The Many Tentacles of the Necurs Botnet

By Jaeson Schultz

Published: 2018-01-18 · Archived: 2026-04-05 19:22:22 UTC

Thursday, January 18, 2018 11:02

This post was written by Jaeson Schultz.

Introduction Over the past five years the Necurs botnet has established itself as the largest purveyor of spam worldwide. Necurs is responsible for emailing massive amounts of banking malware, ransomware, dating spam, pump-n-dump stock scams, work from home schemes, and even cryptocurrency wallet credential phishing. Necurs sends so much spam that at times Necurs' spam campaigns can make up more than 90% of the spam seen by Cisco Talos in one day.

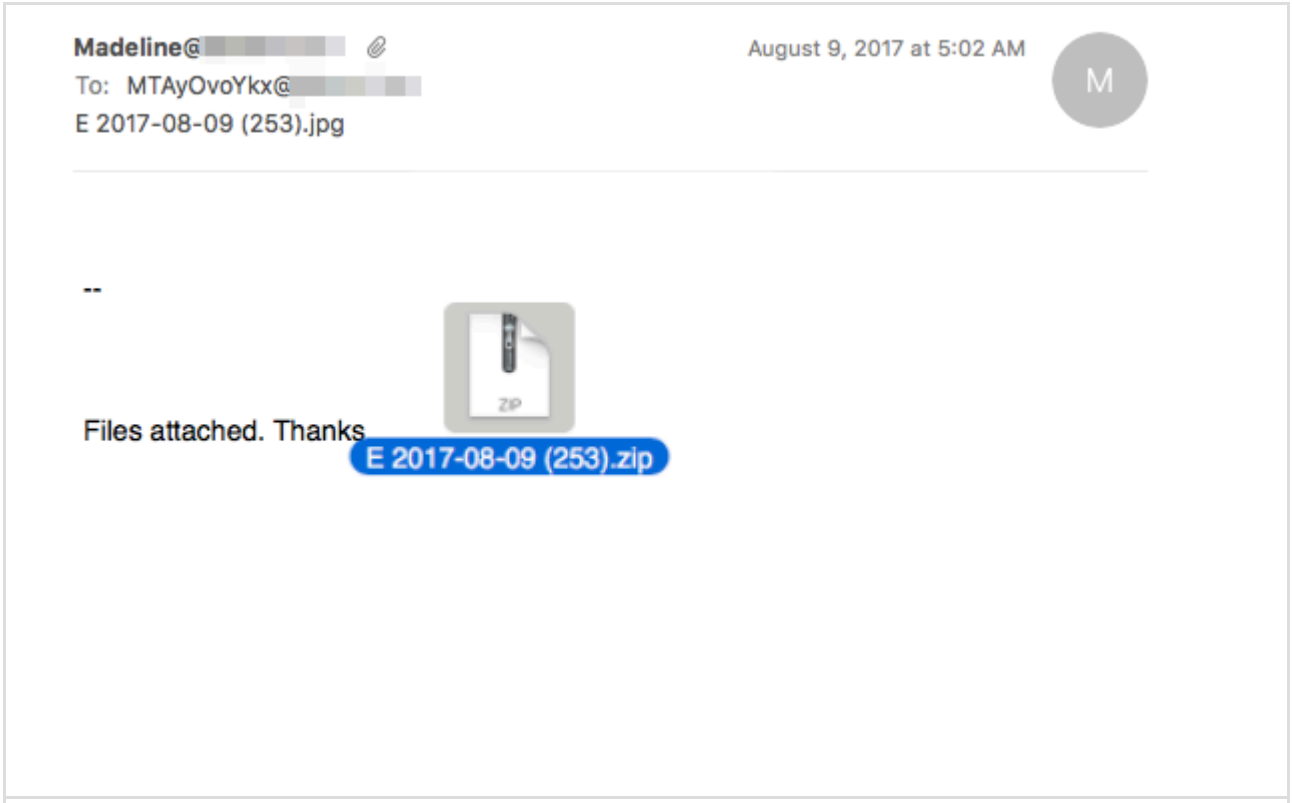
To conduct a deeper analysis of Necurs, Talos extracted 32 distinct spam campaigns sent by Necurs between August 2017 and November 2017. The result was a collection of over 2.1 million spam messages, sent from almost 1.2 million distinct sending IP addresses in over 200 countries and territories.

Necurs Recipients From an email marketing and delivery perspective, Necurs doesn't appear to be too sophisticated. Necurs' recipient database includes email addresses that have been harvested online, commonly deployed role-based accounts, as well as email addresses that appear to have been auto-generated. These are among the worst, most unreliable sources for obtaining email addresses, and any legitimate email marketer wouldn't last a day mailing to addresses such as these. Of course, an illegitimate botnet such as Necurs has no such concerns. For many months the email addresses in Necurs database seemed to be largely static; Necurs hasn't actively added

any new addresses for at least the past year, possibly two years or more. In November of 2017, Necurs stopped mailing to many of the autogenerated accounts.

At one of my personal domains, Necurs has been seen mailing to addresses such as 'equifax@' --an email address that was originally stolen from Equifax years before the 2017 breach. Necurs also often mails to 'thisisatestmessageatall@', another email address I generated and put into the wild, long ago. There are also variations on other legitimate addresses, for example 'aeson@', '20jaeson@', and 'eson@' which are all variations on my address 'jaeson@'. The number 20 was present at the beginning of many of Necurs recipients. Hex 20 corresponds with the space character and is used in percent-encoding, etc. This provides further indication of the harvested nature of these addresses.

Other addresses in Necurs' mailing list appear to have been auto-generated. For example 'EFgUYsxebG@', 'ZhyWaTmu@', and 'MTAyOvoYkx@' have never been aliases at my domain that I've ever used, and the only mail these accounts ever receive comes from Necurs.



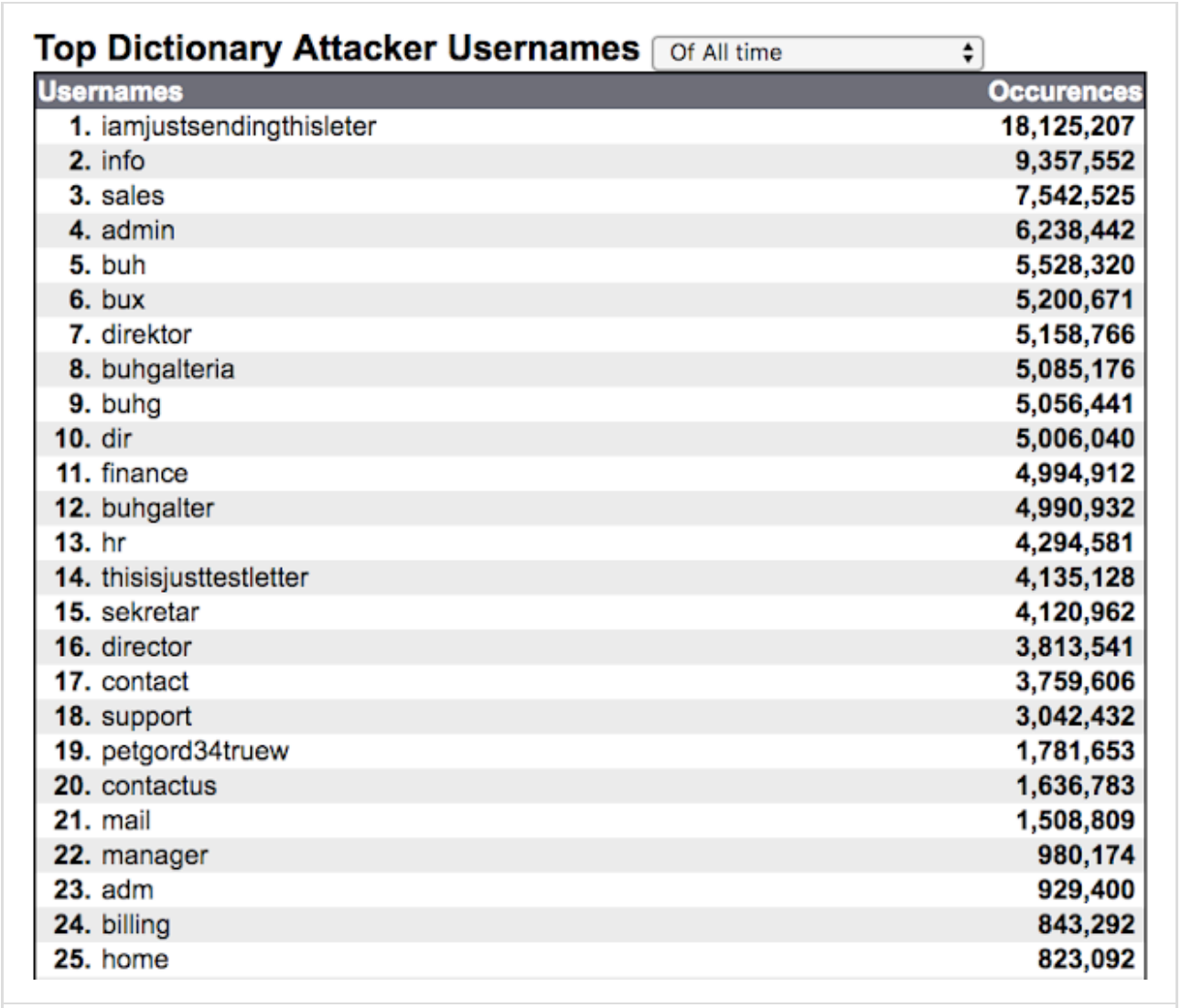
Necurs email received at an auto-generated email address

From our set of Necurs' spam messages, Talos extracted only the user alias portion of the To: address. There are numerous email aliases, such as role-based addresses, that appear to be in Necurs' recipient DB across many different recipient domains. Strangely, the list also included some odd email aliases deployed at multiple domains such as 'unity_unity[0-9]@', 'petgord32truew@', 'iamjustsendingthisleter@', 'docs[0-9]@', and others.

Recipient	# of Domains
webmaster	94
admin	76
info	56
sales	47
no-reply	23
petgord34truew	18
unity_unity[0-9]	14
scans	13
docs[0-9]	7
iamjustsendingthisleter	6

Email alias and the number of domains in our data in which that alias was found

Interestingly, some of these same strange aliases can be found on Project Honeypot's list of the Top Dictionary Attacker Usernames, though it is unclear whether Necurs obtained their aliases from this list, or whether these aliases made Project Honeypot's list as a result of Necurs' spamming activity.

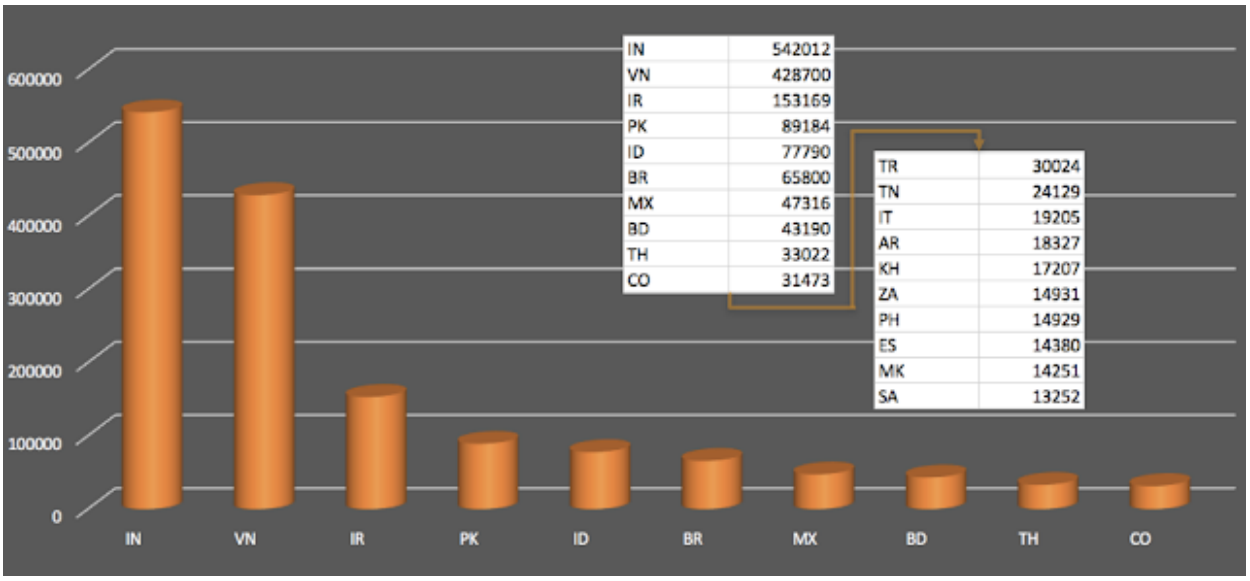


Top Dictionary Attacker Usernames Of All time

Usernames	Occurences
1. iamjustsendingthisleter	18,125,207
2. info	9,357,552
3. sales	7,542,525
4. admin	6,238,442
5. buh	5,528,320
6. bux	5,200,671
7. direktor	5,158,766
8. buhgalteria	5,085,176
9. buhg	5,056,441
10. dir	5,006,040
11. finance	4,994,912
12. buhgalter	4,990,932
13. hr	4,294,581
14. thisisjusttestletter	4,135,128
15. sekretar	4,120,962
16. director	3,813,541
17. contact	3,759,606
18. support	3,042,432
19. petgord34truew	1,781,653
20. contactus	1,636,783
21. mail	1,508,809
22. manager	980,174
23. adm	929,400
24. billing	843,292
25. home	823,092

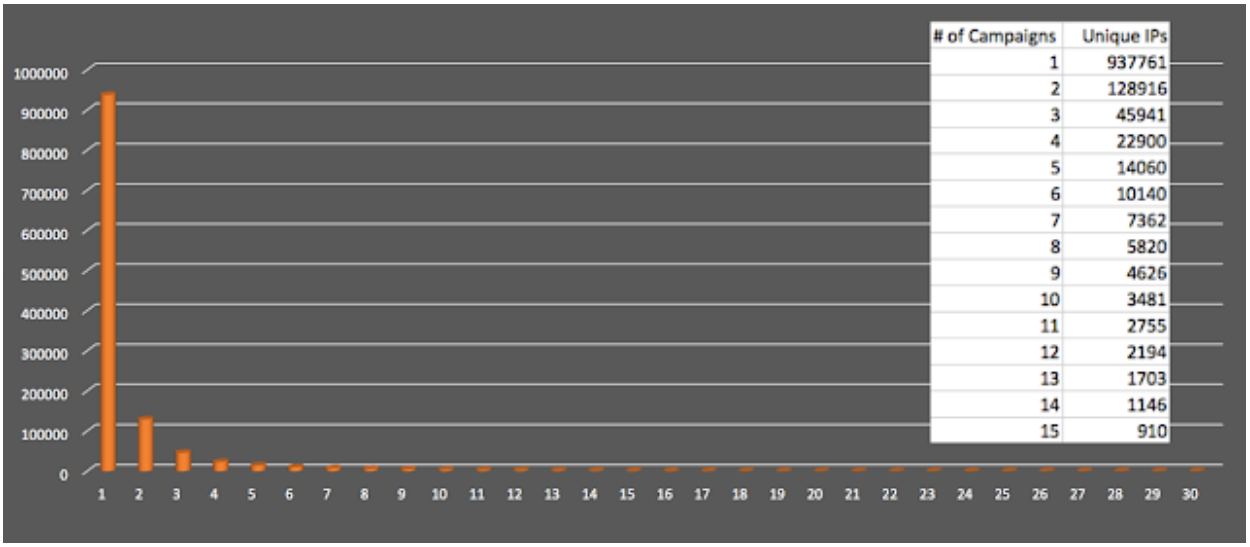
Project Honeypot's Top Dictionary Attacker Usernames

Necurs Sending IPs Next, Talos extracted the sending IP addresses responsible for transmitting Necurs' spam emails, and we grouped the data according to geographical location. Rather than being uniformly distributed worldwide, a majority of Necurs' nodes were concentrated among just a few countries --India (25.7% of total spam), Vietnam (20.3% of total spam), and Iran (7.3% of total spam). More than half (51.3%) of the sending IP addresses in our data came from just these three countries. In contrast, other large industrialized nations were only responsible for tiny fraction of the spam. For example, the United States, was home to 6,314 (less than 1%) of Necurs sending IPs. The country of Russia was only attributed to 38 sending IP addresses out of a nearly 1.2 million total sender IPs!



Number of spam messages sent per country

Talos also analyzed the individual spam campaigns in order to determine how often the sending IP addresses were reused from campaign to campaign. We found very little infrastructure reuse. In fact, **none** of the sending IP addresses in our data were seen across all thirty-two of the campaigns we extracted. Only three sending IP addresses could be found across thirty of Necurs' spam campaigns. The vast, vast majority of sending IP addresses, 937,761 (78.6% of the total), were only ever seen in a single Necurs spam campaign! This means that Necurs botnet is large enough to conduct attacks over several months without substantial reuse of most sending nodes --an impressive feat.

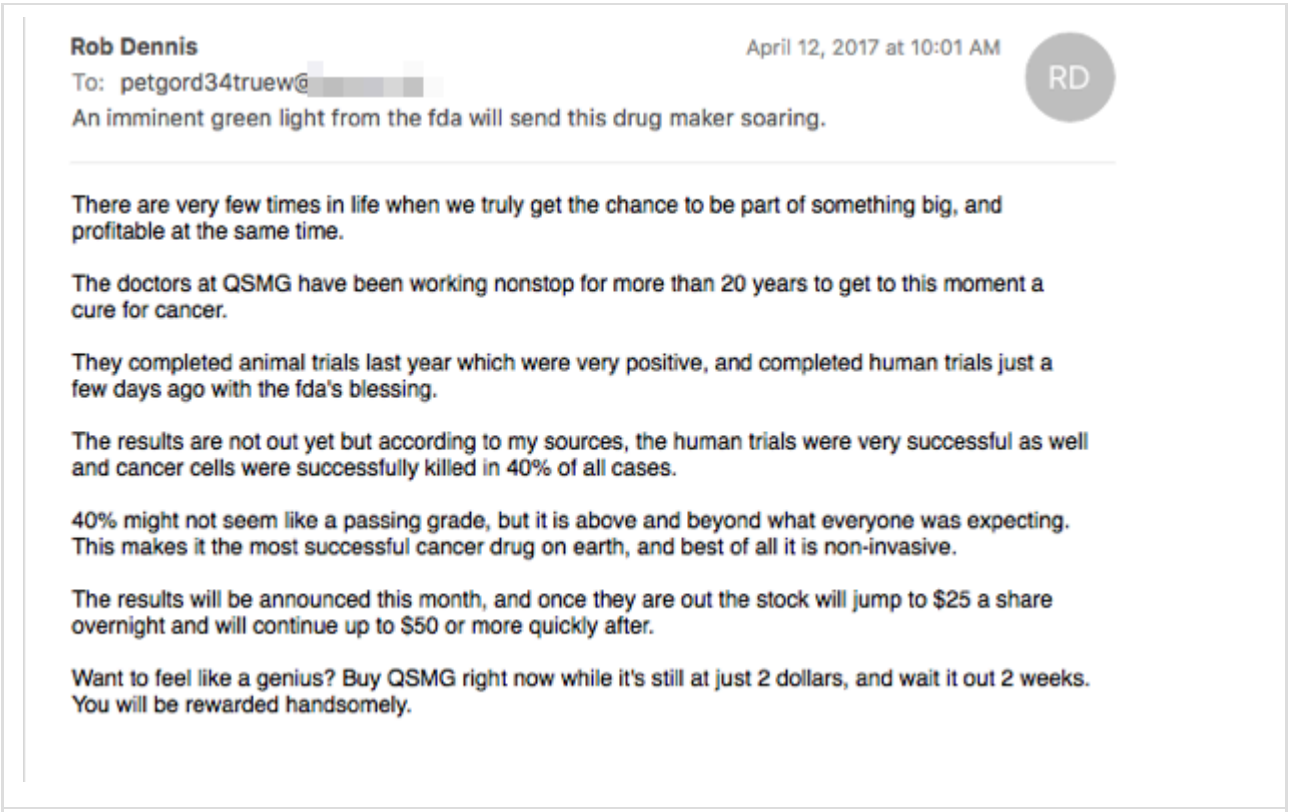


Number of unique IP addresses vs. how many campaigns in which they appeared

Necurs Spam Campaigns Typically email campaigns from Necurs fall into one of two categories:

high-volume weekday campaigns, or low volume continuous campaigns. Necurs has occasionally been seen sending high volume campaigns on weekends, but the vast majority of the time high volume campaigns are limited to the business week only. The mailing list database Necurs is using seems to be segmented, such that the high volume campaigns use one subset of email addresses from the DB, and the low volume campaigns use a different set of email addresses.

Pump-N-Dump Stock Spam Below is an example of a pump-n-dump stock spam sent on April 12th, 2017 by Necurs touting the stock symbol QSMG, Quest Management Incorporated. On the following day the price of QSMG peaked at $2.33, probably netting the criminals a tidy gain on their initial investment. QSMG is currently worth less than $0.02.



Rob Dennis April 12, 2017 at 10:01 AM

To: petgord34truew@

RD

An imminent green light from the fda will send this drug maker soaring.

There are very few times in life when we truly get the chance to be part of something big, and profitable at the same time.

The doctors at QSMG have been working nonstop for more than 20 years to get to this moment a cure for cancer.

They completed animal trials last year which were very positive, and completed human trials just a few days ago with the fda's blessing.

The results are not out yet but according to my sources, the human trials were very successful as well and cancer cells were successfully killed in 40% of all cases.

40% might not seem like a passing grade, but it is above and beyond what everyone was expecting. This makes it the most successful cancer drug on earth, and best of all it is non-invasive.

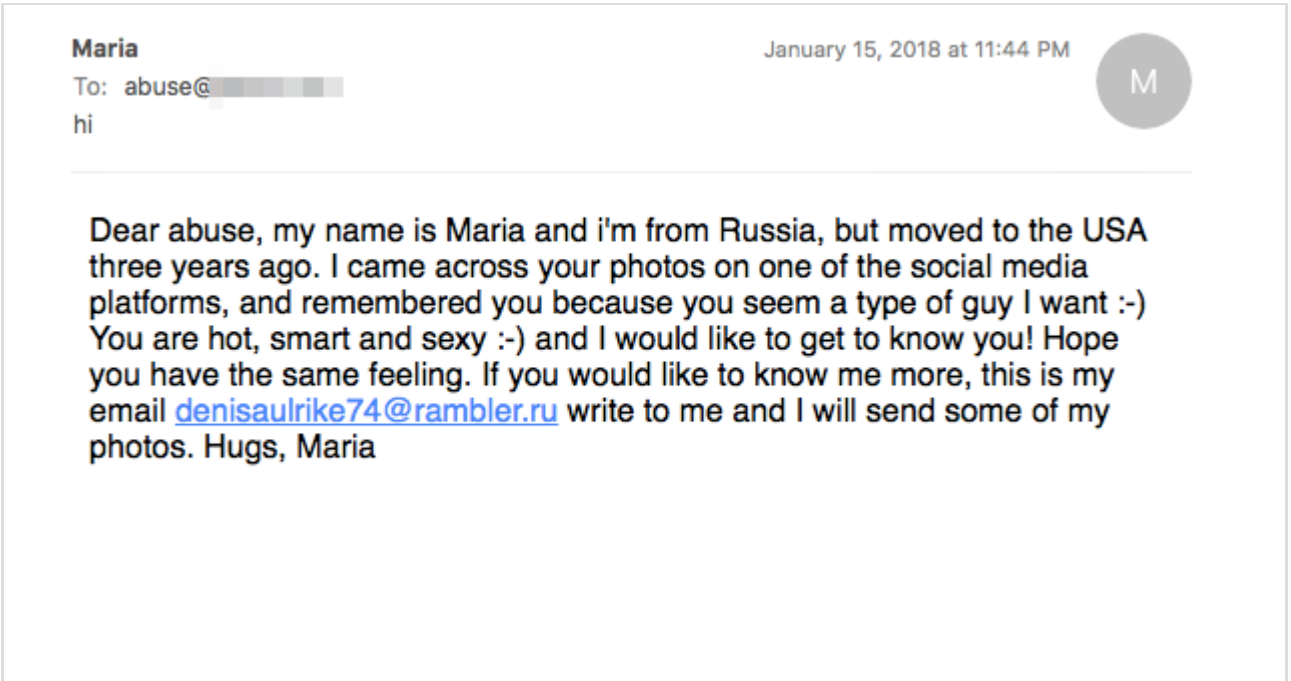
The results will be announced this month, and once they are out the stock will jump to $25 a share overnight and will continue up to $50 or more quickly after.

Want to feel like a genius? Buy QSMG right now while it's still at just 2 dollars, and wait it out 2 weeks. You will be rewarded handsomely.

A message touting the penny stock, QSMG

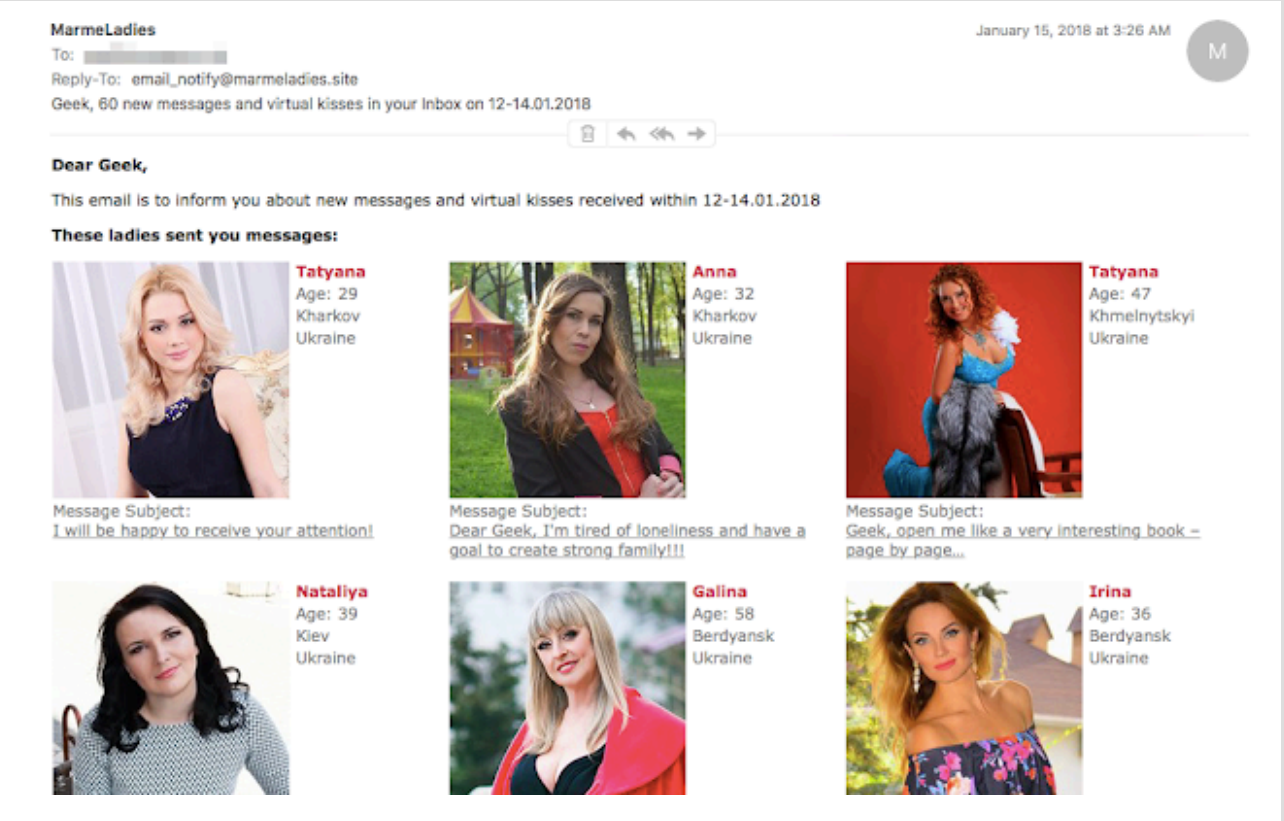
QSMG was at $2.33 on April 13. Currently it is worth less than $0.02

Dating Spam Necurs also sends dating spam. Recent dating spam have arrived without any URLs in the body, except a mailto: link to an email address. Current dating campaigns have involved the free email provider rambler.ru, but other previous dating campaigns have taken advantage of similar free email services such as gmx.com. Necurs' dating campaigns have also been known to include HTML links to fast-fluxed domains, or sometimes compromised websites (Wordpress, etc.).



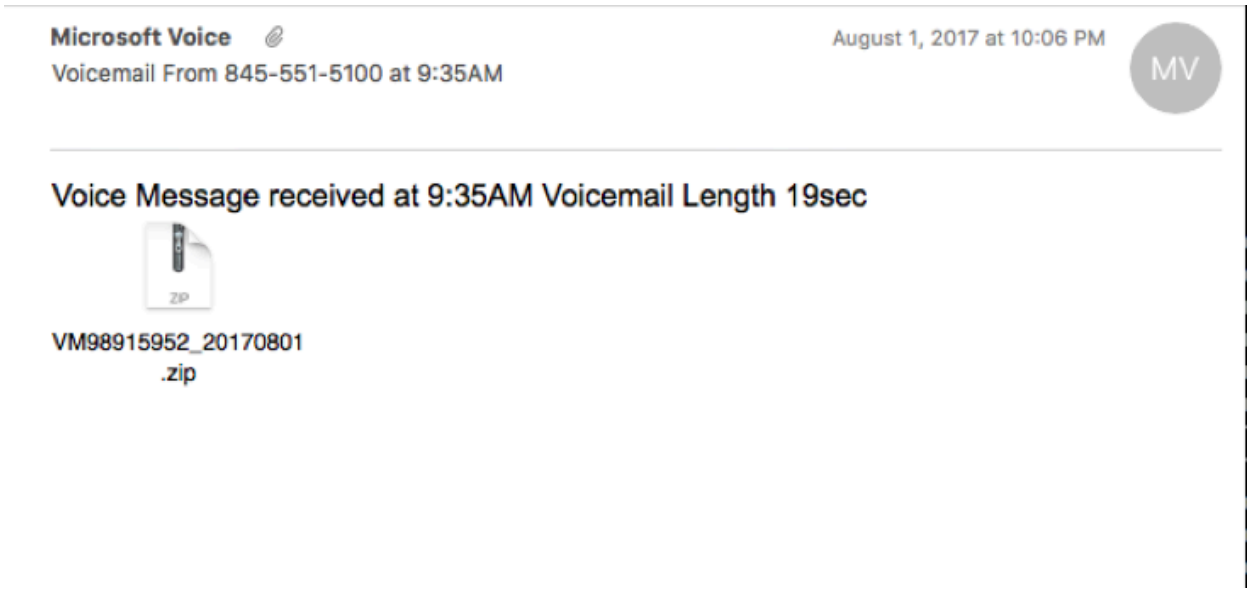
Necurs dating spam featuring an email address at rambler.ru

If you respond to one of these dating messages, you may be enrolled in a Russian dating website such as marmeladies.site. In this case, the criminals are making money by referring new users to these dating sites. Most likely they are being paid on an affiliate model.



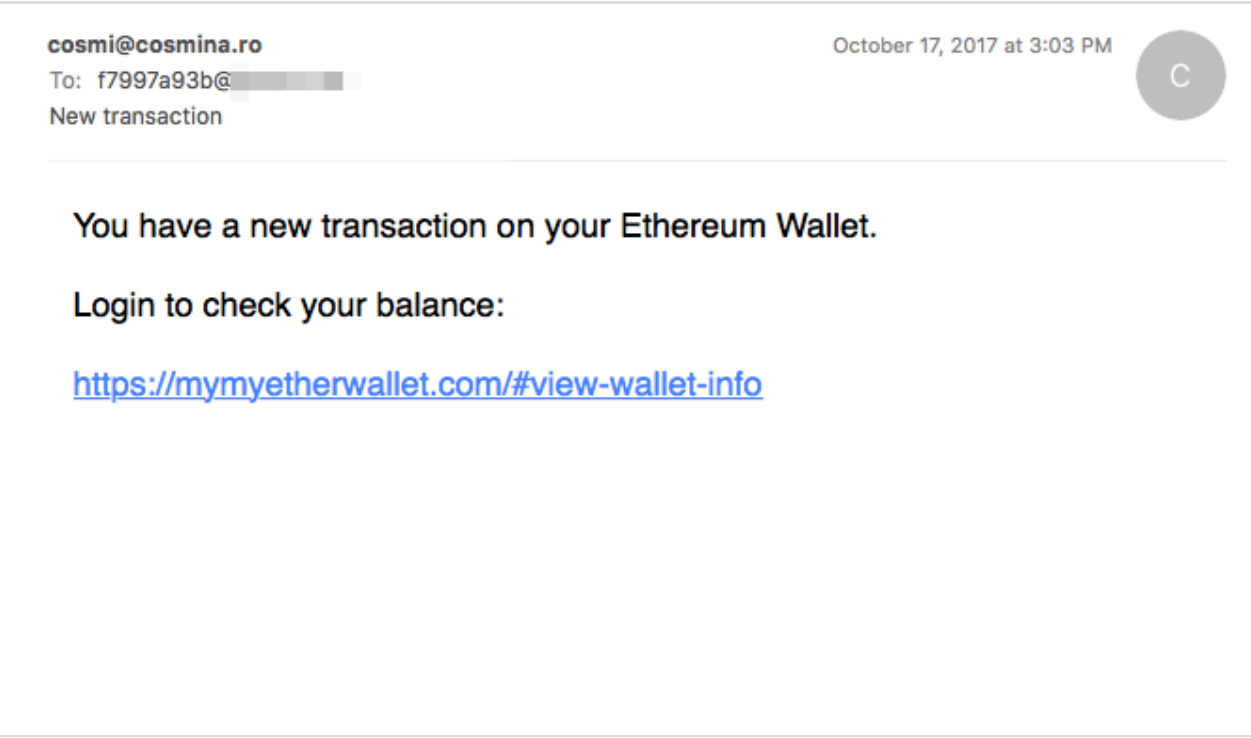
Marmeladies is one of the dating sites to which victims who reply are directed

Ransomware Of course one of Necurs' most well-known payloads is ransomware. Necurs has been one of the biggest distributors of the Locky ransomware. Locky also works on an affiliate model. Inside of each locky sample, in the metadata, is an affiliate ID, which is always the same (3) for Necurs mailings. Most of the time, very little investment is made in the design of the messages themselves, as in the following example.



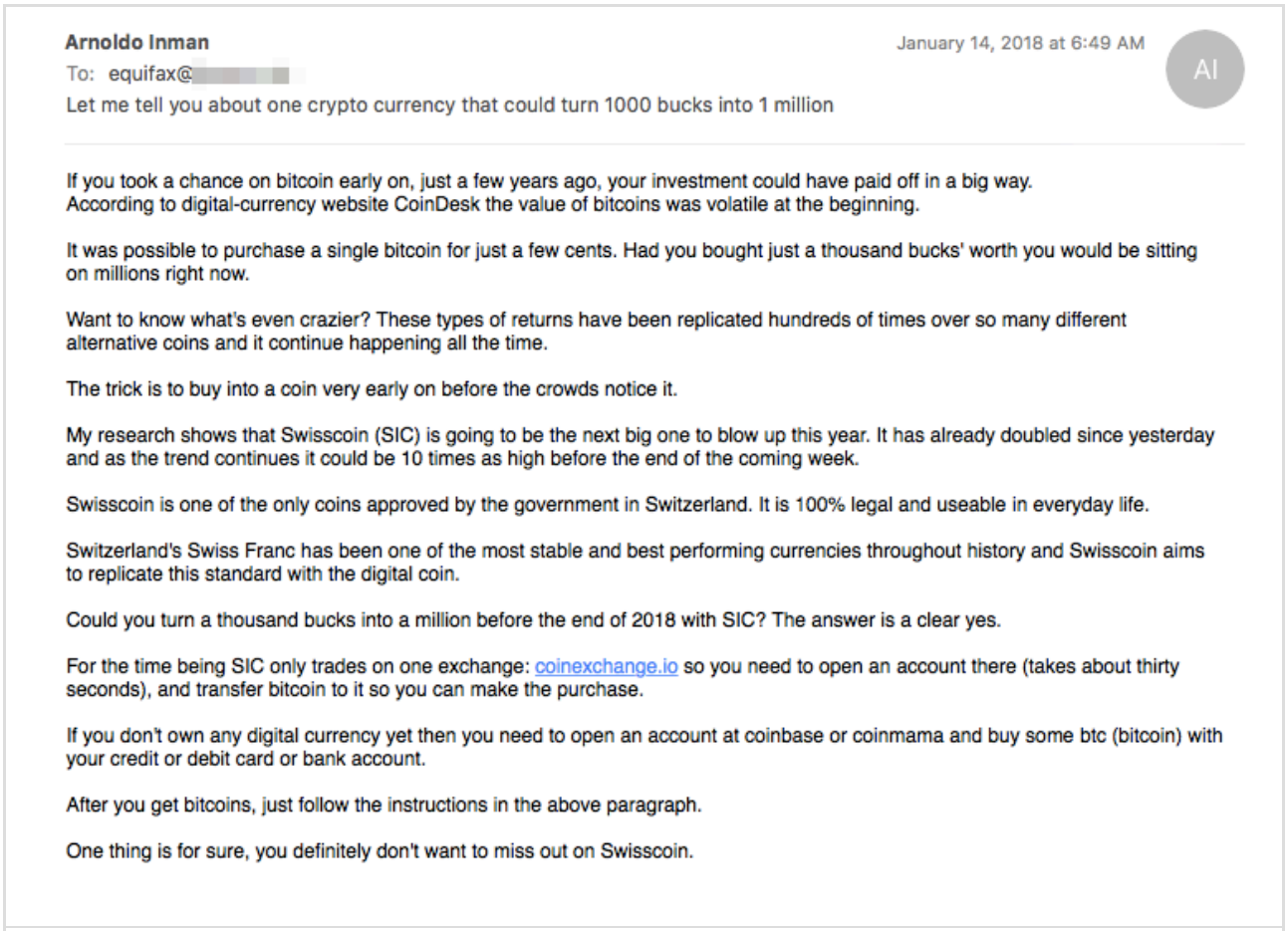
A typical ransomware campaign from Necurs

Cryptocurrency Credential Phishing The rise (and fall) in the value of digital currencies such as Bitcoin and Etherium has not escaped the attention of the Necurs criminals. They have been seen conducting attack campaigns using domains designed to look similar to legitimate wallet management websites. In the email below, note the extra word 'my' in the domain 'mymyetherwallet.com'.



This domain is registered to appear similar to the real Etherium wallet management site, myetherwallet.com

Recently, the Necurs attackers have drawn from previous stock pump-n-dump scams to come up with a relatively new tactic related to cryptocurrency. They had a spam campaign pumping Swisscoin (SIC).



Arnoldo Inman January 14, 2018 at 6:49 AM

To: equifax@

Let me tell you about one crypto currency that could turn 1000 bucks into 1 million

AI

If you took a chance on bitcoin early on, just a few years ago, your investment could have paid off in a big way. According to digital-currency website CoinDesk the value of bitcoins was volatile at the beginning.

It was possible to purchase a single bitcoin for just a few cents. Had you bought just a thousand bucks' worth you would be sitting on millions right now.

Want to know what's even crazier? These types of returns have been replicated hundreds of times over so many different alternative coins and it continue happening all the time.

The trick is to buy into a coin very early on before the crowds notice it.

My research shows that Swisscoin (SIC) is going to be the next big one to blow up this year. It has already doubled since yesterday and as the trend continues it could be 10 times as high before the end of the coming week.

Swisscoin is one of the only coins approved by the government in Switzerland. It is 100% legal and useable in everyday life.

Switzerland's Swiss Franc has been one of the most stable and best performing currencies throughout history and Swisscoin aims to replicate this standard with the digital coin.

Could you turn a thousand bucks into a million before the end of 2018 with SIC? The answer is a clear yes.

For the time being SIC only trades on one exchange: coinexchange.io so you need to open an account there (takes about thirty seconds), and transfer bitcoin to it so you can make the purchase.

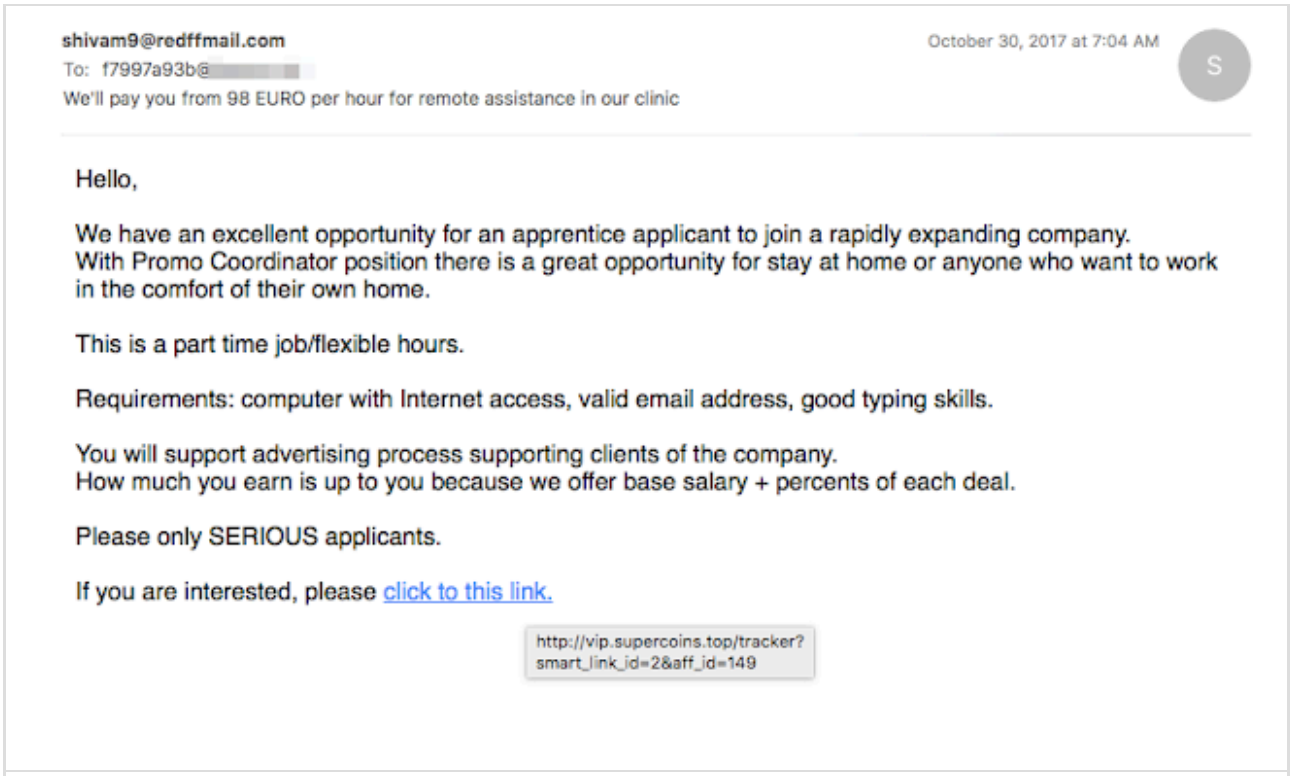
If you don't own any digital currency yet then you need to open an account at coinbase or coinmama and buy some btc (bitcoin) with your credit or debit card or bank account.

After you get bitcoins, just follow the instructions in the above paragraph.

One thing is for sure, you definitely don't want to miss out on Swisscoin.

A Necurs spam email encouraging recipients to buy Swisscoin (SIC)

Job Spam Necurs was recently sending a low volume job spam campaign which includes links to freshly registered domains. For example, in the email below, sent October 30th 2017, we can see they are using a link to the domain, 'supercoins.top'. (The affiliate id in the URL is always the same)



An example of a low volume, job-related spam campaign from Necurs

Attribution

whois-agent@gmx.com Checking the whois record for this domains we see the following registration details. Note the registrant email 'whois-agent@gmx.com'. This is an attempt by the threat actors to convince the casual observer that the domain is somehow registered through a third party whois privacy protection service. Email accounts @gmx.com are free to the public, and in this instance the attackers have simply generated the alias 'whois-agent' for their use in registering domains.

```
Domain Name: supercoins.top
Registry Domain ID: D20171029G10001G_26530340-top
Registrar WHOIS Server: www.eranet.com
Registrar URL: http://www.eranet.com
Updated Date: 2017-10-28T19:02:07Z
Creation Date: 2017-10-28T19:02:07Z
Registry Expiry Date: 2018-10-28T19:02:07Z
Registrar: Eranet International Limited
Registrar IANA ID: 1868
Registrar Abuse Contact Email: info@todaynic.com
Registrar Abuse Contact Phone: +86.7563810566
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID: C20171027C_23059018-top
Registrant Name: Song Ma
Registrant Organization: n.a.
Registrant Street: 45 Main road
Registrant City: Xiamen
Registrant State/Province: FJ
Registrant Postal Code: 361338
Registrant Country: CN
Registrant Phone: +86.5925764225
Registrant Phone Ext:
Registrant Fax: +86.5925764225
Registrant Fax Ext:
Registrant Email: whois-agent@gmx.com
Registry Admin ID: C20171027C_23059018-top
Admin Name: Song Ma
```

A review of the domains registered to 'whois-agent@gmx.com' yields 399 domains (from DT as of January 17, 2018). The list of domains registered to 'whois-agent@gmx.com' reads like a who's-who of criminal activity.

Among some of the more notable domains we can see obvious phishing domains:

```
 amex-notification.com
amexcardmail.com
amexmailnotification.com
natwestonlinebanking.info
hsbc-sec.site
dropbox-ch.co
dropbox-fileshare.com
dropboxmailgate.com
paypa1.info
sage-uk.com
sagepay.info
```

Typo-squattish domains targeting cryptocoin-related sites:

```
 myetlherwa11et.com
myetlherwalllet.com
rnyetherwa11et.com
blockchaifn.info
blockchaign.info
blockchainel.info
blockchaingr.info
blockchait.info
blockchalgn.info
blockchalne.info
blockchalner.info
blockchalng.info
blockchanel.info
blockchart.info
blockchatn.info
blockcheing.info
blockcheit.info
blockclmain.info
blockclnajn.info
bloclnchain.info
bloknchain.info
```

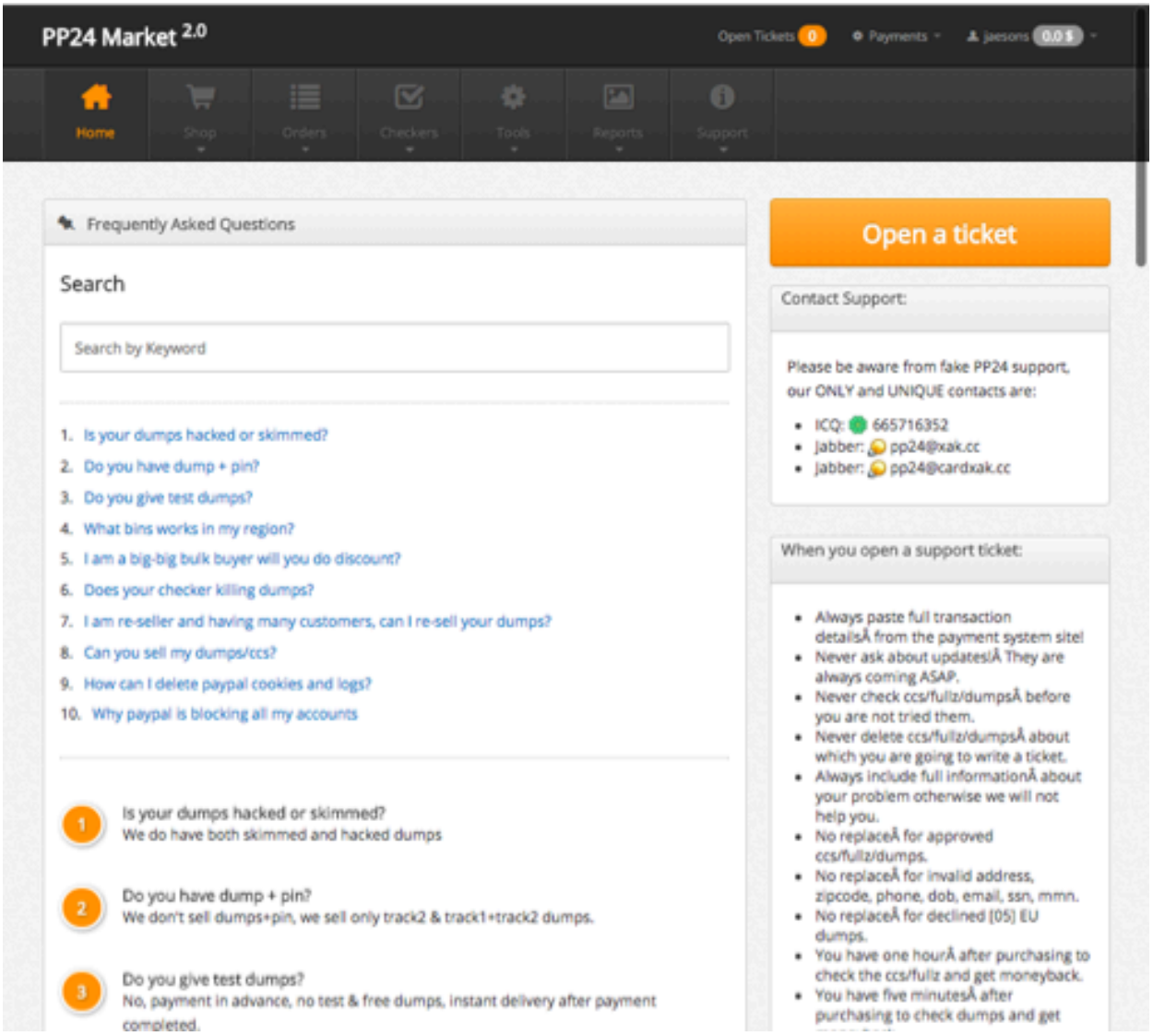
Fake Flash Player Update domains:

```
 flash-ide-update.top
flash-ime-update.top
flash-one-eupdate.top
flash-one-update.info
flash-player-update.info
flash-update-player.info
```

Even domains intended to masquerade as government resources:

```
 asic-gov-au.co
australia-gov-au.com
canadapost-office.info
govonfraud.info
```

A review of some of the domains in passive DNS gives us some other important clues. While most domains are only registered for the minimum of one year, the attackers have chosen to maintain the registration for a longer time on other domains such as 'pp24.ws'. That domain is home to an online marketplace for buying and selling stolen credit card numbers, stolen ssh account credentials and more.



'pp24.ws' is a website dedicated to buying and selling stolen credit card numbers

Passive DNS also reveals instances where the attackers have hosted domains belonging to different registrants on the same IP address. For example, when Talos analyzed the passive DNS records for one of the attacker's domains: 'setinfoconf.com' we found that this domain was hosted on a single IP address for a couple months in late 2016 before being parked. When we reviewed the other domains living on that same IP address we saw a bit of a pattern, and most importantly, some of these domains were NOT in the list of domains owned by 'whois-agent@gmx.com'.

bailiwick	**setinfoconf.com.**
count	1165
first seen	2016-09-28 18:08:15 -0000
last seen	2016-11-04 22:42:12 -0000

setinfoconf.com.	A	31.184.234.236

Returned 12 RRs in 0.05 seconds.

setconftr.pw.	A	31.184.234.236
setinifos.pw.	A	31.184.234.236
setinofis.pw.	A	31.184.234.236
settrconf.pw.	A	31.184.234.236
setconfise.pw.	A	31.184.234.236
setlaconfi.pw.	A	31.184.234.236
setlongconf.pw.	A	31.184.234.236
pop.hlttp.com.	A	31.184.234.236
setinfoco.com.	A	31.184.234.236
setinfoconf.com.	A	31.184.234.236
updatesetconf.com.	A	31.184.234.236
setconf.info.	A	31.184.234.236

whois-protect@hotmail.com When we check the registration information for one of the above domains 'setinofis.pw', we find that there is a different registrant. This time the email address used to register the domain was 'whois-protect@hotmail.com'. Just as with the 'whois-agent@gmx.com' address, this is an attempt to appear to a casual observer that the domain is protected by whois privacy protection when in reality this email account appears to be under the direct control of the attackers themselves.

```
Domain Name: SETINOFIS.PW
Registry Domain ID: D37256486-CNIC
Registrar WHOIS Server: whois.todaynic.com
Registrar URL: http://www.now.cn/
Updated Date: 2016-10-25T08:47:47.0Z
Creation Date: 2016-10-08T19:40:01.0Z
Registry Expiry Date: 2018-10-08T23:59:59.0Z
Registrar: ERANET INTERNATIONAL LIMITED
Registrar IANA ID: 1868
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod
Registry Registrant ID: C86359736-CNIC
Registrant Name: Xing Wang
Registrant Organization: private
Registrant Street: Xiamen
Registrant City: Xiamen
Registrant State/Province: FJ
Registrant Postal Code: 361009
Registrant Country: CN
Registrant Phone: +86.5925778828
Registrant Fax: +86.5925778828
Registrant Email: whois-protect@hotmail.com
Registry Admin ID: C86359741-CNIC
Admin Name: Xing Wang
```

Reviewing the list of 1103 domains (Domain Tools as of January 17, 2018) associated with the 'whois-protect@hotmail.com' email address we see much of the same illicit activity we saw before.

More phishing domains:

```
 amex-psk.org
amexsafetykey.org
applerecoveryprogram.com
applerecoveryprogram.top
barcalys-offers-online.com
bt-europe.com
btconnect.biz
btconnect.info
bttconnect.com
dhl4.com
docusign-australia.com
docusign-net.com
docusigner.org
dropbox-eu.com
dropboxa.com
dropboxes.org
dropboxsharing.com
dropboxsmarter.com
e-intuit.com
efaxplus.com
global-intuit.com
hsbcbank.top
inc-r.com
ing-update.info
kbc-bank.info
paupal.info
```

```
paypa.info
poypa1.info
quickbooks-intuit-uk.com
quickbooks-support.biz
quickbooksonlineaccounting.com
sage-uk.org
sageim.com
sages.biz
sagetop.com
security-hsbc.site
servicebying.com
telestrasystems.com
vodafonestore.net
wellsfargocertificate-637-9270.com
```

More domains targeting cryptocoin-related resources:

```
 blockchfain.info
blokochain.info
myethelrwallet.com
myetherwallet.top
myetherwlallet.com
myethlerwallet.com
rnyetherwlallet.com
```

Similar themed, fake Flash Player updates:

```
 flash-foe-update.win
flash-ire-update.win
flash-new-update.info
flash-old-update.top
flash-ome-update.win
flash-one-eupdatee.top
flash-one-eupdatte.top
flash-one-update.top
flash-one-update.win
flash-onenew-update.info
flash-ooe-update.win
flash-ore-update.win
flash-oue-update.top
flash-owe-update.win
flash-oxe-update.win
flash-oye-update.win
flash-playernewupdate.info
flash-toe-update.win
flash-woe-update.win
```

```
flash-yoe-update.win
flashnew-update.info
flashplayernew-update.info
```

We even see targeting of government resources, just as we did with the other registrant account:

```
 afp-gov-au.com
asic-au-gov.com
asic-gov-au.com
asic-government-au.com
asic-mail-gov-au.com
asic-message-gov-au.com
asic-notification-gov.com
ato-gov-au.net
augovn.com
austgov.com
australiangovernement.com
australiangovernments.com
federalgovernmentaustralia.com
gov-invoices.info
goviau.co
```

tzyywz@qq.com Checking the registration on some of the domains associated with 'whois-privacy@hotmail.com', we can find some domains in which there are other registrants and the whois-privacy@ address is simply an Administrative and Technical Contact. This reveals an additional registrant email address employed by the attackers, 'tzyywz@qq.com'.

```
Domain name: setinfoco.com
Registry Domain ID: 77428276_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.todaynic.com
Registrar URL: http://www.now.cn/
Update Date: 2017-05-14T16:00:00Z
Creation Date: 2016-10-03T09:11:43Z
Registrar Registration Expiration Date: 2017-10-02T16:00:00Z
Registrar: Todaynic.com, Inc.
Registrar IANA ID: 697
Registrar Abuse Contact Email: cs@now.cn
Registrar Abuse Contact Phone: +86.7563810552
Reseller:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: todr179241
Registrant Name: 8NOW LIMITED
Registrant Organization: 8NOW LIMITED
Registrant Street: shanyangxian
Registrant City: ShanXiSheng
Registrant Province/state: BJ
Registrant Postal Code: 726400
Registrant Country: CN
Registrant Phone: +86.13949491448
Registrant Phone EXT:
Registrant Fax: +86.13949491448
Registrant Fax EXT:
Registrant Email: tzyywz@qq.com
Registry Admin ID:
Admin Name: Sung Lee
Admin Organization: private
Admin Street: Xiamen
Admin City: Xiamen
Admin Province/state: FJ
Admin Postal Code: 361016
Admin Country: CN
Admin Phone: +86.592577881228
Admin Phone EXT:
Admin Fax: +86.592577881228
Admin Fax EXT:
Admin Email: whois-protect@hotmail.com
Registry Tech ID:
Tech Name: Sung Lee
Tech Organization: private
```

According to Domain Tools (as of January 17, 2017), that qq.com email address is associated with over 2500 domains. Most of the domains belonging to this registrant email appeared to be domainer-style domains located at TLDs such as .bid and .top, but we also see a heavy dose of illegitimate looking domains in the set as well.

Some typical 'Domainer'-ish domains:

```
 aapk.bid
aapo.bid
aapq.bid
aapu.bid
aapv.bid
aapw.bid
aapx.bid
jbanj.top
jcqth.top
jhtaq.top
jhugs.top
jian0.top
jian1.top
```

```
jian2.top
jian3.top
```

Illegitimate Domains:

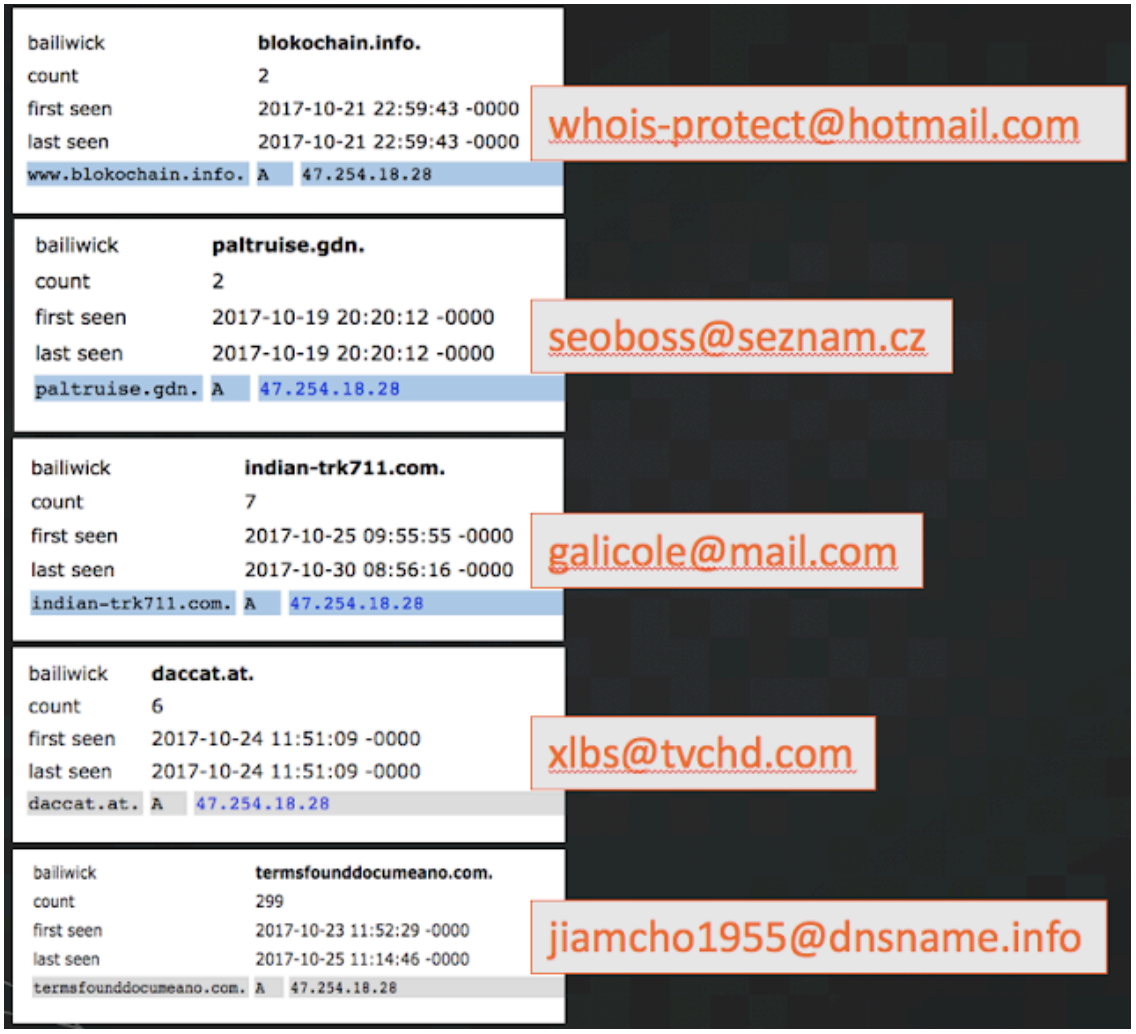
```
 amex-notification.com
amexaccountvalidate.com
amexcardcustomerservice.com
amexcardmail.com
amexcardpersonalsafetykey.com
amexcardpsk.com
amexcardsafetykey.com
amexcardservice.com
amexcardservicevalidate.com
amexcardsupport.com
amexcardsupportservice.com
amexcardsupportteam.com
amexcardverification.com
amexcardverified.com
amexcardverifier.com
amexcloudcervice.com
amexcustomersupport.com
amexmailnotification.com
amexotpcardcustomerservice.com
amexotpcardsupport.com
amexotpgenerate.com
amexotpgeneratesetup.com
amexotpsetup.com
amexotpsetupcustomerservice.com
amexotpsetupservice.com
amexpersonalsafekey.com
amexpersonalsafetykey.com
amexpersonalsafetykeyregistration.com
amexpersonalsafetykeysupport.com
amexpskcustomerservice.com
amexpskkey.com
amexpsksupport.com
amexsafetykeycustomerservice.com
amexverifier.com
amexverifierservice.com
docusign-australia.com
docusign-net.com
dropboxbusinessaccount.com
mail-asic-government-au.com
postbank-kundennummer43.com
```

```
postbank-kundennummerfinnaz.com
salesforceproaccount.com
verifybyamericanexpress.com
verifybyamexcards.com
yandex-login.com
yandex-user578185.com
yandex-user912.com
yandex-user952.com
```

More Domain Registrant Accounts Revealed We can associate even more registrant email accounts with these same threat actors using similar techniques. While researching passive DNS for one of the domains we found previously, 'blokochain.info', we ran across something very interesting. That particular domain was hosted October 21, 2017 on the IP address 47.254.18.28 which belongs to Alibaba as part of their cloud hosting product. When we analyze all the other domains which have been hosted on that same IP we see many domains that belong to the registrant email addresses we already knew about, 'whois-agent@gmx.com' and 'whois-privacy@hotmail.com'. However we also see several domains associated with different registrants.

Returned 28 RRs in 0.03 seconds.

fidom.at.	A	47.254.18.28
daccat.at.	A	47.254.18.28
farleza.co.	A	47.254.18.28
www.farleza.co.	A	47.254.18.28
www.foramis.co.	A	47.254.18.28
forandr.co.	A	47.254.18.28
www.forandr.co.	A	47.254.18.28
www.farforta.co.	A	47.254.18.28
forbulbs.co.	A	47.254.18.28
sdg32623d.com.	A	47.254.18.28
adverti-click.com.	A	47.254.18.28
indian-trk711.com.	A	47.254.18.28
stshippingfirst.com.	A	47.254.18.28
limitedbinarycthe.com.	A	47.254.18.28
atlanticfinanceltd.com.	A	47.254.18.28
www.atlanticfinanceltd.com.	A	47.254.18.28
termsfounddocumeano.com.	A	47.254.18.28
chttpveranyshoissuesthis.com.	A	47.254.18.28
paltruise.gdn.	A	47.254.18.28
gradual.paltruise.gdn.	A	47.254.18.28
kursaal.paltruise.gdn.	A	47.254.18.28
etherified.paltruise.gdn.	A	47.254.18.28
subimposed.paltruise.gdn.	A	47.254.18.28
exteriorising.paltruise.gdn.	A	47.254.18.28
www.hontorbam.top.	A	47.254.18.28
domestosdoom.top.	A	47.254.18.28
blokochain.info.	A	47.254.18.28
www.blokochain.info.	A	47.254.18.28



seoboss@seznam.cz Looking at the list of domains found on this same Alibaba IP we find the domain 'paltruise.gdn'. This domain is registered to the registrant email address, 'seoboss@seznam.cz'. This registrant has registered 125 domains (Domain Tools as of January 17, 2018), many of which have been linked to malicious activities. According tothese links, domains associated with this registrant email have been used as part of the Rig Exploit Kit infrastructure. The domain, 'paltruise.gdn', was hosted on the 47.90.202.68 Alibaba IP address on October 19, 2017 --only two days before the IP was used to host domains belonging to 'whois-protect@hotmail.com'.

galicole@mail.com The domain 'indian-trk711.com' belongs to the registrant email address 'galicole@mail.com'. The 'indian-trk711.com' domain was hosted on the 47.254.18.28 IP on October 25th through October 30th, 2017 --also very close to the timeframe in which we saw the IP hosting the other malicious domains.

As of January 16, 2017, DomainTools attributes 918 domains to the registrant email address 'galicole@mail.com'. Among some of the domains associated with this address we find gems such as:

```
 1royalbankrbcdirect.top
amex-onlinesecurity.top
buydumps.top
```

```
buydumpsonline.top
carder-cvv-shop.top
carder-cvv.name
carding-cvv-shop.top
carding-shop-cvv.top
carding-shop-track2.top
cardingcvv.top
cardingshoponline.top
cvv-carder.name
cvv-online-market.com
cvv-shop-carder.name
cvv-valid.info
cvv2-online-store.top
cvvcarder.name
cvvdumppluspin.top
cvvshopcarder.top
dumps-shop-valid.top
dumps-valid-shop.top
dumpsonlinestore.top
dumpsshopvalid.top
netflic-validatesystem.info
netflix-information.info
netflix-supportvalidate.info
netflix-verifysupport.info
netflix-veriificationbilling.info
netflixveriify.info
shop-dumps-valid.top
shop-online-cvv2.info
shop-online-dump.top
shopcardingonline.top
shopcardingtrack2.top
shopcvv2online.biz
shopcvvcarding.top
shopdumpsvalid.top
shoptrack2carding.top
store-cvv-online.biz
storecarderverified.biz
storecvv2.name
track2-shop-verified.biz
track2cardingshop.top
track2verifiedshop.top
valid-dumps.top
valid-market-cvv.top
valid-shop-cvv.top
valid-shop-dumps.top
validdumpsshop.top
verified-carder-store.com
```

```
verifiedcarderstore.biz
verifieddumpsshop.top
verifiedstorecarder.biz
verifiedtrack2shop.info
```

xlbs@tvchd.com The domain 'daccat.at' is registered to 'xlbs@tvchd.com'. A Google search for this domain produces this link at Hybrid Analysis and indicates that this particular domain was contacted as part of a piece of malware. At Virus Total, 50/68 antivirus engines detect this particular sample as malicious.

jiamcho1955@dnsname.info Searching Google for this registrant email address yields multiplelinks to malware that reaches out to domains owned by 'jiamcho1955@dnsname.info'. Virus Total corroborates this information showing 48 and 53 antivirus detections respectively.

One Instance to Host Them All Reaching out through various contacts, Talos was able to confirm that, in fact, *a single Alibaba cloud instance was controlling this same IP address for the entire time period from October 19, 2017 through October 30, 2017*. Is this IP address some part of a criminal domain hosting service? Or is it that a single nefarious enterprise is behind all of these various registrant email accounts and their associated domains? Only the criminals involved in this enterprise can say for certain. Talos continues to monitor this situation with an eye towards further deciphering the business model deployed by these miscreants.

Conclusion Now that Necurs is back from their regular holiday break they are attempting to fill our inboxes with junk mail and malware once again. On one hand, the size of the Necurs botnet, and its ability to send from different nodes in every campaign makes it difficult to defend against; Standard IP address blocklists are ineffective against such tactics. Fortunately for network defenders, the fact that Necurs does relatively little to curate their recipient database limits the damage they can do. There are only so many times the same recipients will fall for Necurs' same, repetitive tricks. We can expect that Necurs will continue to try variations on some of their tried and true attacks, and so user education against these threats remains paramount.
