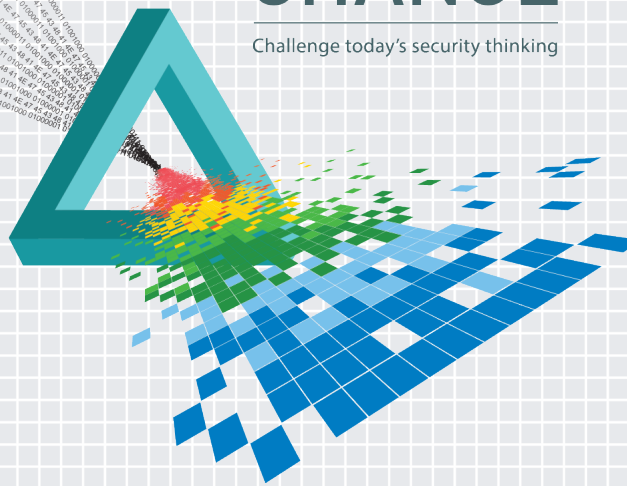
RSAC Studio

CHANGE

Challenge today's security thinking

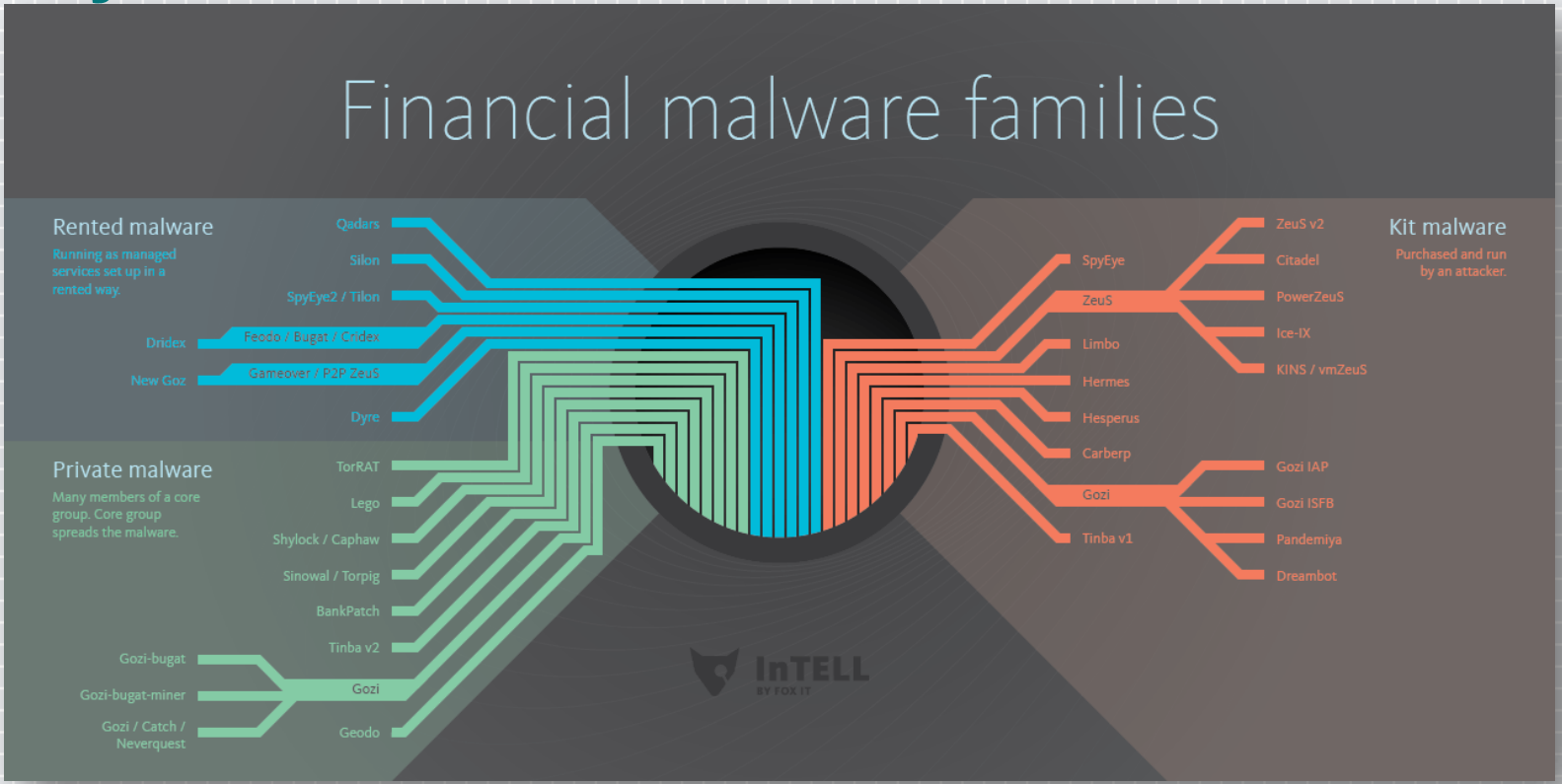


A Short History of Attacks on Finance

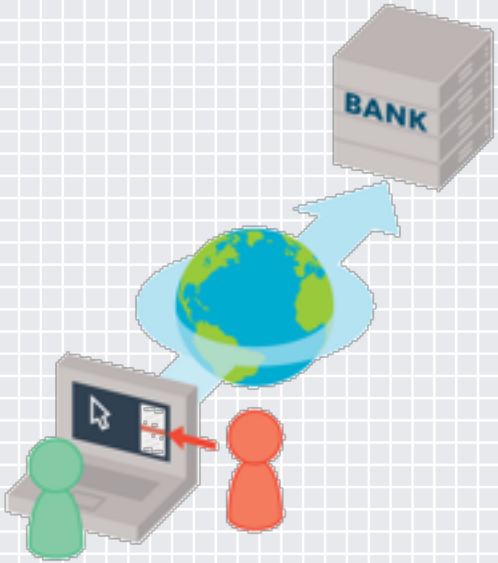
Maurits Lucas

InTELL Business Director
Fox-IT
@lucasmaurits

Today

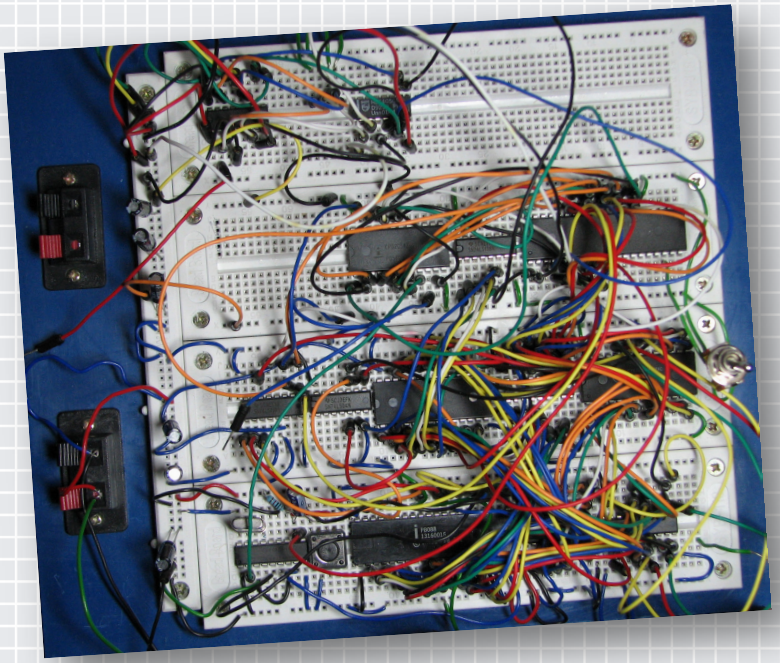

Financial malware families
Rented malware
Running as managed services set up in a rented way.
Qadars
Silon
SpyEye2 / Tilon
Dridex
Feodo / Bugat / Cridex
New Goz
Gameover / P2P ZeuS
Dyre
Private malware
Many members of a core group. Core group spreads the malware.
TorRAT
Lego
Shylock / Caphaw
Sinowal / Torpig
BankPatch
Tinba v2
Gozi-bugat
Gozi-bugat-miner
Gozi / Catch / Neverquest
Gozi
Geodo
SpyEye
ZeuS
Limbo
Hermes
Hesperus
Carberp
Gozi
Tinba v1
ZeuS v2
Citadel
PowerZeuS
Ice-IX
KINS / vmZeuS
Gozi IAP
Gozi ISFB
Pandemiya
Dreambot
Kit malware
Purchased and run by an attacker.
InTELL
BY FOX IT

Man In The Browser



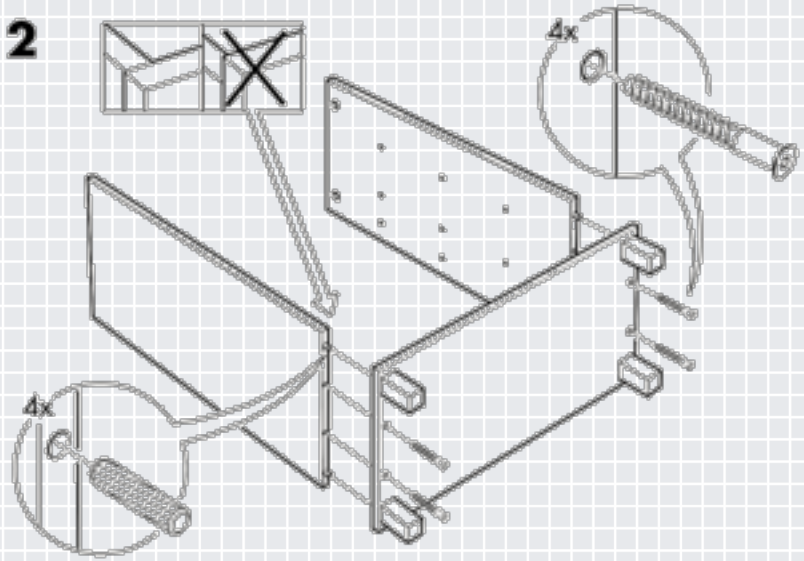
- Most Financial Malware is Man In The Browser malware
- The aim is to defeat SSL / TLS
- Malware hooks the browser
- Modifies pages after it exits the SSL tunnel

Roll your own – 2004 - 2007



- *Bankpatch*
- *Haxdoor*
- *A-311 Death*
- *Limbo / Nethell*
- Lots of tweaking required
- Makes old hands misty eyed…

Cybercrime kits - 2006



- In 2006 **ZeuS** appears
- The original cybercrime kit
- Now anyone can run an attack
- Author goes by the name of **Slavik**
- ZeuS becomes very popular

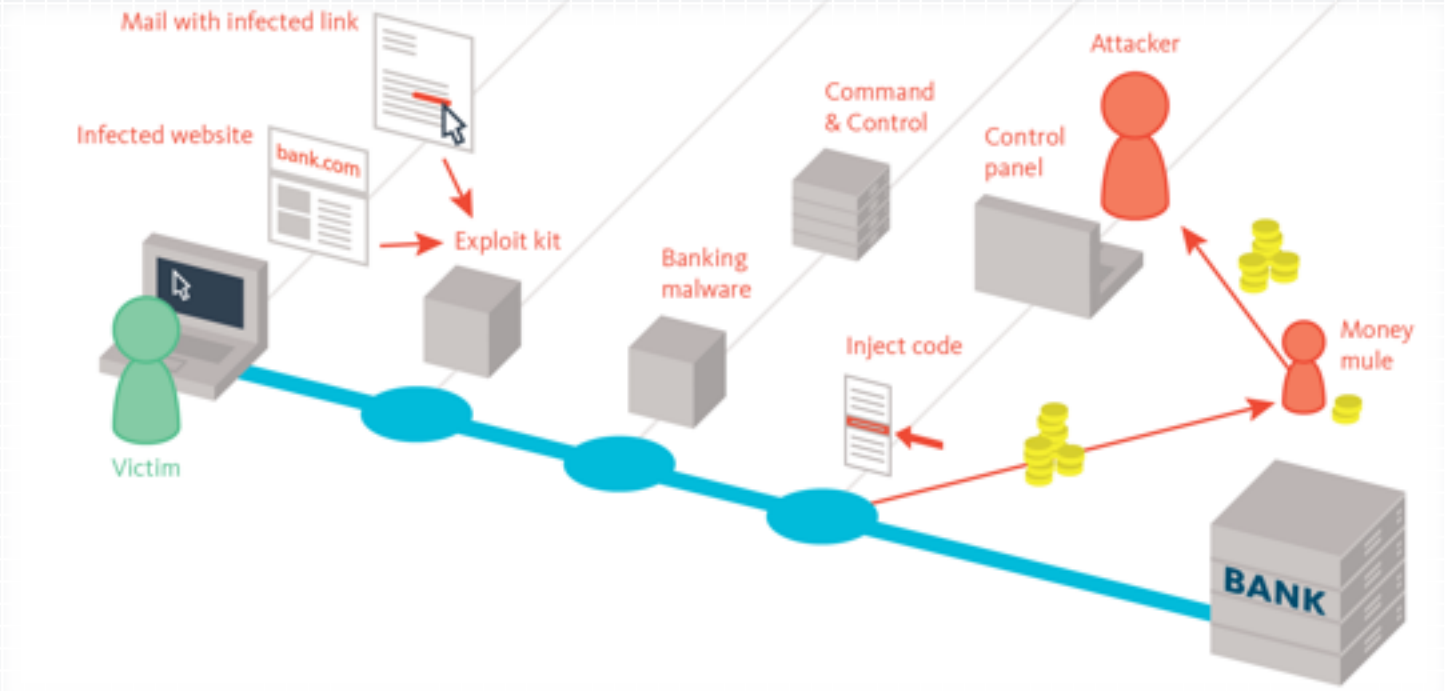
SpyEye enters the stage - 2009

- SpyEye comes out in 2009 gunning for ZeuS market share
- First versions were terrible!
- But cheap: $1000 versus $8000
- Author is **Gribodemon**
- Adopts ZeuS config style
- A battle ensues…

Not the only game in town

- ZeuS and SpyEye were not the only game in town
- **Carberp** – attacks in Europe
- Then went after Russian banks – key members arrested in 2012
- **Sinowal** or “The one that got away” – closed group
- Disappeared in 2013 - unusual

An entire ecosystem appears



An unholy alliance - 2010

What happened

- In October 2010 ZeuS is at version 2.0.8.9
- Suddenly **Slavik** announces he is quitting and

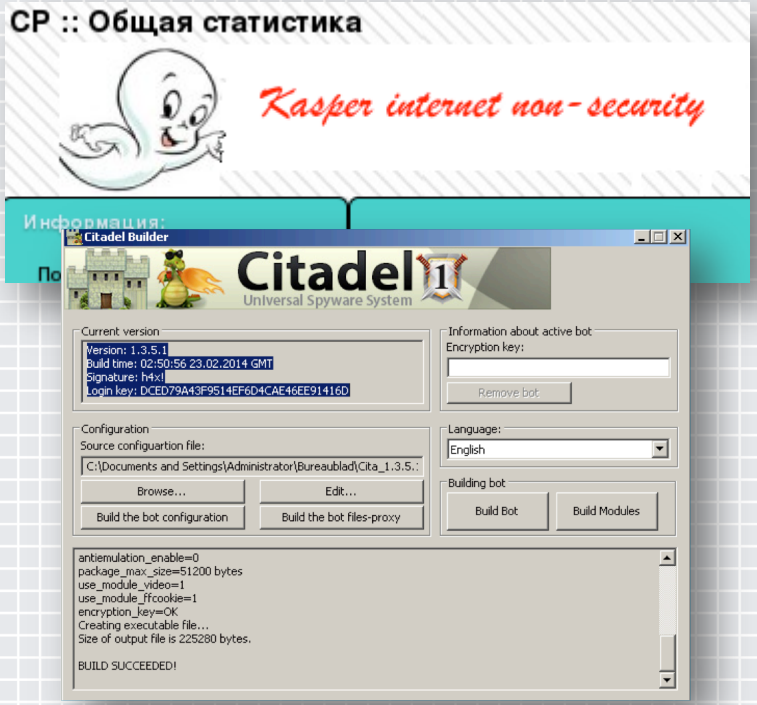
  *handing over support and development to **Gribodemon**, author of SpyEye!*

What *actually* happened

- Slavik was part of a gang using ZeuS to go after high value accounts – **JabberZeuS**
- More profitable than selling ZeuS
- Wants to get rid of kit business
- Starts work on next version which becomes **P2PZeuS**

A big leak - 2011

- Early 2011 the entire ZeuS 2.0.8.9 source code leaks
- Lots of new families appear
  - ICE-IX
  - Citadel
  - KINS
- Cost of malware goes down



The end of SpyEyes - 2013

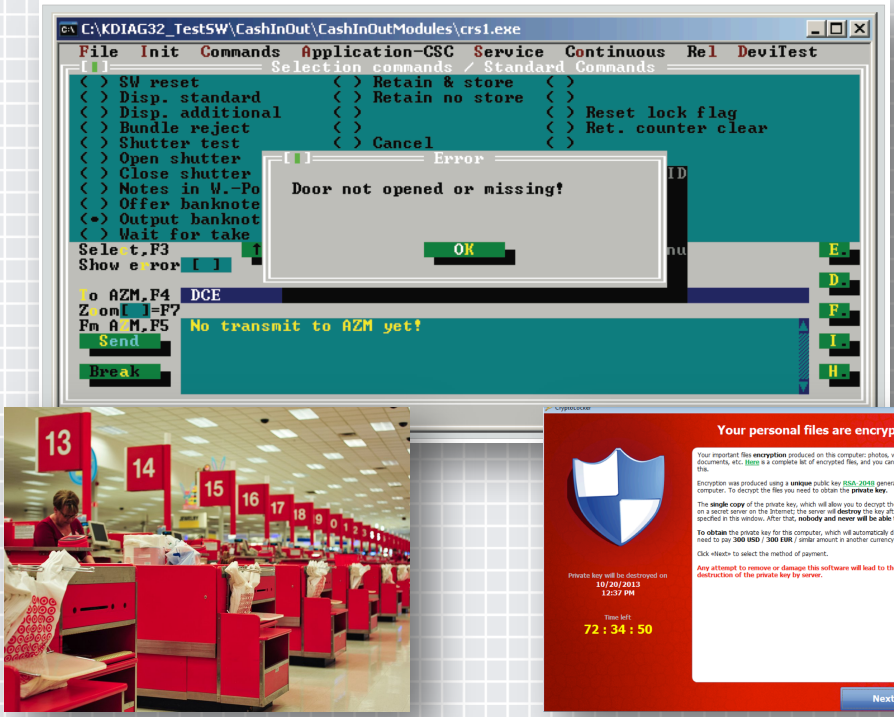
- **Gribodemon** never releases a SpyZeuS
- Instead he too starts working on a managed version of SpyEye, **SpyEye2**
- But he is arrested in 2013 while on holiday in Costa Rica and extradited to the US

P2PZeuS – Halcyon days and demise

- From 2011 – 2014, P2PZeuS is immensely popular
- Active worldwide
- Many groups use it as a platform for attacks
- In 2014 after years of investigation lead by the FBI botnet is taken down
- And Slavik's identity becomes known

And so to the present day

- Former P2PZeuS customers building alternative platforms: **Dyre** and **Dridex**
- Remnants of **Carberp** group involved with **Anunak** – attacks against retail and Russian banks
- Other groups now focusing on retail – Point of Sale
- Copycat Ransomware



What should you take away?

- Financial malware has come a long way – attacks more sophisticated
- Actors in this space are diversifying – retail, ransomware
- Threats evolve, they don't appear out of nowhere
- Context helps you understand - taking a longer view makes things clearer
- Look beyond the malware