https://web.archive.org/web/20200614054535if_/https://www.carbonblack.com/2019/04/24/cb-tau-threat-intelligence-notification-emotet-utilizing-wmi-to-launch-powershell-encoded-code/

CB TAU Threat Intelligence Notification: Emotet Utilizing WMI to Launch PowerShell Encoded Code | VMware Carbon Black

By Swee Lai Lee Malware Analyst @ VMware Carbon Black

Published: 2019-04-24 · Archived: 2026-11-24 02:10:46 UTC

Carbon Black recently learned that a customer had received a malicious email, which was written in German and was attached with a password-protected zip file that contained a malicious document file. This phishing email belongs to the recent Emotet campaign. However, what makes this malware unique is that the document contains malicious VBA code that uses WMI (winmgmts:win32_processStartup) to launch PowerShell with encoded code. This, in turn, downloads a second payload which is the Emotet banking trojan to compromise the victim's machine. Detailed analysis on the Carbon Black User Exchange can be found here.

(You may also find another recent Emotet campaign threat notification here.)

Behavior Summary

Upon execution, the malicious VBA code in the document will utilize WMI to launch powershell encoded code and then download the second stage payload, named as "615.exe", which is the Emotet banking trojan. Thus, the parent process of Wmiprvse.exe will be svchost.exe but not winword.exe.

The downloaded malicious payload "615.exe" will then further compromise in the victim's computer. It will copy and renamed itself to the path "c:\windows\syswow64\repstarta.exe" to continue its persistence in the computer.

Following is the overall process chart of this malware's activity.

e1.png

In addition, CB Defense will display the malicious document overall triggered TTPs.

e2.pnge3.png

If you are a Carbon Black customer and interested in learning about how CB solutions help protect against this attack, click here.

Remediation:

MITRE ATT&CK TIDs

TID	Tactic	Description
T1193	Initial Access	Spearphishing emails with malicious attachments sent to user

T1204	Execution	Users to launch malicious attachments delivered via spearphishing emails.
T1047	Execution	Windows Management Instrumentation (WMI) was used to execute powershell.exe
T1086	Execution	PowerShell was used to download and execute Emotet trojan
T1064	Defense Evasion, Execution	PowerShell executed with encoded instructions
T1043	Command And Control	Emotet Trojan used commonly used port for communication (e.g TCP port 80, 8080, 443, 8443, 7080, 20, 22, 53)

Indicators of Compromise (IOCs)

Indicator	Type	Context
d3c3a90d35f460a458e8ceb9d05bbad8a6650895e8ed2fbc4614f3e03efe6a0a cb396ae3d2b917da9e224e01c1a921d1	SHA256 MD5	Malicious Document
8ff26969cfa5b3cde5608889c479604f712c88570f3e194e40de9fea47a38c52 29aaf29ca1a17951c9bc7e8e617d2c24	SHA256 MD5	Malicious Zip File
61d35071519c66923542e0906df6da7ed2adba21dbb1f65551277d428af2b65e 14f10cd60a7541605e279c34218094f7	SHA256 MD5	Second stage Payload (Emotet Banking Trojan)
hxxps://inovatips[.]com/9yorcan/wb_fk/ hxxps://thetrendgift[.]com/dubf/m_Z/ hxxp://property-in-vietnam[.]com/cgi-bin/N_3s/	URL	Malicious URL used on second phase attack

hxxp://hahawaii[.]org/wp-admin/qw_6/ hxxp://quazar[.]sk/wp-includes/o_g9/		
103[.]12[.]133[.]7 104[.]236[.]135[.]119 105[.]101[.]6[.]219 133[.]242[.]156[.]30 138[.]201[.]140[.]110 147[.]135[.]210[.]39 162[.]243[.]125[.]212 167[.]114[.]210[.]191 173[.]255[.]196[.]209 173[.]255[.]250[.]241 174[.]106[.]108[.]31 174[.]93[.]130[.]148 175[.]100[.]138[.]82 178[.]62[.]37[.]188 184[.]22[.]6[.]124 186[.]4[.]234[.]27 187[.]189[.]195[.]208 187[.]198[.]57[.]250 189[.]159[.]103[.]149 189[.]190[.]169[.]221 190[.]161[.]186[.]116 192[.]186[.]96[.]125 200[.]126[.]225[.]56	IP Address	IP connected by Emotet Trojan

201[.]152[.]34[.]208

201[.]220[.]152[.]101

208[.]78[.]100[.]202

208[.]78[.]100[.]202

211[.]63[.]71[.]72

212[.]122[.]71[.]196

217[.]13[.]106[.]160

24[.]63[.]218[.]229

27[.]130[.]153[.]101

45[.]123[.]3[.]54

45[.]33[.]49[.]124

5[.]230[.]147[.]179

50[.]31[.]0[.]160

60[.]49[.]36[.]149

62[.]75[.]187[.]192

63[.]77[.]201[.]245

64[.]13[.]225[.]150

67[.]205[.]149[.]117

69[.]198[.]17[.]7

70[.]57[.]82[.]196

73[.]217[.]113[.]111

78[.]186[.]5[.]109

83[.]110[.]216[.]26

83[.]222[.]124[.]62

85[.]104[.]59[.]244

87[.]106[.]139[.]101

87[.]106[.]210[.]123 91[.]92[.]191[.]134 94[.]76[.]200[.]114 95[.]128[.]43[.]213		

Source: https://web.archive.org/web/20200614054535if_/https://www.carbonblack.com/2019/04/24/cb-tau-threat-intelligence-notification-emotet-utilizing-wmi-to-launch-powershell-encoded-code/