CERT Tonga

Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

TLP: White[1]

Security Alert: Widespread Emotet Malware Campaign sent to users in Tonga

Dear All/ Constituents,

CERT Tonga has observed a spam campaign spreading Emotet infection across organizations in Tonga. Emotet provides an attacker with a foothold in a network from which additional attacks can be performed, often leading to the deployment of ransomware.

How it works

The campaign observed is most commonly spread via malicious emails containing Microsoft Office attachments, usually Word (.doc, .docx) documents and the email appear to be coming from a source in Tonga (sometimes it seems like to be from a familiar contact). However, the email has been spoofed in order for the target to trust the email and attempt to open the attachment. Furthermore, the bottom of the email tricks the receiver into thinking that the email is not malicious by stating that it has been scanned with antivirus. Emotet can also be spread via embedded URLs in malicious emails.

Once opened, the macro then proceeds to execute a Power Shell script which automatically downloads and run the Emotet Malware often leading to additional attacks including Ransomware. In some cases it moves laterally within a network using exploits to deploy additional malware to the infected network.

What to do

Alert staff

Consider sending out an organization-wide alert to raise awareness of the dangers associated with opening attachments on unusual emails and in particular this campaign.

Update antivirus

Keep antivirus on your computer and servers up-to-date

Patch your computers

Apply appropriate security patches on computers to avoid infection by further exploits

Block macros

Where possible, it is highly recommends blocking macros from the internet, and only allowing the execution of vetted and white listed macros.

In most cases, Emotet's initial infection of a network is via an embedded macro in a Microsoft Office document. Disabling all unknown macros can significantly reduce your network's risk-surface.

[1] CERT Tonga adopts the Traffic Light Protocol

Maintain offline backups

Consider maintaining isolated offline backups of your network to allow recovery in the event of widespread infection, or the deployment of ransomware.

If a computer is infected or has opened the malicious link

If a user opened a the malicious attachment or an infection is believed to exist, it is recommended to update and run an antivirus scan on the system and take action based on the results to isolate the infected computer.

If multiple machines are infected:

Contact your ICT or System Administrators as soon as possible.

Identify, shutdown, and take the infected machines off the network.

Do not login to infected systems using domain or shared local admin accounts.

Consider temporarily taking the network offline to perform identification, prevent reinfections, and stop the spread of the malware.

Issue password reset for both local and domain credentials.

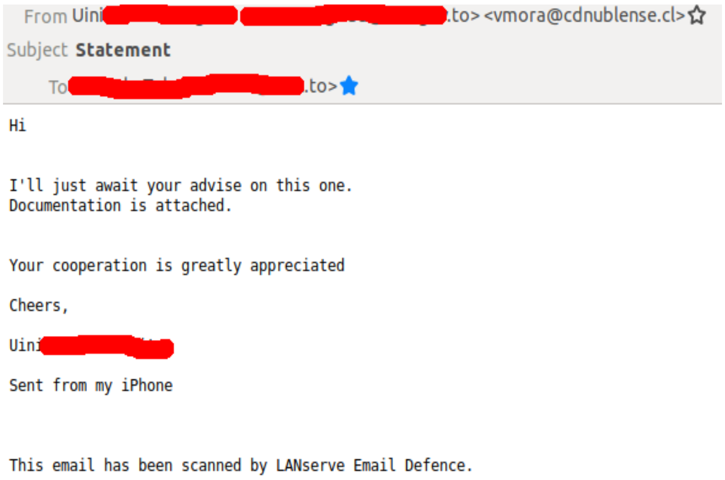
Reference

- https://www.us-cert.gov/ncas/alerts/TA18-201A
- https://www.cyber.gov.au/acsc/view-all-content/advisories/2019-131a-emotet-malware-campaign-recommended-actions

Email Samples

Shown below are examples of malicious spam pushing Emotet malware. It has an attached Word document with macros designed to install Emotet on a vulnerable host.

Sample 1



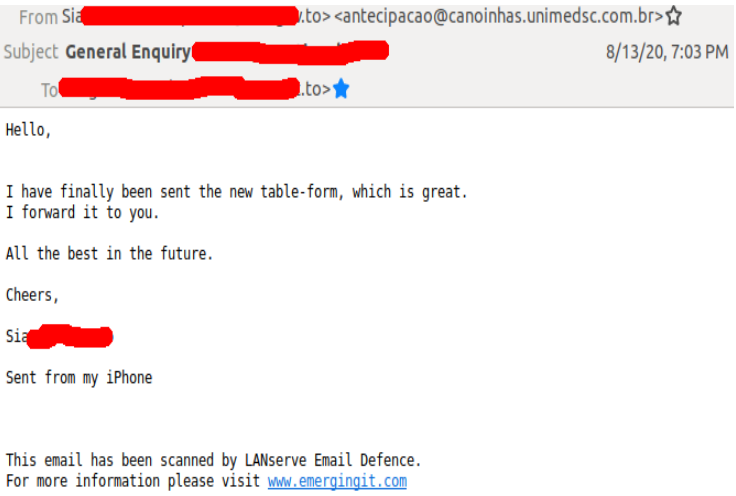
From Uini[redacted].to> <vmora@cdnublense.cl> ☆

Subject **Statement**

To [redacted].to> ★

```
Hi


I'll just await your advise on this one.
Documentation is attached.


Your cooperation is greatly appreciated

Cheers,

Uini[redacted]

Sent from my iPhone



This email has been scanned by LANserve Email Defence.
```

Sample 2



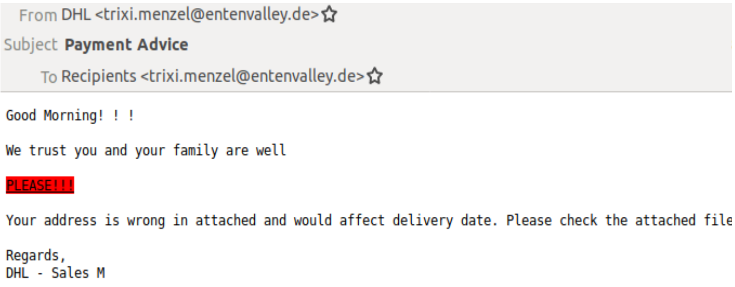
From Sia[redacted].to> <antecipacao@canoinhas.unimedsc.com.br> ☆

Subject **General Enquiry**[redacted] 8/13/20, 7:03 PM

To [redacted].to> ★

```
Hello,


I have finally been sent the new table-form, which is great.
I forward it to you.

All the best in the future.

Cheers,

Sia[redacted]

Sent from my iPhone


This email has been scanned by LANserve Email Defence.
For more information please visit www.emergingit.com
```

Sample 3



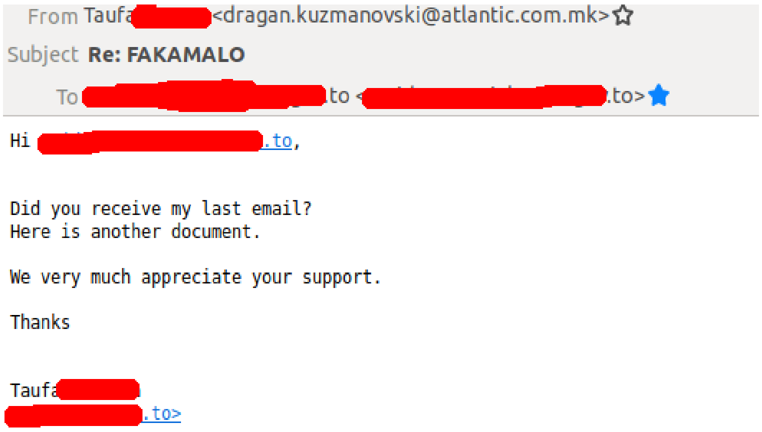
From DHL <trixi.menzel@entenvalley.de> ☆

Subject **Payment Advice**

To Recipients <trixi.menzel@entenvalley.de> ☆

```
Good Morning! ! !

We trust you and your family are well

PLEASE!!!

Your address is wrong in attached and would affect delivery date. Please check the attached file

Regards,
DHL - Sales M
```

Sample 4



From Taufa[redacted]<dragan.kuzmanovski@atlantic.com.mk> ☆

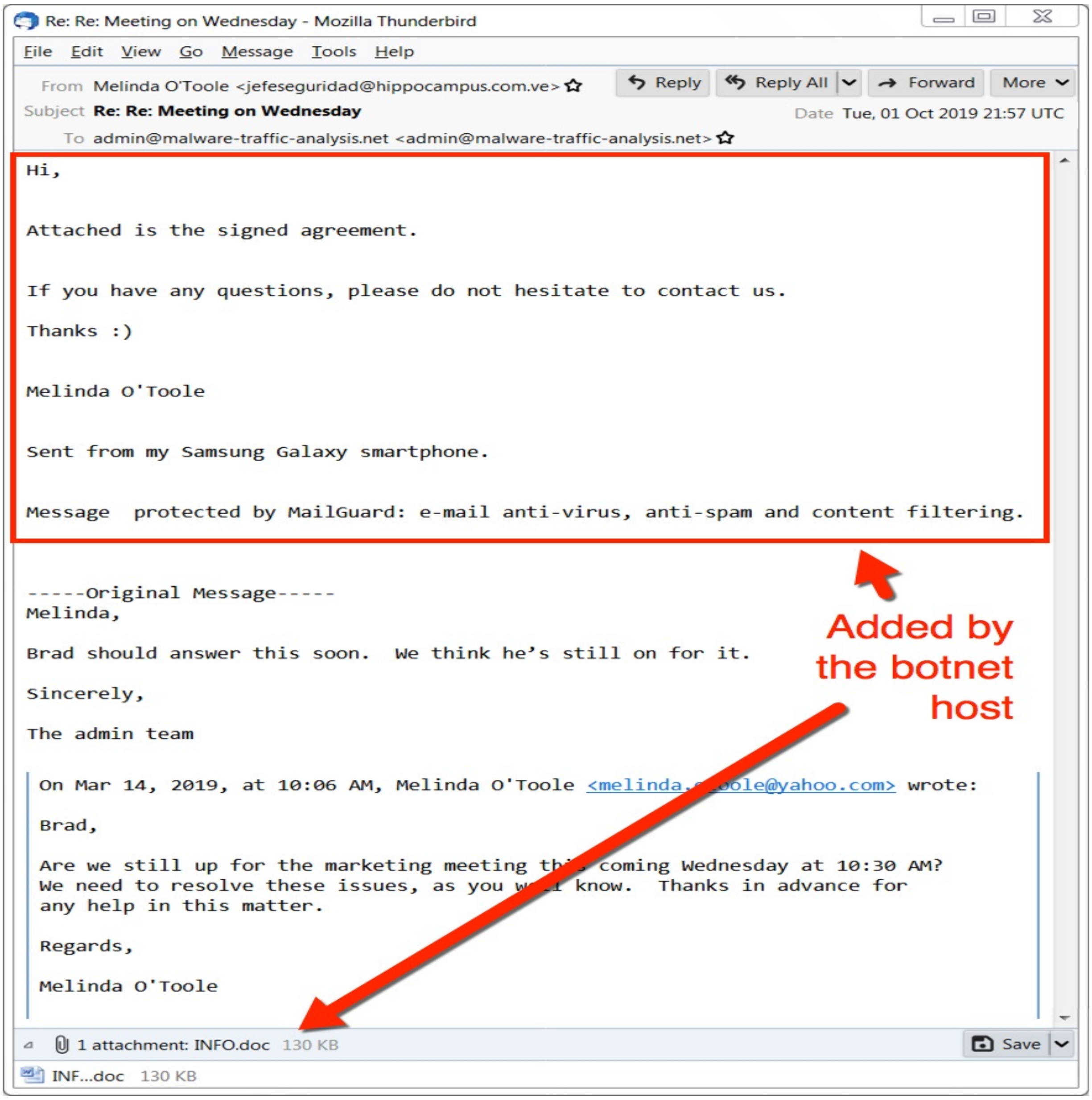
Subject **Re: FAKAMALO**

To [redacted].to <[redacted].to> ★

```
Hi [redacted].to,


Did you receive my last email?
Here is another document.

We very much appreciate your support.

Thanks


Taufa[redacted]
[redacted].to>
```

Sample 5

The sample below varies from samples 1 to 4. It is not an actual observation from here in Tonga but it is displayed here to show that in some cases it seems like it's replying to an ongoing email conversation thread but it adds on the malicious attachment..



Re: Re: Meeting on Wednesday - Mozilla Thunderbird
File Edit View Go Message Tools Help
Reply
Reply All
Forward
More
Save
Added by the botnet host

From Melinda O'Toole <jefeseguridad@hippocampus.com.ve>

Subject **Re: Re: Meeting on Wednesday**

Date Tue, 01 Oct 2019 21:57 UTC

To admin@malware-traffic-analysis.net <admin@malware-traffic-analysis.net>

```
Hi,

Attached is the signed agreement.

If you have any questions, please do not hesitate to contact us.

Thanks :)

Melinda O'Toole

Sent from my Samsung Galaxy smartphone.

Message  protected by MailGuard: e-mail anti-virus, anti-spam and content filtering.

-----Original Message-----
Melinda,

Brad should answer this soon.  We think he's still on for it.

Sincerely,

The admin team

 On Mar 14, 2019, at 10:06 AM, Melinda O'Toole <melinda.otoole@yahoo.com> wrote:

 Brad,

 Are we still up for the marketing meeting this coming Wednesday at 10:30 AM?
 We need to resolve these issues, as you well know.  Thanks in advance for
 any help in this matter.

 Regards,

 Melinda O'Toole
```

1 attachment: INFO.doc 130 KB

INF...doc 130 KB

Please for more information you can contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services