of the cloud resources, remains the most prominent threat to the cloud ecosystem in 2019, subjecting cloud assets to a wide array of attacks.

"Be it cloud, mobile or email, no environment is immune to cyber attacks. In addition, threats such as targeted Ransomware attacks, DNS attacks and Cryptominers will continue to be relevant in 2019, and security experts need to stay attuned to the latest threats and attack methods to provide their organisations with the best level of protection," said Maya Horowitz, Director: Threat Intelligence & Research, Products at Check Point.

Top botnet malware during H1 2019

1. **Emotet (29%)** – Emotet is an advanced, self-propagate and modular Trojan. Emotet once used to employ as a banking Trojan and recently is used as a distributor to other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, it can also be spread through phishing spam emails containing malicious attachments or links.

2. **Dorkbot (18%)** – IRC-based Worm designed to allow remote code execution by its operator, as well as the download of additional malware to the infected system, with the primary motivation being to steal sensitive information and launch denial-of-service attacks.

3. **Trickbot (11%)** – Trickbot is a Dyre variant that emerged in October 2016. Since its first appearance, it has been targeting banks mostly in Australia and the U.K, and lately, it has started appearing also in India, Singapore and Malesia.

Top cryptominers during H1 2019

1. **Coinhive (23%)** – A cryptominer designed to perform online mining of the Monero cryptocurrency without the user's approval when a user visits a web page. Coinhive only emerged in September 2017 but has hit 12% of organisations worldwide hit by it.

2. **Cryptoloot (22%)** – A JavaScript Cryptominer, designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval.

3. **XMRig (20%)** – XMRig is open-source CPU mining software used for the mining process of the Monero cryptocurrency, and first seen in-the-wild on May 2017.

Top mobile malware during H1 2019

1. **Triada (30%)** – A Modular Backdoor for Android which grants superuser privileges to downloaded malware, as it helps it to get embedded into system processes. Triada has also been seen spoofing URLs loaded in the browser.

2. **Lotoor (11%)** – Lotoor is a hack tool that exploits vulnerabilities on Android operating system in order to gain root privileges on compromised mobile devices.

3. **Hidad (7%)** – Android malware which repackages legitimate apps and then releases them to a third-party store. It is able to gain access to key security details built into the OS, allowing an attacker to obtain sensitive user data.

Top banking malware during H1 2019

1. **Ramnit (28%)** – A banking Trojan that steals banking credentials, FTP passwords, session cookies and personal data.

2. **Trickbot (21%)** - Trickbot is a Dyre variant that emerged in October 2016. Since its first appearance, it has been targeting banks mostly in Australia and the UK, and lately, it has started appearing also in India, Singapore and Malesia.

3. **Ursnif (10%)** – Ursnif is Trojan that targets the Windows platform. It is usually spread through exploit kits - Angler and Rig, each at its time. It has the capability to steal information related to Verifone Point-of-Sale (POS) payment software. It contacts a remote server to upload collected information and receive instructions. Moreover, it downloads files on the infected system and executes them.

The “Cyber Attack Trends: Annual Report 2019 1H” gives a detailed overview of the cyber threat landscape. These findings

are based on data drawn from Check Point's ThreatCloud intelligence between January and June 2019, highlighting the key tactics cybercriminals are using to attack businesses.

Download the Check Point Software Technologies Cyber Attack Trends: Annual Report 2019 1H report (PDF File: 3.07MB)