EMOTET MALWARE

LOADER, TROJAN BOTNET, STEALER, BANKING TROJAN

Vairav Advisory Report

20th March 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 014441540

Email: mail@vairav.net

SUMMARY

Emotet is a highly dangerous and sophisticated Trojan that has evolved from a banking Trojan into a dropper, allowing it to reload malware onto devices and cause significant damage. It targets corporate victims and private users through mass spam email campaigns, and it can act like a worm, making it difficult to clean up. Emotet operates as a malware distribution service, allowing its operators to download additional payloads onto infected systems. The malware is known for creating a botnet of infected computers, which its operators sell access to in an Infrastructure-as-a-Service model. Emotet is also used to rent access to infected computers for ransomware operations. In 2021, international action coordinated by Europol and Euro just disrupted the Emotet infrastructure, and the operation was brought under the control of law enforcement. In the year 2023, there has been a concerning development with Emotet, as fresh instances of this Trojan have surfaced, displaying a shift in their attack strategy. This is particularly alarming as it suggests that the threat posed by Emotet is still persistent and evolving, despite international efforts to disrupt its operations.

Introduction of Cyber Adversary

In the murky world of cybercrime, few groups have proven to be as prolific and damaging as Mealybug, the notorious actor behind the Emotet Trojan. Since its inception in 2014, Mealybug has grown from a small-time hacker group to a major player in the underground economy, specializing in Malware-as-a-Service. Their Emotet Trojan has wreaked havoc on both corporate and private users, utilizing sophisticated techniques to evade detection and propagate itself like a worm. Mealybug's success lies in its ability to create a botnet of infected computers, which they then sell access to in an Infrastructure-as-a-Service model. This allows them to make a substantial profit while putting their victims under significant financial strain. As Mealybug continues to evolve and adapt its tactics, it is clear that they represent a significant threat to cybersecurity with the potential for devastating attacks and the ability to sell access to its botnet to other criminal groups.

Tactics, Techniques, and Procedure

The Emotet Trojan is primarily distributed through spam email campaigns that contain malicious attachments. The first stage of the infection involves social engineering techniques to persuade the victim to open an attached Microsoft Office file (.one). Once opened and macros enabled, the malware can execute its code without requiring any further user interaction. The downloaded files contain malicious VBA (Visual Basic Analysis) code that is triggered when the document is opened. The VBA code can utilize WMI (Windows Management Instrumentation) to launch a PowerShell/CMD script that downloads the malware's payload from a remote server.

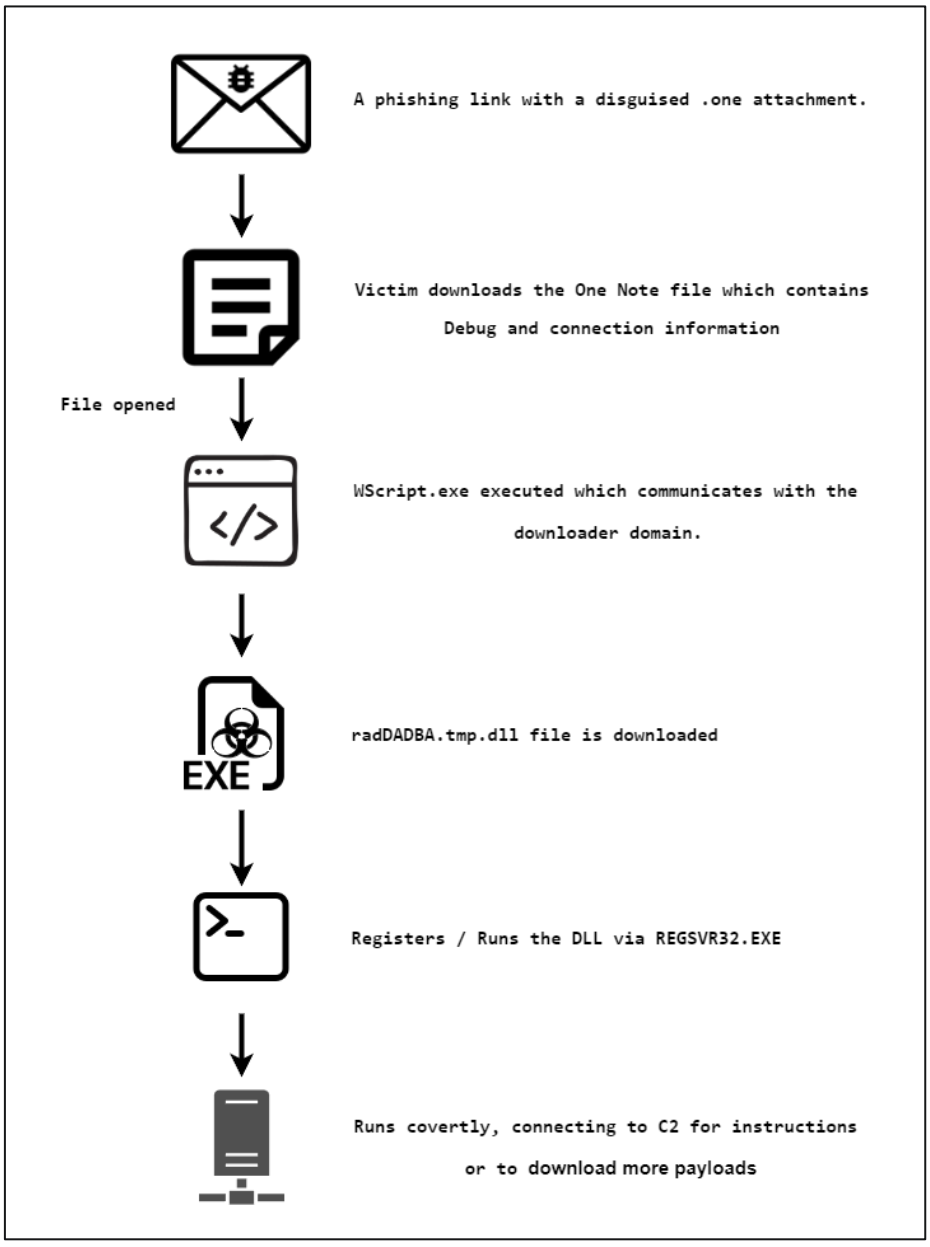

Figure 1: Emotet's chain of infection.

Notably, the PowerShell/CMD script is encoded, making it difficult to detect by traditional antivirus solutions. Emotet takes measures to establish a foothold in the infected system, such as copying itself into subfolders and modifying the value in the registry. Additionally, the malware allows the attackers to download further payloads and sends information to and from a remote server during the infection process. Finally, Emotet waits for commands from command-and-control servers as the last stage of execution.

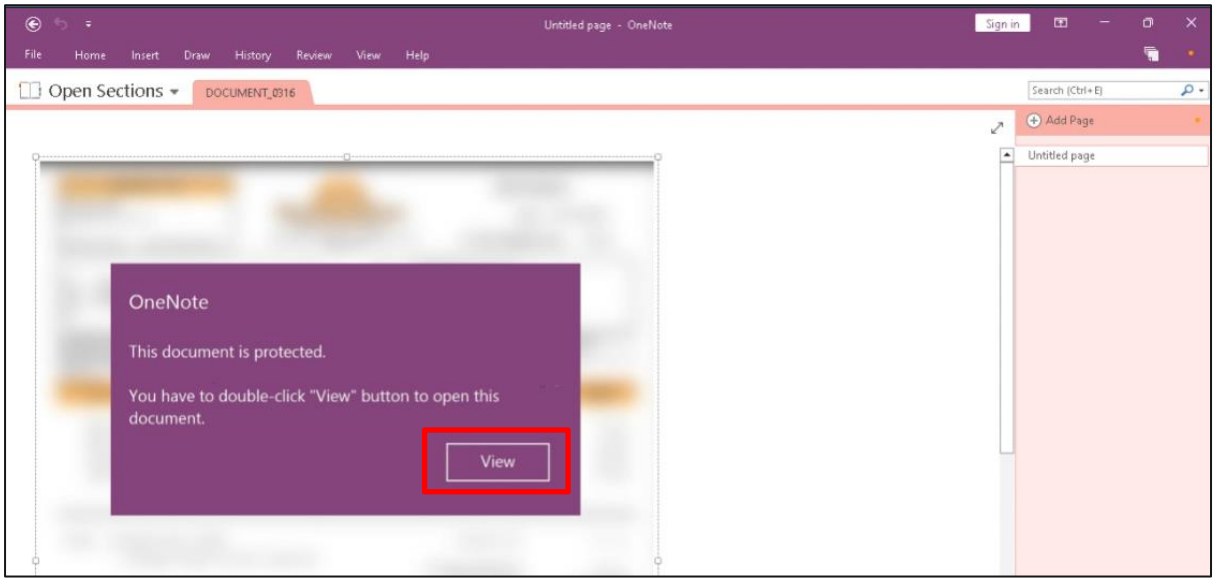

Figure 2: Opening the One Note file from the attachment.

Upon opening and clicking the View button on one note file it executes **wscript.exe**, and the following processes occur: The machine sends a TCP packet to IP address **203.26.41.131:443** using port **49719**. Upon conducting a Virus Total check on the IP address, it was discovered to be malicious.

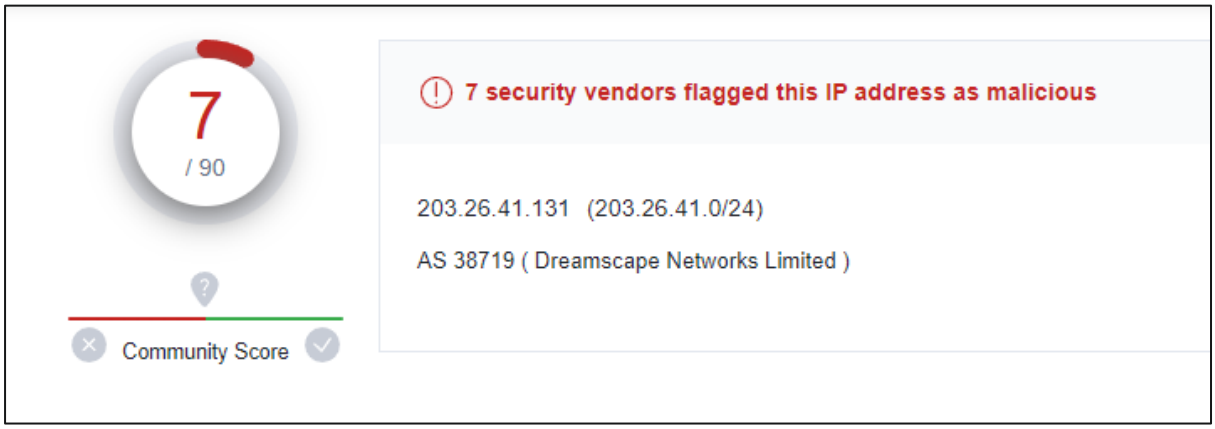

Figure 3: Virus Total score of the IP address the machine was communicating with.

Upon searching the IP address on AlienVault, it was found to be associated with 168 URLs, most of which were identified as malicious after being checked on Virus Total.

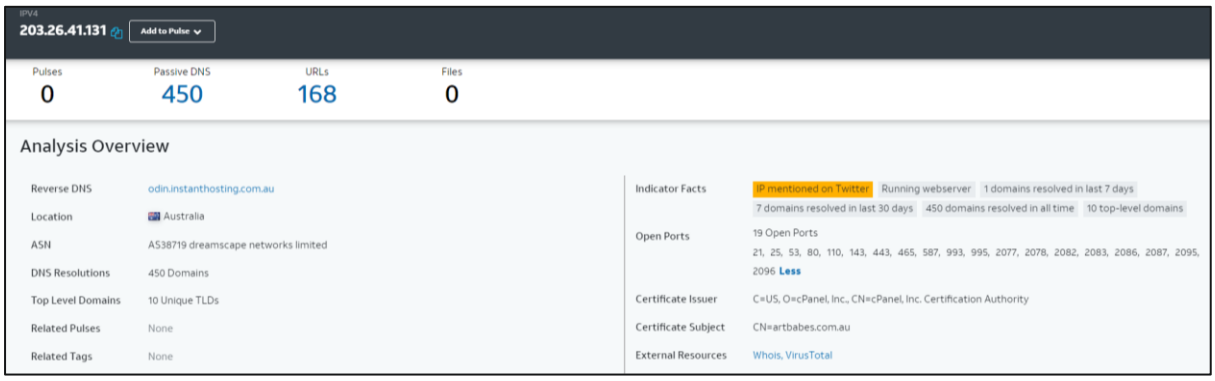

Figure 4: AlienVault result for the communicated IP address.

The malware dropped an executable file named **radDADBA.tmp.dll**, with an MD5 hash of **bfc060937dc90b273eccb6825145f298**. While checking the md5 on Virus total it was found that the file was a MALWARE TROJAN EVADER.

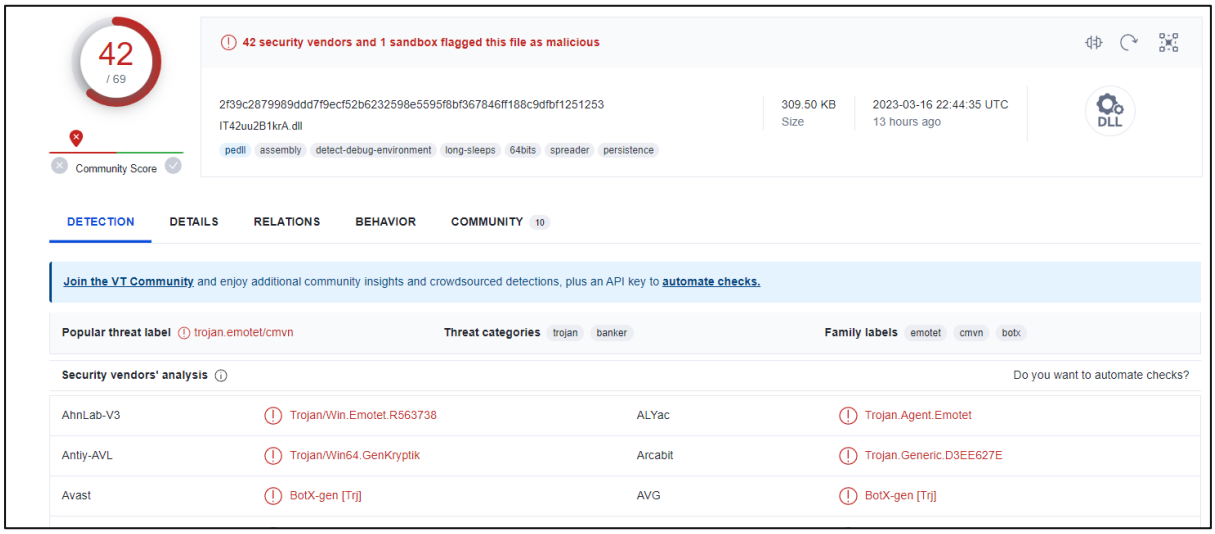

Figure 5: Virus Total score of the dropped file.

In a temporary directory "C:\Users\admin\AppData\Local\Temp\OneNote\16.0\Exported\" it creates multiple files. The same executable content radDADBA.tmp.dll, with an MD5 hash of **bfc060937dc90b273eccb6825145f298**, was dropped and overwritten. Now it registers/runs the DLL via regsvr32.exe and also drops the same .dll file again and again. After running regsvr32.exe it checks LSA protection, reads the software policy settings multiple times, also reads the settings of System Certificates, and lastly, it connects to the CnC server with IP **91.121.146.47:8080**.

MITRE ATT&CK techniques

The Emotet malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

Tactic	Technique
Initial Access	Phishing (T1566) • Spear phishing Attachment (T1566.001) • Spearphishing Link (T1566.002)
	Valid Accounts (T1078) • Local Accounts (T1078.003)
Execution	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003) • Visual Basic (T1059.005)
	Scheduled Task/Job (T1053) • Scheduled Task (T1053.005)
	User Execution (T1204) • Malicious Link (T1204.001) • Malicious File (T1204.002)
	Windows Management Instrumentation (T1047)
Persistence	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Create or Modify System Process (T1543) • Windows Services (T1543.003)
	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
	Valid Accounts (T1078) • Local Accounts (T1078.003)

Privilege Escalation	Boot or Logon Auto start Execution (T1547) • Registry Run Keys/ Startup Folder (T1547.001)
	Create or Modify System Process (T1543) • Windows Service (T1543.003)
	Process Injection (T1055) • Dynamic-link Library Injection (T1543.001)
	Scheduled Task/ Job (T1053) • Scheduled Task (T1053.005)
	Valid Accounts (T1078) • Local Accounts (T1078.003)
Defense Evasion	Obfuscated Files or Information (T1027) • Software Packing (T1027.002)
	Process Injection (T1055) • Dynamic-link Library Injection (T1543.001)
	Valid Accounts (T1078) • Local Accounts (T1078.003)
Credential Access	Brute Force (T1110) • Password Guessing (T1110.001)
	Credentials from Password Stores (T1555) • Credentials from Web Browsers (T1555.003)
	Network Sniffing (T1040)
	OS Credential Dumping (T1003) • LSASS Memory (T1003.001)
	Unsecured Credentials (T1552) • Credentials In Files (T1552.001)
Discovery	Account Discovery (T1087) • Email Account (T1087.003)
	Network Sniffing (T1040)
	Process Discovery (T1057)

Lateral Movement	Exploitation of Remote Services (T1210)
	Remote Services (T1021) • SMB/Windows Admin Shares (T1021.002)
Collection	Archive Collected Data (T1560)
	Email Collection (T1114) • Local Email Collection (T1114.001)
Command and Control	Encrypted Channel (T1573) • Asymmetric Cryptography (T1573.002)
	Non-Standard Port (T1571)
Exfiltration	Exfiltration Over C2 Channel (T1041)

Indicators of Compromise (IOCs)

IP Addresses

203[.]26[.]41[.]131

52[.]113[.]194[.]132

91[.]121[.]146[.]47

Hashes

bfc060937dc90b273eccb6825145f298

Domains

hxxp:// penshorn.org

Threat Summary	
Name	Emotet
Threat Type	Malware Trojan Evader
Detection Names	Trojan, Loader, Stealer, Banking Trojan
Symptoms	Emotet symptoms on infected computers include network traffic anomalies, changes to registry keys, new files and services, and suspicious network connections.
Additional Information	Emotet can bypass basic antivirus programs and spreads like a computer worm, attempting to infect other computers in the network.
Distribution methods	Spear-phishing techniques
Damage	It can steal sensitive information, spread it to other computers on the network, install additional malware, and even launch ransomware attacks. The damages caused by Emotet can include financial losses, data breaches, and reputational harm.
Malware Removal (Windows)	Removing Emotet malware requires a thorough cleaning of all infected systems and network devices, including running a reputable antivirus or antimalware software to detect and remove the malware. Additionally, all affected passwords should be changed, and any suspicious accounts should be investigated.

Vairav Recommendations

We recommend the following to mitigate and prevent ransomware attacks:

1. Implement robust email security

Organizations should implement email security measures such as spam filters, email gateways, and advanced threat protection to block malicious emails, including those containing Emotet malware. Emotet is typically spread through phishing emails that contain a malicious attachment or link. By implementing robust email security measures, organizations can prevent these emails from reaching their employees' inboxes, reducing the risk of a malware infection.

2. Blocking unwanted extension files in emails

The organization should block receiving of unwanted file extensions to be delivered via email. The extensions that need to be blocked are .one, .dat, .bat, .dll, .hta, and .iso. It is recommended to block the mentioned extension as they are being used to deliver the malware.

2. Educate employees about phishing

Employees should be educated on identifying and avoiding phishing emails, which are often used to spread Emotet malware. This can include providing training on how to spot and report suspicious emails, as well as regularly testing employees with simulated phishing emails.

3. Implement multi-factor authentication

Organizations should implement multi-factor authentication for all remote access and sensitive systems to prevent attackers from stealing login credentials. Emotet is often used as a means of gaining access to sensitive systems and data. By implementing multi-factor authentication, organizations can prevent attackers from using stolen login credentials to access these systems.

4. **Keep software and operating systems up to date**

Emotet can take advantage of vulnerabilities in software and operating systems to gain access to systems and spread them throughout a network. By keeping the software and operating systems up to date, organizations can reduce the likelihood of a successful Emotet attack.

5. **Use endpoint protection software**

Endpoint protection software can help detect and remove Emotet malware from infected systems, preventing it from spreading throughout a network. Regular scanning and updating of the software are necessary to ensure its effectiveness.

6. **Regularly back up important data**

Emotet is often used as a means of stealing sensitive data from organizations. By regularly backing up important data and storing it in a secure location, organizations can ensure that they have access to this data even if it is lost or stolen due to a malware infection.

7. **Monitor network traffic**

Monitoring network traffic can help detect and prevent Emotet malware infections. By monitoring for suspicious activity, organizations can take action to prevent the spread of malware.

8. **Have an incident response plan**

An incident response plan can help organizations respond quickly and effectively in the event of a malware infection. This can help prevent the spread of malware and minimize damage to systems and data.

9. **Perform Vulnerability Assessment and Penetration Testing**

Organizations should regularly perform vulnerability assessments and penetration testing of their networks, servers, and end-user zones to identify potential vulnerabilities and address them before they can be exploited by Emotet malware or other threats.

10. Have a Threat Intelligence

Threat intelligence can keep organizations informed about active and emerging threats like Emotet malware, helping them to recognize and defend against them. This can include subscribing to threat intelligence feeds, monitoring dark web forums, and conducting regular threat assessments.

It is of utmost significance to bear in mind that the cyber adversaries responsible for Emotet malware are prone to persistently adapt their tactics, tools, and procedures to circumvent detection and achieve triumph in their assaults. Hence, both organizations and individuals are urged to remain updated with the latest techniques, tactics, and procedures of Emotet and adopt pre-emptive measures to safeguard themselves against potential attacks.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Email: mail@vairav.net

Website: https://vairav.net