



Necurs: Estructura, Actividad y Descripción en detalle

Jaeson Schultz
Technical Leader, Security Research



Agenda



La composición de la botnet Necurs

- ¿Dónde están las ubicaciones de la mayoría de los bots Necurs?
- ¿Cuánto se reutiliza la infraestructura de Necurs en diferentes campañas de spam?
- ¿Cuál es el tamaño de la red de bots Necurs en general?

El origen, la composición y el uso de la base de datos de destinatarios de Necurs

- ¿Dónde obtuvieron Necurs las direcciones de correos electrónicos de las víctimas?
- ¿Cómo se ha mantenido la base de datos de los destinatarios con el tiempo?

Una mirada al interior de las tácticas y la infraestructura utilizada por los criminales Necurs

- ¿Cuáles son los diversos enfoques de ingeniería social tomados?
- ¿Cómo evolucionan los ataques de Necurs?

Puntos de datos para considerar hacia la atribución: ¿quién está detrás de esta empresa?

- ¿Qué dicen los registros de dominio de los atacantes sobre sus objetivos actuales?
- ¿Qué indica la seguridad operacional de los atacantes sobre su tolerancia al riesgo?
- ¿Dónde están los atacantes de Necurs?



Los Datos

- Extractamos 32 compañías completas de spam de Necurs

(entre agosto de 2017 – noviembre de 2017)

- Mas que 2.1 millones mensajes spam
- 1,192,498 direcciones IP únicas del remitente de 216 países

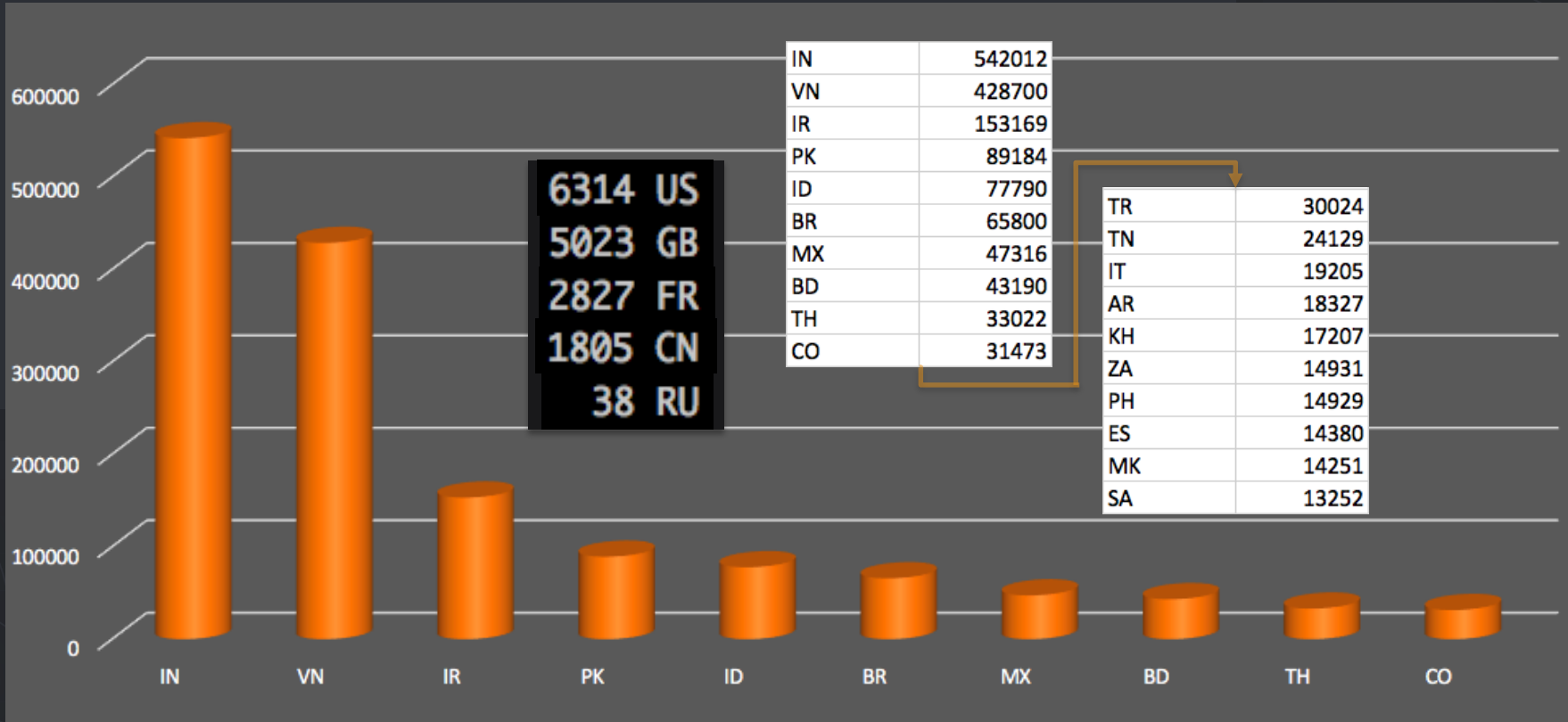
spamcop.net

- Estados de cuenta bancarios, Facturas comerciales, Transacciones de Ethereum, Citas rusas, Escaneos de documentos, Pump-n-Dump (stock de centavo), Mensajes de correo de

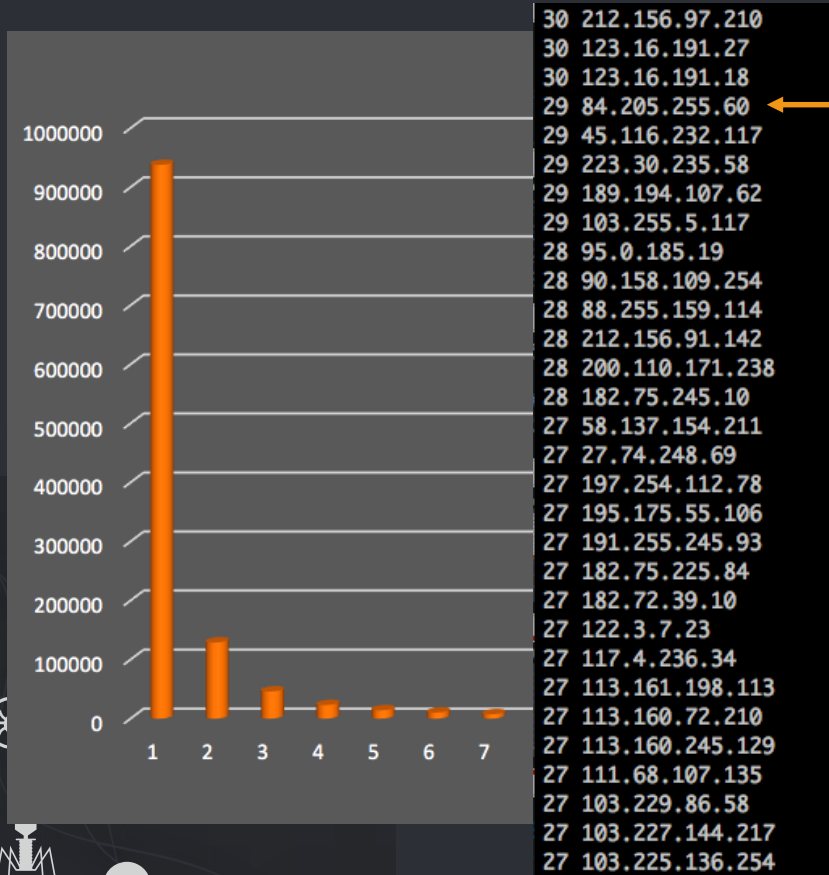
VOZ



Spam por País



Reutilización de direcciones IP



srv2.n1.syzefxis.gov.gr.

# of Campaigns	Unique IPs
1	937761
2	128916
3	45941
4	22900
5	14060
6	10140
7	7362
8	5820
9	4626
10	3481
11	2755
12	2194
13	1703
14	1146
15	910
16	710
17	558
18	378
19	311
20	262
21	190
22	135
23	89
24	54
25	44
26	22
27	16
28	6
29	5
30	3

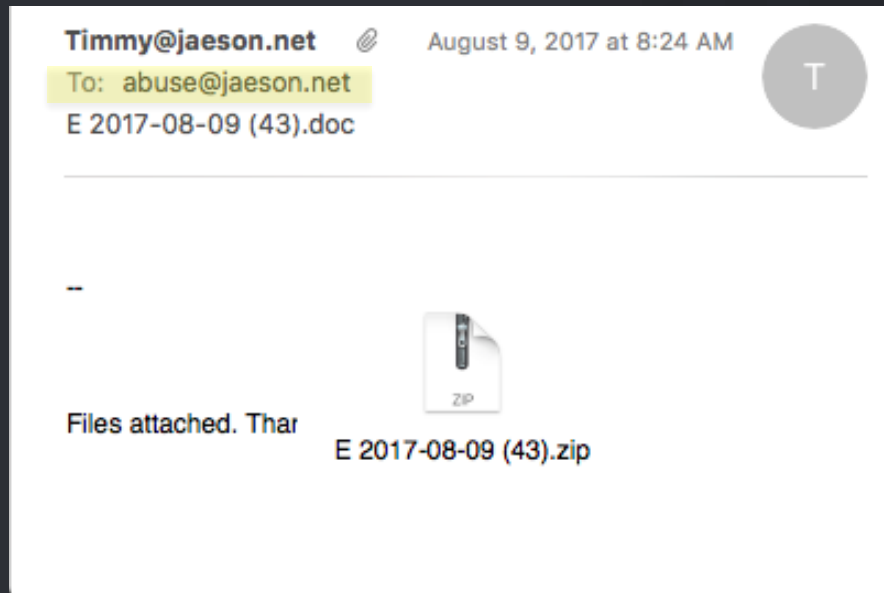
Destinatarios Necurs



- Cosechado por Internet

~~• Auto generado~~

- Cuentas comunes/
basadas en roles



Destinatarios Comunes de Necurs

Destinatario	# de Dominios
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

Destinatarios Comunes de Necurs

Top Dictionary Attacker Usernames Of All time	
Username	Occurrences
1. iamjustsendingthisleter	18,125,199
2. info	9,334,317
3. sales	7,519,260
4. admin	6,217,159
5. buh	5,528,318
6. bux	5,200,657
7. direktor	5,158,753
8. buhgalteria	5,085,163
9. buhg	5,056,428
10. dir	5,006,040
11. finance	4,994,525
12. buhgalter	4,990,919
13. hr	4,292,344
14. thisisjusttestletter	4,135,128
15. sekretar	4,120,962
16. director	3,812,851
17. contact	3,752,781
18. support	3,039,824
19. petgord34truew	1,781,015
20. contactus	1,634,084
21. mail	1,508,197
22. manager	979,514
23. adm	929,062
24. billing	843,289
25. home	823,089
26. business	817,189

Spam Campañas de Necurs



Las Campañas de Necurs típicamente vienen en dos variedades:

- Volumen alto, de lunes a viernes
- Volumen bajo, constante



Campaña de spam - Acciones



Rob Dennis

April 12, 2017 at 10:01 AM

RD

To: petgord34truew@jaeson.net

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.



Campaña de spam - Acciones

Market summary > Quest Management Inc

OTCMKTS: QSMG - Dec 7, 4:00 PM EST



0.020 USD 0.000 (0.00%)

1 day

5 day

1 month

3 month

1 year

5 year

max

2.33 Apr 13, 2017



Open 0.020
High 0.022
Low 0.020

Mkt cap 1.44M
P/E ratio -
Div yield -

[→ Financial news, comparisons and more](#)

Campaña de spam - Citas

Barbara

November 23, 2017 at 9:34 AM

B

To: tech@jaeson.net

hi

Hi to the hottest man in the world, which is tech, my name is Barbara and i'm from Russia, but currently living in the USA.

I just wanted to let you know that seeing your profile made me want to have you in my life.

You are type of guy, who can help through bad times and share the good times and I would love to have someone like you next to me.

If its mutual, email me, this is my email terezaxyqlgisela@rambler.ru and I will send some of my photos.

Hugs,
Barbara

Campaña de spam - Citas



MarmeLadies

November 9, 2017 at 10:35 AM

M

To: paz@lasvegans.net

Reply-To: email_notify@marmeladies.site

Your profile at MarmeLadies is Active now!

Dear Geek,

Your profile at MarmeLadies has been reviewed and activated!

Email: paz@lasvegans.net

Password: faux99gv

Simply follow the link below to enjoy our services:

<http://marmeladies.site/member.php>

Please be advised that you'll be receiving more letters and thus your chances to meet the perfect match will grow if you fill in your profile (description of you and the person you're looking for, your height and body type, etc.) and attach your photos.

Your e-mail used for registration: paz@lasvegans.net

Thank you for using our services!

To contact MarmeLadies Client Support, please follow the link:

<http://marmeladies.site/contact.php>

This notification was generated automatically and you are receiving it since you've registered at MarmeLadies

If you'd like to cancel your registration and stop receiving all notifications, please follow the link <http://marmeladies.site/unsubscribe.php>

--

MarmeLadies mail delivery system!!!

Auto-generated e-mail, please, do not reply!!!



Campaña de spam - Ransomware

Microsoft Voice 

August 1, 2017 at 10:06 PM

Voicemail From 845-551-5100 at 9:35AM

MV

Voice Message received at 9:35AM Voicemail Length 19sec



VM98915952_20170801
.zip

Campaña de spam - Ransomware

vpsonlinebillmanager@vodafone.com

To: petgord34truew@jaeson.net

Online Bill Manager - Your Phone Bill is ready to view

August 2, 2017 at 8:23 AM



Vodafone bill is ready

Dear Customer,

You can now take a look and manage [your latest Vodafone bill](#) for invoice date 02/08/2017.

Your total bill for this month is £ 441.46

Don't forget, your line rental is charged a month in advance and calls are charged in arrears.

[Click here to view your bill](#)

http://support.cl-support.co.uk/Bill_02082017.doc

Benefits of Online Billing

- Print replica Paper Bills
- Monitor who uses what and how costs are accrued
- Practical breakdowns of usage across account and handsets
- View costs accrued so far in the month and set alerts
- Available 24/7

Finally, if you're yet to take full advantage of our Online Bill

Useful Information

Logging In

If you've forgotten or don't know you log-in details, click on "Forgotten Password" on the log-in page. Your User ID is your Account Number.

Paper-free Billing

As part of our Corporate Social Responsibility and efforts to protect the environment, we are encouraging customers to cancel their paper bills and utilise our fantastic Online Bill Manager. If you're yet to cancel your paper bill, contact us and we'll be happy to help.

Contact Us

Phone:
03333 044550
Email:
customer.service@vodafone.com

Campaña de spam -



Glenna Robinson

April 17, 2017 at 5:21 PM

GR

To: petgord34truew@jaeson.net

Do not miss on this chance to triple your money in the market

There is a rare opportunity in the market right now, so rare that it may only happen once in a lifetime.

I have it on good information that a small biotech company is about to receive approval from the f d a for a life-saving medicine.

This medicine is poised to become the next biggest seller in the world as it has just been shown to kill cancer.

This is why there has been a lot of activity surrounding the stock. People are trading it on wrong information, and it's in the red today because of that.

I highly suggest that you buy in right now while fools are getting out, and the stock is cheap because it's going to go up twenty fold in the next 2 weeks

when the public announcement comes out, and the medicine is officially approved. Move quickly though, because otherwise you will miss out.



Campaña de spam - Cryptocoins

cosmi@cosmina.ro

October 17, 2017 at 6:03 PM



To: f7997a93b@jaeson.net

New transaction

You have a new transaction on your Ethereum Wallet.

Login to check your balance:

<https://mymyetherwallet.com/#view-wallet-info>



Campaña de spam - Cryptocoins

← → ↻ <https://www.myetherwallet.com> ☆

DON'T GET PHISHED, please! 🙏 Thank you! 😊
1. BOOKMARK MYETHERWALLET.COM 2. INSTALL EAL or MetaMask or Cryptonite

3.10.9.6
English ▾
Gas Price: 50 Gwei ▾
Network ETH (MyEtherWallet) ▾

MyEtherWallet

[New Wallet](#) [Send Ether & Tokens](#) [Swap](#) [Send Offline](#) [Contracts](#) [ENS](#) [DomainSale](#) [Check T](#) »

Create New Wallet

Enter a password

Do NOT forget to save this!

Create New Wallet

Already have a wallet somewhere?

- Ledger / TREZOR / Digital Bitbox : Use your **hardware wallet** . Your device *is* your wallet.
- MetaMask Connect via your **MetaMask Extension** . So easy! Keys stay in **MetaMask extension**



Campaña de spam - Pharma

ipeter.mather1t@onlymail.com

June 15, 2017 at 1:09 PM

To: petgord34truew@jaeson.net

Become better now – Upgrade your brain memory and intellectual potential

Take these tabs to increase your memory and improve your mental power.

The first science-based brain-boosting solution that actually works,
all you gotta do to change your life is to join up [visit a website](http://www.niledeal.com/wp-content/themes/davinci/71551dc49e3.html).

[http://www.niledeal.com/wp-content/themes/
davinci/71551dc49e3.html](http://www.niledeal.com/wp-content/themes/davinci/71551dc49e3.html)

Campaña de spam -



• uiuljbdwcq@jaeson.net	uiuljbdwcq@jaeson.net	Vi offriamo la possibilita di guadag...	Sep 28, 2017
• dekonind@brtph8a0.bnr.ca	uiuljbdwcq@jaeson.net	messaggio 1789	Sep 27, 2017
d.bemosi@crisconf.it	uiuljbdwcq@jaeson.net	Re: CV # 0666	Sep 27, 2017
fwd.1092816258zvdK@anzeige...	uiuljbdwcq@jaeson.net	offerta # 8622	Sep 27, 2017
coopsanaalnn@epm.net.co	uiuljbdwcq@jaeson.net	lo brucio con passione...	Sep 23, 2017
• estenico@infonie.fr	uiuljbdwcq@jaeson.net	Ragazza calda che si desidera!	Sep 23, 2017
pakavso@locos.com	uiuljbdwcq@jaeson.net	lo brucio con passione...	Sep 23, 2017
• a.duss@agenzia lavoro.tn.it	uiuljbdwcq@jaeson.net	Ottime notizie	Sep 22, 2017
webshop@masternet.it	uiuljbdwcq@jaeson.net	Ottime notizie	Sep 22, 2017

dekonind@brtph8a0.bnr.ca

September 27, 2017 at 10:25 PM

To: uiuljbdwcq@jaeson.net
messaggio 1789

D

Caro uiuljbdwcq,

Io sono HR manager di una grande compagnia internazionale.
La nostra azienda è alla ricerca di collaboratori intraprendenti.
Il stipendio possibile da 2900 a 5800 euro al mese.

Se Le interessa nostra offerta - si prega di visitare il [Nostro Sito](#)

Con i migliori saluti,
HR Manager
Ufficio Internazionale



Campaña de spam - Trabajo



d5b4e4a20@jaeson.net	d5b4e4a20@jaeson.net		May 16, 2017
suyamto.sudjono@medcoenergi...	d5b4e4a20@jaeson.net	cooperacion con una compania inte...	Jun 4, 2017
zcwogtx269@7desejos.com.br	d5b4e4a20@jaeson.net	Crecimiento de carrera	Jun 4, 2017
emily@hlkn.tamu.edu	d5b4e4a20@jaeson.net	Horario flexible	Jun 4, 2017
Postmaster@bariloche.com.ar	d5b4e4a20@jaeson.net	DELIVERY FAILURE: User obertohr (...)	Jun 4, 2017
annettaann1093@germanmails....	d5b4e4a20@jaeson.net	Vacancia abierta	Jun 5, 2017
chiki1@codetel.net.do	d5b4e4a20@jaeson.net	Ocupacion parcial	Jun 5, 2017
postmaster@gesmedia.es	d5b4e4a20@jaeson.net	Undeliverable: El empleo parcial	Jun 6, 2017
hvu@netlogicmicro.com	d5b4e4a20@jaeson.net		Aug 17, 2017

emily@hlkn.tamu.edu

To: d5b4e4a20@jaeson.net

Horario flexible

June 4, 2017 at 7:17 PM

Not Jaeson

E

¡Hola!

estamos en búsqueda de empleados que trabajen a distancia.
Mi nombre es Cora, soy el gerente de personal de una gran empresa internacional.

La mayor parte del trabajo usted puede realizar desde casa, es decir, a distancia.
Salario es de 2500 a 5000 EUR.

Si usted está interesado en esta oferta de trabajo, a continuación,
por favor visite [Nuestro Sitio](#)

Atención a las condiciones e <http://www.jp.dpseals.com/9412ebb3972.html>

Atribución de Necurs



peter3nn@striker.ottawa.on.ca

November 2, 2017 at 12:30 PM

To: f7997a93b@jaeson.net

Interesting work

P

Good day!

We considered your resume to be very attractive and we thought the vacant position in our company could be interesting for you.

Our firm specializes in online services in the matter of business administration.
We cooperate with different countries and currently we have many clients in yours region.
Due to this fact, we need to increase the number of our destination representatives' regular staff.

Part-time and full-time employment are both currently important.
We offer a flat wage from \$1500 up to \$7000 per month.

If you are interested in our offer, please [visit our web page](#).

Attention! Accept applications only on this and next week

[http://vip.newbinconsult.top/tracker?
smart_link_id=2&aff_id=149](http://vip.newbinconsult.top/tracker?smart_link_id=2&aff_id=149)

Respectively submitted
Personnel department



whois-agent@gmx.com



```
Domain Name: newbinconsult.top
Registry Domain ID: D20171102G10001G_26926219-top
Registrar WHOIS Server: www.eranet.com
Registrar URL: http://www.eranet.com
Updated Date: 2017-11-01T20:56:06Z
Creation Date: 2017-11-01T20:56:06Z
Registry Expiry Date: 2018-11-01T20:56:06Z
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
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
Admin Organization: n.a.
Admin Street: 45 Main road
Admin City: Xiamen
Admin State/Province: FJ
Admin Postal Code: 361338
Admin Country: CN
Admin Phone: +86.5925764225
Admin Phone Ext:
Admin Fax: +86.5925764225
Admin Fax Ext:
Admin Email: whois-agent@gmx.com
Registry Tech ID: C20171027C_23059018-top
```



whois-agent@gmx.com



Email Address *Exactly Matching* "WHOIS-AGENT@GMX.COM"

Reverse Whois Report Preview

Report Compiled: 11/17/2017

#	Domain	Whois Record
1	ACKNOWLEDGEPRODUCE.COM	10/26/2017, 10/27/2017, 11/1/2017
2	ACONNECTGATEWAY.COM	2/29/2016, 5/9/2016, 9/27/2016, 11/24/2016, 12/5/2016, 12/14/2016, 2/27/2017, 3/2/2017
3	ADREBANO.COM	11/23/2015, 11/25/2015, 11/30/2015, 11/25/2016
4	ADVERMARKET.NET	12/4/2014, 1/26/2015, 7/17/2015, 9/11/2015, 12/2/2015, 12/6/2015
5	ADVERTI-CLICK.COM	10/21/2017, 10/22/2017, 10/23/2017, 10/26/2017, 10/29/2017, 10/31/2017, 11/1/2017, 11/2/2017
6	AEXP-SUPPORT.COM	1/25/2016, 1/26/2016, 6/30/2016, 12/6/2016, 1/27/2017
7	AEXPCREDITCARD.COM	2/22/2016, 2/23/2016, 7/1/2016, 12/6/2016, 2/24/2017
8	AEXPGLOBAL.COM	2/22/2016, 2/23/2016, 6/29/2016, 12/4/2016, 2/24/2017
9	AEXPSUPPORT.COM	1/25/2016, 1/26/2016, 10/16/2016, 1/23/2017, 1/27/2017
10	AGROPIDA.INFO	1/17/2017, 1/23/2017, 5/26/2017



whois-agent@gmx.com



67	BLOCKCHATN.INFO	10/27/2017
68	BLOCKCHEING.INFO	10/24/2017, 10/25/2017
69	BLOCKCHEIT.INFO	10/26/2017, 10/27/2017, 10/28/2017, 11/13/2017, 11/14/2017
70	BLOCKCLHAIM.COM	11/2/2017, 11/3/2017, 11/4/2017
71	BLOCKCLHAIM.INFO	11/3/2017, 11/4/2017, 11/8/2017
72	BLOCKCLHALN.COM	11/2/2017, 11/3/2017
73	BLOCKCLHALN.INFO	10/31/2017
74	BLOCKCLHAN.COM	11/2/2017, 11/3/2017
75	BLOCKCLHAN.INFO	11/3/2017, 11/4/2017
76	BLOCKCLMAIN.INFO	10/30/2017, 10/31/2017
77	BLOCKCLNAFN.COM	11/2/2017, 11/3/2017, 11/8/2017
78	BLOCKCLNAJN.INFO	10/30/2017, 10/31/2017
79	BLOCKCLNALN.COM	11/2/2017, 11/3/2017
80	BLOCKCLNALN.INFO	11/3/2017, 11/4/2017, 11/8/2017
81	BLOCKCLNEIN.COM	11/2/2017, 11/3/2017, 11/4/2017
82	BLOCKCLNEIN.INFO	11/3/2017, 11/4/2017, 11/8/2017
83	BLOCLNCHAIN.INFO	10/30/2017, 10/31/2017
84	BLOEKCHAIN.INFO	10/31/2017, 11/1/2017, 11/2/2017, 11/4/2017
85	BLOKNCHAIN.INFO	10/30/2017, 10/31/2017, 11/1/2017



whois-agent@gmx.com



PP24 Market 2.0

Open Tickets 0 Payments jaesons 0.0\$



Home



Shop



Orders



Checkers



Tools



Reports



Support

SSH Shop

SSH SEARCH

Country	United States (209)	ZIP	
State		City	
Seller	-- All --	BlackList	☒ ALL ☐ Yes ☐ No
Load date	All	Count rows	100
<button>Search in database</button>			

Search results

found 100 ssh accounts

Buy selected

Select all

Nº	Seller	IP	Country	ZIP	State	City	BlackList	Check_SSH	Load date	Price
1	kavergreen	71.0.***.***	United States	89109	Nevada	Las Vegas	+	<button>Check</button>	25.04.2017	0.50
2	kavergreen	23.25.***.***	United States	15024	Pennsylvania	Cheswick	+	<button>Check</button>	25.07.2017	0.50

3

Do you give test dumps?

No, payment in advance, no test & free dumps, instant delivery after payment completed.

- Check the description and get money back.
- You have five minutes after purchasing to check dumps and get

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.hlhttp.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

Registrant Name: Wang Lao
Registrant Organization: n.a.
Registrant Street: 41 Main road
Reg. Registrant Name: Wun Seng
Reg. Registrant Organization: n.a.
Reg. Registrant Registrant Name: Whois Agent
Reg. Registrant Registrant Organization: NA
Reg. Registrant Registrant Street: Xiamen
Reg. Registrant Registrant City: Xiamen
Reg. Registrant Registrant Province/state: FUJIAN
Reg. Registrant Registrant Postal Code: 361000
Registrant Registrant Country: CN
Registrant Registrant Phone: +57.59222577844
Registrant Registrant Phone EXT:
Registrant Registrant Fax: +57.59222577844
Registrant Registrant Fax EXT:
Registrant Registrant Email: whois-protect@hotmail.com

tzyywwz@qq.com

Domain name: setinfo.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: todrl79241
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: tzyywwz@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



Otros Registrantes de Dominios

bailiwick	paltruisse.gdn.
count	2
first seen	2017-10-19 20:20:12
last seen	2017-10-19 20:20:12 -0000
paltruisse.gdn.	A 47.254.18.28

seoboss@seznam.cz

bailiwick	blokochain.info.
count	2
first seen	2017-10-21 22:59:43
last seen	2017-10-21 22:59:43 -0000
www.blokochain.info.	A 47.254.18.28

whois-protect@hotmail.com

bailiwick	indian-trk711.com.
count	7
first seen	2017-10-25 09:55:55
last seen	2017-10-30 08:56:16 -0000
indian-trk711.com.	A 47.254.18.28

galicole@mail.com

Returned 28 RRs in 0.03 seconds.

eznam.cz

	A	47.254.18.28
	A	47.254.18.28
	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
		8.28
		8.28
		8.28

otect@hotmail.com

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
		no.com.
	A	47.254.18.28
	A	questhis.com.
	A	47.254.18.28
gradual.paltruisse.gdn.	A	47.254.18.28
kursaal.paltruisse.gdn.	A	47.254.18.28
etherified.paltruisse.gdn.	A	47.254.18.28
subimposed.paltruisse.gdn.	A	47.254.18.28
exteriorising.paltruisse.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

mail.com



Otros Registrantes de Dominios

bailiwick **daccat.at.**

count 6

first seen 2017-10-24 11:51:09

last seen 2017-10-24 11:51:09 -0000

daccat.at. A 47.254.18.28

xlbs@tvchd.com

bailiwick **termsfounddocumeano.com.**

count 109

first seen 2017-10-25 14:39:19

last seen 2017-10-25 23:49:48

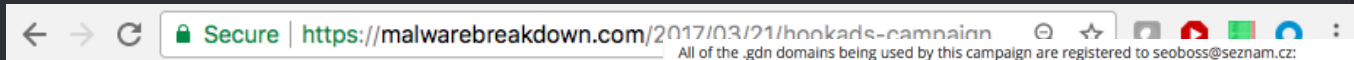
termsfounddocumeano.com. A 47.90.202.68

jiamcho1955@dnsname.info

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
paltruisse.gdn.	A	47.254.18.28
gradual.paltruisse.gdn.	A	47.254.18.28
kursaal.paltruisse.gdn.	A	47.254.18.28
etherified.paltruisse.gdn.	A	47.254.18.28
subimposed.paltruisse.gdn.	A	47.254.18.28
exteriorising.paltruisse.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



All of the .gdn domains being used by this campaign are registered to seoboss@seznam.cz:

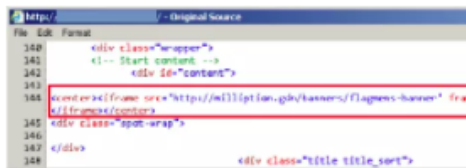
Exploit Kit

HookAds Campaign Leads to RIG EK

March 21, 2017 malwarebreakdown 0 Comments HookAds, IOCs, Rig

The HookAds campaign was first discovered by researchers at Malwarebytes malware. In this case the user would be browsing a legitimate website, often a malvertising chain.

On the decoy adult sites there is a malicious iframe that points to a fake ad s



Decoy site contains iframe pointing to an

The domain millip10n.gdn resolves to 62.75.195.128. The campaign has been

Domains	First Seen
millip10n.gdn	3/13/2017
decipio.gdn	3/13/2017
africal.gdn	3/17/2017

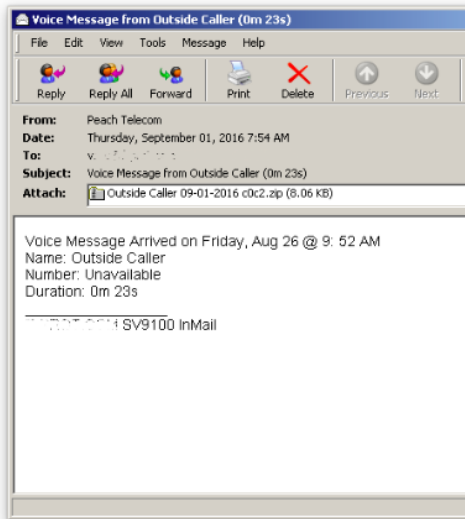
Domain	Registrant Email	Registered
decipio.gdn	seoboss@seznam.cz	3/5/2017
restribe.gdn	seoboss@seznam.cz	3/5/2017
procody.gdn	seoboss@seznam.cz	3/5/2017
vessed.gdn	seoboss@seznam.cz	3/5/2017
africal.gdn	seoboss@seznam.cz	3/5/2017
coolinin.gdn	seoboss@seznam.cz	3/5/2017
millip10n.gdn	seoboss@seznam.cz	3/5/2017
resourdish.gdn	seoboss@seznam.cz	3/5/2017
werned.gdn	seoboss@seznam.cz	3/1/2017
psittan.gdn	seoboss@seznam.cz	3/1/2017
westponent.gdn	seoboss@seznam.cz	3/1/2017
confidely.gdn	seoboss@seznam.cz	3/1/2017
elecommon.gdn	seoboss@seznam.cz	3/1/2017
cominents.gdn	seoboss@seznam.cz	3/1/2017
slightfall.gdn	seoboss@seznam.cz	2/27/2017
wallther.gdn	seoboss@seznam.cz	2/27/2017
dravitalia.gdn	seoboss@seznam.cz	2/27/2017
paltruise.gdn	seoboss@seznam.cz	2/27/2017
irritorian.gdn	seoboss@seznam.cz	2/27/2017
unexperic.gdn	seoboss@seznam.cz	2/27/2017



Secure | <https://www.cyren.com/blog/articles/locky-adds-new>

Locky Adds New File Format and Attacks UK

Cyren caught a new Locky email spam campaign today which is delivering the Locky downloader script component as an HTML file, specifically HTA files. The emails are disguised as voice messages from Peach Telecom, which suggests that the campaign is targeting UK users.



While reviewing the domains of the download URL's, we found one particular domain, which was recently created and was registered using the email galicole@mail.com.

Whols Info

```
Domain Name: HOTCARSHHHS6632.COM
Registry Domain ID: 2056315296_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2016-08-31T09:34:43Z
Creation Date: 2016-08-31T09:34:42Z
Registrar Registration Expiration Date: 2017-08-31T09:34:42Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303 Domain Status: clientTransferProhibited
Registrant Email: galicole@mail.com
```

This registrant email has a history of registering domains for the binary payload of Locky Ransomware in August:

```
rejoincomp2.in
tryfriedpot.co.in
```



Metadata

File name:	noi.exe
File type:	PE32 executable (GUI) Intel 80386,...
File size:	577536
Analysis date:	2017-10-26 09:10:15
MD5:	0aad7d043dc9089d96edf01ba3072
SHA1:	55b6f60e24db768b43b2c78d7fc02
SHA256:	75636cf72cf1f9b82ad40e14a14db4
SHA512:	N/A
SSDEEP:	N/A
IMPHASH:	N/A
Authentihash:	N/A
Related resources	VirusTotal Hybrid-Analysis Threat

APTNotes

No reports found.

Domains

Domain

[ocsp.int-x3.letsencrypt.org](#)
[isrg.trustid.ocsp.identrust.com](#)
[daccat.at](#)



50 / 68

50 engines detected this file

SHA-256 75636cf72cf1f9b82ad40e14a14db4a8746aa6ceba9b9dd96e4e36ead2033c0b
File name 0aad7d043dc9089d96edf01ba30727e0.viobj
File size 564 KB
Last analysis 2017-11-30 22:58:40 UTC

Detection

Details

Relations

Behavior

Community 1

Ad-Aware



Trojan.GenericKD.12518269

AegisLab



Troj.W32.Gen.m5ir

AhnLab-V3



Win-Trojan/Sagecrypt.Gen

ALYac



Trojan.GenericKD.12518269

Arcabit



Trojan.Generic.DBF037D

Avast



Win32:Malware-gen

AVG



Win32:Malware-gen

Avira



TR/Crypt.ZPACK.tqnww

AVware



Trojan.Win32.Generic!BT

Baidu



Win32.Trojan.WisdomEyes.16070401.9500.9960

BitDefender



Trojan.GenericKD.12518269

CAT-QuickHeal



Trojan.Yakes

ClamAV



Win.Malware.Agent-6357365-0

jiamcho1955@dnsname.info



reverse.it



Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain

Address

popoiuiuntnt.net

78.158.214.94



Fingerprint

Network Behavior

Injects into remote processes
Modifies auto-execute functionality by setting/creating
Writes data to a remote process
Reads the active computer name
Scans for artifacts that may help identify the target
Contacts 1 domain and 1 host. View the [network sect](#)

Associated Artifacts for [popoiuiuntnt.net](#)

Whois Field	Value
Address	Gong Yu Lu, 1061 - 900
City	Suqian
Country	CN
Creation Date	Wed, 19 Jul 2017 16:08:31 GMT
DNSSEC	unsigned
Domain Name	POPOIUIUNTNT.NET
Email	abuse@internet.bs
Email	jiamcho1955@dnsname.info
Expiration Date	Thu, 19 Jul 2018 16:08:31 GMT
name	Jian Cho
Name Server	NS2.BIOUGERTERT.AT
Organization	NA
Registrar	Internet Domain Service BS Corp.
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status	clientTransferProhibited - http://www.icann.org/epp#clientTransferProhibited
Last Update	Tue, 01 Aug 2017 09:20:46 GMT
Whois Server	whois.internet.bs
Zip Code	23635

TALOS

www.talosintelligence.com

blog.talosintel.com

[@talossecurity](https://twitter.com/talossecurity)

jaeson@cisco.com

[@jaesonschultz](https://twitter.com/jaesonschultz)

