Tonga National Computer Emergency Response Team

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

TLP: White[1]

Security Alert: Widespread Emotet Malware Campaign appears to be targeting users in Tonga

Dear All/ Constitiuents,

CERT Tonga has observed a spam campaign spreading Emotet infection across organisations 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 PowerShell 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 organisation-wide alert to raise awareness of the dangers associated with opening attachments on unusual emails and in particular this campaign.

- **Update anitvirus**

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

1 CERT Tonga adopts the Traffic Light Protocol

- **Block macros**

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

- **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.

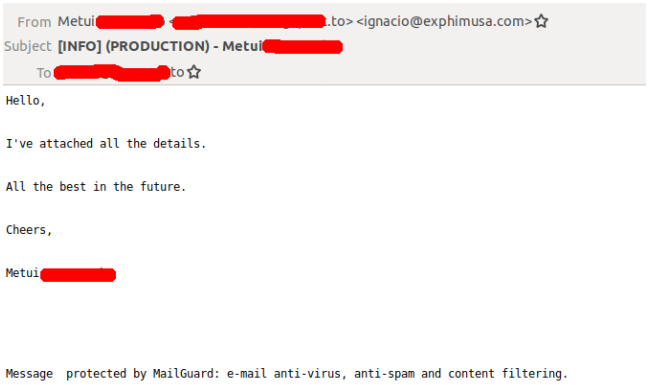
Reference

- ACSC- https://www.cyber.gov.au/threats/advisory-2019-131-emotet-malware-campaign
- https://www.us-cert.gov/ncas/alerts/TA18-201A

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 Metui[redacted].to> <ignacio@exphimusa.com>
Subject **[INFO] (PRODUCTION) - Metui[redacted]**
To [redacted].to

Hello,

I've attached all the details.

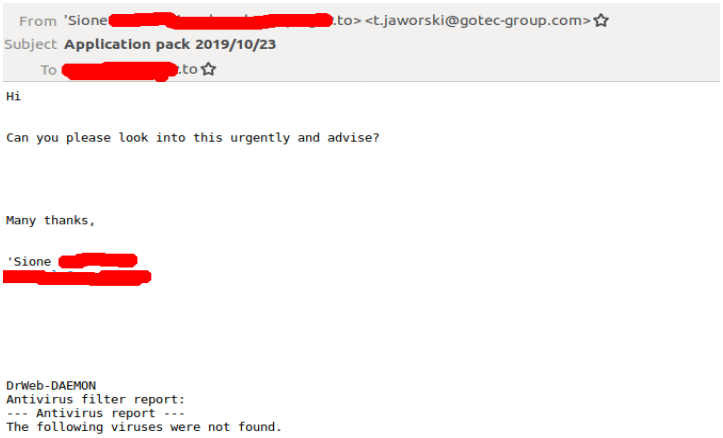
All the best in the future.

Cheers,

Metui[redacted]

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

Sample 2



From 'Sione[redacted].to> <t.jaworski@gotec-group.com>
Subject **Application pack 2019/10/23**
To [redacted].to

Hi

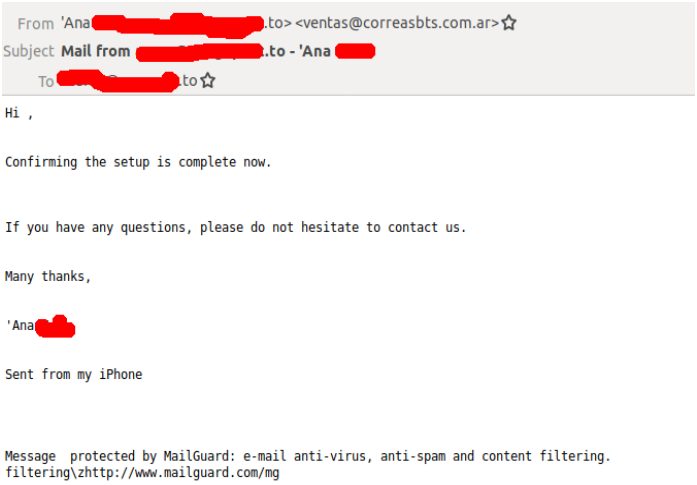
Can you please look into this urgently and advise?

Many thanks,

'Sione [redacted]

DrWeb-DAEMON
Antivirus filter report:
--- Antivirus report ---
The following viruses were not found.

Sample 3



From 'Ana[redacted].to> <ventas@correasbts.com.ar>
Subject **Mail from [redacted].to - 'Ana [redacted]**
To [redacted].to

Hi ,

Confirming the setup is complete now.

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

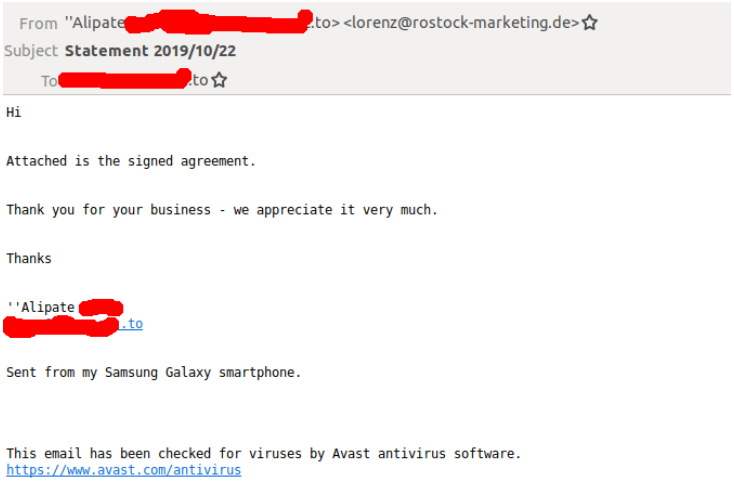
Many thanks,

'Ana[redacted]

Sent from my iPhone

Message protected by MailGuard: e-mail anti-virus, anti-spam and content filtering.
filtering\zhttp://www.mailguard.com/mg

Sample 4



From ''Alipate[redacted].to> <lorenz@rostock-marketing.de>
Subject **Statement 2019/10/22**
To [redacted].to

Hi

Attached is the signed agreement.

Thank you for your business - we appreciate it very much.

Thanks

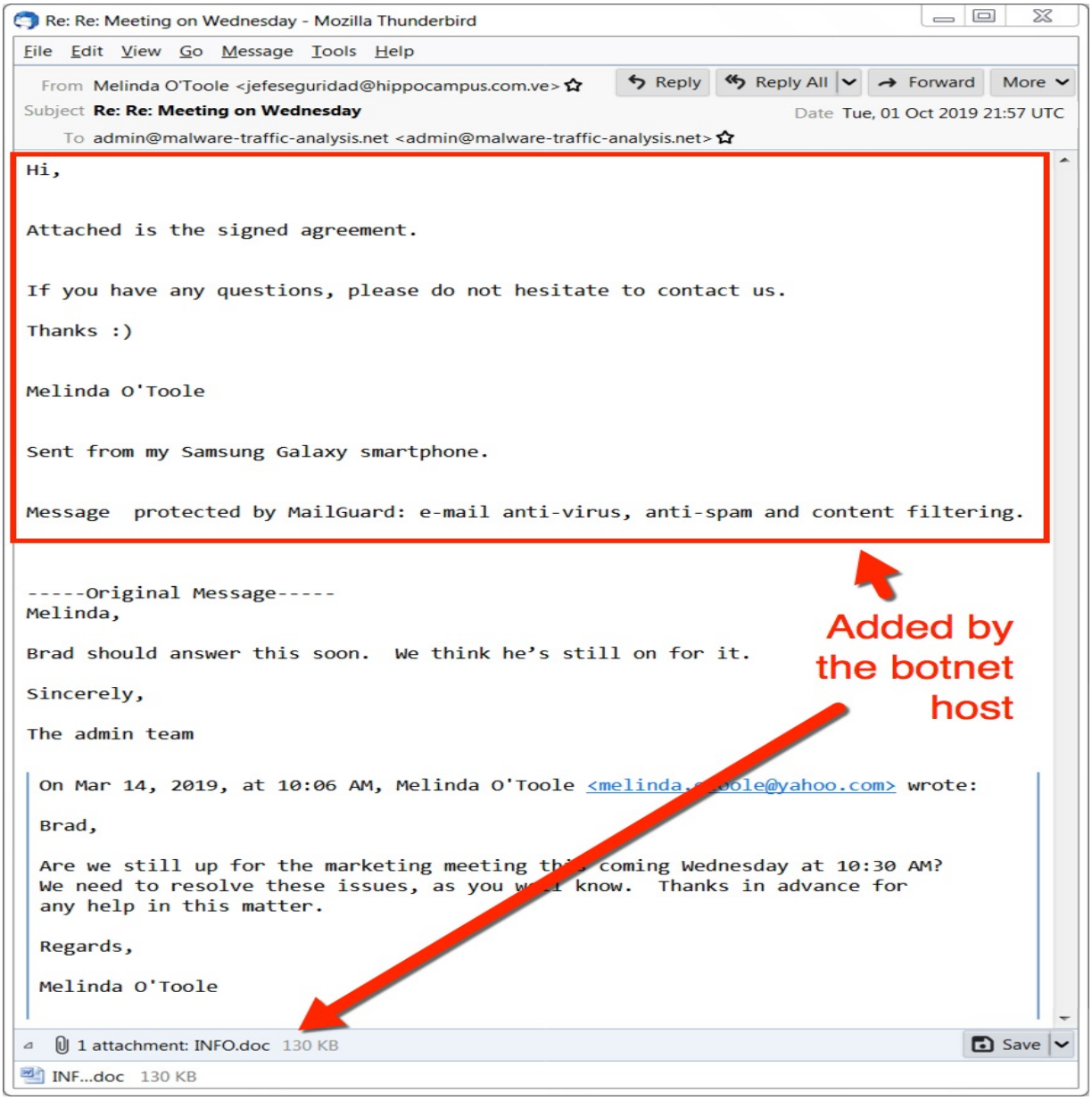
''Alipate [redacted]
[redacted].to

Sent from my Samsung Galaxy smartphone.

This email has been checked for viruses by Avast antivirus software.
https://www.avast.com/antivirus

Sample 5

The sample below varies from samples 1 to4. 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..



For more information please contact us:

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