Malspam is Different Spam

Martijn Grooten, Virus Bulletin

botconf
The botnet fighting conference 2019
Workshops December 3rd, 2019
7th edition
Bordeaux
FRANCE
7th edition
Conference from the 4th to the 6th of December, 2019

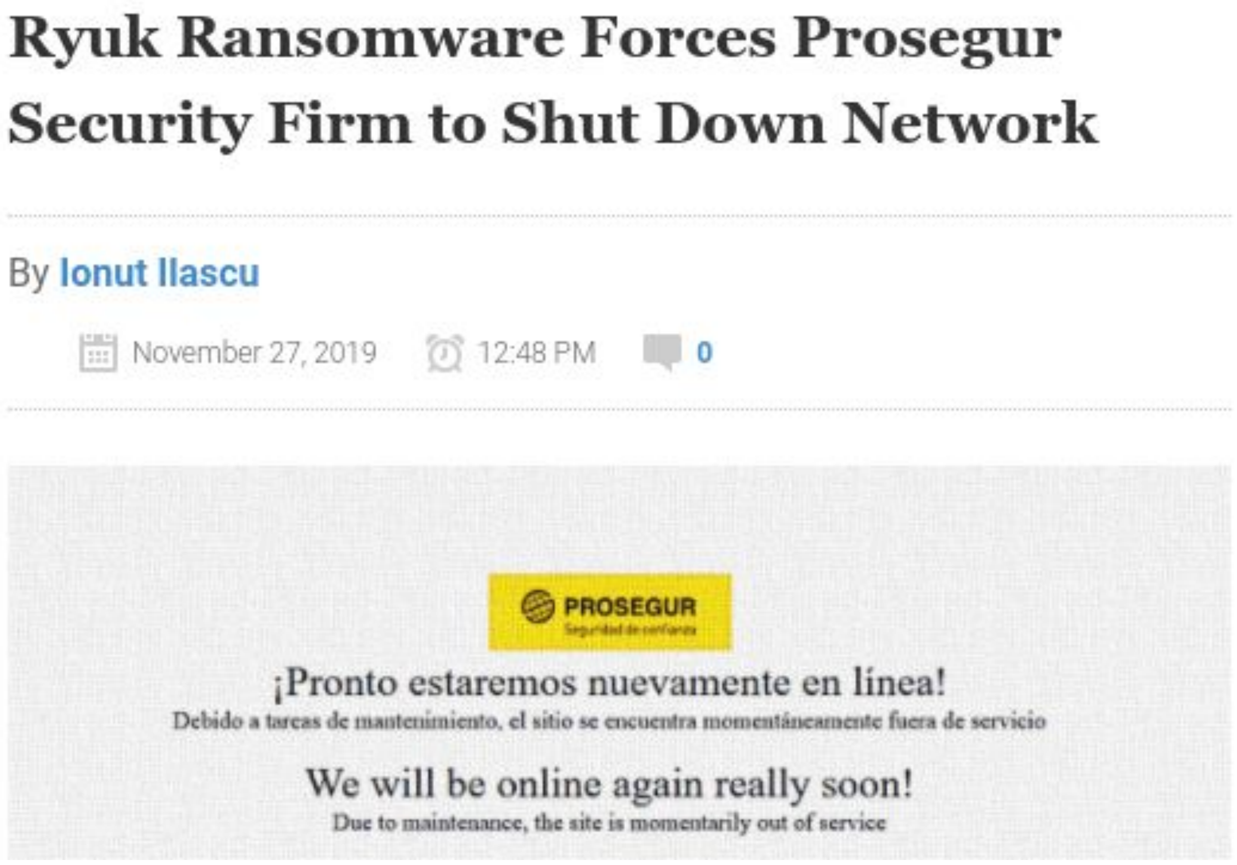
martijn_grooten

TLP:WHITE

virus BULLETIN

SPAM
- LIMITED EDITION -
PUMPKIN SPICE

pfizer
pfizer



Ryuk Ransomware Forces Prosegur Security Firm to Shut Down Network

By Ionut Ilascu

November 27, 2019 12:48 PM 0

PROSEGUR
Seguridad de confianza

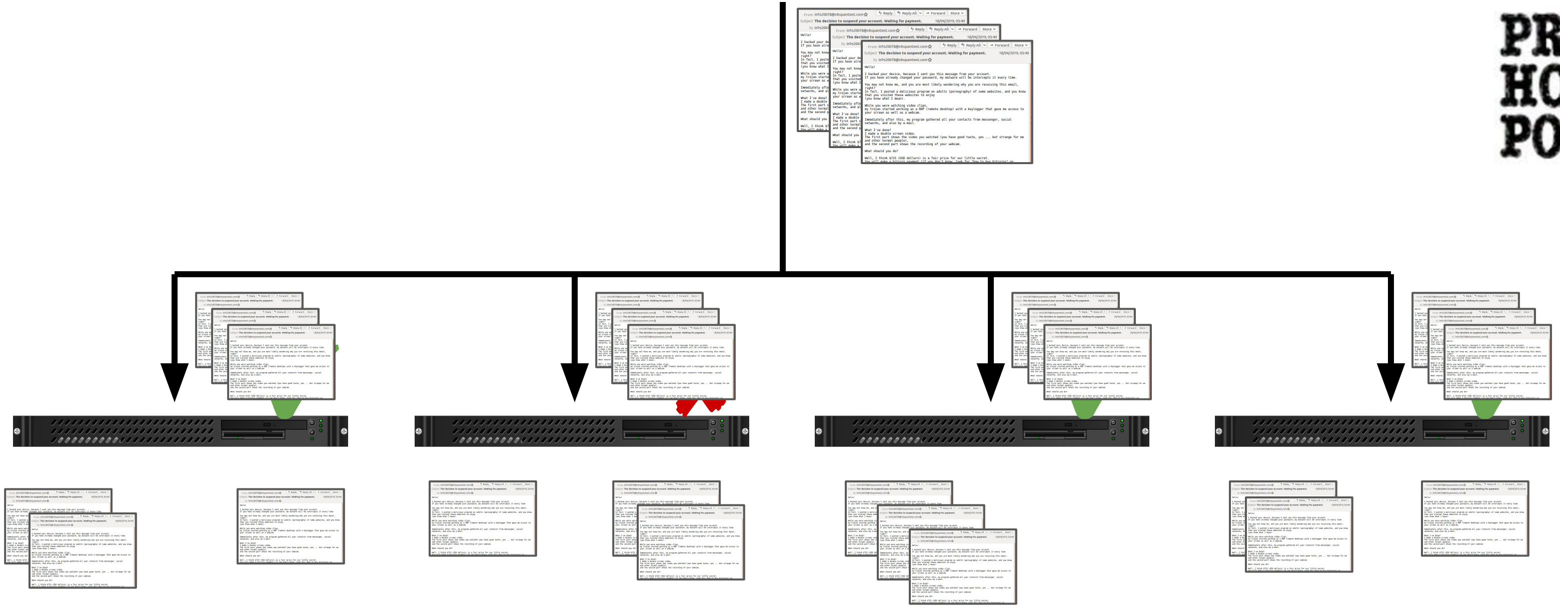
¡Pronto estaremos nuevamente en línea!

Debido a tareas de mantenimiento, el sitio se encuentra momentáneamente fuera de servicio

We will be online again really soon!

Due to maintenance, the site is momentarily out of service

We test email security *products*



From info20078@vbspamtest.com
Subject **The decision to suspend your account. Waiting for payment.** 18/04/2019, 03:40
To info20078@vbspamtest.com

```
Hello!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email,
right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know
that you visited these websites to enjoy
(you know what I mean).

While you were watching video clips,
my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to
your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social
networks, and also by e-mail.

What I've done?
I made a double screen video.
The first part shows the video you watched (you have good taste, yes ... but strange for me
and other normal people),
and the second part shows the recording of your webcam.

What should you do?

Well, I think $715 (USD dollars) is a fair price for our little secret.
```

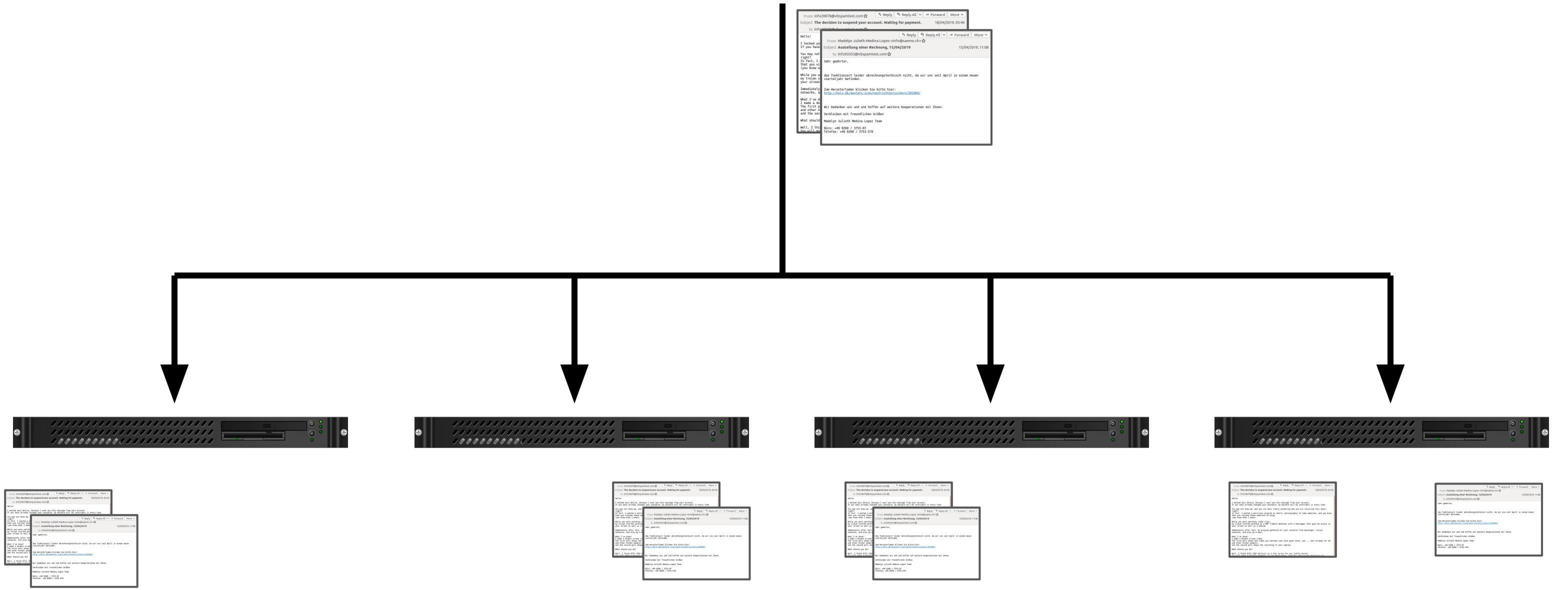
abusix

PROJECT HONEY POT tm

virus BULLETIN

martijn_grooten

We test *email* security products



```
From info20078@vbspamtest.com
Subject The decision to suspend your account. Waiting for payment.    18/04/2019, 03:40
To info

Hello!

I hacked yo
If you have

You may not
right?
In fact, I
that you vi
(you know w

While you w
my trojan s
your screen

Immediately
networks, a

What I've d
I made a do
The first p
and other n
and the sec

What should

Well, I thi
You will ma
```

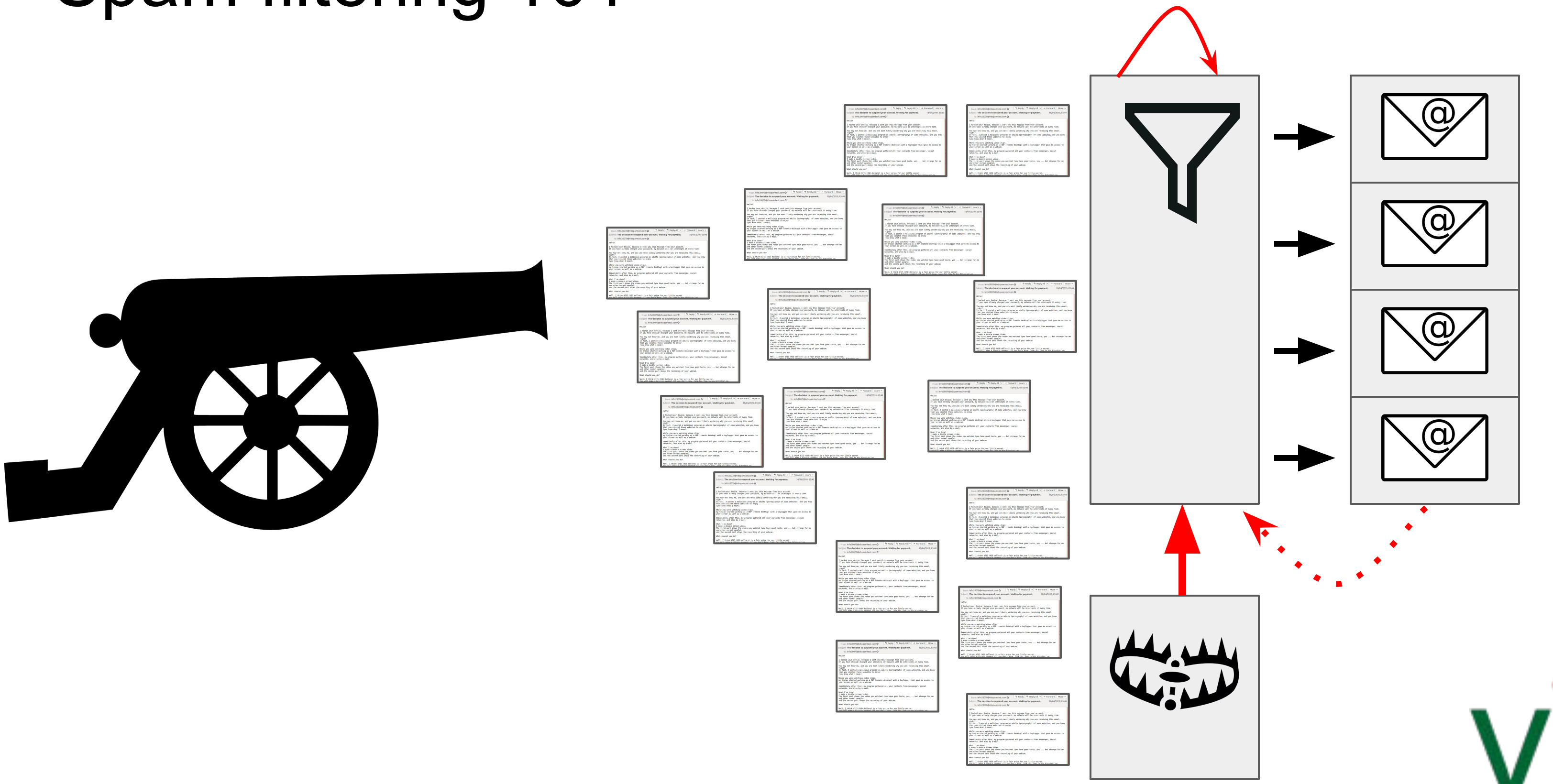
```
From Madelyn Julieth Medina Lopez <info@saemo.ch>
Subject Austellung einer Rechnung, 15/04/2019    15/04/2019, 11:08
To info03353@vbspamtest.com

Sehr geehrter,



das funktioniert leider abrechnungstechnisch nicht, da wir uns seit April in einem neuen
vierteljahr befinden.


Zum Herunterladen klicken Sie bitte hier:
http://holz.dk/awstats-icon/nachrichten/sichern/201904/



Wir bedanken uns und und hoffen auf weitere Kooperationen mit Ihnen.

Verbleiben mit freundlichen Grüßen

Madelyn Julieth Medina Lopez Team

Büro: +49 0260 / 3753-07
Telefax: +49 0260 / 3753-578
```

martijn_grooten

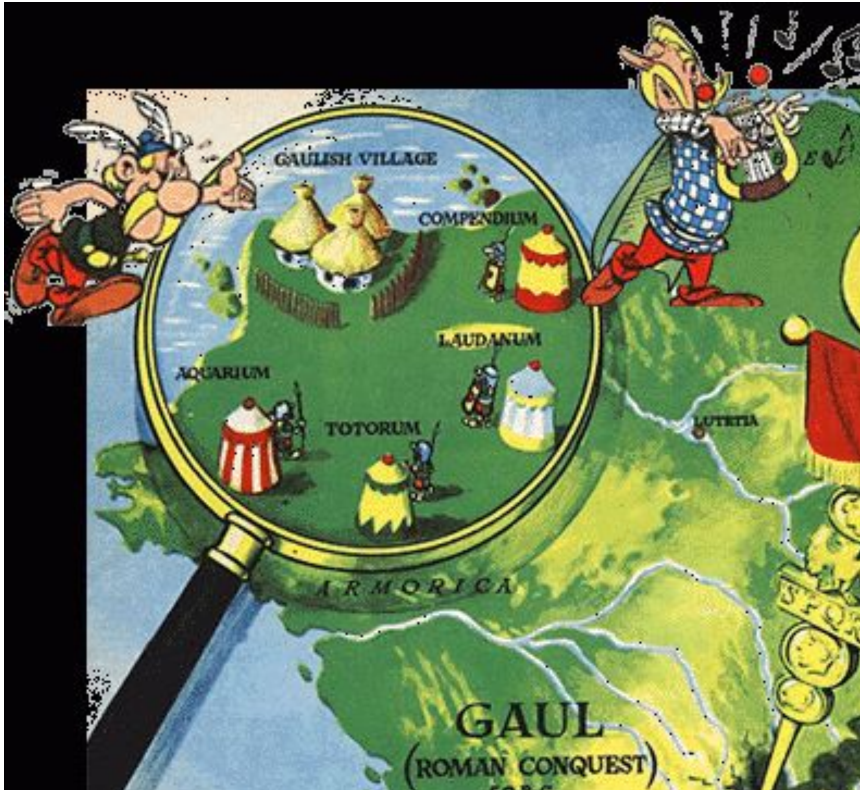
Spam filtering 101

- IP, domain blacklists
- Sender verification (SPF, DKIM, DMARC etc.)
- Content filtering
- Link/attachment scanning

Spam filtering 101

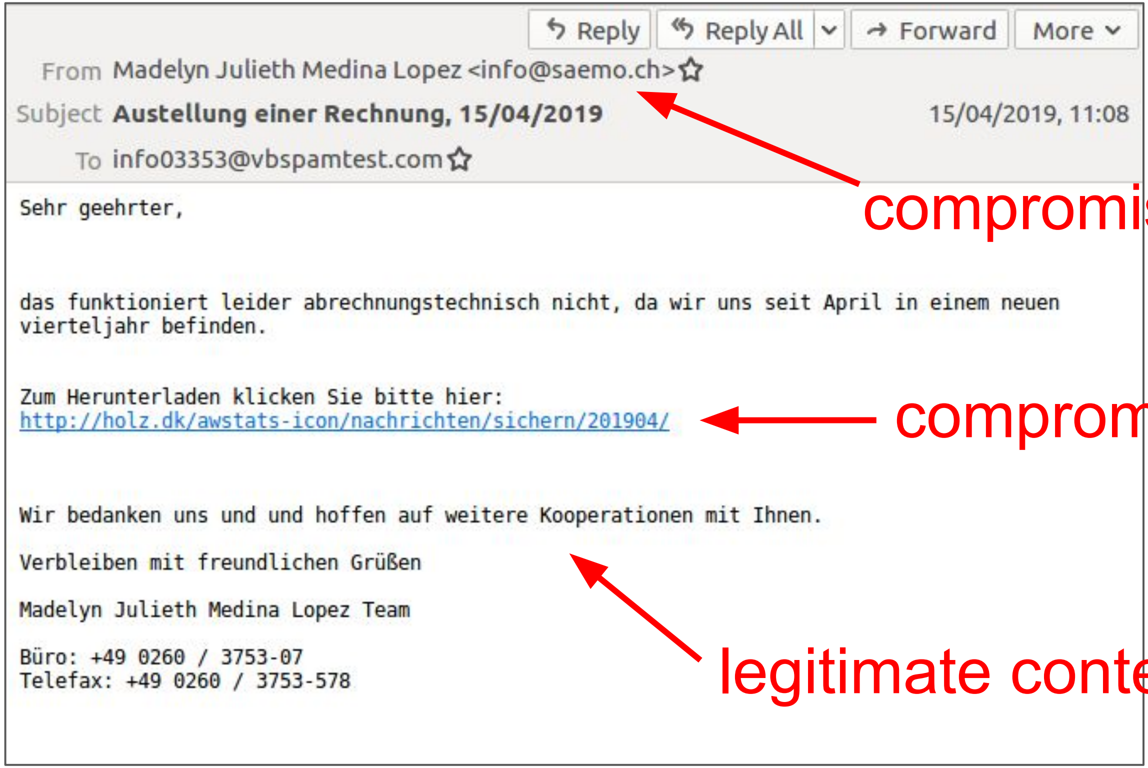


spam scales badly



GAULISH VILLAGE
COMPENDIUM
LAUDANUM
AQUARIUM
TOTORUM
LUTETIA
ARMORICA
GAUL
(ROMAN CONQUEST)

Better spam



From Madelyn Julieth Medina Lopez <info@saemo.ch>

Subject **Austellung einer Rechnung, 15/04/2019** 15/04/2019, 11:08

To info03353@vbspamtest.com

Sehr geehrter,

das funktioniert leider abrechnungstechnisch nicht, da wir uns seit April in einem neuen vierteljahr befinden.

Zum Herunterladen klicken Sie bitte hier:
http://holz.dk/awstats-icon/nachrichten/sichern/201904/

Wir bedanken uns und und hoffen auf weitere Kooperationen mit Ihnen.

Verbleiben mit freundlichen Grüßen

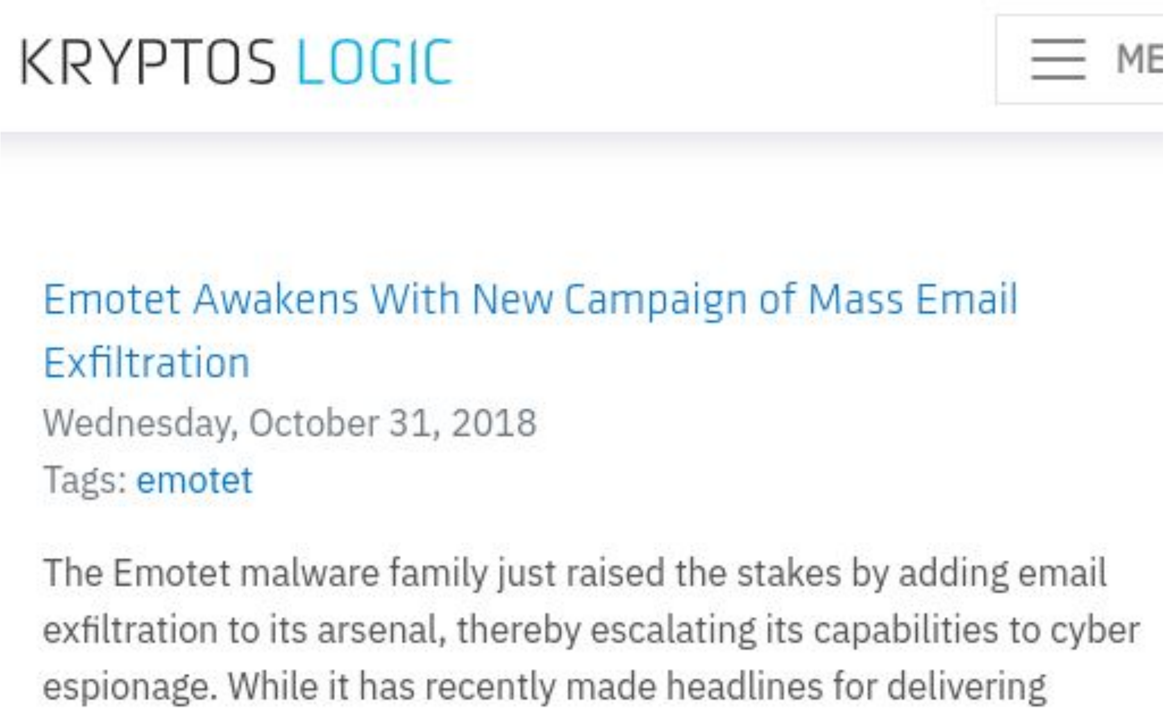
Madelyn Julieth Medina Lopez Team

Büro: +49 0260 / 3753-07
Telefax: +49 0260 / 3753-578

compromised mail server

compromised web server

legitimate content



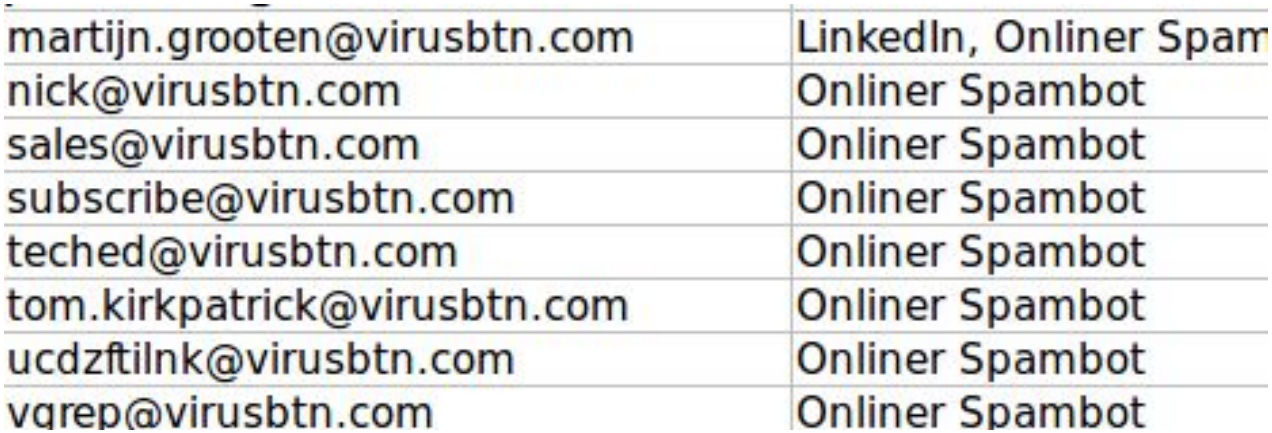
Emotet Awakens With New Campaign of Mass Email Exfiltration

Wednesday, October 31, 2018

Tags: emotet

The Emotet malware family just raised the stakes by adding email exfiltration to its arsenal, thereby escalating its capabilities to cyber espionage. While it has recently made headlines for delivering

Harvesting email addresses 1.0



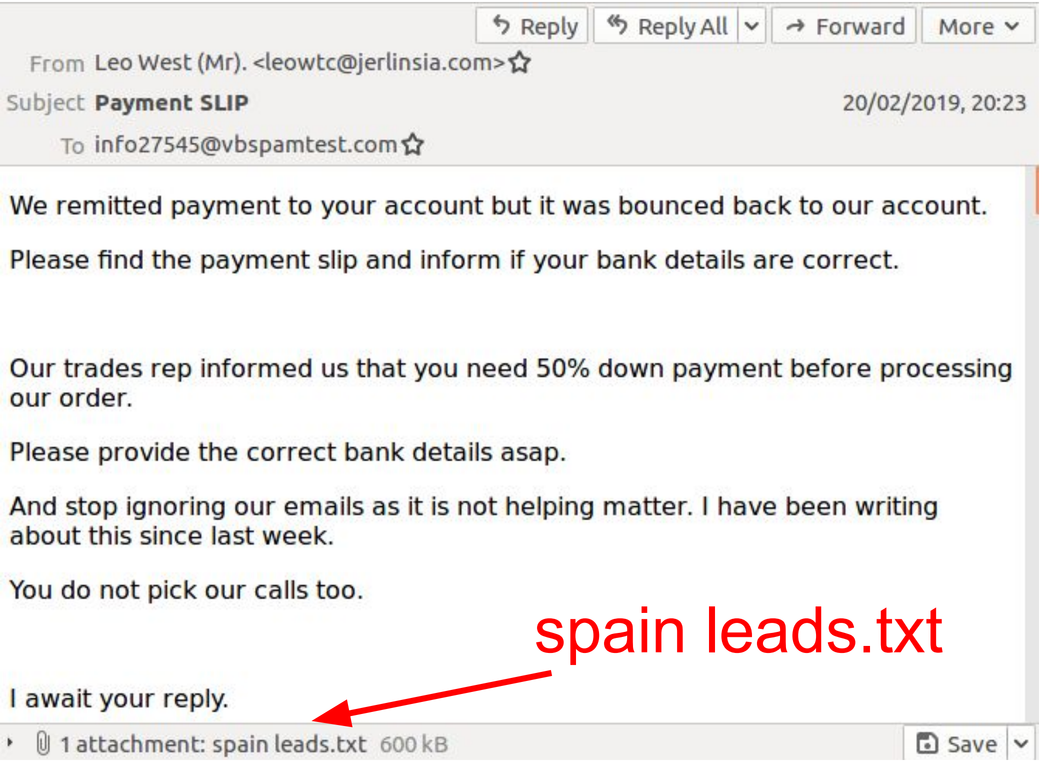
martijn.grooten@virusbtn.com	LinkedIn, Onliner Spam
nick@virusbtn.com	Onliner Spambot
sales@virusbtn.com	Onliner Spambot
subscribe@virusbtn.com	Onliner Spambot
teched@virusbtn.com	Onliner Spambot
tom.kirkpatrick@virusbtn.com	Onliner Spambot
ucdzftilnk@virusbtn.com	Onliner Spambot
vgrep@virusbtn.com	Onliner Spambot

me!

left in 2006...

?????

Harvesting email addresses 2.0



From Leo West (Mr). <leowtc@jerlinsia.com>

Subject **Payment SLIP** 20/02/2019, 20:23

To info27545@vbspamtest.com

We remitted payment to your account but it was bounced back to our account.

Please find the payment slip and inform if your bank details are correct.

Our trades rep informed us that you need 50% down payment before processing our order.

Please provide the correct bank details asap.

And stop ignoring our emails as it is not helping matter. I have been writing about this since last week.

You do not pick our calls too.

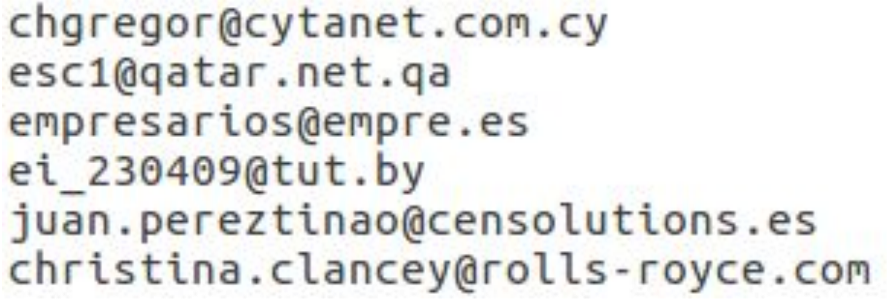
I await your reply.

1 attachment: spain leads.txt 600 kB

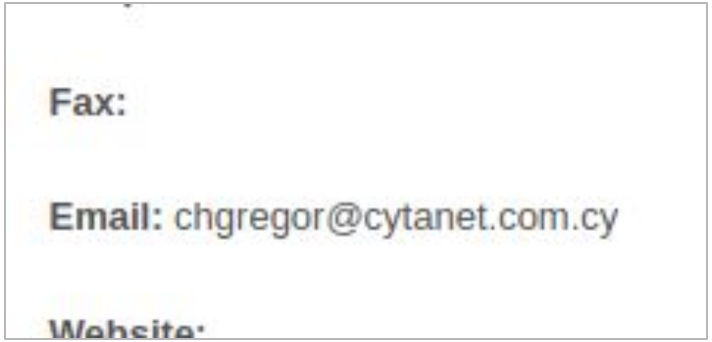
spain leads.txt

martijn_grooten

Harvesting email addresses 2.0



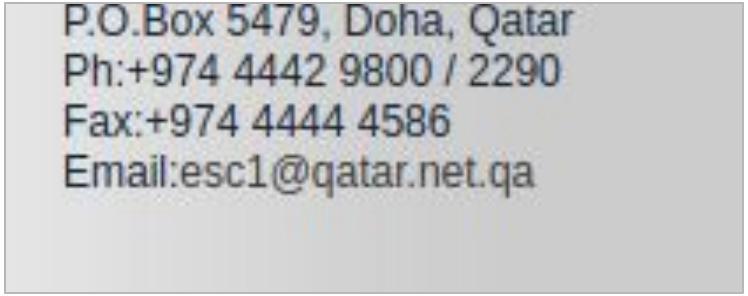
```
chgregor@cytanet.com.cy
esc1@qatar.net.qa
empresarios@empre.es
ei_230409@tut.by
juan.pereztinao@censolutions.es
christina.clancey@rolls-royce.com
```



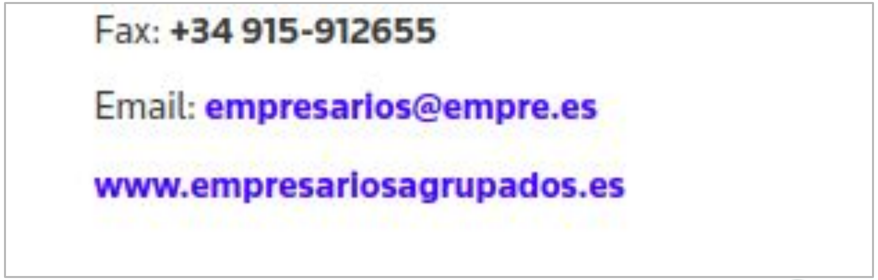
Fax:

Email: chgregor@cytanet.com.cy

Website:



P.O.Box 5479, Doha, Qatar
Ph:+974 4442 9800 / 2290
Fax:+974 4444 4586
Email:esc1@qatar.net.qa



Fax: **+34 915-912655**

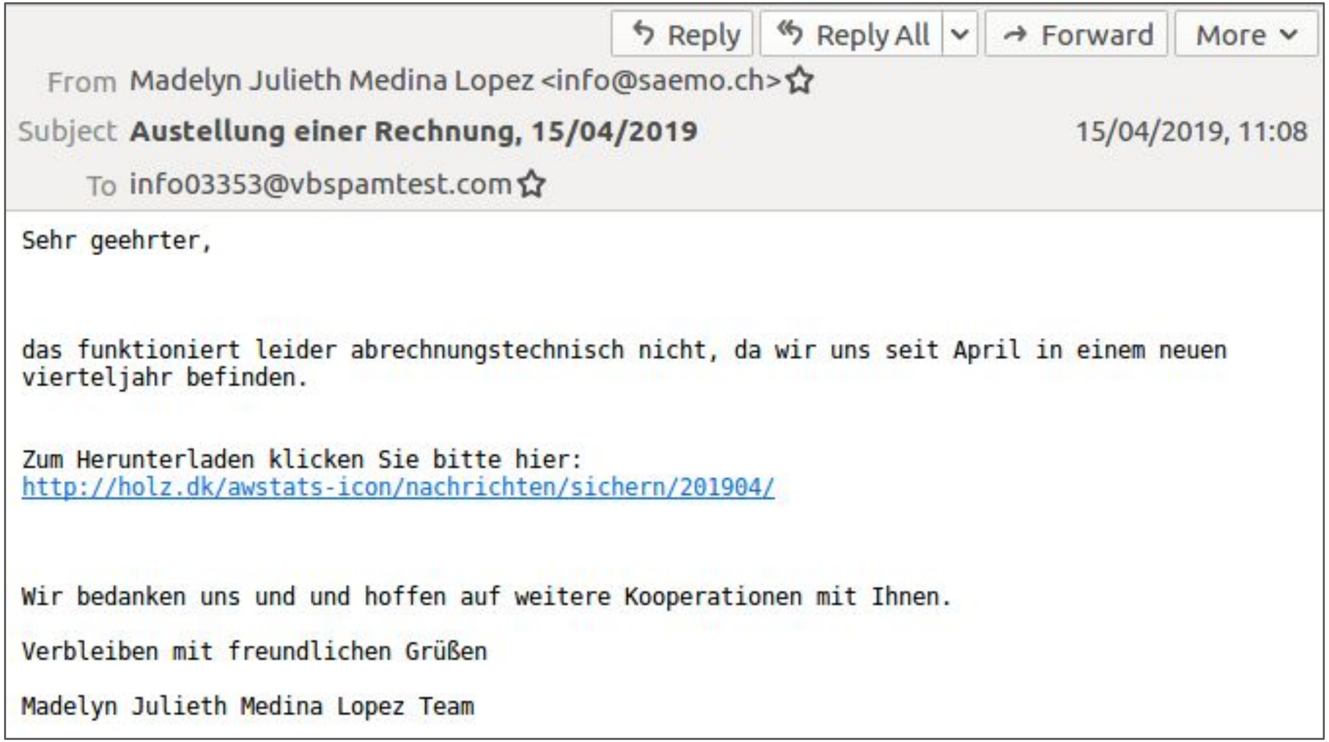
Email: **empresarios@empre.es**

www.empresariosagrupados.es

Things we have learned

- Most of today's malspam (malware, phishing) focuses on quality rather than on quality
- Block rates vary a lot but easily can be 90% or lower, compared to ~99.9% of more traditional spam
- Emails with malicious links tend to have lower block rates than emails with attachments

A tale of two emails



From Madelyn Julieth Medina Lopez <info@saemo.ch>

Subject **Austellung einer Rechnung, 15/04/2019** 15/04/2019, 11:08

To info03353@vbspamtest.com

Sehr geehrter,

das funktioniert leider abrechnungstechnisch nicht, da wir uns seit April in einem neuen vierteljahr befinden.

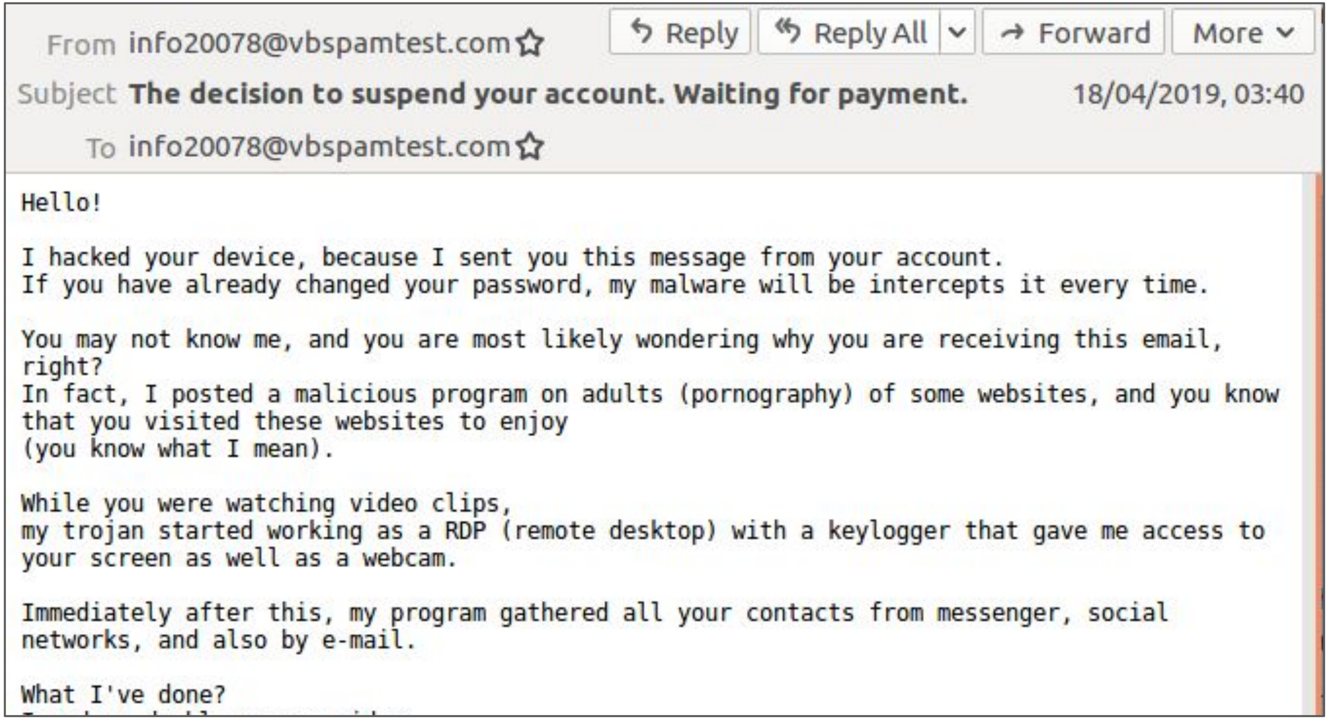
Zum Herunterladen klicken Sie bitte hier:
http://holz.dk/awstats-icon/nachrichten/sichern/201904/

Wir bedanken uns und und hoffen auf weitere Kooperationen mit Ihnen.

Verbleiben mit freundlichen Grüßen

Madelyn Julieth Medina Lopez Team

A tale of two emails



From info20078@vbspamtest.com

Subject **The decision to suspend your account. Waiting for payment.** 18/04/2019, 03:40

To info20078@vbspamtest.com

Hello!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email,
right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know
that you visited these websites to enjoy
(you know what I mean).

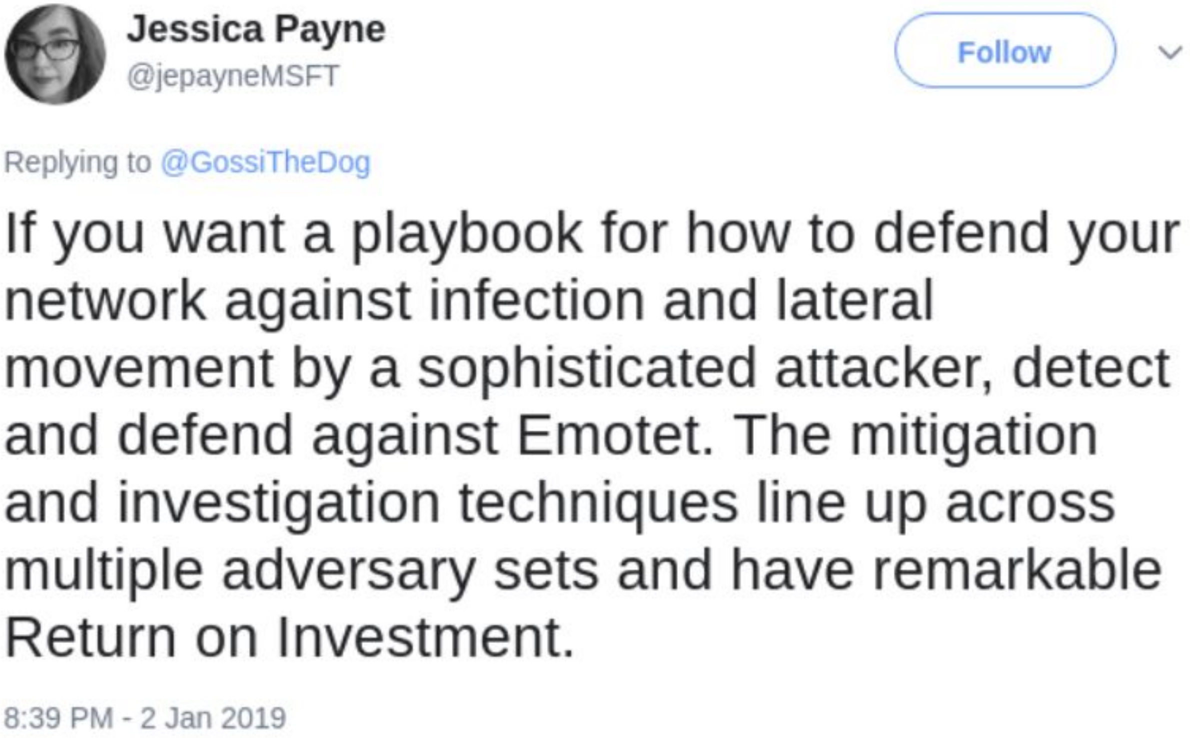
While you were watching video clips,
my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to
your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social
networks, and also by e-mail.

What I've done?

Advice for defenders

- Your email security product is not perfect
- Your threat intel feed is going to be incomplete
- Don’t focus too much on APTs



Jessica Payne
@jepayneMSFT

Replying to @GossiTheDog

If you want a playbook for how to defend your network against infection and lateral movement by a sophisticated attacker, detect and defend against Emotet. The mitigation and investigation techniques line up across multiple adversary sets and have remarkable Return on Investment.

8:39 PM - 2 Jan 2019

Advice for researchers

You want (mal)spam fast, accurate and of high quality.

Pick any two:

- Fast + accurate: ‘old’ spam traps
- Accurate + high quality: malware repositories
- Fast + high quality: ‘mixed’ email feeds

Conclusion

spam scales badly, but malspam does not need to scale

Thank you for listening

Questions? Ask, or martijn.grooten@virusbulletin.com

(or martijn@lapsedordinary.net)

(or Twitter, LinkedIn, WhatsApp, Signal, ...)

🐦 martijn_grooten

virus
BULLETIN