TS/NOFORN

MARION MARSCHALEK

@PINKFLAWD

MARION@CYPHORT.COM

BCC0 7607 2FFA BCA8 9048 D648 D169 73AF F372 F2CA

CYPHORT

Welcome to the keynote circuit – I thought that‘s where old people like me go to die? ;)

- Halvar Flake, Oct.14 2014

http://www.mirror.co.uk/


DEFENDERS
http://www.moviepilot.com


SOPHISTICATED
WEAPONRY
http://www.screenrant.com/

SOPHISTICATED WEAPONRY WITH SUPERPOWERS

MICKEY MOUSE DEATH STAR

- YOU DON‘T SEE YOUR ADVERSARY
- YOU DON‘T KNOW WHOSE DEATH STAR IT IS THERE ON YOUR MACHINE
- YOU PROBABLY WON‘T EVEN FIND THE DEATH STAR ON YOUR MACHINE

CYPHORT

http://glee.wikia.com

Cyber!

- Intellectual property being stolen
- Political opponents put to jail
- Internet communication being blocked
- Vendor finding a new exploit
- Same time, hacker writes 5 more
- Control of media
- Enterprises loosing customer data
- Nation states spying on their citizens
- Nation states being hacked
- Little Paul loosing his homework

CYPHORT

SUSPECT #1

- FILESIZE:192512
- COMPILETIME: 2010:05:06
- C&C: CALLIENTEFEVER.INFO
- HTTP ACCEPT-LANGUAGE: FR

```
push    offset aHttpCallientef ; "http://callientefever.info/img/nev
push    offset aNotifurl ; "NotifUrl"
mov     eax, ebp
mov     [esp+1954h+var_1938], ebp
call    AddConfParam
push    offset aHttpCallient_0 ; "http://callientefever.info/img/nev
push    offset aSyncurl ; "SyncUrl"
mov     eax, ebp
call    AddConfParam
push    offset aTfc_config_key ; "TFC_Config_Key"
push    ebp
mov     ebx, offset aSoftwareMicr_0 ; "Software\\Microsoft\\Net3D"
call    AddConfParam2
push    offset aTfc_confgig_na ; "TFC_Confgig_Name"
push    ebp
mov     ebx, offset aConfig ; "Config"
call    AddConfParam2
call    QueryTFCKey
lea     esi, [esp+194Ch+var_1934]
mov     edx, offset a1_506 ; "1.506"
mov     [esp+194Ch+var_1934], 0
call    GetLength_mb
```

CYPHORT

SUSPECT #1

- DYNAMIC API LOADING BY NAME HASH

```
for (i=0; i<expcount; i++) {
    exp_len = strlen(exports[i]);
    temp = 0;
    result = 0xAB34CD77;
        for (j=0; j<exp_len; j++) {

            temp = (rotl(temp,7) ^ exports[i][j]);
        }
        result ^= temp;
        result ^= 0xAB34CD77;
        printf("%8x\t%s\n", result, exports[i]);
}
```

SUSPECT #1

PING

EXEC

HTTPF

ASPFLOOD

TCPFLOOD

WEBFLOOD

POSTFLOOD

ATCLEAR

STATISTICS

KILL

SET

UPLOAD

UPDATE

PLUGIN

FLOODING ALL THE THINGS

CYPHORT

SUSPECT #1


http://callientefever.info/
Google
This is a research system operated by Kaspersky Lab
For more information please visit:
www.kaspersky.com
www.securelist.com
For abuse please contact: theflame [AT] kaspersky [dot] com
KASPERSKY lab

CYPHORT

SUSPECTS #[2-4]

- FileSize: 184320
- CodeSize: 139264
- CompileTime: 2010:02:16 18:05:54+01:00

- FileSize: 184320
- CodeSize: 139264
- CompileTime: 2010:03:11 17:55:03+01:00

- FileSize: 792064
- CodeSize: 583680
- CompileTime: 2011:10:25 20:28:39+01:00

SUSPECT #4

- FileSize: 792064
- CompileTime: 2011:10:25 20:28:39+01:00
- API name hashing key AB34CD77h
- http://1.9.32.11/bunny/test.php?rec=nvista

Anti-Analysis | Threads & Files | CPU Data | C&C Commands | LUA

```
.rdata:001A47E0 ; char aRb_0[]
.rdata:001A47E0 aRb_0           db 'rb',0                       ; DATA XREF: FseekStuff+EF↑o
.rdata:001A47E3                 align 4
.rdata:001A47E4 aSelfdir_tmpdat db '%SELFDIR%\_tmpdat',0
.rdata:001A47F6                 align 4
.rdata:001A47F8 aSelfdirPerfl_2 db '%%SELFDIR%%\PerfLib_Perfdata_42%i.dat',0
.rdata:001A47F8                                                 ; DATA XREF: WriteToPerfdata+
.rdata:001A481E                 align 10h
.rdata:001A4820 aSelfdirPerfl_1 db '%%SELFDIR%%\PerfLib_Perfdata_41%i.dat',0
.rdata:001A4820                                                 ; DATA
.rdata:001A4846                 align 4
.rdata:001A4848 aSelfdirPerfl_3 db '%%SELFDIR%%\PerfLib_Perfda
.rdata:001A4848                                                 ; DATA
.rdata:001A486E                 align 10h
.rdata:001A4870 aSelfdirPerfl_4 db '%%SELFDIR%%\PerfLib_Perfda
.rdata:001A4870                                                 ; DATA
.rdata:001A4896                 align 4
.rdata:001A4898 aS0             db '%s0',0                      ; DATA
.rdata:001A489C aV3gr6bZ2c_0    db 'V3gr6B&Z2c',0               ; DATA
.rdata:001A48A7                 align 4
.rdata:001A48A8 aV3gr6bZ2c_1    db 'V3gr6B&Z2c',0               ; DATA
.rdata:001A48B3                 align 4
.rdata:001A48B4 aV3gr6bZ2c      db 'V3gr6B&Z2c',0               ; DATA
.rdata:001A48BF                 align 10h
.rdata:001A48C0 aV3gr6bZ2c_2    db 'V3gr6B&Z2c',0
.rdata:001A48CB                 align 4
.rdata:001A48CC a0123456789abcd db '0123456789ABCDEF',0
.rdata:001A48DD                 align 10h
.rdata:001A48E0 aAbcdefghijklmn db 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',0
.rdata:001A48E0                                                 ; DATA XREF: .data:0FF_4B9B40
.rdata:001A4921                 align 4
```

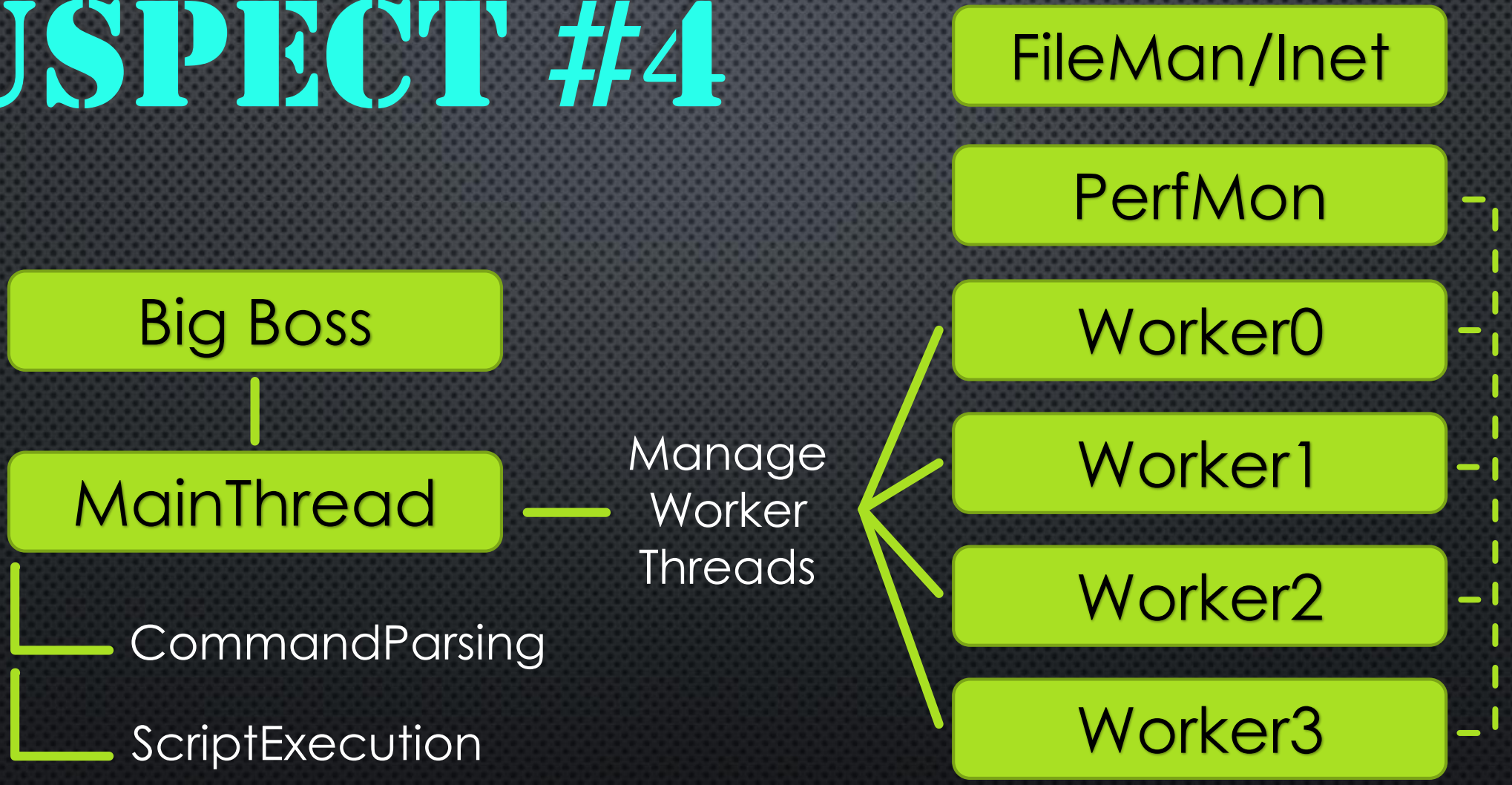
NOT FUNNY.

SUSPECT #4

AV Product Enumeration	SELECT * FROM AntiVirusProduct
Firewall Product Enumeration	SELECT * FROM FirewallProduct
Sandbox Check	"klavme", "myapp", "TESTAPP", "afyjevmv.exe“, Timing Condition

CYPHORT

SUSPECT #4


FileMan/Inet
PerfMon
Big Boss
Worker0
MainThread
Manage
Worker
Threads
Worker1
Worker2
CommandParsing
Worker3
ScriptExecution

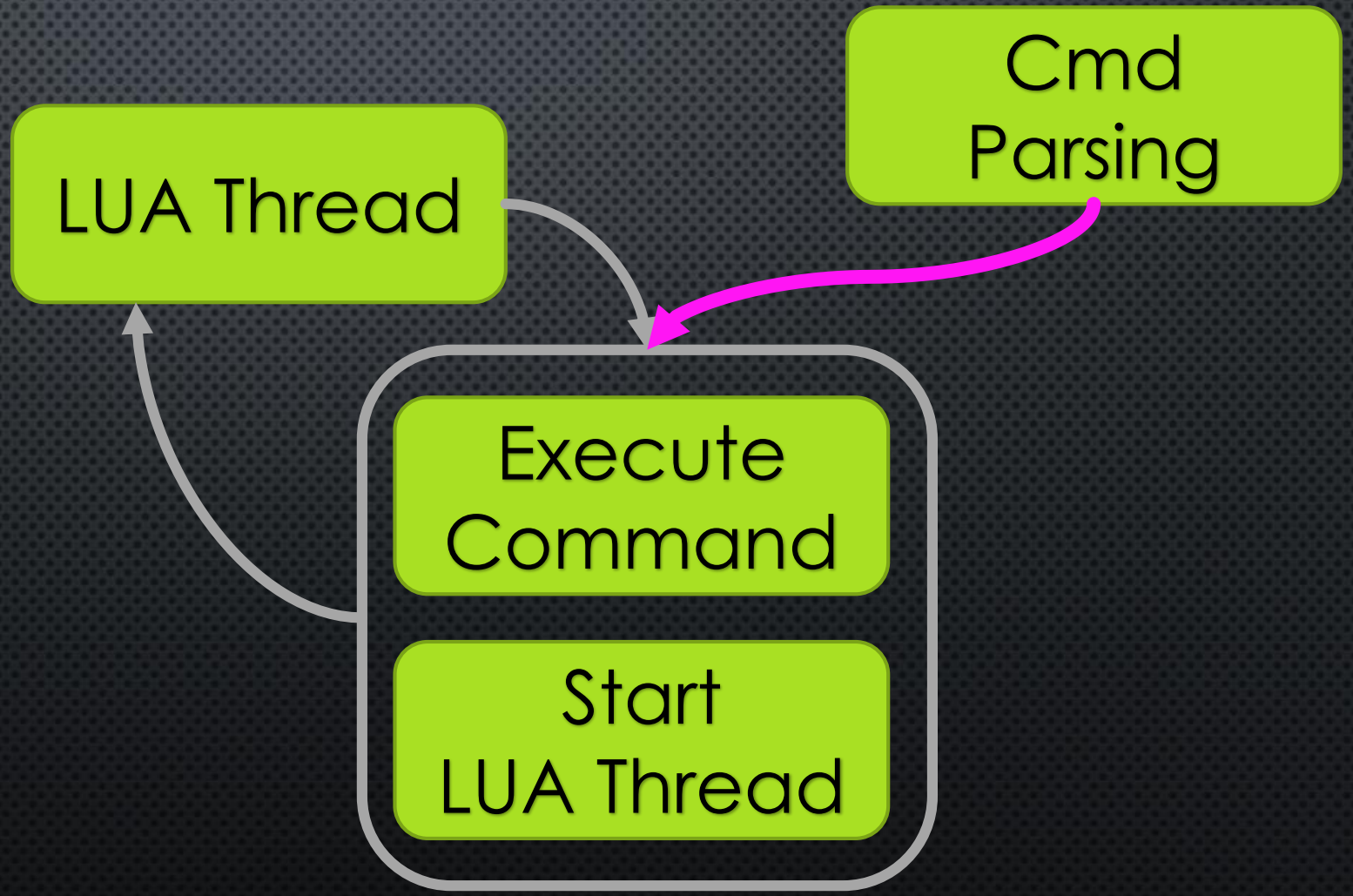
SUSPECT #4

- Config stored in HKLM\Software\Microsoft\Ipsec

- http://le-progres.net/images/php/test.php?rec=11206-01
- http://ghatreh.com/skins/php/test.php?rec=11206-01
- http://www.usthb-dz.org/includes/php/test.php?rec=11206-01

SUSPECT #4

Advanced Command and Script Parsing



CYPHORT

SUSPECT #4

Advanced Command and Script Parsing

4 WORKER THREADS

EXECUTING LUA SCRIPTS

LUA 5.1 + C/INVOKE CODE

CALLBACK FROM LUA TO C++

CYPHORT

SUSPECT #4

GETCONFIG

FTPPUT

FTPGET

SENDFILE

GETFILE

UNINSTALL

RESTARTHEARER

RESTART

CLEANHEARER

CRONTASKA

CRONTASKR

CRONTASKL

MAXPOSTDATA

SETURL

STOP

SETCPULIMIT

TIMEOUT

WAITFOR

UPDATEDIETIME

CYPHORT

Analyzing CVE-2011-4369 – Part One

by admin · December 20, 2011 · Uncategorized

Adobe pulled a fast one a couple days ago when they pushed out their most recent patch. In doing so they addressed CVE-2011-2462, but also mentioned another vulnerability that exploited the PRC format (also related to U3D). This additional vulnerability was not one I had come across until a few days ago and below is my initial analysis of the PDF structure, and barebones dynamic analysis.

https://www.pdfxray.com/interact/e6db130bb8768a5f65e7e52aa235e66e/

Structure Breakdown

This PDF does not make use of any encryption or advanced capabilites, but does have an interesting structure. The document itself consists on 17 pages which is a key fact to note because it is later used by the JavaScript. These pages are defined in object 1 with pages 8-11 being those that reference the PRC streams.

Located within the last object (64) is the JavaScript triggered to run when the document is opened (JS is contents for the first page) which will be analyzed later. Located throughout the document are several objects containing a stream that defines PRC content.

The first file dropped on to the system is "AcroRd32Info.cab" which is then expanded using "C:WINDOWSsystem32expand.exe" that writes "acrord32info.exe". VirusTotal identifies this file as a generic dropper, but does not provide any malware family

http://www.virustotal.com/file-scan/report.html?id=c6a182f410b4cda0665cd792f0…

After writing to "C:WINDOWSsystem32wbemLogswbemprox.log" another file is written to "C:WINDOWSmsappsnetmgr.exe". VirusTotal identifies this file as an injector, but again, does not provide any malware family. Before the main process is terminated a registry value is set so that "netmgr.exe" runs when the system starts.

http://www.virustotal.com/file-scan/report.html?id=be14d781b85125a60747249646…

Running "netmgr.exe" manually creates a process and executes svchost.exe which waits for a few seconds and then terminates. Within the "netmgr.exe" are references to "http://1.9.32.11/bunny /test.php?rec=nvista", but it is unclear what role, if any, this site plays. Part two will include more analysis on the binary files dropped by the PDF.

Vulnerability Summary for CVE-2011-4369

Original release date: 12/16/2011

Last revised: 01/29/2013

Source: US-CERT/NIST

http://blog.9bplus.com/analyzing-cve-2011-4369-part-one/

Suspect #5

- FileSize: 966144
- CodeSize: 128512
- CompileTime: 2011:10:25 19:28:00+01:00
- Dropper for Suspect #4
- Same C&Cs as Suspect #4

CYPHORT

SUSPECT #5

ACRORD32INFO.EXE

Location	Remote Host	Port Number
Oakville, Canada	69.90.160.65	80
Montréal, Canada	70.38.107.13	80
Montréal, Canada	70.38.12.10	80

http://www.threatexpert.com/report.aspx?md5=c40e3ee23cf95d992b7cd0b7c01b8599

Please confirm

IDA has determined that the input file was linked with debug information, and the symbol filename is:
'C:\Users\user\Desktop\bunny 2.3.2\Release\Transporter2.pdb'
Do you want to look for this file at the local symbol store
and the Microsoft Symbol Server?

Yes

Don't display this message again

SRSLY?

v 2.3.2

SUSPECT #5

- Drops payload in %Windir%\msapps\netmgr.exe
- Stores configuration in Registry
- Creates entry in HKLM\..\CurrentVersion\Run for netmgr.exe
- Reaches out to remote servers

CYPHORT

Swiss Cheese Attribution

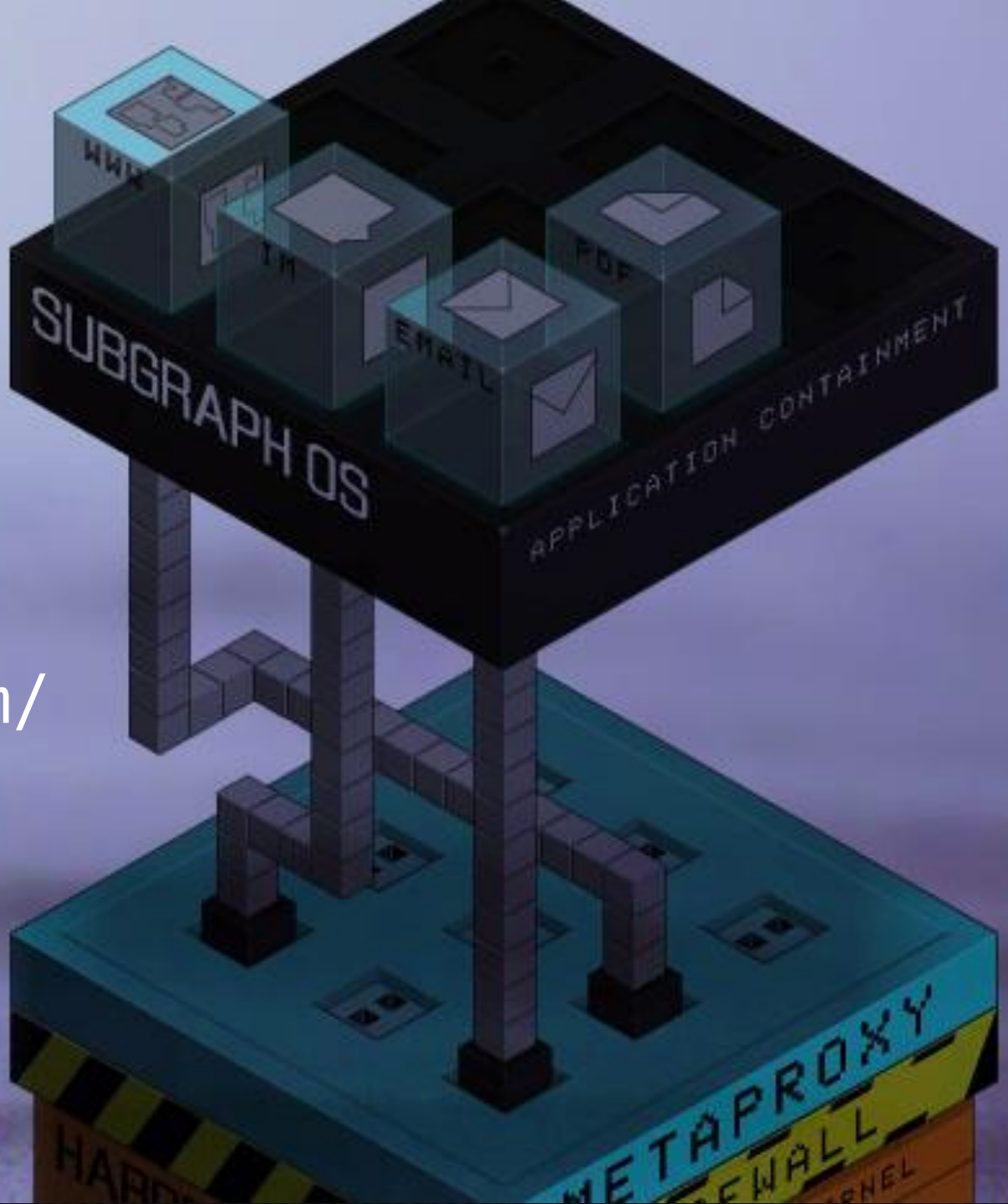
- Project named bunny, version 2.3.2
- DDoS botnet operators
- Accept-Language: fr
- C&C Servers hosted in Canada
- C&C domains resemble French/Iranian websites
- Author no english native-speaker ...
- LUA? Must be Flame


Wars not make
one great.


OPEN
whispersystems
Security, simplified.
Open Source security for mobile devices.
https://whispersystems.org/


Open Garden
You are the Internet
http://www.theverge.com

SUBGRAPH OS
https://subgraph.com/



BetterCrypto·org

Applied Crypto Hardening

HTTP://WWW.WOODMANN.COM/COLLABORATIVE/TOOLS/INDEX.PHP/CATEGORY:RCE_TOOLS

HTTP://WWW.WOODMANN.COM/COLLABORATIVE/KNOWLEDGE/INDEX.PHP/CATEGORY:RCE_KNOWLEDGE

Time to do malware research right.

Viper is a *binary management and analysis framework* dedicated to malware and exploit researchers.

http://viper.li/

Acknowledgements

- Mr. White, Mr. Orange, Mr. Blonde & Mr. Pink
- Morgan Marquis-Boire
- Inbar Raz
- Nicolas Brulez
- @EmergencyKittens

CYPHORT

Thank you!

Marion Marschalek
@pinkflawd
marion@cyphort.com

CYPHORT

http://karmadecay.com/

ANALYZE IT

- 2A64D331964DBDEC8141F16585F392BA
- 40E0F0681C79D70AC0329E68A94294CB
- 8132EE00F64856CF10930FD72505CEBE
- E8A333A726481A72B267EC6109939B0D
- 3BBB59AFDF9BDA4FFDC644D9D51C53E7
- C40E3EE23CF95D992B7CD0B7C01B8599