EMOTET.TROJAN:

THE MOST DESTRUCTIVE MALWARE TO DATE IS BACK

SUMMARY

Emotet.Trojan, the sophisticated banking malware discovered in 2014, continues to be active still in 2020 with novel Techniques, Tactics, and Procedures (TTP). The malware aims to infect a massive number of endpoints and exfiltrate sensitive data.

Since the start of 2019, researchers have been observing an increase in the targeted emotet attacks across the globe. Between June 2019 and September 2019, the malware activity took a prompt interlude.

By the end of September 2019, emotet resumed its C2 server activity. Currently, the malware is spreading across the USA, Europe, and Australia and targeting digital users right from individuals to data-driven companies and national governing bodies. The US Department of Homeland Security described emotet as the most destructive malware to date for its persistence and ability to spread.

EVOLUTION OF EMOTET

Emotet is a customized banking Trojan, designed by the threat group named Mealybug. The malware is a combination of complex modules, each to perform a unique function, such as upgrading the malware to its latest version, rotation of C2 server to exfiltrate information, identify vulnerable WiFi networks, and whatnot!

VERSIONS

- During mid, late 2014, researchers found the first & second versions of emotet that intercepted network traffic with Automatic Transfer Systems (ATM) to steal payment data.

- In January 2015, the third version of emotet was observed, which evaded detection by anti-malware solutions and targeted the Swiss Bank.
- In December 2016, the fourth version of emotet spreading via the RIG 4.0 exploit kit was observed.

EMOTET TODAY

Since April 2017, emotet started spreading via high-volume email campaigns and launched a third-party Trojan, Dridex. Although researches declared the removal of banking functionality, the malware's modular design made it to infect via RIG exploits, network shares, and spam emails with links to zipped executables.

Recently detected traces of emotet found to have Wi-Fi worm module that enables the malware to spread rapidly across the devices of victims connected to insecure wireless networks.

HOW DOES EMOTET WORK?

1 INTRUSION VIA SPAM EMAILS

INTRUSION

Emotet malware can self-propagate using socially engineered spam emails, embedded with malicious script, links, macro-enabled documents (with file extensions .doc, .docx, Xls, and so on) or PDF attachments in a legitimate-looking theme that incline a target to download the attachment or click the URL. Emails with emotet use subject lines that can persuade a target to click on the link/document, such as:

- Your refund is here!
- Your invoice
- Track your order

To evade detection by threat intel databases, an emotet attacker first scans and compromises vulnerable websites/applications to host malicious emotet variants onto servers and starts distributing the malware.

Once a target opens infected attachments/ embedded URLs in the spam emails, the emotet payload gets downloaded from a malicious or compromised website and executed automatically.

After executing the payload, an attacker can customize the functionality of Emotet malware to allow communication with C2 (Command and Control) server or download another payload like Azorult, which can steal passwords, cryptocurrency wallets, and credit card details.

Recently, emotet attackers found using it as "Malware-as-a-Service" that allows other attackers to deploy additional malware in the target system (or) network. The malware can launch Trickbot that exploits eternal blue and double pulsar vulnerabilities in the Windows operating system to install secondary Trojans, such as “Ryuk” ransomware.

LATERAL MOVEMENT

When a target opens macro-enabled Outlook documents or malicious links, emotet starts executing automatically. The malware’s persistence and worm-like capabilities let it launch other malware onto end-points. The launched malware then starts harvesting payment data, access credentials, or any critical information from the affected devices. Emotet malware uses brute-forcing to gain access to admin accounts having weak passwords and drop itself in the systems within the network.

2 INTRUSION BY WI-FI INFECTION

INTRUSION

Recently another version emotet has been identified, which can spread to nearby Wi-Fi networks under certain circumstances. Now, emotet infected devices are a danger to both internal networks and any nearby wireless networks with the physical proximity of the original victim.

Initially, emotet uses a self-extracting RAR file on an initial victim device. Once the RAR file extracts itself, the malware starts the execution and profiling of nearby wireless networks by gaining access to Wi-Fi handles in the victim’s device.

After obtaining Wi-Fi handles, the malware starts enumerating available wireless networks on the victim’s device by calling the WlanEnumInterfaces function, which returns the enumerated wireless networks with all the information about the networks, including SSID, signal encryption, and network authentication method.

On receiving network data, emotet starts moving in a series of brute-forcing loops on each wireless network by using two internal lists of weak passwords until a successful connection attempt. Once the connection is successful, the malware then sleeps for a period of 14 seconds and sends an HTTP POST request to its C2 server.

LATERAL MOVEMENT

Once the connection with a new wireless network is successful, Emotet enumerates the list of servers and computers connected to this wireless network and starts brute-forcing. If the brute-force attack is successful, then emotet malware, copies itself in server/computer, using the credentials, and a new cycle of attack starts to enumerate the wireless network, present in the victim's physical proximity. As part of the persistence mechanism, the executable gets installed by masquerading itself as a legitimate windows service.

MITIGATION MEASURES AND SECURITY BEST PRACTICES

Below are a few mitigation measures and security best practices to secure endpoints and networks from emotet's infection.

- Update the malware definition file of Antivirus/Anti-malware solutions, daily
- Enable real-time protection and schedule a full system scan to run every week. Also, run a quick scan daily
- Restrain from connecting to public Wi-Fi networks
- Backdoor Trojans like Trickbot, use windows eternal blue vulnerability. Similarly, other malware exploits the recently released vulnerabilities. Hence, perform a vulnerability assessment to check and remediate all Operating systems and application-related vulnerabilities from time to time
- Use strong passwords to ensure zero brute force attempts and update user credentials regularly
- Check before opening an email. Block (or avoid) downloading strange attachments, and refrain from opening suspicious links
- On suspicion that a system is infected with emotet, isolate the suspected system from the network under professional observation

ABOUT SISA

SISA is a global Payment Security Specialist, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services and solutions.

SISA is a recognized PCI QSA, PA QSA, PCI ASV, P2PE-QSA, 3DS Assessor, PCI Forensic Investigator, and PCI PIN Security Assessor and has a comprehensive bouquet of advanced products and services for risk assessment, security compliance and validation, monitoring and threat hunting, as well as training for various payment security certifications.