RSA CONFERENCE 2013

Security in knowledge

Studio: Trickle-Down Cyberwarfare

Alex Stamos

Artemis Internet

Session ID: STU-T19A

Session Classification: General Interest

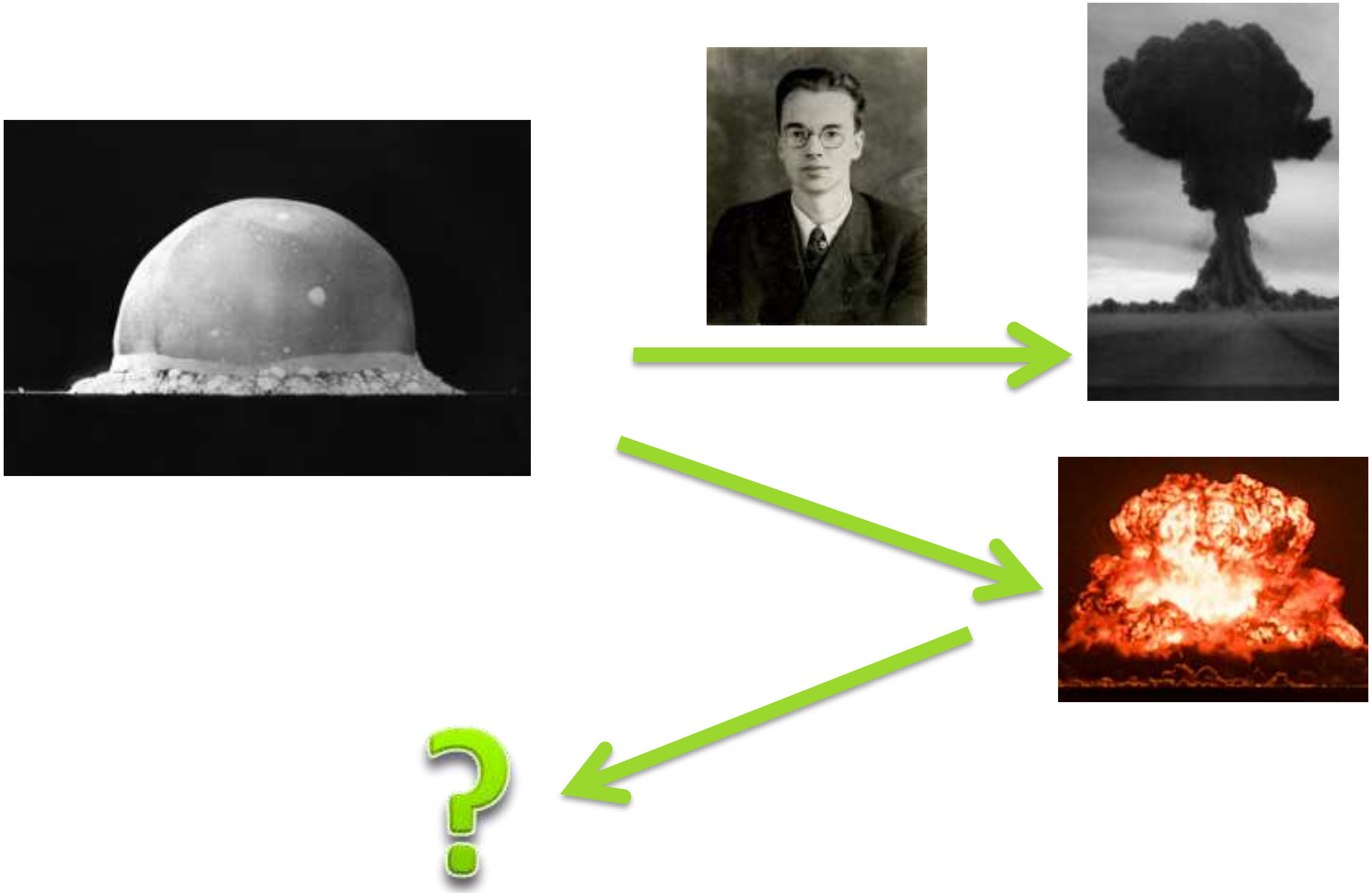
Agenda

- The Trickle Down Effect
- Stuxnet
- Flame
- Red October
- What can we learn from these?

The Trickle Down Effect

- Innovations in warfare always decrease the cost for later adopters.

The Trickle Down Effect



The Trickle Down Effect

- How about with cyber warfare?

- Mid-2000’s Nation State APT:
  - Spear-phish
  - Exploit tied to intelligence on AV
  - Active Directory attacks to spread horizontally
  - Access production data via internal interfaces

Well, maybe not that scary…

So what's next?

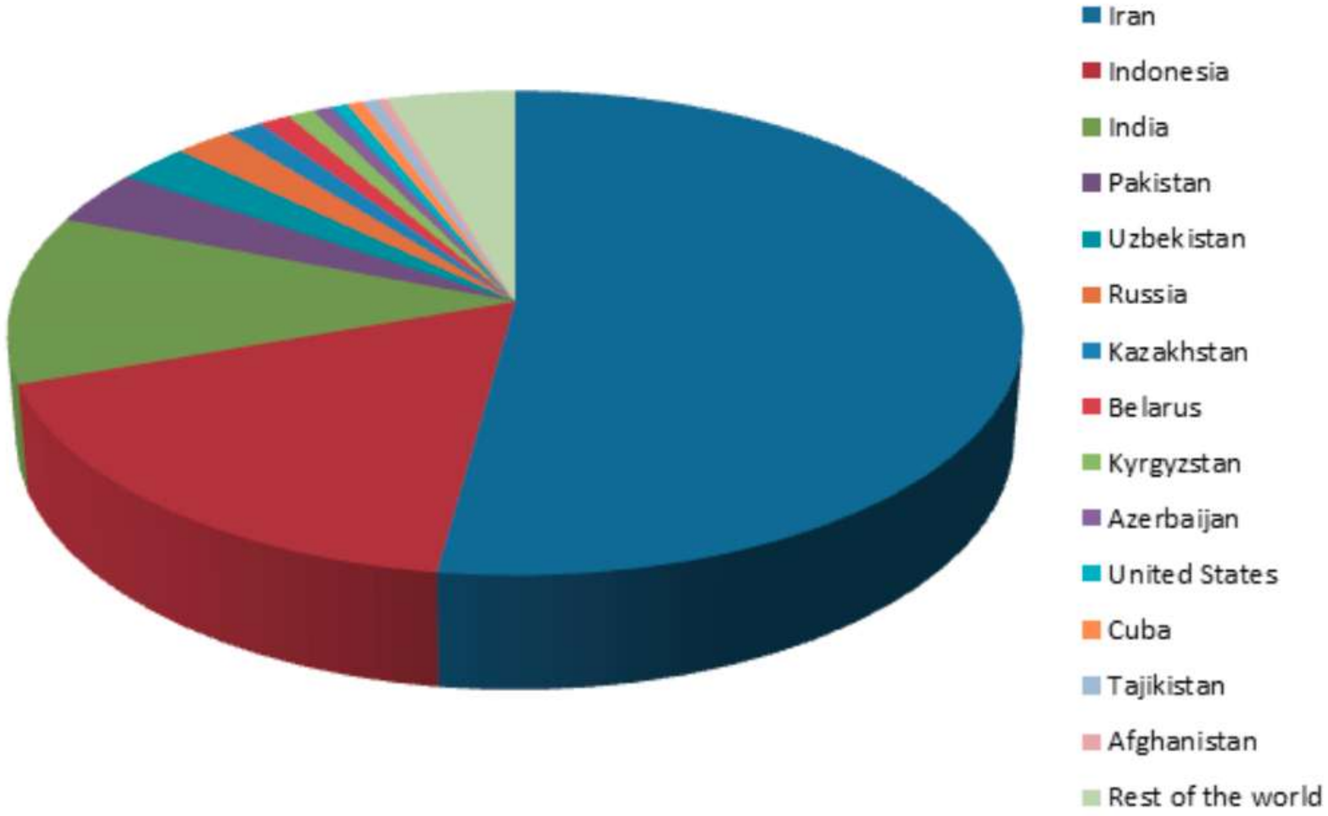
- Let us examine the state of the art in nation-state attacks…

Stuxnet

Why discuss Stuxnet?

- Five zero-day vulnerabilities
- Two stolen certificates
  - Interestingly, a big goal of Aurora
- Almost surgically targeted
- Eight propagation methods
- Partridge in a malware pear tree

Stuxnet



http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

The Real Payload

Zero-Day* Vulnerabilities:

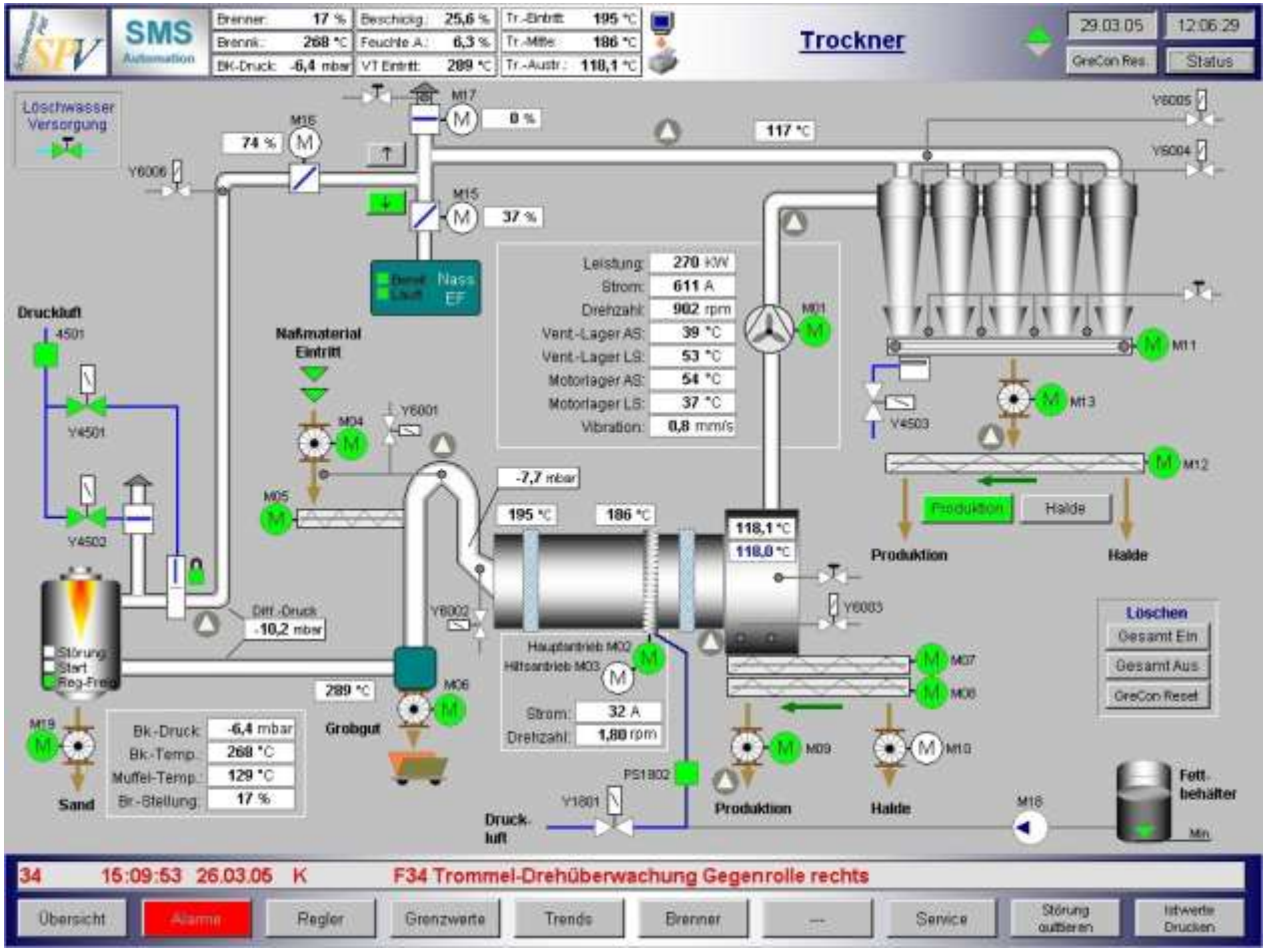
- MS10-046 (Shell LNK / Shortcut)
- MS10-061 (Print Spooler Service)
- MS10-073 (Win32K Keyboard Layout)
- MS08-067 (NetPathCanonicalize())
- MS10-092 (Task Scheduler)
- **CVE-2010-2772 (Siemens SIMATIC Static Password)**

When and Where?

- Stuxnet is targeted for the Natanz Nuclear Facility
  - Targets a configuration with six centrifuge cascades in a very specific configuration
  - Attacks specific controllers/hardware used at Natanz
  - Certainly had a test environment
- How can you get a foot in the door? USB keys

CVE-2010-2772 (Static Password)

- Siemens’ controllers for centrifuges run WinCC
- WinCC SQL database servers
  - Connect using a hardcoded password
  - Loads Stuxnet as binary into a table
  - Executes binary as a stored procedure



Trockner

29.03.05 12:06:29

Brenner:	17 %	Beschickg.:	25,6 %	Tr.-Eintritt:	195 °C
Brennk.:	268 °C	Feuchte A.:	6,3 %	Tr.-Mitte:	186 °C
BK-Druck:	-6,4 mbar	VT Eintritt:	289 °C	Tr.-Austr.:	118,1 °C

Leistung:	270 KW
Strom:	611 A
Drehzahl:	902 rpm
Vent.-Lager AS:	39 °C
Vent.-Lager LS:	53 °C
Motorlager AS:	54 °C
Motorlager LS:	37 °C
Vibration:	0,8 mm/s

Bk-Druck:	-6,4 mbar
Bk-Temp.:	268 °C
Muffel-Temp.:	129 °C
Br.-Stellung:	17 %

Hauptantrieb M02
Hilfsantrieb M03

Strom:	32 A
Drehzahl:	1,80 rpm

Diff.-Druck -10,2 mbar

34 16:09:53 26.03.06 K F34 Trommel-Drehüberwachung Gegenrolle rechts

RSACONFERENCE2013

Presenter Logo

CVE-2010-2772 (Static Password)

- Step7 DLL is renamed and replaced with an attack DLL
- If the PLC matches the desired profile, it's infected
- Breaks centrifuges while reporting everything is fine

Stuxnet: Fun Facts

- Black Market value of these vulns… probably millions
- Probably set back Iran’s nuclear program by years
- Stolen code signing certificates actually signed the virus to make it look legitimate
- Virus phoned command and control centers to gather data, update, and presumably limit the scope of infection
- C&C not core to mission, built to be autonomous
- Learn more:
  - http://www.youtube.com/watch?v=rOwMW6agpTI
  - http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
  - http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/
  - https://www.youtube.com/watch?v=rsXe2Gr2e3Q

Flame

Flame

- Spyware platform
- Does crazy things like:
  - Get all the GPS tags from all your photos
  - Get your contact list from any Bluetooth attached phone
  - Screenshots, keystroke logging, audio recording

Flame (Stuxnet's Cousin)

- Certificate weakness of MD5 demonstrated in 2008
- Microsoft forgot about one Microsoft Terminal Server support service still issuing MD5 certificates
  - Attackers devised a new way to find MD5 collisions
  - Harder challenges, 1 ms time window to get the right timestamp
- Created an arbitrary MS root certificate for signing anything

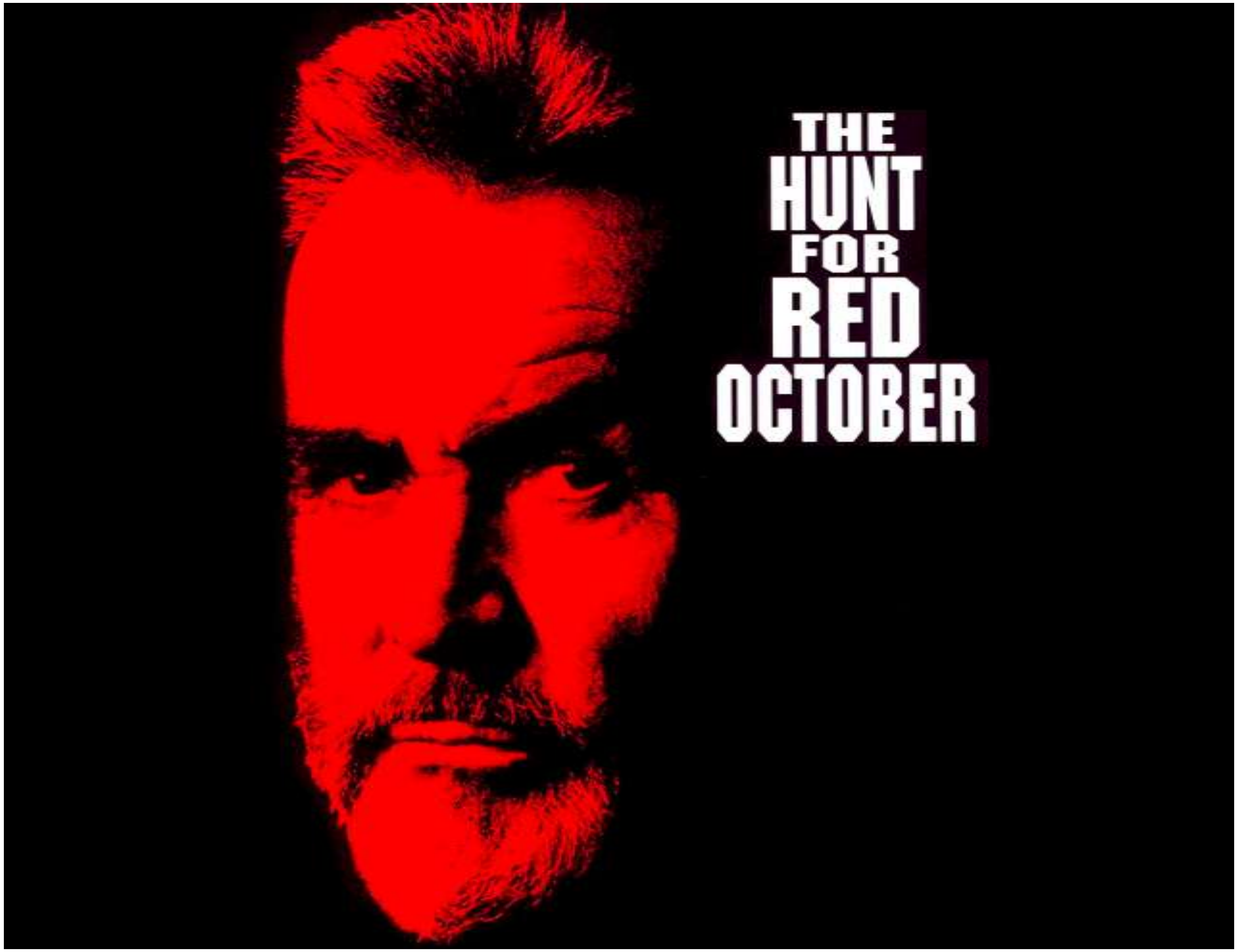
Windows Update

I personally have some responsibility here…

- Windows Update runs in two modes, WSUS and WU
  - WU has two cryptographic checks, WSUS one
  - Sometimes possible to trick old client into accepting one

1. WPAD MITM Attack
2. Unencrypted control channel
3. Supply malicious CAB signed with bad ICA

And that brings us to…

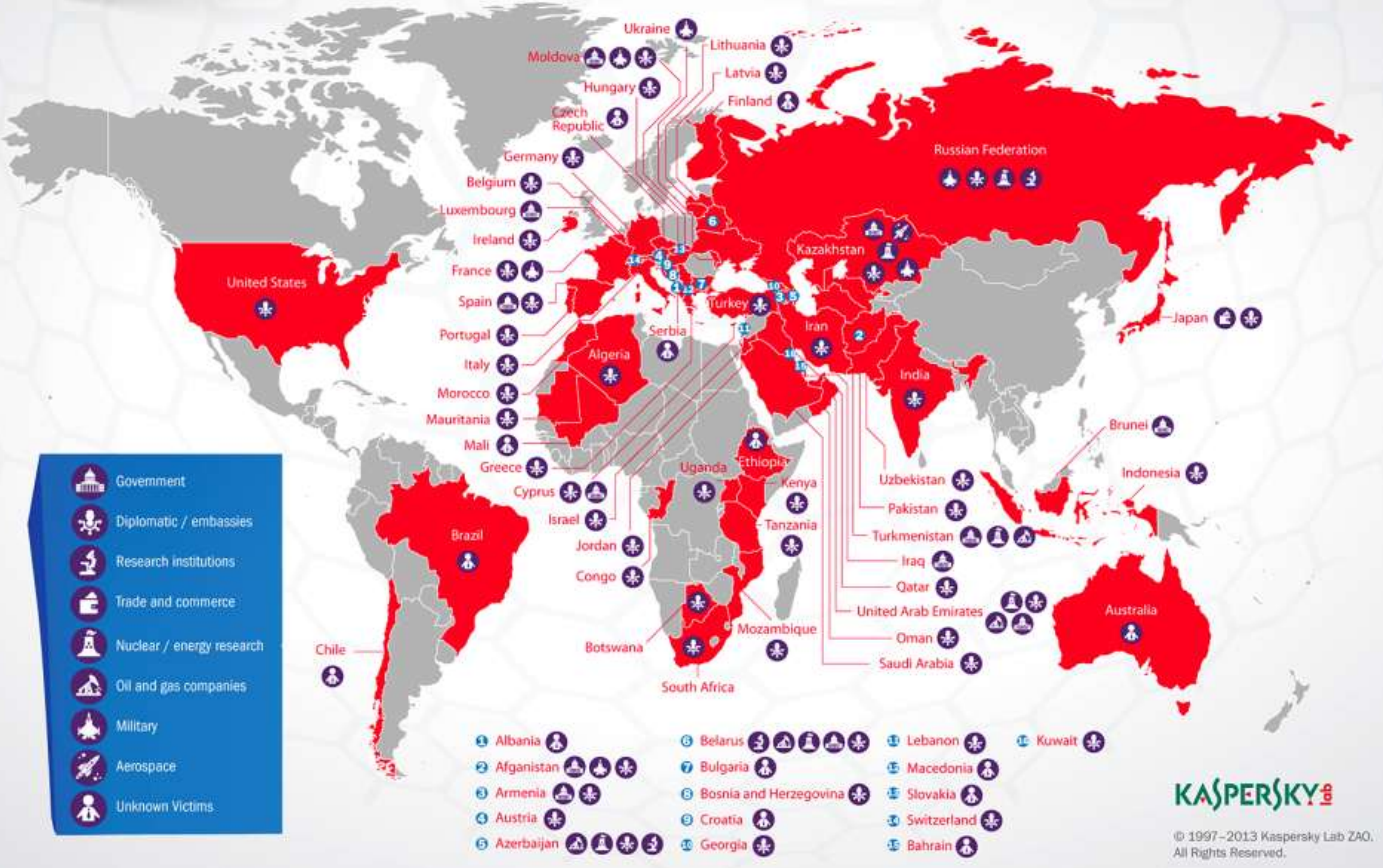


Red October

- Found thanks to fantastic work by Kaspersky
- A true platform, with 1,000 pluggable modules
  - Only a handful have been fully analyzed
  - Recon, automated data gathering, multiple exfiltration mechanisms
  - Mostly ripped-off exploits, however
- Much wider spread than Flame/Stuxnet
  - Some control channel servers date back to May 2007!

Operation "Red October"

Victims of advanced cyber–espionage network



KASPERSKY lab

What have we learned?

Shared Aspects of “Super Malware”

- Autonomous
  - Doesn’t require real-time C&C
  - Complicated C&C routing difficult to trace
- Platform
  - Scripting VMs allow for easy customization
  - Modular structure with self-update
- Advanced/Numerous Exploits
  - Millions of dollars of “cyber munitions” burned for specific goals
  - Notable move away from memory corruption

What have we learned?

- Air gapping is not enough
- Halvar was right about anti-exploit technologies
  - Few memory corruption bugs used
  - But: Lots of logical flaws left
- Logical issues much harder to find and mitigate
  - Can only be caught by humans!
- Hypothetical crypto attacks will eventually be used
  - Nobody’s laughing at Applebaum et al and their PS3s

What have we learned?

- The makers of Flame are willing to attack Microsoft
  - US corporations as collateral damage
- Limited C&C can make detection much harder
  - Too much emphasis on network IOC right now
- Local privilege escalation is no joke
  - Necessary due to priv-sep technologies
- Anti-virus is useless in targeted scenarios
  - Tell you something you don’t know…
- Investment in malware platforms can pay off
  - Five years of service from Red October

Other fun issues…

- Encryption Oracle Issues Everywhere
  - BEAST, CRIME
  - Lesson: Crypto is hard, TLS still has flaws
- TurkTrust et. al.
  - CA compromise is a legitimate threat
  - Lesson: Public PKI useless for high-value transactions
  - Lesson: SSL Pinning, HSTS Pre-Load are critical

Other fun issues…

- IPv6 Fraud is heating up
  - Gmail reporting huge spam issues
  - Lesson: IP reputation is dead, long-live network reputation

- New TLDs are going to be fun fun fun
  - Starting in late summer 2013, get ready for 20/week
  - Lesson: Brand Management is Risk Management

The New Threat Landscape

- Fully automated APT
- Semi-autonomous hacking groups competing with nation state teams
- APT exploits very quickly re-deployed
- C&C detection will not save you
- “Good Guys” and “Bad Guys” is becoming an outmoded idea
- End of Scarcity means End of Easy Trust

Thank you!

Ask me about lunch on Thursday!

alex@artemis.net