TrickBot Campaign Uses Fake Payroll Emails to Conduct Phishing Attacks

unit42.paloaltonetworks.com/trickbot-campaign-uses-fake-payroll-emails-to-conduct-phishing-attacks/

Bryan Lee, Brittany Barbehenn, Mike Harbison

December 9, 2019

By Bryan Lee, Brittany Barbehenn and Mike Harbison

December 9, 2019 at 6:00 AM

Category: Cloud, Malware, Unit 42

Tags: Bot, cloud malware, Cybercrime, GSuite, Phishing, Trickbot

This post is also available in: 日本語 (Japanese)

Executive Summary

By using a combination of Cortex XDR and the AutoFocus contextual threat intelligence service, Unit 42 discovered a recent Trickbot campaign leveraging legitimate cloud service providers to obfuscate malicious delivery behavior.

Trickbot is a well-known, modular credential stealer first discovered in 2016. It has been thought to be a descendent of another well-known credential stealer called Dyreza, or Dyre, due to similarities in functionalities and codebase. Due to its modularity, operators of Trickbot are able to gain access to different functions and capabilities by retrieving additional modules from the command and control (C2) servers. These include capabilities such as a worming function (i.e. copying itself to other devices), email inbox parser, and network reconnaissance.

Between November 7 - 8, 2019, Unit 42 identified a Trickbot distribution campaign delivered via phishing emails with subject lines using topics around payroll or annual bonuses shown below.

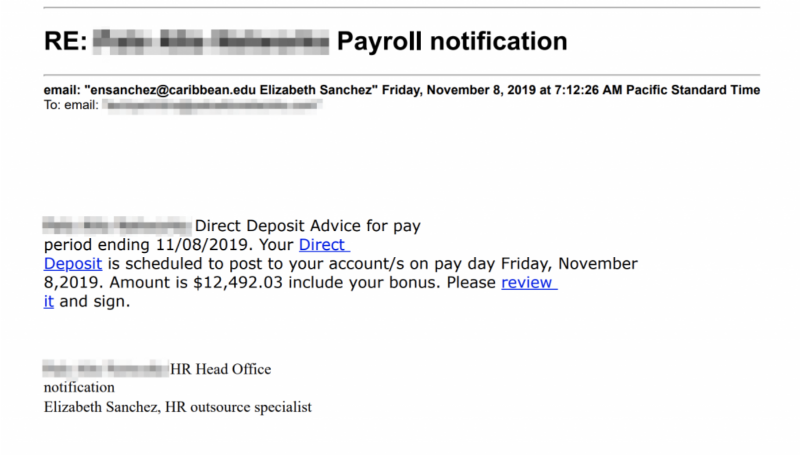
- “Re: <Company Name> annual bonus document is ready”
- “Re: annual bonus form for <name>”
- “RE: <name> Payroll notification”
- “RE: <Company Name>Payroll notification”

Generally, Trickbot and similar tools have been largely associated with using malspam with malicious document attachments as the delivery mechanism of choice by their operators likely due to ease-of-use, relatively low resource cost, and high success rates. In this campaign, instead of solely relying on email attachments, the adversaries included links to what appeared to be a legitimate Google Docs document which itself contained links to malicious files hosted on Google Drive. To further obfuscate the malicious activity, the adversaries leveraged a legitimate Email Delivery Service (EDS) called SendGrid to distribute the initial emails, and also hide the Google Drive links in the documents behind a SendGrid URL.

Once the user is fully redirected to the file hosted on Google Drive, an executable file is downloaded. This executable is a downloader tool designed to retrieve a Trickbot payload. Similar behavior was observed in August 2019 by Cofense.

Attack Details

The emails sent by the attackers appeared to originate from individuals at .edu email addresses which were likely compromised by the adversary. They then used SendGrid's EDS to distribute the actual emails. This would have increased their likelihood of bypassing email filters, as it is a popular service used by organizations around the world. The body of the emails contained lure text consistent with the subject lines and links that utilized a SendGrid function called *Click Tracking* which sends a notification back to the sender of the email for tracking purposes. The following screenshots show a sampling of the emails received:

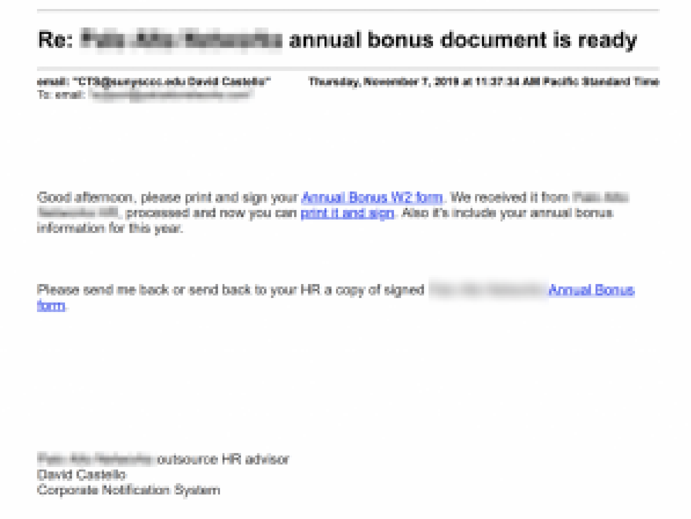


RE: [redacted] Payroll notification

email: "ensanchez@caribbean.edu Elizabeth Sanchez" Friday, November 8, 2019 at 7:12:26 AM Pacific Standard Time
To: email: [redacted]

[redacted] Direct Deposit Advice for pay period ending 11/08/2019. Your Direct Deposit is scheduled to post to your account/s on pay day Friday, November 8,2019. Amount is $12,492.03 include your bonus. Please review it and sign.

[redacted] HR Head Office
notification
Elizabeth Sanchez, HR outsource specialist



Re: [redacted] annual bonus document is ready

email: "CTS@sunyscc.edu David Castello" Thursday, November 7, 2019 at 11:37:34 AM Pacific Standard Time
To: email: [redacted]

Good afternoon, please print and sign your Annual Bonus W2 form. We received it from [redacted], processed and now you can print it and sign. Also it's include your annual bonus information for this year.

Please send me back or send back to your HR a copy of signed [redacted] Annual Bonus form.

[redacted] outsource HR advisor
David Castello
Corporate Notification System

Figure 1. Screenshots of Trickbot phishing emails

Once the victim clicks on the links, they are redirected to a Google Doc document which has a link to a file hosted on Google Drive. This file is a simple downloader which has a single function of retrieving the Trickbot payload then executing it on the victim host. The attack flow can be seen in Figure 2.

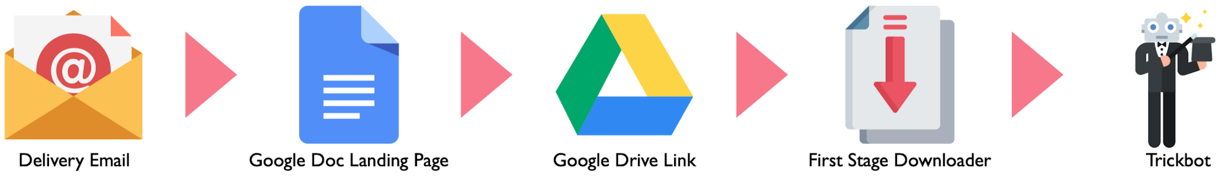


Figure 2. Trickbot attack chain

In this campaign, we identified two downloaders:

Phishing Theme	File Name	SHA256

Annual bonus	StatementReport.exe	b8c2329906b4712caa0f8ca7941553b3ed6da1cd1f5cb70f1409df5bc1f0ee4a
Payroll	Preview_Report.exe	f8aaf313cc213258c6976cd55c8c0d048f61b0f3b196d768fbf51779786b6ac6

Table 1. Trickbot downloader files

Both of these downloaders are signed by PERISMOUNT LIMITED and appear as Microsoft Word documents to Windows users, as shown in Figure 3. Due to default settings in most Windows deployments of not displaying file extensions, these files will not appear as obvious executables to a victim. Once these files are executed by the victim, a decoy pop-up is displayed to reduce suspicion of any malicious behavior. Regardless of whether or not the user hits “OK” or closes the pop-up window, the file will still proceed with the download and installation of the Trickbot payload. The payload in this case is a file named MHk6kyiq.Z6O and is saved in the user’s temp directory where it is eventually executed.

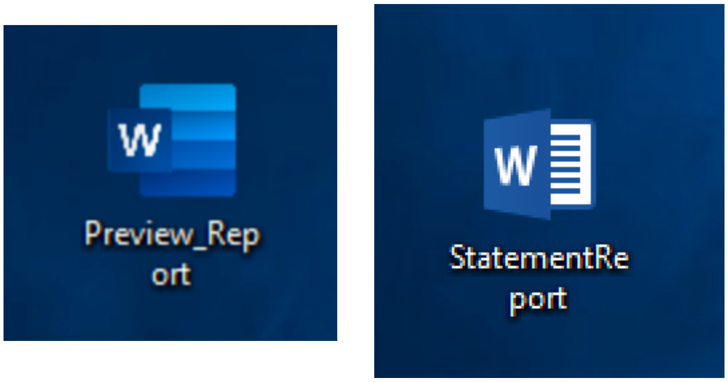
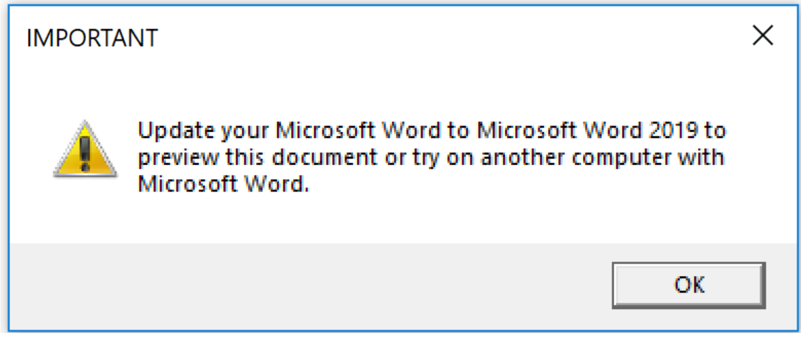


Figure 3. Downloaders using Microsoft Word icons



IMPORTANT

Update your Microsoft Word to Microsoft Word 2019 to preview this document or try on another computer with Microsoft Word.

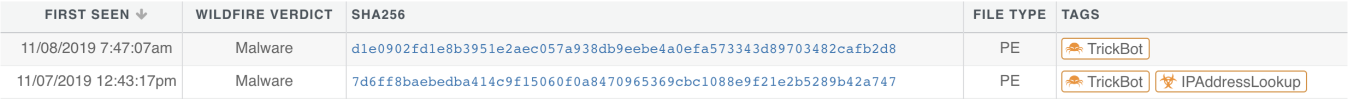
Figure 4. Decoy pop-up from downloader

Using Cortex XDR and AutoFocus, we observed that once the files were executed by the victim, they would then retrieve the corresponding Trickbot payload from a first stage C2 server. Analyzing these domains indicate that they are owned by legitimate organizations which suggests the adversaries were able to compromise the legitimate servers and hijack them to be a part of their delivery infrastructure. This tactic further increases the chance of evasion by the adversary as it is unlikely these domains would be categorized as malicious and in some cases, may actually have legitimate business use cases for the targeted organizations. Table 2 below depicts the downloader and URL used for each Trickbot payload.

Downloader	**C2**	**Trickbot Payload File**	**SHA256**
StatementReport.exe	savute[.]in/supp.php	nfdsus12.exe	d1e0902fd1e8b3951e2aec057a938db9eebe4a0efa573343d89
Preview_Report.exe	lindaspryinteriordesign[.]com/supp.php	nfdusdarm.exe	7d6ff8baebedba414c9f15060f0a8470965369cbc1088e9f21e2b

Table 2. Trickbot Payload Download Locations

The two payloads, nfdsus12.exe and nfdusdarm.exe, were immediately identified as Trickbot by the AutoFocus threat intelligence service via the tagging system. AutoFocus tags are groupings of behaviors that are designed to immediately identify specific malware families, threat actors, campaigns, or exploits. These tags are developed and maintained by the Unit 42 research team and are continuously updated as threats evolve.



FIRST SEEN ↓	WILDFIRE VERDICT	SHA256	FILE TYPE	TAGS
11/08/2019 7:47:07am	Malware	d1e0902fd1e8b3951e2aec057a938db9eebe4a0efa573343d89703482cafb2d8	PE	TrickBot
11/07/2019 12:43:17pm	Malware	7d6ff8baebedba414c9f15060f0a8470965369cbc1088e9f21e2b5289b42a747	PE	TrickBot IPAddressLookup

Figure 5. Trickbot payload tagging in AutoFocus

This specific variant appeared to be a newer version of Trickbot, using the file path %APPDATA%\cashcore to store its files and configurations. Once the payload is executed, it will spawn a child process (svchost.exe) in a suspended state, replace the memory with malicious code, and resume the process. The technique is known as process hollowing. From there, basic system information is collected, and it will attempt to communicate to its second-stage C2 infrastructure to retrieve additional modules.

Using Cortex XDR and its data analytics processing engine, we were able to validate this activity via the causality chain function as shown in Figure 6.

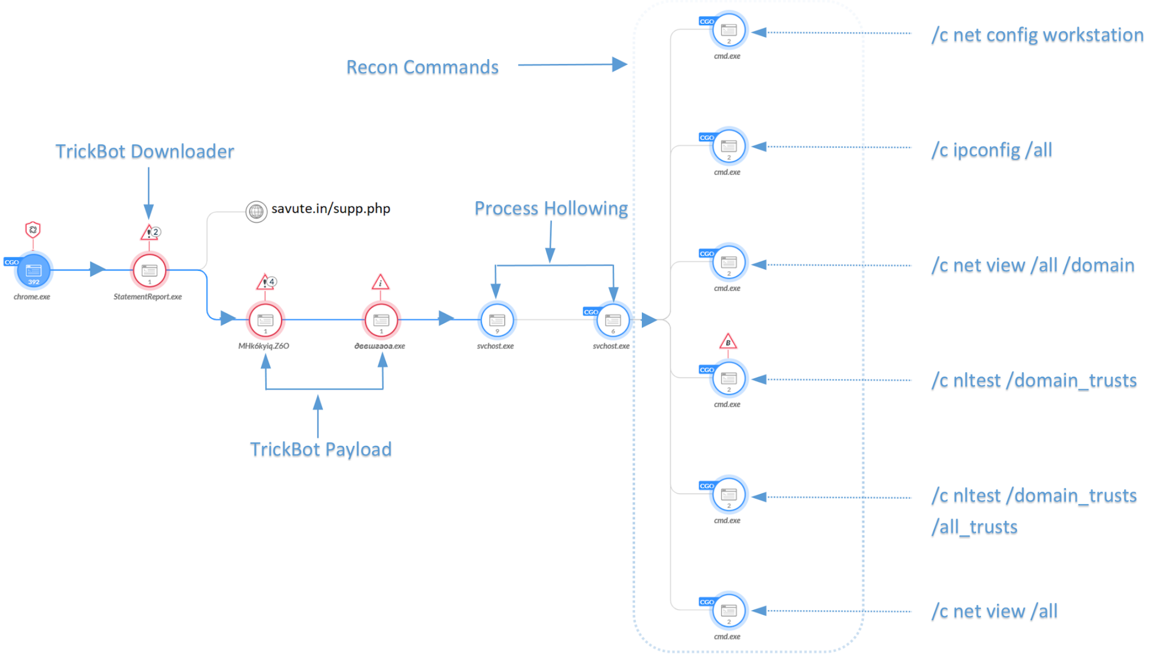


Figure 6. Cortex XDR causality chain

This workflow illustrates the described attack chain:

1. Initial downloader, statementreport.exe is executed by the user
2. Performs an HTTPS GET request to savute[.]in/supp.php
3. Payload file MHk6kyiq.Z6O is downloaded to the victim and saved in the user's temp folder.
4. Payload is executed by the downloader and the downloader terminates
5. Payload is renamed to двшгаоа.exe and copied to the users %APPDATA%\cashcore directory
6. File versioninfo.iniis created in the %APPDATA%\cashcore directory. This file is similar to older Trickbot variants that use the file settings.ini. Unlike settings.ini, versioninfo.ini is not encrypted or obfuscated, but contains random data to appear like a legitimate ini file.
7. двшгаоа.exe spawns an instance of svchost.exe which spawns another instance of svchost.exe which is then injected with the Trickbot payload. In this example, a built-in network recon module was run, which enumerated the victim host and network.
8. For persistence, this Trickbot variant created a scheduled task named System cache service which is scheduled to run at user logon and upon initial execution checks itself every 11 minutes to see if it is already running.

The Wider Campaign

Using AutoFocus, we used the string supp.php within the URL as a pivot point to search for any other files that were delivered from that URL. An additional five samples were discovered that were also all tagged as Trickbot, making a total of seven samples. These samples used a different C2 delivery server, but behaviorally were the same. The two additional C2 servers also appeared to be legitimate domains which had likely been compromised and hijacked by the adversaries. Details about these samples can be seen in Table 3.

Executing another search in AutoFocus looking for the occurrence of the string cashcore within any File Activity revealed over 800 additional samples, also all tagged as Trickbot. These samples were all ingested into our WildFire malware analysis platform between November 4 - 22, 2019, suggesting that this specific variant was first found earlier this month and is currently still in use. These samples also encompassed a range of Trickbot related files, from the Trickbot payload itself as well as various Trickbot modules. All known indicators for this variant of Trickbot is available in the indicators section of this blog.

Date Observed	C2	Trickbot Payload	SHA25
11/7/19	clementeolmos[.]com/supp.php	erfd1.exe	24e3fa3
e9fd22631de9c918ac834eb14e01c76aa4d33069c7622daafcd03b4f1574aad0			
d7687e1d98484b093e8da7fb666b2d644197fc3ea22b3931a6150c259479b0c			
11/19/19	maisonmarielouise[.]org/supp.php	SetupDesktop.exe	dc8f25
b3d2e7158620ece90fbc062892db55bf564c6154eb85facab57a459e3bd1156f			

Table 3. Additional Trickbot payloads observed

Conclusion

By using a combination of Cortex XDR and AutoFocus, Unit 42 researchers were able to rapidly identify and discover behaviors associated with a newer Trickbot campaign without significant manual analysis. In this campaign, we discovered the adversaries leveraging legitimate services such as SendGrid and GSuite in an effort to obfuscate malicious activity. With the wider adoption of various cloud services by most organizations, these types of tactics should be expected to occur with even more frequency as these are additional avenues that can be abused by an adversary to evade detection.

In this campaign, due to the abuse of legitimate cloud services, the detection and prevention of the initial delivery may have been more challenging than if the adversaries had used their own infrastructure. However, having a policy, such as preventing unknown executable files to be downloaded or executed on the endpoint, may help prevent these attacks from succeeding against businesses.

- Palo Alto Networks customers may learn more via AutoFocus and the Trickbot tag.
- All Trickbot samples are properly detected as malware in WildFire
- Trickbot C2 URLs have been added to URL Filtering

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org. *(This is added to blogs pre-shared with the CTA, when loaded into WordPress it will be added when appropriate).*

Indicators of Compromise

Trickbot Downloader Samples

f8aaf313cc213258c6976cd55c8c0d048f61b0f3b196d768fbf51779786b6ac6

b8c2329906b4712caa0f8ca7941553b3ed6da1cd1f5cb70f1409df5bc1f0ee4a

Trickbot Payload Samples

7d6ff8baebedba414c9f15060f0a8470965369cbc1088e9f21e2b5289b42a747
d1e0902fd1e8b3951e2aec057a938db9eebe4a0efa573343d89703482cafb2d8
24e3fa3fb1df9bd70071e5b957d180cd51bcf10bab690fa7db7425ca6652c47c
e9fd22631de9c918ac834eb14e01c76aa4d33069c7622daafcd03b4f1574aad0
d7687e1d98484b093e8da7fb666b2d644197fc3ea22b3931a6150c259479b0c6
dc8f259fb55a330d1a8e51d913404651b8d785d4ae8c9c655c57b4efbfe71a64
b3d2e7158620ece90fbc062892db55bf564c6154eb85facab57a459e3bd1156f

Trickbot Payload URLs

savute[.]in/supp.php
lindaspryinteriordesign[.]com/supp.php
maisonmarielouise[.]org/supp.php
clementeolmos[.]com/supp.php

Related Trickbot SHA 256

List of hashes on GitHub