24th Annual FIRST Conference MALTA 17 - 22 June 2012

McAfee® An Intel Company

Pinkslipbot: A deep look at how malicious code adapts and evolves

Guilherme Venere
Malware Researcher
Anti Malware Operation Team

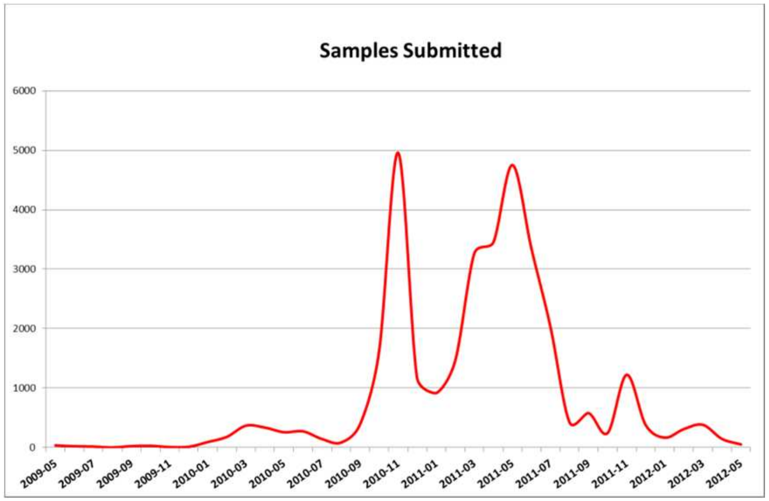
SAFE NEVER SLEEPS.™

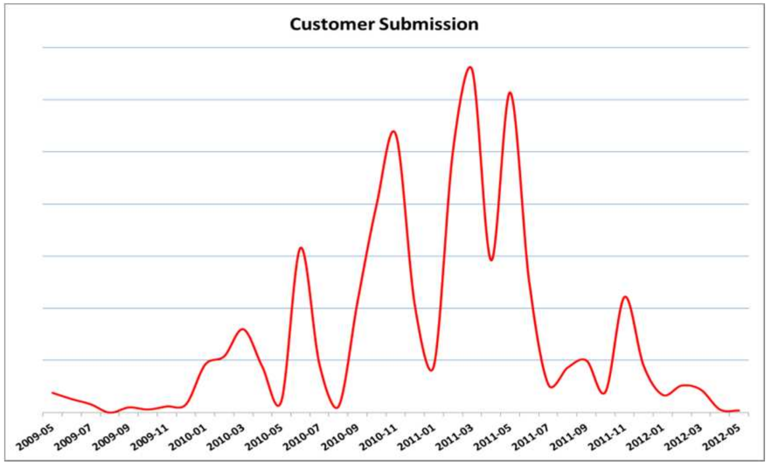
Know Your Enemy

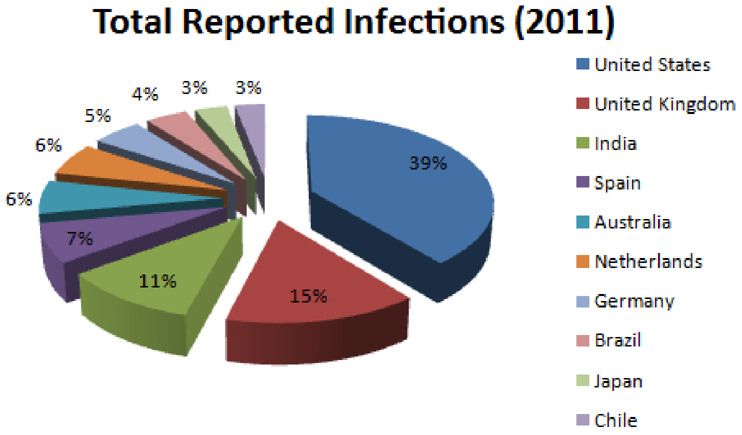
- Server-side polymorphic worm. EXE and DLL modules
- First seen around 2007
- Features common backdoor functionalities
- Spread method
  - Compromised webpages with injected code
  - Network shares (exploits included!)
  - AutoRun (mostly old variants)
  - Spam E-mail attachments (old variants)
- No known source code available
- Very effective in local corporate networks due to spread methods
  - This received attention from the media last year
    http://www.techweekeurope.co.uk/news/nhs-computers-hit-by-qakbot-infection-6636
    http://www.bankinfosecurity.com/breach-may-have-targeted-jobless-a-3655
    http://www.infosecurity-magazine.com/view/18164/qakbot-author-is-no-crackpot-says-symantec/
- **Actively developed over the years**

Pinkslipbot historic data

- Outbreaks follow defined pattern
- Interim time used for development
- Major code change around 2009 improved effectiveness
- But that had its consequences: too much attention!
- Low profile lately.
  - Major code change in sight?

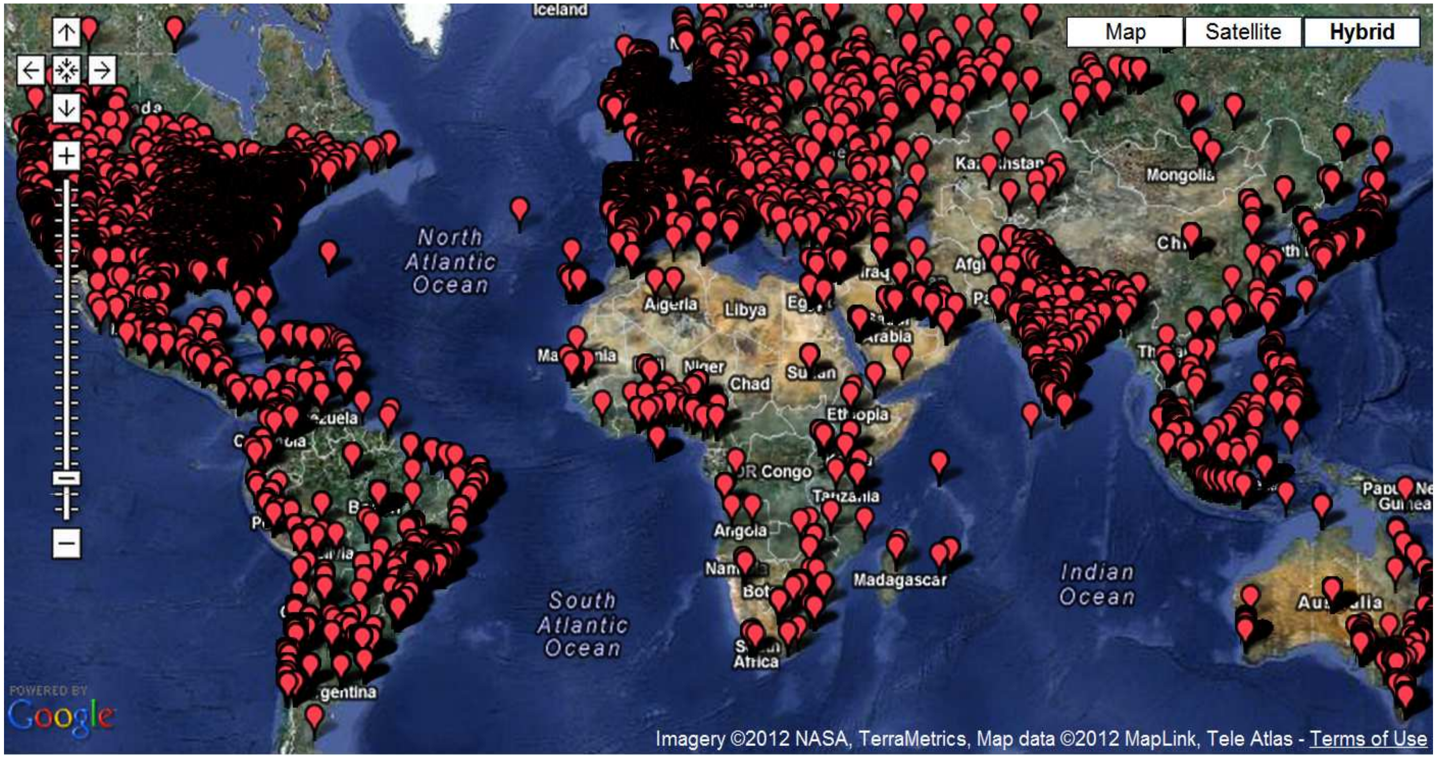


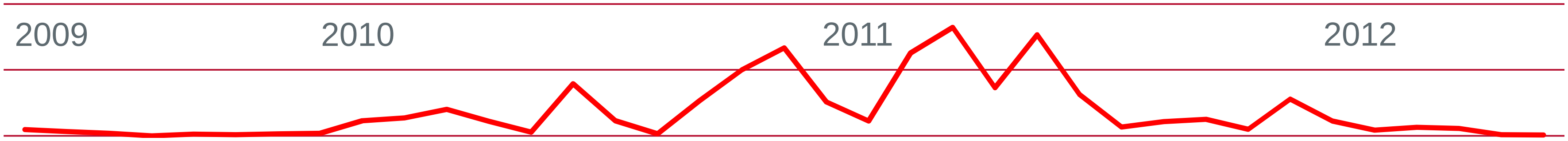




Pinkslipbot historic data

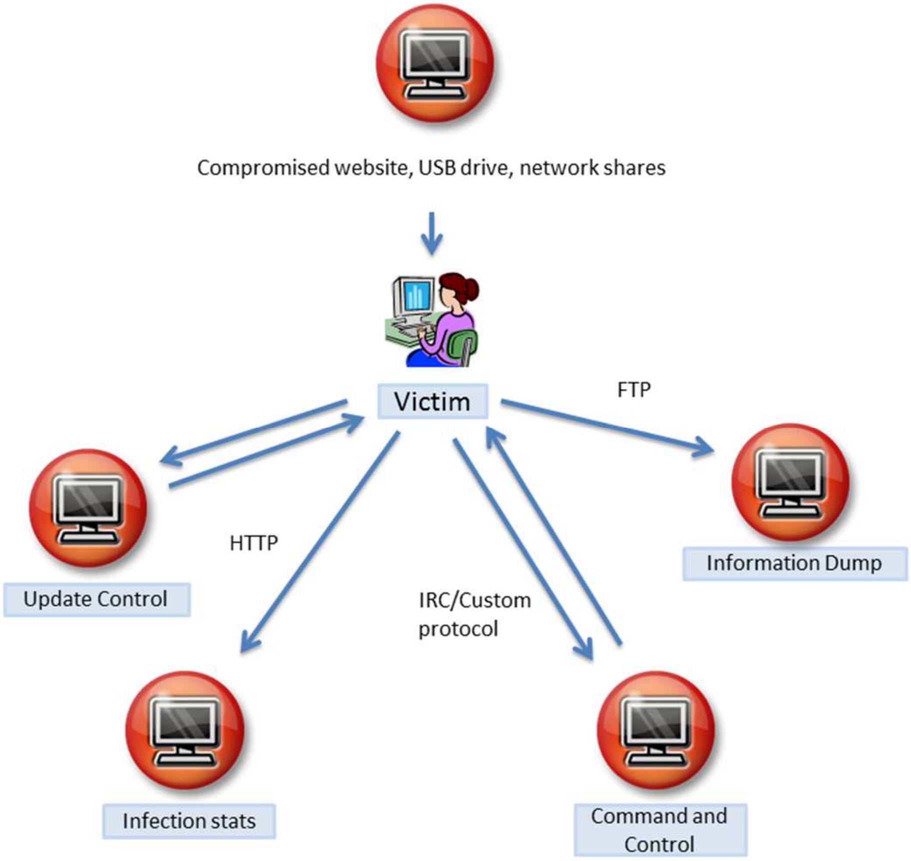
This Google Maps view shows reported infections by Pinkslipbot in 2011

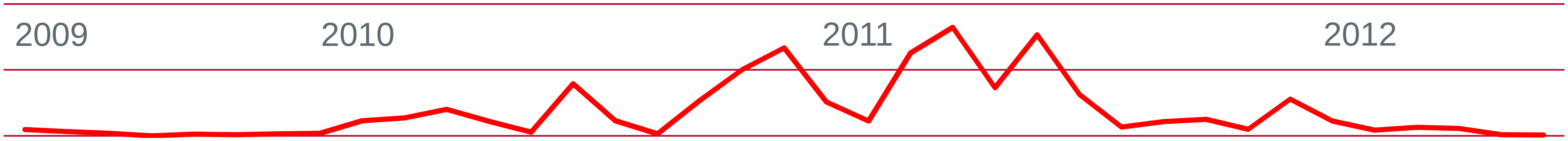




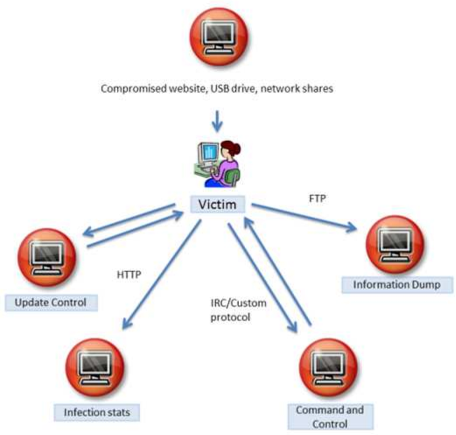
Pinkslipbot network model

McAfee
An Intel Company





Pinkslipbot network model



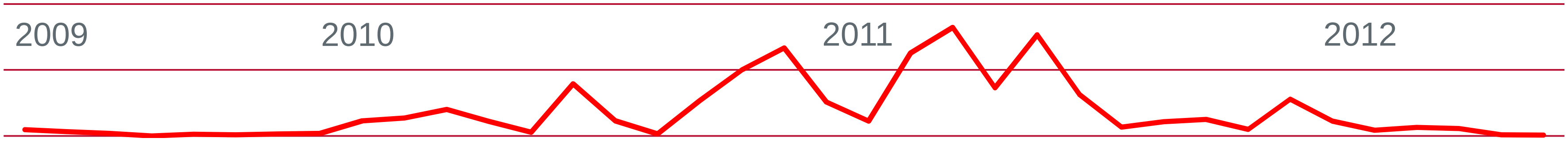
w1.webinspector.biz
a.rtbn2.cn
c.rtbn2.cn
www.cdcdcdcdc2121cdsfdfd.com
ijk.cc
w1.madway.net
w1.rstk.us

109.95.114.252
nt202.cn
up002.cn
adserv.co.in
up004.cn
www.cdcdcdcdc2121cdsfdfd.com
Irc.zief.pl:65520

hostrmeter.com:31666
up002.cn
adserv.co.in
up004.cn
up01.co.in
up02.co.in
upa01.in
nt14.in
incitylocal.com
www.cdcdcdcdc2121cdsfdfd.com

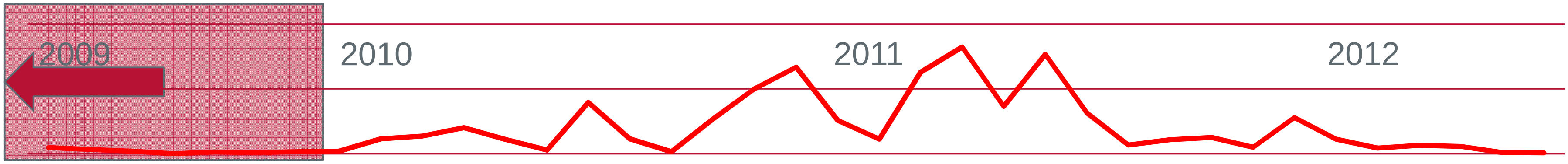
ppcimg.in
du01.in
du02.in
yimg.com.ua
citypromo.info
bgstat.in
redserver.com.ua:31666
spotrate.info
karnadya.com.my
flwest.com
falahuddarain.com
silfersystem.com
gemini.com.co

yimg.com.ua
corpgift.in
soros.in.ua
googstat.info
abirvalg.co.in
69.175.80.89:21
195.3.145.32:8080



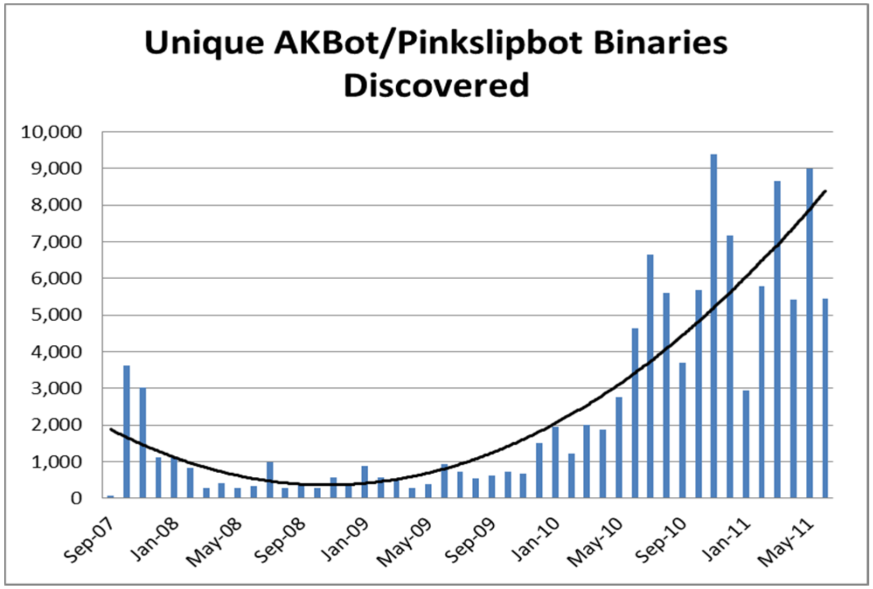
Pinkslipbot prehistory

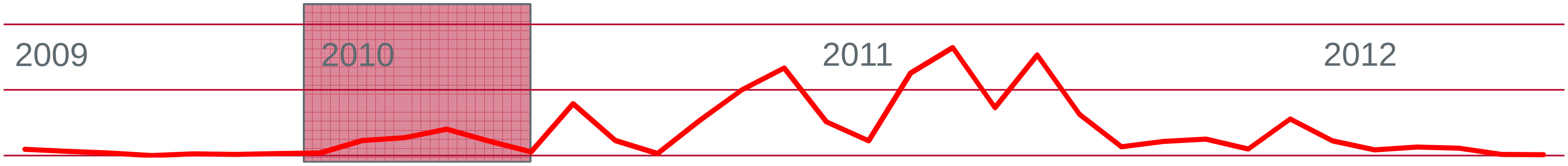
- Packer/Obfuscation varies wildly
- Some samples with strings in Russian
- Samples were small (~14KB-45KB)
- Configuration uses *Rolling-XOR* encryption called SXOR by virus authors
- Spread methods included spam with zipped DOC attachments
  - Default password ‘**Hello999W0rld777**’
- Infection count low
- Group behind it is not well organized yet



Pinkslipbot – Q1 2010

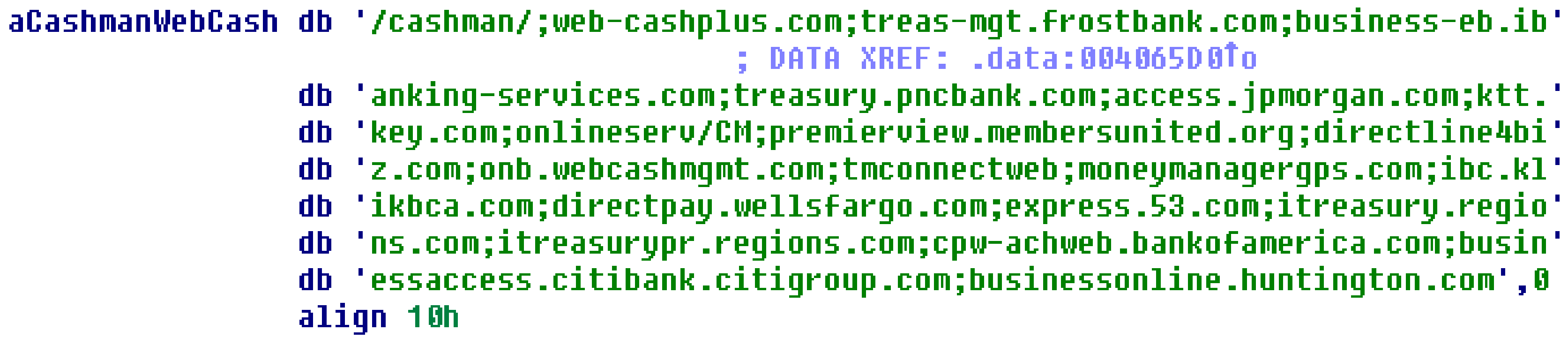
- Many samples using custom packer
- Client side polymorphism
- Wild variety of code seen in samples
- Apparently the group behind Pinkslipbot attempt major rework of code
  - Seems they were not successful



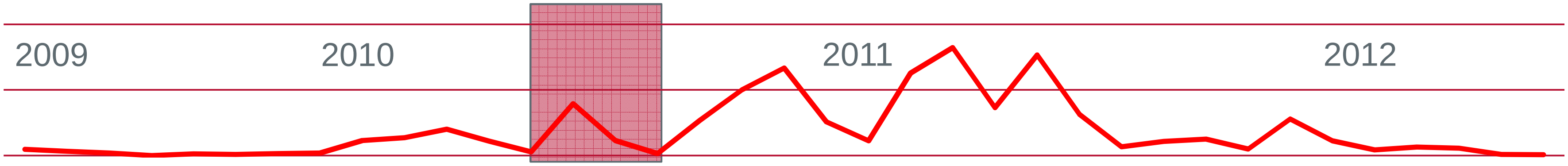


Pinkslipbot – Q2 2010

- File obfuscation start to look like those used by Zeus
- Starts to use server-side polymorphism
- Almost no changes since 2009
  - Reverted to old code
- Users of the following banks were targeted:

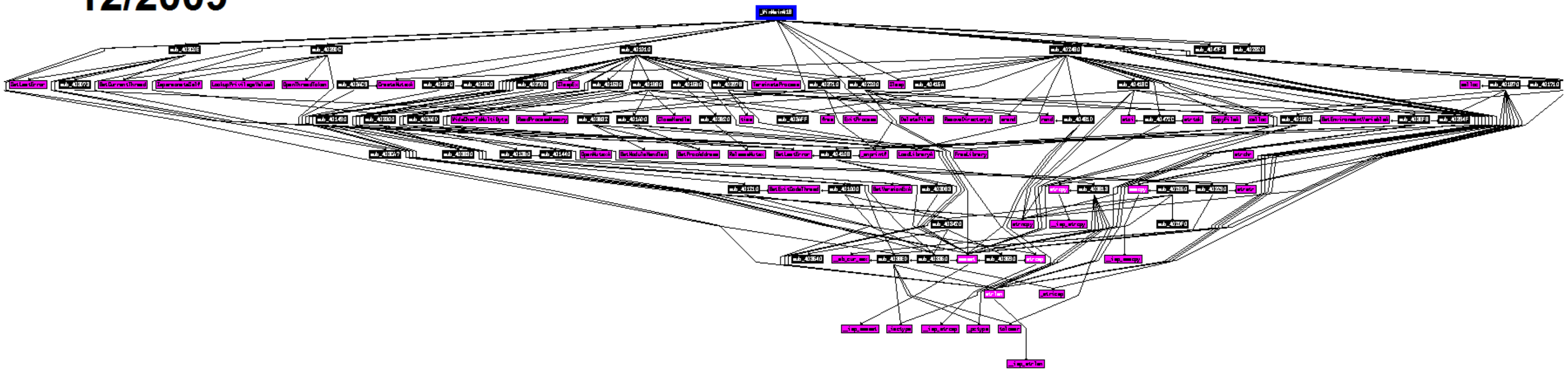


```
aCashmanWebCash db '/cashman/;web-cashplus.com;treas-mgt.frostbank.com;business-eb.ib'
                                        ; DATA XREF: .data:004065D0↑o
                db 'anking-services.com;treasury.pncbank.com;access.jpmorgan.com;ktt.'
                db 'key.com;onlineserv/CM;premierview.membersunited.org;directline4bi'
                db 'z.com;onb.webcashmgmt.com;tmconnectweb;moneymanagergps.com;ibc.kl'
                db 'ikbca.com;directpay.wellsfargo.com;express.53.com;itreasury.regio'
                db 'ns.com;itreasurypr.regions.com;cpw-achweb.bankofamerica.com;busin'
                db 'essaccess.citibank.citigroup.com;businessonline.huntington.com',0
                align 10h
```

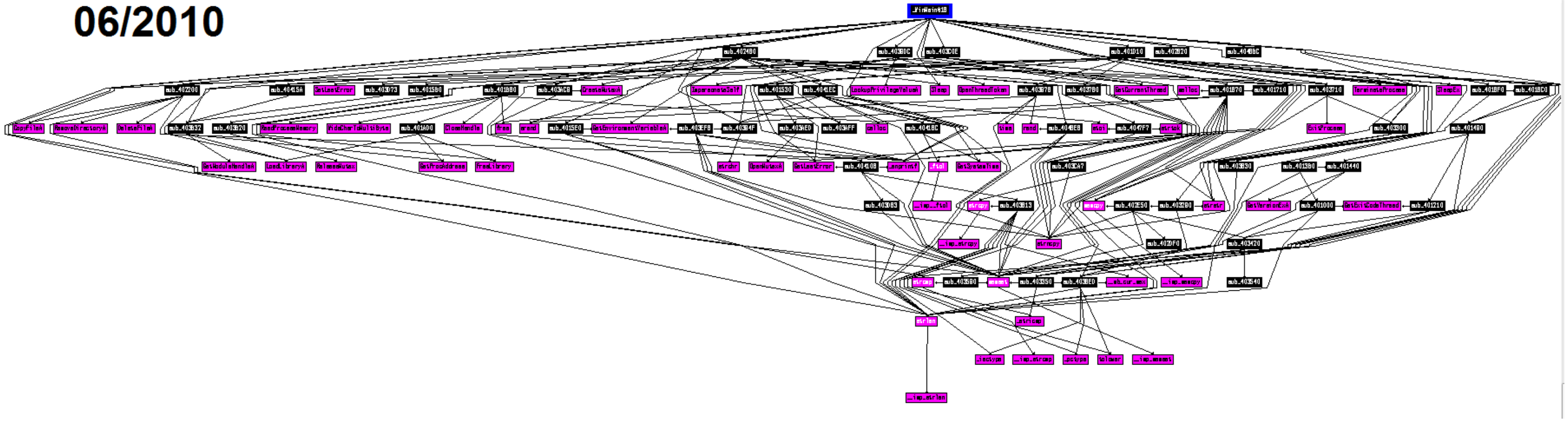


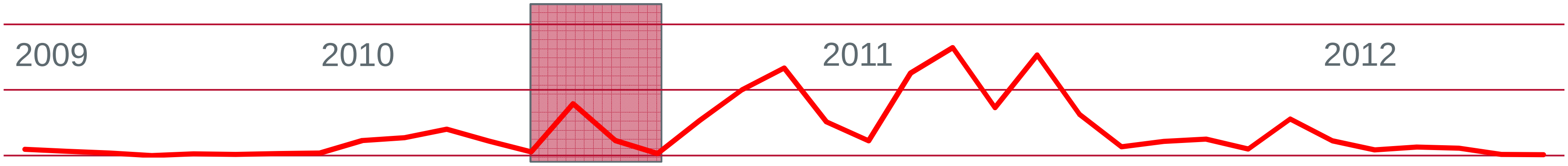
Pinkslipbot – Q2 2010

12/2009



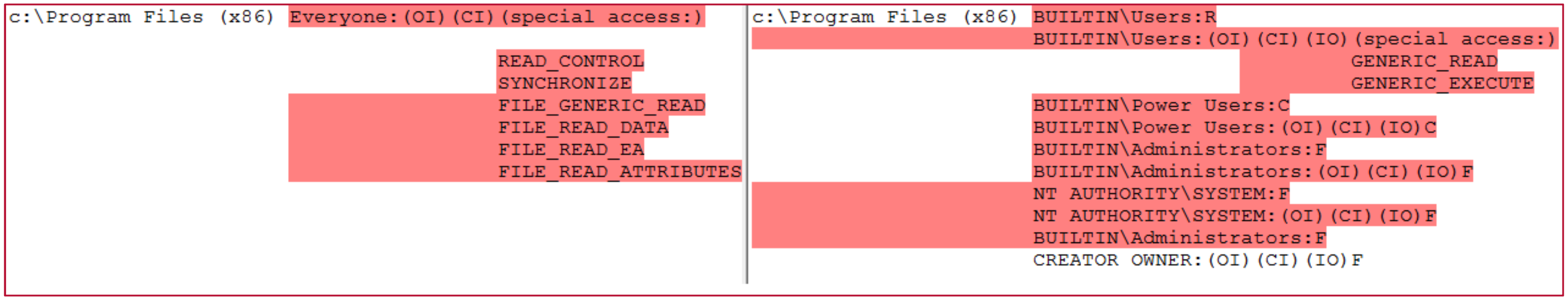
06/2010





Pinkslipbot – Q3/Q4 2010

- **Major code change.** Base for today's version
  - EXE keep DLL alive in processes
- Adds features to steal digital certificates
- Download BackDoor-EXI, fully featured backdoor
- Pinkslipbot begins to disable AV by changing NTFS ACL permissions



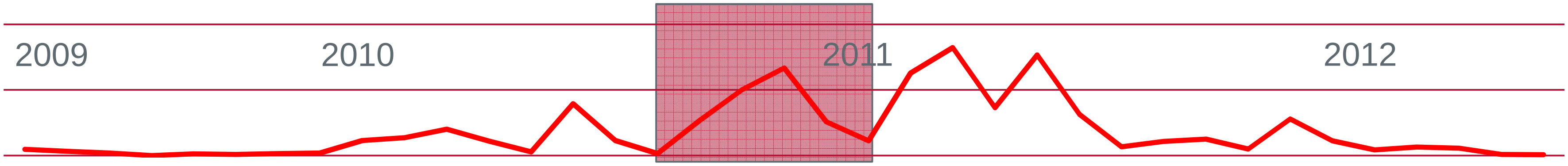
Infected

```
c:\Program Files (x86) Everyone:(OI)(CI)(special access:)

                                 READ_CONTROL
                                 SYNCHRONIZE
                                 FILE_GENERIC_READ
                                 FILE_READ_DATA
                                 FILE_READ_EA
                                 FILE_READ_ATTRIBUTES
```

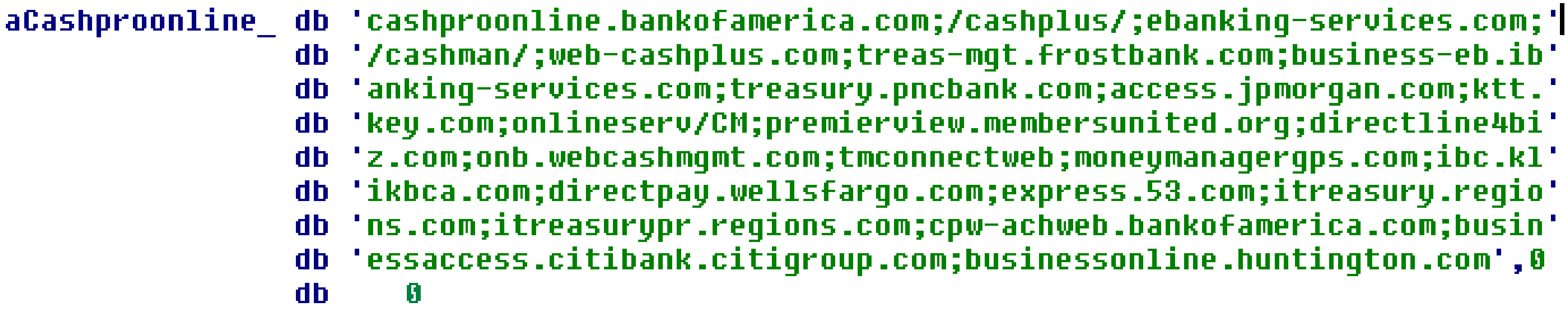
Clean

```
c:\Program Files (x86) BUILTIN\Users:R
                       BUILTIN\Users:(OI)(CI)(IO)(special access:)
                                                 GENERIC_READ
                                                 GENERIC_EXECUTE
                       BUILTIN\Power Users:C
                       BUILTIN\Power Users:(OI)(CI)(IO)C
                       BUILTIN\Administrators:F
                       BUILTIN\Administrators:(OI)(CI)(IO)F
                       NT AUTHORITY\SYSTEM:F
                       NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
                       BUILTIN\Administrators:F
                       CREATOR OWNER:(OI)(CI)(IO)F
```

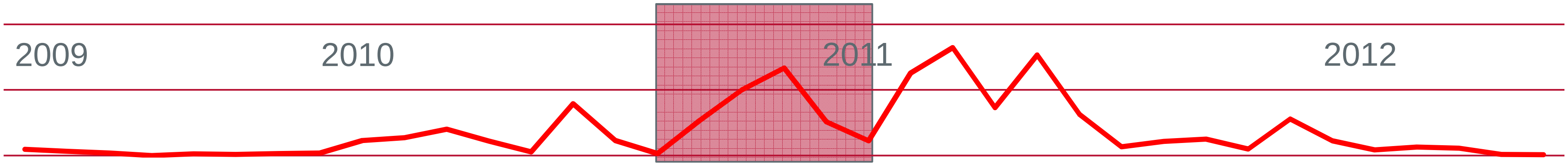


Pinkslipbot – Q3/Q4 2010

- Change in network infrastructure to bulletproofed servers in Ukraine
- Stolen data sent to FTP server
- Able to infect HTML files (.asp, .pl, .php, .htm, .cfm) with <script> code
- Users of the following banks were targeted:

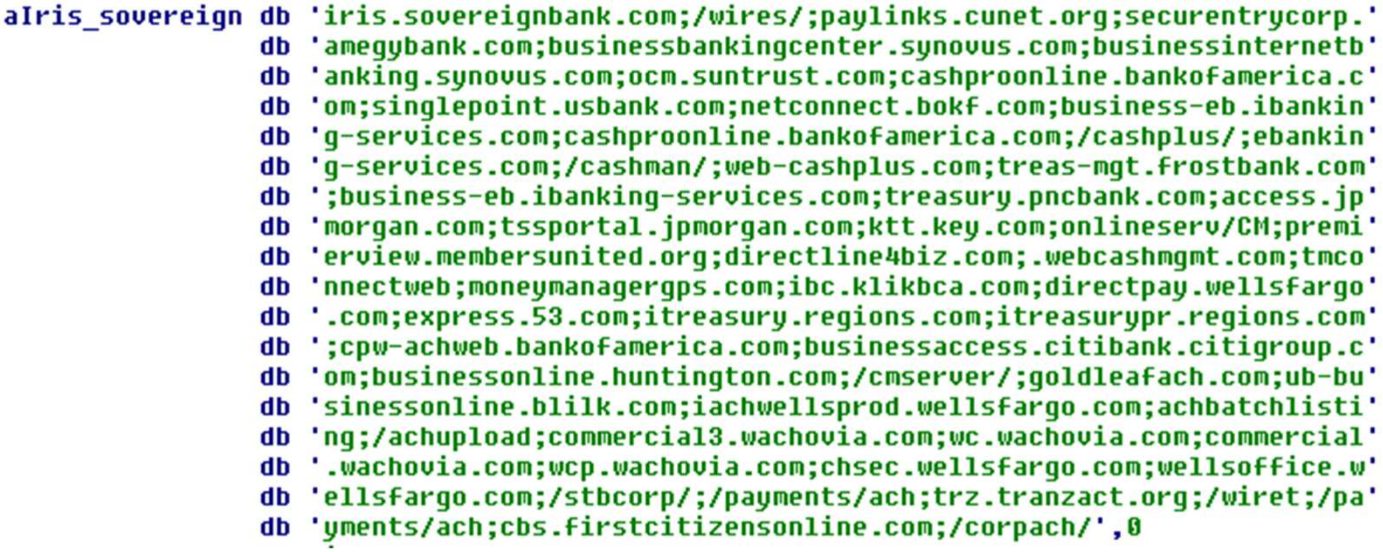


```
aCashproonline_ db 'cashproonline.bankofamerica.com;/cashplus/;ebanking-services.com;'
                db '/cashman/;web-cashplus.com;treas-mgt.frostbank.com;business-eb.ib'
                db 'anking-services.com;treasury.pncbank.com;access.jpmorgan.com;ktt.'
                db 'key.com;onlineserv/CM;premierview.membersunited.org;directline4bi'
                db 'z.com;onb.webcashmgmt.com;tmconnectweb;moneymanagergps.com;ibc.kl'
                db 'ikbca.com;directpay.wellsfargo.com;express.53.com;itreasury.regio'
                db 'ns.com;itreasurypr.regions.com;cpw-achweb.bankofamerica.com;busin'
                db 'essaccess.citibank.citigroup.com;businessonline.huntington.com',0
                db    0
```

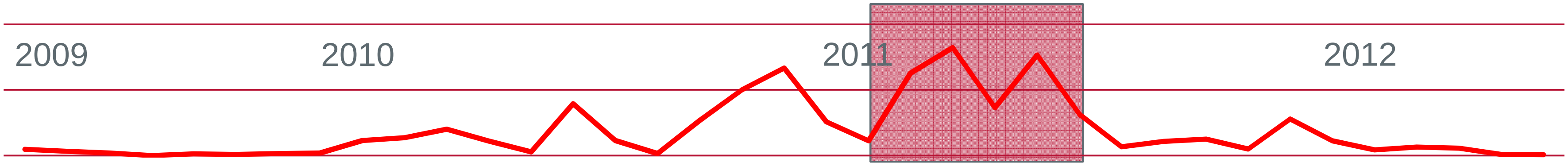


Pinkslipbot – Q1/Q2 2011

- Starts to use UPX + second-level obfuscator
- Social Engineering: AutoRun variant uses folder icons
- DLL component and configuration now comes embedded in EXE resource section
- Users of the following banks were targeted:



```
aIris_sovereign db 'iris.sovereignbank.com;/wires/;paylinks.cunet.org;securentrycorp.'
                db 'amegybank.com;businessbankingcenter.synovus.com;businessinternetb'
                db 'anking.synovus.com;ocm.suntrust.com;cashproonline.bankofamerica.c'
                db 'om;singlepoint.usbank.com;netconnect.bokf.com;business-eb.ibankin'
                db 'g-services.com;cashproonline.bankofamerica.com;/cashplus/;ebankin'
                db 'g-services.com;/cashman/;web-cashplus.com;treas-mgt.frostbank.com'
                db ';business-eb.ibanking-services.com;treasury.pncbank.com;access.jp'
                db 'morgan.com;tssportal.jpmorgan.com;ktt.key.com;onlineserv/CM;premi'
                db 'erview.membersunited.org;directline4biz.com;.webcashmgmt.com;tmco'
                db 'nnectweb;moneymanagergps.com;ibc.klikbca.com;directpay.wellsfargo'
                db '.com;express.53.com;itreasury.regions.com;itreasurypr.regions.com'
                db ';cpw-achweb.bankofamerica.com;businessaccess.citibank.citigroup.c'
                db 'om;businessonline.huntington.com;/cmserver/;goldleafach.com;ub-bu'
                db 'sinessonline.blilk.com;iachwellsprod.wellsfargo.com;achbatchlisti'
                db 'ng;/achupload;commercial3.wachovia.com;wc.wachovia.com;commercial'
                db '.wachovia.com;wcp.wachovia.com;chsec.wellsfargo.com;wellsoffice.w'
                db 'ellsfargo.com;/stbcorp/;/payments/ach;trz.tranzact.org;/wiret;/pa'
                db 'yments/ach;cbs.firstcitizensonline.com;/corpach/',0
```

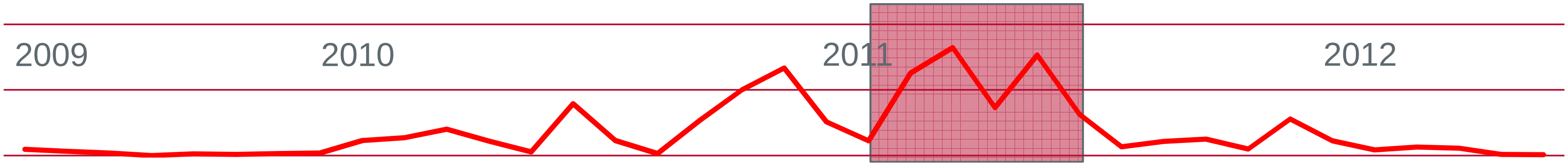


Pinkslipbot – Q1/Q2 2011

- First variants featuring user-mode rootkits
- Used to protect the main EXE and to hijack IE functions

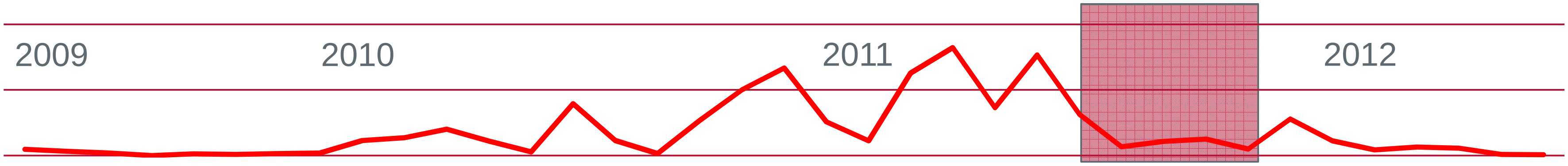
ntdll.dll!NtQuerySystemInformation
ntdll.dll!NtResumeThread
kernel32.dll!GetProcAddress
WININET.dll!InternetCloseHandle
WININET.dll!HttpOpenRequestA
WININET.dll!InternetReadFile
WININET.dll!InternetQueryDataAvailable
WININET.dll!HttpSendRequestA
WININET.dll!HttpSendRequestW
WININET.dll!InternetReadFileExA

iphlpapi.dll!GetTcpTable
iphlpapi.dll!AllocateAndGetTcpExTableFromStack
WS2_32.dll!connect
WS2_32.dll!send
WS2_32.dll!WSASend
WS2_32.dll!WSAConnect
ADVAPI32.dll!RegEnumValueW
ADVAPI32.dll!RegEnumValueA
USER32.dll!TranslateMessage
USER32.dll!GetClipboardData
USER32.dll!CharToOemBuffA

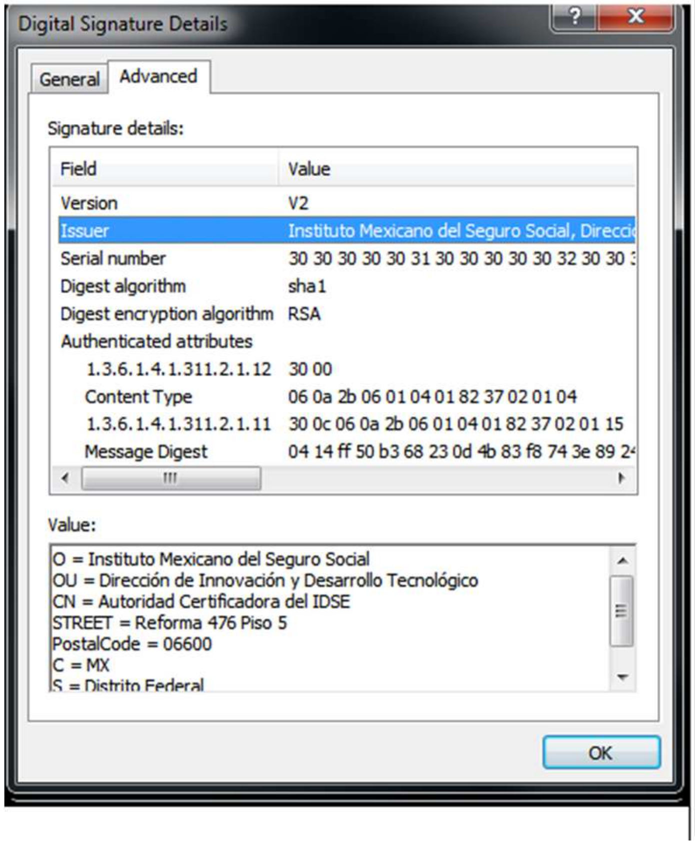


Pinkslipbot – Q3/Q4 2011

- Intense development cycle
- Not very effective in customer networks
- Hints that they might be targeting specific AV features
- First stolen digital certificates being used in binaries
- Change in SXOR encryption for configuration file
  - New heavy encryption layer added



Pinkslipbot – Q3/Q4 2011

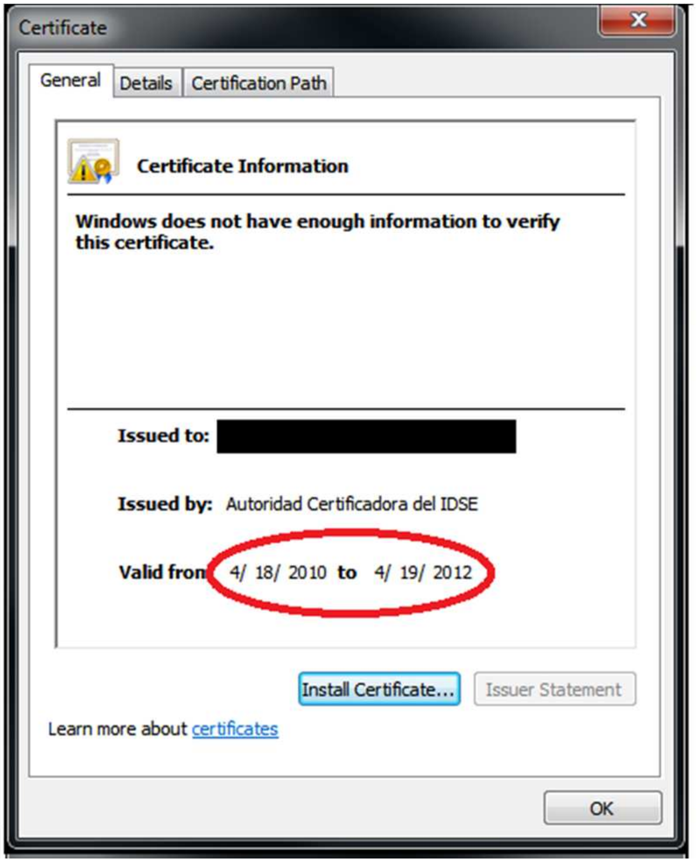


Signature details:

Field	Value
Version	V2
Issuer	Instituto Mexicano del Seguro Social, Direcci
Serial number	30 30 30 30 30 31 30 30 30 30 30 32 30 30 3
Digest algorithm	sha1
Digest encryption algorithm	RSA
Authenticated attributes	
1.3.6.1.4.1.311.2.1.12	30 00
Content Type	06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0c 06 0a 2b 06 01 04 01 82 37 02 01 15
Message Digest	04 14 ff 50 b3 68 23 0d 4b 83 f8 74 3e 89 2

Value:

O = Instituto Mexicano del Seguro Social
OU = Dirección de Innovación y Desarrollo Tecnológico
CN = Autoridad Certificadora del IDSE
STREET = Reforma 476 Piso 5
PostalCode = 06600
C = MX
S = Distrito Federal



Certificate Information

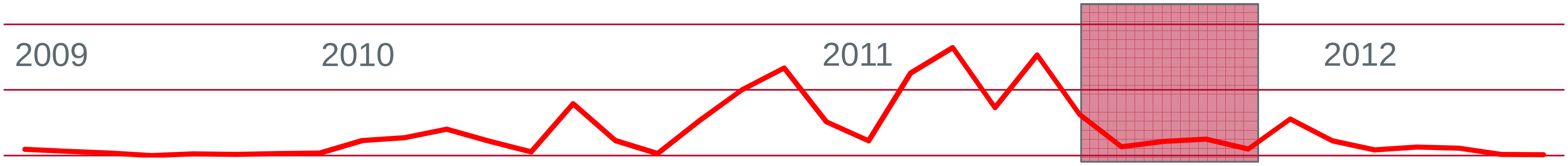
Windows does not have enough information to verify this certificate.

Issued to: [redacted]

Issued by: Autoridad Certificadora del IDSE

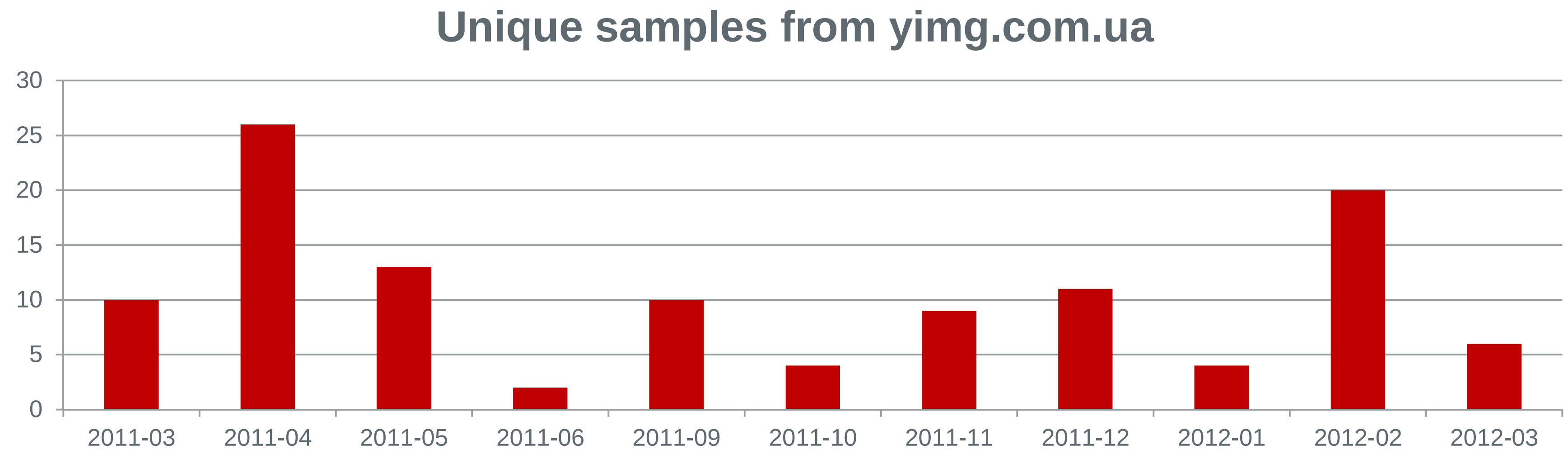
Valid from 4/ 18/ 2010 to 4/ 19/ 2012

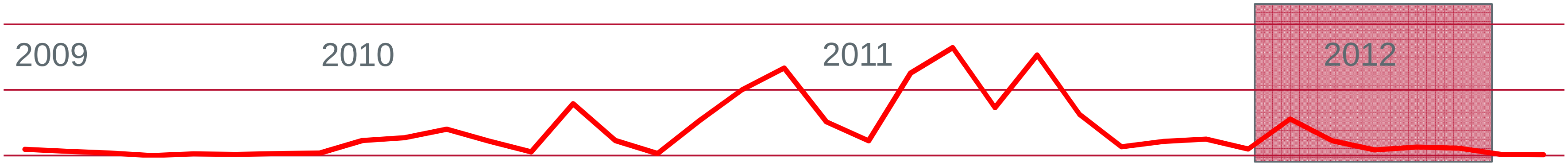
Learn more about certificates



Pinkslipbot – Q1 2012

- Obfuscator looks more and more like that used by Zeus variants
- Virus activity under control
- Activity from update server:





Future (Current) Developments

- New variant showing up week prior to this conference
  - New obfuscation, same as many Zbot variants
  - Doubled number of affected banks
  - Change in behavior:
    - DLL module is directly injected in memory (no file on disk!)

- Future developments
  - Improved rootkit
  - More anti-AV features
  - Change in spread method

- Interaction with other malware families
  - Partner with another backdoor or integrate in its own code
  - Code integration with Zeus

2009
2010
2011
2012

Acknowledgments

- McAfee Labs Threat Advisory
  - https://kc.mcafee.com/corporate/index?page=content&id=PD22960
- McAfee Labs Sample Database Team
- Personal Communication (McAfee Labs): Abhishek Karnik, Mark Olea, Srinivasa Kanamatha, François Paget
- For contributions during preparation of this report:
  - Jacomo Dimmit (Team Cymru)
  - Ivo Peixinho (Brazilian Federal Police)

Guilherme_Venere@mcafee.com
@gvenere