Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

After four months of idleness, Emotet reappears and deploys loaders

Date of Publication	Admiralty Code	TA Number
January 11, 2023	A1	TA2023019

Summary

First appeared: 2014
Attack Region: Worldwide
Attack: The latest distribution effort by Emotet makes use of the EtterSilent malware document builder and has implemented a new social engineering tactic through an Excel attachment that instructs users on how to bypass Microsoft's "Mark-of-the-Web" detection.

Attack Regions

Attack Details

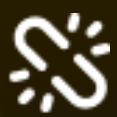
#1 The Emotet banking Trojan was initially found in 2014 as one of the most expensive and damaging malware. The phishing efforts that spread Emotet used the same email thread hijacking approach to deceive victims and spread malware.

#2 Emotet, which was initially designed as a banking Trojan, has transformed into a modular Trojan. Instead of being used as an independent Trojan, it now serves as a "loader-as-a-service" to disseminate other types of harmful malware.

#3 The campaign employs a unique social engineering tactic through a new Excel attachment with instructions for circumventing Microsoft's Protected View. When the file is opened, the macros instantly execute, initiating the loading of the Emotet virus.

#4 The attacker retains access to the system by adding several keys to the Windows registry, which will execute the DLL with regsvr32.exe at every restart. The Emotet malware version is a modular malware variant that is used as a downloader for other malware variants such as TrickBot and IcedID. It has been largely run by a Russian-based, financially motivated threat group, though this may not have been the case in recent campaigns.

Recommendations



Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0011** Command and Control
T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1040** Network Sniffing	**T1049** System Network Connections Discovery
T1102 Web Service	**T1106** Native API	**T1137** Office Application Startup	**T1218** System Binary Proxy Execution
T1547 Boot or Logon Autostart Execution	**T1566** Phishing	**T1573** Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	91.187.140[.]35 87.106.97[.]83 83.229.80[.]93 82.98.180[.]154 82.223.21[.]224 167.172.253[.]162 167.172.199[.]165 165.22.254[.]236 164.90.222[.]65 163.44.196[.]120 160.16.143[.]191 160.16.142[.]56 159.89.202[.]34 159.69.237[.]188 159.65.140[.]115
SHA256	e59c11ed62c813d1c19e02277e14bbeff0312440b4fdc235d3bcbfe1938743b6,ce2f3dddfce26433d18f020c8a3337d39d6d2af1eba61967db9be8359bf19fb1,91e19d7aefdd6717a1f79167281e78b95afb84195ba7525f5efb6e0a3665ac6b,36a2e445f25b38c95129260794ec0973b44f52ec69e8b819cf799fdab76319b5,09931bd43b6b1d5f664d4ea3b7d3b78a2e4a2e67a958032ea92640835d7b9f8f

TYPE	VALUE
SHA1	f8a58b9737cef1223e6cab7839f0921ab791317e d7412689e7f0df8f3425ffaf2a0ac5176202b9c3 ac5ad5ff7434c1ecbc3c96fcfc530a9f98f64a5e a7e30946af32f0087bbee19dcb908fce2d9e6814 91f1cabf131ca0dccd8180b6faed2fea24ffcddd 64af6f0e006d740601a92816d4eef1f7b6007b89 b7857b40b7e62fd5824c8d44cf3cf0afb993093d a6e306f8841ff6fbd50188c738469143a6934df0 53c841713e555456095cdeb74537d20c3ed840f3 05a0a49fc4dd8a0826265ccd3294ad6cfb84c1ae
MD5	ef0229e461dd8e1475537a44e3bfe3f6 a856da67745c9910bb6efd1a63755f3b 9ddfcfe774cbfa02fb31e36b819d7d91 6886babbe16ed7b5a8c84d54d2f9ca3e 5240ba05dc7e3179ab47487be788910e 154014e2aec1638d8feb1c3900752a60 f4239e545b7e85527babcf8cb130df6f e0b2f7f3feb79adcacf84e5e141ebd83 bc899c459a26537cea1e3dcca4fa2af9 6493581b246b731e4937fbee64a68803
URLs	hxxp://atici.net/old/PkZI74DD/oxnv3[.]ooccxx hxxp://clanbaker.org/css/khhl7kT2n69n/oxnv4[.]ooccxx hxxps://j2ccamionmagasin.fr/css/1Mp8y/oxnv2[.]ooccxx hxxps://cs.com.sg/Backup/Bk778kXNKMiH5vH/oxnv1[.]ooccxx

References

https://www.intrinsec.com/emotet-returns-and-deploys-loaders/?cn-reloaded=1

https://github.com/Intrinsec/IOCs/blob/main/Emotet/INTRINSEC_MLW_EMOTET_IOCs_09_01_2023.csv

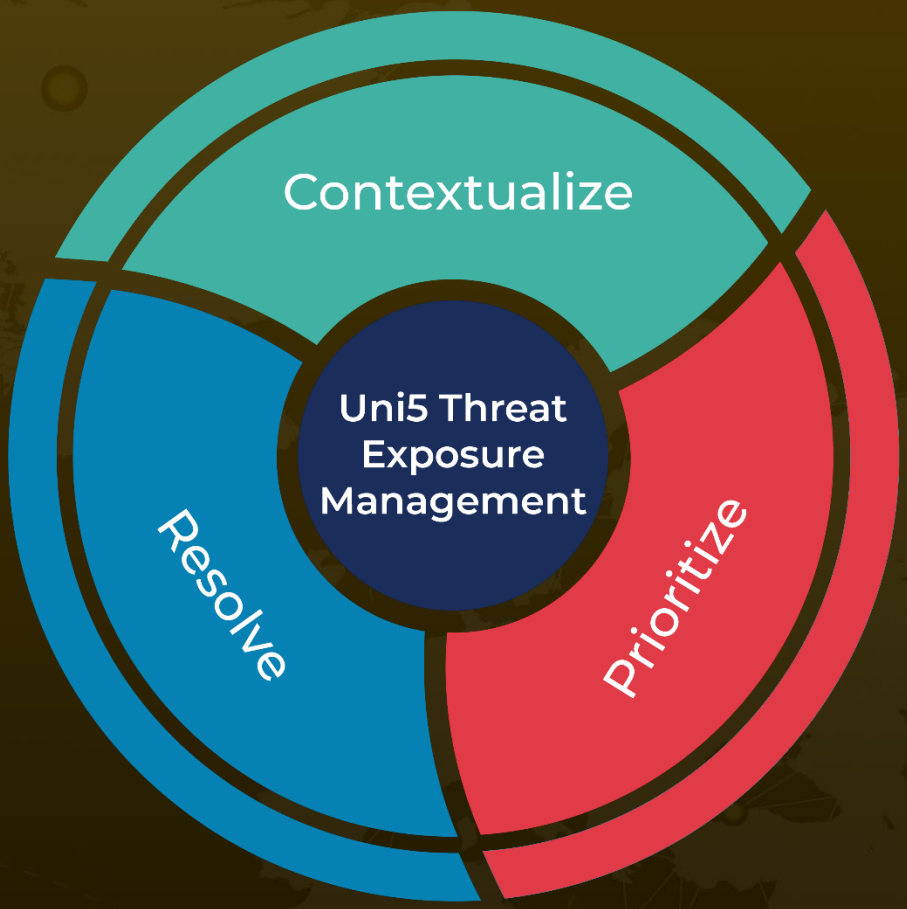
https://www.cisa.gov/uscert/ncas/alerts/aa20-280a

https://attack.mitre.org/software/S0367/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 11, 2023 • 3:33 AM

More at www.hivepro.com