The Epic Turla Operation: Information on Command and Control Server infrastructure

v1.00 (August 7, 2014)

Short Report

by

TO BE ON THE SAFE SIDE

Laboratory of Cryptography and System Security (CrySyS Lab)

http://www.crysys.hu/

Budapest University of Technology and Economics

Department of Networked Systems and Services

http://www.bme.hu/

Authors:

CrySyS Malware Intelligence Team in collaboration with Ukatemi Technologies

1. Introduction

Together with international partners, we have investigated the Turla/Uroburos/Snake related Epic/Wipbot/TavDig/Wordlcupsec operations and the command and control server infrastructure of it. Although hundreds of servers related to the threats were discovered by the community, most of them are not alive as of the analysis. We tried to obtain as much information as possible on the operation, structure and data related to these servers.

2. List of active C&C servers

The following C&C servers were alive at the time of our analysis:

- http://www.arshinmalalan.com/themes/v6/templates/css/

  proxies to http://busandcoachdirectory.com.au/[redacted]

- http://www.kidsbedsforkids.com/googlecheckout/library/css/
- http://voyagez-avec-nous.fr/inc/pgeditor/template/

1.1 Server side scripts

The servers are implemented in PHP.

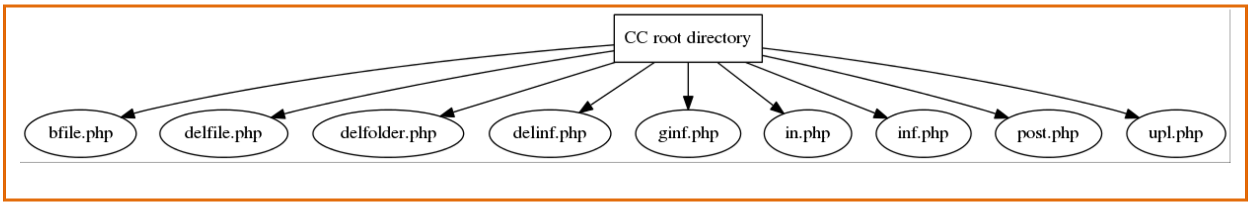

Figure 1 – PHP files found on the C&C servers

The scripts found on the examined servers differ, but mainly contain the followings:

- **bfile.php**: It can be used for downloading a file from the server. Uses 2 POST parameters.
- **delfile.php**: Deletes a file. It also needs 2 POST parameters.
- **delfolder.php**: Deletes a folder.
- **delinf.php**: Likely it was used by a previous version of the malware. It deletes the "inf" file of the given victim, but now it is useless.
- **ginf.php**: Gets the inf file of the victim, whose id is passed as a POST parameter.
- **in.php**: This is where the victims checks in. Stores the ip address, counter, timestamp and data. In some cases this was just a proxy. The proxy used TCP sockets and forwarded the whole data and did not make any log (e.g.: arshinmalalan forwarded data to busandcoachdirectory.com.au
- **inf.php**: Simple script showing results of phpinfo() PHP call

- **post.php**: Debug file
- **upl.php**: Uploads a new task
- **[redacted].php**: It creates and displays a list of all the victims with timestamp + IP controlled by that specific C&C. (Summarizes information stored in the data directories)
- **[redacted2].php**: On multiple servers a backdoor was found which was password protected. The backdoor seems to be very similar or identical to the one used in attacks by MiniDuke attackers.

1.2 Data storage

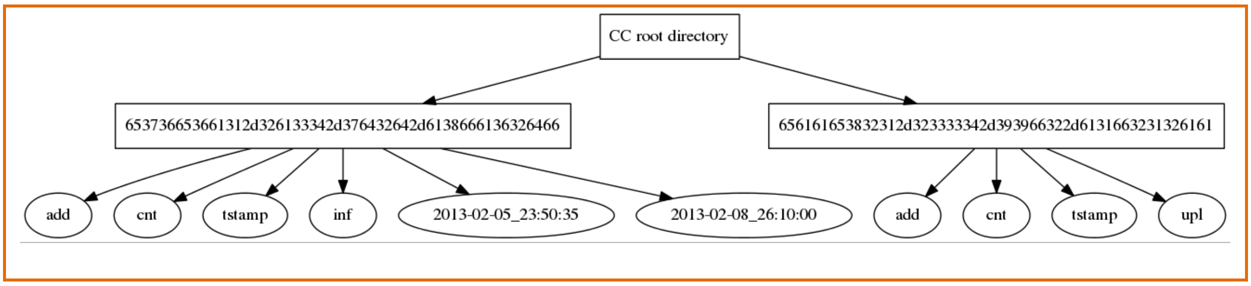
CC root directory
653736653661312d326133342d376432642d6138666136326466
656161653832312d323333342d393966322d6131663231326161
add
cnt
tstamp
inf
2013-02-05_23:50:35
2013-02-08_26:10:00
add
cnt
tstamp
upl

Figure 2 Sample directory structure for data storage

Client instances are identified by UUIDs, and the associated data is stored in dedicated directories. The directory names are derived from UUIDs with the following algorithm (python code snippet): `binascii.hexlify(str(uuid)[::-1]).`

Examples for conversion UUID to directory name:

```
aa212f1a-2f99-4332-128eaae ->
656161653832312d323333342d393966322d6131663231326161
fd26af8a-d2d7-43a2-1a6e67e ->
653736653661312d326133342d376432642d6138666136326466
```

Each directory may contain the following files:

- **add**: IP addresses associated with this client separated by semicolon.
- **cnt**: Number of times the client connected to the server.
- **tstamp**: Timestamp of the last connection.
- **inf**: Encrypted command for the client to execute.
- **i**: Unknown, generally empty. Most likely created for debug purposes.
- **[timestamp]**: Encrypted result of a command execution. (The file name is the timestamp of the file upload)

1.3 Data encryption

The command and the execution result files are encrypted using El-Gamal and AES-256. The malware samples include the command decoding private keys and these files are thus decryptable, but uploaded result files cannot be decrypted. We identified a number of implementation problems that make the encryption less secure but we were not able to break it:

- Using time seeded random generator (in combination with ad-hoc XORing buffers into the output) while storing the timestamp on the server side (the name of the uploaded file)
- Using small random numbers
- Text-book El-Gamal implementation that has some published weaknesses (Why Textbook ElGamal and RSA Encryption Are Insecure)

1.4 Victims

We've identified 165 unique victim IP addresses.

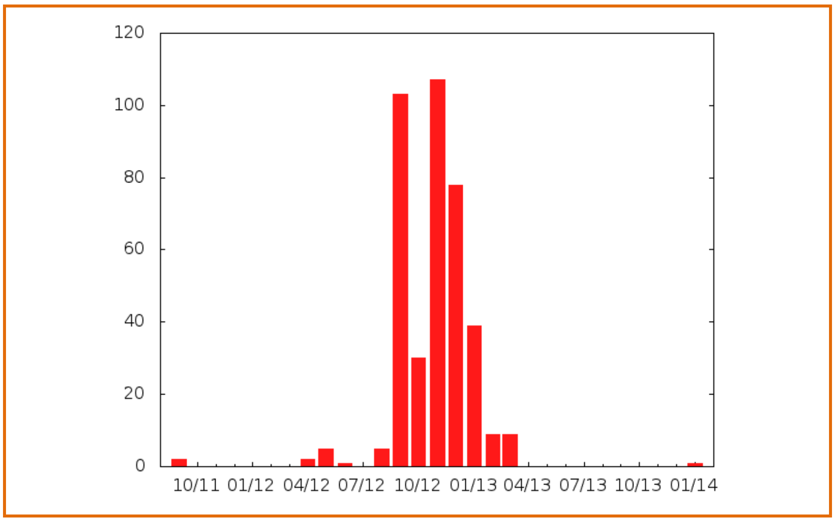

Figure 3 Last check-in date by number of UUIDs

Top countries by number of victim IP addresses:

1. THAILAND: 66
2. RUSSIAN FEDERATION: 16
3. SLOVENIA: 15
4. MONTENEGRO: 10
5. MACEDONIA: 10
6. UNITED STATES: 10

A heat map on the victim list can be found below.

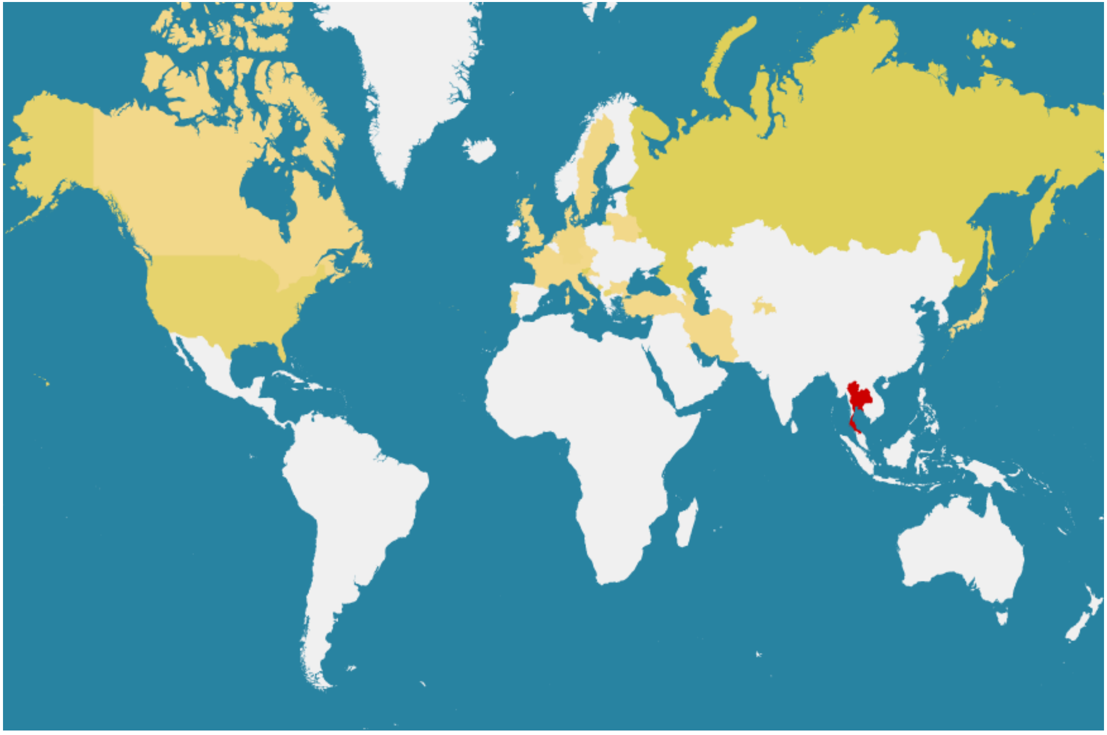

Figure 4 Heat map of victims – Data gathered from analyzed C&C servers directly

1.5 List of all samples of decrypted command files

For each victim, command files (PE executables) might be stored on the C&C servers as described in the section above about data storage. We found a number of files on the C&C servers. We have successfully decrypted all these files and collected their hash identifiers (MD5, SHA1, SHA256).

```
voyagez-avec-nous.fr - main 'upgrade' upl file
efd33fdb3dfdd2303a174e3eeb97949e
673d6d637ba884f7a70cb911f573460d872ae384
826862b6585cd1cc7e3d501ebad2f001ace903e3318653f452327009182715ec

www.arshinmalalan.com - d9102f08-853e-4a94-[redacted]
bca8051030d3273ac424864e6be9c995
2c2233aa7c08f1f87ed2ab7f95cb38a02aada7d7;
b34a9ac8c4cafdd4921c93f3cecaf64a32c954399dcca00e66ce9022429825a3

www.arshinmalalan.com - bb039b03-d7f3-4973-[redacted]
bfd95878915efb2d33e9b20a61de5796
58bfbf3e42b96ef870bf07789f1bc4a8415bfc95
1d4c1a96dd3681a13936f478b6894fb9b963e3b71e2b6cf59e5cf629ec8d222e

busandcoachdirectory.com.au - cd817264-3248-4659-[redacted]
0e98e0d634446b88d607bc9454d56e93
81198fecea42029f27bdd9685e55c170fe8d2ffa
3cd521891ba6cc5cf2e84f1c4c56a2fe2f8ca2aece2c9ef7eb6e0043f9514d5f

busandcoachdirectory.com.au - cd4b822c-50b3-4aa6-[redacted]
dc5db183ba8ceab4f093ac92fd8df21c
```

```
81334c9030408b28c37ffcbfe897c7f49a531767
d4e46bcc3ce7bc803cbda3e0d109fe11f2577518779e43dc031be3e6ba6b09e8

busandcoachdirectory.com.au - 3befc03a-b8fc-4409-[redacted]
dc5db183ba8ceab4f093ac92fd8df21c
81334c9030408b28c37ffcbfe897c7f49a531767;
d4e46bcc3ce7bc803cbda3e0d109fe11f2577518779e43dc031be3e6ba6b09e8

busandcoachdirectory.com.au - 4944c842-2b56-4756-[redacted]
2849fdd549823f23d92e4aeda9940dc1
83fb1b6ae1c4c5dc3fd8a0b13ab3760cd8de8ff5
571b808b90e063da31e98c9757246870fc33d09168d70bcfa80d2378aaa47ebe

busandcoachdirectory.com.au - 15C428094A6611806FD86C9C08321CE8
2a5454b6c374598504682436aef1f215
e9317d65febb4304c036545fea44cdbfc89f3bd3;
c537c7eef90e286a48cf09f201c64aa6351d35726e441e00c834b4f55a2e67fe

busandcoachdirectory.com.au - aa168c4c-d951-4bd8-[redacted]
0e98e0d634446b88d607bc9454d56e93
81198fecea42029f27bdd9685e55c170fe8d2ffa
3cd521891ba6cc5cf2e84f1c4c56a2fe2f8ca2aece2c9ef7eb6e0043f9514d5f

busandcoachdirectory.com.au - fcbd5564-57f9-464d-[redacted]
e9580b6b13822090db018c320e80865f
5576358fdf4b281df1cc472d12c81060e8415ba2
2007aa72dfe0c6c93beb44f737b85b6cd487175e7abc6b717dae9344bed46c6c

busandcoachdirectory.com.au - 41d8808e-8475-41a9-[redacted]
636dae414eb5db930eb4e519931ee99a
5c380a59a726571522a5d399589d2558ac3c231f
b546280bb875d3981d03c855602e7693d2c177f74620c8e0772d2a155f049776

busandcoachdirectory.com.au - 2c30a9b3-6595-4556-[redacted]
3a34980e80b6a6b68daa67d499e3d2ce
c08611e7f49c517bd3dc9b4862773d899b5ec298;
f472741bec78fdfcc42dfc5d792343390207c9c42775a7df398c32b39ee84784

busandcoachdirectory.com.au - 4008daf6-c937-469e-[redacted]
2849fdd549823f23d92e4aeda9940dc1
83fb1b6ae1c4c5dc3fd8a0b13ab3760cd8de8ff5
571b808b90e063da31e98c9757246870fc33d09168d70bcfa80d2378aaa47ebe
```

5. Decrypted command files - hashes

In addition to PE executables, command files can also be windows batch files. We found around ~10 different batch files. Some of these were highly customized to the target, therefore we do not share actual content for these.

The content of a data collecting batch file can be seen below:

```
dir c:\
dir "C:\Users\"
ipconfig -all
netstat -an
net view /DOMAIN
net view
arp -a
dir %TEMP%\
```

6. Sample command file - batch