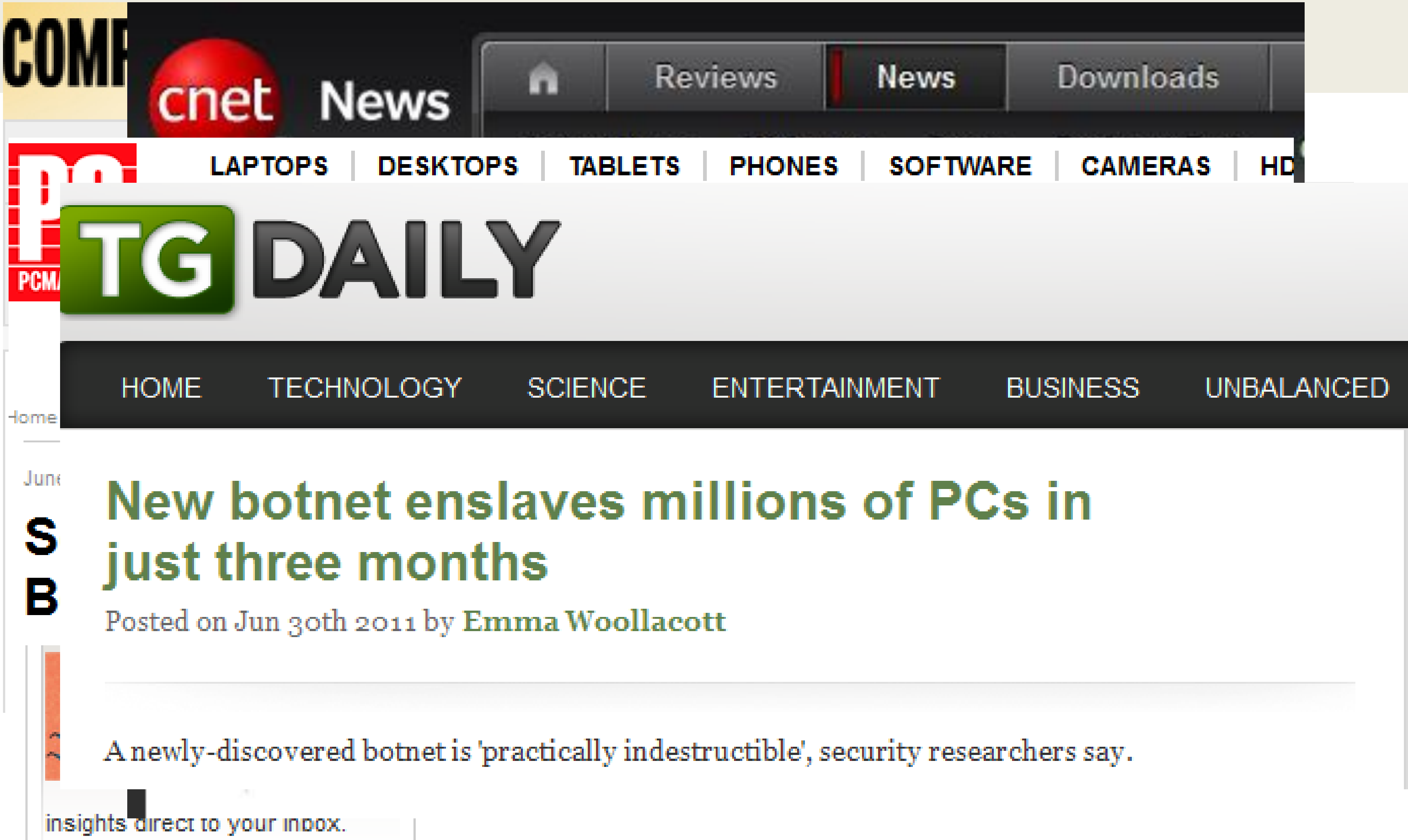
The hidden part of TDSS

Sergey (k1k) Golovanov, Malware Expert

Global Research and Analysis Team

Kaspersky Lab



New botnet enslaves millions of PCs in just three months

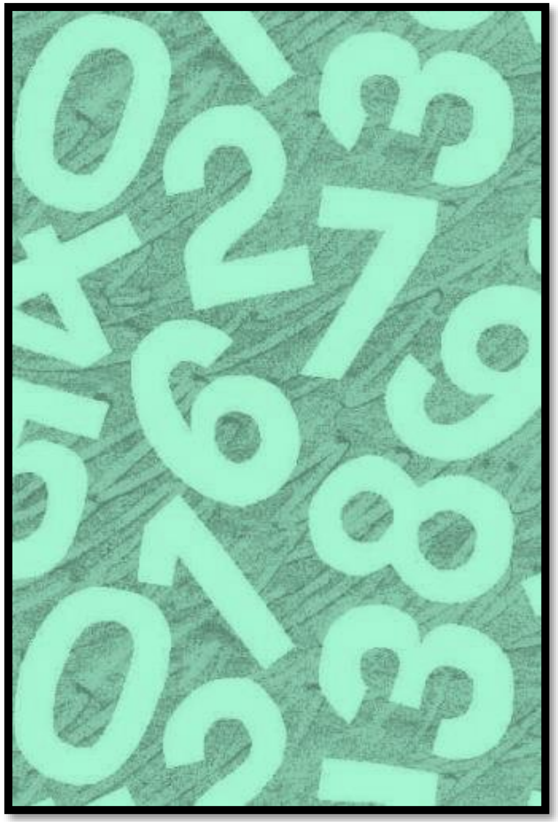
Posted on Jun 30th 2011 by Emma Woollacott

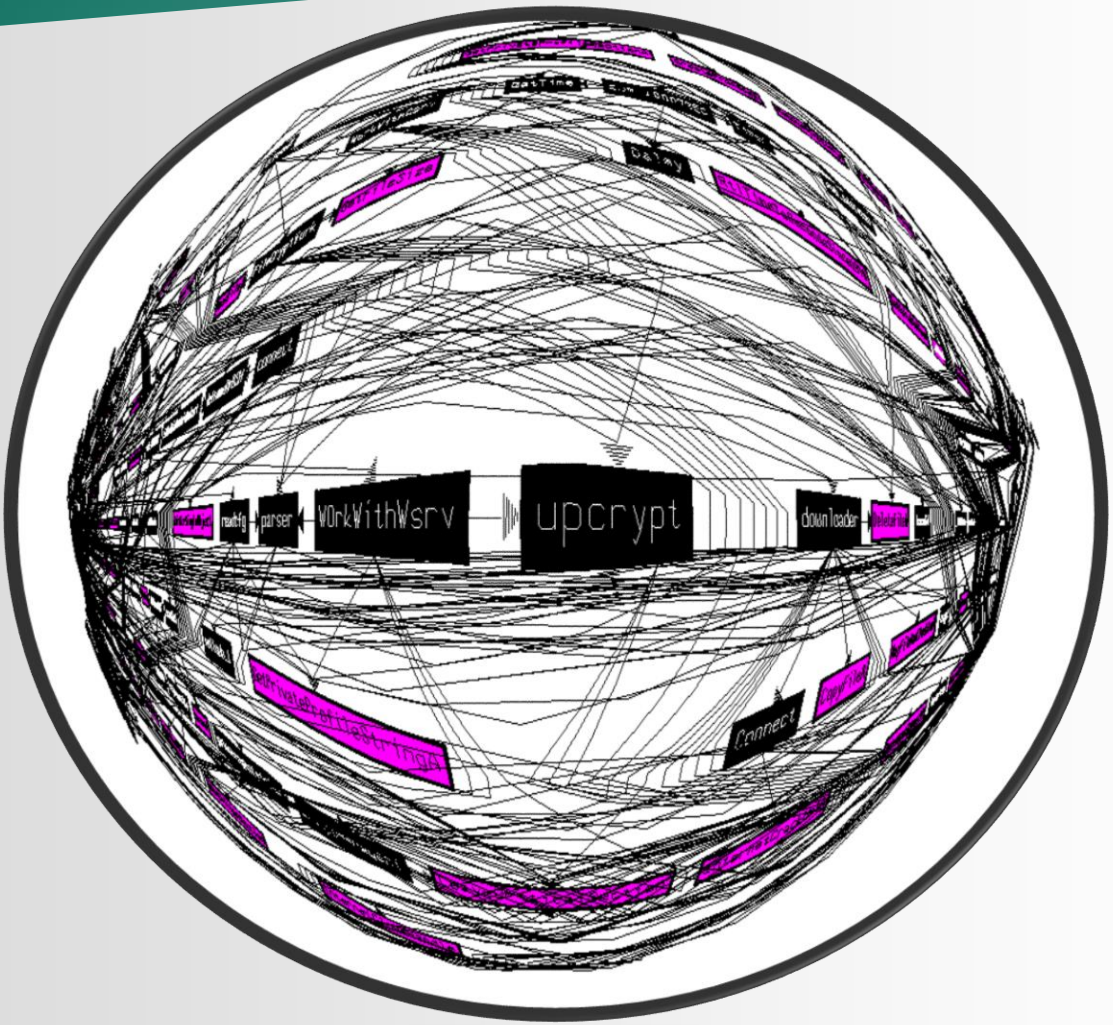
A newly-discovered botnet is 'practically indestructible', security researchers say.

insights direct to your inbox.

Content

1. TDSS Overview
2. Reversing TDSS networking
3. Analyzing p2p functionality
4. Monitoring active bot
5. Getting CnC stats





TDSS Overview

Main modules

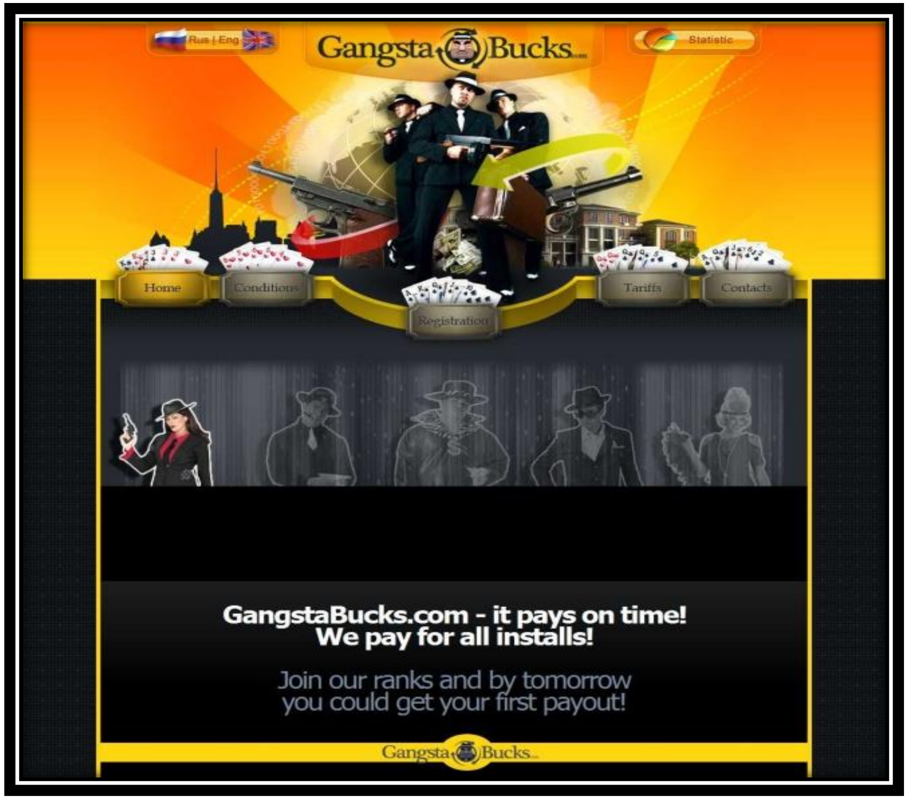
•MBR infector – bypass drivers digital signatures protection

•x64 rootkit – TDSS works on every modern Windows system

•Clicker – clicks banners and links

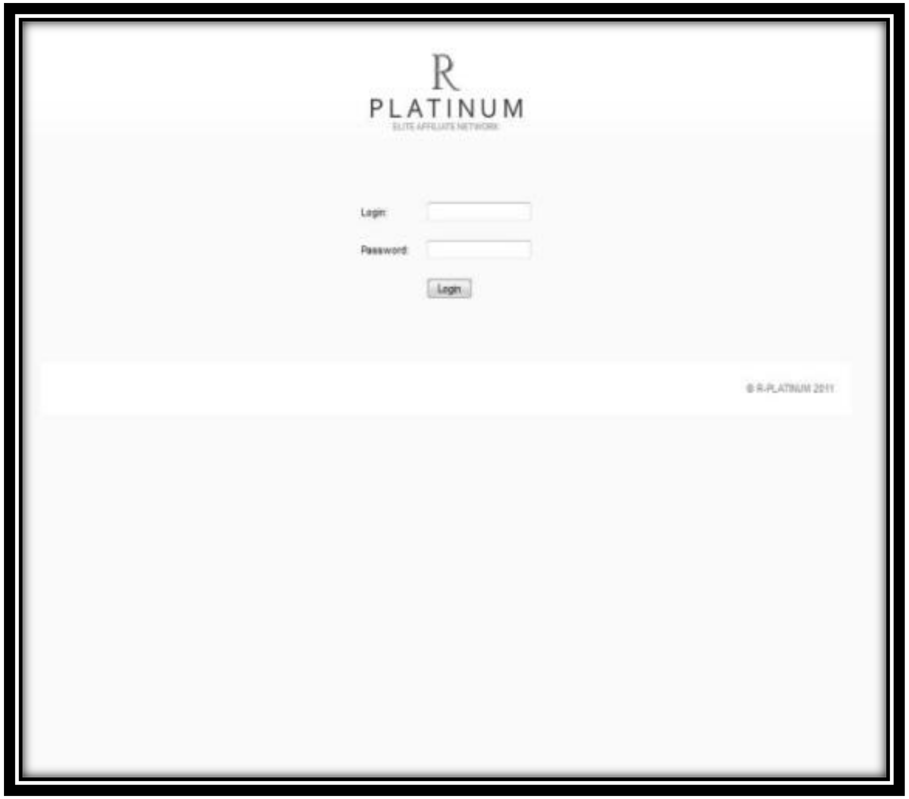
•Target on Black SEO – promoting web site via Google, Bing, Altavista and more

Affiliate Network



GangstaBucks.com - it pays on time!
We pay for all installs!

Join our ranks and by tomorrow
you could get your first payout!



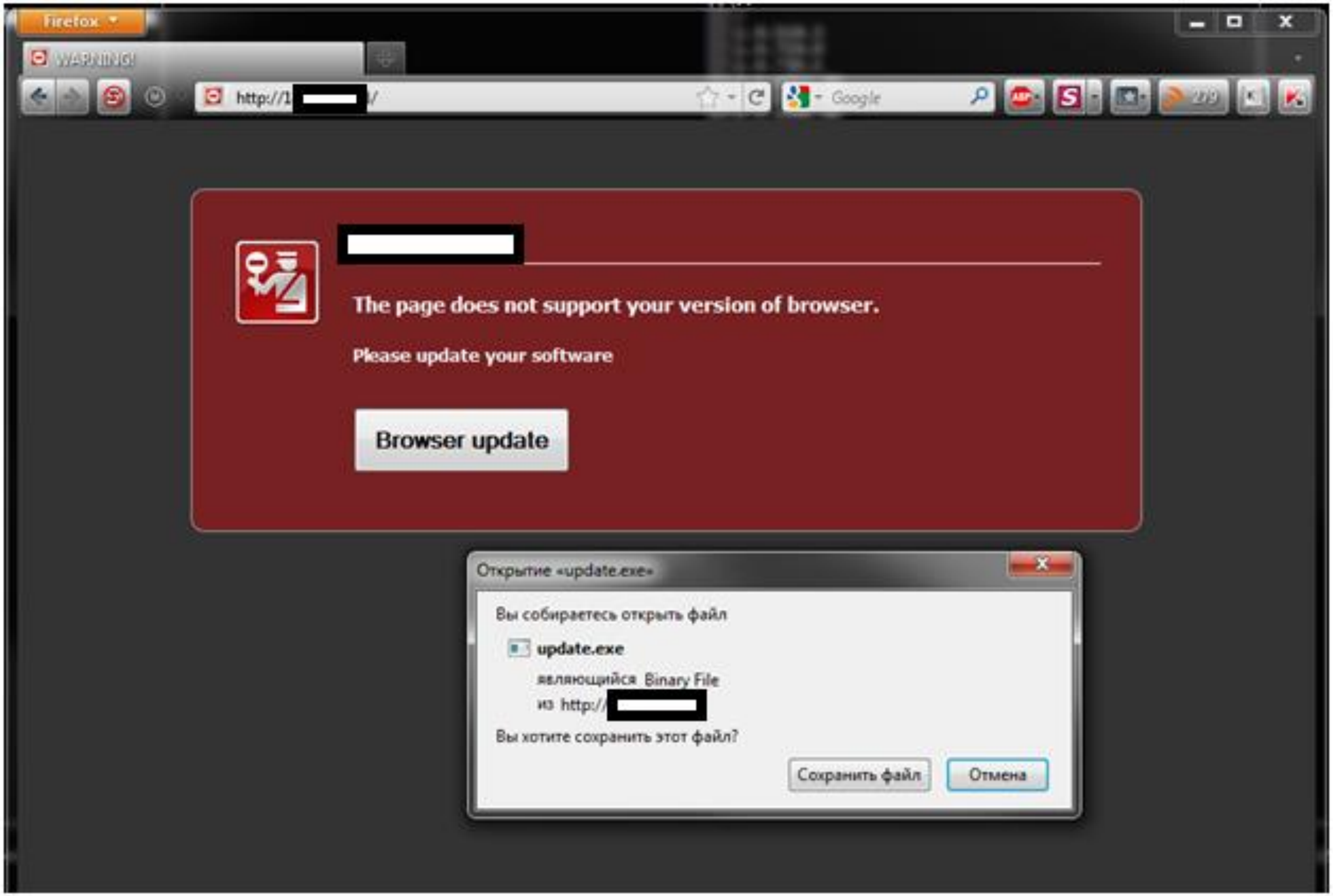
Login:

Password:

© R-PLATINUM 2011

- Two Affiliate Networks are spreading TDSS
- 20 - 200 USD for 1 000 installs
- Affiliates installs TDSS via SPAM, Worms, Exploits and etc.

Malicious DHCP



[redacted]

The page does not support your version of browser.

Please update your software

Открытие «update.exe»

Вы собираетесь открыть файл

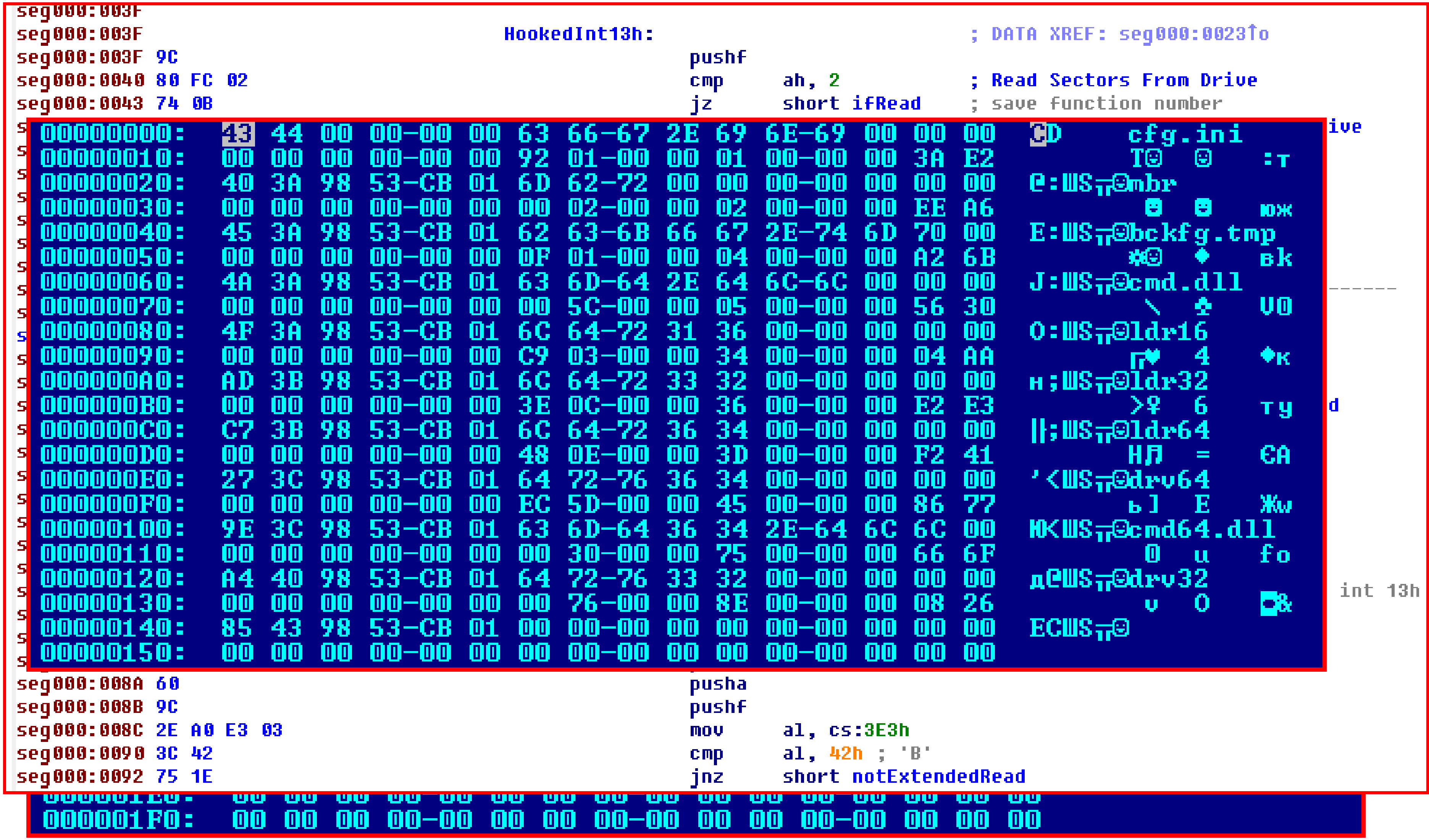
update.exe

являющийся Binary File

из http://[redacted]

Вы хотите сохранить этот файл?

Boot

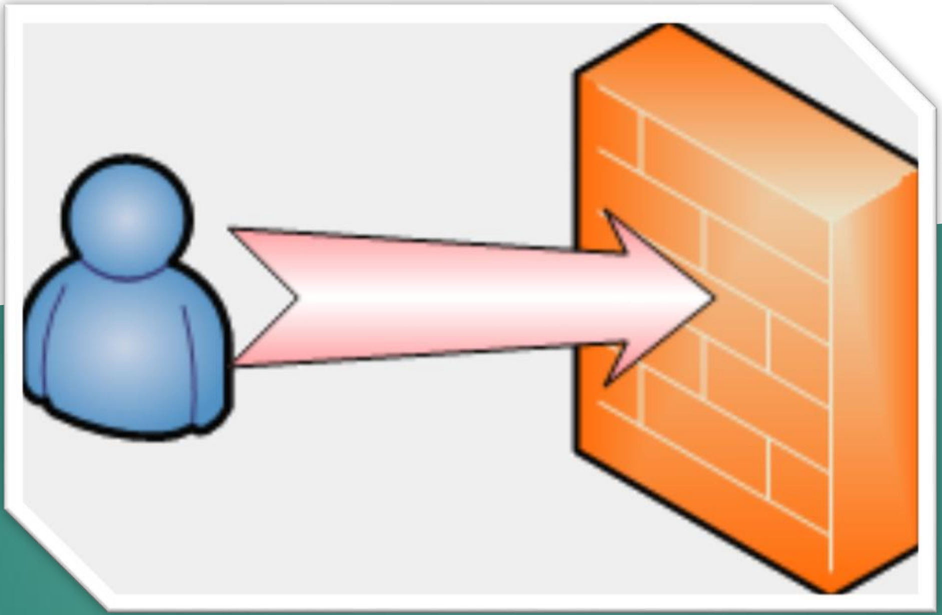


```
seg000:003F
seg000:003F                                  HookedInt13h:                               ; DATA XREF: seg000:0023↑o
seg000:003F 9C                                                   pushf
seg000:0040 80 FC 02                                             cmp     ah, 2            ; Read Sectors From Drive
seg000:0043 74 0B                                                jz      short ifRead     ; save function number
```

```
00000000:  43 44 00 00-00 00 63 66-67 2E 69 6E-69 00 00 00   CD    cfg.ini
00000010:  00 00 00 00-00 00 92 01-00 00 01 00-00 00 3A E2         Т☺  ☺   :т
00000020:  40 3A 98 53-CB 01 6D 62-72 00 00 00-00 00 00 00   @:ШS╦☺mbr
00000030:  00 00 00 00-00 00 02 00-00 02 00 00-00 00 EE A6         ☻  ☻    юж
00000040:  45 3A 98 53-CB 01 62 63-6B 66 67 2E-74 6D 70 00   E:ШS╦☺bckfg.tmp
00000050:  00 00 00 00-00 0F 01 00-00 04 00 00-00 00 A2 6B        ☼☺  ♦    вk
00000060:  4A 3A 98 53-CB 01 63 6D-64 2E 64 6C-6C 00 00 00   J:ШS╦☺cmd.dll
00000070:  00 00 00 00-00 00 5C 00-00 05 00 00-00 00 56 30         \  ♣    V0
00000080:  4F 3A 98 53-CB 01 6C 64-72 31 36 00-00 00 00 00   O:ШS╦☺ldr16
00000090:  00 00 00 00-00 C9 03 00-00 34 00 00-00 04 AA 00        ╔♥  4   ♦к
000000A0:  AD 3B 98 53-CB 01 6C 64-72 33 32 00-00 00 00 00   н;ШS╦☺ldr32
000000B0:  00 00 00 00-00 3E 0C 00-00 36 00 00-00 E2 E3 00        >♀  6    ту
000000C0:  C7 3B 98 53-CB 01 6C 64-72 36 34 00-00 00 00 00   ╟;ШS╦☺ldr64
000000D0:  00 00 00 00-00 48 0E 00-00 3D 00 00-00 F2 41 00        H♫  =    ЄA
000000E0:  27 3C 98 53-CB 01 64 72-76 36 34 00-00 00 00 00   '<ШS╦☺drv64
000000F0:  00 00 00 00-00 EC 5D 00-00 45 00 00-00 86 77 00        ь]  E    Жw
00000100:  9E 3C 98 53-CB 01 63 6D-64 36 34 2E-64 6C 6C 00   Ю<ШS╦☺cmd64.dll
00000110:  00 00 00 00-00 00 30 00-00 75 00 00-00 66 6F 00         0  u    fo
00000120:  A4 40 98 53-CB 01 64 72-76 33 32 00-00 00 00 00   д@ШS╦☺drv32
00000130:  00 00 00 00-00 00 76 00-00 8E 00 00-00 08 26 00         v  О    ◘&
00000140:  85 43 98 53-CB 01 00 00-00 00 00 00-00 00 00 00   ЕCШS╦☺
00000150:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```

```
seg000:008A 60                                                   pusha
seg000:008B 9C                                                   pushf
seg000:008C 2E A0 E3 03                                          mov     al, cs:3E3h
seg000:0090 3C 42                                                cmp     al, 42h ; 'B'
seg000:0092 75 1E                                                jnz     short notExtendedRead
```

```
000001E0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001F0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
```



Reversing TDSS networking.

Client to Server

1. Original request

command|noname|30127|0|0.03|0.15|5.1 2600 SP2.0|en-us|iexplore|351|0 ~~and Benchmark(20000000,md5(1))|~~1614895754

2. RC4 or its modification where Key is the targeted host name

ХЪ7U>tюjЇ\+_Э→/СИY>Ко↓н>4L•хоУч¶@_►F_M!aw♀:Ыlр↔d;_fщ☻§ю¶♥0язl

3. BASE64

r1writ0aL0PIWZtL7hntuzRMB3hv0/cUQL4QRrxNIeB3

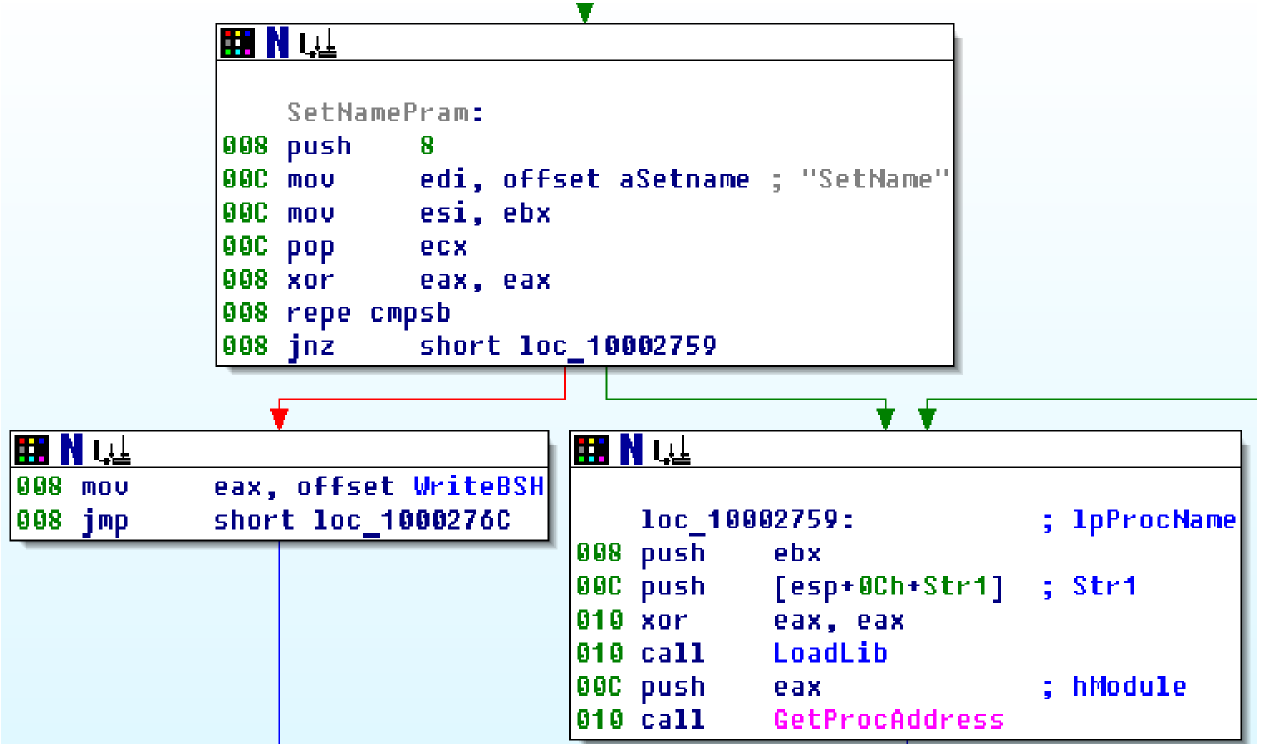
4. Additional trash

4EszDdXaN1U+dP5qr1writ0aL0PIWZtL7hntuzRMB3hv0/cUQL4QRrxNIeB3DDr

5. HTTPS

Server to Client

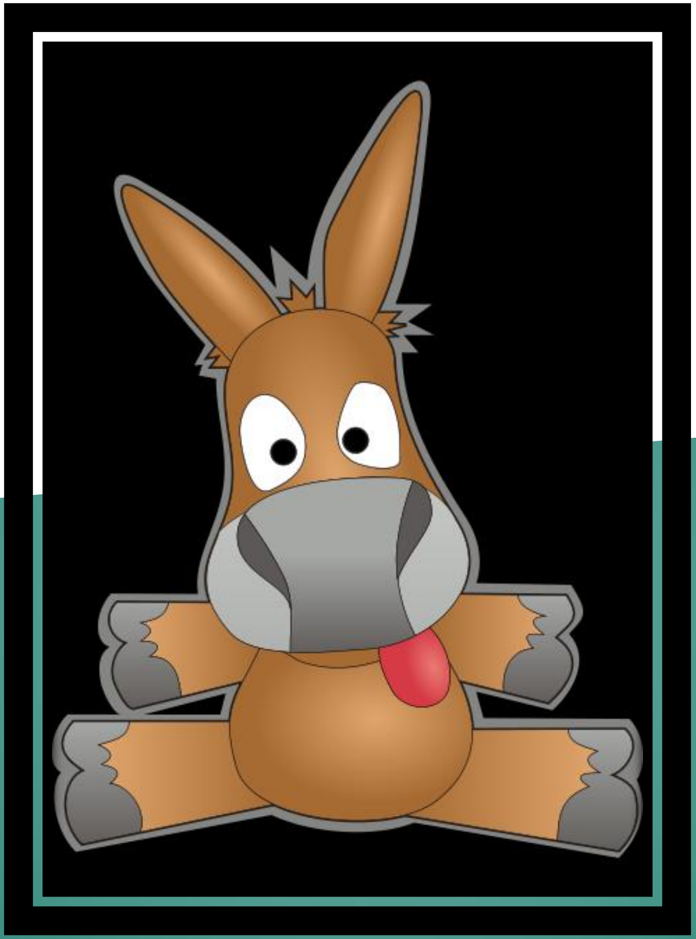
1. Set Name parameter – additional unique key for RC4 or its modification



```
    SetNamePram:
008 push    8
00C mov     edi, offset aSetname ; "SetName"
00C mov     esi, ebx
00C pop     ecx
008 xor     eax, eax
008 repe cmpsb
008 jnz     short loc_10002759
```

```
008 mov     eax, offset WriteBSH
008 jmp     short loc_1000276C
```

```
    loc_10002759:                  ; lpProcName
008 push    ebx
00C push    [esp+0Ch+Str1]         ; Str1
010 xor     eax, eax
010 call    LoadLib
00C push    eax                    ; hModule
010 call    GetProcAddress
```

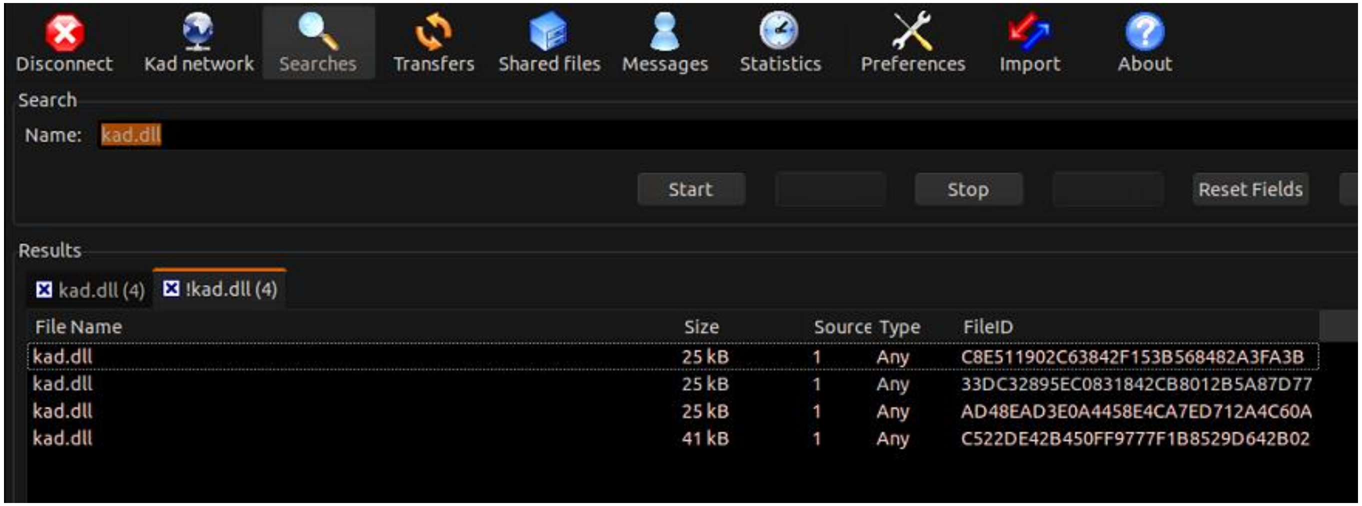


ANALYZING P2P FUNCTIONALITY

Analyzing p2p functionality

KAD.DLL algorithm:

1. Share encrypted file named as “ktzrules”
2. Upload kad.dll on TDSS infected PCs
3. Kad.dll loads public nodes.dat file with KAD Client/Servers IPs
4. Kad.dll searchs for “ktzrules” file in public KAD network
5. Kad.dll downloads “ktzrules” and executes commands



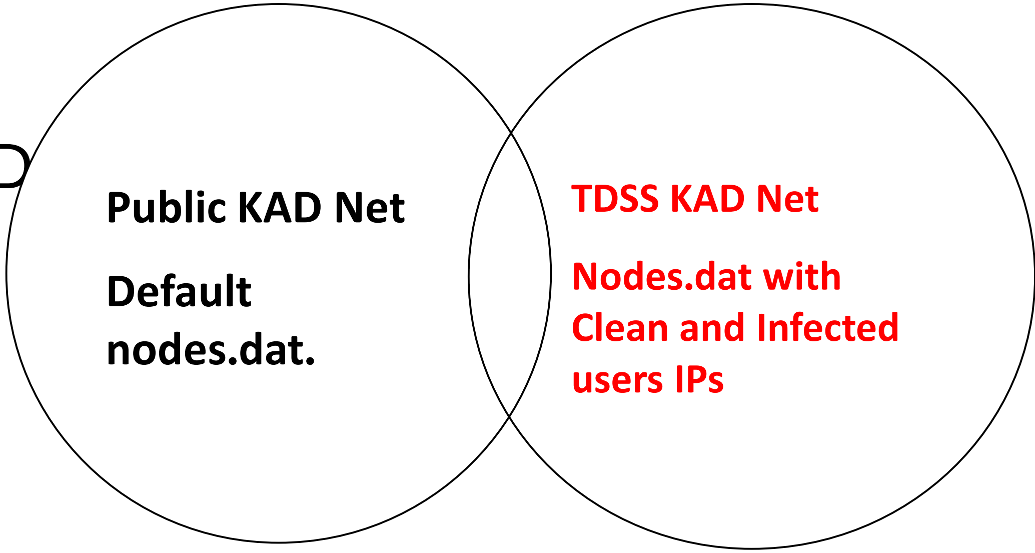
Name: kad.dll

File Name	Size	Source	Type	FileID
kad.dll	25 kB	1	Any	C8E511902C63842F153B568482A3FA3B
kad.dll	25 kB	1	Any	33DC32895EC0831842CB8012B5A87D77
kad.dll	25 kB	1	Any	AD48EAD3E0A4458E4CA7ED712A4C60A
kad.dll	41 kB	1	Any	C522DE42B450FF9777F1B8529D642B02

Analyzing p2p functionality

KAD.DLL functions:

1. SearchCfg – find “ktzrules” file with commands
2. LoadExe – Find and download exe file from KAD
3. ConfigWrite – write in configuration file
4. Search – find specified file in KAD
5. Publish – publish specified file
6. Knock – download new nodes.dat file

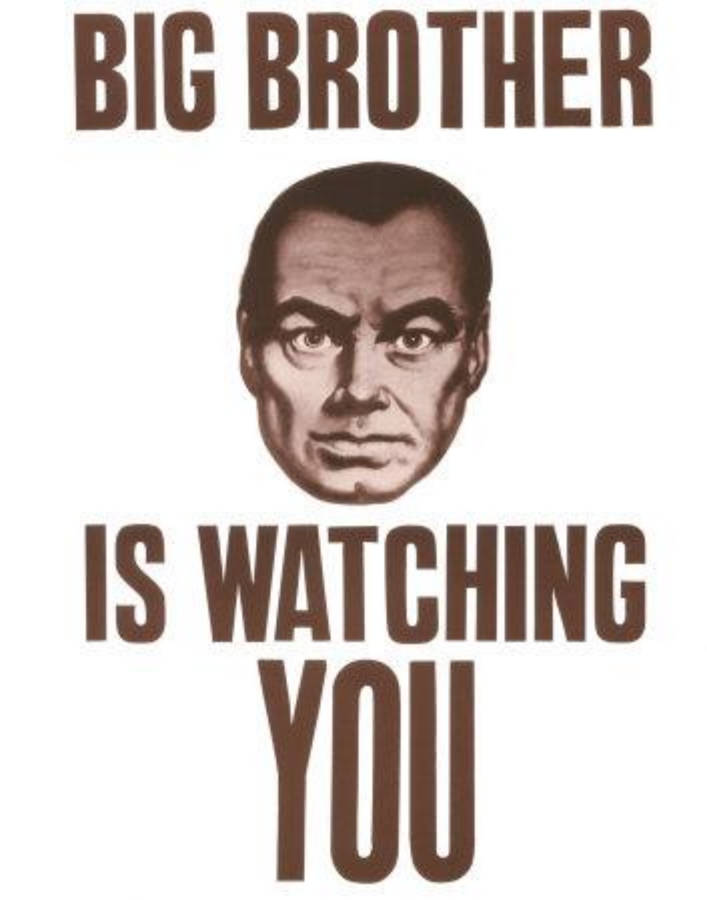


Public KAD Net

Default nodes.dat.

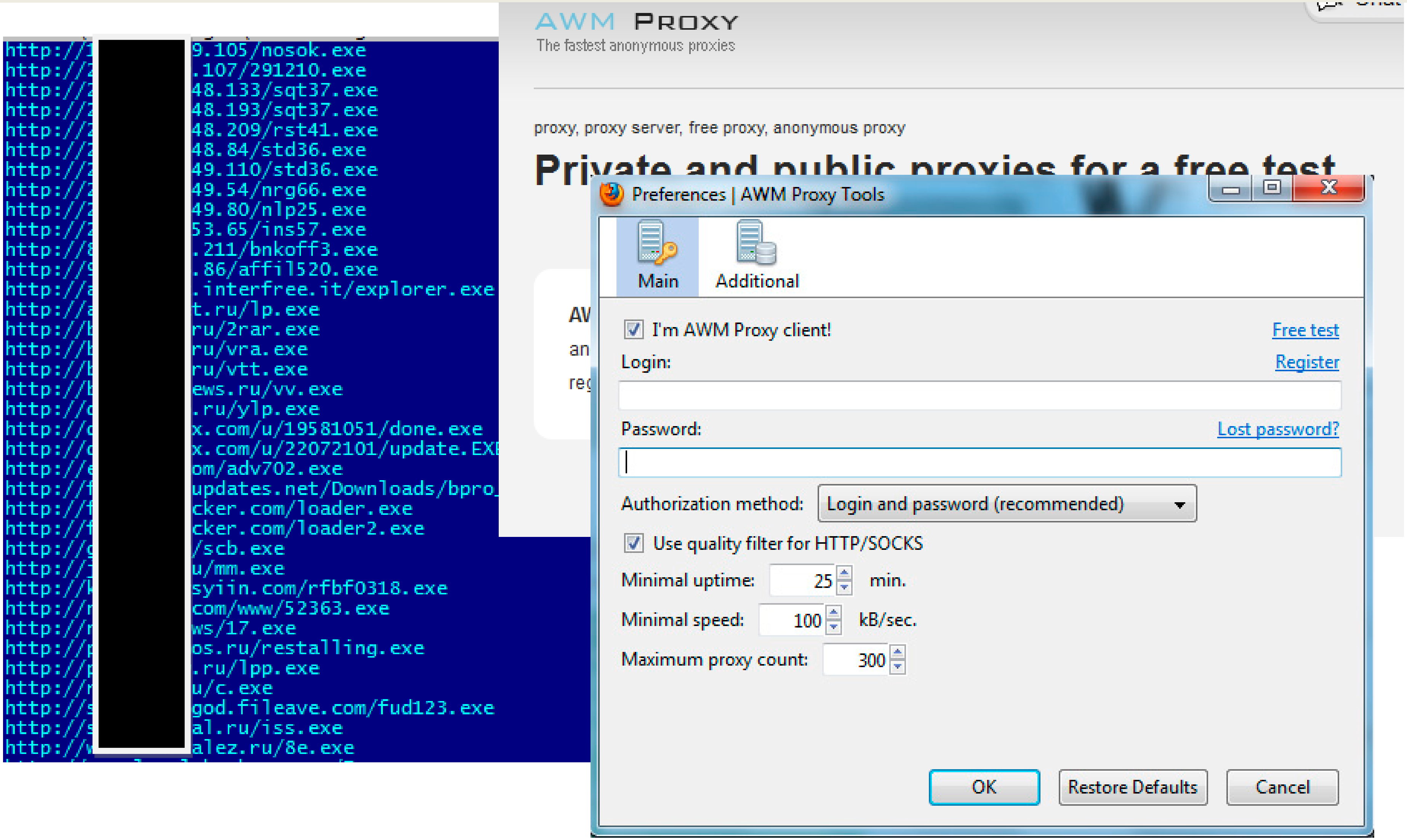
TDSS KAD Net

Nodes.dat with Clean and Infected users IPs



Monitoring active bot

Installs and proxy



```
http://[redacted]9.105/nosok.exe
http://          .107/291210.exe
http://          48.133/sqt37.exe
http://          48.193/sqt37.exe
http://          48.209/rst41.exe
http://          48.84/std36.exe
http://          49.110/std36.exe
http://          49.54/nrg66.exe
http://          49.80/nlp25.exe
http://          53.65/ins57.exe
http://          .211/bnkoff3.exe
http://          .86/affil520.exe
http://          .interfree.it/explorer.exe
http://          t.ru/lp.exe
http://          ru/2rar.exe
http://          ru/vra.exe
http://          ru/vtt.exe
http://          ews.ru/vv.exe
http://          .ru/ylp.exe
http://          x.com/u/19581051/done.exe
http://          x.com/u/22072101/update.EX
http://          om/adv702.exe
http://          updates.net/Downloads/bpro_
http://          cker.com/loader.exe
http://          cker.com/loader2.exe
http://          /scb.exe
http://          u/mm.exe
http://          syiin.com/rfbf0318.exe
http://          com/www/52363.exe
http://          ws/17.exe
http://          os.ru/restalling.exe
http://          .ru/lpp.exe
http://          u/c.exe
http://          god.fileave.com/fud123.exe
http://          al.ru/iss.exe
http://          alez.ru/8e.exe
```

AWM PROXY

The fastest anonymous proxies

proxy, proxy server, free proxy, anonymous proxy

Private and public proxies for a free test

Preferences | AWM Proxy Tools

☑ I'm AWM Proxy client!

Free test

Login:

Register

Password:

Lost password?

Authorization method: Login and password (recommended)

☑ Use quality filter for HTTP/SOCKS

Minimal uptime: 25 min.

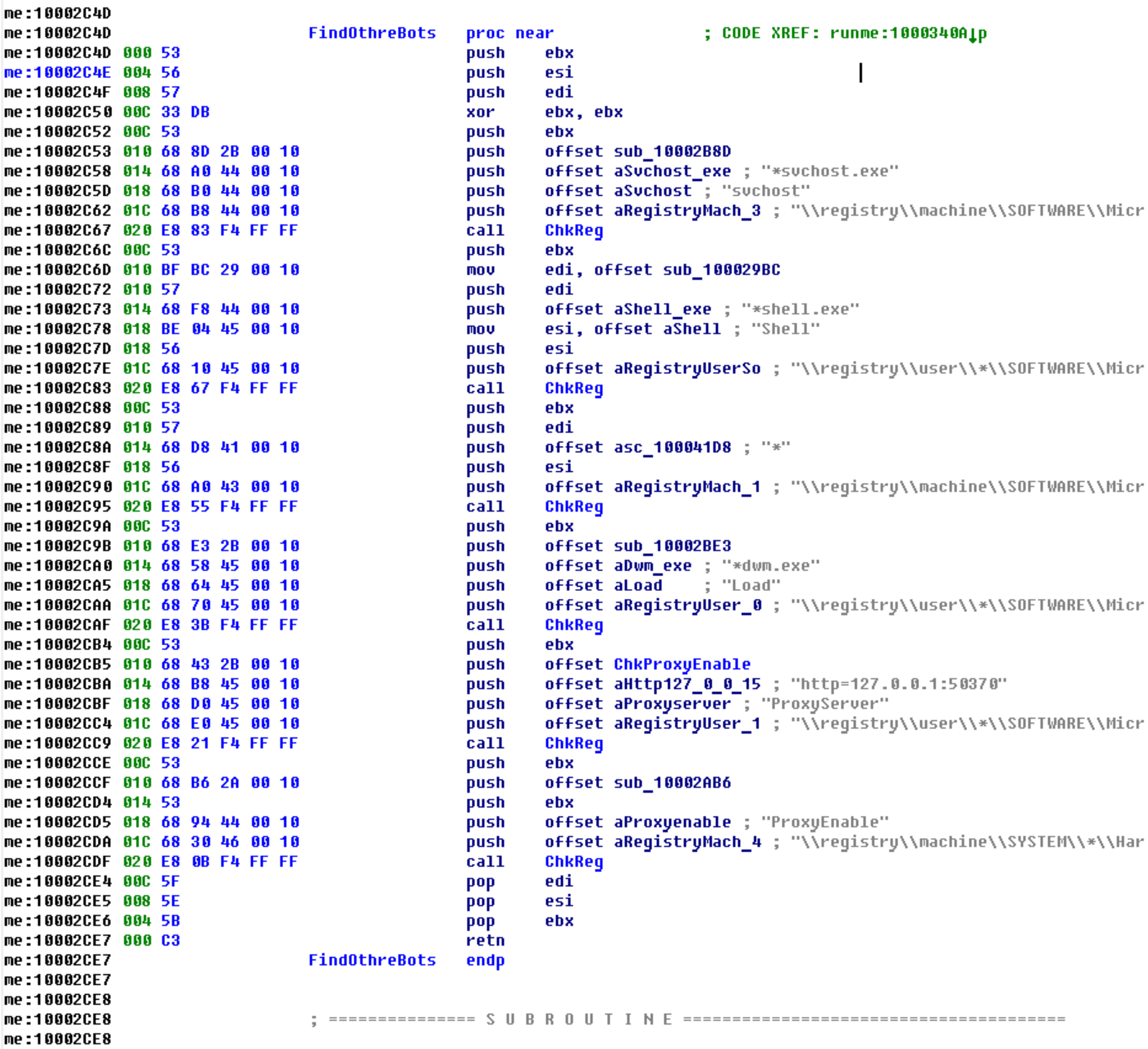
Minimal speed: 100 kB/sec.

Maximum proxy count: 300

Anti-Virus

- Gbot
- ZeuS
- Clishmic
- Optima

Full list includes ~30 malware families name



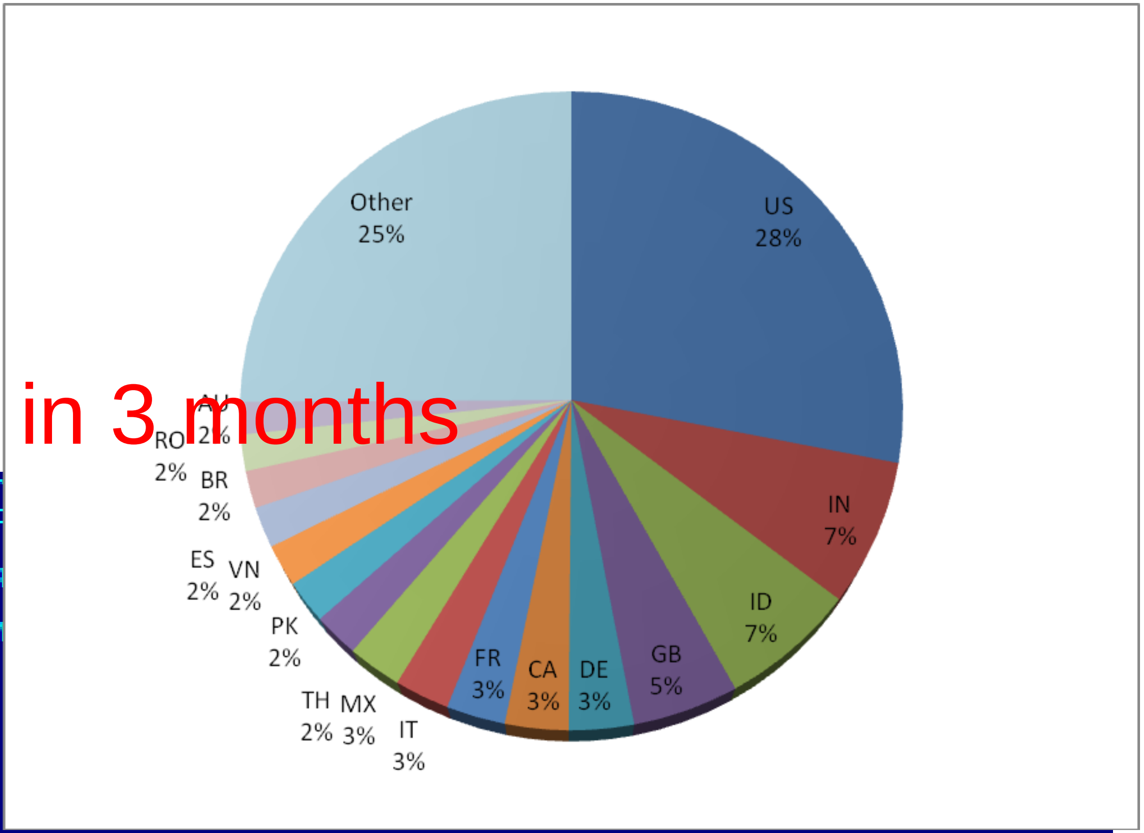
```
me:10002C4D
me:10002C4D                      FindOthreBots  proc near               ; CODE XREF: runme:1000340A↓p
me:10002C4D 000 53                              push    ebx
me:10002C4E 004 56                              push    esi
me:10002C4F 008 57                              push    edi
me:10002C50 00C 33 DB                           xor     ebx, ebx
me:10002C52 00C 53                              push    ebx
me:10002C53 010 68 8D 2B 00 10                  push    offset sub_10002B8D
me:10002C58 014 68 A0 44 00 10                  push    offset aSvchost_exe ; "*svchost.exe"
me:10002C5D 018 68 B0 44 00 10                  push    offset aSvchost ; "svchost"
me:10002C62 01C 68 B8 44 00 10                  push    offset aRegistryMach_3 ; "\\registry\\machine\\SOFTWARE\\Micr
me:10002C67 020 E8 83 F4 FF FF                  call    ChkReg
me:10002C6C 00C 53                              push    ebx
me:10002C6D 010 BF BC 29 00 10                  mov     edi, offset sub_100029BC
me:10002C72 010 57                              push    edi
me:10002C73 014 68 F8 44 00 10                  push    offset aShell_exe ; "*shell.exe"
me:10002C78 018 BE 04 45 00 10                  mov     esi, offset aShell ; "Shell"
me:10002C7D 018 56                              push    esi
me:10002C7E 01C 68 10 45 00 10                  push    offset aRegistryUserSo ; "\\registry\\user\\*\\SOFTWARE\\Micr
me:10002C83 020 E8 67 F4 FF FF                  call    ChkReg
me:10002C88 00C 53                              push    ebx
me:10002C89 010 57                              push    edi
me:10002C8A 014 68 D8 41 00 10                  push    offset asc_100041D8 ; "*"
me:10002C8F 018 56                              push    esi
me:10002C90 01C 68 A0 43 00 10                  push    offset aRegistryMach_1 ; "\\registry\\machine\\SOFTWARE\\Micr
me:10002C95 020 E8 55 F4 FF FF                  call    ChkReg
me:10002C9A 00C 53                              push    ebx
me:10002C9B 010 68 E3 2B 00 10                  push    offset sub_10002BE3
me:10002CA0 014 68 58 45 00 10                  push    offset aDwm_exe ; "*dwm.exe"
me:10002CA5 018 68 64 45 00 10                  push    offset aLoad     ; "Load"
me:10002CAA 01C 68 70 45 00 10                  push    offset aRegistryUser_0 ; "\\registry\\user\\*\\SOFTWARE\\Micr
me:10002CAF 020 E8 3B F4 FF FF                  call    ChkReg
me:10002CB4 00C 53                              push    ebx
me:10002CB5 010 68 43 2B 00 10                  push    offset ChkProxyEnable
me:10002CBA 014 68 B8 45 00 10                  push    offset aHttp127_0_0_15 ; "http=127.0.0.1:50370"
me:10002CBF 018 68 D0 45 00 10                  push    offset aProxyserver ; "ProxyServer"
me:10002CC4 01C 68 E0 45 00 10                  push    offset aRegistryUser_1 ; "\\registry\\user\\*\\SOFTWARE\\Micr
me:10002CC9 020 E8 21 F4 FF FF                  call    ChkReg
me:10002CCE 00C 53                              push    ebx
me:10002CCF 010 68 B6 2A 00 10                  push    offset sub_10002AB6
me:10002CD4 014 53                              push    ebx
me:10002CD5 018 68 94 44 00 10                  push    offset aProxyenable ; "ProxyEnable"
me:10002CDA 01C 68 30 46 00 10                  push    offset aRegistryMach_4 ; "\\registry\\machine\\SYSTEM\\*\\Har
me:10002CDF 020 E8 0B F4 FF FF                  call    ChkReg
me:10002CE4 00C 5F                              pop     edi
me:10002CE5 008 5E                              pop     esi
me:10002CE6 004 5B                              pop     ebx
me:10002CE7 000 C3                              retn
me:10002CE7                      FindOthreBots  endp
me:10002CE7
me:10002CE8
me:10002CE8                      ; ============== S U B R O U T I N E ========================================
me:10002CE8
```

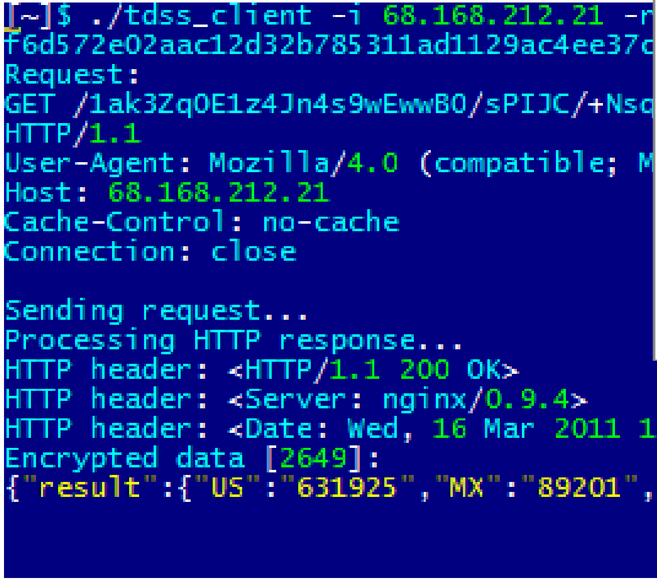
Getting CnC stats

Getting CnC stats

60 proxy CnCs
3 MySQL DBs

5M infected PCs in 3 months





```
[~]$ ./tdss_client -i 68.168.212.21 -r
f6d572e02aac12d32b785311ad1129ac4ee37c
Request:
GET /1ak3Zq0E1z4Jn4s9wEwwB0/sPIJC/+Nsq
HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; M
Host: 68.168.212.21
Cache-Control: no-cache
Connection: close

Sending request...
Processing HTTP response...
HTTP header: <HTTP/1.1 200 OK>
HTTP header: <Server: nginx/0.9.4>
HTTP header: <Date: Wed, 16 Mar 2011 16:41:08 GMT> HTTP header: <Content-Type: text/html> HTTP header:
Encrypted data [2649]:
{"result":{"US":"631925","MX":"89201","GB":"80959","TH":"76313","IN":"71901","FR":"68737","IT":"59532",
```

Summary

•MBR infector – bypass drivers digital signatures protection
•x64 rootkit – TDSS works on every modern Windows system
•Clicker – click banners and links
•Target on Black SEO – promoting web site via Google, Bing, Altavista and more

•P2P botnet – no servers, no centers, sophisticated crypto protection for command file in hidden KAD network.
•Own AV – detects more then 30 malware families
•Clients Proxy –additional anonymizer via infected PCs
•5 millions infected computers

http://www.facebook.com/KasperskyConference

http://www.kaspersky.com/educational-events

IT Security
for the Next Generation
Conference for Young Professionals
in the Field of Information Security
13-15 April 2011
Munich
KASPERSKY lab
IT Security for the Next Generation
KASPERSKY
Name Mark Seeger
Amount One thousand five hundred euros
€ 1500
Name Viviane Zwanger
Amount One thousand euros
€ 1000
Name Christian Siecke
Amount One thousand euros
€ 1000
Chair for
Prof. Dr. Claudia Ecker

WATCHMEN

03.06.09

Thank You

Qu35t10n5?

Sergey (k1k) Golovanov, Malware Expert

Global Research and Analysis Team

Kaspersky Lab