Digital Vengeance

Exploiting the Most Notorious C&C Toolkits

@professor__plum

I'M GONNA POP SOME SHELLS
GOT A FEW EXPLOITS IN MY POCKET

```
>$ whoami
plum
>$ finger
Login  Name                TTY    Idle  Login   Time   Office
plum   @Professor__Plum    pts/2        Sun     09:39  bc.symantec.com
plum   @Professor__Plum    pts/0   3yr  Tue     18:21  gin.bluecoat.com
plum   @Professor__Plum    pts/3   5yr  Fri     02:48  ???.nsa.gov
>$ █
```

Disclaimer

- The views expressed herein do not necessarily state or reflect the views of my current or former employers.
- I am not responsible for any use or misuse of the information provided.
- Implementation of the information given is at your own risk.

The sophisticated attack

"… identified an **extremely sophisticated** cyber attack"
RSA

"Government and non-government entities are under constant attack by evolving and **advanced persistent threats** and criminal actors. These adversaries are **sophisticated**, **well-funded**, and **focused**."
Office of Personnel Management

"The threat is very **persistent**, **adaptive** and **sophisticated** – and it is here to stay,"
SWIFT

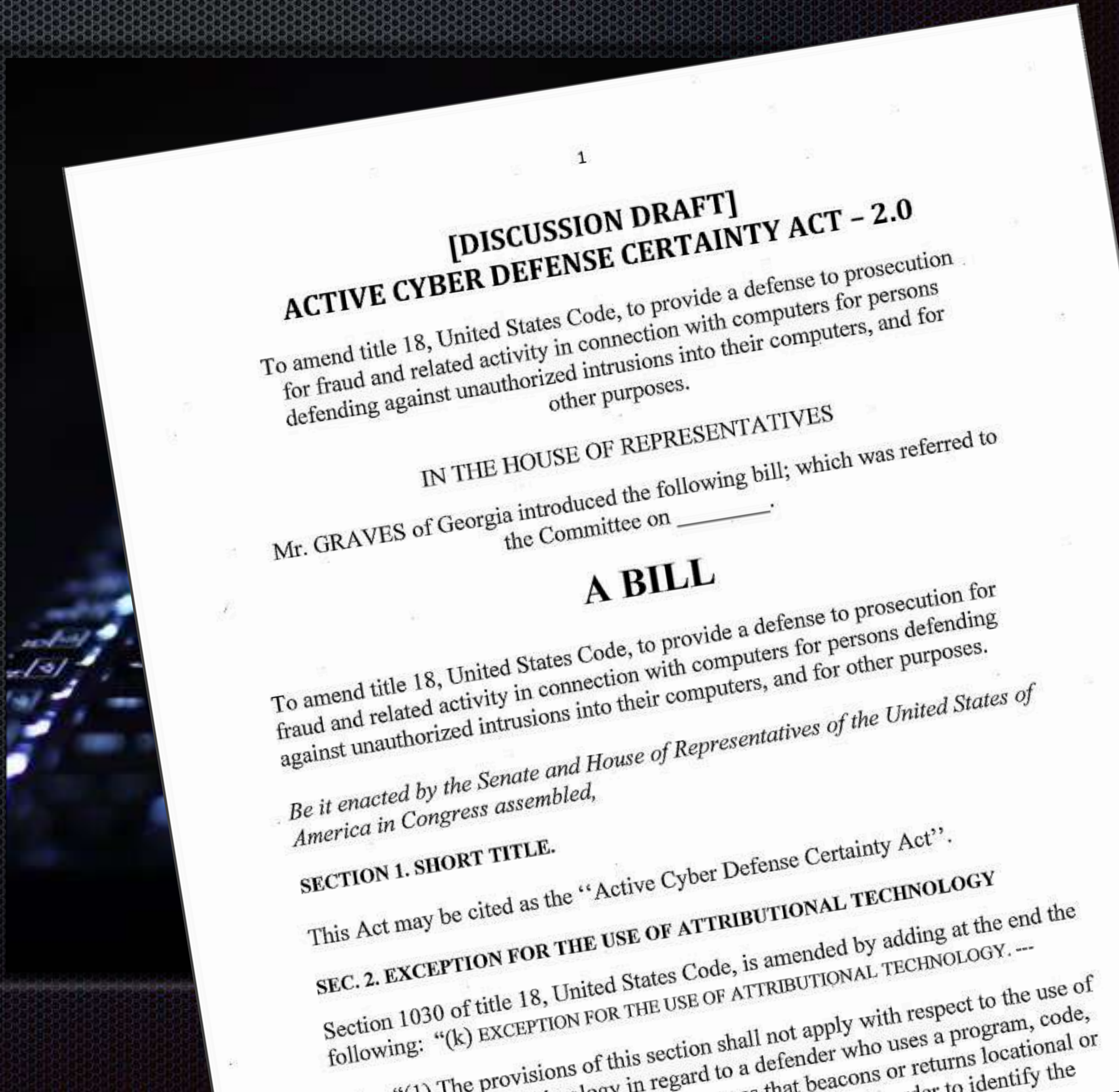
"The malware that was used would have slipped or probably got past 90% of internet defenses that are out there today in private industry"
Joseph Demarest, assistant director of the FBI's cyber division

"hackers obtained data on tens of millions of current and former customers and employees in a **sophisticated** attack"
Anthem

"It is **simply not possible** to beat these hackers"
James A. Lewis Cybersecurity Expert at Center for Strategic and International Studies (CSIS)

Hacking back

- 36% of BH 2012 attendees surveyed said they engaged in some form of hacking back
- Many feel justified in hacking back because their government isn't doing enough to protect them
- The ACDC would exempt victims from hacking laws when the aim is to identify the assailant, cut off attacks or discover stolen files.



1

[DISCUSSION DRAFT]

ACTIVE CYBER DEFENSE CERTAINTY ACT – 2.0

To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. GRAVES of Georgia introduced the following bill; which was referred to the Committee on ________.

A BILL

To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Active Cyber Defense Certainty Act''.

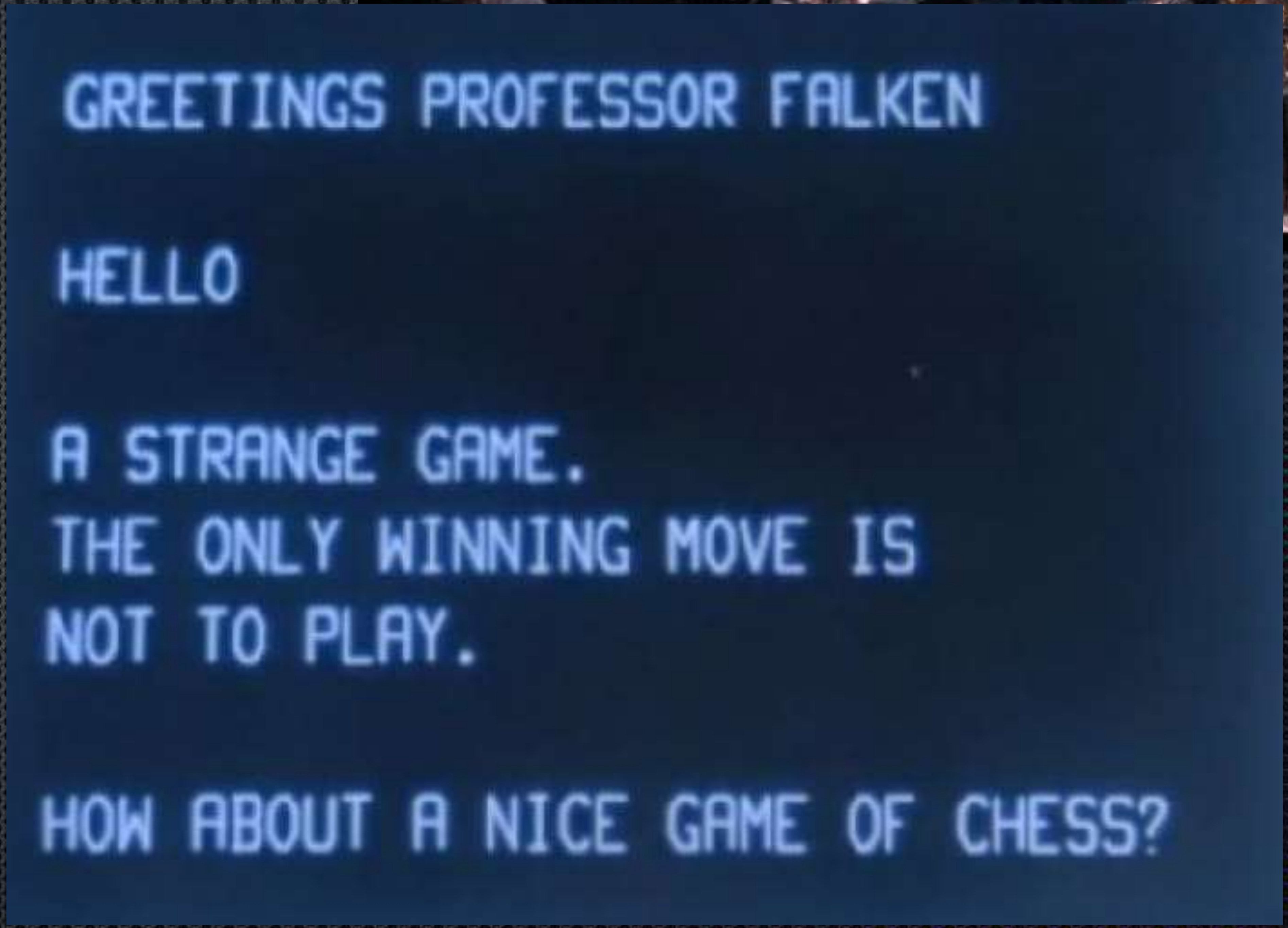
SEC. 2. EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY

Section 1030 of title 18, United States Code, is amended by adding at the end the following: "(k) EXCEPTION FOR THE USE OF ATTRIBUTIONAL TECHNOLOGY. ---

"(1) The provisions of this section shall not apply with respect to the use of ology in regard to a defender who uses a program, code, that beacons or returns locational or der to identify the

Hacking back

- Most likely Illegal
- Little to no gain
- Much at risk
  - Liability
  - Reputation
  - Productivity
  - Escalation



```
GREETINGS PROFESSOR FALKEN

HELLO

A STRANGE GAME.
THE ONLY WINNING MOVE IS
NOT TO PLAY.

HOW ABOUT A NICE GAME OF CHESS?
```

"(ii) does not include conduct that—

"(I) destroys or renders inoperable information that does not belong to the victim that is stored on a computers of another;

"(II) causes physical or financial injury to another person;

"(III) creates a threat to the public health or safety; or

"(IV) exceeds the level of activity required to perform reconnaissance on an intermediary computer to allow for attribution of the origin of the persistent cyber intrusion;

"(C) the term 'attacker' means a person or an entity that is the source of the persistent unauthorized intrusion into the victim's computer; and

"(D) the term 'intermediary computer' means a person or entity's computer that is not under the ownership or control of the attacker but has been used to launch or obscure the origin of the persistent cyber-attack.".

‘‘(i) means any measure—

‘‘(I) undertaken by, or at the direction of, a victim; and

‘‘(II) consisting of accessing without authorization the computer of the attacker to the victim’ own network to gather information in order to:

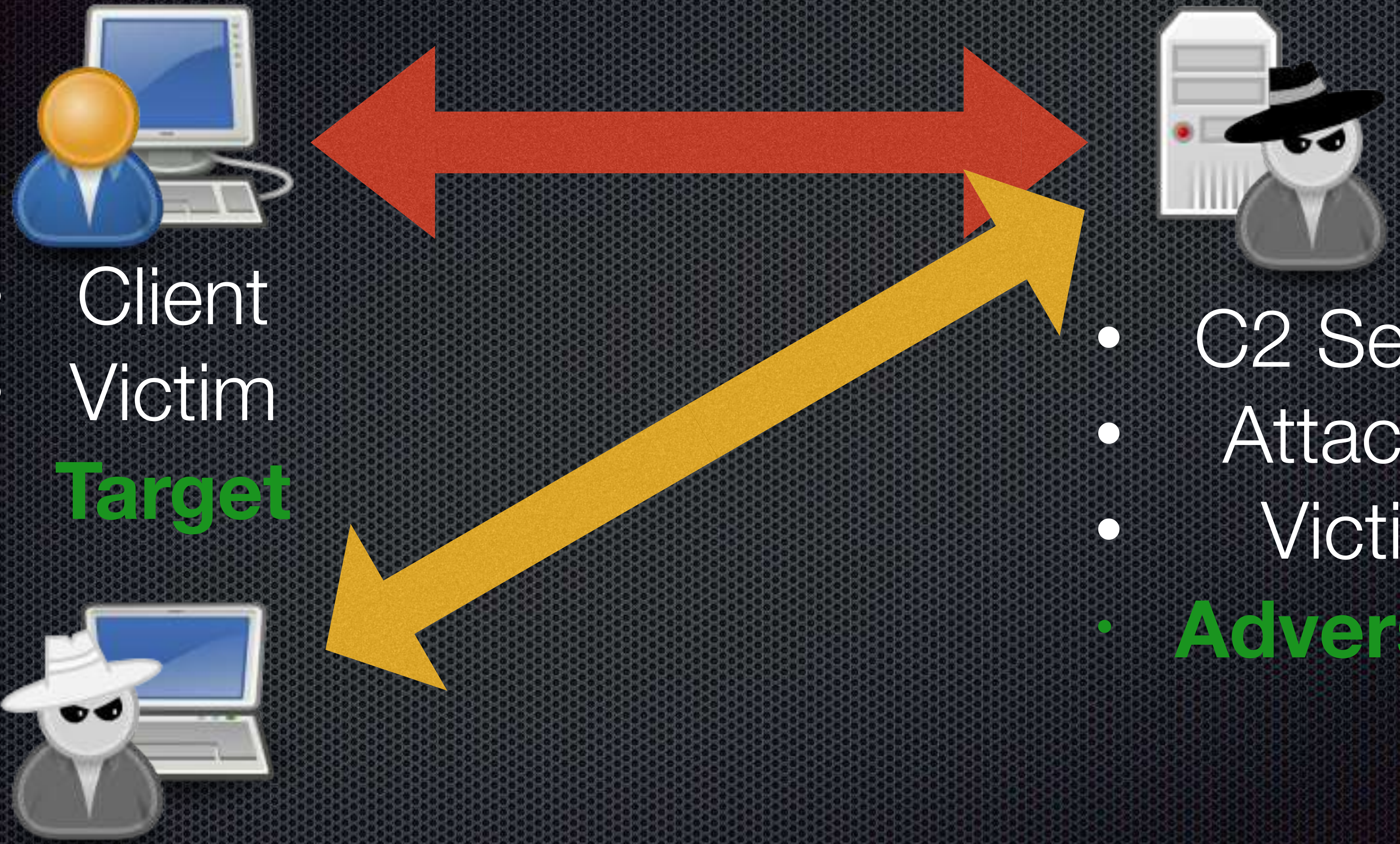
1) establish attribution of criminal activity to share with law enforcement and other United States Government agencies responsible for cybersecurity;

2) disrupt continued unauthorized activity against the victim’s own network; or

3) monitor the behavior of an attacker to assist in developing future intrusion prevention or cyber defense techniques, but;

```
>$ killall -s SIGKILL rants
```

RAT terminology



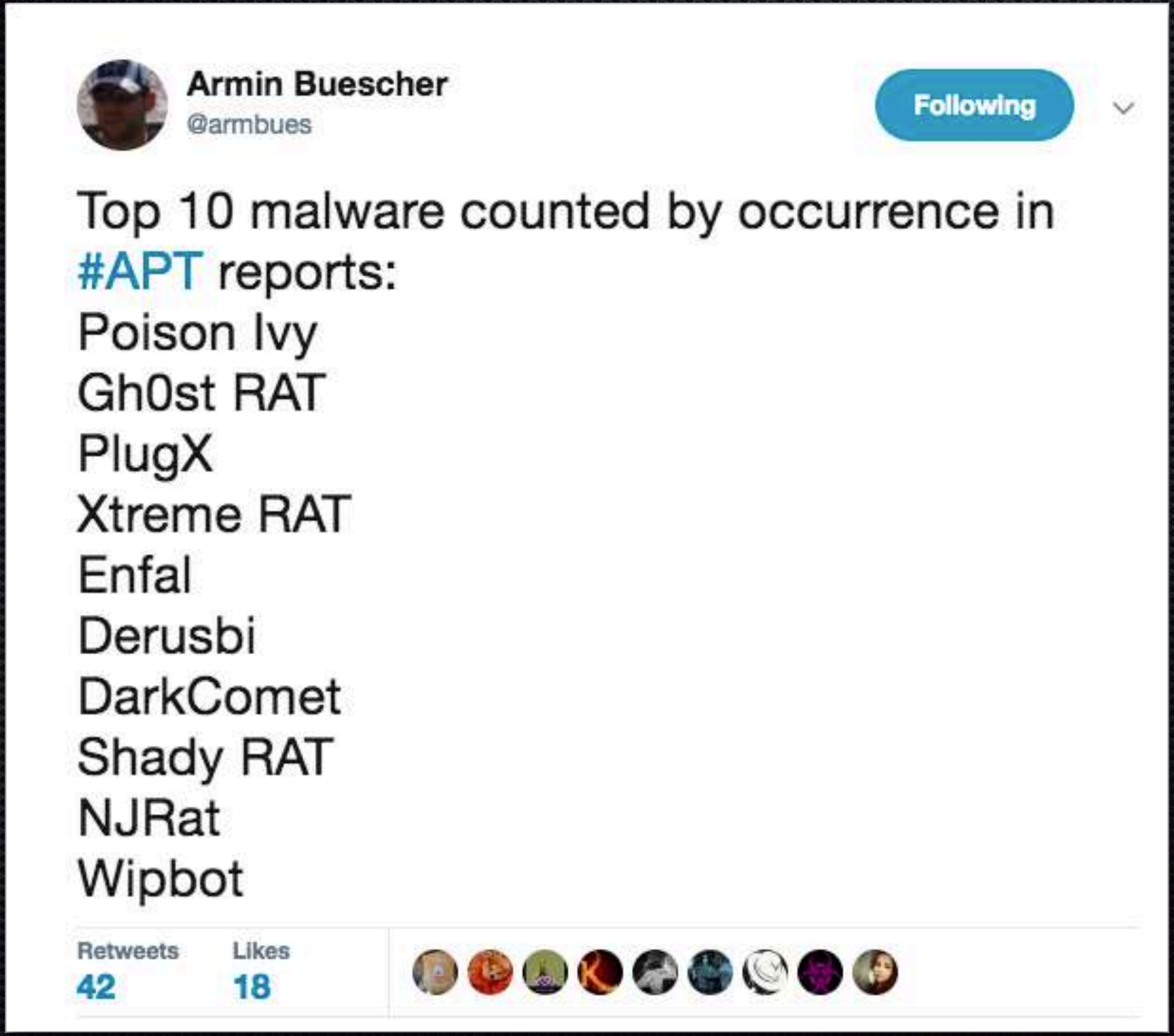
- Client
- Victim
- **Target**

- C2 Server
- Attacker
- Victim
- **Adversary**

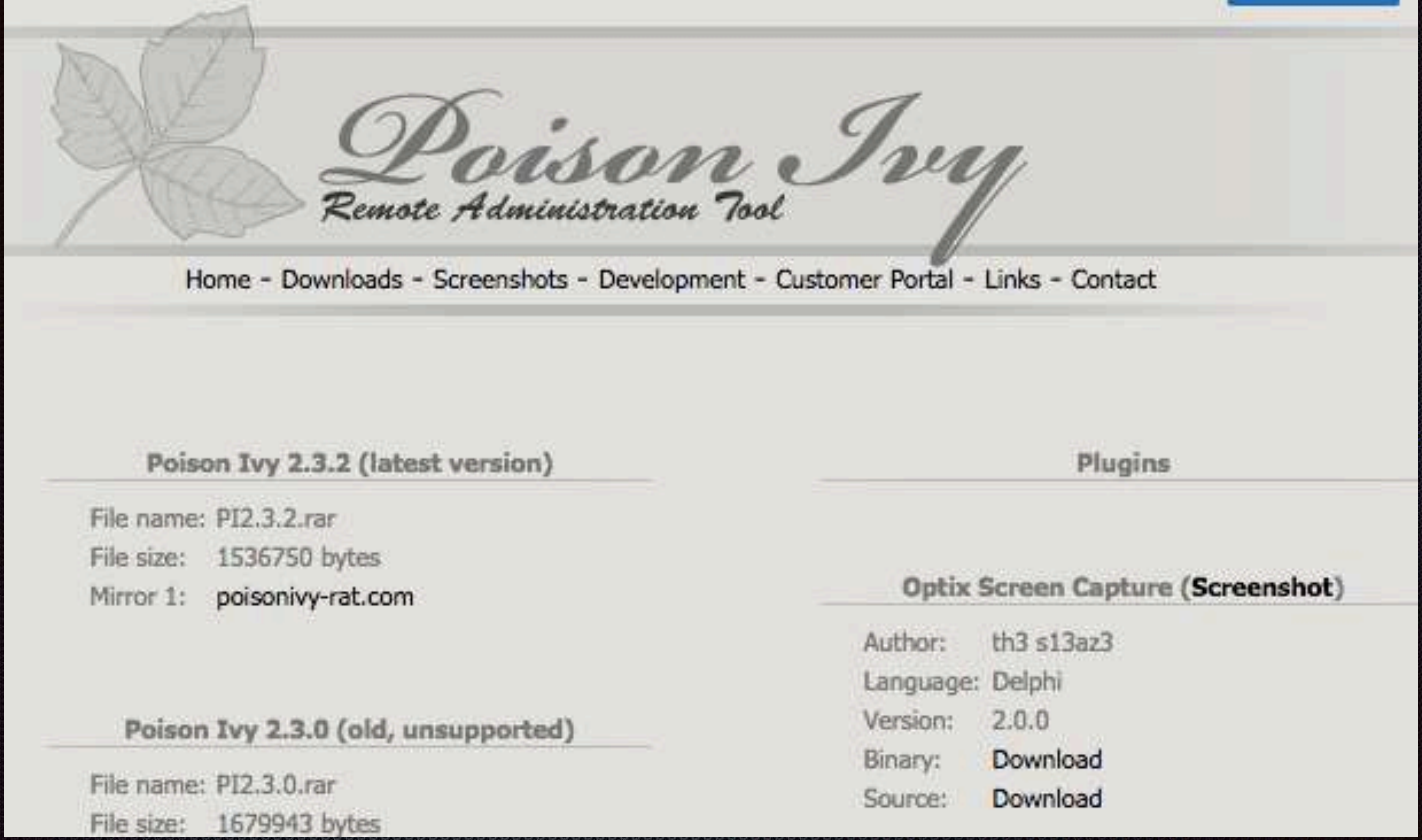
- **Retaliator** - one who returns assault in kind

*icons credit Open Security Architecture

Sophisticated attack hit list



Top 10 malware counted by occurrence in #APT reports:
Poison Ivy
Gh0st RAT
PlugX
Xtreme RAT
Enfal
Derusbi
DarkComet
Shady RAT
NJRat
Wipbot



Poison Ivy
Remote Administration Tool

Home - Downloads - Screenshots - Development - Customer Portal - Links - Contact

Poison Ivy 2.3.2 (latest version)

File name: PI2.3.2.rar
File size: 1536750 bytes
Mirror 1: poisonivy-rat.com

Poison Ivy 2.3.0 (old, unsupported)

File name: PI2.3.0.rar
File size: 1679943 bytes

Plugins

Optix Screen Capture (Screenshot)

Author: th3 s13az3
Language: Delphi
Version: 2.0.0
Binary: Download
Source: Download

- Buffer overflow exploit by Andrzej Dereszowski
- Follow on work by Jos Wetzels

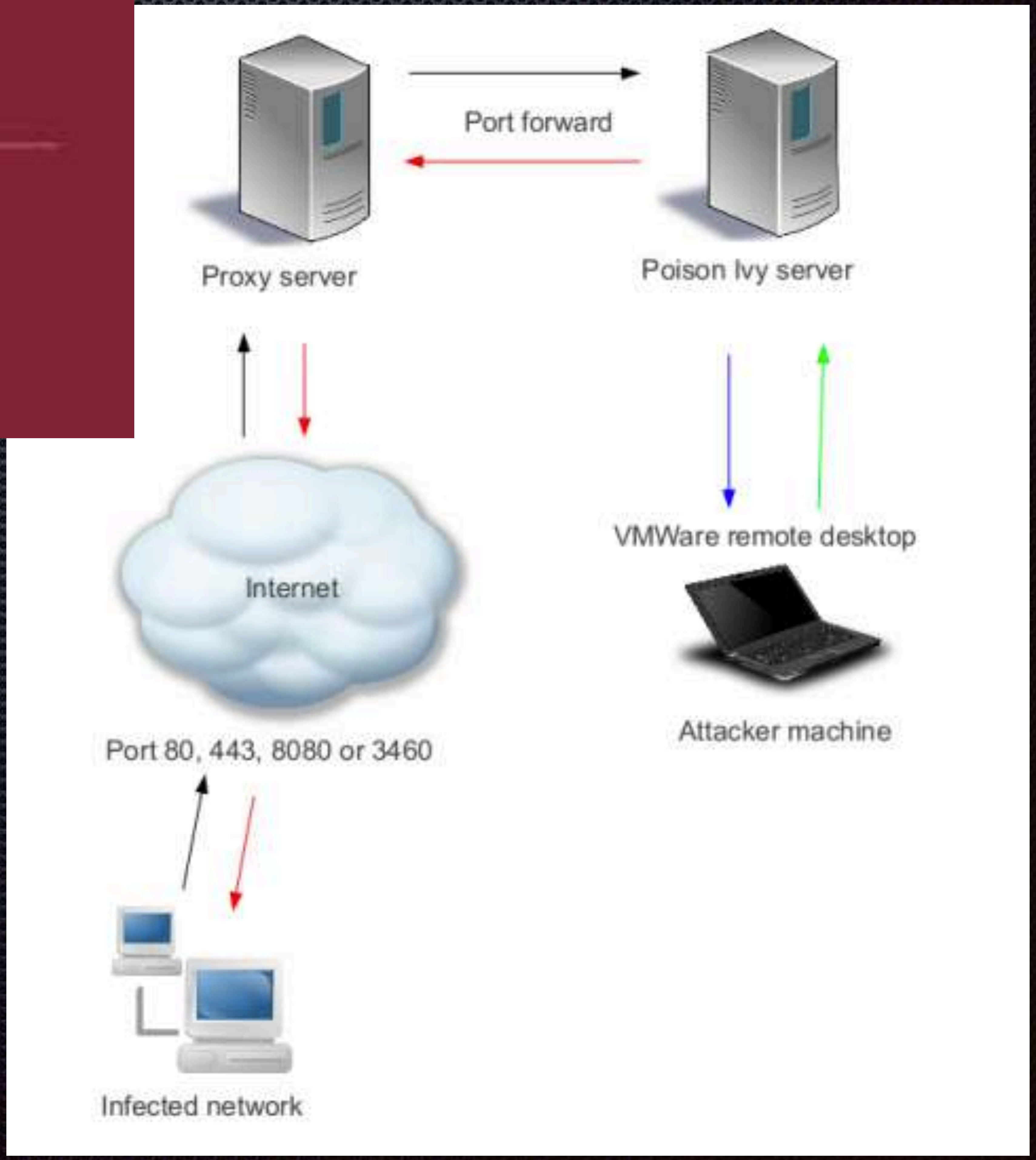
APT1 & Poison Ivy

malware.lu

itrust consulting

APT1

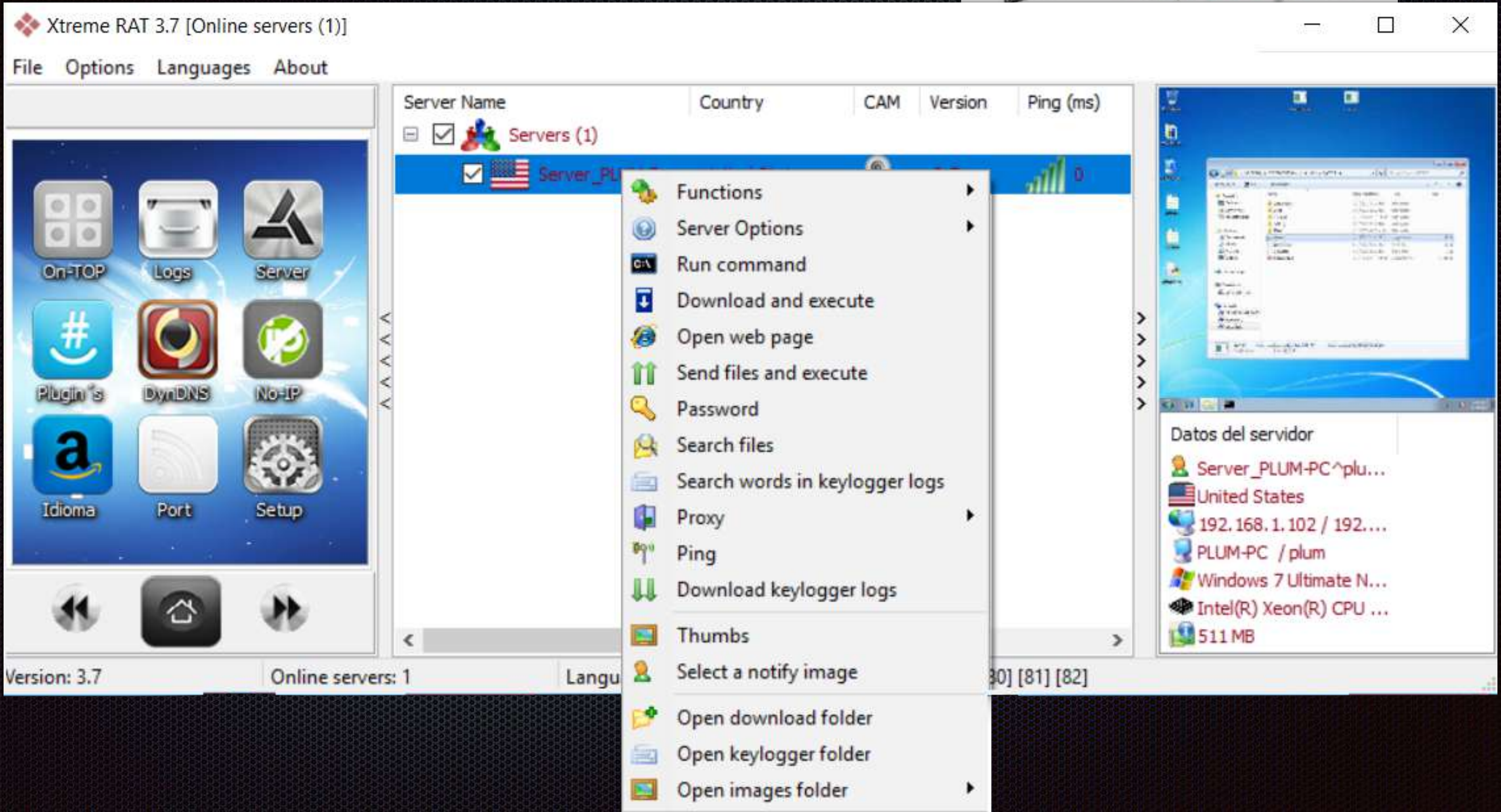
MANDIANT



- Remote file download exploit by Shawn Denbow and Jesse Hertz
- Follow on work by Jos Wetzels

```
>$ chmod +r new_exploits
```

Xtreme RAT



Xtreme RAT 3.7 [Online servers (1)]

Datos del servidor

Server_PLUM-PC^plu...
United States
192.168.1.102 / 192....
PLUM-PC / plum
Windows 7 Ultimate N...
Intel(R) Xeon(R) CPU ...
511 MB

Version: 3.7 | Online servers: 1 | Langu... | ...0] [81] [82]

Xtreme RAT Targets Israeli Government

Posted on: October 29, 2012 at 8:33 pm Posted in: Malware, Spam

(Threat Research Manager)

Packrat: Seven Years of a South American Threat Actor

December 8, 2015

Tagged: Argentina, Brazil, Disinformation, Ecuador, South America

Categories: Author, Claudio Guarnieri, John Scott-R

Authors: John Scott-Railton*, Morgan Ma

Senior Researcher, Citizen Lab, Munk School of

Read the pr

Media cove

World, Globa

Summ

W32.Extrat: Syrian Conflict Used To Deliver Xtreme RAT

By: Satnam Narang SYMANTEC EMPLOYEE

8 Jan 2013

2

utor: Jeet

Gaza cybergang, where's your IR team?

mber 28, 2015, 8:00 am

Xtreme RAT cyberespionage targeted U.S., U.K. governments

The recen

Hackers dropping Zeus in favour of Xtreme RAT Trojan, reports FireEye

RATs more powerful than banking Trojans, says FireEye

raeli police a

's say

Spyware malware found in Mexico's government

Researchers at cybersecurity firm Arbor Networks have located Xtreme RAT Access Trojan) malware in the Mexican government's computer systems, a malicious activities found on its infrastructure.

June 03, 2014

Molerats campaign turns to Xtreme RAT to target orgs

Attackers targeting organizations across the globe are now opting to use a freely available remote access trojan called Xtreme RAT for their exploits.

On Monday, researchers at FireEye detailed in a blog post how the attack campaign, dubbed "Molerats," has been ongoing since October 2011.

XTREMERAT MALWARE TARGETS ISRAELI GOVERNMENT AGENCY

January 27, 2014 , 1:28 pm

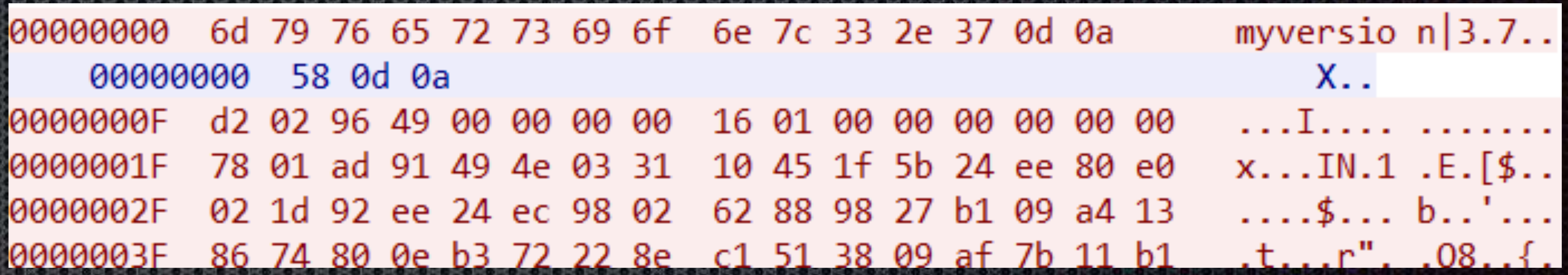
by Michael Mimoso Follow @mike_mimoso

Espionage malware used in attacks against Israel, as well as Syrian activists, in the last 18 months has been linked to a new attack against Israel's Civil Administration, the rning body in the West Bank.

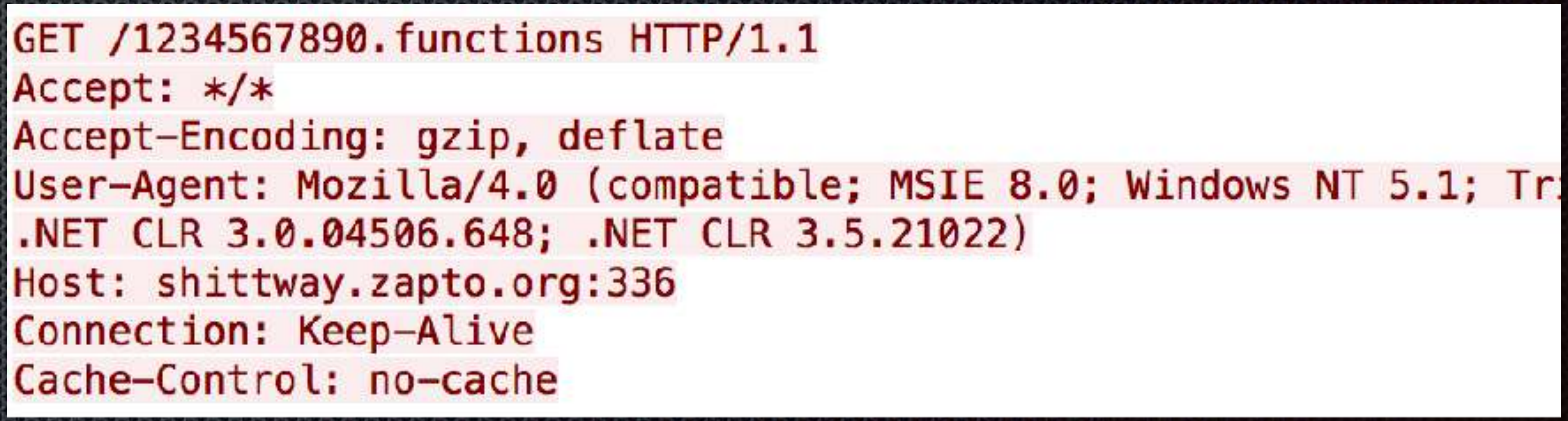
les of XtremeRAT, a data-stealing come

Xtreme Rat

- TCP connection starts with the string “myversion|3.x\r\n”
- C2 responds with “X\r\n”
- Alternatively Xtreme rat can use a fake HTTP request of the form GET /[0-9]{1,10}.functions

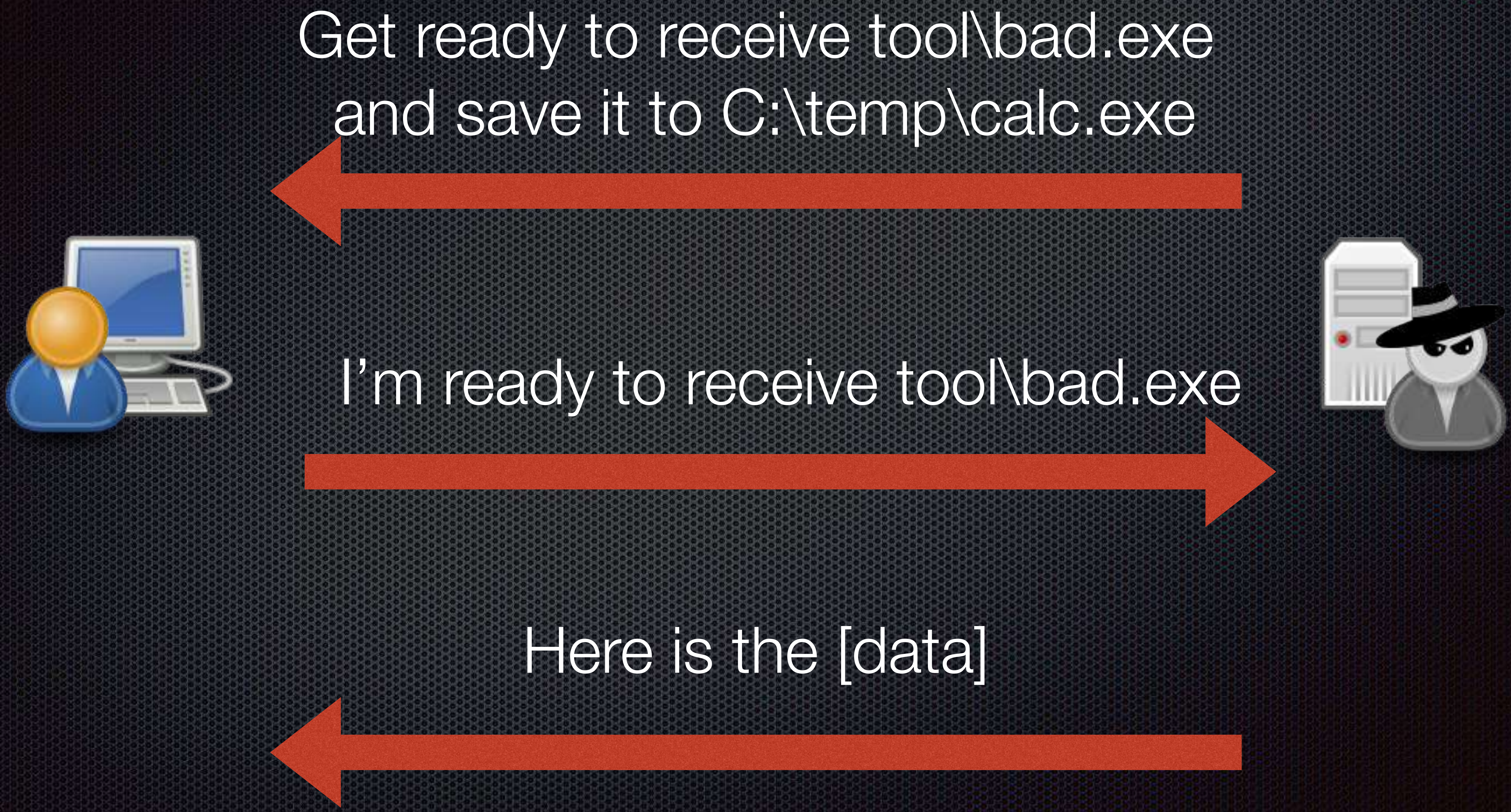


```
00000000  6d 79 76 65 72 73 69 6f  6e 7c 33 2e 37 0d 0a       myversio n|3.7..
    00000000  58 0d 0a                                              X..
0000000F  d2 02 96 49 00 00 00 00  16 01 00 00 00 00 00 00   ...I.... .......
0000001F  78 01 ad 91 49 4e 03 31  10 45 1f 5b 24 ee 80 e0   x...IN.1 .E.[$..
0000002F  02 1d 92 ee 24 ec 98 02  62 88 98 27 b1 09 a4 13   ....$... b..'...
0000003F  86 74 80 0e b3 72 22 8e  c1 51 38 09 af 7b 11 b1   .t...r". .Q8..{.
```



```
GET /1234567890.functions HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Tr
.NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: shittway.zapto.org:336
Connection: Keep-Alive
Cache-Control: no-cache
```

Remote file upload



Get ready to receive tool\bad.exe
and save it to C:\temp\calc.exe

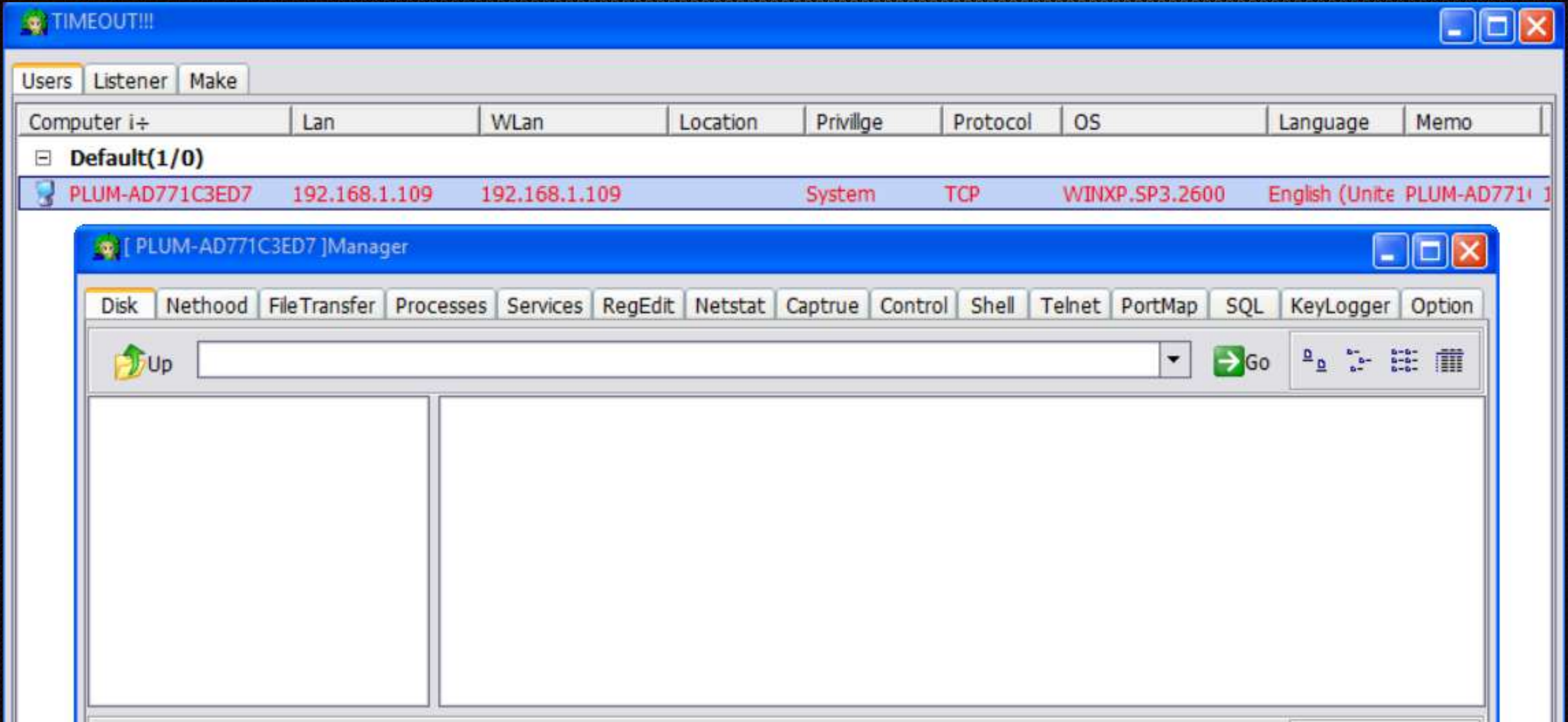
I’m ready to receive tool\bad.exe

Here is the [data]

Remote file download

- Win.ini (Sanity check)
- Event logs
- desktop.ini
- %SYSTEMROOT%\repair\SAM
- %SYSTEMROOT%\repair\system
- https://attackerkb.com/Windows/blind_files

PlugX / Korplug / Destory



Computer i÷	Lan	WLan	Location	Privillge	Protocol	OS	Language	Memo
Default(1/0)								
PLUM-AD771C3ED7	192.168.1.109	192.168.1.109		System	TCP	WINXP.SP3.2600	English (Unite	PLUM-AD771(1

Korplug military targeted attacks: Afghanistan & Tajikistan

BY ROBERT LIPOVSKY POSTED 12 NOV 2014 - 03:17PM

RAT

PlugX: New Tool For a Not So New Campaign

Posted on: September 10, 2012 at 10:00 am Poste

Author: Rol

her)

PlugX used against Mongolian targets

Snorre Fagerland - November 24, 2013

The Chinese backdoor trojan PlugX has been used in a number of

a long, gradual development, and is now considered one

indicated.

in a binary blob

Backdoor.Korplug: Loading Malicious Components Through Trusted Applications

By: Andrea Lelli

Report: PlugX Is RAT of Choice for Nation States

By Sean Michael Kerner, Posted February 13, 2015

details tactics used in nation-state attacks.

February 27, 2015

PlugX APT group uses backdoor in India campaign

A campaign aimed at organizations in India stretching out

and evolving, according to

Operation Cloud Hopper – APT10 goes after Managed Service Providers

April 6, 2017 By Pierluigi Paganini

12 FEB 2015 NEWS

China, Vietnam and PlugX Dominate APT Landscape

Tara Seals US/North America News Reporter, Infosecurity Magazine

Email Tara

ities in the advanced persistent threat

targeted country

OOPS, THEY DID IT AGAIN: APT TARGETS RUSSIA AND BELARUS WITH ZEROT AND PLUGX

FEBRUARY 02, 2017 Darien Huss, Pierre T, Axel F and Proofpoint Staff

The connection between the Plugx Chinese gang and the latest Internet Explorer Zeroday

SEPTEMBER

PlugX RAT Used to Gather Intel on Afghan, Russian Military: Report

Eduard Kovacs on November 13, 2014

Share 26 G+1 5 Tweet Recommend 13 RSS

he notorious remote access Trojan (RAT) known as PlugX (Korplug) has been use

in Afghanistan, Russia, Tajikistan, Kazakhstan and

SOPHOS

Security made simple.

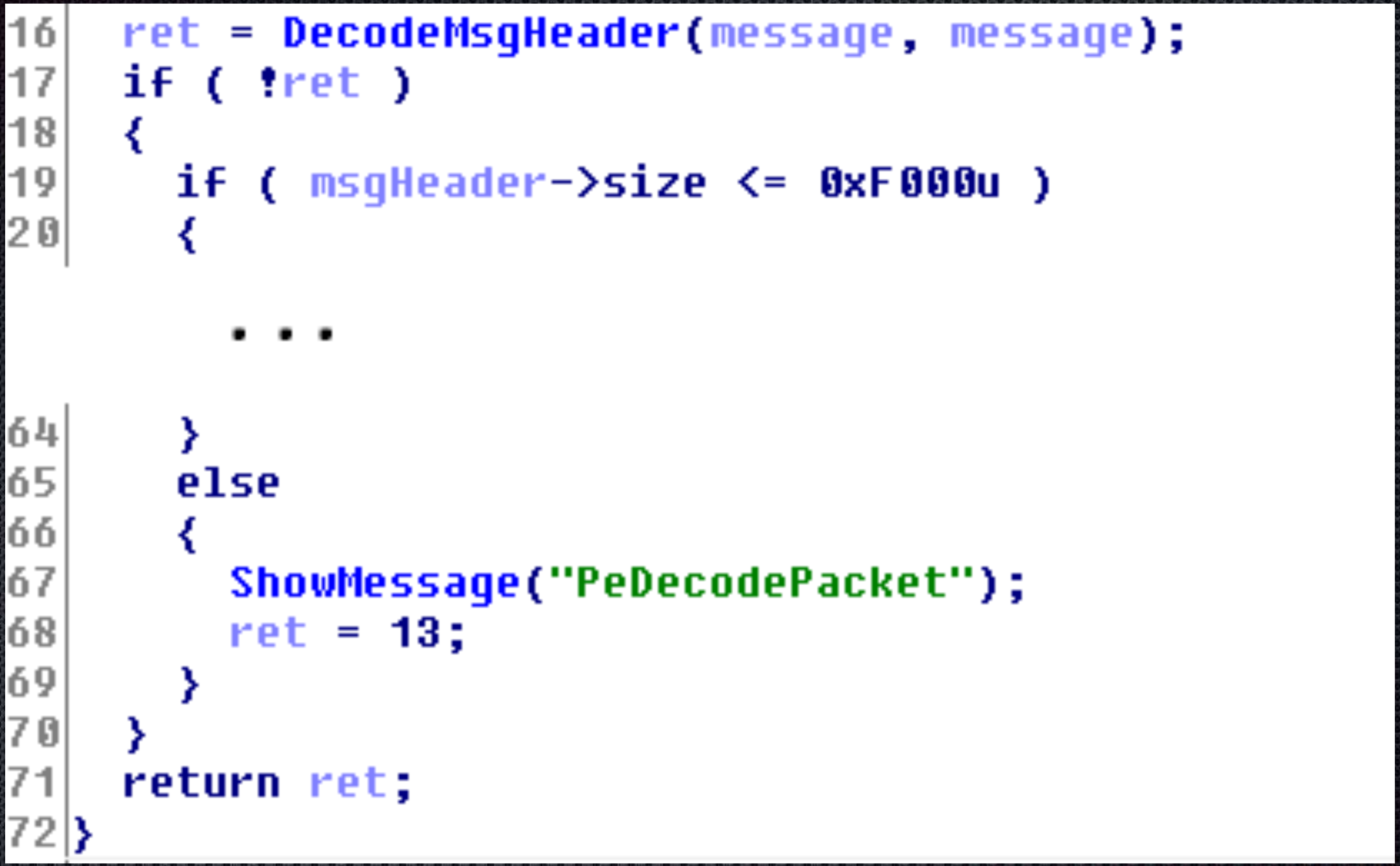
PlugX – The Next Generation

black hat ASIA 2014

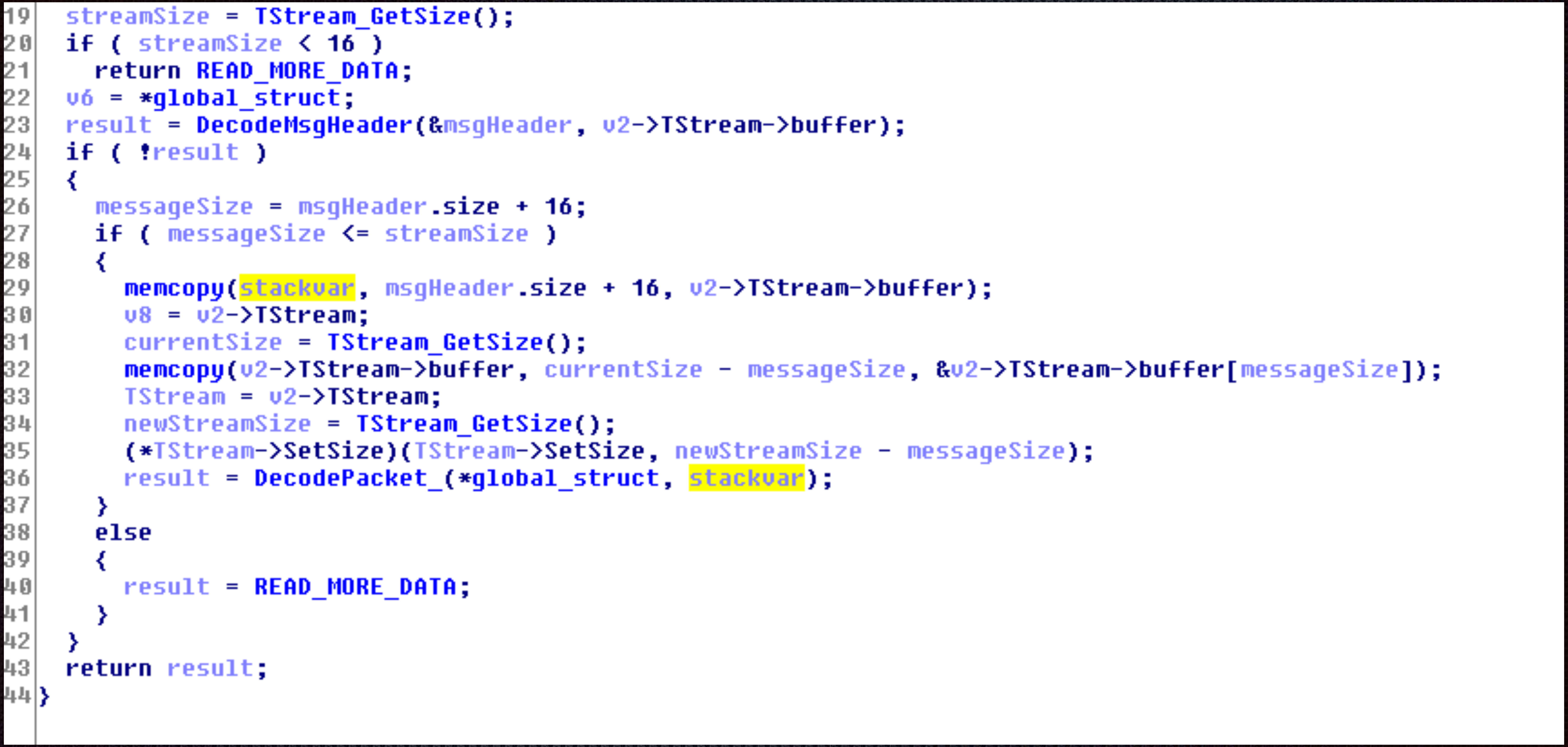
I Know You Want Me - Unplugging PlugX

Takahiro Haruyama / Hiroshi Suzuki

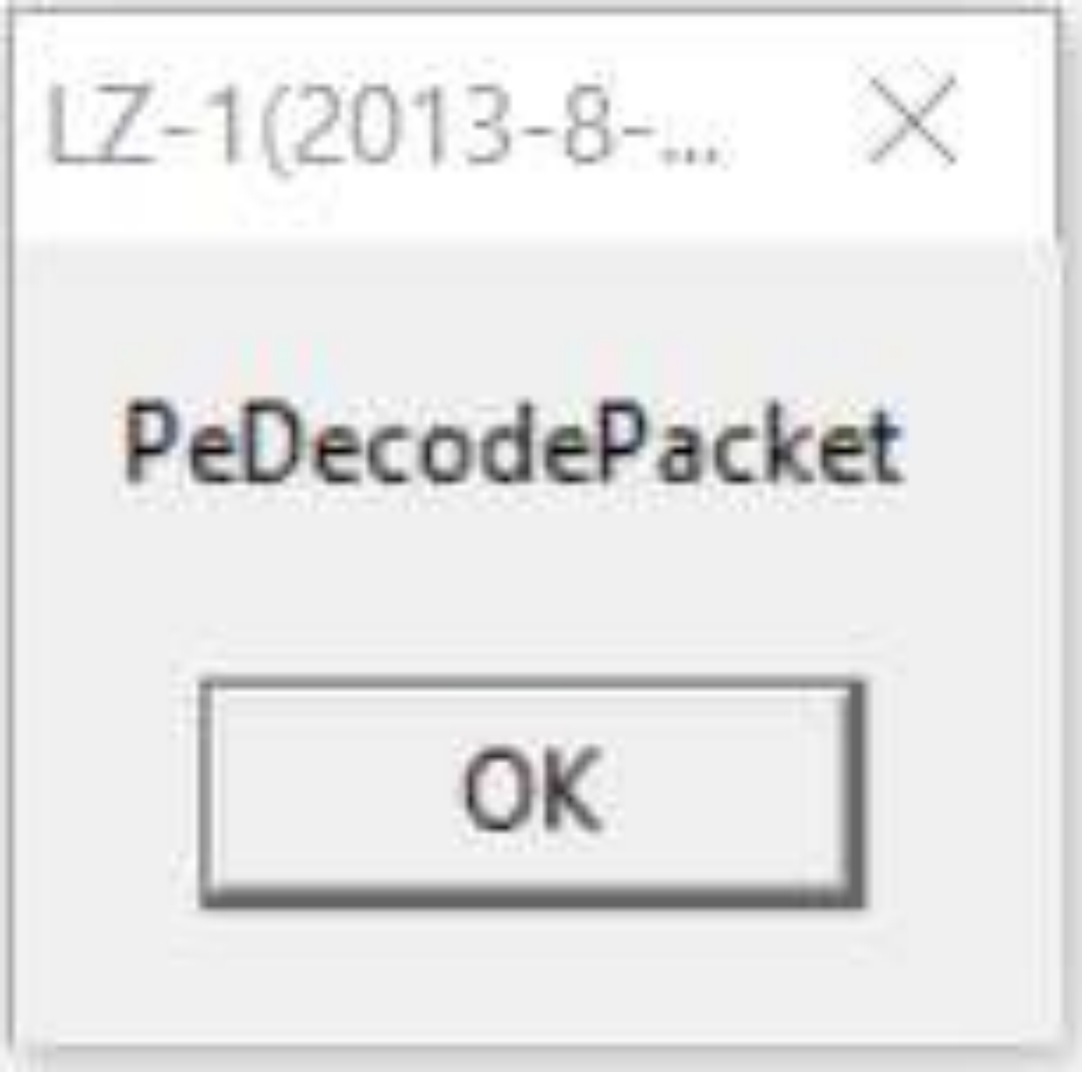
Internet Initiative Japan Inc.



```
  ret = DecodeMsgHeader(message, message);
  if ( !ret )
  {
    if ( msgHeader->size <= 0xF000u )
    {

      . . .

    }
    else
    {
      ShowMessage("PeDecodePacket");
      ret = 13;
    }
  }
  return ret;
}
```



```
  streamSize = TStream_GetSize();
  if ( streamSize < 16 )
    return READ_MORE_DATA;
  v6 = *global_struct;
  result = DecodeMsgHeader(&msgHeader, v2->TStream->buffer);
  if ( !result )
  {
    messageSize = msgHeader.size + 16;
    if ( messageSize <= streamSize )
    {
      memcopy(stackvar, msgHeader.size + 16, v2->TStream->buffer);
      v8 = v2->TStream;
      currentSize = TStream_GetSize();
      memcopy(v2->TStream->buffer, currentSize - messageSize, &v2->TStream->buffer[messageSize]);
      TStream = v2->TStream;
      newStreamSize = TStream_GetSize();
      (*TStream->SetSize)(TStream->SetSize, newStreamSize - messageSize);
      result = DecodePacket_(*global_struct, stackvar);
    }
    else
    {
      result = READ_MORE_DATA;
    }
  }
  return result;
}
```



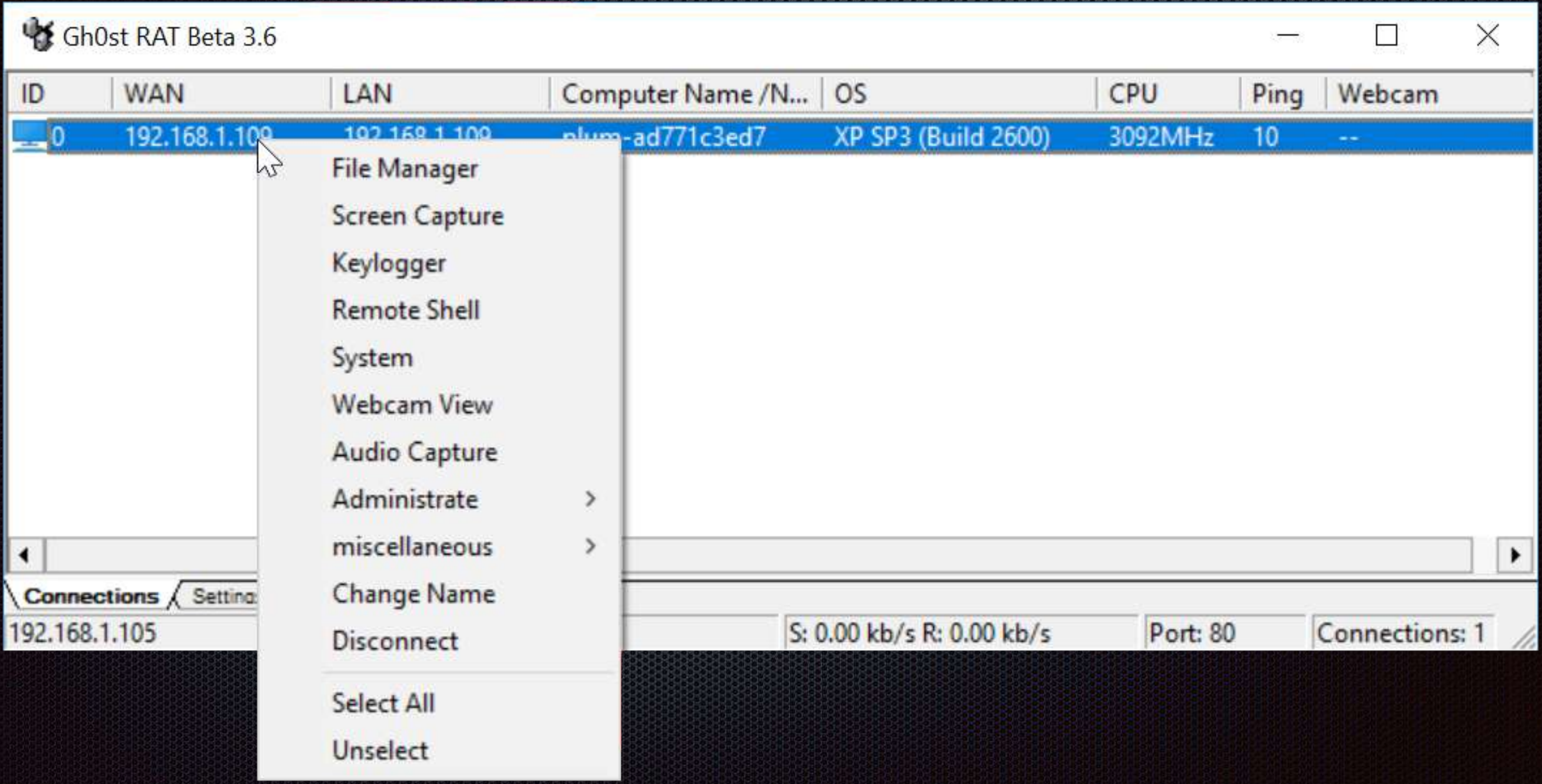
LZ-1(2013-8-...

PeDecodePacket

Oracle VM VirtualBox Manager
2:51 PM
plum@Ballroom: ~
Windows 10 (Gh0st) [Running] - Oracle VM VirtualBox
Record
Show/hide Main Window
Select Area On Screen
About
Quit
Recycle Bin
RATs
PlugX.exe
data
ENG
1:51 PM
6/20/2017
2
Right Ctrl

```
plum@Ballroom:~$ msfconsole
The PGconn, PGresult, and PGError constants are deprecated, and will be
removed as of version 1.0.

You should use PG::Connection, PG::Result, and PG::Error instead, respectively.

Called from /opt/metasploit-framework/embedded/lib/ruby/gems/2.4.0/gems/activesupport-4
.2.8/lib/active_support/dependencies.rb:274:in `block in require'

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v4.14.28-dev-                        ]
+ -- --=[ 1663 exploits - 951 auxiliary - 293 post        ]
+ -- --=[ 486 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

Gh0st RAT



ID	WAN	LAN	Computer Name /N...	OS	CPU	Ping	Webcam
0	192.168.1.109	192.168.1.109	plum-ad771c3ed7	XP SP3 (Build 2600)	3092MHz	10	--

192.168.1.105 S: 0.00 kb/s R: 0.00 kb/s Port: 80 Connections: 1

ware > Musical Chairs: Multi-Year Campaign Involving New Variant of Gh0st Malware

Chairs: Multi-Year Campaign Involving New Variant of Gh0st Malware

andon Levene, Robert Falcone and Jen Miller-Osborn
mber 8, 2015 at 12:15 PM
gory: Malwar Prevention, Unit 42 Tag

TECHNOLOGY

Vast Spy System Loots Computers in 103 Coun

The VOHO campaign: Gh0st RAT spread by water-holing

campaign was first chronicled by RSA in July, when it coined the phrase 'water holing'. holing VOHO campaign. What at first

Infamous RAT "Gh 0st RAT", used in targeted attacks targeting Taiwan

Posted on July 11, 2013

Threat C

Amnesty UK website hacked to serve lethal Gh0st RAT Trojan

esty International's UK website was hacked to host the dangerous Gh0st RAT Trojan his week, security firm Websense has revealed.
| May 11, 2012

as hacked to host the dangerous Gh0st RAT has revealed.
E-2012-0507 Java vuln visitors would ha

Human Rights organisation website Serves Gh0st RAT Trojan

Mohit Kumar

G20 2014 Summit Lure used to target Tibetan activists

BY ESET RESEARCH POSTED 14 NOV 2014 - 03:29PM

GOVERNMENT

'Night Dragon' Attacks From China Strike Energy Companies

Kunming Attack Leads to Gh0st RAT Variant

Posted on: March 13, 2014 at 9:30 am Posted in: Malware
Author: Kervin Alintanahin (Threats Analyst)

rating Hustle, Chinese APT kly Use Zero-Day E-2015-5119) Follo eak

eat Research

NEWS

Gh0stRAT malware attacks continue,

Many advanced persistent threat attacks use the malware, bel developed in China

The many faces of Gh0st Rat

Plotting the conn

Tracking GhostNet:

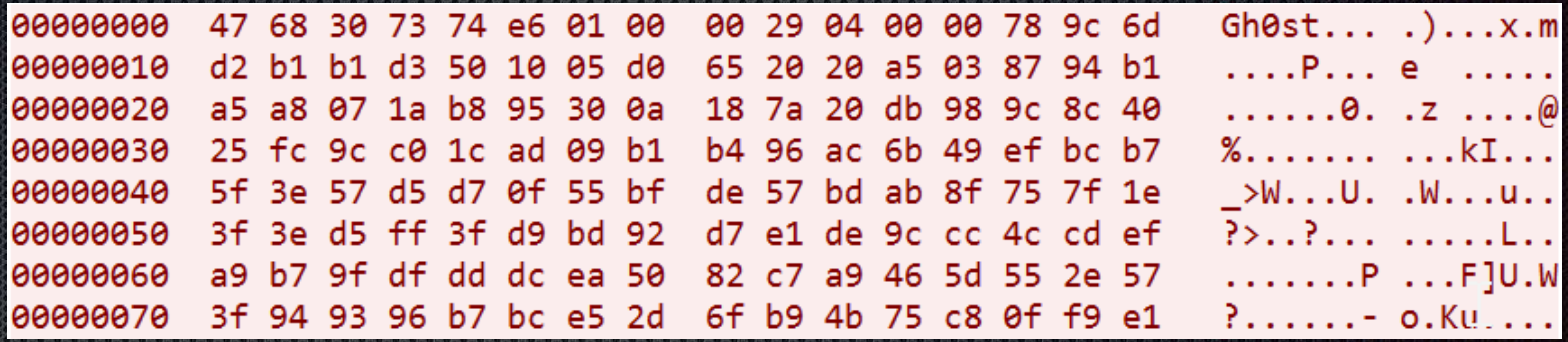
Investigating a Cyber Espionage Network

ETERNALBLUE EXPLOIT SPREADING GH0ST RAT,

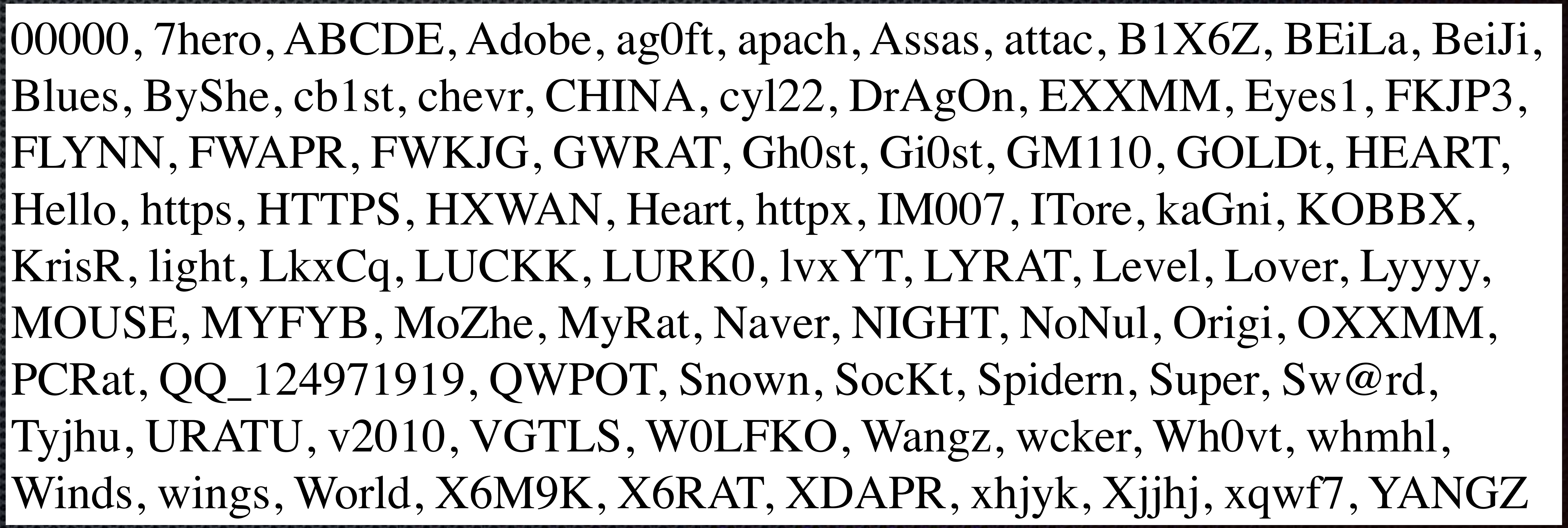
n Spring

Gh0st RAT

- Most notably identified by C2 traffic which start with the 5 byte marker “Gh0st” (or other 5 byte marker)



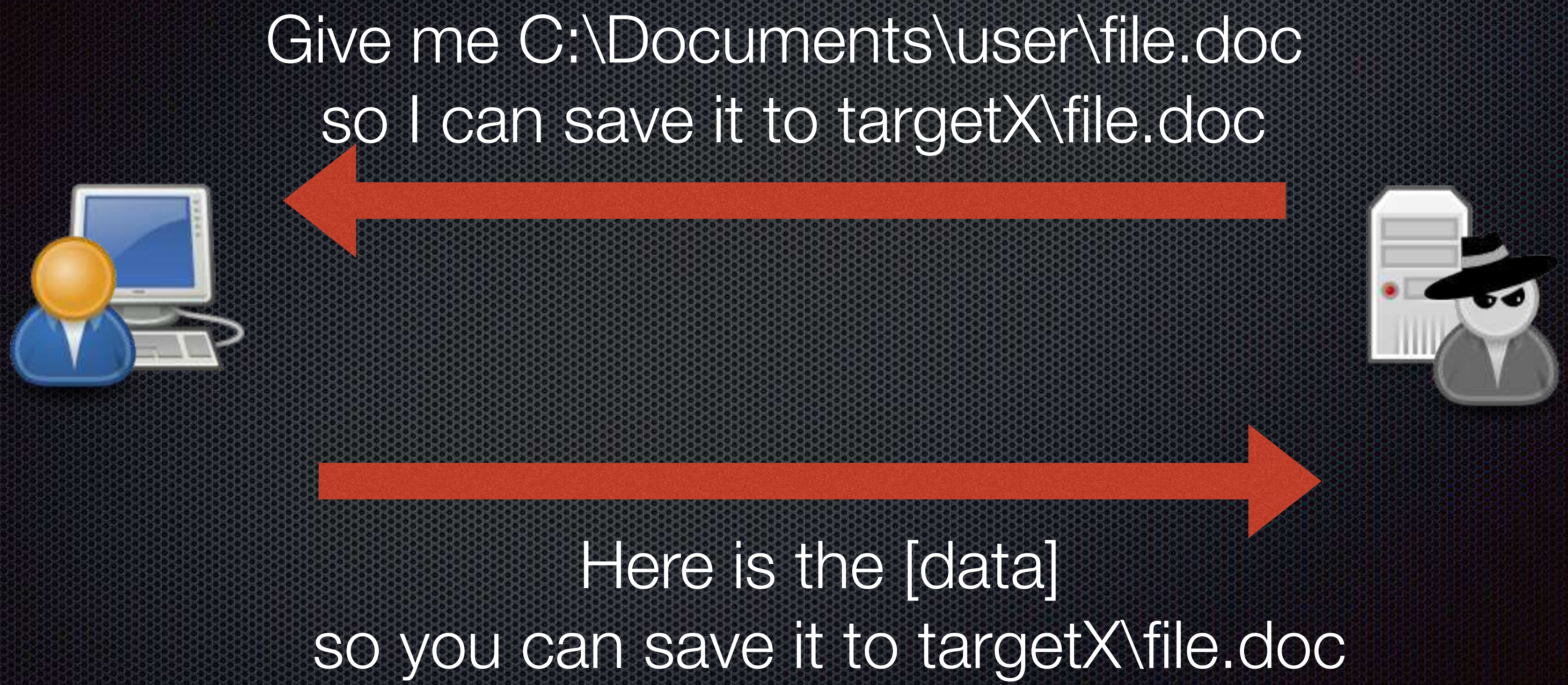
```
00000000  47 68 30 73 74 e6 01 00  00 29 04 00 00 78 9c 6d   Gh0st... .)...x.m
00000010  d2 b1 b1 d3 50 10 05 d0  65 20 20 a5 03 87 94 b1   ....P... e  .....
00000020  a5 a8 07 1a b8 95 30 0a  18 7a 20 db 98 9c 8c 40   ......0. .z ....@
00000030  25 fc 9c c0 1c ad 09 b1  b4 96 ac 6b 49 ef bc b7   %....... ...kI...
00000040  5f 3e 57 d5 d7 0f 55 bf  de 57 bd ab 8f 75 7f 1e   _>W...U. .W...u..
00000050  3f 3e d5 ff 3f d9 bd 92  d7 e1 de 9c cc 4c cd ef   ?>..?... .....L..
00000060  a9 b7 9f df dd dc ea 50  82 c7 a9 46 5d 55 2e 57   .......P ...F]U.W
00000070  3f 94 93 96 b7 bc e5 2d  6f b9 4b 75 c8 0f f9 e1   ?......- o.Ku....
```



00000, 7hero, ABCDE, Adobe, ag0ft, apach, Assas, attac, B1X6Z, BEiLa, BeiJi, Blues, ByShe, cb1st, chevr, CHINA, cyl22, DrAgOn, EXXMM, Eyes1, FKJP3, FLYNN, FWAPR, FWKJG, GWRAT, Gh0st, Gi0st, GM110, GOLDt, HEART, Hello, https, HTTPS, HXWAN, Heart, httpx, IM007, ITore, kaGni, KOBBX, KrisR, light, LkxCq, LUCKK, LURK0, lvxYT, LYRAT, Level, Lover, Lyyyy, MOUSE, MYFYB, MoZhe, MyRat, Naver, NIGHT, NoNul, Origi, OXXMM, PCRat, QQ_124971919, QWPOT, Snown, SocKt, Spidern, Super, Sw@rd, Tyjhu, URATU, v2010, VGTLS, W0LFKO, Wangz, wcker, Wh0vt, whmhl, Winds, wings, World, X6M9K, X6RAT, XDAPR, xhjyk, Xjjhj, xqwf7, YANGZ

“The many faces of Gh0st Rat” — Snorre Fagerland

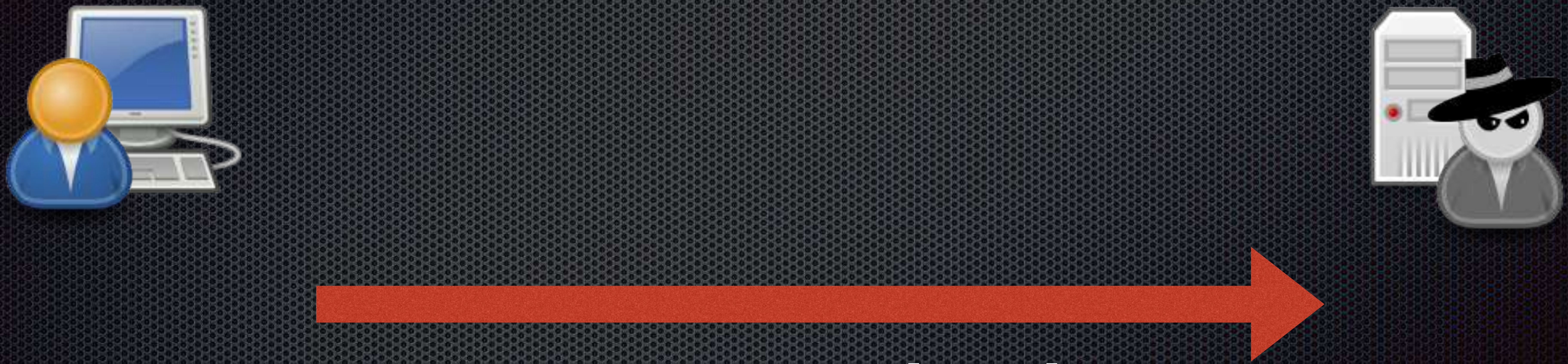
Remote file upload



Give me C:\Documents\user\file.doc
so I can save it to targetX\file.doc

Here is the [data]
so you can save it to targetX\file.doc

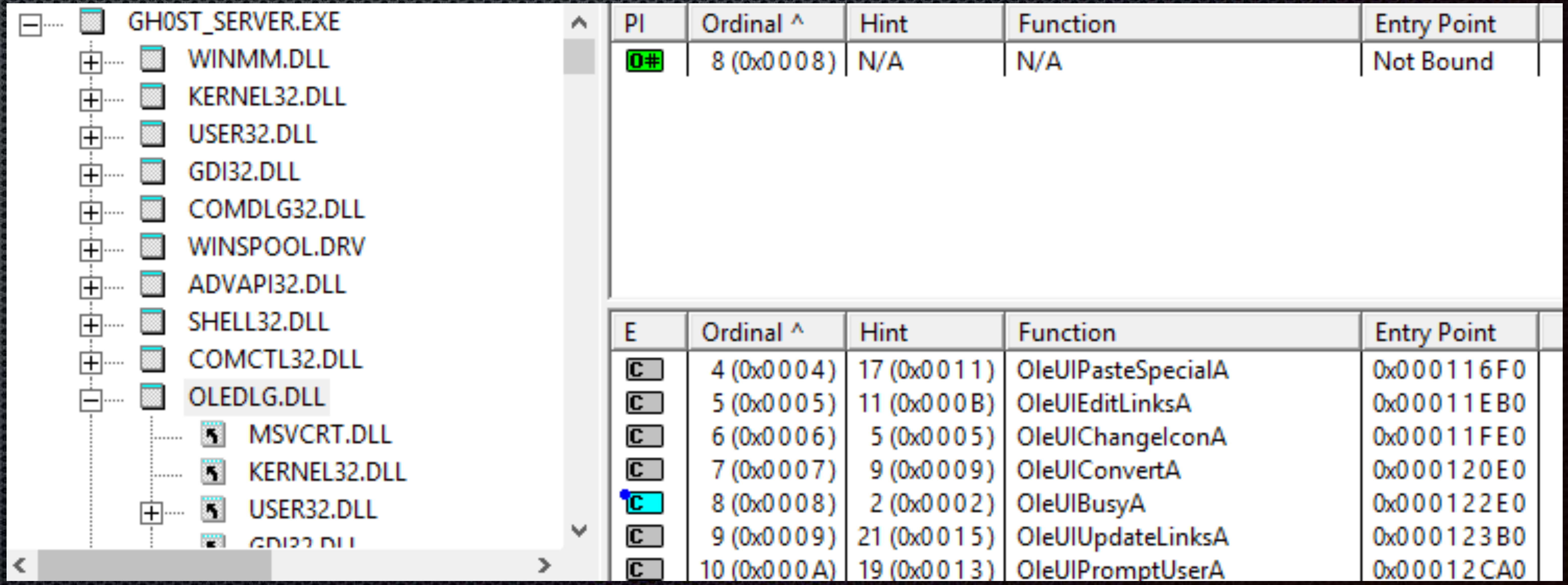
Remote file upload



Here is the [data]
so you can save it to C:\...\startup\backdoor.exe

DLL side load vulnerability

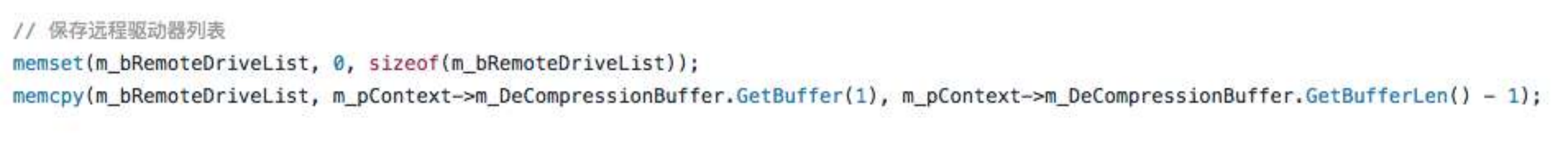
- Gh0st Server has a dependency on oledlg.dll
- Only imports one function
  - #8 OleUIBusyA(int)
- Return 1 and all is good



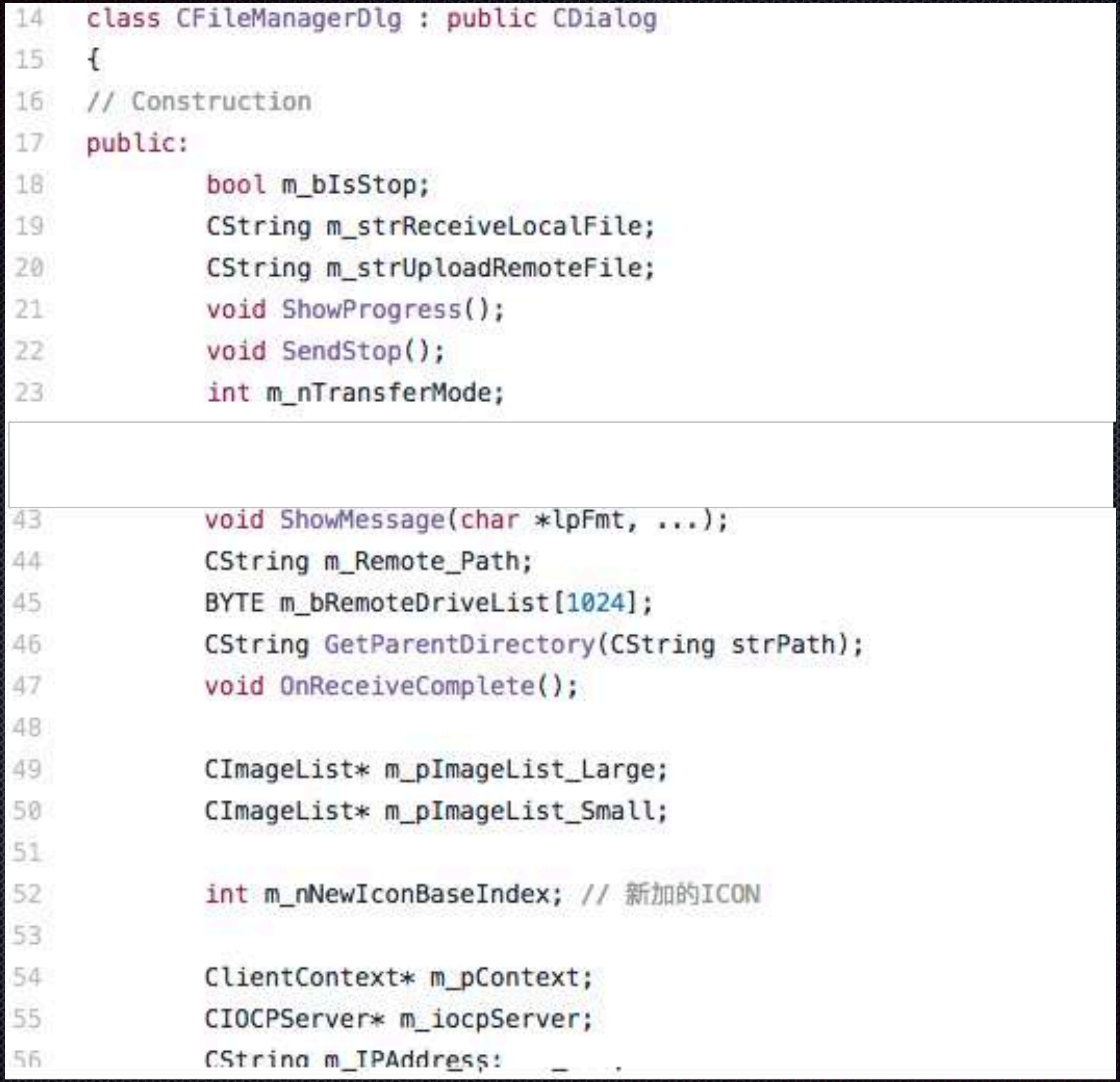
```
GH0ST_SERVER.EXE
    WINMM.DLL
    KERNEL32.DLL
    USER32.DLL
    GDI32.DLL
    COMDLG32.DLL
    WINSPOOL.DRV
    ADVAPI32.DLL
    SHELL32.DLL
    COMCTL32.DLL
    OLEDLG.DLL
        MSVCRT.DLL
        KERNEL32.DLL
        USER32.DLL
        GDI32.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
O#	8 (0x0008)	N/A	N/A	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	4 (0x0004)	17 (0x0011)	OleUIPasteSpecialA	0x000116F0
C	5 (0x0005)	11 (0x000B)	OleUIEditLinksA	0x00011EB0
C	6 (0x0006)	5 (0x0005)	OleUIChangeIconA	0x00011FE0
C	7 (0x0007)	9 (0x0009)	OleUIConvertA	0x000120E0
C	8 (0x0008)	2 (0x0002)	OleUIBusyA	0x000122E0
C	9 (0x0009)	21 (0x0015)	OleUIUpdateLinksA	0x000123B0
C	10 (0x000A)	19 (0x0013)	OleUIPromptUserA	0x00012CA0



```
// 保存远程驱动器列表
memset(m_bRemoteDriveList, 0, sizeof(m_bRemoteDriveList));
memcpy(m_bRemoteDriveList, m_pContext->m_DeCompressionBuffer.GetBuffer(1), m_pContext->m_DeCompressionBuffer.GetBufferLen() - 1);
```



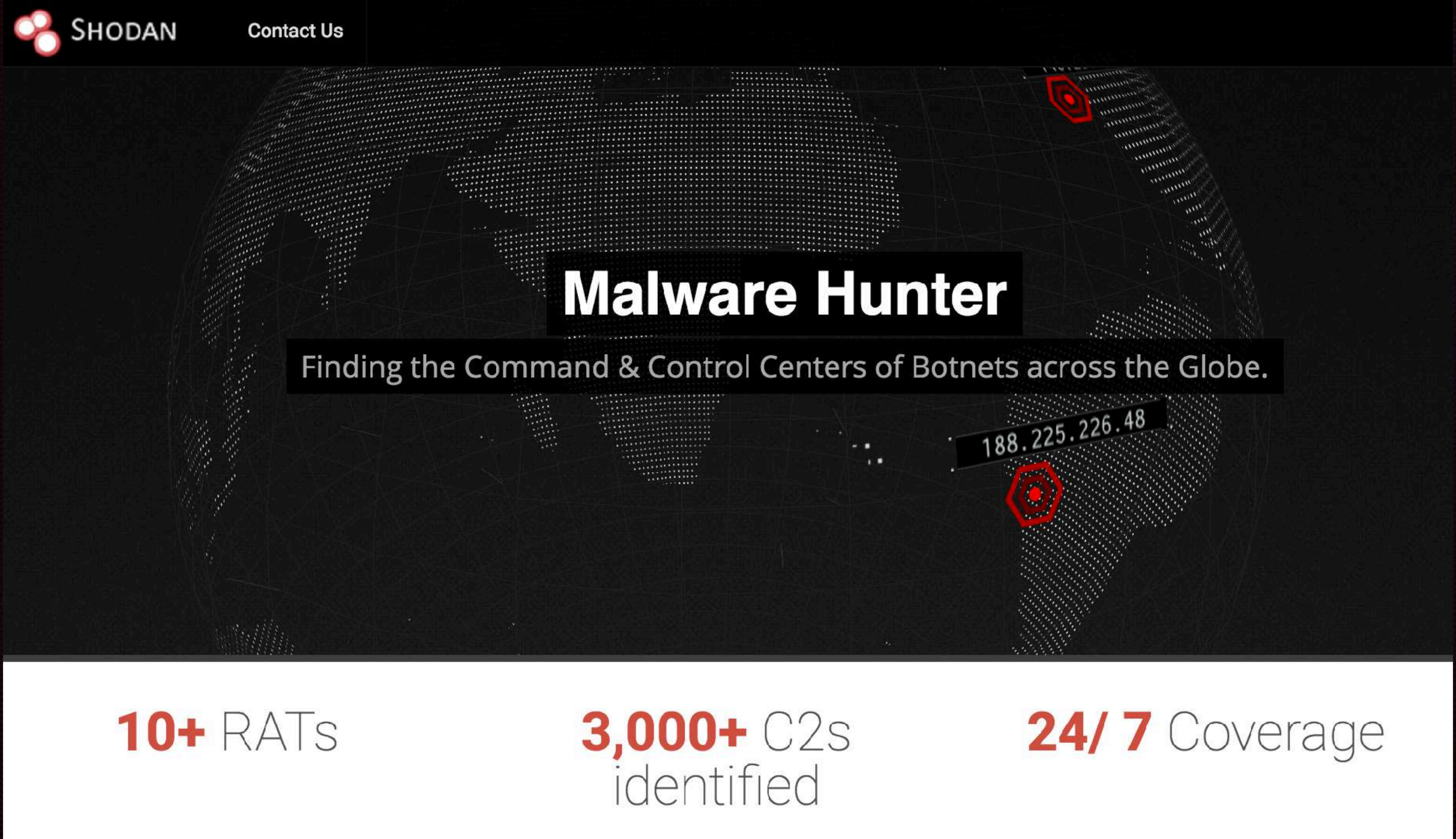
```
class CFileManagerDlg : public CDialog
{
// Construction
public:
        bool m_bIsStop;
        CString m_strReceiveLocalFile;
        CString m_strUploadRemoteFile;
        void ShowProgress();
        void SendStop();
        int m_nTransferMode;

        void ShowMessage(char *lpFmt, ...);
        CString m_Remote_Path;
        BYTE m_bRemoteDriveList[1024];
        CString GetParentDirectory(CString strPath);
        void OnReceiveComplete();

        CImageList* m_pImageList_Large;
        CImageList* m_pImageList_Small;

        int m_nNewIconBaseIndex; // 新加的ICON

        ClientContext* m_pContext;
        CIOCPServer* m_iocpServer;
        CString m_IPAddress;
```

Exploitation

- Control pointer to pointer
- Could use a information disclose vuln (if I had one)
- Thus, take the lazy man’s approach and heap spray
- DEP would break this but it also seems to break the EXE

Decode implant configs

- https://github.com/kevthehermit/RATDecoders
    - Gh0st
    - Xtreme Rat
    - Poision Ivy
    - DarkComet
    - Many others



Malware Hunter

Finding the Command & Control Centers of Botnets across the Globe.

10+ RATs

3,000+ C2s identified

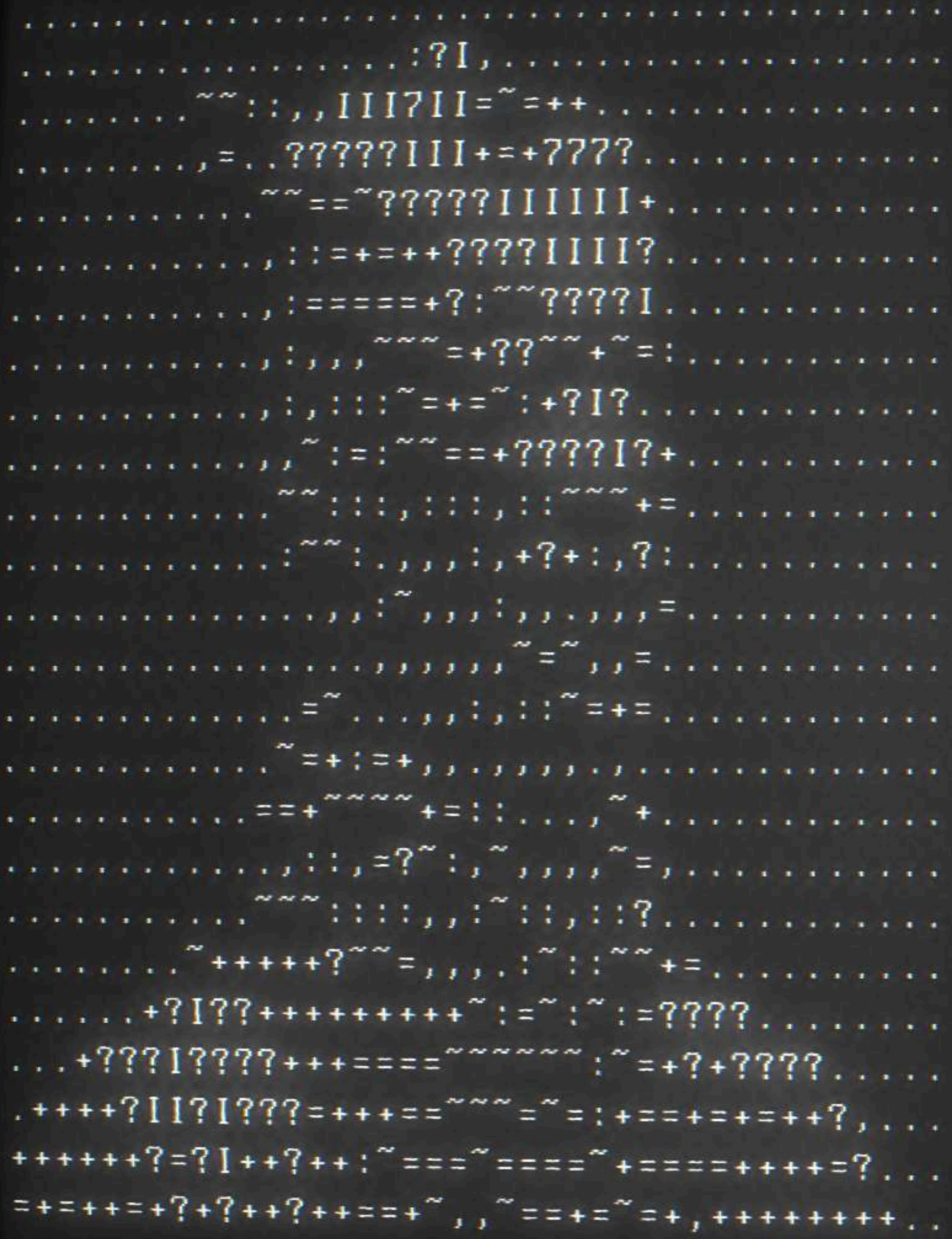
24/ 7 Coverage

```
plum@Ballroom:~$
```

Terminal
2:25 PM
En
Record
Show/hide Main Window
Select Area On Screen
About
Quit
plum@Ballroom: ~
Windows 10 (Gh0st) [Running] - Oracle VM VirtualBox
Recycle Bin
RATs
Gh0st english.exe
Gh0st english.ini
temp
Home
temp
ENG
1:25 PM
6/20/2017
2
Right Ctrl

Post exploitation

- Netstat
  - IP address of other victims
  - May show RDP connections in (or out)
- Walk FS looking for other hacking tools
- Install persistance
- Install keylogger
- Steal credentials



"He who is prudent and lies in wait for an enemy who is not, will be victorious."

-- Sun Tzu, The Art of War

Thank you

@professor__plum