Return of Emotet malware | Zscaler

By Deepen Desai

Published: 2021-11-16 · Archived: 2026-04-05 13:31:58 UTC

Key Points

- Emotet is one of the most dangerous, prolific, and long-lasting malware Trojans that has ever existed.
- In January 2021, a law enforcement action disrupted the Emotet malware and its infrastructure. It also led to the arrest of some of the threat actors involved with the malware.
- After almost a year-long hiatus, Emotet has returned to the threat landscape as of Nov 14, 2021.
- Distribution of the malware was via the TrickBot malware and email campaigns.

After an almost year-long hiatus, the prolific malware Emotet has returned to the threat landscape. An early report indicated it returned on Sunday November 14, 2021 and it was being distributed via the TrickBot botnet. A later report indicated that it was also being distributed via email campaigns.

The Emotet malware was first detected back in 2014 and it focused on banking fraud. In recent years, Emotet pivoted and it became an initial access broker providing victim access for several ransomware groups.

In January 2021, law enforcement disrupted the Emotet malware and its infrastructure. It also arrested some of the threat actors behind it. This led to the disappearance of the malware for almost a year. Some security researchers thought it was gone for good...

While the Threatlabz team's technical analysis for the payloads involved is ongoing, the new version of the Emotet malware is similar to its past variants in many aspects. In our quick analysis, we've observed some changes in the command and control data and encryption used. It also appears to be using HTTPS instead of plain HTTP for command and control communication. It looks like most of the functionality is the same as earlier variants, and it will likely pick up where it left off, providing initial access to the ransomware operators.

Spam Campaigns

As we can see from the below screenshot of spam email, Emotet starts by leveraging a 'reply chain' email strategy in their spam campaigns. It has been using MS word document ".docm", MS excel ".xlsm" and password protected ".zip" files as attachments.


Image

Image 1: Reply chain email screenshots

Cloud Sandbox Detection


Image

Image 2: Zscaler Cloud sandbox detection

MITRE ATT&CK TTP Mapping

Tactic	Technique
T1010	Application Window Discovery
T1012	Query Registry
T1018	Remote System Discovery
T1055	Process Injection
T1036	Masquerading
T1057	Process Discovery
T1082	System Information Discovery
T1055	Process Injection
T1083	File and Directory Discovery
T1518	Security Software Discovery
T1547	LSASS Driver
T1218	Rundll32
T1562	Disable or Modify Tools

T1564	Hidden Files and Directories

Indicators of Compromise

IOC	**Notes**
c7574aac7583a5bdc446f813b8e347a768a9f4af858404371eae82ad2d136a01	Reference sample
81.0.236[.]93:443 94.177.248[.]64:443 66.42.55[.]5:7080 103.8.26[.]103:8080 185.184.25[.]237:8080 45.76.176[.]10:8080 188.93.125[.]116:8080 103.8.26[.]102:8080 178.79.147[.]66:8080 58.227.42[.]236:80 45.118.135[.]203:7080 103.75.201[.]2:443 195.154.133[.]20:443 45.142.114[.]231:8080 212.237.5[.]209:443 207.38.84[.]195:8080 104.251.214[.]46:8080 138.185.72[.]26:8080	Configured C2s

51.68.175[.]8:8080 210.57.217[.]132:8080 51.178.61[.]60:443 168.197.250[.]14:80 45.79.33[.]48:8080 196.44.98[.]190:8080 177.72.80[.]14:7080 51.210.242[.]234:8080 185.148.169[.]10:8080 142.4.219[.]173:8080 78.47.204[.]80:443 78.46.73[.]125:443 37.44.244[.]177:8080 37.59.209[.]141:8080 191.252.103[.]16:80 54.38.242[.]185:443 85.214.67[.]203:8080 54.37.228[.]122:443 207.148.81[.]119:8080 195.77.239[.]39:8080 66.42.57[.]149:443 195.154.146[.]35:443	
-----BEGIN PUBLIC KEY----- MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEQF90tsTY3Aw9HwZ6N9y5+be9Xoov	ECDH & ECDSA Key

pqHyD6F5DRTl9THosAoePIs/e5AdJiYxhmV8Gq3Zw1ysSPBghxjZdDxY+Q== -----END PUBLIC KEY----- -----BEGIN PUBLIC KEY----- MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE86M1tQ4uK/Q1Vs0KTCk+fPEQ3cuw TyCz+gIgzky2DB5Elr60DubJW5q9Tr2dj8/gEFs0TIIEJgLTuqzx+58sdg== -----END PUBLIC KEY-----	
-----BEGIN PUBLIC KEY----- MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE2DWT12OLUMXfzeFp+bE2AJubVDsW NqJdRC6yODDYRzYuuNL0i2rI2Ex6RUQaBvqPOL7a+wCWnIQszh42gCRQlg== -----END PUBLIC KEY----- -----BEGIN PUBLIC KEY----- MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE9C8agzYaJ1GMJPLKqOyFrlJZUXVI lAZwAnOq6JrEKHtWCQ+8CHuAIXqmKH6WRbnDw1wmdM/YvqKFH36nqC2VNA== -----END PUBLIC KEY-----	ECDH & ECDSA Key
015a96c0567c86af8c15b3fe4e19098ae9d0ea583e6bc0bb71c344fc993a26cf	Spam attachment
https://evgeniys[.]ru/sap-logs/D6/ http://crownadvertising[.]ca/wp-includes/OxiAACCoic/ https://cars-taxonomy.mywebartist[.]eu/-/BPCahsAFjwF/ http://immoinvest.com[.]br/blog_old/wp-admin/luoT/ https://yoho[.]love/wp-content/e4laFBDXIvYT6O/ https://www.168801[.]xyz/wp-content/6J3CV4meLxvZP/	Malicious URLs used in spam campaign, embedded inside “.docm” or “.xlsm” files

https://www.pasionportufuturo[.]pe/wp-content/XUBS/	

Explore more Zscaler blogs
