Trickbot — a concise treatise

By Vishal Thakur

Published: 2021-07-13 · Archived: 2026-04-05 23:04:43 UTC

12 min read

Apr 4, 2019

Post-execution scope of impact and threatscape details of a sophisticated malware

First Edition, April 2019

Vishal Thakur

```
If you want to support me, follow me on Patreon: https://www.patreon.com/malienist
```

Introduction

Since its initial release, Trickbot has been an advanced, modular malware, built on complex, well-written code and backed by continuous improvement and on-going development. The modular structure of the code is the most important part of this malware. Other than giving it a clearly defined and segmented flow, it allows the authors to have the ability to add new modules with new purposes to the existing malware, which they have been doing regularly throughout the history of the malware. Trickbot is a beautiful piece of code, used for malicious purposes.

Technical analysis of this malware has been published throughout its existence in the wild and there are some good, detailed publishings that are available on the internet that go into great technical details regarding the inner workings of the code and flow of Trickbot. Here's one of my earlier publications that goes into the flow of execution for Trickbot. This should give the audience a pretty good basic idea of how it operates. Another really good resource on Trickbot is the research published by hasherezade at MalwareBytes and GitHub.

```
NOTE: In this edition, we look at some never-before published information about this malware. These
```

In this publication, the focus is on the post-exploitation scenario and also the overall reach and distribution of the payload itself. There are a few things that stand out particularly around the targeting of the external entities and the ways it is achieved through some ingenious techniques applied by the authors, mainly in the target list in the config. We'll also try to break down the targeting strategy by regions, industry etc. This will allow us to understand the bigger impact that this malware can inflict on the victims and the companies/services/businesses

that are the final true target for the distributors. We also look at gathering threat intelligence based on the IOCs, features, geo-locations and techniques that are discovered through deep analysis of the final payload.

```
NOTE: None of the websites, companies or services mentioned in this publication have vulnerabilities
```

Trickbot Targets, a history of

The target configs have evolved over time. As Trickbot started gaining ground in the banking malware field back in 2016, new targets were added to the config regularly. At first, it was mainly focused around banks in different regions and the MalActors kept expanding that list, adding new banks to the config every month. At one point in time, it covered banks in a surprisingly diverse geo-location set. There were banks from America, Europe, Australia and Asia (mainly Indian banks like ICICI, HDFC etc) that were included in the configs and being actively targeted by this malware. At some point later, the MalActors probably came to realise that they would be better off focussing their efforts in the western world, mainly to maximise their profits.

We saw a great focus from the very start on Australian and NZ banking institutions when it came to the target configs. At one time, most of the top-tier and second-tier banks in Australia were being targeted by this malware. Also, its been reported in the past that Australian region was one of the first regions to see deployment of this malware, when it was first released. A very interesting thing to note is that only one Australian bank still remains in the target list — CBA (it is also one of the first banks to be targeted originally, when Trickbot first made appearance in the wild).

All major banks of the world have been targets since the beginning and most of them are still there.

Change of direction — Interesting new targets

A s we dive deeper into the inner workings and techniques of this malware, we discover many interesting things about the way it has been designed to function as framework for stealing sensitive information and converting that data into a revenue generating process.

Apart from the straight-forward banking targets, where the MalActors are able to steal money from the victims' accounts, it is interesting to see that they have started targeting entities that are not banks but hold very important information. Information that can be used to gain **access to other entities**, can be sold for a substantial dollar value or simply used for **profiling** victims or **extortion**.

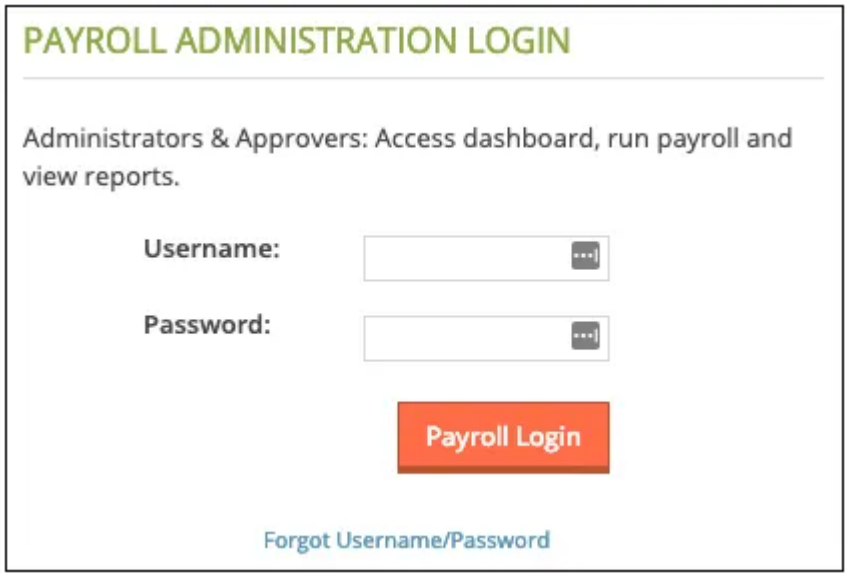
These are the non-banking targets that we found to be interesting:

Payroll

These sites are targeted to gain access to victims' payroll information. Information such as salary slips (which give out more than just salary info) and tax-related documents can be obtained from these sites. This info is highly sensitive and very personal. The MalActors can use this info in many ways. Having knowledge of someone's personal finance can be leveraged in many obvious and not-so-obvious ways. For example, this info can be then used to craft up special ransomware to target these individuals and then the ransom amount can be set in

accordance with their ability to pay. We can see that there are three such service providers that are targeted currently:

```
ADP – adp.com
https://*runpayroll.adp.com/*PAYCHEX – paychex.com/
https://myapps.paychex.com/*_remote/*SurePayroll - surepayroll.com
https://secure.surepayroll.com/SPF/Login/Auth.aspx
```



One of the payroll services targeted

Records

This one was a big surprise. These are companies that provide access to records that cover a huge landscape which includes, but is not restricted to, legal information, debt-collection, law enforcement related information, healthcare, insurance, government, corporates and more. What exactly are they planning to do with this information is anyone's guess and not a hard one at that. It looks like they are trying to get into these systems without having to pay for it and then not having to worry about any of it being traced back to them if or when they end up using this information illegally. Although there's no direct financial gain by targeting these services, the information extracted by using these services can be very valuable. Again, obvious use-cases that come to mind are selling this info on the dark web and/or extortion.

These are the two services that are targeted for records:

```
accurint.com
lexisnexis.com
```

Finance

Targets in this category are not that big a surprise and are the closest in nature to the biggest target category, banking. These site include share-trading platforms, money-exchange websites etc. The financial gain the

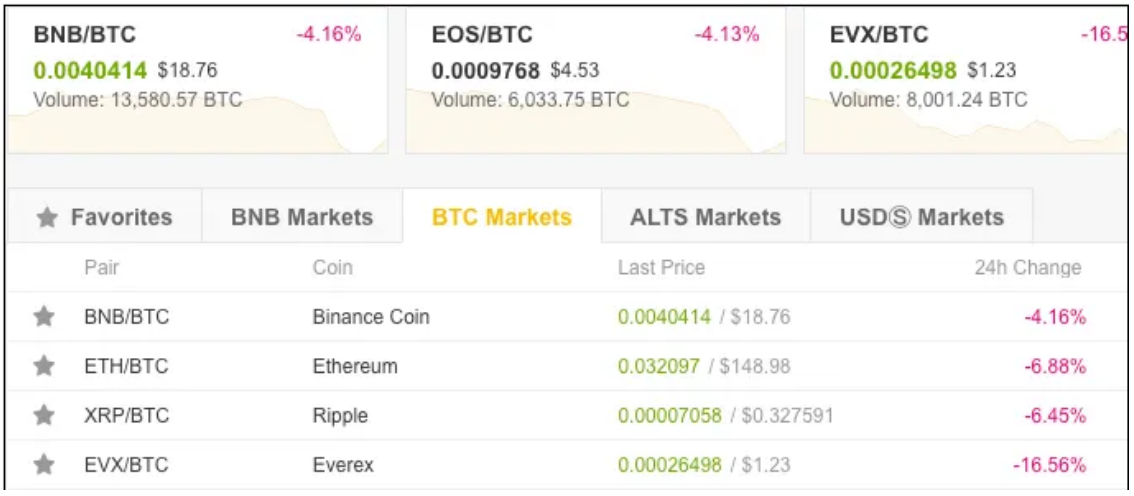
MalActors are going for seems to be quite straight-forward — money. If they are successful in getting access to the victims' accounts, they then have the ability to transfer funds out of these accounts.

```
eTrade.com
netteller.com
fundsxpress.com
discover.com
ameritrade.com
desjardins.com
schwab.com
```

Bitexchange

This one is interesting — it's a crypto currency exchange. Now, the currency itself is not doing as well as it was a while back but the potential money these exchanges hold is quite staggering. There are a lot of people (I'm looking at you) that are waiting for the next boom to happen! At this time, we can see one bitexchange in the target list and it is fully functional (no point in targeting mt. gox).

```
binance.com
```



Binance — a BitExchange target

Fleet Management

This is another interesting entry — fleetone.com. Its hard to tell what exactly the MalActors stand to gain from this site, other than the obvious information stealing, which can then be used in many different ways. The most beneficial and lucrative way to monetise this information is phishing emails sent to users, with some financial angle, based on the financial activity found on this website.

```
fleetone.com
```

Hospitality

One of the targets happens to be a hotel chain with over 6800 hotels globally. Its hard to tell if the MalActors are going after the saved PI belonging to the users or their loyalty credits. Most probably both, as the PI can be used in a number of ways to monetise the stolen information and at the same time, loyalty credits can sold/exchanged for financial gain. It is interesting to see they have picked only one hotel chain at this time, as this indicates this could be a test run and we could see more hotels added to this list, based on the results of this campaign.

```
choicehotels.com
```

eCommerce

These have been a target for a long time. At the time of this publication, there are two eCommerce targets and they are the biggest players in the game. You guessed it, Amazon and eBay.

Trickbot targets by Industry

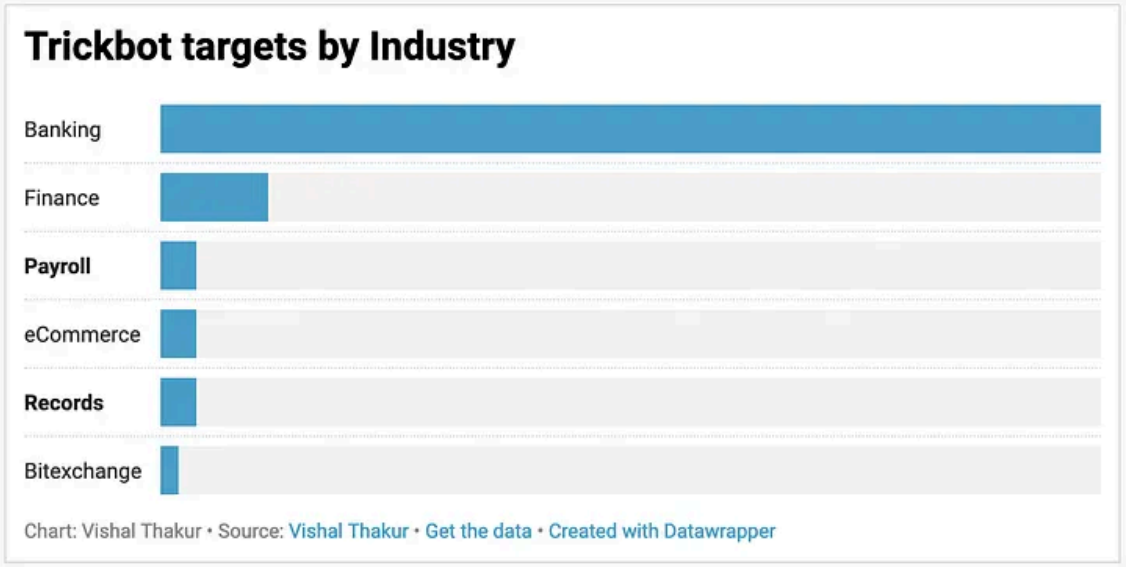
Banking still constitutes the biggest part of the target list and for obvious reasons. As noted above though, there has been a big shift back to the western banking institutions and Asian banks are completely out of the list.

Financial services industry targets have grown and have an interesting mix of trading platforms and money exchange services.

Most interesting segments are the records services and the payroll services. These can be the most devastating targets from the victims' point of view as they can be used for far more devious purposes than just financial gain.

Here's a chart that gives us an idea of the target segment sizes by industries:

Press enter or click to view image in full size



Targets by industry

Trickbot targets by Geo-location

The biggest chunk of the targets are located in the US, closely followed by Europe. There are a few Canadian targets and the lowest number is Australian. At this time, New Zealand and India have completely dropped off the list.

Germany has the highest number of targets in the list in the European region, followed by Austria and Spain.

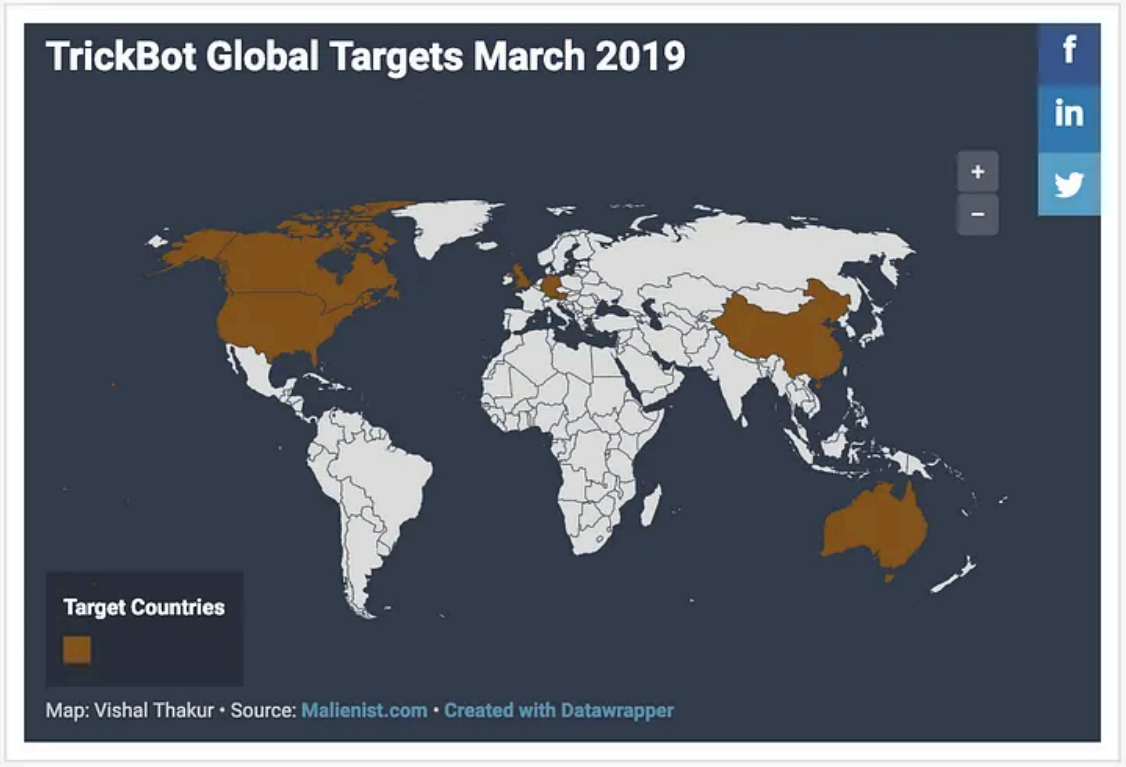
Get Vishal Thakur's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Most of the non-banking targets are US-based.

Press enter or click to view image in full size



Trickbot target banks by country

Since banking still is the largest part of the target scope for Trickbot, it is a good idea to break it down based on the country of operation. This list is ever-changing but the bulk of these institutions remain in the list for at least a while.

USA

```
nwolb.com
partnersfcu.org
vectrabank.com
```

```
bank.bbt.com
online.citi.com
securentrycorp.zionsbank.com
cibc.com
capitalonebank.com
huntington.com
bawagpsk.com
calbanktrust.com
mtb.com
usbank.com
jpmorgan.com
navyfederal.org
chase.com
web*.secureinternetbank.com (multiple targets)
bbvacompass.com
usaa.com
wellsfargo.com
securentrycorp.nbarizona.com
pnc.com
capitalone.com
suntrust.com
onepass.regions.com
tdbank.com
bankofamerica.com
key.com
express.53.com**see the extended list for wild-card targets
```

Germany

```
sparda.de
comdirect.de
netbank.de
commerzbank.de
fidor.de
deutsche-bank.de
ksk-koeln.de
haspa.de
consorsbank.de
dkb.de
postbank.de
targobank.de
santander.de
berliner-bank.de
norisbank.de
hypovereinsbank.de
lzo.com/de**see the extended list for wild-card targets
```

Austria

```
raiffeisen.at
bankaustria.at
sparkasse.at
```

Canada

```
bnc.ca
tangerine.ca
scotiabank.com
```

UK

```
lloydsbank.co.uk
rbsdigital.com
ulsterbankanytimebanking.co.uk
secure.halifax-online.co.uk
```

Australia

```
commbank.com.au
```

Wildcards

While analysing the config, one of the first things that leaps out at you is the excessive use of wildcards in the target URIs. The entire config is full of them. There are wild-carded URIs specific to target entities and then there are more that are non-specific, very general in nature, based purely on substrings. These are the interesting ones.

The use of wild-carded URIs increases the scope of the targets for this malware, significantly. For example, the entry "**/wcmfd/wcmpw/CustomerLogin**" returns at least 8 targets at the time of this writing. On the other hand, the entry "**https://*/uux.aspx**" returns a possible target list that stretches to more than a hundred websites, at the time of this writing. This is a very important piece of information that needs to be factored in when researching the broader targeting of online entities by Trickbot.

```
If we keep digging in and adding up the potential targeting including the broader, extended lists of
```

Here are some examples of Wild-carded URI targeting:

```
/Authentication/Login* –
*/Accounts/AccountOverview.asp*
.com/pub/html/login.html*
```

```
*engine/login/businesslogin*
/business/login/Login.jsp*
banking-business/portal*
*portal/*portal*
https://*.de/*/entry*
*ortal?bankid=*
```

Wild-card: /wcmfd/wcmpw/CustomerLogin*

— Extended targets:

Press enter or click to view image in full size

```
*/wcmfd/wcmpw/CustomerLogin*

https://www.frcorporateonline.com/wcmfd/wcmpw/CustomerLogin
https://bob.flagstar.com/wcmfd/wcmpw/CustomerLogin
https://fsb.enterprisebanker.com/wcmfd/wcmpw/CustomerLogin
https://cbonline.enterprisebanker.com/wcmfd/wcmpw/CustomerLogin
https://bmb.cnb.com/wcmfd/wcmpw/CustomerLogin
https://bridgebanking.bridgenb.com/wcmfd/wcmpw/CustomerLogin
https://eb.republicbank.com/wcmfd/wcmpw/CustomerLogin
https://eb.cadencebank.com/wcmfd/wcmpw/CustomerLogin
```

Wild-card: https://*ptlweb/WebPortal*

— Extended targets:

```
Extended (wildcards) list of German banks:http://webapp.de/ptlweb/WebPortal*
https://www.vbinswf.de/ptlweb/WebPortal*
https://www.gls-online-filiale.de/ptlweb/WebPortal
http://webapp.de/ptlweb/WebPortal
https://www.vriz.de/ptlweb/WebPortal
www.vbrbinvorpommern.de/ptlweb/WebPortal
https://www.vbga.de/ptlweb/WebPortal
https://www.gls-online-filiale.de/ptlweb/WebPortal
www.vrbankrheinsieg.de/ptlweb/WebPortal
https://www.apobank.de/ptlweb/WebPortal
https://www.raibalauenburg.de/ptlweb/WebPortal
https://internetbanking.gad.de/ptlweb/WebPortal
https://www.ethikbanken.de/ptlweb/WebPortal
https://www.vbloeningen.de/ptlweb/WebPortal
https://www.vr-bank-westmuensterland.de/ptlweb/WebPortal
https://www.vtb-direktbank.de/ptlweb/WebPortal
https://www.vb-niers.de/ptlweb/WebPortal
```

```
www.kd-bank.de/ptlweb/WebPortal
https://banking.steylerbank.de/ptlweb/WebPortal
https://www.eu-banking.de/ptlweb/WebPortal
https://onlinebanking.bank11.de/ptlweb/WebPortal
https://www.vbnh.de/ptlweb/WebPortal
https://www.voba-bigge-lenne.de/ptlweb/WebPortalVolksbank - subsidiaries/branches:https://www.husume
https://www.volksbank-koeln-bonn.de/ptlweb/WebPortal
www.volksbank-erft.de/ptlweb/WebPortal
https://www.volksbank-kleverland.de/ptlweb/WebPortal
https://www.dervolksbanker.de/ptlweb/WebPortal76
```

Wild-card: https://*/uux.aspx

— Extended targets:

Press enter or click to view image in full size

```
https://*/uux.aspx

https://savvyatdubuquebank.com/DubuqueBankandTrustOnline/uux.aspx
https://savvyatrmbank.com/rockymountainbankonline/Uux.aspx
https://internetbanking.tcunet.com/TeachersCreditUnionOnline/Uux.aspx
https://myibc.com/ibconline_40/uux.aspx
https://greateriowacuonline.org/greateriowacuonline_41/Uux.aspx
https://onlinebanking.avidbank.com/avidbankonline_40/Uux.aspx
https://ebanking.unifyfcu.com/ufcuonline/Uux.aspx
https://online.sesloc.org/SeslocFederalCreditUnionOnline/uux.aspx
https://secure.nbkc.com/nbkcbankonline/Uux.aspx
https://www.citadelonlinebanking.com/citadelonline/uux.aspx
https://digital.visionsfcu.org/visionsfcu/uux.aspx
```

The full list of the targets covered by this wild-card:

```
Extended list (wildcards) of US banks:savvyatdubuquebank.com/DubuqueBankandTrustOnline/uux.aspx
savvyatrmbank.com/rockymountainbankonline/Uux.aspx
internetbanking.tcunet.com/TeachersCreditUnionOnline/Uux.aspx
myibc.com/ibconline_40/uux.aspx
greateriowacuonline.org/greateriowacuonline_41/Uux.aspx
onlinebanking.avidbank.com/avidbankonline_40/Uux.aspx
ebanking.unifyfcu.com/ufcuonline/Uux.aspx
online.sesloc.org/SeslocFederalCreditUnionOnline/uux.aspx
secure.nbkc.com/nbkcbankonline/Uux.aspx
www.citadelonlinebanking.com/citadelonline/uux.aspx
digital.visionsfcu.org/visionsfcu/uux.aspx
foundersonline.foundersfcu.com/ffcuonline/uux.aspx
online.chartway.com/chartwayonline/uux.aspx
www.mytrustmark.com/TrustmarkNationalBankOnline/Uux.aspx
```

```
secure.eccu.org/eccuonline/Uux.aspx
onlinebanking.mefcudirect.com/MEFCUOnline/Uux.aspx
onlinebanking.robinsfcu.org/robinsfcuonline_40/Uux.aspx
lacapfcu.com/LCFCUOnline/Uux.aspx
securebanking.fsnb.com/thefortsillnationalbankonline/Uux.aspx
secure5.onlineaccess1.com/siucuonline/UUX.aspx
savvyatwisconsinbankandtrust.com/wisconsinbankandtrustonline/Uux.aspx
fxonline.thebankhere.com/fairfaxstatesavingsbankonline_41/Uux.aspx
online.asbhawaii.com/americansavingsbankfsbonline/Uux.aspx
savvyatillinoisbank.com/IllinoisBankandTrustOnline/Uux.aspx
citynet.cnb1901.com/tcnbloonline/uux.aspx
online.inwoodbank.com/InwoodNationalBankOnline/uux.aspx
internet-banking.nusenda.org/NusendaCUOnline_41/uux.aspx
online.umpquabank.com/UmpquaBankOnline/Uux.aspx
online.dfcufinancial.com/dfcufinancialonline/Uux.aspx
secure.mybanktx.com/CNBTTXOnline_41/UUX.aspx
ebanking.nwcu.com/northwestcommunitycuonline/uux.aspx
homebanking.cypruscu.com/cypruscreditunionononline/Uux.aspx
ffinsecure.com/ffinonline_41/uux.aspx
onlinebanking.interracu.com/InterraCreditUnionOnline_40/uux.aspx
online.uhcu.org/uhcuonline_41/uux.aspx
online.navyarmyccu.com/NavyArmyCCU/uux.aspx
online.starfinancial.com/StarFinancialOnline/Uux.aspx
digitalbanking.firstcitizens.com/FCBTCOnline/uux.aspx
secure.4frontcu.com/4frontcuonline/Uux.aspx
digital.gulfbank.com/GCBTCOnline/uux.aspx
secure.onpointcu.com/opccuonline_42/uux.aspx
onlinebanking.syb.com/SYBTCOnline/Uux.aspx
secure.southside.com/SouthsideBankOnline_40/uux.aspx
secure.suffolkfcu.org/suffolkfcu/uux.aspx
online.memcu.com/memcu/uux.aspx
online.hillsbank.com/hillsbankandtrustonline_40/Uux.aspx
my.montecito.bank/montecitobankandtrustonline/uux.aspx
online.soopercu.org/soopercreditunionononline_41/uux.aspx
secure.cbank.com/CommunityBankOnline/Uux.aspx
olb.bscu.org/bscu/uux.aspx
online.trailwest.bank/TrailWestBankOnline/Uux.aspx
ebanking.bankwest-sd.com/bankwestinconline/uux.aspx
secure.lubbocknational.com/LubbockNationalOnline/uux.aspx
online.capitalcu.com/CapitalCreditUnionOnline_42/Uux.aspx
securebanking.northwest.com/northwestbankonline_41/Uux.aspx
secure.bannerbank.com/bannerbankonline_41/uux.aspx
secure.mercbank.com/MercantileBankofMichiganOnline/uux.aspx
secure.farmbureaubank.com/FarmBureauBankOnline/UUX.aspx
online.aacreditunion.org/AAFCUOnline_40/uux.aspx#/login
savvyatnmb-t.com/newmexicobankandtrustonline/Uux.aspx
onlinebanking.thecooperativebank.com/thecooperativebankonline/Uux.aspx
```

```
fnbnorwayonlinebanking.com/FNBNorwayOnline_41/uux.aspx
online.bankofguam.com/bankofguamonline_41/Uux.aspx
onlinebanking.citizensbanknm.com/CitizensBankOnline/Uux.aspx
svbankingonline.com/ScottValleyBankOnline_40/uux.aspx
onlinebanking.1stunitedcu.org/uscuonline/Uux.aspx
eslbusinessbanking.esl.org/ESLFederalCreditUnionOnline/uux.aspx
secure.alliancebank.com/alliancebank/uux.aspx
secure.mysummit.bank/summitcommunitybankonline/uux.aspx
online.texasbnk.com/texasbankonline/Uux.aspx
secure.121fcu.org/121financialcreditunionononline_41/Uux.aspx
online.firstunitedbank.com/firstunitedbank/uux.aspx
securebanking.centrisfcu.org/centrisfcu/uux.aspx
online.todaysbank.com/todaysbankonline/uux.aspx
online.minnequaworks.com/MinnequaWorksCreditUnionOnline_42/Uux.aspx
online.uvacreditunion.org/uvaccuonline/uux.aspx
onlinebanking.anbbank.com/ANBBankOnline/uux.aspx
online.cannonfcu.org/CannonFederalCreditUnionOnline_41/Uux.aspx
online.fireflycu.org/fireflycu/uux.aspx
secure.peoplesbankonline.com/pbtconline_41/Uux.aspx
onlinebanking.caminofcu.org/caminofederalcreditunionononline_41/uux.aspx
onlinebanking.hiway.org/HiwayFederalCreditUnionOnline/Uux.aspx
curcuohiovalleycu.org/OhioValleyCommunityCUOnline/uux.aspx
onlineaccess.nrlfcu.org/nrlfederalcreditunionononline/uux.aspx
onlinebanking.redrocks.org/redrockscreditunionononline/uux.aspx
securebanking.cbbank.com/cbb/Uux.aspx
ebank.pfcu4me.com/pfcuonline/uux.aspx
www.ebanking.uiccu.org/UICCUOnline/uux.aspx
onlinebanking.dominioncu.com/dominioncreditunionononline_41/uux.aspx
ob2.mymax.com/MAXCreditUnionOnline/uux.aspx
banking.firstmarkcu.org/firstmarkcreditunionononline_40/Uux.aspx
secure.ucbi.com/unitedcommunitybankonline/Uux.aspx
curcuohiovalleycu.org/OhioValleyCommunityCUOnline/uux.aspx
online.southwestnb.com/southwestnationalbankonline/Uux.aspx
onlinebanking.wasatchpeaks.com/WasatchPeaksFCUOnline_41/Uux.aspx
online.firstpremier.com/FirstPremierBankOnline/uux.aspx
ibanking.ilwucu.org/ILWUCreditUnionOnline/uux.aspx
online.mygenfcu.org/MyGenFCU/uux.aspx
online.ttcu.com/ttcu/uux.aspx
savvyatcitywidebanks.com/citywidebanksonline/Uux.aspx
texas.savvyatfirstbanklubbock.com/firstbankandtrustcompany/Uux.aspx
onlinebanking.robinsfcu.org/RobinsFCUOnline_40/uux.aspx
onlinebanking.afcu.org/afcuonline_41/uux.aspx
olb.gucu.org/GeorgiaUnitedCreditUnionOnline/uux.aspx
online.bankofthepacific.com/BankofthePacificOnline_40/uux.aspx
stearnsconnect.stearnsbank.com/StearnsBankOnline/uux.aspx
mycb.columbiabankonline.com/columbiabankonline/uux.aspx
onlinebanking.fccu.org/fccuonline/uux.aspx
```

```
online.bmifcu.org/bmifederalcreditunionononline_41/Uux.aspx
e.sfcu.org/sfcuonline/uux.aspx
online.hfcu.org/HanscomFCUOnline/uux.aspx
onlinebanking.plumasbank.com/PlumasBankOnline/uux.aspx
online.thecommercebank.com/CommerceBankofWashingtonOnline/uux.aspx
online.dacotahbank.com/dacotahonline1/Uux.aspx
online.eaglecu.org/eaglecu/uux.aspx
online.communitychoicecu.com/communitychoicecu//uux.aspx
secure.mybanktx.com/CNBTTXOnline_41/UUX.aspx
online.valleyfirstcu.org/valleyfirstcreditunionononline_41/Uux.aspx
online.uccu.com/ucfcuonline_42/uux.aspx
cconline.coastccu.org/CoastCentralCUOnline/Uux.aspx
onlinebanking.saintsavenuebank.com/SABOnline/uux.aspx
secure.firstbankkansas.com/FirstBankKansasOnline_41/Uux.aspx
onlinebanking.pyramidfcu.com/pfcuonline_40/Uux.aspx
```

Here are some more interesting wild-carded URIs:

```
*.com/fi*/bb/*
*.com/fi*/pb/*
*.com/fi*/retail/*
*.com/fnfg/retail/*
*.com/pub/html/login.html*
*/Authentication/Login*
*/Accounts/AccountOverview.asp*
*/EBC_EBC1961/* - targets multiple banks
*/bbw/cmserver/welcome*
*/onlineserv/CM*
```

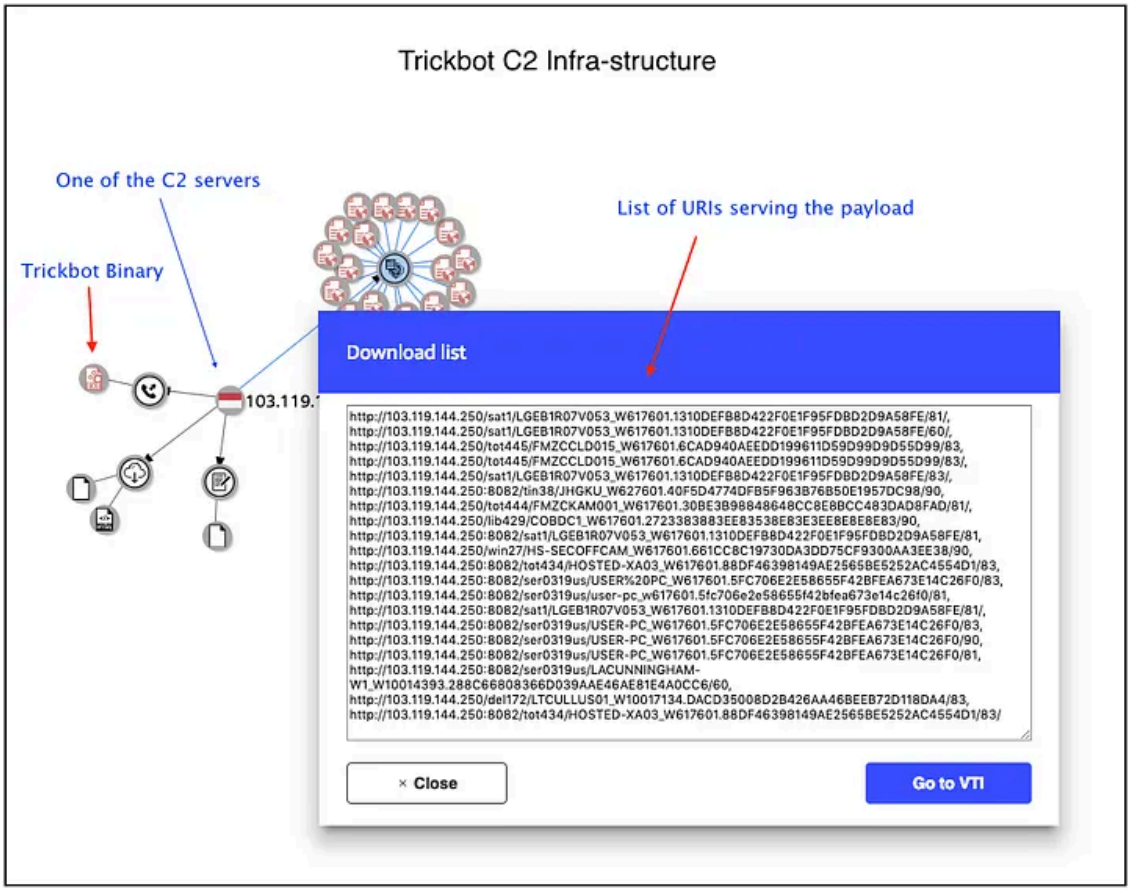
The above targets cover a wide range of banking sites.

Threat Intelligence: The C2 infra-structure

Distribution chain for Trickbot is quite straight-forward. The initial infection-vector is phishing, from there on it follows the usual flow of execution, which has been covered in one of my previous publications, available here.

A look at the C2 infra-structure from a threat-intel angle reveals interesting findings. The servers are usually setup for multiple paths of delivery, through different URIs. Some of these servers have been used to distribute more than one payload and some of them are easy to trace/connect as they have been known to serve binaries that are common to multiple C2 servers. This is interesting and important information from a threat-hunting angle, and can be used by threat-intel teams to provide meaningful and effective mitigations/protections for their organisations.

Press enter or click to view image in full size

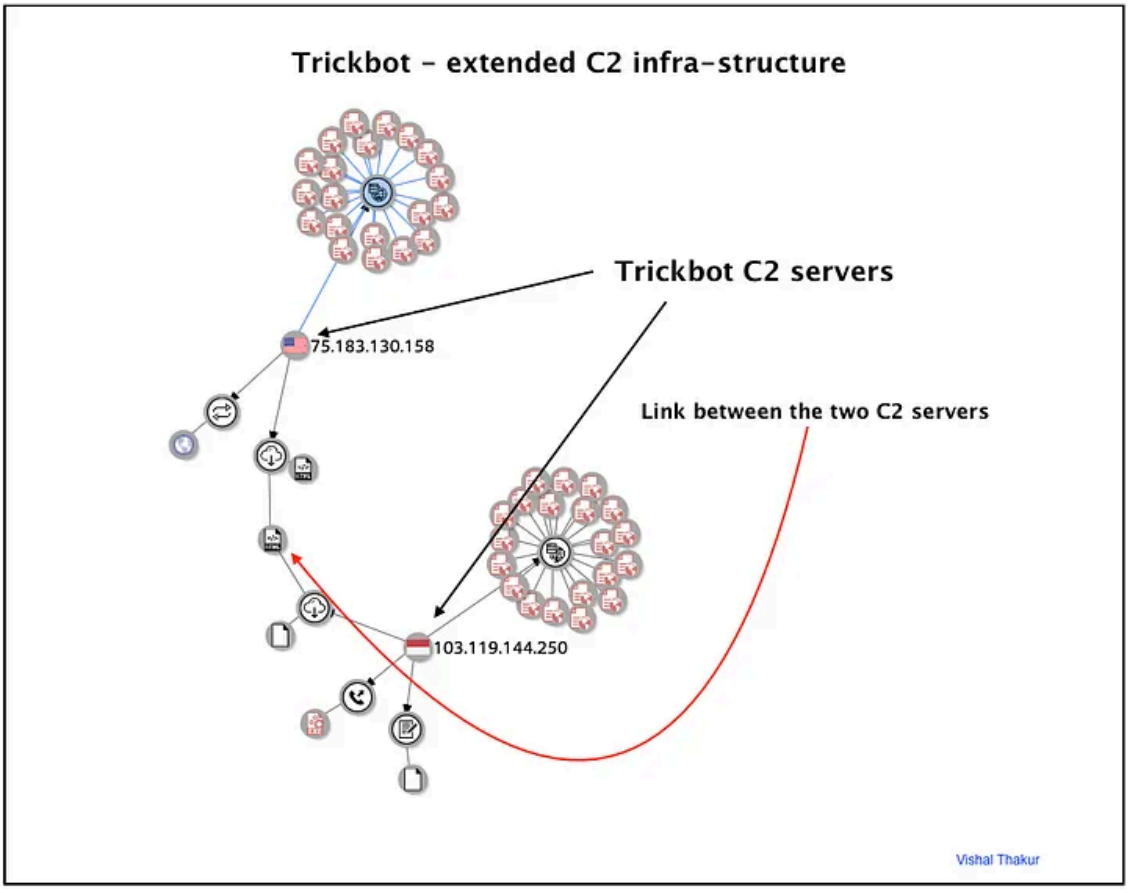


List of URIs serving the binaries from one C2 server

It is possible to connect the dots and build a useful repository of C2 servers for Trickbot and use it for tracking future campaigns (a task that is currently being executed by the author). Also, this information can be used to see what other malware families share infra-structure and how researchers can use this information to build better intelligence around these malware families (also currently an active project).

It is very interesting to see how the infra-structure is used effectively with room for collaboration between MalActors.

Press enter or click to view image in full size



Link between two Trickbot C2 servers can be seen by the shared binary

Conclusion

Trickbot has been around for quite some time now. It started as a banking malware, targeting banking institutions to start with and then pivoted into other, similar industries, with the sole purpose of maximising profits. Recently, the MalActors have broadened their target base even more, venturing into non-banking institutions and also targeting really interesting sectors such as records, legal and bit-exchanges. We also saw a fleet-management company targeted in the latest config.

The biggest and most-effective technique has been the use of wild-carded target URIs — this takes the targeting to the next level. As we saw earlier, this technique serves two purposes, first one is to increase the targeting (eg. hundreds of banks targeted in one line of config) and the second one is to hide the targets from researchers (the actual names are not included in the list at any point). This is the most efficient, well-thought and perfectly executed technique in a financial malware.

We know that Trickbot is a well-coded, sophisticated and modular malware. Based on that alone, we should expect it to keep evolving, moving into different directions (most of the current modules were added gradually after the initial release — lateral movement, outlook-targeting, POS targeting etc). The MalActors behind it will keep researching and looking for new sources of revenue, new industries to target and new ways of doing so. We haven’t seen the last of it or even the best of it yet. And we’ll keep researching this interesting malware in the future.
