

Son of SpyEye – a crimeware soap opera

SESSION ID: CLE-T11

Maurits Lucas

InTELL Business Director
Fox-IT
@lucasmaurits



Contents

- ◆ Who we are: About Fox-IT and InTELL
- ◆ It begins: ZeuS or Zbot
- ◆ Anatomy of a MITB attack
- ◆ The early years: the battle between ZeuS and SpyEye
- ◆ An unholy alliance followed by a leak
- ◆ He's back: P2PZeuS – first of a new generation
- ◆ Hiding in the crowd: Tilon
- ◆ The unmasking of Tilon
- ◆ Endgame?

RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN



About Fox-IT

GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm

Belgacom boss says no company or country could have withstood cyber-attack of this size and sophistication

Ian Traynor in Brussels

The Guardian Thursday 9 October 2014 10:05 BST

Malware attack hits thousands of Yahoo users per hour

By Faith Karimi and Joe Sutton, CNN
January 6, 2014 -- Updated 1342 GMT (2142 HKT)

SHARE THIS



Recommend 5.5k



Most Popular >>

Today's five most popular stories

Mary Kay Letourneau, convicted of child abuse, arrested in Washington state

Judge rules Chicago gun ban unconstitutional

Fox-IT technology leadership



GROUPON

www.groupon.nl
*Voorbeeld van toekomstige deals

tot **70% KORTING**

RISK ASSESSMENT / SECURITY & HACKTIVISM

Sudden spike of Tor users likely caused by one "massive" botnet

Proven track record

What our customers say

“Fox are different, they focus on the evolving criminal ecosystem, they track Actors, they provide global visibility of the threat landscape in real-time and when it comes to credit cards they have saved us hundreds if not millions in the past 6 months, everything we get from them is actionable. Then there is the other value they have, a track record of working with the Russians and bringing people to court, this helps us also.” – VP Threat Intelligence, Global FinServ

“We built a Threat Platform to create real-time visibility of our enterprise architecture and assets, what was missing was actionable intelligence, after a thorough review of the major suppliers we selected Fox-IT from Europe. The biggest difference was their understanding of how the criminals evolve and the impact to our business. InTELL paid for itself within 6 weeks and within the first nine months they had saved us in excess of 10 of million in Fraud which we would not have detected without InTELL.” - CISO, Global Retailer



Three attack phases

Preparation

Attack execution

Recovery



InTELL

Prevention



DetACT

Detection



FOXCERT

Reaction

InTELL

Three layers of intelligence

Actionable info

Infected IP lists
Compromised cards
Account thefts
Mule lists
STIX / TAXII

Real-time threats

(Forensic) malware analysis
MO analysis
Detection rules
Attack preparation
Alerting

Global trends

Peer & sector threats
Geographical trends
Technical trends
Actor attribution
Brand protection

RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



It begins

It begins – ZeuS

- ◆ The *original* “cybercrime kit”
- ◆ First appears in 2006
- ◆ Version 1 from 2006 – 2009, V2 from 2009 - 2011
- ◆ Aim: steal credentials and money from customers of financial institutions
- ◆ Also known as: Prg, Zbot, Infostealer.Banker.C, Banker.C, Infostealer.C, ntos and notos
- ◆ Infected machines download a *Config* containing the attack(s) and “phone home” to a command & control server
- ◆ ZeuS can carry out *Man in the Browser* attacks



Anatomy of a MITB attack

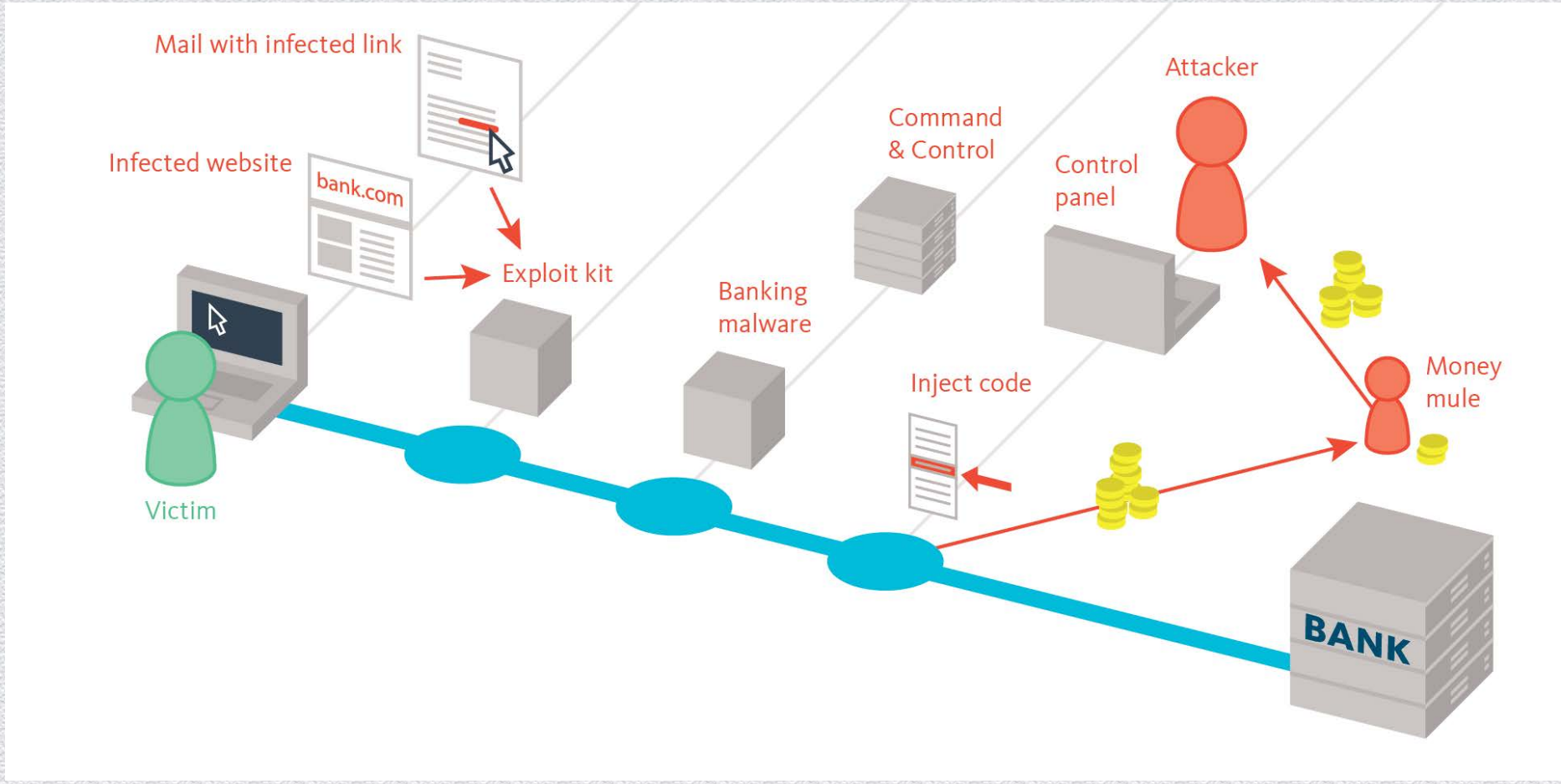
What is MITB?

- ◆ Aimed at defeating TLS / SSL as a measure to protect content between server and user
- ◆ Malware “hooks” web browser, enabling it to modify content just before it is rendered
- ◆ Any TLS / SSL has already been terminated
- ◆ Result: modify contents at will while “lock” icon and URL look fine to user.



Important: MITB malware \neq attack!

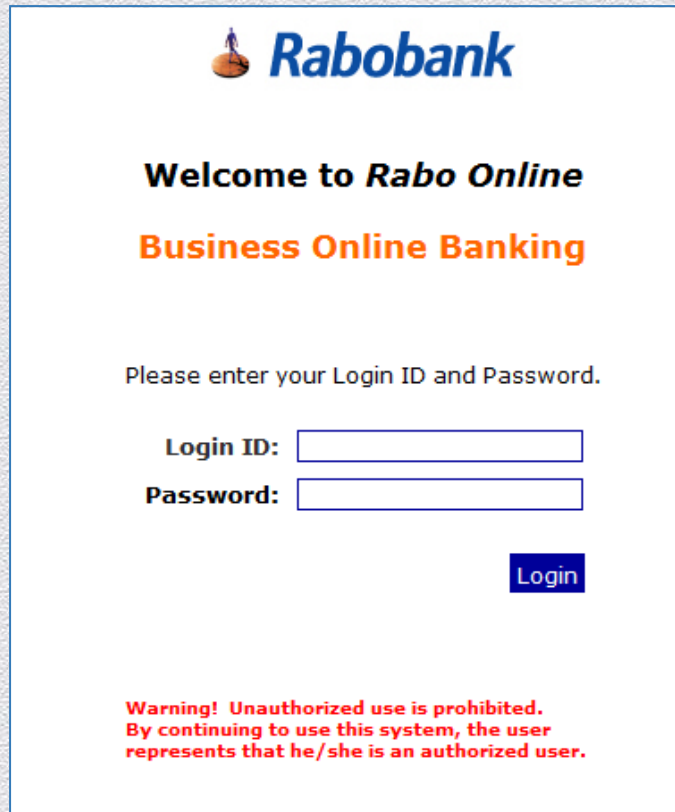
- ◆ The malware is not the attack!
- ◆ It is a *platform* from which the attack is launched
- ◆ The *inject code* forms the actual attack
- ◆ Attackers can (and do) switch malware families!
- ◆ Malware does have its own functionality:
 - ◆ Steal credentials
 - ◆ Copy traffic
 - ◆ Take screenshots
 - ◆ Keylogger
 - ◆ RDP
 - ◆ SOCKS proxy – so you can connect from victim IP




Main components in MITB attack

All of this so you can

Turn this




**Welcome to Rabo Online
Business Online Banking**

Please enter your Login ID and Password.

Login ID:
Password:

**Warning! Unauthorized use is prohibited.
By continuing to use this system, the user
represents that he/she is an authorized user.**

Into this





**Welcome to Rabo Online
Business Online Banking**

Please enter your Login ID and Password.

Login ID:
Password:
Passcode:

Source: attack.on-web-cashplus.com



**SpyEye - the early
years**

SpyEye

- ◆ First appeared in 2009
- ◆ Initially in beta with fast development
- ◆ Competitor to ZeuS
- ◆ The author went by the aliases **Gribodemon** and **Harderman**
- ◆ Quickly gained market share

2012 02/09 00:55:51

2399 k +448

Find INFO Statistic FTP accounts Settings

Screen shots BOA Grabber VISA CC Grabber Certificate Grabber

Get Credit Cards v0.1 +662

Bot GUID :

Report date region : 08/02/2012 ... 08/02/2012 clean

Data :

Limit :

with CVV only :

with Address only :

submit

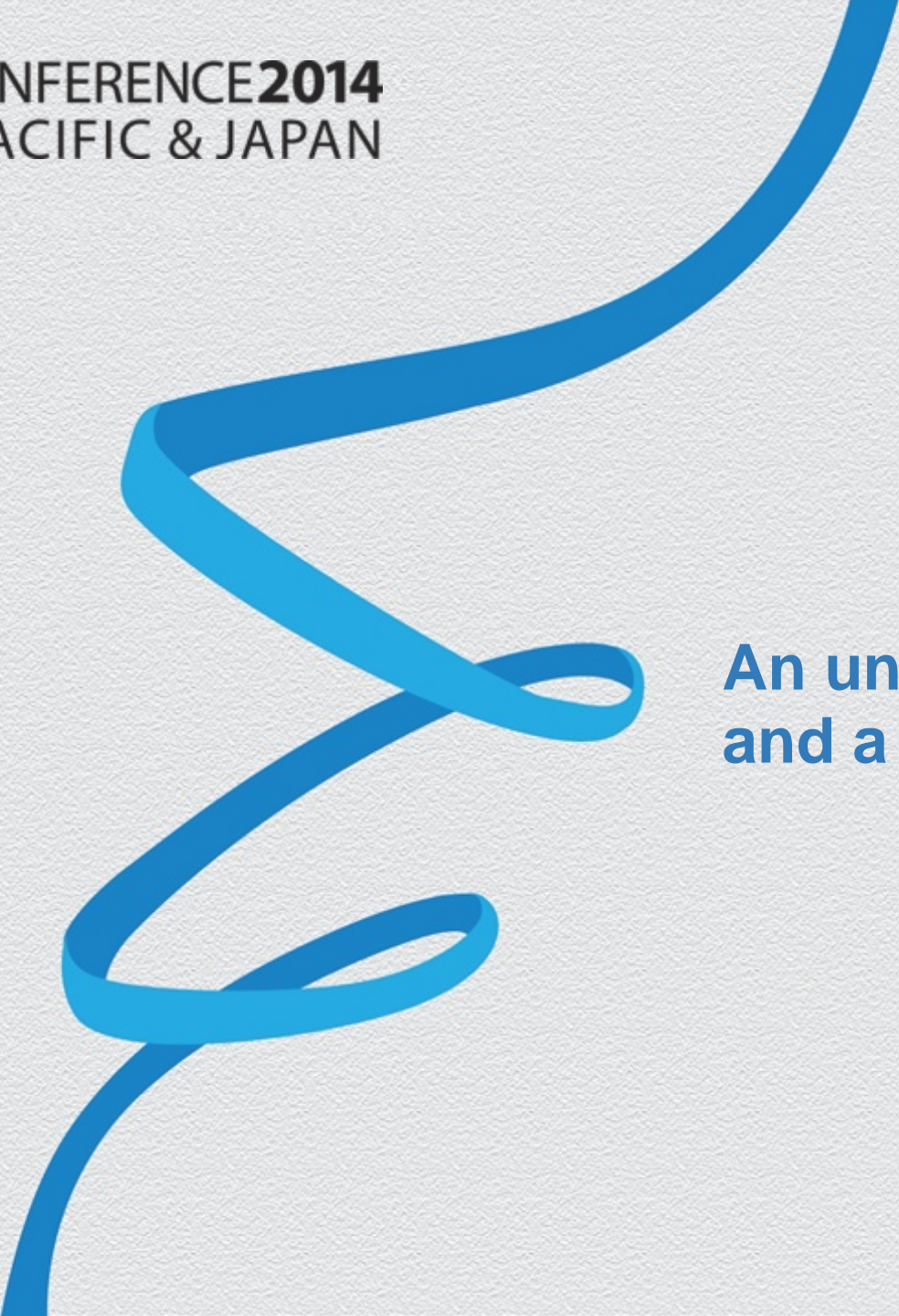
SpyEye modules

- ◆ The core SpyEye software could be extended with modules which delivered extra functionality
- ◆ Popular ones we saw being used over time:

Name	Function
customconnector.dll	Support for multiple fallback C&C servers
socks5.dll	Socks backconnect
ccgrabber.dll	Generic algorithm for grabbing cc details
ffcertgrabber.dll	Grab certs from Firefox cert store
rdp.dll	RDP functionality
ftp.dll	FTP backconnect
emailgrabber.dll	Grab contents of Outlook address book
ftpgrabber.dll	Grab FTP creds from multiple clients
ActiveAZ	Automatically insert transactions

SpyEye versus ZeuS

- ◆ SpyEye aggressively went after ZeuS market share
- ◆ SpyEye “retailed” at \$1,000 USD versus ZeuS at \$8,000 USD for a ZeuS V2
- ◆ A fierce battle ensued
- ◆ When dropped on a machine, SpyEyewould check for the presence of ZeuS and, if found, remove it
- ◆ SpyEye adopted the ZeuS config format for web injects, making it easier to switch
- ◆ This example was followed by others, ZeuS style web injects are now the “MS Word” of malware configs




**An unholy alliance
and a leak**

An unholy alliance

- ◆ In October 2010 ZeuS was at V2.0.8.9 with no updates for quite some time
- ◆ Suddenly Slavik announces development will cease and
- ◆ **Support will be handed over to Gribodemon, the SpyEye author!**
- ◆ Stories abound of the imminent appearance of a Super SpyEye – nothing ever materialised
- ◆ But we did see “unofficial” versions, meaning the source had been shared

A big leak

- ◆ Early in 2011 the entire ZeuS 2.0.8.9 sourcecode was leaked
- ◆ This meant anyone could develop MITB malware based on the ZeuS sourcecode
- ◆ An enormous amount of ZeuS type malware families exploded onto the scene, some becoming successful products in their own right:
 - ◆ ICE-IX
 - ◆ Citadel
- ◆ But some were barely improvements on the original
- ◆ Soon after SpyEye development started to falter and 1.3.48 in October 2011 was the last version



**A new chapter –
Malware as a Service**

P2PZeuS

- ◆ Slavik never gave up on ZeuS!
- ◆ After the leak of 2.0.8.9, he worked on version 2.1
- ◆ This was not sold as a kit, but could only be rented: Malware as a Service
- ◆ ZeuS 2.1 migrated to ZeuS 3 in September 2011 with a P2P C&C protocol
- ◆ This became P2PZeus build 1
- ◆ P2PZeuS was also malware as a service
- ◆ A core gang including Slavik used it to target commercial banking

But where was Gribodemon?

- ◆ SpyEye development meanwhile had ceased
- ◆ Gribodemon seemed to have vanished or retired
- ◆ In August 2012 a new trojan appears and is named Tilon because the loader seems based on Silon
- ◆ But in the fall of 2013 we analyse Tilon in depth including its backend and it turns out *only* the loader comes from Silon.
- ◆ Most of the core is a reworked, further developed SpyEye
- ◆ Developed means the team have access to the SpyEye sourcecode – which was never leaked!

What actually happened in 2011

- ◆ Slavik was already part of a gang which went after high value accounts
- ◆ ZeuS support had become a drain and unwelcome attention
- ◆ He turned over ZeuS to Gribodemon to take away heat
- ◆ Gribodemon realised this too – kit malware is a hassle!
- ◆ Around release of SpyEye 1.3.48 they started work on a rented / managed trojan
- ◆ This was SpyEye2, erroneously labelled “Tilon”
- ◆ Some SpyEye customers where invited to switch
- ◆ Most weren't



**Tilon? SpyEye2 you
mean!**

The evidence

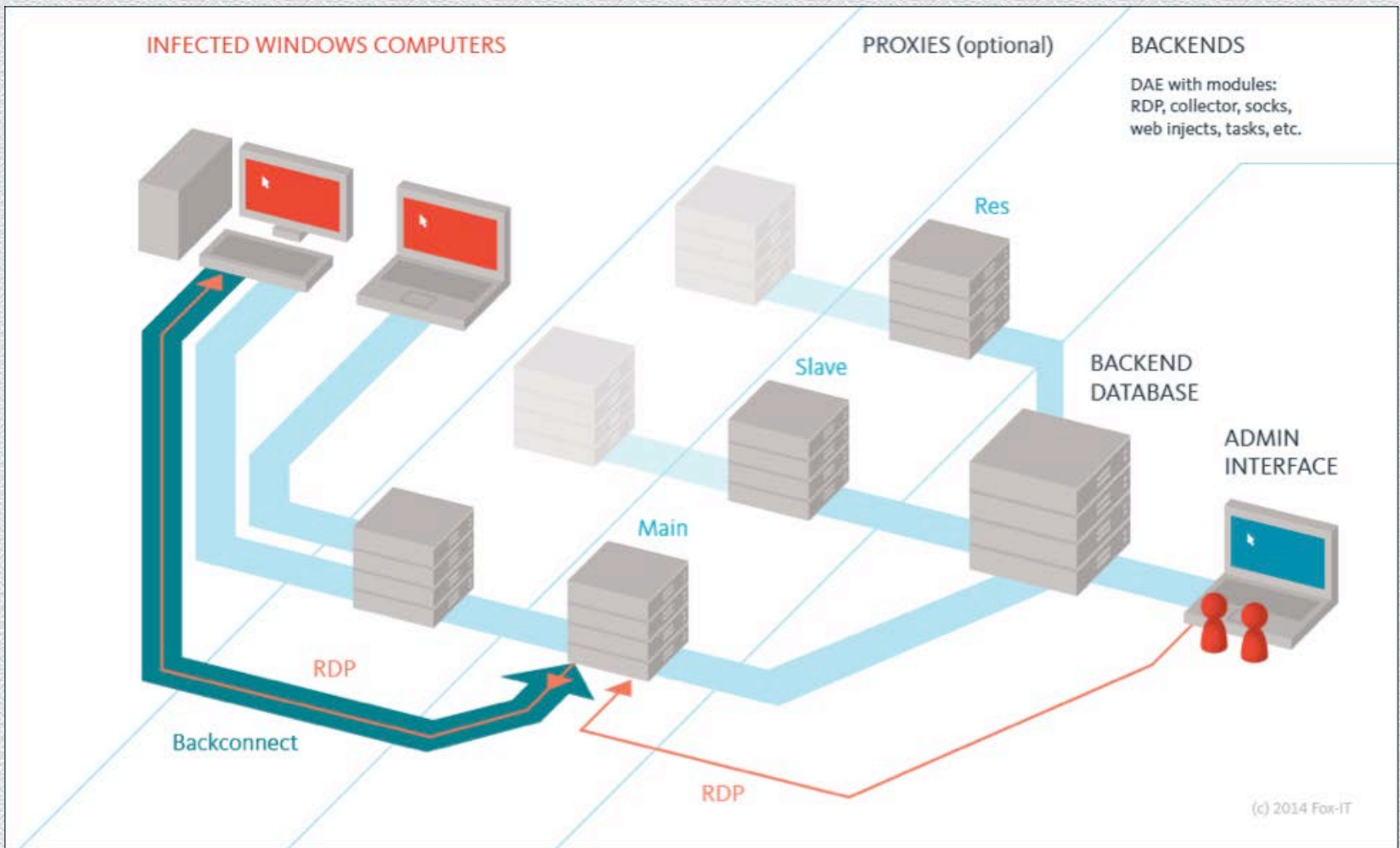


Exhibit 1: Infrastructure

The Tilon backend components are very similar to SpyEye

Exhibit 2: Code comparison functions

SpyEye 1.3.48

```
push esi
push edi
mov esi, offset aHttp ; "http:"
lea edi, [ebp+var_94]
movsd
movsw
lea ecx, [eax+1]
mov [ebp+var_C], ebx
movsw
mov [ebp+var_44], 'tnoC'
mov [ebp+var_40], '-tne'
mov [ebp+var_3C], 'epyT'
mov [ebp+var_38], 'pa :'
mov [ebp+var_34], 'cilp'
mov [ebp+var_30], 'oita'
mov [ebp+var_2C], '-x/n'
mov [ebp+var_28], 'scf'
mov [ebp+var_6C], 'tnoC'
mov [ebp+var_68], '-tne'
mov [ebp+var_64], 'epyT'
mov [ebp+var_60], 'pa :'
mov [ebp+var_5C], 'cilp'
mov [ebp+var_58], 'oita'
mov [ebp+var_54], '-x/n'
mov [ebp+var_50], 'pmoc'
mov [ebp+var_4C], 'sser'
mov [ebp+var_48], bl
mov [ebp+var_24], 75410A0Dh
mov [ebp+var_20], 'roht'
mov [ebp+var_1C], 'tazi'
mov [ebp+var_18], ':noi'
mov [ebp+var_14], 'saB'
mov [ebp+var_10], 'ci'
test ecx, ecx
jz short loc_425308
```

SpyEye2

```
cmp dword_1004F450, 0
mov esi, offset aHttp ; "http:"
lea edi, [ebp+Buf2]
movsd
movsw
mov [ebp+var_1C], 75410A0Dh
mov [ebp+var_18], 'roht'
mov [ebp+var_14], 'tazi'
mov [ebp+var_10], ':noi'
mov [ebp+var_C], 'saB'
mov [ebp+var_8], 'ci'
jz short loc_1000B2D6

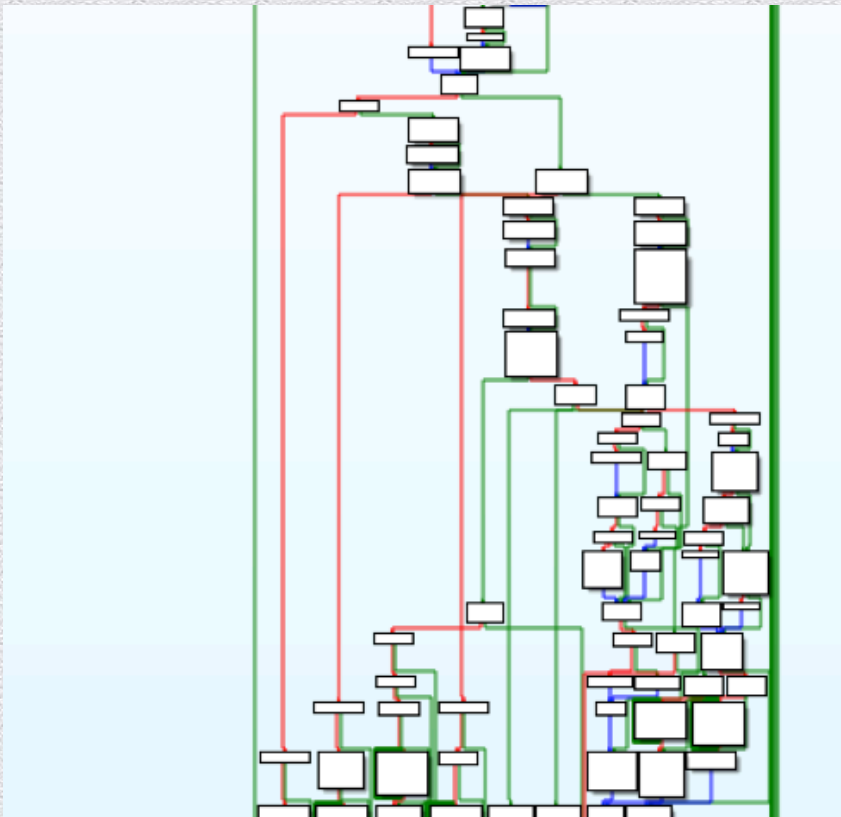
...

loc_1000B2D6:
cmp [ebp+var_68], 0
mov [ebp+var_3C], 'tnoC'
mov [ebp+var_38], '-tne'
mov [ebp+var_34], 'epyT'
mov [ebp+var_30], 'pa :'
mov [ebp+var_2C], 'cilp'
mov [ebp+var_28], 'oita'
mov [ebp+var_24], '-x/n'
mov [ebp+var_20], 'scf'
mov [ebp+var_64], 'tnoC'
mov [ebp+var_60], '-tne'
mov [ebp+var_5C], 'epyT'
mov [ebp+var_58], 'pa :'
mov [ebp+var_54], 'cilp'
mov [ebp+var_50], 'oita'
mov [ebp+var_4C], '-x/n'
mov [ebp+var_48], 'pmoc'
mov [ebp+var_44], 'sser'
mov [ebp+var_40], 0
jnz short loc_1000B3CB
```

Content-Type: application/x-fcs, Content-Type: application/x-compress, Authorization: Basic

Exhibit 3: Internal structure of function

SpyEye 1.3.48



SpyEye V2

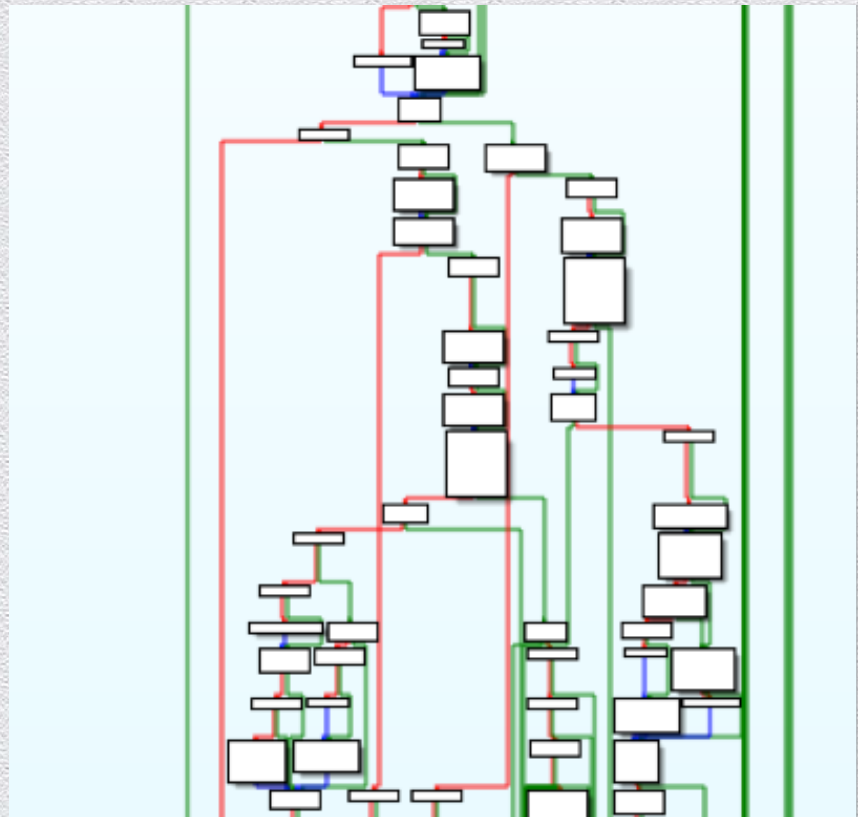


Exhibit 4: Changed Firefox settings

```
unicode 0, <\prefs.js>,0
db 'user_pref("browser.safebrowsing.enabled", false);',0Dh,0Ah ; DATA XREF:
db 'user_pref("browser.safebrowsing.malware.enabled", false);',0Dh,0Ah
db 'user_pref("security.warn_entering_weak", false);',0Dh,0Ah
db 'user_pref("security.warn_entering_weak.show_once", false);',0Dh,0Ah
db 'user_pref("security.warn_viewing_mixed", false);',0Dh,0Ah
db 'user_pref("security.warn_viewing_mixed.show_once", false);',0Dh,0Ah
db 'user_pref("privacy.clearOnShutdown.cookies", false);',0Dh,0Ah
db 'user_pref("privacy.clearOnShutdown.sessions", false);',0Dh,0Ah
db 'user_pref("network.http.spdy.enabled", false);',0Dh,0Ah,0
```

- ◆ The exact same settings in the same order are present in both
- ◆ The only difference is the last setting, this only appears in SpyEye2
- ◆ But this feature was added to Firefox after SpyEye 1.3.48 was released
- ◆ But before SpyEye2
- ◆ They just added it to the bottom...

Exhibit 5: Various tidbits

- ◆ RDP configuration files are very similar
- ◆ Both refer to “Sausages” and “Sausage Patterns”
- ◆ All previous examples were from main program section, not modules
- ◆ Shows that authors had access to SpyEye core sourcecode
- ◆ SpyEye 1 had version numbers 1.x.y, last released being 1.3.48 and 1.3.49 in development
- ◆ SpyEye 2 has version numbers 2.0.x

So that rivalry, how did it end?

SpyEye 1+2 Gribodemon



LATEST RUSSIAN CITIZEN EXTRADITION
RAISES CONCERN OVER 'VICIOUS TREND'

EGYPT: THOUSANDS OF PRO-MORSI ACTIVISTS DEFEAT GOVT BAN

(P2P)ZeuS - Slavik

**WANTED
BY THE FBI**

o Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoor"

DESCRIPTION

Birth Used: October 28, 1983	Hair: Brown (usually shaves his head)
Height: Approximately 5'9"	Eyes: Brown
Weight: Approximately 180 pounds	Sex: Male
NCIC: W890989955	Race: White

Occupation: Bogachev works in the Information Technology field.

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may be located at various locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

CAUTION