LINKÖPINGS UNIVERSITET

June 10th, 2016 by Ivan Bütler

Is there an arms race in cyber space?

About Me – Ivan Bütler

http://e1.compass-security.com/
ivan.buetler@compass-security.com

… from Switzerland

… like hacking, cracking, securing, security

… Lecturing at the University of Applied Science in Rapperswil, Lucerne and Zurich

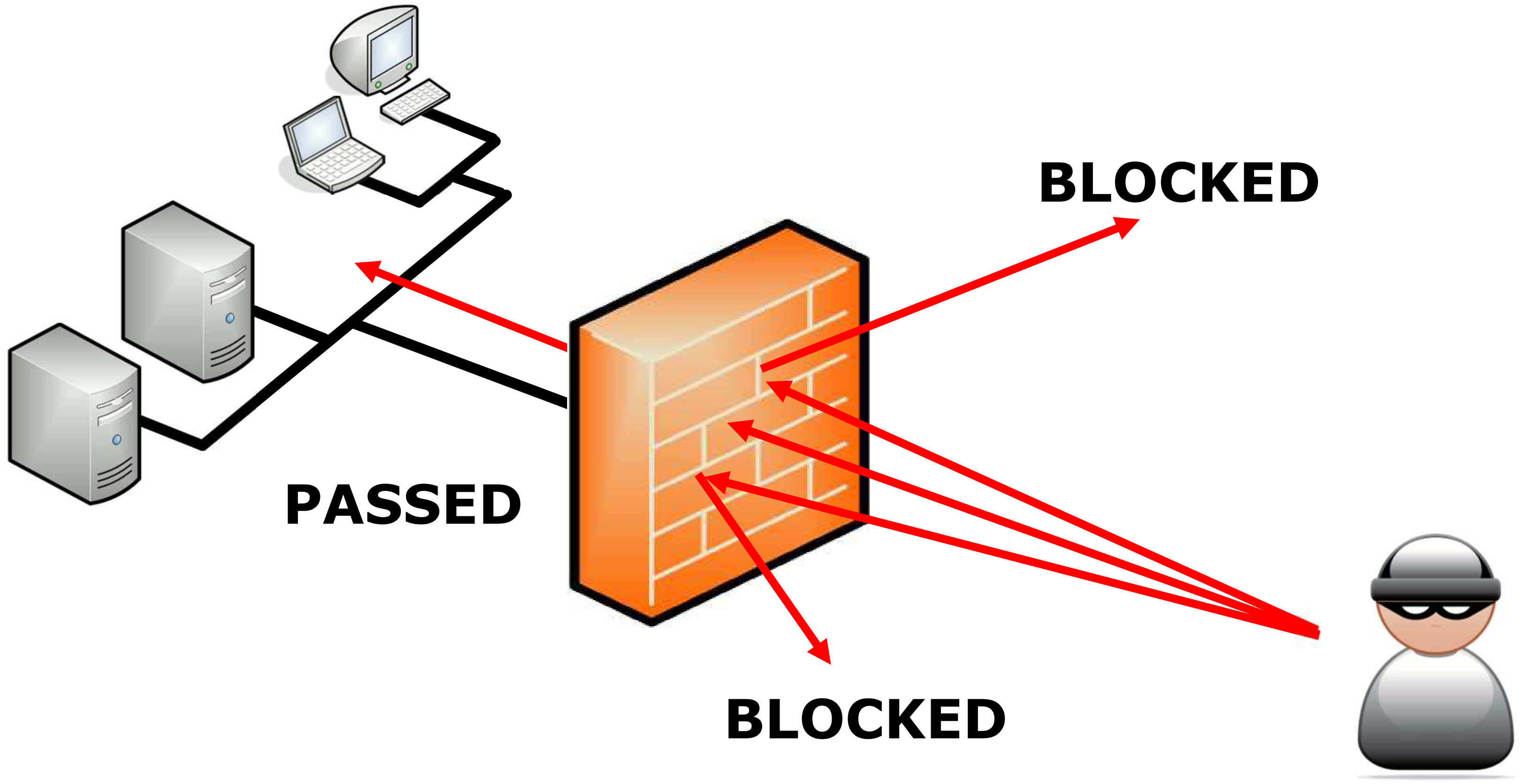
… like building CTF games and infrastructures

… speaker @ Blackhat US, AppSec US, EU, CN

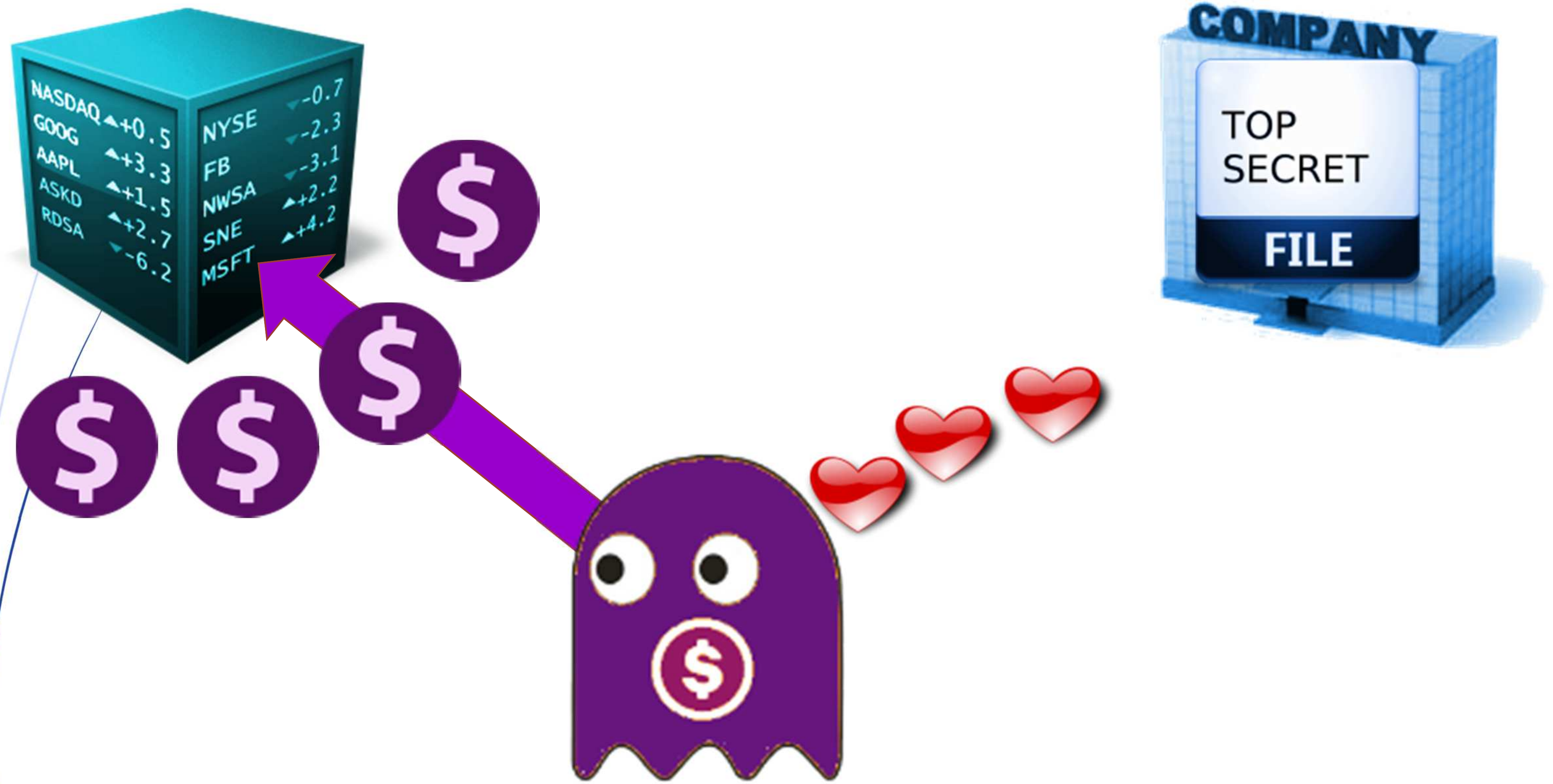
Who are you going to ask **if she is rich**?

What I have learned from being a Pentester

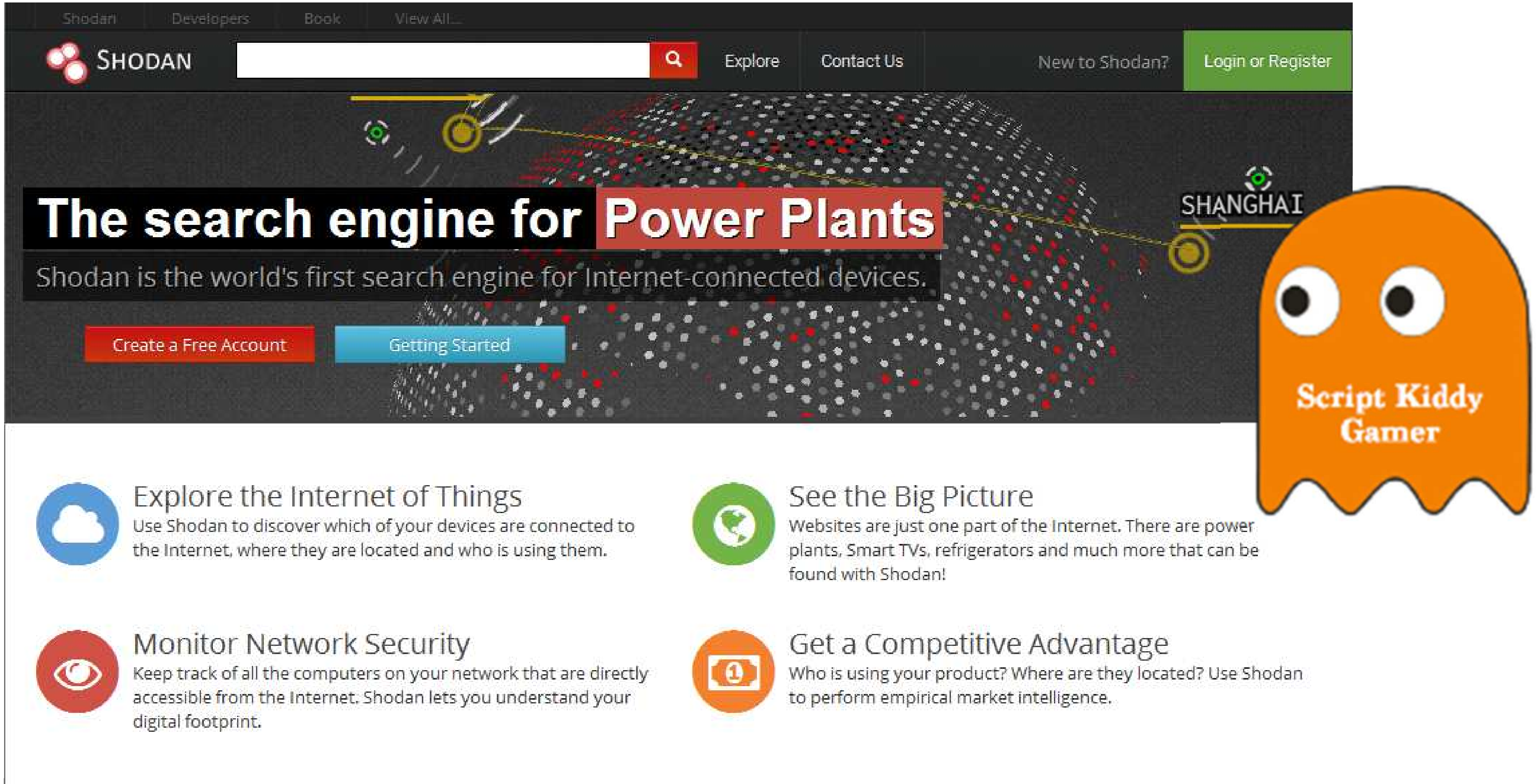
Direct Attacks



Business Case for Cyber Criminals



Search & Hack // Shodan Internet of Things



The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

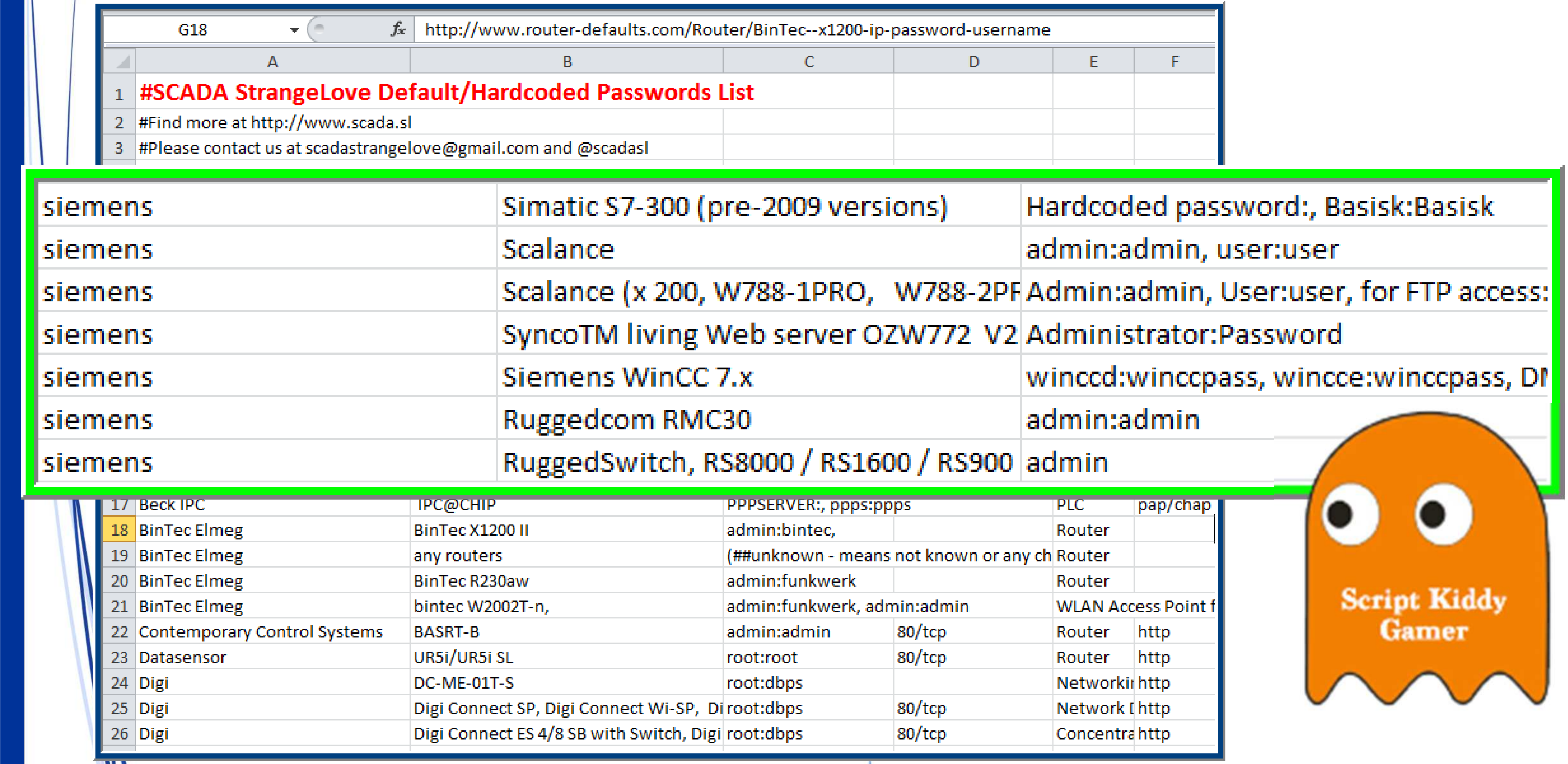
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

#### Default Passwords

- https://github.com/scadastrangelove/SCADAPASS



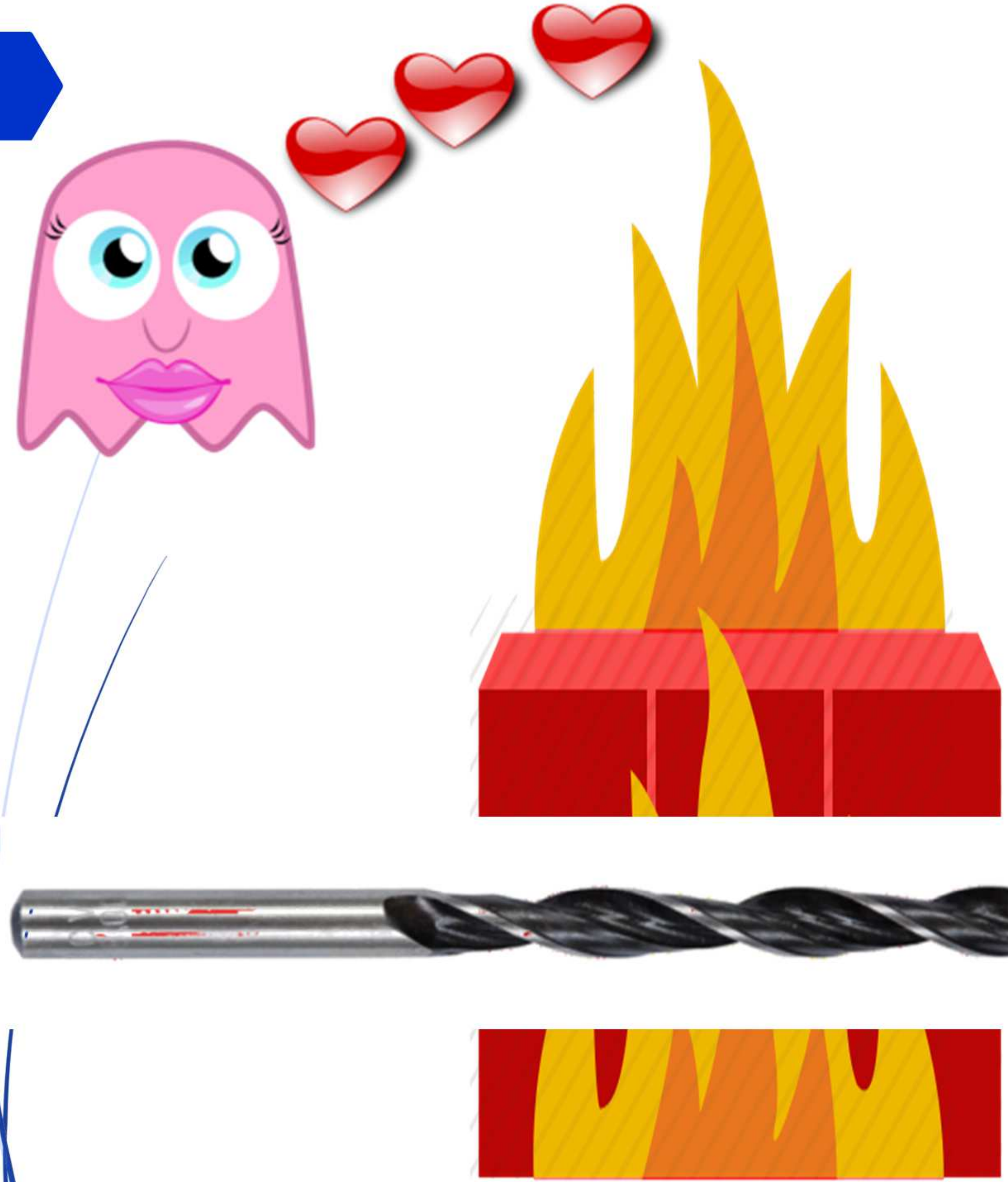
G18 http://www.router-defaults.com/Router/BinTec--x1200-ip-password-username

	A	B	C	D	E	F
1	#SCADA StrangeLove Default/Hardcoded Passwords List					
2	#Find more at http://www.scada.sl					
3	#Please contact us at scadastrangelove@gmail.com and @scadasl					

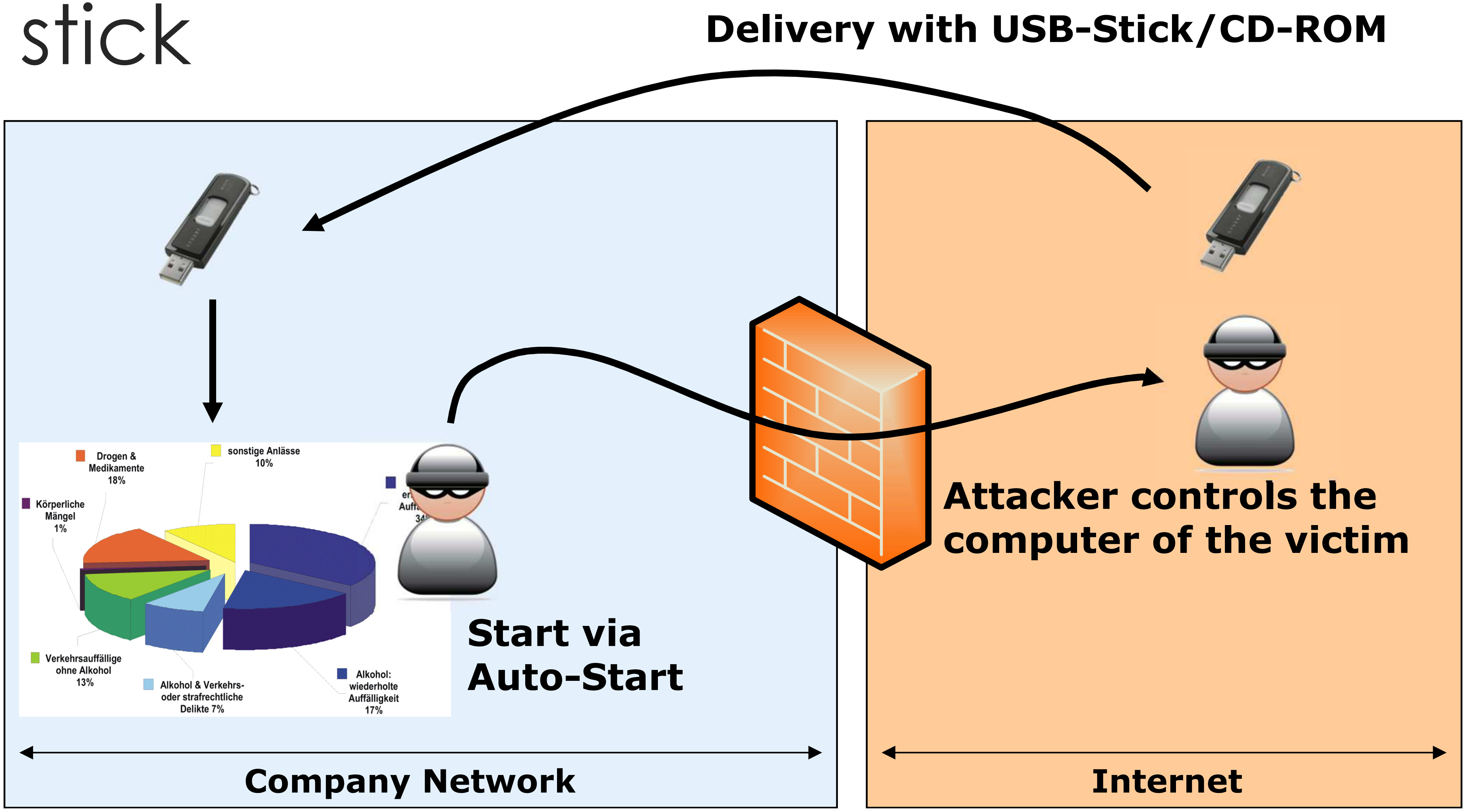
siemens	Simatic S7-300 (pre-2009 versions)	Hardcoded password:, Basisk:Basisk
siemens	Scalance	admin:admin, user:user
siemens	Scalance (x 200, W788-1PRO, W788-2PF	Admin:admin, User:user, for FTP access:
siemens	SyncoTM living Web server OZW772 V2	Administrator:Password
siemens	Siemens WinCC 7.x	winccd:winccpass, wincce:winccpass, DI
siemens	Ruggedcom RMC30	admin:admin
siemens	RuggedSwitch, RS8000 / RS1600 / RS900	admin

	A	B	C	D	E	F
17	Beck IPC	IPC@CHIP	PPPSERVER:, ppps:ppps		PLC	pap/chap
18	BinTec Elmeg	BinTec X1200 II	admin:bintec,		Router	
19	BinTec Elmeg	any routers	(##unknown - means not known or any ch		Router	
20	BinTec Elmeg	BinTec R230aw	admin:funkwerk		Router	
21	BinTec Elmeg	bintec W2002T-n,	admin:funkwerk, admin:admin		WLAN Access Point f	
22	Contemporary Control Systems	BASRT-B	admin:admin	80/tcp	Router	http
23	Datasensor	UR5i/UR5i SL	root:root	80/tcp	Router	http
24	Digi	DC-ME-01T-S	root:dbps		Networki	http
25	Digi	Digi Connect SP, Digi Connect Wi-SP, Di	root:dbps	80/tcp	Network [	http
26	Digi	Digi Connect ES 4/8 SB with Switch, Digi	root:dbps	80/tcp	Concentra	http

Indirect Attack



Fake Job Application using an USB stick



Delivery with USB-Stick/CD-ROM

Start via Auto-Start

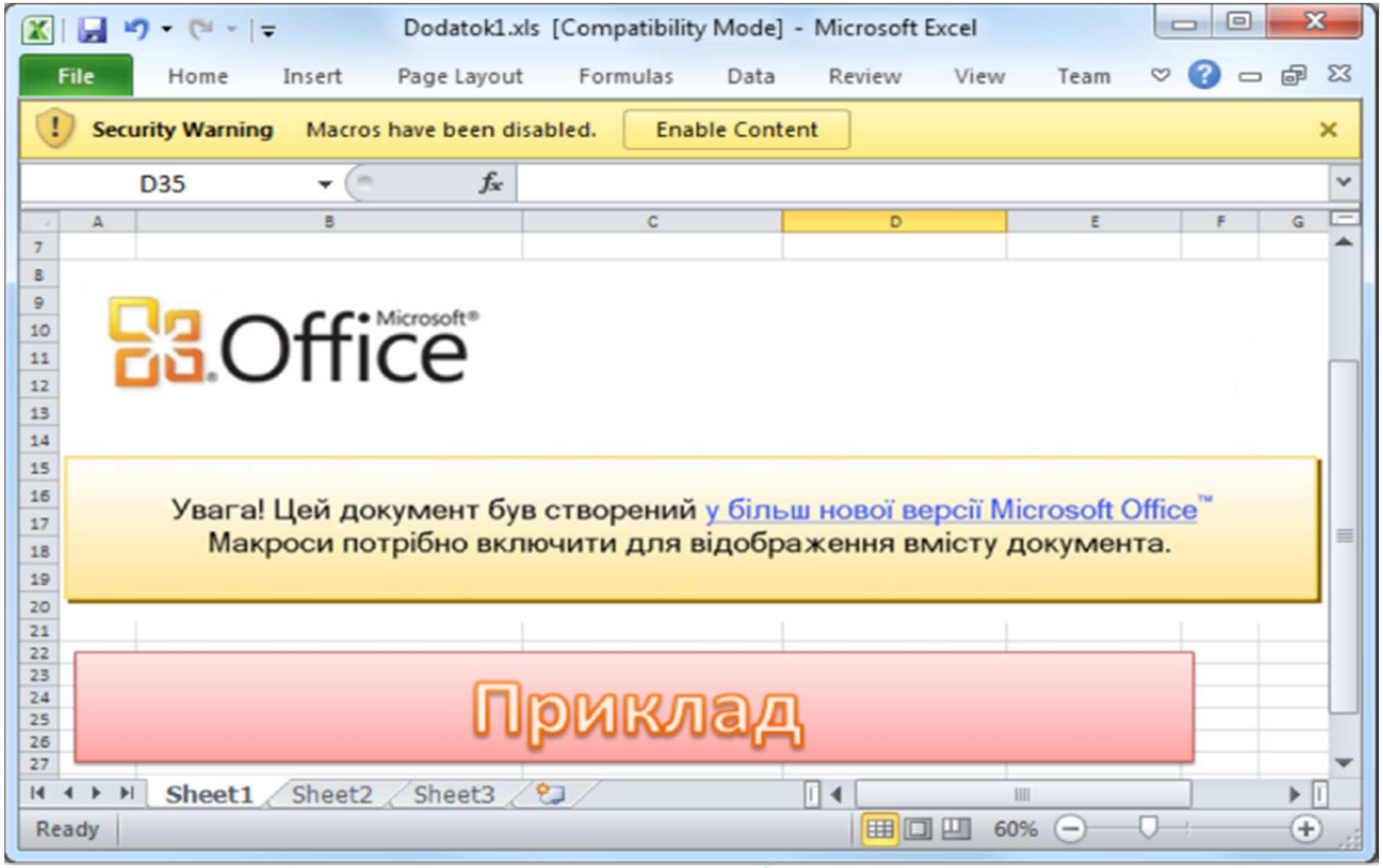
Attacker controls the computer of the victim

Company Network

Internet

Drogen & Medikamente 18%
sonstige Anlässe 10%
Körperliche Mängel 1%
er
Auff
34
Verkehrsauffällige ohne Alkohol 13%
Alkohol & Verkehrs- oder strafrechtliche Delikte 7%
Alkohol: wiederholte Auffälligkeit 17%

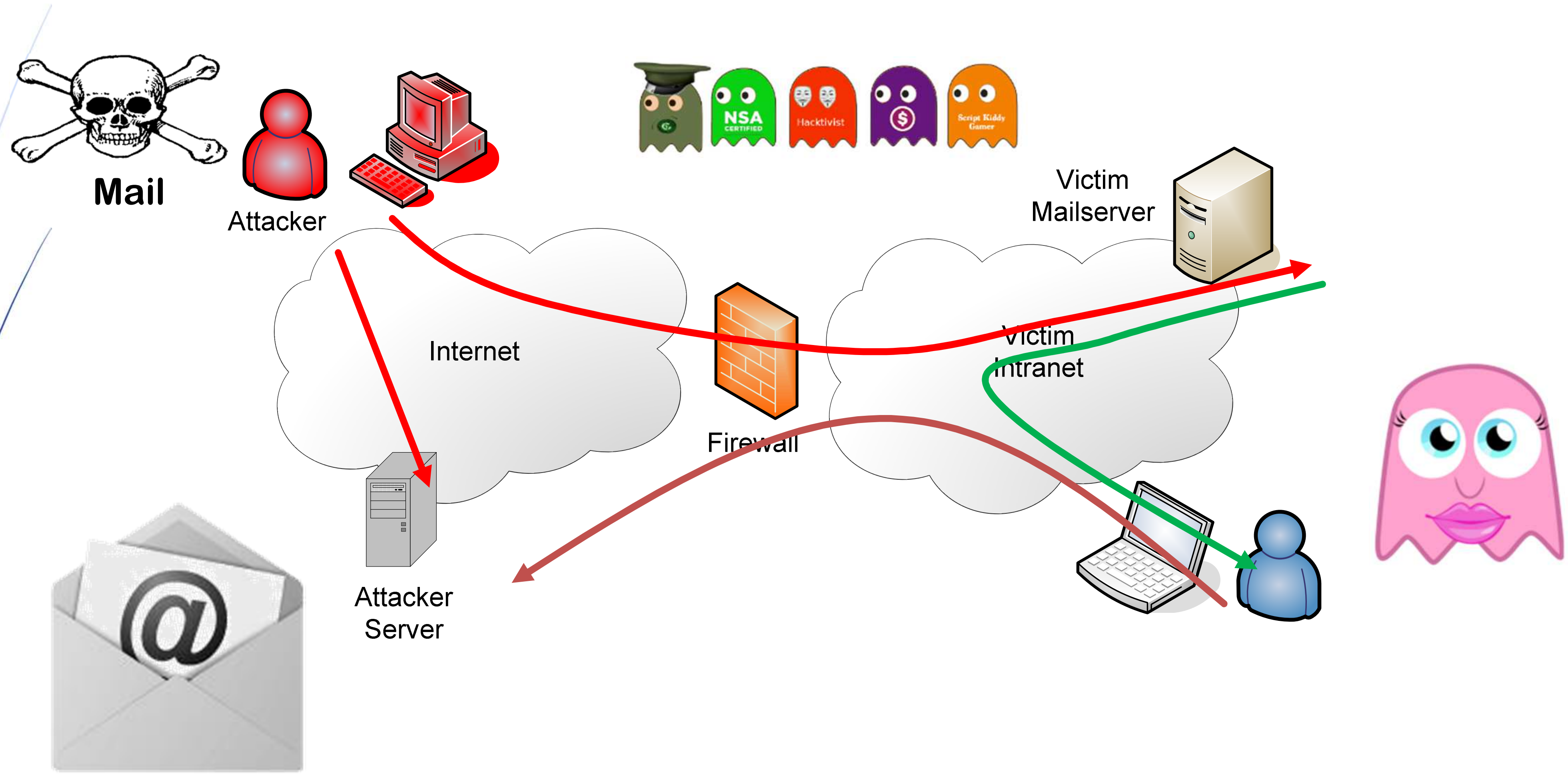
Ukraine 6 hour Blackout // Dec 23th, 2015



Увага! Цей документ був створений у більш нової версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документа.

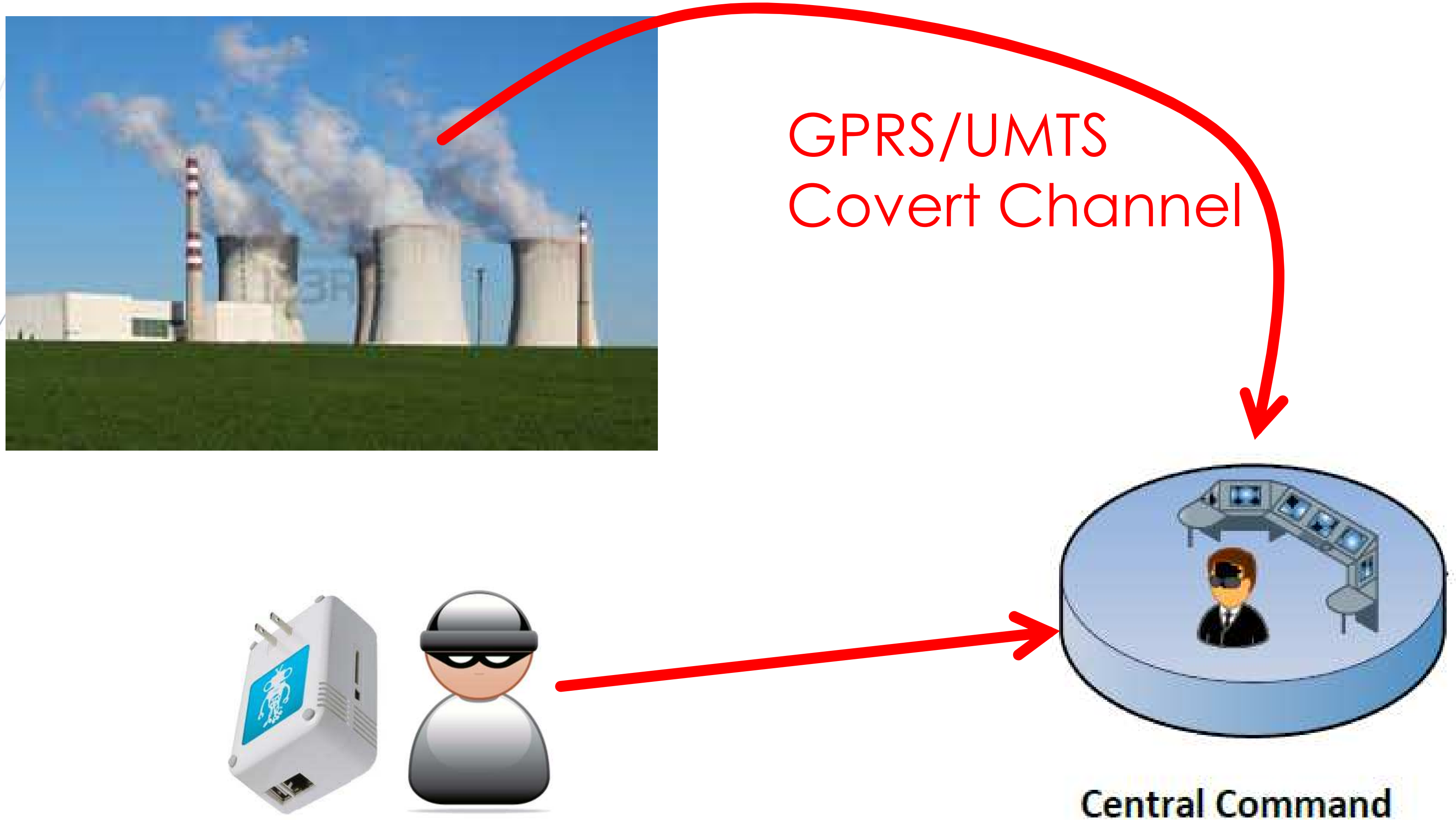
Приклад

MS Word Virus Example



Attacking Offline Networks

PlugBot Concept (Inside-Out)

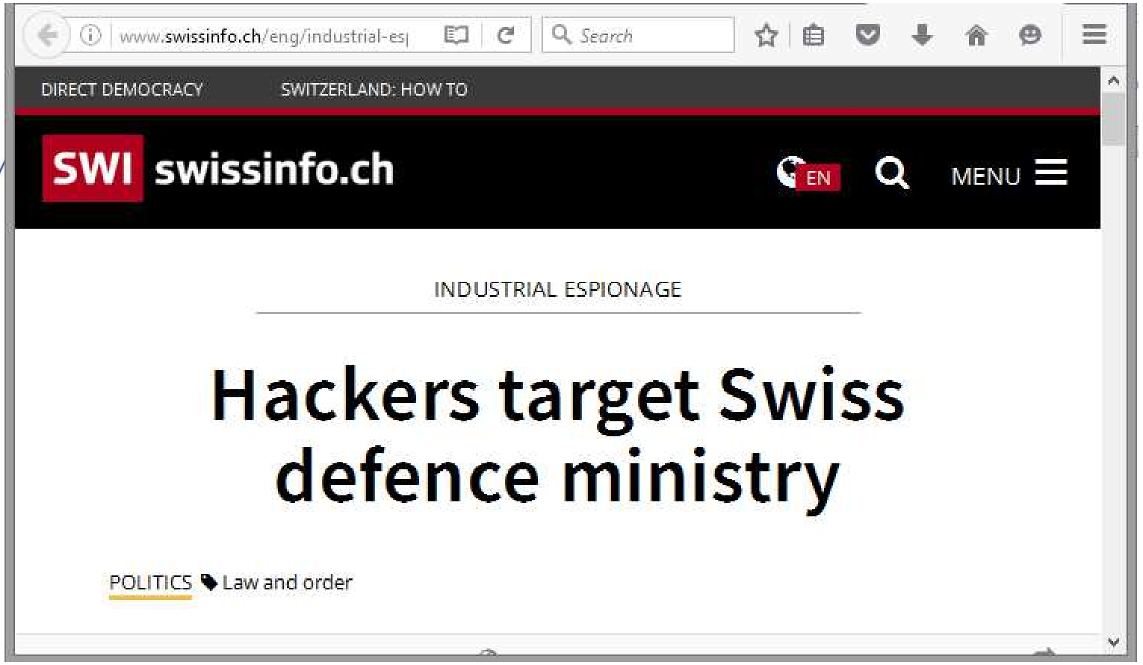


GPRS/UMTS
Covert Channel

Central Command

May you ask yourself, is this an ‘arms race in cyber space’ ?

Swiss Government and Military Department became victim of a cyber espionage attack



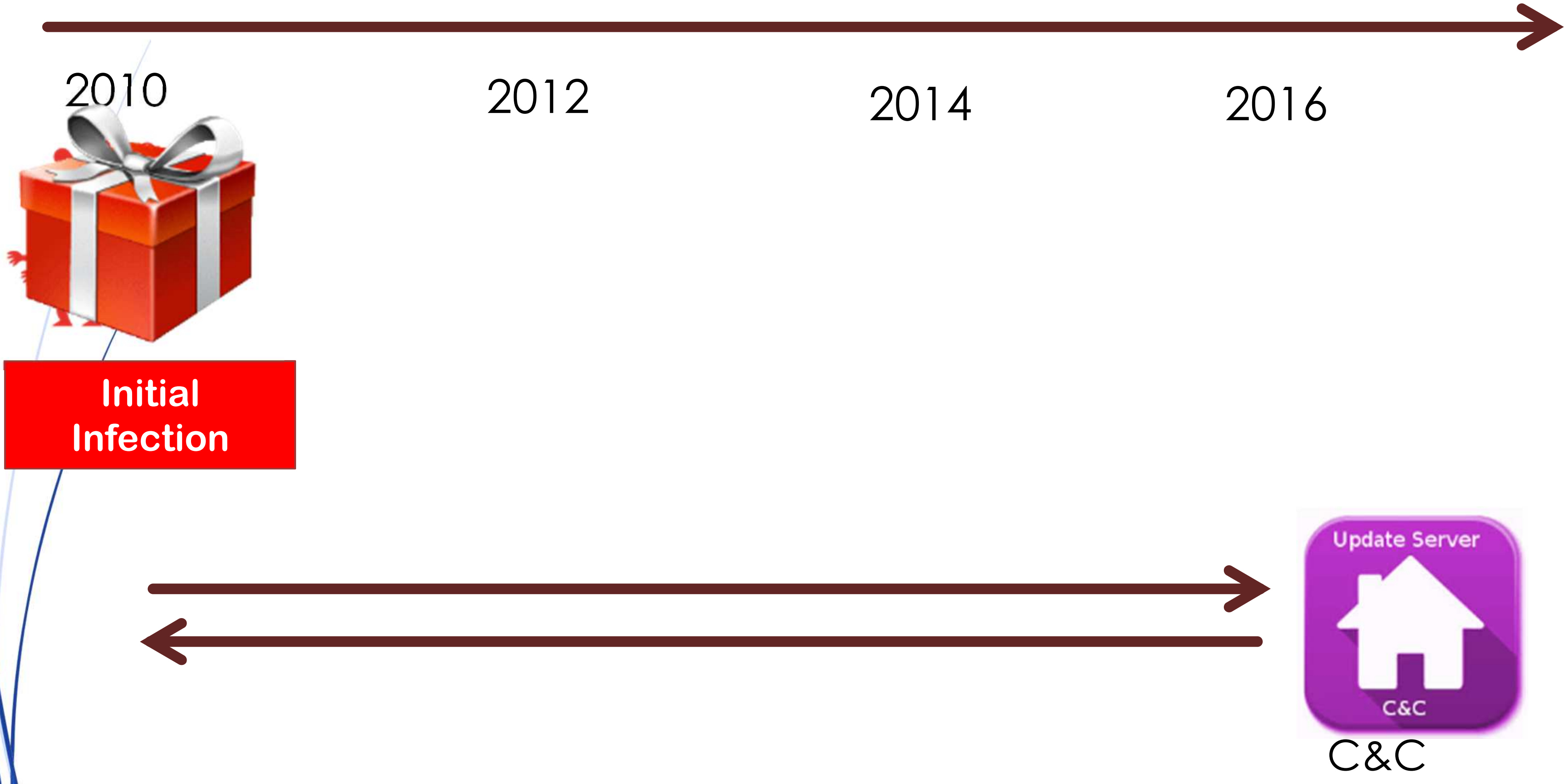
INDUSTRIAL ESPIONAGE

Hackers target Swiss defence ministry

POLITICS Law and order

- https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html
  http://www.swissinfo.ch/eng/industrial-espionage_hackers-target-swiss-defence-ministry/42131890

Initial Infection – harmless ‚game‘



2010

2012

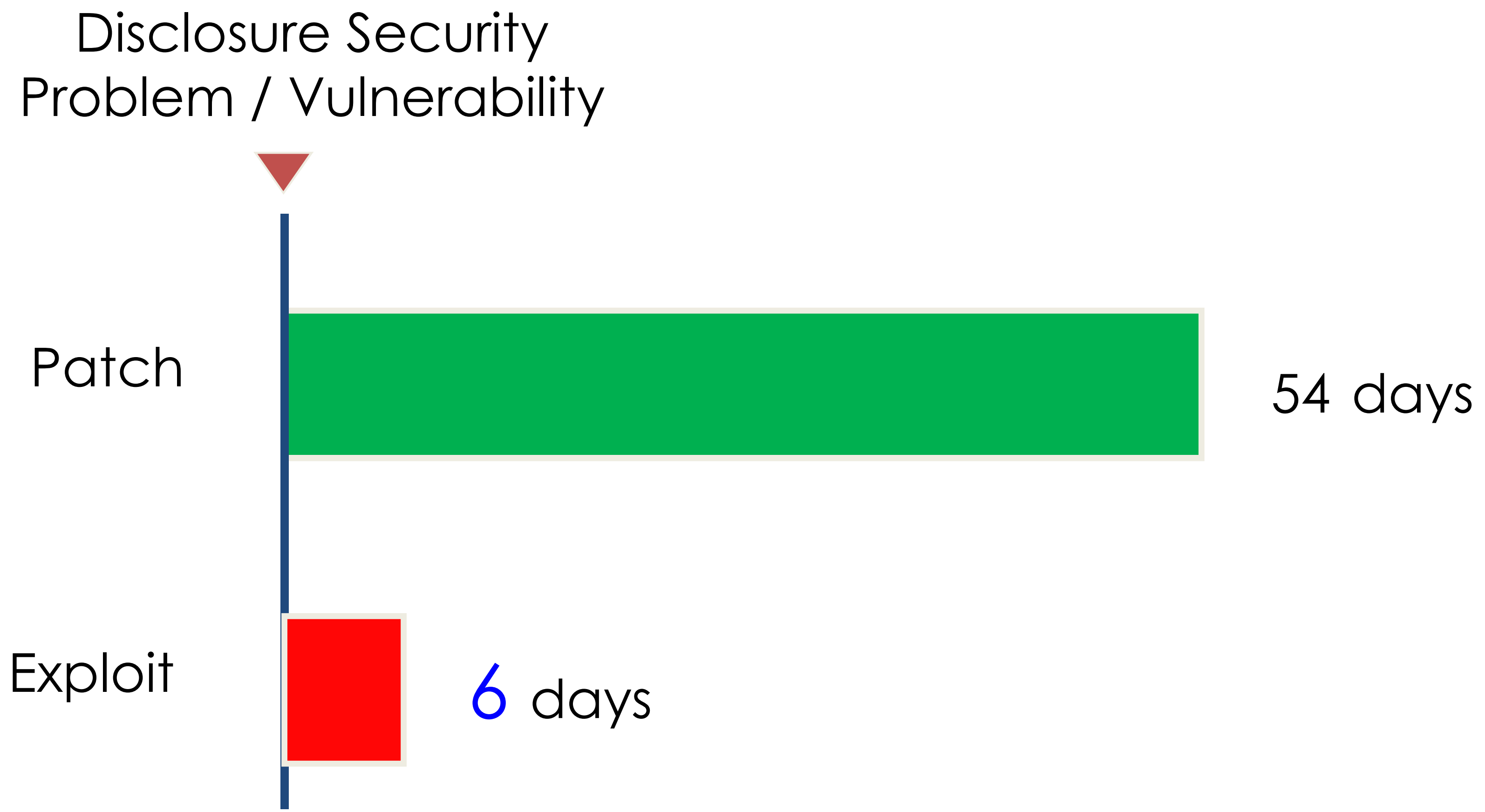
2014

2016

Initial Infection

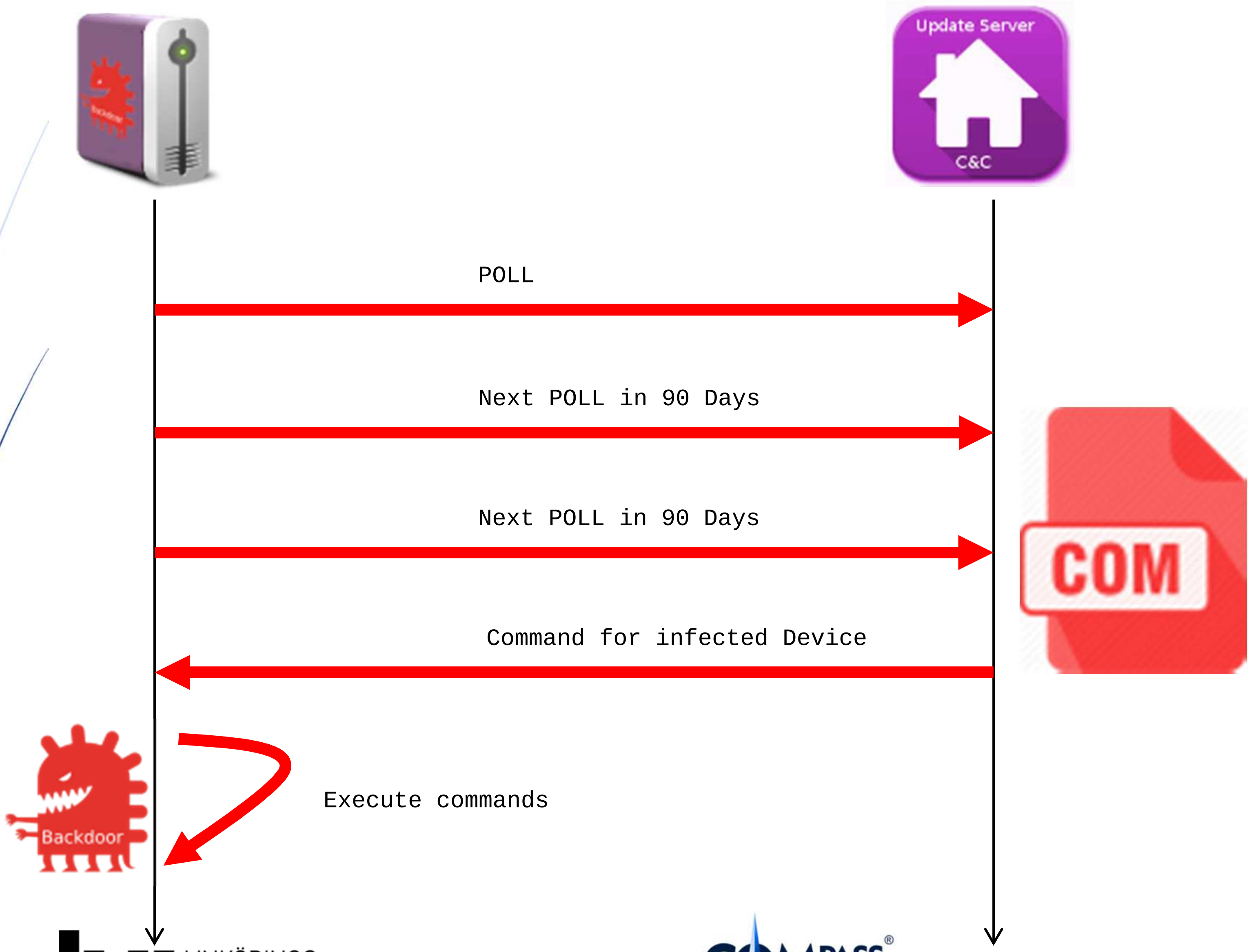
C&C

The Power of the Statistics



- [3] ETHZ Stefan Frei 2009 (Dissertation): We found that exploit availability consistently exceeds patch availability since 2000

Very very slow polling of C&C



POLL

Next POLL in 90 Days

Next POLL in 90 Days

Command for infected Device

Execute commands

Elevate Privileges to Local Admin and gaining AD Domain Admin Privileges

2010

2012

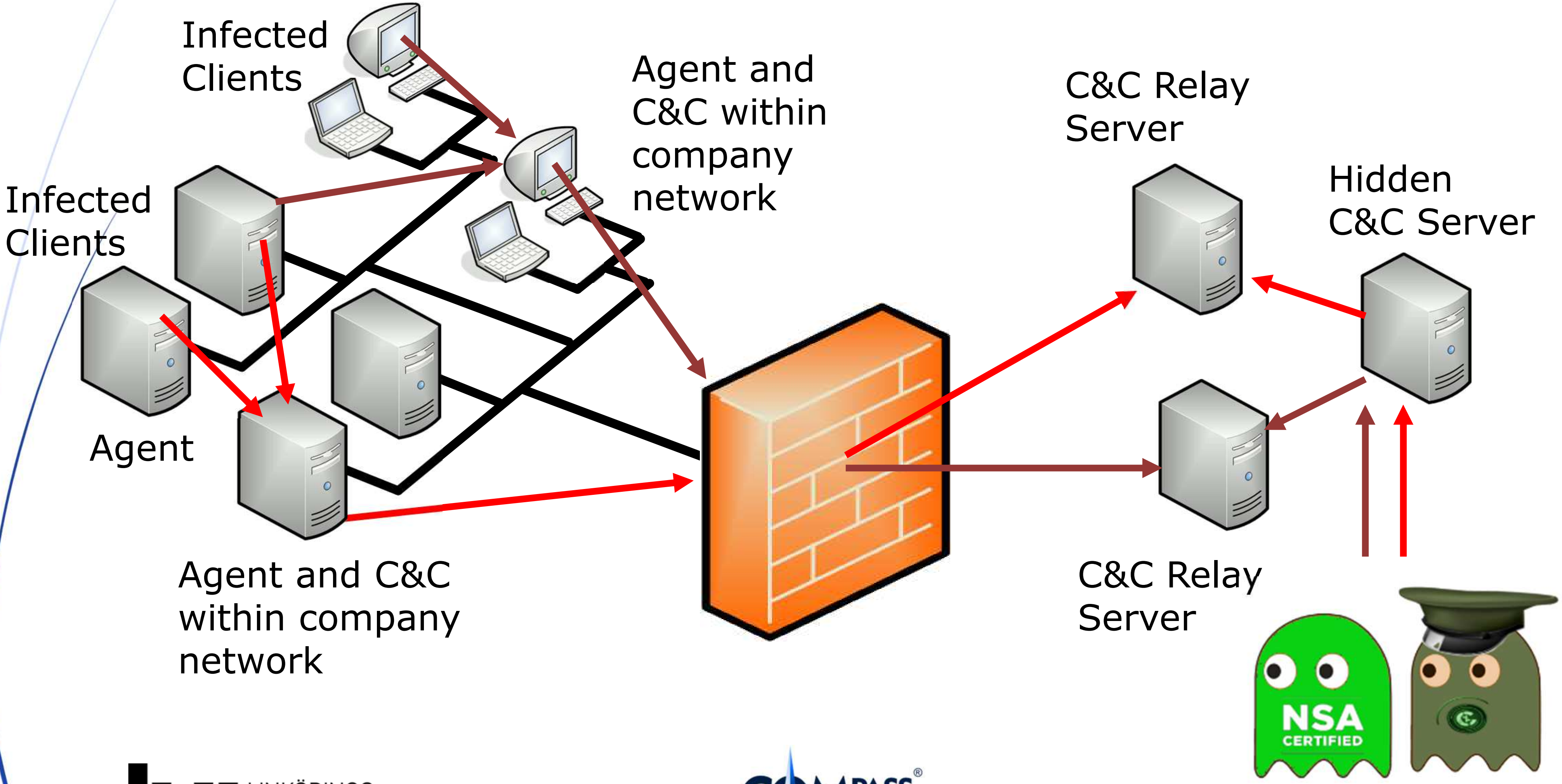
2014

2016

Initial Infection

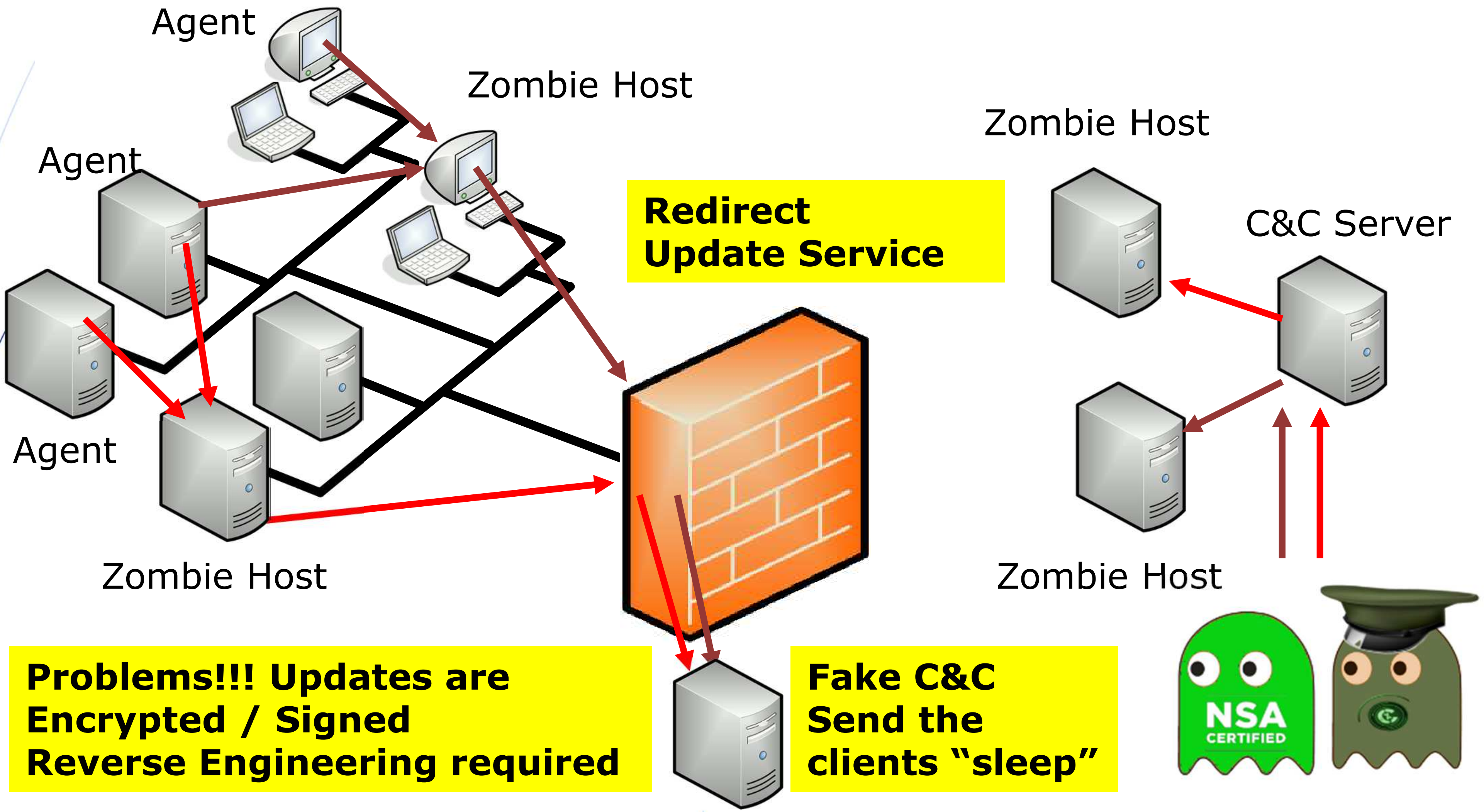
C&C

Multi-stage polymorphic cyber warfare framework



Crucial decision; how to respond? What immediate actions?

Defense Strategy using Fake C&C

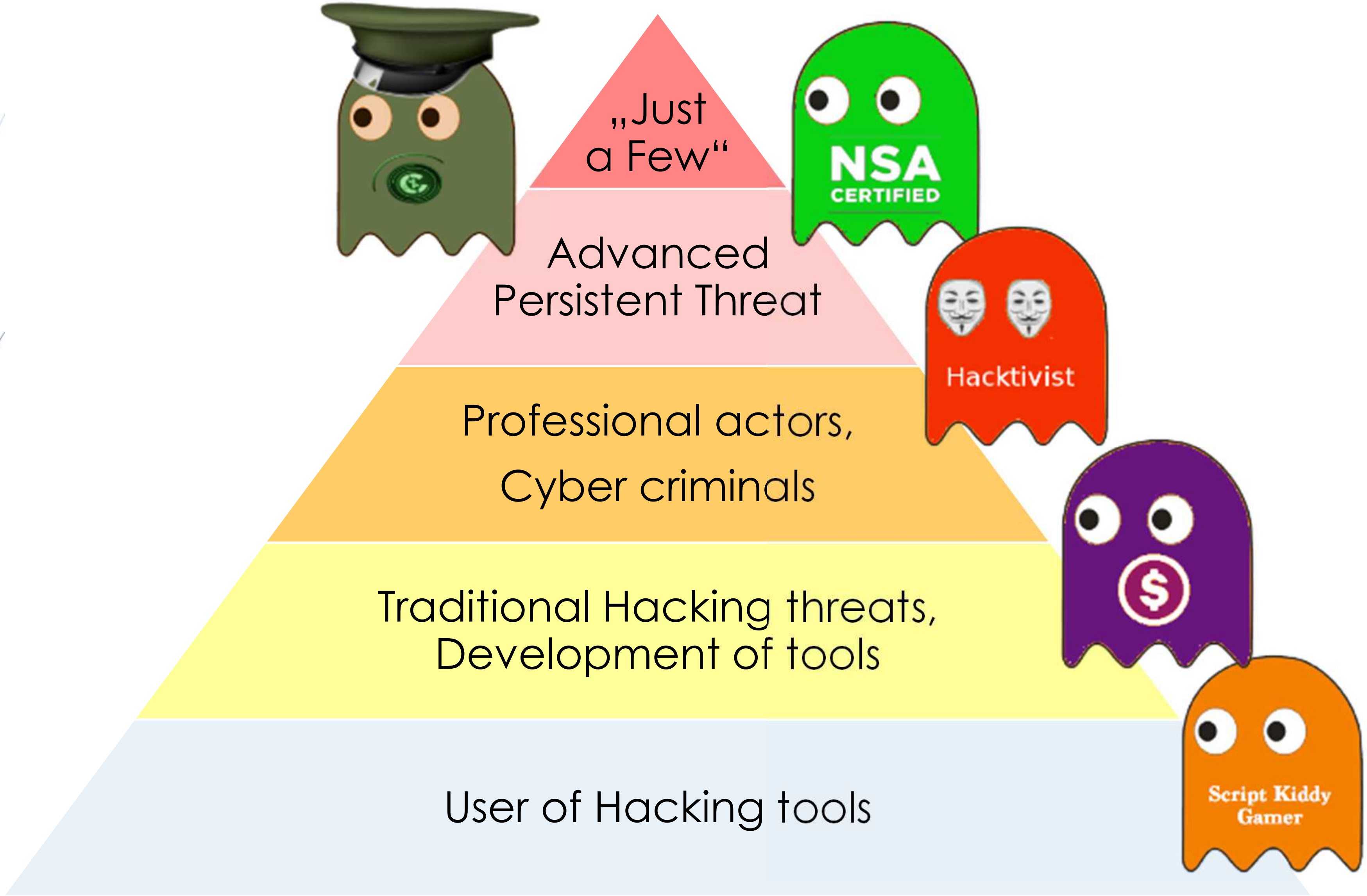


Redirect Update Service

Problems!!! Updates are Encrypted / Signed Reverse Engineering required

Fake C&C Send the clients "sleep"

Threat Pyramid



„Just a Few“

Advanced Persistent Threat

Professional actors, Cyber criminals

Traditional Hacking threats, Development of tools

User of Hacking tools

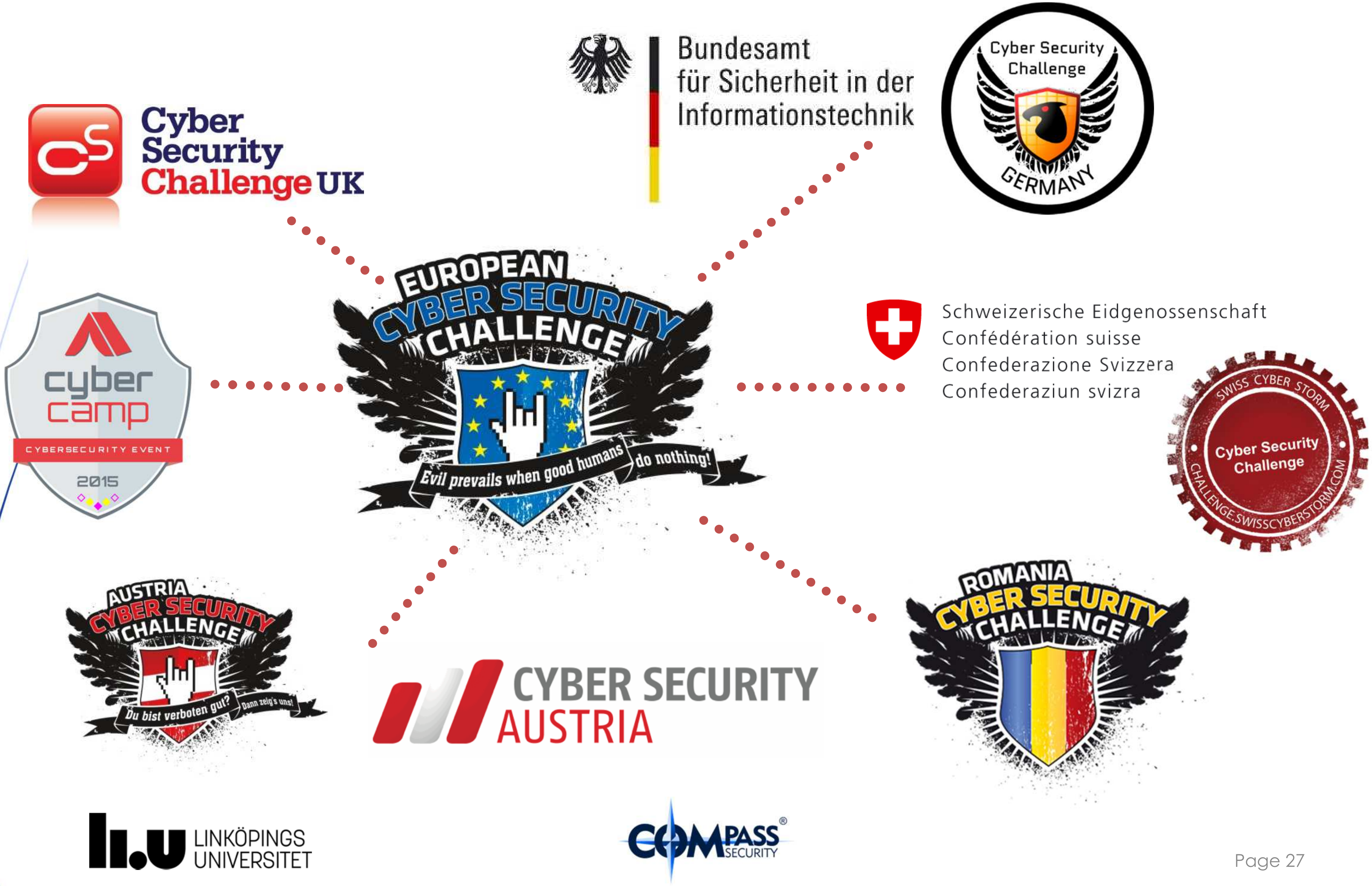
What does it mean from a management perspective?

Having the right people, having trust and confidence; this is a key factor!

- Reverse engineering -> malware
- Reverse engineering -> C&C protocol
- Creation of a fake C&C service
- Interception and pattern based redirections
- Really, really, really good people

European Cyber Security Challenge 2015

http://www.europeancybersecuritychallenge.eu


Cyber Security Challenge UK
Bundesamt für Sicherheit in der Informationstechnik
Cyber Security Challenge GERMANY
cyber camp CYBERSECURITY EVENT 2015
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
SWISS CYBER STORM
Cyber Security Challenge
CHALLENGE.SWISSCYBERSTORM.COM
AUSTRIA CYBER SECURITY CHALLENGE
Du bist verboten gut? Dann zeig's uns!
CYBER SECURITY AUSTRIA
ROMANIA CYBER SECURITY CHALLENGE
LINKÖPINGS UNIVERSITET
COMPASS SECURITY

One last question;
Do we need offensive capabilities?

Thank You! – Questions?

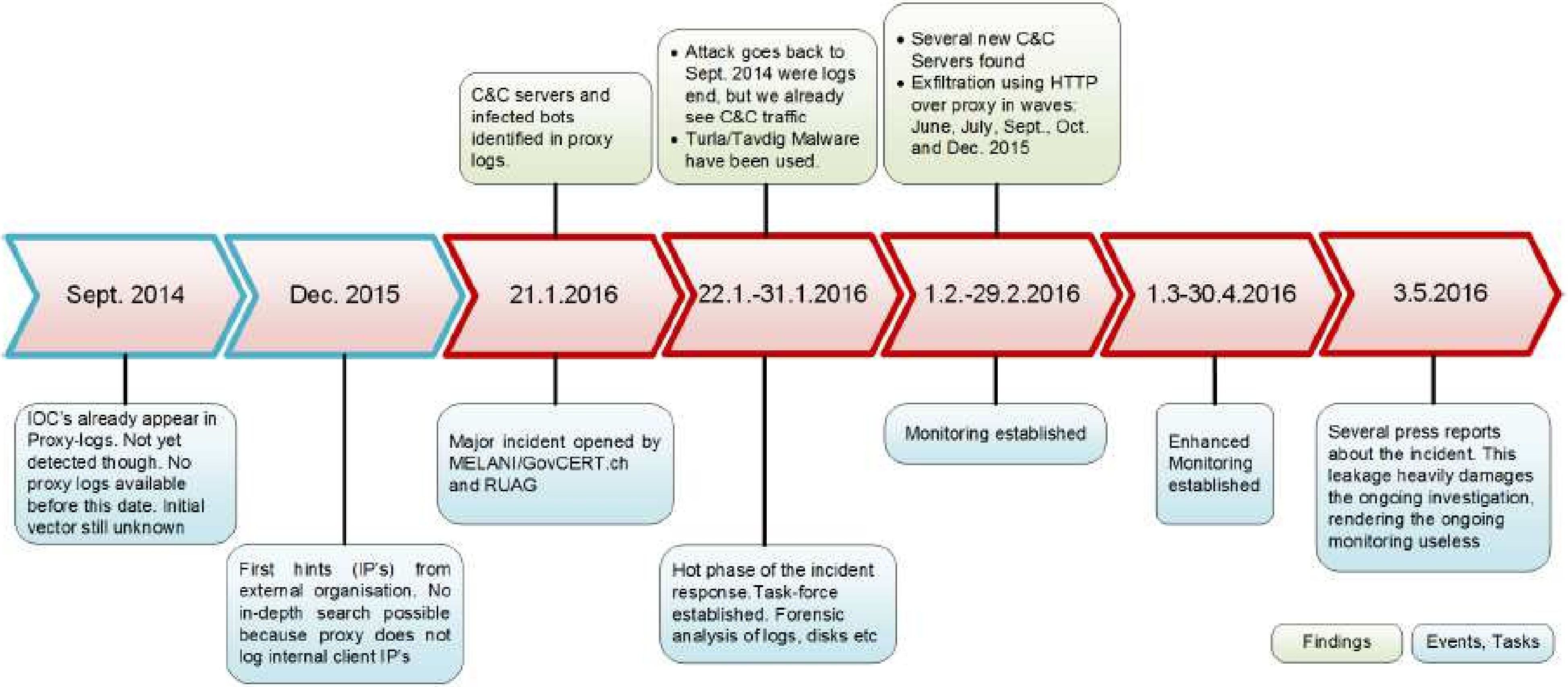
Ivan Bütler

http://e1.compass-security.com/

References

- National Cyber Defense Strategy in Switzerland https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf
- GovCert Report about this cyber espionage https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html
- http://www.swissinfo.ch/eng/industrial-espionage_hackers-target-swiss-defence-ministry/42131890

Swiss GovCert report



C&C servers and infected bots identified in proxy logs.

- Attack goes back to Sept. 2014 were logs end, but we already see C&C traffic
- Turla/Tavdig Malware have been used.

- Several new C&C Servers found
- Exfiltration using HTTP over proxy in waves. June, July, Sept., Oct. and Dec. 2015

IOC's already appear in Proxy-logs. Not yet detected though. No proxy logs available before this date. Initial vector still unknown

First hints (IP's) from external organisation. No in-depth search possible because proxy does not log internal client IP's

Major incident opened by MELANI/GovCERT.ch and RUAG

Hot phase of the incident response. Task-force established. Forensic analysis of logs, disks etc

Monitoring established

Enhanced Monitoring established

Several press reports about the incident. This leakage heavily damages the ongoing investigation, rendering the ongoing monitoring useless

Figure 1: Timeline of Attack

- https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html
http://www.swissinfo.ch/eng/industrial-espionage_hackers-target-swiss-defence-ministry/42131890