# The Epic Turla Operation: Solving some of the mysteries of Snake/Uroboros

Kaspersky Lab Global Research and Analysis Team

Version 1.0
August 6, 2014

# Technical appendix: malware samples and indicators of compromise (IOC)

## A. Keylogger module

File name: varies
MD5: a3cbf6179d437909eb532b7319b3dafe
Compilation timestamp: 2012.10.02 10:51:50 (GMT)
Compiler: Microsoft Visual Studio 2010
File format: PE32 DLL
Exports: _LowLevelKeyboardProc@12

Creates the log file: `%TEMP%\~DFD3O8.tmp`. If failed, tries to write to the file `f:\keyhook.log`

Each time the keylogger starts, it appends the following header to the log file:

```
--------------------------------------------------------------------------------
New Session: %fully qualified computer name% %timestamp%
--------------------------------------------------------------------------------
```

It then creates a hidden console window and registers its only export _LowLevelKeyboardProc@12 as a hook procedure for low-level keyboard input events (WH_KEYBOARD_LL hook).

Depending on the results, it writes a line to its log file. In case the hook was installed, the line is "Started…", else *"LoadLibrary '%path to its file%' failed, %error code%"*.
It also starts a thread that retrieves the current foreground window handle every 100 milliseconds. This handle is then used in the keyboard hook procedure.

The low-level keyboard hook procedure intercepts WM_KEYDOWN, WM_KEYUP and WM_SYSKEYDOWN system messages and writes information about each keystroke to the log file. Every time a new window becomes active, it retrieves its name and the path to its application and writes this information to the log file:

```
[%path to the application's executable file%: "%window title%"]
```

## B. The “Epic/Tavdig/Wipbot” backdoor (Main backdoor module)

**Analyzed file (others are similar):**

Compilation timestamp: 2013.10.15 10:43:09 (GMT)
File format: PE32 DLL, modified (the file is supposed to be started by a custom loader)
Exports:

1000837F: ModuleStart
100083A9: ModuleStop
100083BB: start

The main functionality is implemented in a single function that is called by the DllMain entry point. The exported functions allow to call the same function directly (exported as “start”) or to start/stop it in a separate thread (“ModuleStart”/”ModuleStop”) and with slightly different parameters. This indicates the backdoor can also function as a plugin for the Turla Carbon system.

The main function executes in an infinite loop. It collects most of the available information about the system, transmits it to the C&C server and executes the commands it receives back. The module delays execution for random periods while it discovers running processes with one of the following filenames:

- tcpdump.exe
- windump.exe
- ethereal.exe
- wireshark.exe
- ettercap.exe
- snoop.exe
- dsniff.exe

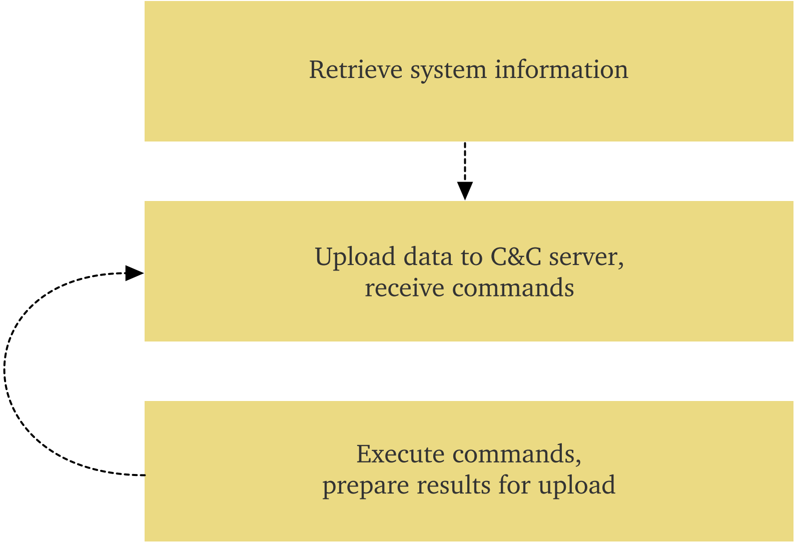
The following system information is collected:

1. Hardware information.
    - Registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SystemInformation`, value names: `SystemManufacturer`, `SystemProductName`.
    - All registry subkeys of the key `HARDWARE\DESCRIPTION\System\CentralProcessor`, value name: `ProcessorNameString`.
    - Available system memory status, total/free.
2. OS version information; the newest version known to it is Windows 7 / 2008R2. Unidentified versions are marked as “not support this version of Windows”.
3. Computer name (“ComputerNamePhysicalDnsFullyQualified”).

4. User name, local group name.
5. Common directory names: system, current, temporary directories.
6. Additional system information:
   - System and user language settings
   - User locale information: country name, current date, time zone.
   - Uptime
7. Disk space information for all available logical drives.
8. List of available network shares.
9. List of all user accounts, privilege classes, time of the last logon.
10. List of current IPV4 TCP connections and UDP listeners.
11. Information about installed Windows updates from the file `%WINDOWS%\SoftwareDistribution\ReportingEvents.log`.
12. Detailed list of running processes and their owners.
13. List of all window titles.
14. Directory listing of available logical drives and of the directories:
    - `Desktop`
    - `%TEMP%`
    - `%WINDOWS%\Temp`

The retrieved information is compressed using bzip2, encrypted with AES and then encoded using Base64 before being transmitted to the C&C server. When there is a file waiting for upload (usually, this is file that contains the results of the previously received and executed command), it is read from disk and uploaded to the server instead of the system information.

The C&C communication is implemented on top of the standard HTTP/HTTPS protocols. The list of the C&C URLs is hardcoded in the binary but may be overridden by further commands.

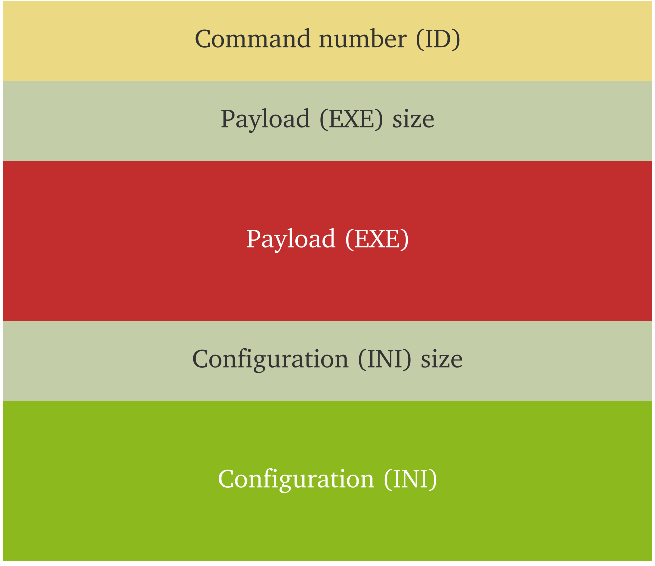

Retrieve system information
Upload data to C&C server, receive commands
Execute commands, prepare results for upload

C&C server communication cycle

The module uses Wininet API functions for issuing HTTP POST requests to the server. The module transmits the collected information in the body of the POST request and gets new commands from the server's response. The request body can be empty if there is no new information to upload. The response is usually an HTML document and the commands are Base64-encoded strings enclosed in `<div>/</div>` tags. Every command is encrypted using asymmetric encryption with temporary AES session keys.

Each command is a mixed text/binary buffer. It consists of two parts: payload and configuration. The configuration is an INI file that controls the further behavior of the module. It is extracted into a temporary file named `%TEMP%\~D%random%.tmp`. The payload, if exists, is supposed to be an executable file and may be executed if there is a corresponding command present in the INI part.

The format of the decoded command is the following:



Format of the C&C command buffer

Available commands are:

| Name | Description |
|---|---|
| exe | Execute a command, redirect its output to the file `%TEMP%\~D%random%.tmp`. The file is then uploaded during the next C&C communication cycle. |
| down | Change the C&C URL to a given value. |
| del_task | Delete a file. |
| result | Set the filename that is supposed to contain the results of command execution. Effectively, any existing file may be marked for upload by this command. |

| Name | Description |
|---|---|
| delete | Mark the file `%TEMP%\~tmp085.dat` to be deleted on reboot. |
| name | Set the filename to be deleted or created (depends on other parameters) |

## C. Malware samples

### Lateral movement tools:

```
a3cbf6179d437909eb532b7319b3dafe - custom keylogger
1369fee289fe7798a02cde100a5e91d8 - UPX compressed “dnsquery.exe”
c0c03b71684eb0545ef9182f5f9928ca - dnsquery.exe
```

### Epic/Tavdig backdoors:

```
4dc22c1695d1f275c3b6e503a1b171f5
111ed2f02d8af54d0b982d8c9dd4932e
7731d42b043865559258464fe1c98513
24b354f8cfb6a181906ceaf9a7ec28b0
fdba4370b60eda1ee852c6515da9da58
3ab3d463575a011dfad630da154600b5
a347af5cc3c5429911e5167b2d30e1ac
6b207521c9175d2274ba3debcc700a1d
cb264c9efa566f41975a3cebf903efb5
e9c0d32a15a24b1110fcc18ab04a6738
d102e873971aa4190a809039bc789e4d
d7ca9cf72753df7392bfeea834bcf992 - dropped by the Java CVE-2012-1723 exploits
42b7b0bd4795fc8e336e1f145fc2d27c
ab686acde338c67bec8ab42519714273
8e90d8b68a053d22b54fb39f1cf01a41
d22b0ec4e9b2302c07f38c835a78148a
764d643e5cdf3b8d4a04b50d0bc44660
d31f1d873fa3591c027b54c2aa76a52b
ea1c266eec718323265c16b1fdc92dac
bc2eff0a1544e74462e7377cf0de5a36
d22b0ec4e9b2302c07f38c835a78148a
86f28e8d9d6bda11abcf93b76074b311
d28661163ae91848e01a733836bfe0aa
09b7f890ccded1a6210119df8a9a08f9
5c4a51ce7aa76579616a01a0a3cfab38
aa58167c57cac1bc562c77766ca249f5
3a785ede87bfbd2c1c29887e9c36c801
7731d42b043865559258464fe1c98513
0e441602449856e57d1105496023f458
```

### Dropper packages that installs both Epic and Turla Carbon system:

```
c7617251d523f3bc4189d53df1985ca9 - Postanovlenie apelljacionnoj instancii.scr
0f76ef2e6572befdc2ca1ca2ab15e5a1 - Opredelenie.scr
```

### PDF exploits used in spearphishing attacks drops Epic backdoor:

```
6776bda19a3a8ed4c2870c34279dbaa9 - Note_№107-41D.pdf
dba209c99df5e94c13b1f44c0f23ef2b - unknown.PDF
f44b1dea7e56b5eac95c12732d9d6435 - unknown.PDF
4c65126ae52cadb76ca1a9cfb8b4ce74 - unknown.PDF
```

### SCR/EXE files - used in spearphishing/social engineering:

```
4d667af648047f2bd24511ef8f36c9cc - NATO position on Syria.scr
ab686acde338c67bec8ab42519714273 - Russia position on Syria.scr
1c3634c7777bd6667936ec279bac5c2a - Talking Points.scr
80323d1f7033bf33875624914a6a6010 - Program.scr
77083b1709681d43a1b0503057b6f096 - Security protocol.scr
01a15540481f28163e7b4908034efbe3 - unknown.exe (“WorldCupSec” )
6a24071fde3b5d713c58801dcdd62044 - unknown.exe (“WorldCupSec” )
626955d20325371aca2742a70d6861ab - unknown.exe (“TadjMakhal”)
16eba8e5f0440a213935e1af4976d801 - unknown.exe (“RussiaPositions”)
0c35a8f9f9b6ab2f7e3b4408abc61f73 - pdfview.exe
d685403d000f8f6b25a6746f6f05a51c - winword.exe
```

### Fake “Adobe Flash Player” Epic backdoor installers:

```
7c52c340ec5c6f57ef2fd174e6490433 - adobe_flash_player.exe
030f5fdb78bfc1ce7b459d3cc2cf1877 - Shockwave_Flash_Player.exe
```

### Fake “Microsoft Security Essentials Quick Scan” Epic backdoor installer

```
89b0f1a3a667e5cd43f5670e12dba411
```

### Turla Carbon Pfinet backdoors

```
e9580b6b13822090db018c320e80865f - Pfinet backdoor
071d3b60ebec2095165b6879e41211f2 - Pfinet backdoor
```

## Turla Carbon package

cb1b68d9971c2353c2d6a8119c49b51f

## Related Turla sample module

626576e5f0f85d77c460a322a92bb267

## Java Exploits used in waterhole attacks

536eca0defc14eff0a38b64c74e03c79

f41077c4734ef27dec41c89223136cf8

15060a4b998d8e288589d31ccd230f86

e481f5ea90d684e5986e70e6338539b4

21cbc17b28126b88b954b3b123958b46

acae4a875cd160c015adfdea57bd62c4

## D. Epic C&C Server URLs (hacked sites used as 1st level proxies):

hxxp://losdivulgadores[.]com/wp-content/plugins/wp-themes/
hxxp://gspersia[.]com/first/fa/components/com_sitemap/
hxxp://blog.epiccosplay[.]com/wp-includes/sitemap/
hxxp://gofree[.]ir/wp-content/plugins/online-chat/
hxxp://homaxcompany[.]com/components/com_sitemap/
hxxp://www.hadilotfi[.]com/wp-content/themes/profile/
hxxp://mortezanevis[.]ir/wp-content/plugins/wp-static/
hxxp://ncmp2014[.]com/modules/mod_feed/feed/
hxxp://mebroad[.]com/wp-content/gallery/posters/img/
hxxp://gruenerenate[.]de/wp-content/plugins/bbpress/includes/lang/
hxxp://www.arshinmalalan[.]com/themes/v6/templates/css/in.php
hxxp://products.parentsupermarket[.]com/phpMyAdmin/
hxxp://c-si[.]ir/includes/
hxxp://mkiyanpoor[.]ir/wp-includes/
hxxp://www.massage-ketsch[.]de/wp-includes/
hxxp://onereliablesource[.]com/wp-content/plugins/sitemap/
hxxp://petrymantenimiento[.]com/wp-content/plugins/wordpress-form-manager/lang/
hxxp://ohsoverydarling[.]com/wp-content/themes/verification/
hxxp://poissonnerieantoine[.]com/web/wp-content/themes/titan/view/
hxxp://www.gholghola[.]com/azemashoorhost/smarty/tmpl/
hxxp://www.saglikdetay[.]com/wp-includes/images/icons/
hxxp://www.entesharati[.]com/wp-content/plugins/edd-paginate/
hxxp://iranabad[.]com/sarzamin/cms/application/classess/plugins/
hxxp://deltateam[.]ir/components/com_sitemap/
hxxp://akva-clean[.]ru/typo3temp/
hxxp://discontr[.]com/wp-content/themes/twentytwelve/
hxxp://curaj[.]net/pepeni/images/
hxxp://executrek[.]org/components/com_sitemap/
hxxp://amoodgostar[.]com/wp-content/themes/simplebanner/
hxxp://gayamore[.]com/gallery/090607/
hxxp://www.automation-net[.]ru/typo3temp/
hxxp://www.lacitedufleuve[.]com/Connections1/
hxxp://www.aspit[.]sn/administrator/modules/mod_feed/

## E. Intermediary level proxies (hacked sites used as 2nd/3rd level):

hxxp://masterciw[.]com/<br>
hxxp://khrn[.]tk/wp-includes/
hxxp://pradlolux[.]cz/system/helper/
hxxp://original-key[.]com/catalog/controller/payment/
hxxp://www.noraci[.]com/wp-includes/
hxxp://tuvpr[.]com/backup/wp-includes/
hxxp://www.boshraamin[.]com/wp-includes/
hxxp://www.bestjob[.]my/system/modules/comments/
hxxp://rollinghillsfitness[.]com/wp-includes/

## F. Motherships, hosting Epic Control panels and exploits

hxxp://avg-update.sytes[.]net/
hxxp://newsforum.servehttp[.]com/
hxxp://newsweek.servehttp[.]com/
hxxp://adobe.faqserv[.]com/
hxxp://cqcount.servehttp[.]com/
hxxp://easycounter.sytes[.]net/
hxxp://newsweek.serveblog[.]net/
hxxp://image.servepics[.]com/
hxxp://bgl.serveftp[.]net/