Trickbot Malware: new year—old lure

By Vinay Pidathala

Published: 2021-01-27 · Archived: 2026-04-06 00:05:00 UTC

2021 will be a challenging year for security professionals. The fall out from the SUNBURST attack and the Solarwinds hack is yet to be fully understood and we all remain in an elevated state of awareness and concern.

Our Threat labs team is constantly looking for new emerging threats by analyzing security events and over 40 million sessions a day on our isolation-powered cloud security company and recently observed the re-emergence of a previously known threat, commonly known as Trickbot.

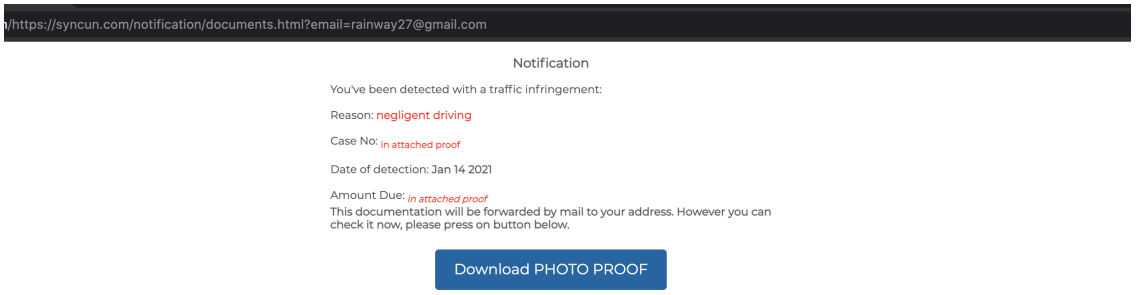
Trickbot is a prolific malware that has persisted through the times. In 2020 it was greatly responsible for distributing ransomware and was the most popular malware operation that used COVID-19 lures. It was so prolific that in Oct 2020, Microsoft along with its partners obtained a court order to disrupt and take down the infamous Trickbot. It did so by bringing down the infrastructure that was used by the attackers to distribute and send commands to infected endpoints.

In this blog, we are going to detail analysis of a campaign that shows how Trickbot infections might be back and active. In the most recent campaign we observed across our global Menlo Security cloud platform, we noticed the attackers used an interesting lure to get users to click and install the Trickbot malware on the endpoint.

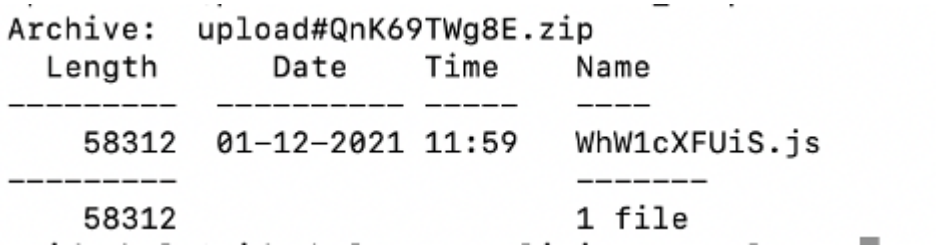
This ongoing campaign that we identified exclusively targeted **legal and insurance verticals in North America.** The initial vector appears to be an email, which includes a link to a URL. While in the past Trickbot has used weaponized documents, the infection mechanism detailed in this campaign seems to be a new modus operandi used by this group.Once the user clicks on the initial url in the email, the user is redirected to a compromised server that coaxes the user into downloading a malicious payload. The figure below shows the redirection chain.

#	URL	Result	Method	Process	Remote IP	Body Size
3	http://r.news.anicia.it/tr/cl/kSt5WYyxS9...	302	GET	chrome:5964	185.107.232....	90 bytes
5	https://palettas.pe/docs/notification.ht...	200	GET	chrome:5964	104.244.124....	22,909 bytes
7	https://palettas.pe/docs/images/bee.png	404	GET	chrome:5964	104.244.124....	236 bytes
11	https://palettas.pe/favicon.ico	404	GET	chrome:5964	104.244.124....	236 bytes
14	https://palettas.pe/docs/docs.php	200	GET	chrome:5964	104.244.124....	14,747 bytes

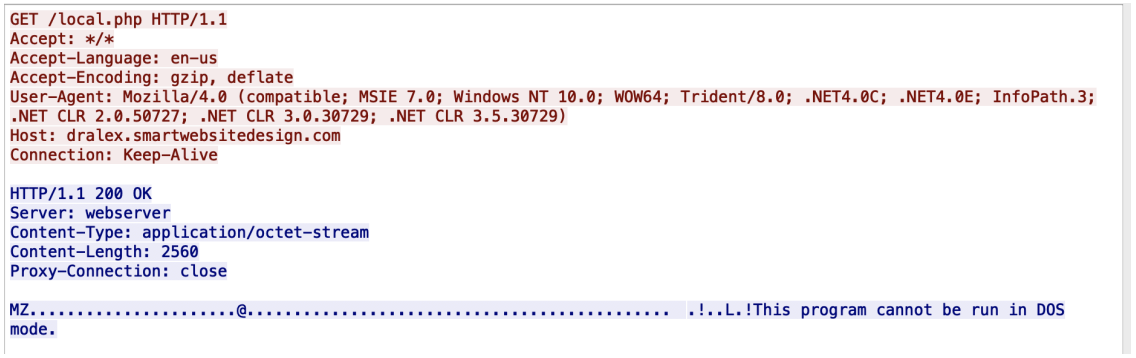
The final page that the user lands on, looks like the screenshot below. The Trickbot attackers are trying to scare the user into downloading a malicious payload, by using the lure of a traffic infringement.



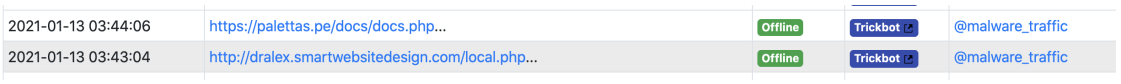
Clicking on the “Download Photo Proof” button, downloads a zip archive with a malicious javascript file to the endpoint.



The embedded javascript is heavily obfuscated, which has been a TTP typical of the Trickbot malware. If the user opens the downloaded javascript file, an HTTP request is made to the CnC server to download the final malicious binary.



Both the initial URL from which the malware is downloaded and the CnC that it connects to are tagged as Trickbot on URLHaus, which is a popular threat feed.



At the time of writing this blog, some of the URLs identified in this Trickbot campaign have very little to no detection on VT.

URLs

Scanned	Detections	URL
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=aclaro@barry.edu
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=peytonlaberge@gmail.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=fwgptkkccj@iccpeds.com
2021-01-16	1 / 83	https://syncun.com/notification/documents.html?email=pfahlmad@msu.edu
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=thatperson7058@gmail.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=tiffanymizell1@gmail.com
2021-01-12	0 / 83	http://syncun.com/
2021-01-16	1 / 83	https://syncun.com/notification/documents.html?email=tom.miklavcic@johnstonequipment.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=hfulghum@arts-engineering.com
2021-01-18	1 / 83	https://syncun.com/notification/documents.html?email=marlenescreations@yahoo.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=cpl100@hotmail.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=donna33@comcast.net
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=maryann719@hotmail.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=
2021-01-23	1 / 83	https://syncun.com/notification/documents.html?email=rainway27@gmail.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=amjcbsn006@yahoo.com
2021-01-15	0 / 83	https://syncun.com/notification/documents.html?email=gbagley@hpymca.org
2021-01-16	1 / 83	https://syncun.com/notification/docs.php
2021-01-19	1 / 83	https://syncun.com/notification/documents.html?email=redacted_email
2021-01-16	1 / 83	https://syncun.com/notification/documents.html

Menlo Labs is still analyzing the heavily obfuscated javascript and the binary payload that gets downloaded to the endpoint. We intend to publish additional details about similarities and differences if any between pre and post takedown efforts of this botnet.

Conclusion:

Where there’s a will, there’s a way. That proverb certainly holds true for the bad actors behind trickbot’s operations. While Microsoft and it’s partners' actions were commendable and trickbot activity has come down to a trickle, the threat actors seem to be motivated enough to restore operations and cash in on the current threat environment. Shut the door on threat actors for good with Menlo Security solutions.

Source: https://www.menlosecurity.com/blog/trickbot-new-year-old-lure