TrickBooster – TrickBot's Email-Based Infection Module

deepinstinct.com/2019/07/12/trickbooster-trickbots-email-based-infection-module/

July 12, 2019

Learn more

July 12, 2019 | adinah_b

250 million Email addresses harvested and counting…

Author: Shaul Vilkomir-Preisman

Supporting research: Tom Nipravski

Update: Further developments on how TrickBooster operates is accessible here.

Ever since its discovery in 2016 TrickBot has remained a continuously active and very adaptive actor in the cybercrime threat landscape. What was once a malware family focused on financial data theft is now a robust, elaborate and sophisticated threat, multi-purposed for various types of malicious activity. Recent findings from a currently active and ongoing TrickBot campaign, which features extensive use of signed malware binaries, indicate that it

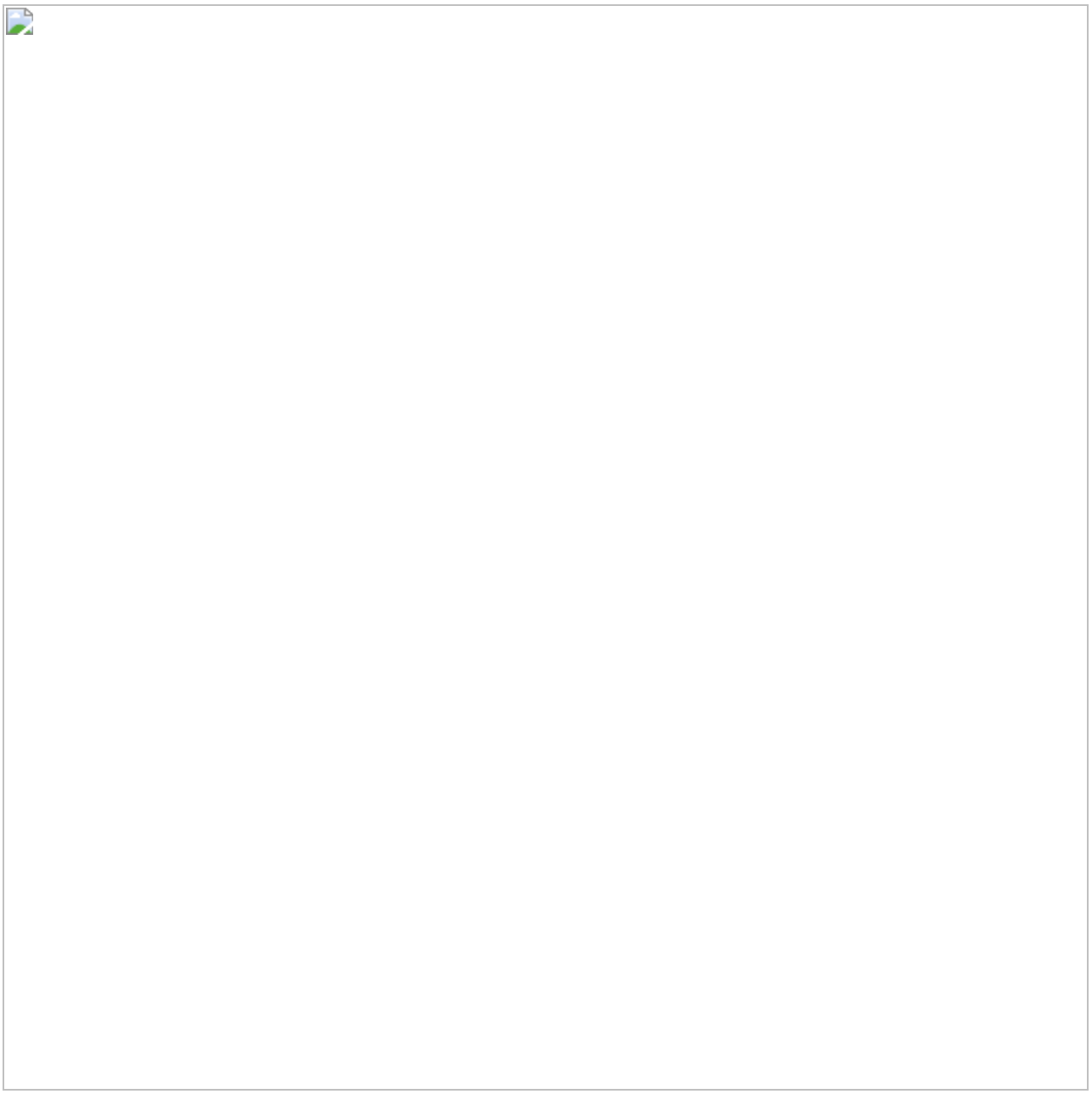
now has a new variant. Alongside its recent addition of a cookie stealing module it has gained a new partner in crime – a malicious email-based infection and distribution module that shares its code signing certificates (details in IOC section below).

The module is employed to harvest Email credentials and contacts from a victim's address book, inbox, outbox, it can send out malicious spam Emails from the victim's compromised account, and finally delete the sent messages from both outbox and the trash folder, so as to remain hidden from the user. We believe this module is used by Trickbot for several purposes; prorogation and infection, spreading spam for monetization purposes, and harvesting email accounts which can then be traded and used by other campaigns.

During our investigation of this new module and the network infrastructure associated with it, we were able to access infection servers from which the malware is downloaded onto victim machines, as well as command and control servers. We managed to recover a data base containing **250 million e-mail accounts** harvested by TrickBot operators, which most likely were also employed as lists of targets for malicious delivery and infection. The data base includes millions of addresses from government departments and agencies in the US and the UK.

In this blog post we will present our main findings so far based on research conducted in the last 10 days. Our research and analysis into this module, its activity and capabilities continues, and we will update with more details as they become available.

Attack Flow



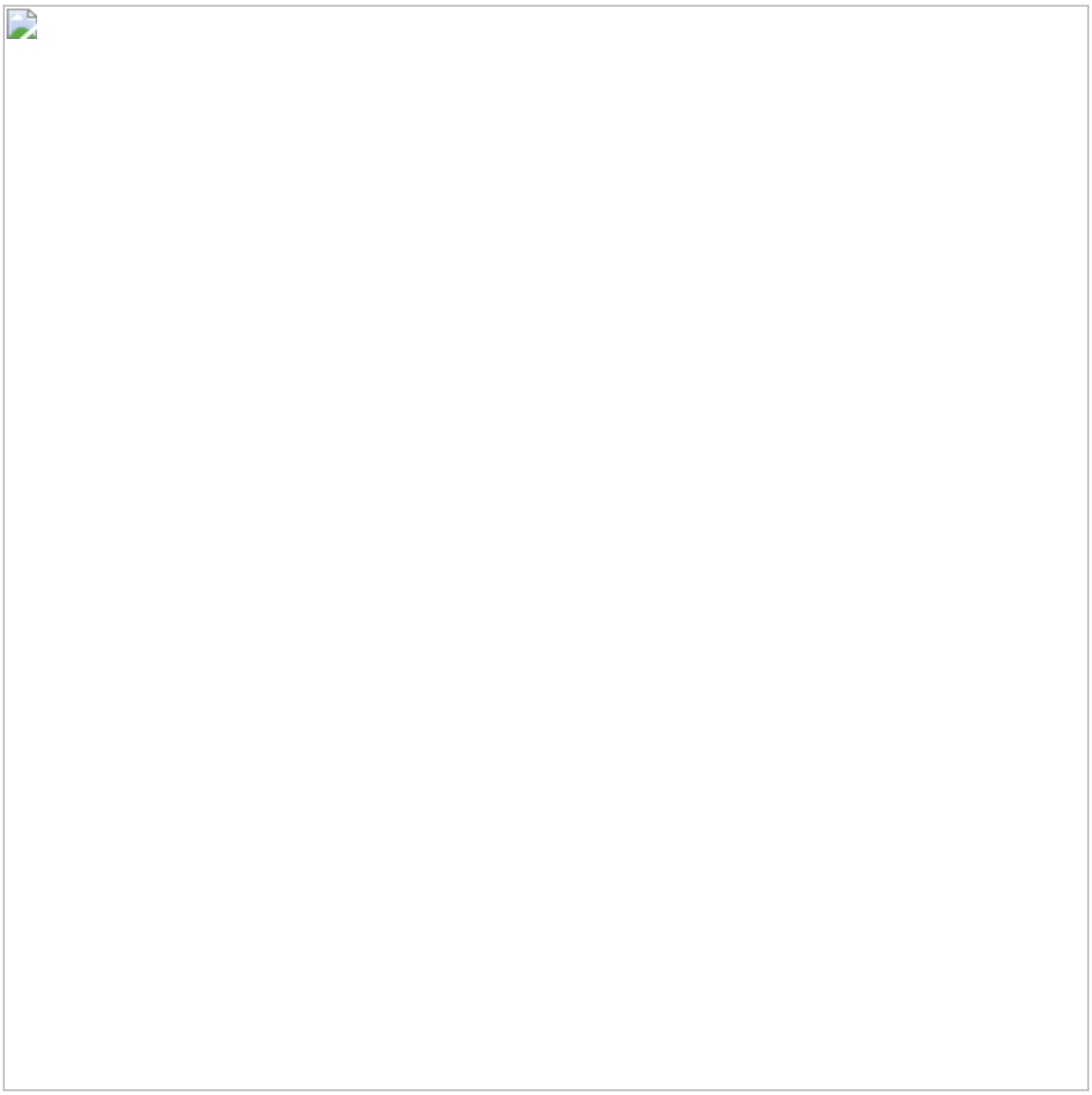
Infographic showing TrickBooster infection flow.

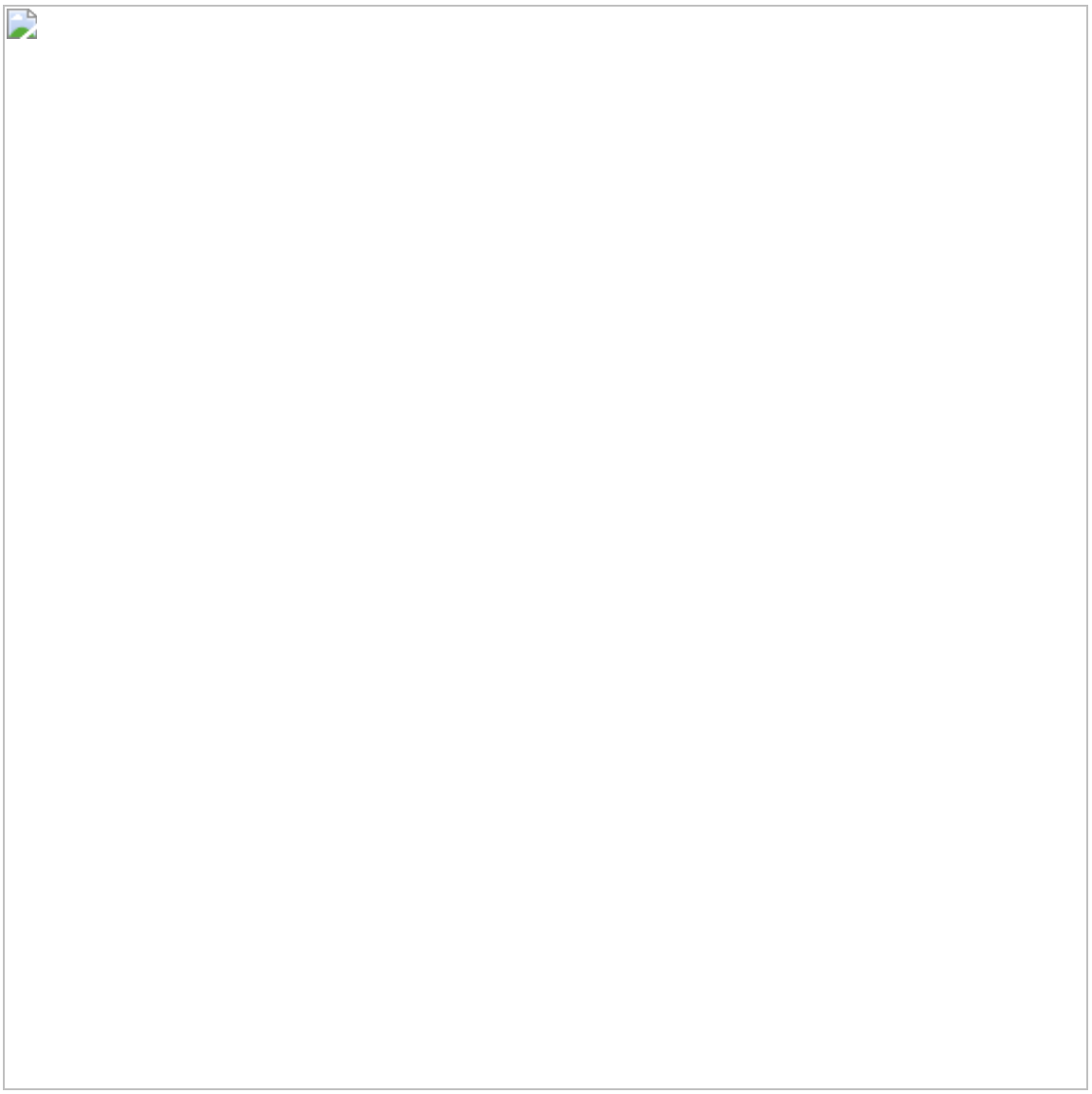
- Stage 1 – Victim machine, infected with TrickBot, receives instruction from TrickBot command and control to download TrickBooster, which is signed with a valid certificate.
- Stage 2 – TrickBooster reports back to dedicated command and control server, sending lists of harvested e-mail credentials and addresses.
- Stage 3 – TrickBooster command and control server instructs bot to send malicious spam e-mails.
- Stage 4 – TrickBooster bot sends malicious infection and spam e-mails.

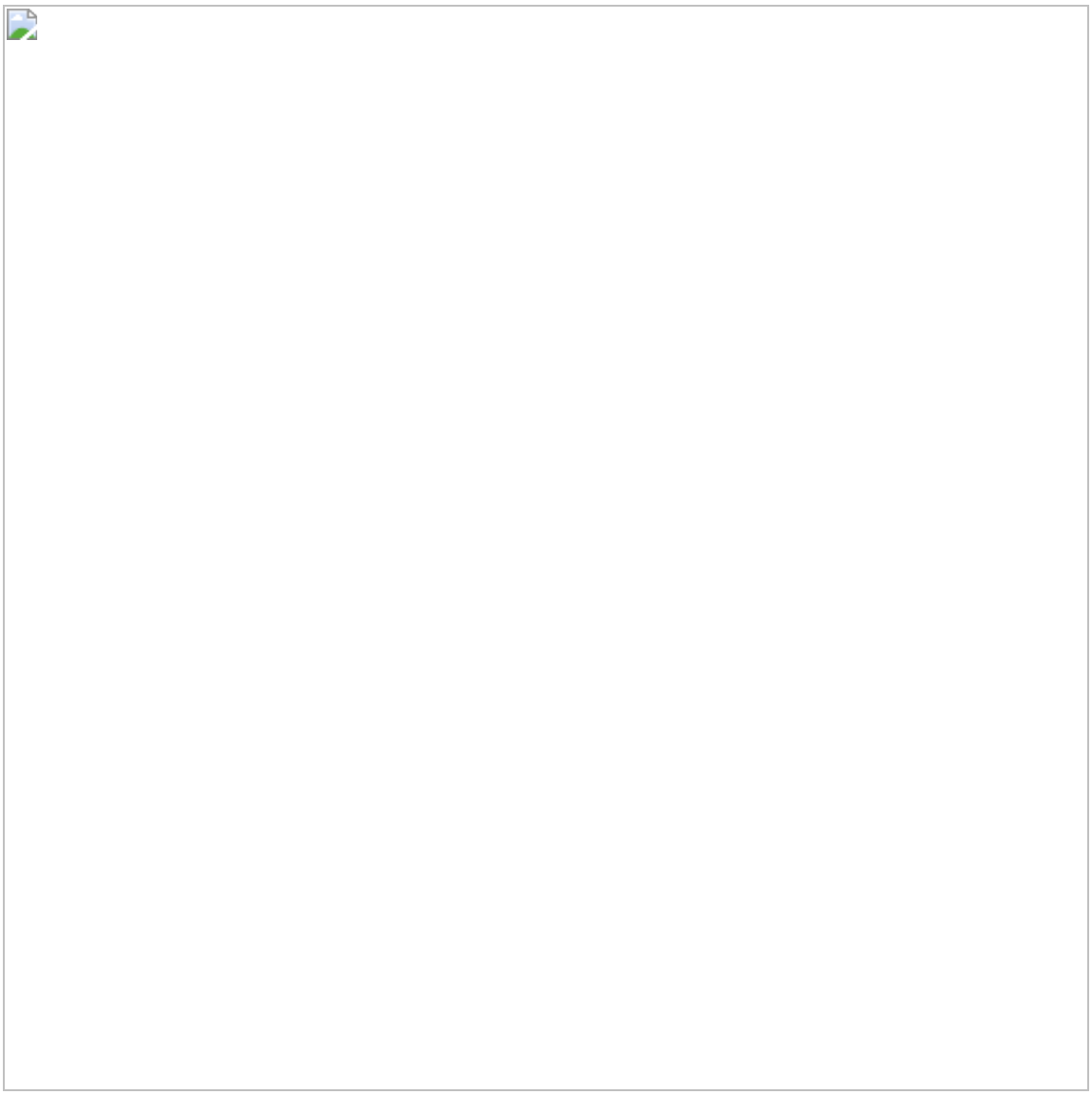
Deep Instinct's Investigation and Findings

Our investigation started when Deep Instinct detected and prevented a TrickBooster infection attempt using a signed malware binary at a customer environment in the US almost two weeks ago.

Seeing a signed malware binary delivered to a customer environment prompted us to investigate further. We analyzed the malware sample and found swaths of PowerShell code in its memory. Analysis of this PowerShell code immediately led us to the conclusion that we are dealing with a mail-bot.







PowerShell code snippets extracted from TrickBooster's memory, showing functions to harvest e-mails addresses and send malicious spam e-mails.

Following initial analysis, we started looking for more leads on the malware, cross referencing certificate information, sample similarity, and infrastructure used to both deliver and control the malware. We discovered more samples of the malware, both signed and not, additional infrastructure used in the campaign – both to distribute (infection points) and control the malware (C2 Servers). TrickBot samples were also found, signed using the same code signing certificates.

These code signing certificates were apparently issued to various small-to-medium businesses based in the UK. One of which seemingly has very little use for code signing certificates, an air-conditioning, heating and plumbing company, while others do indeed may have a legitimate use for them, according to their registrations.

We continued monitoring the campaign and the infrastructure involved in it, both its infection points and C2 Servers, which were going on and off line, and employing various Geo-IP restrictions and other mechanisms to hamper analysis. It was at one of these servers that we

found something that made us realize how successful this campaign is - an Email dump containing approximately 250 million Email addresses.

The Email Database

The recovered Email dump contains massive amounts of commonly used mail provider addresses such as Gmail, Yahoo, etc., but is not limited to these alone. It also contains large amounts **of e-mail addresses from various Government departments and other high-profile targets in both the US and the UK.**

Other organizations found include universities in the UK and Canada, and several provincial agencies and Governments in Canada.

The numbers of listing for common mail providers were as follows:

- Gmail.com – 25,863,076 addresses
- Yahoo.com – 19,079,339 addresses
- Hotmail.com – 11,120,126 addresses
- Aol.com – 7,135,831 addresses
- Msn.com – 3,512,034 addresses
- Yahoo.co.uk – 2,070,848 addresses

Spot checking a few thousands of these compromised Email addresses against previously recorded leaks and breaches, leads us to believe that this is a new mass compromise of e-mails, not previously seen or reported before.

This case, and this significant finding, highlights the success and sophistication of TrickBot, an already very accomplished piece of malware. For a threat actor in the cybercrime sphere, collaborating with a spam malware can bring many possible advantages. Chief among them is the increased ability to distribute your own malware, as spam-bots of all sorts, have been and will likely continue to be, a backbone of malware distribution in general.

As mentioned, TrickBooster is a powerful addition to TrickBot's vast arsenal of tools, modules and collaborations with other malware. This is not only due to the greatly increased spreading and information harvesting ability, but also due to the cover-up of the 'implant' left behind. Following initial deployment of the malware on the victim machine, the implant left behind by the malware, after it finishes initial execution and clean-up goes successfully undetected.

This clean-up is thorough and involves deleting the original infecting executable file, which is a very common practice employed by many malware families. The result is that it is missed by nearly all scanning security vendors, an impressive stealth factor that is much desired among malware operators.

This file, whose main functionality appears to be an e-mail collector targeting *OUTLOOK.exe,* begins its execution by creating an additional thread where this module is looking for an *OUTLOOK.exe* window by using "FindWindow" function with "rctrl_renwnd32" as class name (an identifier of the *OUTLOOK.exe* window).

On the other thread - this module is using COM objects to interact with *OUTLOOK.exe*. It starts doing so by initializing a COM object (CoInitializeEx) and continuing to interact with it by creating an instance of "Microsoft.Office.Interop.Outlook" with "CoCreateInstance". It then tries to start OUTLOOK.exe by using "OleRun" function.

When *OUTLOOK.exe* is executed - this module knows to start interacting with it by using Microsoft Outlook Messaging API (MAPI).

MAPI provides the messaging architecture for Microsoft Outlook 2013 and Outlook 2016. It provides a set of interfaces, functions, and other data types to facilitate the development of Outlook messaging applications. Applications use MAPI to manipulate email data, to create email messages and the folders to store them in, and to support notifications of changes to existing MAPI-related data.

This, and more research and analysis of TrickBooster is still ongoing with more details to be published in the near future.

During our investigation of TrickBooster, we have contacted DigiCert/Thawte, who issued the code signing certificates used to sign both TrickBot and TrickBooster samples used in this campaign and requested their revocation. The offending certificates have been revoked by DigiCert/Thawte.

We are also in the process of reporting and providing details to CERTs and other relevant authorities, and we will work with partners in the community to make available the e-mail address dumps in a secure manner.

Indicators of compromise (IOCs)

Shared Certificate Details

Shared Cert 1

- Cert SHA1: 5DE6E48A350F60CE11D9D3AC437BE8CCBC3D415C
- Issued to: https://beta.companieshouse.gov.uk/company/08306316
- TrickBot signed sample (SHA256): 3f651b525ceaa941c143b2adc3244b3d4b9af299ad09beea345867258dfbf5e7
- TrickBooster signed sample (SHA256): 620020a21c8074d689e80fc1ae29acf8c34d3481ed380f20ad445b88a7bf442e

Shared Cert 2

- Cert SHA1: 30A852583F8C2CA4710B431C800E4924C2C727EF
- Issued to: https://beta.companieshouse.gov.uk/company/08549469
- TrickBot signed samples (SHA256):

33eed709eb06f57d371fa97097f821858ad4143900c7aa4c302ce190d51370ff

dcaa278d0dbbd0b068615aeef5a87db1cbe664a6f51c5e9cc6a09fe354990fa6

TrickBooster signed sample (SHA256):

65596dd44caa7fa9e8d048dfb5a5e46b04874060eb888d320ee2ced752669f5e

Shared Cert 3

- Cert SHA1: 67ED536B62CFE6855F1821DB1FE084616F0592E4
- Issued to: https://beta.companieshouse.gov.uk/company/08480288
- TrickBot signed sample (SHA256):

e7e64753cf91d1d35c3098fcd491f53dda01e83c47f6bede3d5bfe6775fb20c8

TrickBooster signed sample (SHA256):

d96fd330c765b88f3503899755624cbe020ab3e2c53e28d7dee38e7b35f3eab2

TrickBooster Infection servers (servers known to host TrickBooster executables in this campaign)

hxxp://104.216.111.171/

hxxp://85.204.116.92/

TrickBooster Command & Control servers (servers controlling TrickBooster bots involved in this campaign)

185.86.148.63:2050

178.156.202.242:2050

62.109.25.254 (likely Command & Control Server)

TrickBooster file hashes (SHA256, involved in this campaign)

620020a21c8074d689e80fc1ae29acf8c34d3481ed380f20ad445b88a7bf442e

65596dd44caa7fa9e8d048dfb5a5e46b04874060eb888d320ee2ced752669f5e

d96fd330c765b88f3503899755624cbe020ab3e2c53e28d7dee38e7b35f3eab2

f7eeaee88c68056ab4087b4a5c7c5797f9075d0384b271f136776ff5249cb497

48d591518b306a91853ac65697dd888a0afa442014b878d777879064091f73e1

fe527937e1e512b72111102d9e18c10120b77cd9832230950ce55a718e75a9f0

FUD TrickBooster “Implant” file hashes (SHA256)

4ba33bf8a5e8b065f5055dd2c655dc2a271e9587b037e9b3e548b6c51cab3e9e

702e96fef5b2ad643a0f702b26a3fd237592f778e4fbc707c80e93326fd08d58

6bf8f079021c8018f6ab37a29091e838918734bf9d1c532852561b6a0d71f12d

Additional File hash IOCs (SHA256)

2787838d3eb2fd14e80eff102b3967c3e5f1ed9f26f0ecc856ee68dfa28b9fd5

688b4a4ef3ac5de4f2c87bb5061f3f0729efe5818d2463437f4e742d9efbcf05

ef61dc27b55fb493c94ffd7022669c95e999fb6e60eb83a78fd462eab5f4b5d6

98a60cb7e0a0337a132def0ad766b8c5dda0d6777bf531d2a5f2493bb3de4348

00ba7cd7bb268fa6f6ef09fa679e5f5d68a27be512da24c556ea04673e852978

b02494ffc1dab60510e6caee3c54695e24408e5bfa6621adcd19301cfc18e329

fc0770975ca3337984c3d4912ef592c805333e8bdf76fd4d3256ebc4e5916be7

f446f39223567f99ae2fb60f372583bc37d54ffe055f20eda8382c14eeea01f5

688b4a4ef3ac5de4f2c87bb5061f3f0729efe5818d2463437f4e742d9efbcf05

4abeab45c0503957e16373fe8f872d6055402614d317b1aa969becf07a6fdb05

748891c0ea84b6f8e2b44ec78acd474338c16e8bc24a975b867ac56ad994d939

ddd9d1a3c2cf31e2d361922c91efc9be6a253ad5854bb2adfdb02bc21a43817b