Recent Cyber Attacks:
Inherent Risks, Countermeasures, Perspectives

Prof. em. Dr. Klaus Brunnstein
Universität Hamburg

IMF 2013
7th International Conference on IT Security Incident Management & IT Forensics

March 12th - 14th, 2013
Nuremberg (Nürnberg), Germany

Content:

1) Changing World – Changing Crime:

1.1) Information Economy: Towards Enterprise 3.0

1.1A) ICT in Enterpises: From Mainframes towards Web 2.0

Phase 1 (1960+): Centralised IT-Systems:

- **1a: Mainframes/Terminals, dedicated Software**
- **1b: Databanks, Accounting and Office Applications**

Phase 2 (1985+): Decentralised IT-Systems with Dedicated Networks:

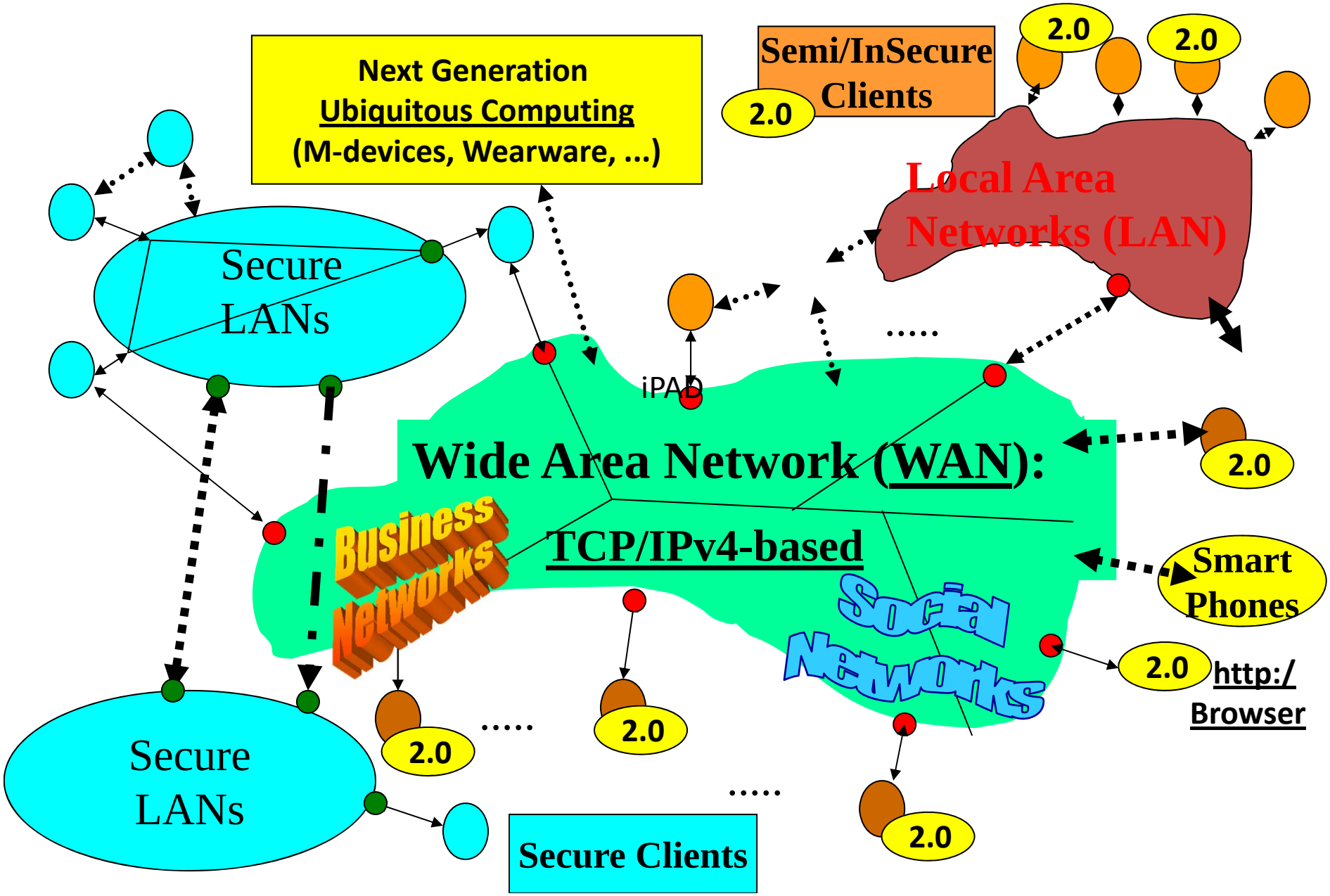
- **2a: Personal Computers, Mainframes, Connection via LANs**
- **2b: Client-Server Architectures, Enterprise Applications**

Phase 3 (2000+): Globalisation using Internet & Web 2.0:

- **3a: Local & Global Communication using IP-Protocol**
- **3b: Enterprises use World Wide Web (html, htt-Protocol)**
- **3c: Business Intelligence, Communication/Interaction, Social Media**

1.1B): „Information Economy“ and Web 2.0: High Complexity!

2013: ~1M Server, >1.5 G Klienten



1) Changing World – Changing Crime:

1.1) Information Economy: Towards Enterprise 3.0

1.1C) ICT in Enterpises: From Mainframes towards Web 3.0

Phase 1 (1960+): Centralised IT-Systems:

1a: Mainframes/Terminals, Dedicated Software

1b: Databanks, Accounting and Office Applications

Phase 2 (1985+): Decentralised IT-Systems with Dedicated Networks:

2a: Personal Computers, Mainframes, Connection via LANs

2b: Client-Server Architectures, Enterprise Applications

Phase 3 (2000+): Globalisation using Internet & Web 2.0:

3a: Local & Global Communication using IP-Protocol

3b: Enterprises use World Wide Web (html, htt-Protocol)

3c: Business Intelligence, Communication, Social Media

Phase 4 (2010+): RealTime-Processing: Enterprise 3.0

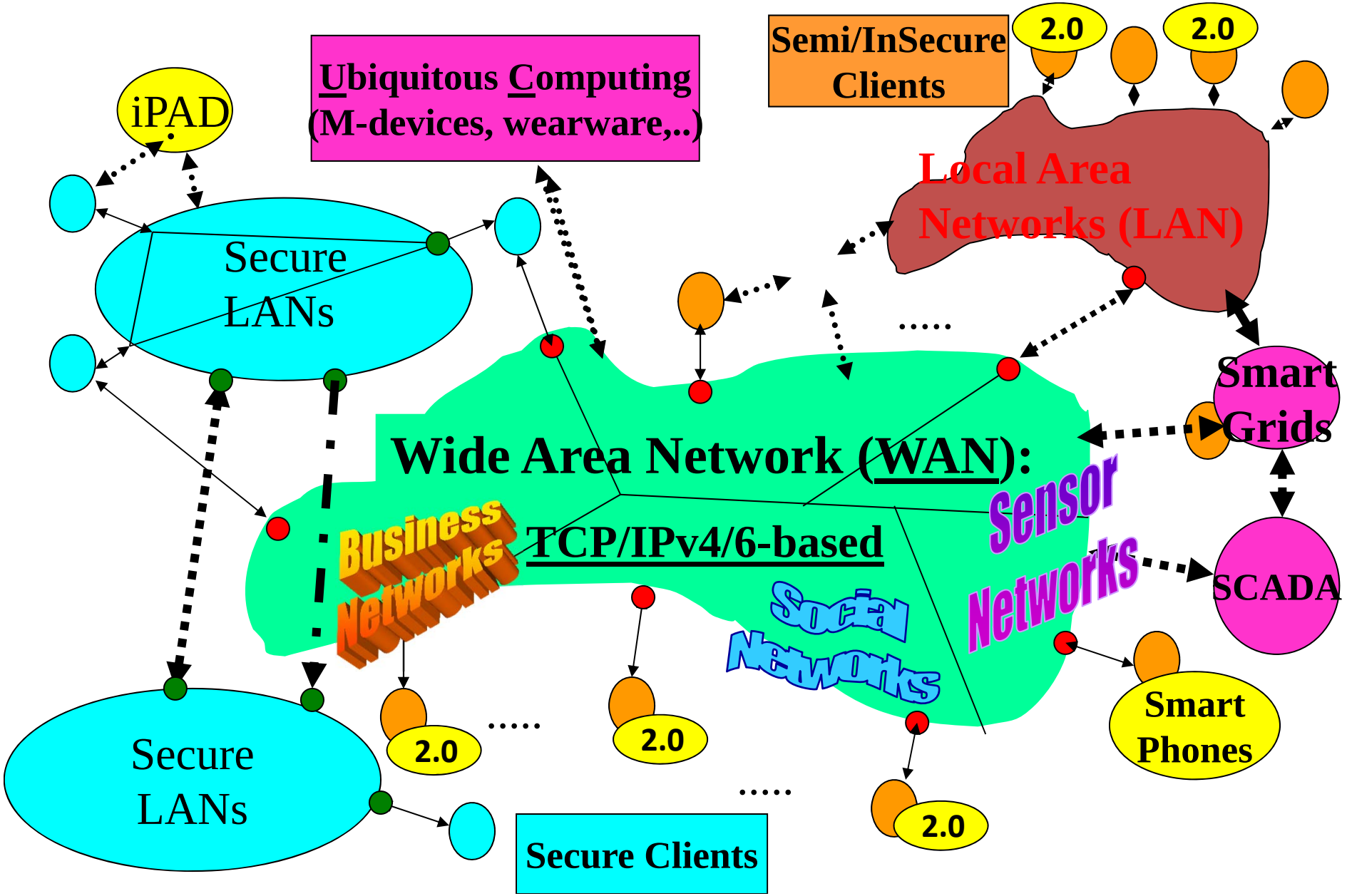
4a) Sensors as Source of Information

4b) Communication with / Remote Control of Engines

4c) Remotely Operated Production/Logistics

1.1D) „Information Economy“and „Web 3.0“:Growing Complexity

2015: >1M Server, >3G Klienten, >1T Sensors(“Smart Grids“)



1) Changing World – Changing Crime:

1.2A) NewCrime: CyberCrime, CyberWar

„Crime“ and „War“ go Cyber:

- Originally, „Crime“ developed as LEGAL category, defined in NATIONAL contexts, including
  → Murder, Theft, Fraud, Rape, Espionage, Terrorism, …
- To cover legally also INTERNATIONAL contexts, further categories of the „International Criminal Law“ were defined in specific TREATIES, adressing topics such as:
  → Crimes against peace, Genocide, Piracy, Slavery, War of Aggression, War Crimes.
- „War Crimes“ (regulated in Hague and Geneva Conventions), adressed topics such as
  → Ill-treatment/Murder of Prisoner-of-Wars, any Devastation not justified by Military/Civilian necessities

1) Changing World – Changing Crime:

1.2B) NewCrime: CyberCrime, CyberWar

Development of regulations:

As international cooperation as well as conflicts develop in Cyber Space, national laws hardly apply.

Attempts to develop international treaties (conventions) are limited (e.g. European Council, Budapest convention), adressing

→ Illegal Access/Interception, Data/System Interferences, Misuse of Devices, Computer-related Forgery/Fraud

Status: Presently, NO international convention adresses „War or international conflicts in Cyberspace“. As legal procedures develop only slowly (esp. in transnational contexts), it seems reasonable to approach Cyber conflicts from technical ground.

1) Changing World – Changing Crime:

1.2C) NewCrime: Advanced Persistent Threats

Advanced Persistent Threats (APT):

A Structure for describing Cyber Threats:

Read: Bodmer, Kilger, Carpenter and Jones (BKCG): "Reverse Deception: Organized Cyber Threat Counter-Exploitation", New York: McGraw-Hill Osborne Media

Terminology (speakers review):

Threat : APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded.

Advanced : This term is used (esp. by developers of "new" technologies) to claim their "intelligence-gathering techniques" from "traditional" (aka "less advanced") ones (such as Malware Detection, Intrusion Detection) as "innovative". Related tools combine different methods to detect and possibly compromise suspicious targets.

Persistent: Under the assumption that "attacks" are EXTERNAL, continuous long-time monitoring of perimeters should lead to the identification of attackers and consequently a continuous surveillance of related "targets".

1) Changing World – Changing Crime:

1.2D) NewCrime: Advanced Persistent Threats

BKCG define the following Criteria for an APT:

Objectives - Which **final goals** is the APT pursuing
(e.g. **Stealing Information**, Damaging Industrial Processes: **Stuxnet**)

Skills and methods - **Tools and techniques used** during APTs
(e.g. spear fishing, **using exploits**)

Resources – **Prerequisites** (e.g. knowledge) for performing an APT

Actions – Detailed **analysis of actions** associated with an APT
(→ **Part 2: Stuxnet/Flame/Red October analysis, Mandiant Report**)

Origins of Attack – Description of all points where attack started (originated), including detailed analysis which systems contributed to the attack
(**Frequent problem**: **traces may be hidden/spoofed**: → **Part 2**: **Stuxnet**, …)

Temporal Behaviour – **time series** of all steps/processes observed during an APT

Risk – Effects of an APT as long as undetected

More Criteria:

Methods to Detect/Analyse/Survey APTs: Forensic methods, such as Reverse Engineering software, Remote Installation methods/tools, Botnets, Sinkholes.

Comment: Systematic scientific classification of APTs needs further development. Presently, "Advanced Persistent Threats" are a buzzword used for marketing related products.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1 The Stuxnet complex:

2.1) The Stuxnet complex (September 2010 - February 2013)

- → A) SCADA Technology: Siemens SIMATIC WinCC
- → B) Stuxnet 1.0: ref. Symantec September 2010
- → C) Stuxnet 0.5: ref. Symantec February 2013
- → D) Duqu: ref. Kaspersky October 2012

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1A1 The Stuxnet complex: SCADA Technology

Quelle Wikipedia: **SCADA: Supervisory Control and Data Acquisition**:

SCADA (**supervisory control and data acquisition**) is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large scale processes that can include multiple sites, and large distances.[1] These processes include industrial, infrastructure, and facility-based processes, as described below:

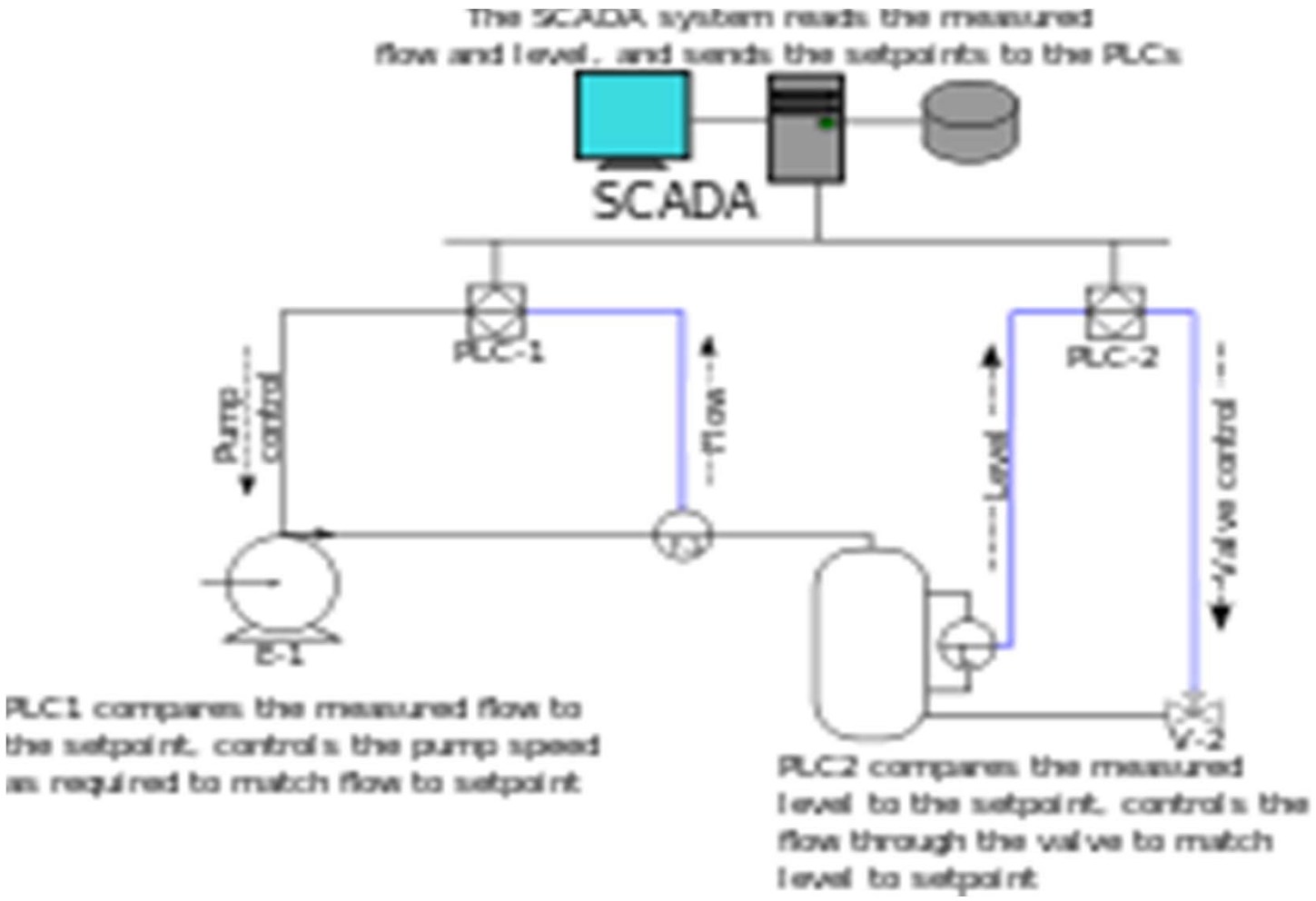
Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.

Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.

Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access, and energy consumption.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1A2 The Stuxnet complex: SCADA Technology



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1A3 The Stuxnet complex: SCADA Technology

Quelle: http://www.automation.siemens.com/

„Prozessvisualisierung mit Plant Intelligence

Unsere SCADA-Software bietet höchste Funktionalität und eine benutzerfreundliche Bedienoberfläche. Mit dem projektier- und skalierbaren System profitieren Sie von absoluter Offenheit zu Bürowelt und Produktion – z. B. via integrierter Prozessdatenbank und durch Plant Intelligence für mehr Transparenz in der Produktion. Zahlreiche Optionen und Add-ons ergänzen und erweitern den Leistungsumfang“

„Branchenlösungen mit SIMATIC WinCC

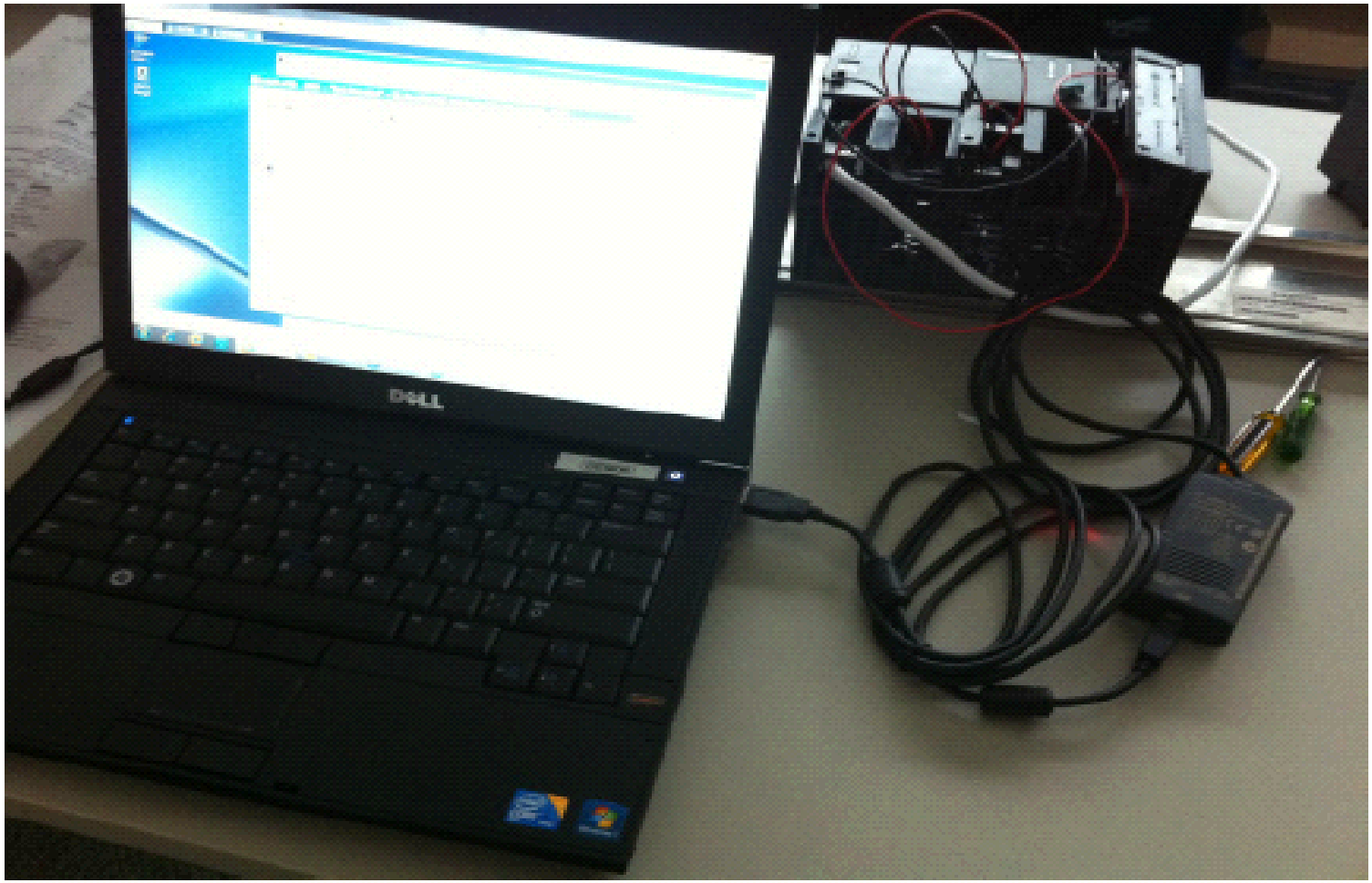
Erfahren Sie, wie Sie aus dem branchenneutralen SCADA-System WinCC mit den richtigen Optionen und Add-ons eine lmaßgeschneiderte Branchenlösung erstellen können.“

Anmerkung: Kopie (sic!) der SIMATIC Webseiten (1/2).

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1A4 The Stuxnet complex: SCADA Technology

Figure 16
Test equipment

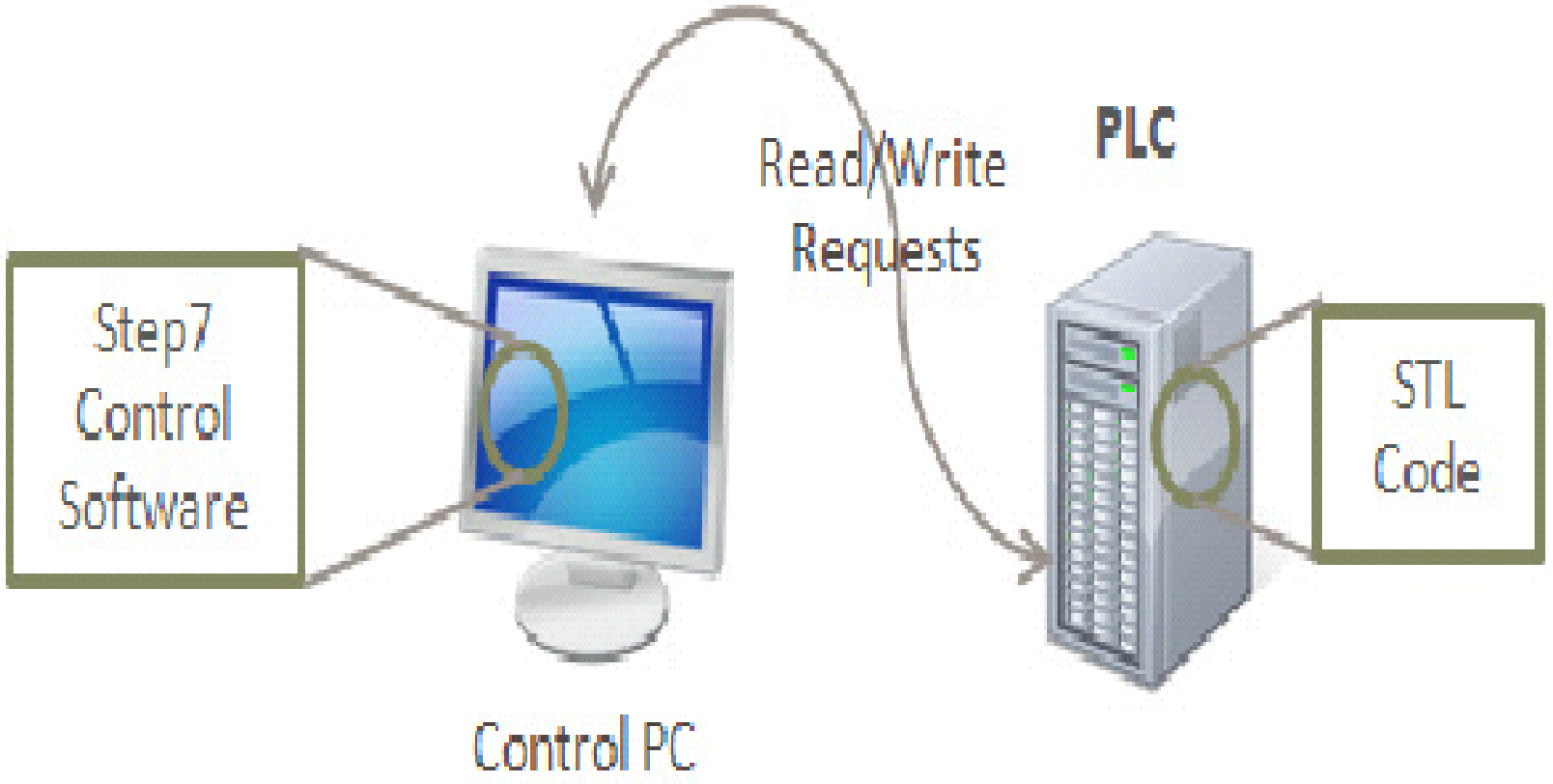


2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1A5 The Stuxnet complex: SCADA Technology

Figure 15

PLC and Step7



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B1 The Stuxnet complex: Stuxnet 1.0

Source: Symantec „W32.Stuxnet Dossier“, September 2010

Executive Summary:

Stuxnet is a threat targeting a specific industrial control system (*) likely in Iran(*), such as a gas pipeline or power plant.

The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLC)

(PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries.

Stuxnet was discovered in July 2010, but is confirmed to have existed at least one year prior and likely even before.

Comments: (*) SIMATIC WinCC

(**) First STUXNET known since November 2008!

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B2 The Stuxnet complex: Stuxnet 1.0 Propagation:

…. **Stuxnet contains many features such as**:

Self-replicates through removable drives **(USB!)** exploiting a vulnerability allowing auto-execution.

Spreads in a LAN through a vulnerability in the **Windows Print Spooler (***)**.

Copies and executes itself on remote computers through network shares.

Copies and executes itself on remote computers running a WinCC database server loaded.

Comment: (***) **Microsoft Vulnerabilities**

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B3 The Stuxnet complex: Stuxnet 1.0 Exploitation:

Updates itself through a peer-to-peer mechanism within a LAN.

Exploits a total of 4 unpatched Microsoft vulnerabilities, 2 of which are **previously mentioned vulnerabilities for self-replication** and the other two are **escalation of privilege vulnerabilities** that have yet to be disclosed.

Contacts a command and control server that allows the hacker to download and execute code, including updated versions.

- **Contains a Windows rootkit** that hide its binaries.
- Attempts to **bypass security products**.
- Fingerprints a specific industrial control system and **modifies code on Siemens PLCs** to potentially sabotage the system.
- **Hides modified code** on PLCs, essentially a rootkit for PLCs.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B4 The Stuxnet complex: Stuxnet 1.0 Timeline (#1/2)

→ **November 20, 2008** Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.

→ **April, 2009** Security magazine Hakin9 releases details of a remote code execution vulnerability in Printer Spooler service (later MS10-061).

→ **June, 2009** Earliest Stuxnet sample seen (no exploit MS10-046/ no signed driver files).

→ **January 25, 2010** Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.

→ **March, 2010** First Stuxnet variant to exploit MS10-046.

→ **June 17, 2010** Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).

→ **July 13, 2010** Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).

→ **July 16, 2010** Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files.

Verisign revokes Realtek Semiconductor Corps certificate.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B6 The Stuxnet complex: Stuxnet 1.0 Timeline (#2/2)

→ **July 17, 2010** Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.

→ **July 19, 2010 Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems.**

Symantec renames detection to W32.Stuxnet.

→ **July 20, 2010 Symantec monitors the Stuxnet Command and Control traffic.**

→ **July 22, 2010** Verisign revokes the JMicron Technology Corps certificate.

→ **August 2, 2010** Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.

→ **August 6, 2010** Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.

→ **September 14, 2010** Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August.

→ Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.

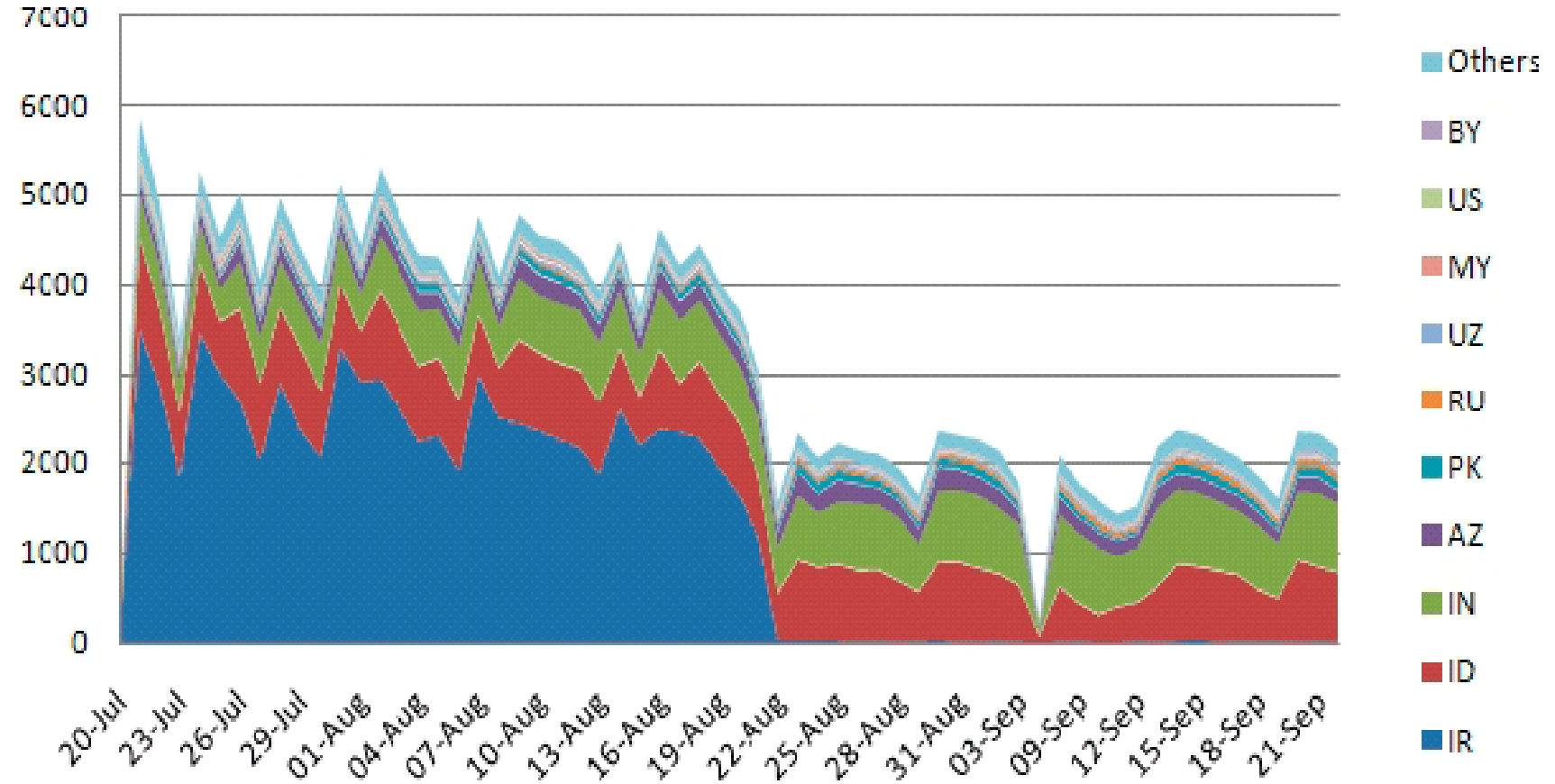
→ **September 30, 2010 Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.**

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B7 The Stuxnet complex: Stuxnet 1.0 Infection by Country

Figure 5

Rate of Stuxnet infection of new IPs by Country



Internetabkürzungen: IR=Iran, ID=Indonesien, IN=Indien, AZ=Azerbeidshan, PK=Pakistan, RU=Russland, ZU=Uzbekistan, MY=Malaysia, US=USA, BY=Belarus

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B8 The Stuxnet complex: Stuxnet 1.0 Functions:

2.2.3f1 Stuxnet Infection Routine flow

2.2.3f2 Stuxnet Command and Control flow

2.2.3f3 Stuxnet Downloading latest Version

Remark: Folios discussed in presentation, but not for distribution, following aVTC (Uni-Hamburg) ethical principle „Never distribute essential details of malicious code or malicious code in an executable form!“

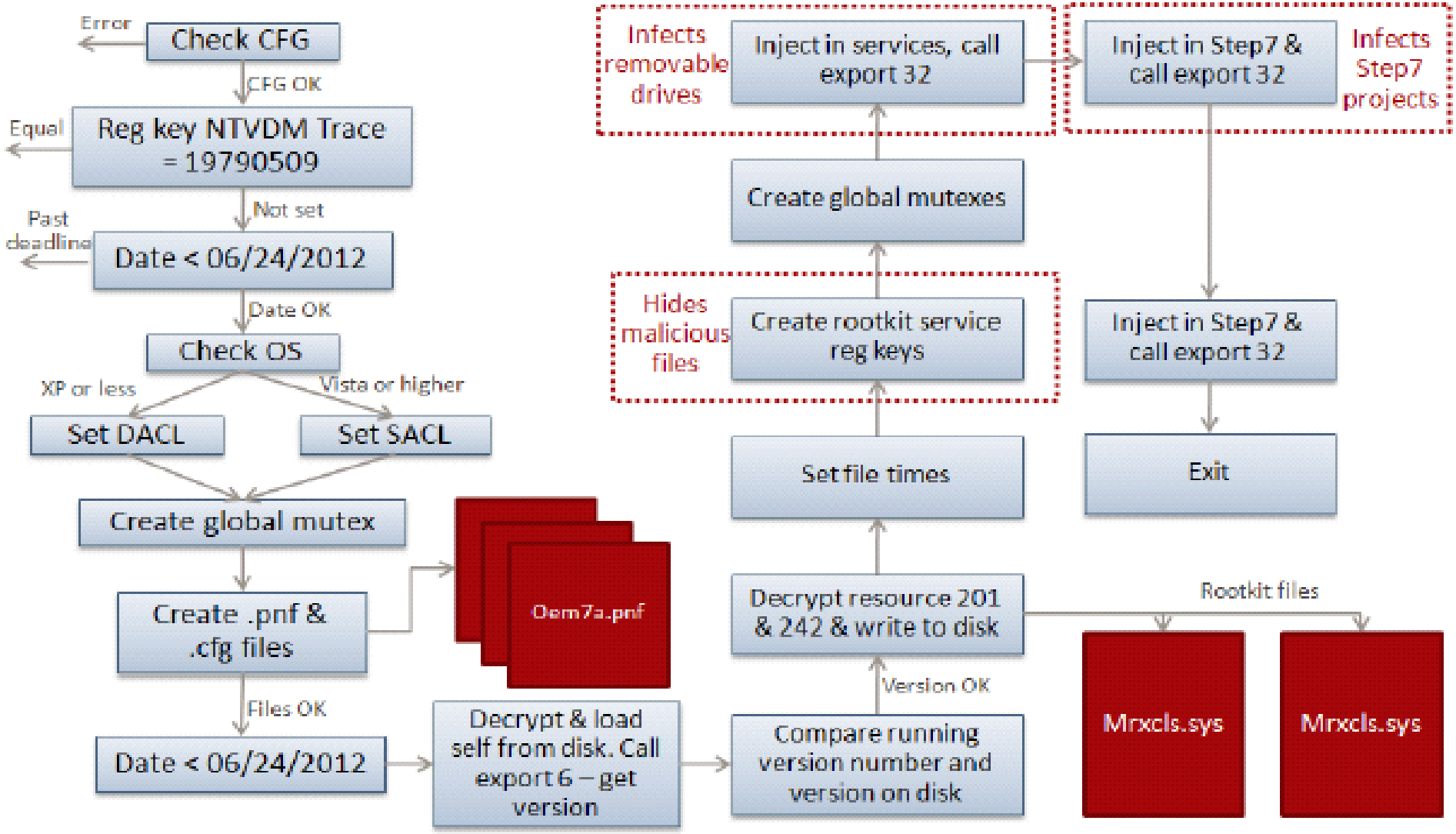
Remark: aVTC = antiVirus Test Center, University of Hamburg

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B9 The Stuxnet complex: Stuxnet 1.0 Infection Flow:

Figure 7

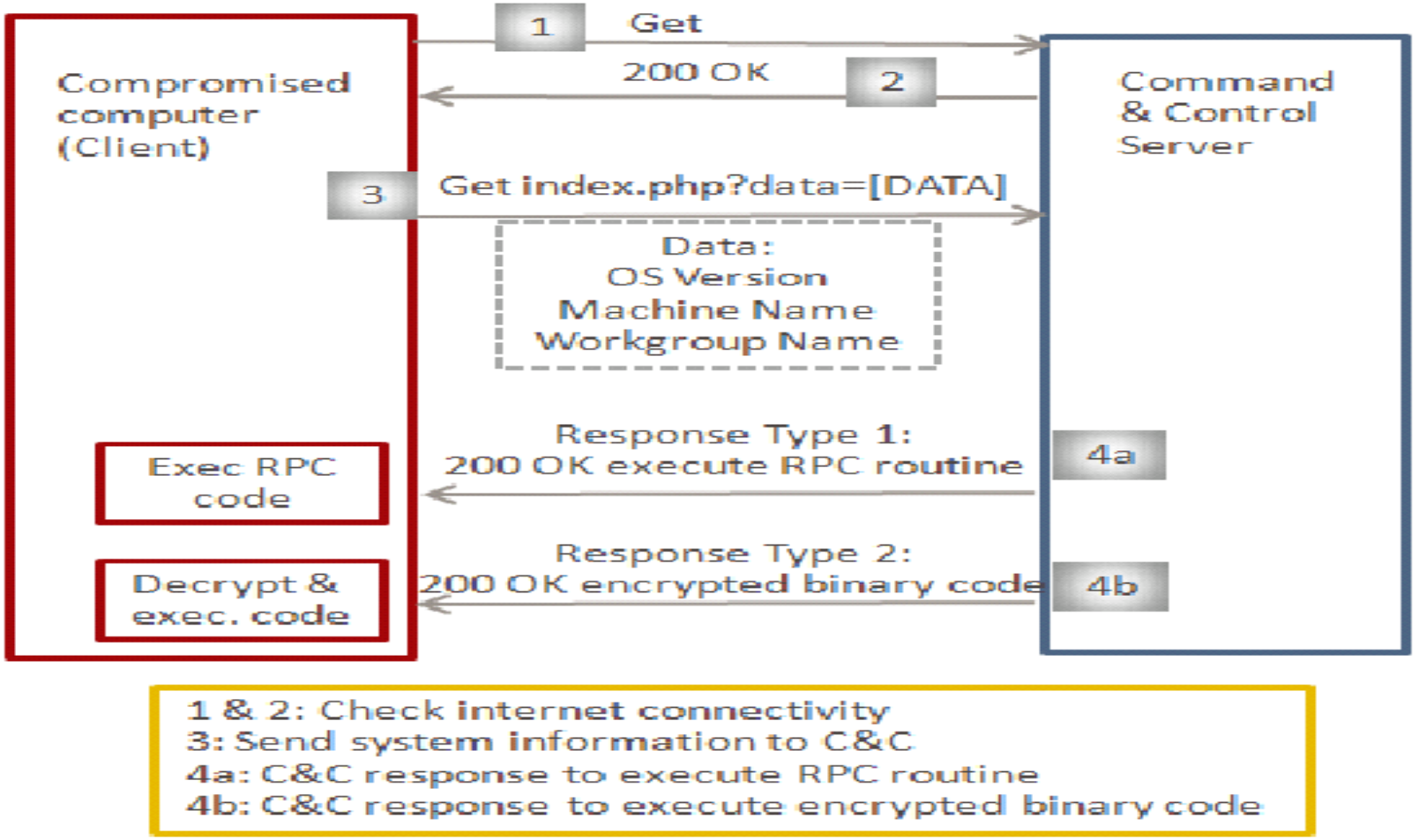
Infection routine flow



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B10 The Stuxnet complex: Stuxnet 1.0 C&C Flow

Figure 8
Command and Control

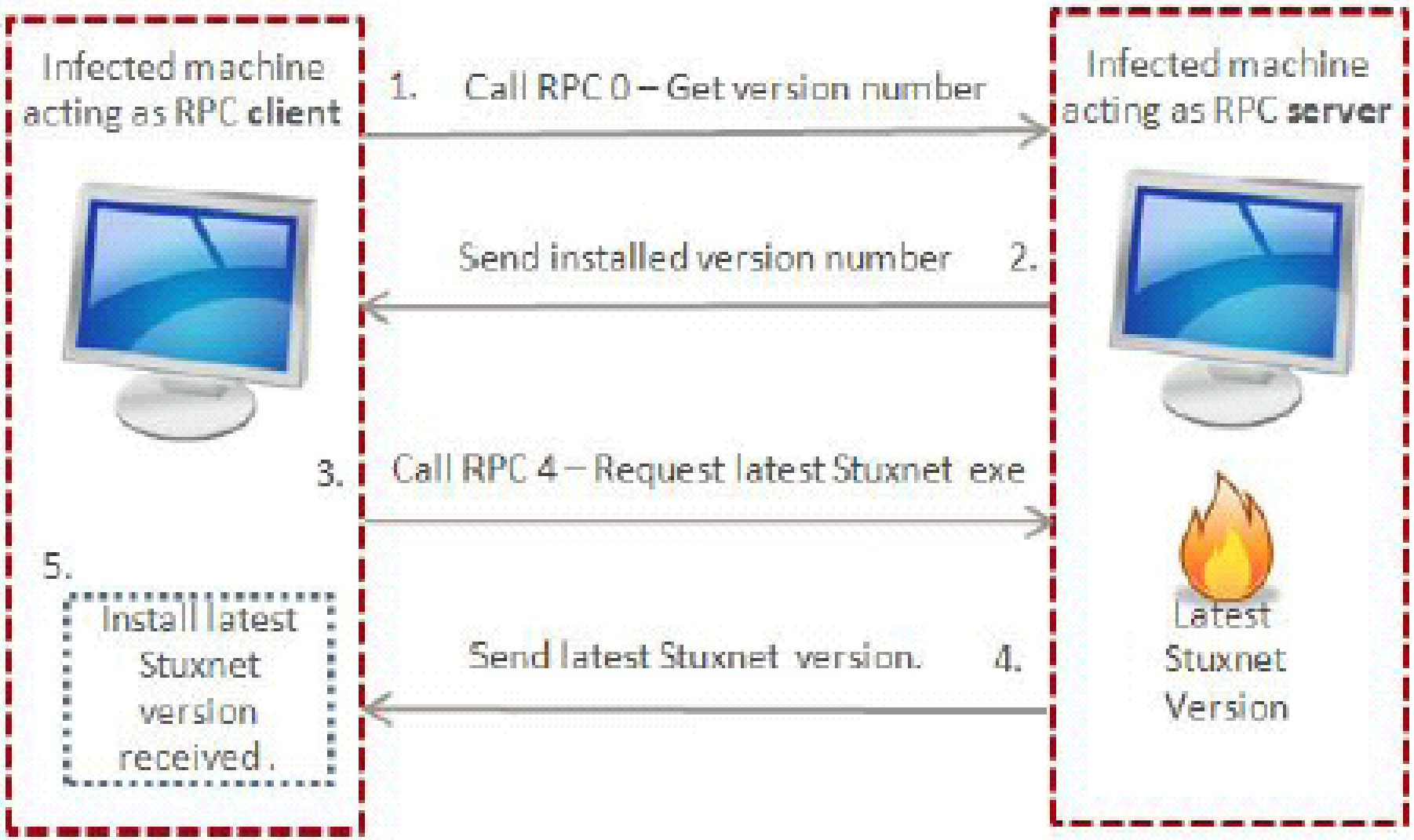


2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B11 The Stuxnet complex: Stuxnet 1.0 Download Process

Figure 9

Example of an old client requesting latest version of Stuxnet via P2P



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1B12 The Stuxnet complex: Stuxnet 1.0 Public Reports

Public Media about Stuxnet´s developers :

New York Times (2011-01-15): „Israeli Test on Worm Called Crucial in Iran Nuclear Delay“
Autoren: W.J.Broad, J.Markoff, D.E.Sanger

Thesis: Israeli experts developed Stuxnet, assisted by US experts

Forbes (2011-01-17): „The New York Times Fails To Deliver Stuxnet's Creators“
Autor: J. Carr

Contradiction: not sufficient evidence for developers!

Spiegel Online (2011-01-18): „Stuxnet: Angst vor einem zweiten Tschernobyl“
Autor: J.Patalong

Speculation: some (unnamed) „experts“ assume that Maximum Credible Accident (MCA) may happen if infected systems connect to Internet, and warn about possible imitators!

(MCA: deutsch =GAU)

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1C1 The Stuxnet complex: Stuxnet 0.5

After detection of Stuxnet 1.0 In-the-Wild (ITW) in July 2010, **analysis required several months** (unprecedented complexity), with **earliest version dated 2009**.

Only in 2012, a version predating the 1.0 version was detected, which was in operation between 2007 and 2009 with indications that it, or even earlier variants of it, were **in operation as early as 2005**.

Key new findings in Stuxnet 0.5 (!presently oldest version detected!)**:**

- → **Built using the Flamer platform**
- → **Spreads by infecting Step 7 projects including on USB keys**
- → **Stops spreading on July 4, 2009**
- → **Does not contain any Microsoft exploits**
- → **Has a full working payload against Siemens 417 PLCs that was incomplete in Stuxnet 1.x versions**
- → As with version 1.x, **Stuxnet 0.5 is a complicated and sophisticated piece of malware requiring a similar level of skill and effort to produce.**
- → **Despite the age of the threat and kill date, Symantec sensors have still detected a small number of dormant infections (Stuxnet 0.5 files found within Step 7 project files) worldwide over the past year.**

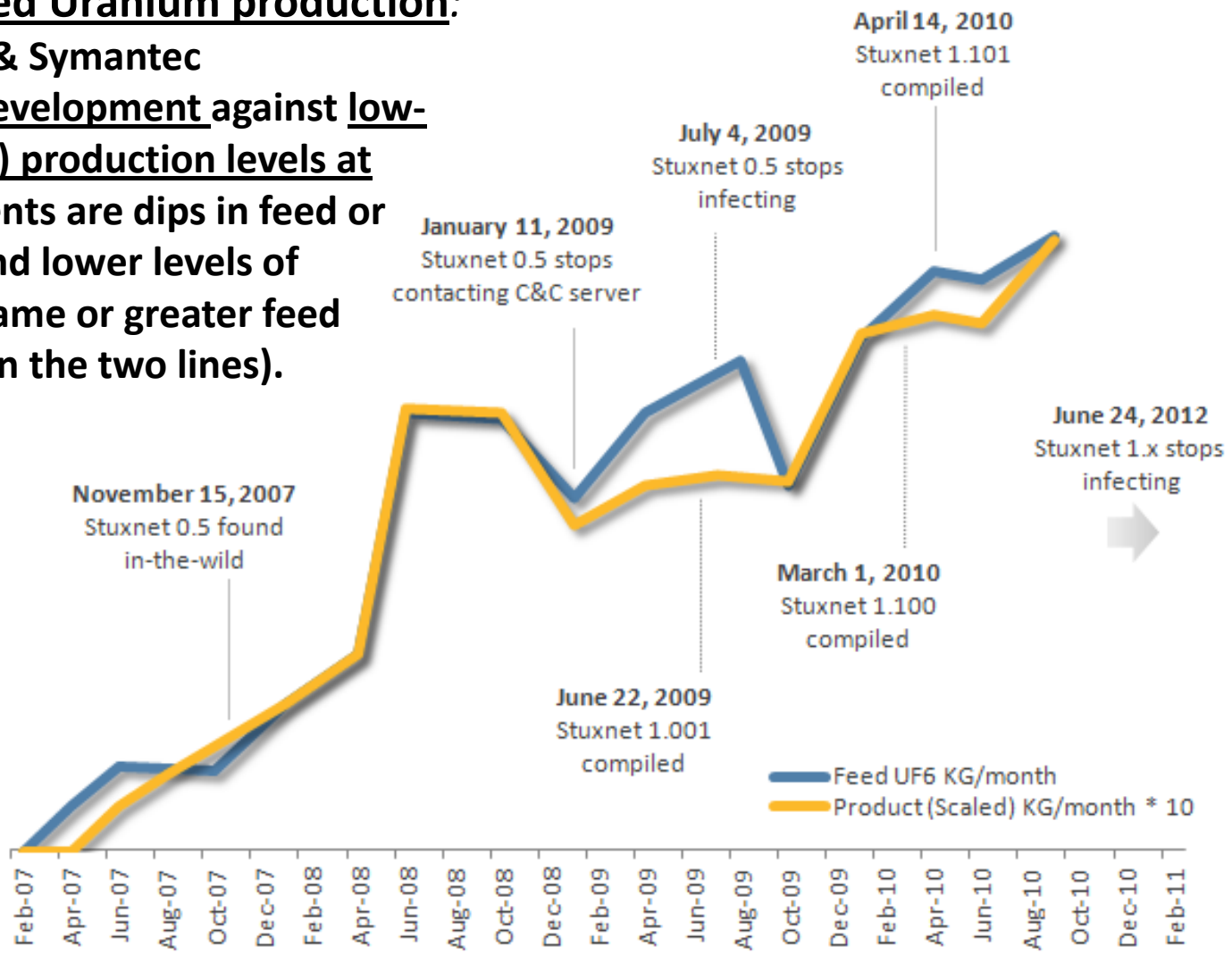
2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1C2 The Stuxnet complex: Stuxnet 0.5

Figure 1. Low Enriched Uranium production:

Source: ISIS & Symantec

Key dates of Stuxnet development against low-enriched uranium (LEU) production levels at Natanz. Interesting events are dips in feed or production amounts and lower levels of production given the same or greater feed amounts (gaps between the two lines).



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1C3 The Stuxnet complex: Stuxnet 0.5

Video „Stuxnet: How it infects PLCs“ (5:44 min)

→http://www.symantec.com/tv/products/details.jsp?vid=673432595001

Video „Stuxmet 0.5: The Missing Link“ (3:06 min)

→http://www.symantec.com/tv/products/details.jsp?vid=2180741043001

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1D1 The Stuxnet complex: Duqu Trojan

Source: Kaspersky Labs (October 2012):

Essentials of Duqu Trojan:

→ **Duqu: sophisticated Trojan**, probably written by the group which created the Stuxnet worm (though Duqu doesNOT replicate and doesNOT attack PLCs). At least 7 variants, configured to run for 30 or 36 days.

→ **Similarities between Duqu and Stuxnet:** Usage of various encryption keys, including ones that haven't been made public prior to Duqu, injection techniques, usage of zero-day exploits, usage of stolen certificates to sign the drivers

→ **Main purpose**: act as a backdoor into an attacked system and support collection any kind of information from its targets (which may be industrial targets), possibly also from Certification Authorities. Duqu uses **"infostealer"**

→ **Infection works** through a targeted attack involving a Word document which exploits the 0-day CVE-2011-3402 vulnerability, allowing an attacker to run code with highest privilege level, bypassing most of the protection mechanisms from Windows or security software.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1D2 The Stuxnet complex: Duqu Trojan

Essentials of Duqu Trojan: (continued)

→ **Duqu connects to various C&C servers** in India, Belgium, **Germany ("B"),** India, Netherlands, UK, Singapore, South Korea, Switzerland, **Vietnam ("A")** and several more used as C&C proxies. Probably, a dozen C&C servers were active between 2009 and 2011.

→ On **20 October 2011** a **major cleanup operation of the Duqu network (including C&C Servers "A" and "B")** was initiated, where every single server used as far back as 2009 was cleaned.

→ **Main Server 'A' – Vietnam:** Server 'A' was located in Vietnam and was **used to control certain Duqu variants found in Iran**. This was a **Linux server** running CentOS 5.5, as all other Duqu C&C servers run CentOS – version 5.4, 5.5 or 5.2. (reason for this choice is unknown).

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1D3 The Stuxnet complex: Duqu Trojan

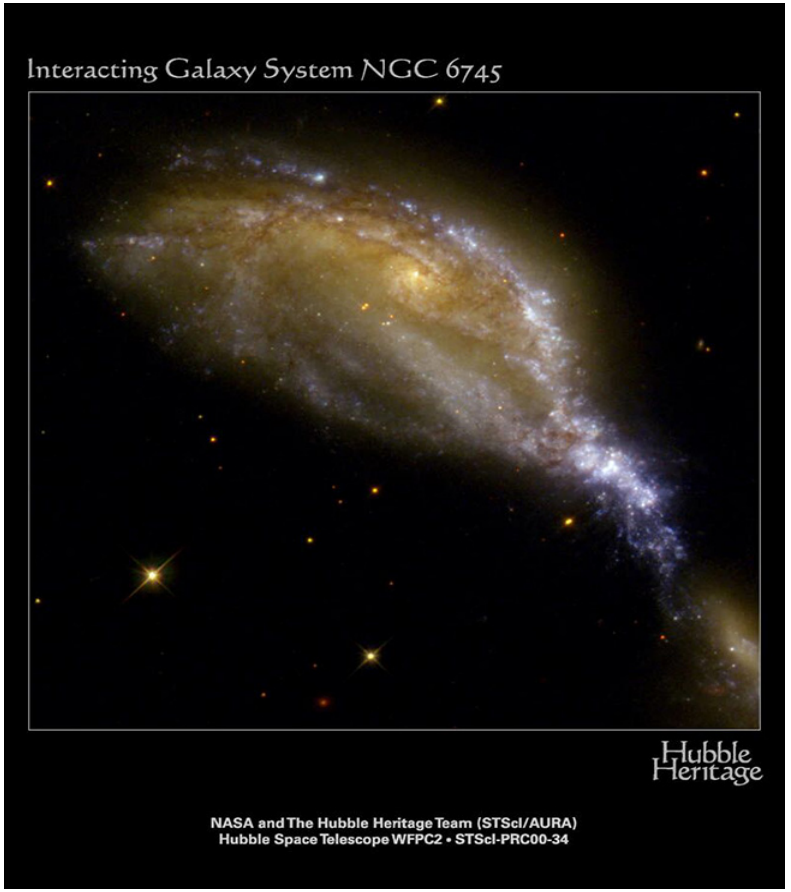
→ **Server 'B' – Germany:** This server was located at a **data center in Germany** that **belongs to a Bulgarian hosting company**. It was **used by the attackers to log in to the Vietnamese C&C**. Immediately after cleaning up the server, the attackers rebooted it and logged in again to make sure all evidence and traces were erased.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.1D4 The Stuxnet complex: Duqu Trojan

Possible evidence of the authors´of Duqu

- → 1) Similarities between Stuxnet and Duqu: same team?
- → 2) Strange interest of some author in astronomy: infostealer.exe has a portion of a JPEG file picked up by the Hubble telescope (“Interacting Galaxy System NGC 6745”)
- → 3) The Duqu Word document containing infostealer.exe has a font called "Dexter Regular", by "Showtime Inc.," (c) 2003; Showtime Inc. is the cable broadcasting company behind the TV series Dexter, possibly some “footprint” of one author.



2) A Survey of Attacks on Enterprises&Industrial Infrastructures

2.2 The Flame complex:

2.2) The Flame Complex:

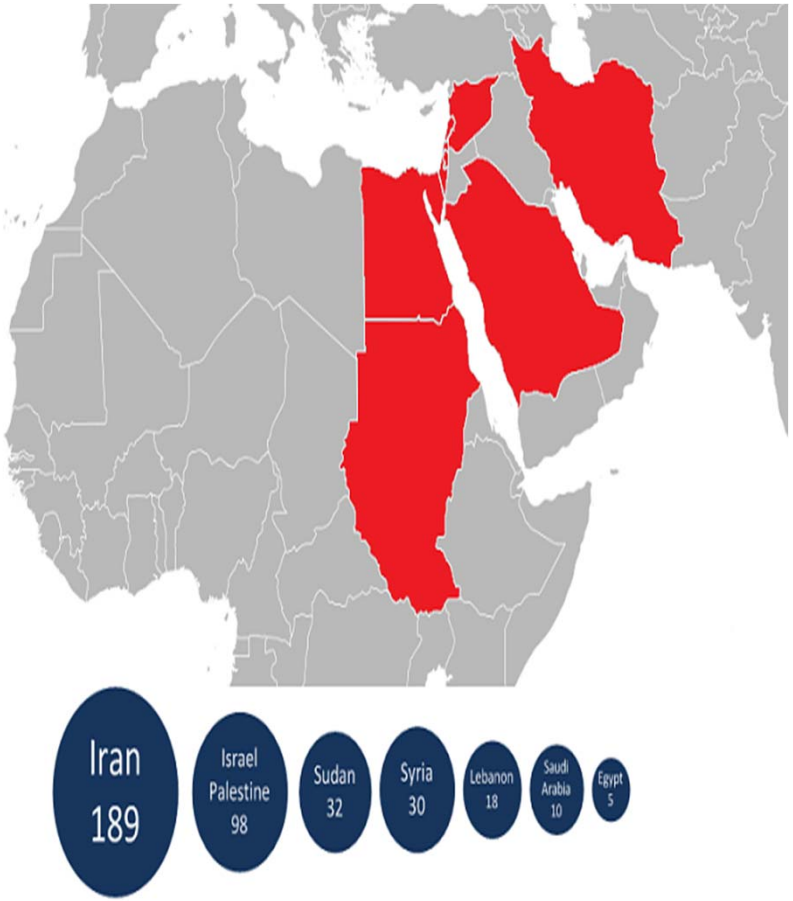
- → A) Flame/Wiper: ref. Kasperksy Labs (May 2012)
- → B) Gauss: ref. Kasperksy Labs (August 2012)
- → C) SPE=miniFlame: ref. Kasperksy Labs (October 2012)
- → D) Comparison Stuxnet-Flame

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2A1 The Flame complex: Flame/Wiper:

Source: Kaspersky Labs (May 2012):

- → Following Kapspersky Lab, many media reported about a „virus“ named Wiper, SkyWiper or Flame, which with its 20 MB code was regarded as the „most complex attack on IT systems“ so far observed.
- → „Flame“ was reported to be capable of stealing all kind of data, and it can monitor any mobile communication (via Bluetooth) and transfer screen content as well as input from keyboards.
- → „Flame“ attacks were reported from Near East, esp. From Iran.



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2A2 The Flame complex: Flame/Wiper:

Features of „Flame“:

- → „Flame“ is a sophisticated attack toolkit, a backdoor, a Trojan, and it has worm-like features, allowing it to replicate in a local network and on removable media if it is commanded so by its master.
- → „Flame“ consists of 20 attack modules which support espionage activities; more modules can be added easily.
- → First report about a „Flame“-based attack in spring 2010, but measures for detection and cleaning exist only since May 2012.
- → Unconfirmed reports in US media (NYT, WP) that president Bush senior ordered the development by US and Israeli experts (similar to Stuxnet)
- → At least some developers have significant knowledge about cryptography and digital certificates.
- → Strange is written in Lua: a scripting language which can very easily be extended and interfaced with C code. Many parts of Flame have high order logic written in Lua - with effective attack subroutines and libraries compiled from C++.

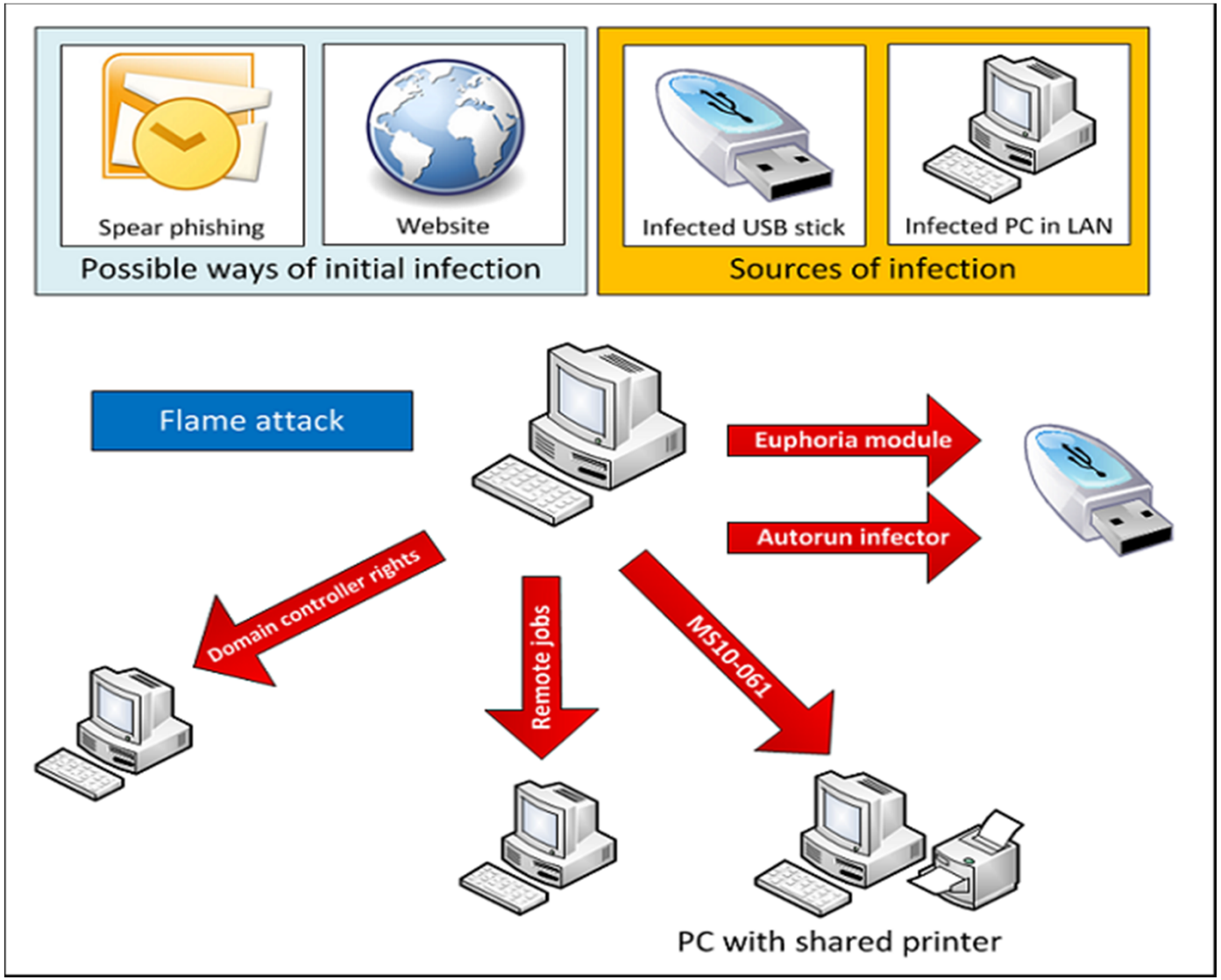
2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2A3 The Flame complex: Flame/Wiper:

- → Replication in local networks: printer vulnerability MS10-061 (as Stuxnet)
- → The replication part appears to be operator commanded, like Duqu, and also controlled with the bot configuration file. Most infection routines have counters of executed attacks and are limited to a specific number of allowed attacks.
- → Once a system is infected, Flame begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations, intercepting the keyboard, and so on. All this data is available to the operators through the link to Flame's command-and-control servers.
- → Remote jobs tasks: When Flame is executed by a user who has administrative rights to the domain controller, it is also able to attack other machines in the network: it creates backdoor user accounts with a pre-defined password that is then used to copy itself to these machines.
- → Flame's modules together account for over 20MB. Much of these are libraries designed to handle SSL traffic, SSH connections, sniffing, attack, interception of communications and so on.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2A4 The Flame complex: Flame Architecture



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2B1 The Flame complex: Gauss

Source: Kaspersky Labs SecureList (August 2012)

- → **Gauss project: developed in 2011-2012 along the same lines as the Flame project. First infections observed September 2011. The malware has been actively distributed in the Middle East for at least the past 10 months. The largest number of Gauss infections has been recorded in Lebanon, in contrast to Flame, which spread primarily in Iran.**
- → **Function: as Flame, Gauss is an espionage toolkit esp. stealing credentials for various banking systems and social network, email and IM accounts. Collected information is sent to a set of C&C servers. The code includes commands to intercept data required to work with several Lebanese banks - for instance, Bank of Beirut, Byblos Bank, and Fransabank. No self-replication found (so far), original attack vector unknown!**
- → **Naming: several Gauss modules are named after famous mathematicians, esp. modules named 'Gauss‘ (the central ionformation-colleting module), 'Lagrange', 'Godel', 'Tailor', 'Kurt' (apparently refering to Goedel).**

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

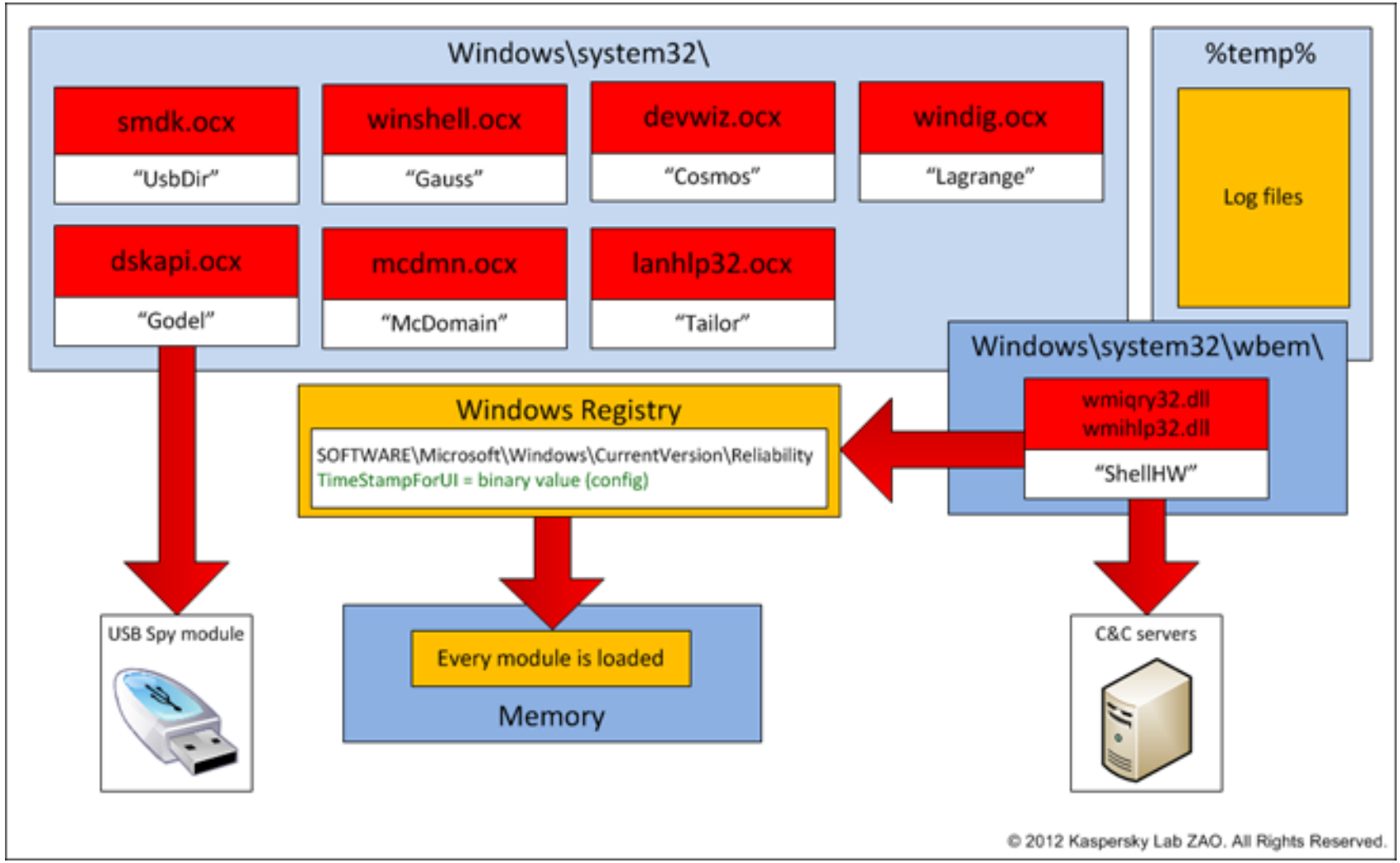
2.2B2 The Flame complex: Gauss

→ **Details of Gauss functions**: Information is collected using various modules, each of which with its own unique functionality. Essential modules (located at %system32%\)

Module	name	Description
Cosmos:	devwiz.ocx	Collects information about CMOS, BIOS
Kurt, Godel	dskapi.ocx	Infects USB drives with data-stealing module, using an .LNK exploit for the CVE-2010-2568 vulnerability, similar to Stuxnet
Tailor	lanhlp32.ocx	Collects information about network interfaces
McDomain	mcdmn.ocx	Collects information about user's domain
UsbDir	smdk.ocx C	Collects information about computer's drives
Lagrange	windig.ocx	Installs a custom 'Palida Narrow' font
Gauss	winshell.ocx	Installs browser plugins that collect passwords and cookies
ShellHW	wmiqry32.ocx wmihlp32.ocx	Main loader and communication module

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

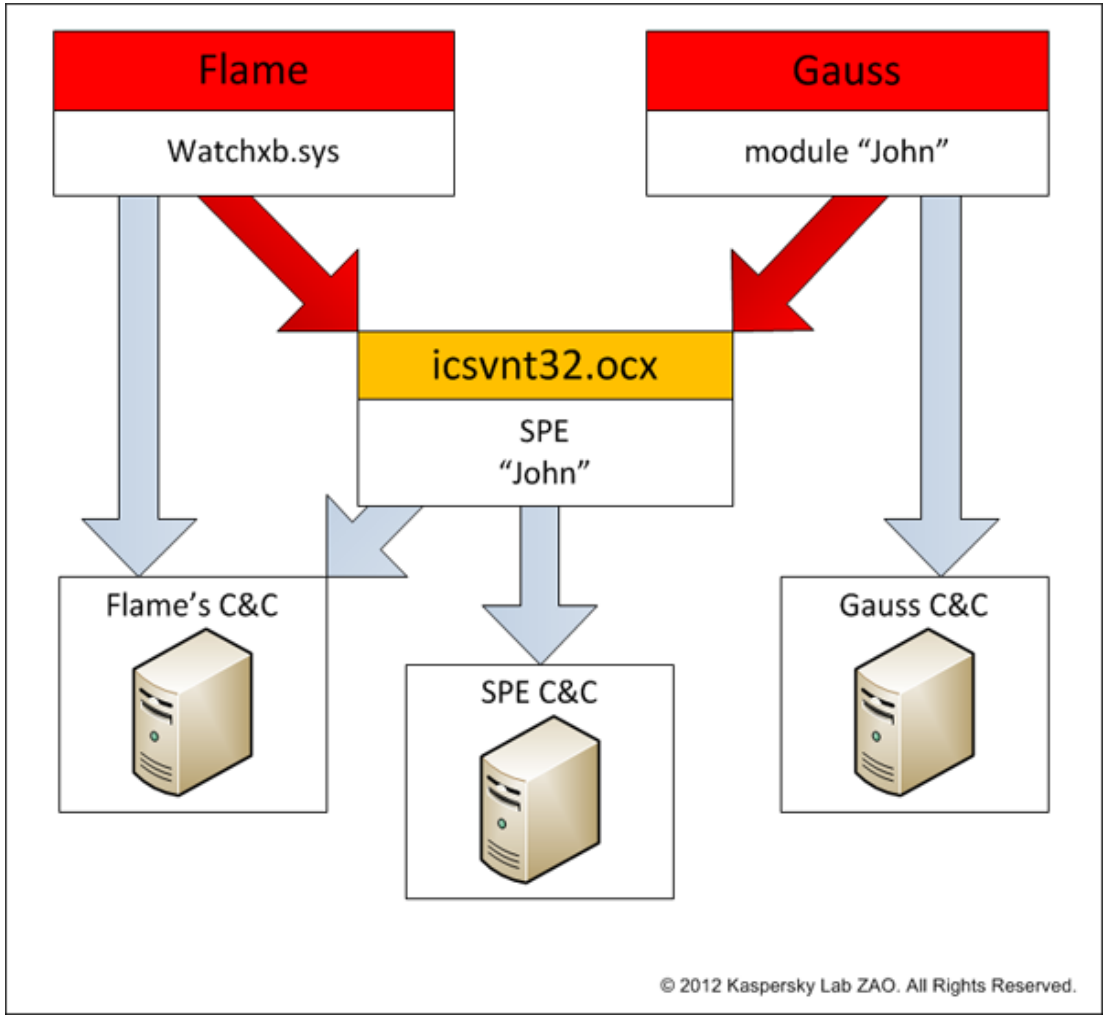
2.2B3 The Flame complex: Gauss



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2C1 The Flame complex: MiniFlame/SPE

Related to Flame and Gauss, SPE (=MiniFlame), detected in 2007) is a special combination of Flame and Gauss modules (esp. Cosmos, Godel (Kurt), Tailor, McDomain, UsbDir, Lagrange, Gauss and ShellHW) . SPE´s variants (versions 4.x and 5.x) have been detected on few machines (<20).



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.2D1 The Flame complex: Comparison Stuxnet-Flame

Statistics of Stuxnet and Flame variants:

Source: Kaspersky Labs (KL)

Name	Incidents (KL stats)	Incidents (approx.)
Stuxnet	More than 100 000	More than 300 000
Gauss	~ 2500	~10 000
Flame (FL)	~ 700	~5000-6000
Duqu	~20	~50-60
miniFlame (SPE)	~10-20	~50-60

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A1 „Red October“ attacks

Source: Kasperksy Labs (January 14, 2013): The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies Kaspersky Jan.14,2013

“Executive Summary

“In **October 2012**, Kaspersky Lab’s Global Research & Analysis Team initiated a new threat research **after a series of attacks against computer networks of various international diplomatic service agencies**. A **large scale cyber-espionage networ**k was revealed and analyzed during the investigation, which **we called «Red October» (after famous novel «The Hunt For The Red October»)**.

- This report is based on d**etailed technical analysis of a series of targeted attacks against diplomatic, governmental and scientific research organizations in different countries, mostly related to the region of Eastern Europe, former USSR members and countries in Central Asia**.
- The **main objective of the attackers was to gather intelligence from the compromised organizations**, which included computer systems, personal mobile devices and network equipment.
- The **earliest evidence** indicates that the **cyber-espionage campaign was active since 2007** and is **still active** at the time of writing (January 2013). Besides that, registration data used for the purchase of several Command & Control (C&C) servers and unique malware filenames related to the current attackers **hints at even earlier time of activity dating back to May 2007**.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A2 „Red October“ attacks

Attack Phase 1: Initial infection

→ The **malicious code** was **delivered via e-mail as attachments** (MS Excel/Word and, probably PDF documents) which were **rigged with exploit code for known security vulnerabilities** in the mentioned applications. In addition to Office documents (CVE-2009-3129, CVE-2010-3333, CVE-2012-0158), it appears that the **attackers also infiltrated victim network(s) via Java exploitation** (known as the **'Rhino'** exploit (CVE-2011-3544).

→ Right **after the victim opened** the malicious document or **visit malicious URL** on a vulnerable system, the **embedded malicious code initiated the set**up of the main component which in turn handled **further communication with the C&C servers**.

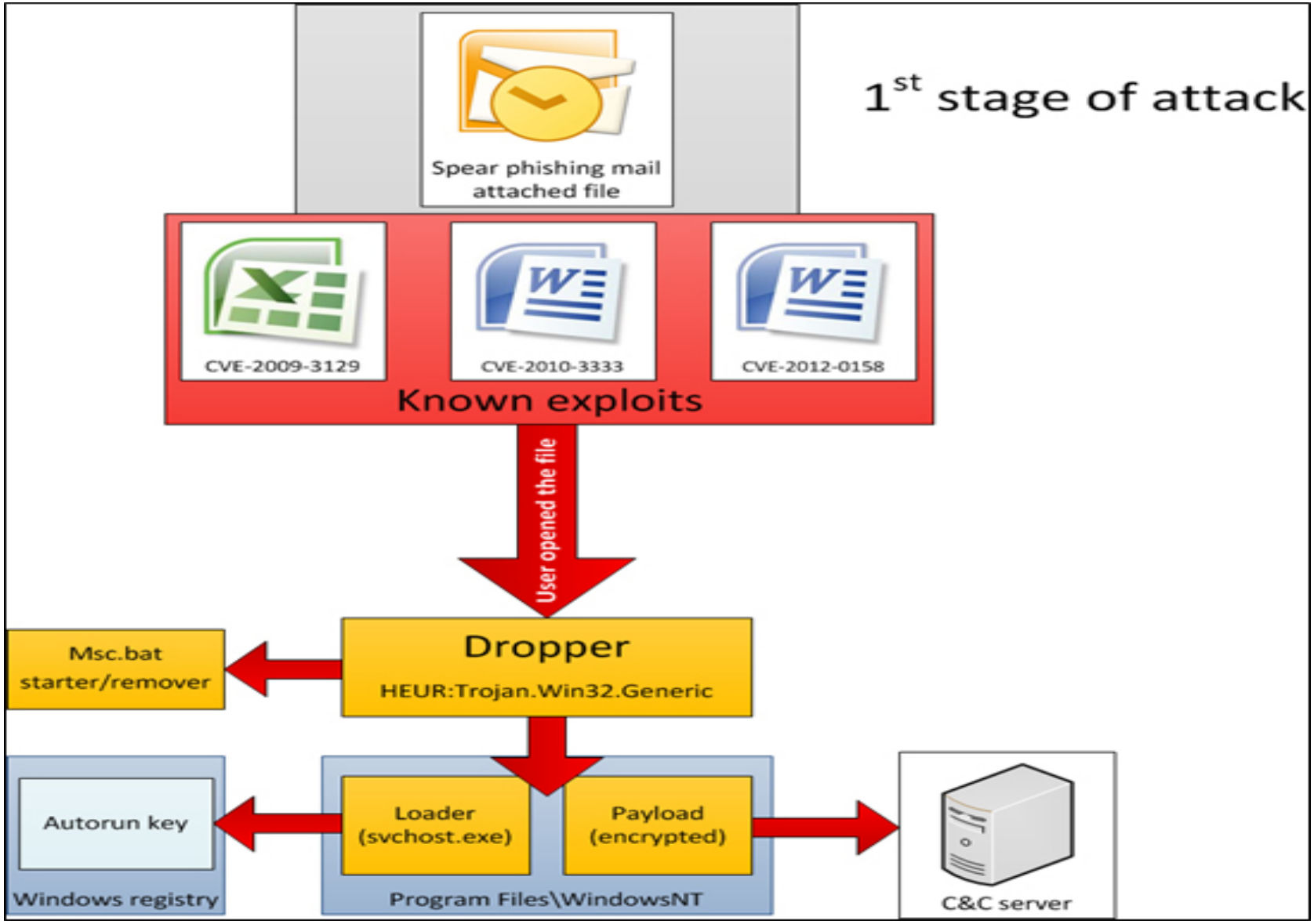
→ Next, the system receives a number of **additional spy modules from the C&C server**, including modules to handle **infection of smartphones**.

Attack Phase 2: Espionage Operation:

→ The main purpose of the **spying modules is to steal information**. This includes files from **different cryptographic systems, such as «Acid Cryptofiler»,** which is known to be **used in organizations of European Union/European Parliament/European Commission** since the summer of 2011. All **gathered information is packed, encrypted and only then transferred to the C&C server.**

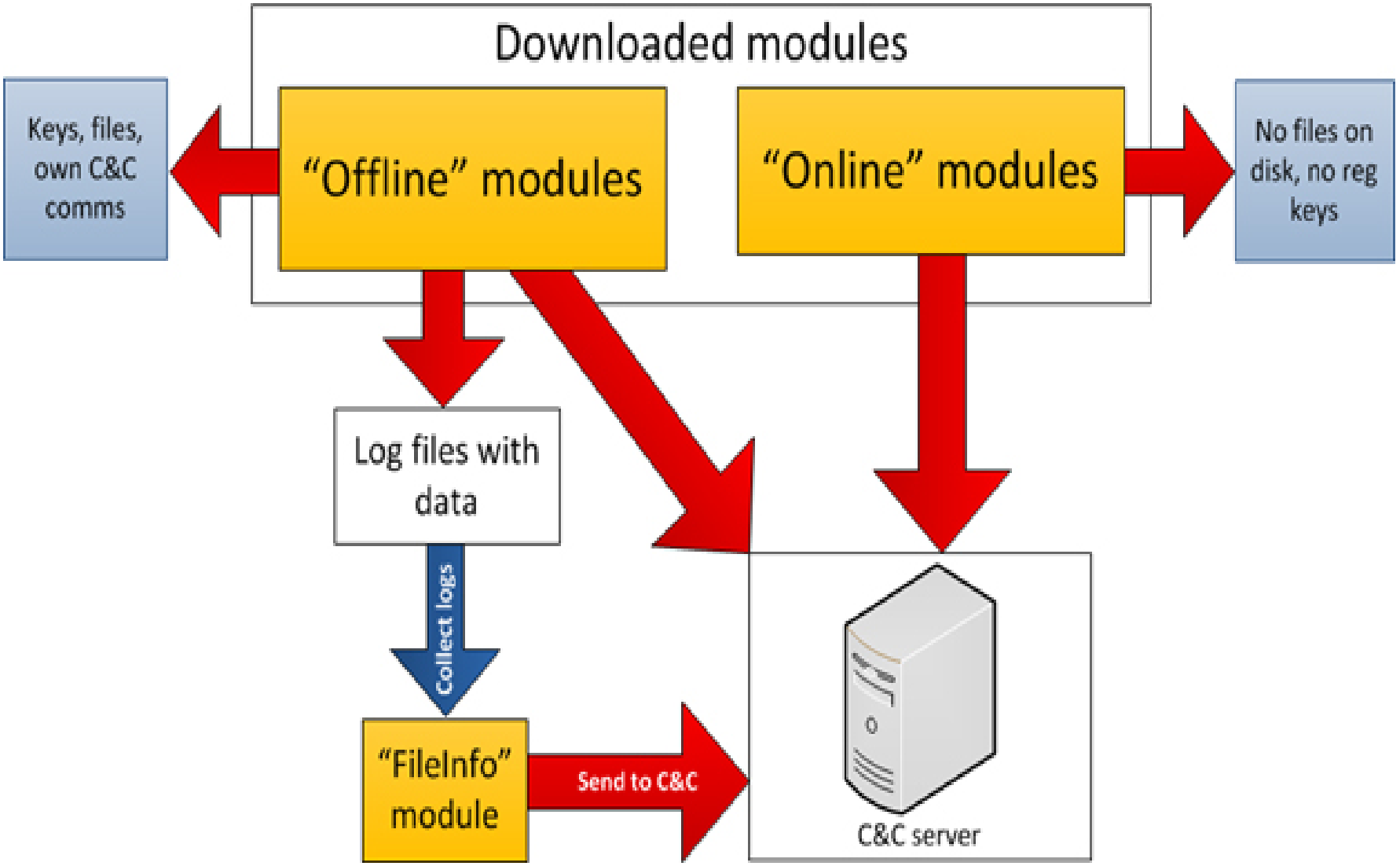
2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A3 „Red October“ attacks



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A4 „Red October“ attacks



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A5 „Red October“ attacks

Timeline:

→ Identified **over 1000 different malicious files** related to **over 30 modules** of this Trojan kit. Most of them were **created between May 2010 and October 2012**.

→ **115 file-creation dates** identified which are related to these campaigns via emails during the last two and a half years.

Targets:

→ Identification of targets: “First, we used the **Kaspersky Security Network (KSN)** and **then** we **set up our own sinkhole server**. The data received using two independent ways was correlating and this confirmed objective findings.

→ **More than 300 unique systems discovered**, which had detected at least one module of this Trojan kit.

→ **Victims**: RUSSIAN FEDERATION 35 KAZAKHSTAN 21 AZERBAIJAN 15 BELGIUM 15
INDIA 15 AFGHANISTAN 10 ARMENIA 10 … GERMANY 4 (Embassy)…

C&C information:

→ **10 different servers identified which exhibited confirmed malicious behavior**.
Most of these severs are located in Germany, at Hetzner Online Ag.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A6 „Red October“ attacks

IP	Active	Confirmed Malicious	Location	Hosting
141.101.239.225	Oct-12	Yes	Russia	Leadertelecom Ltd.
178.63.208.49	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
188.40.19.247	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
37.235.54.48	Oct-12	Yes	-unclear- ? Austria / UK /Spain	Edis Gmbh
78.46.173.15	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
88.198.30.44	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
88.198.85.161	Oct-12	Yes	Germany	Nuremberg Hetzner Online Ag
92.53.105.40	Oct-12	Yes	Russia	Ooo Lira-s
31.41.45.119	Nov-12	Yes	Russia	Relink Ltd
176.9.241.254	Nov-12	Yes	Germany	Nuremberg Hetzner Online Ag

“By scanning the Internet for **computers with port 40080 open**, we were able **to identify three such servers** in total, which we call **"mini-motherships“, including ONE from NUREMBERG**

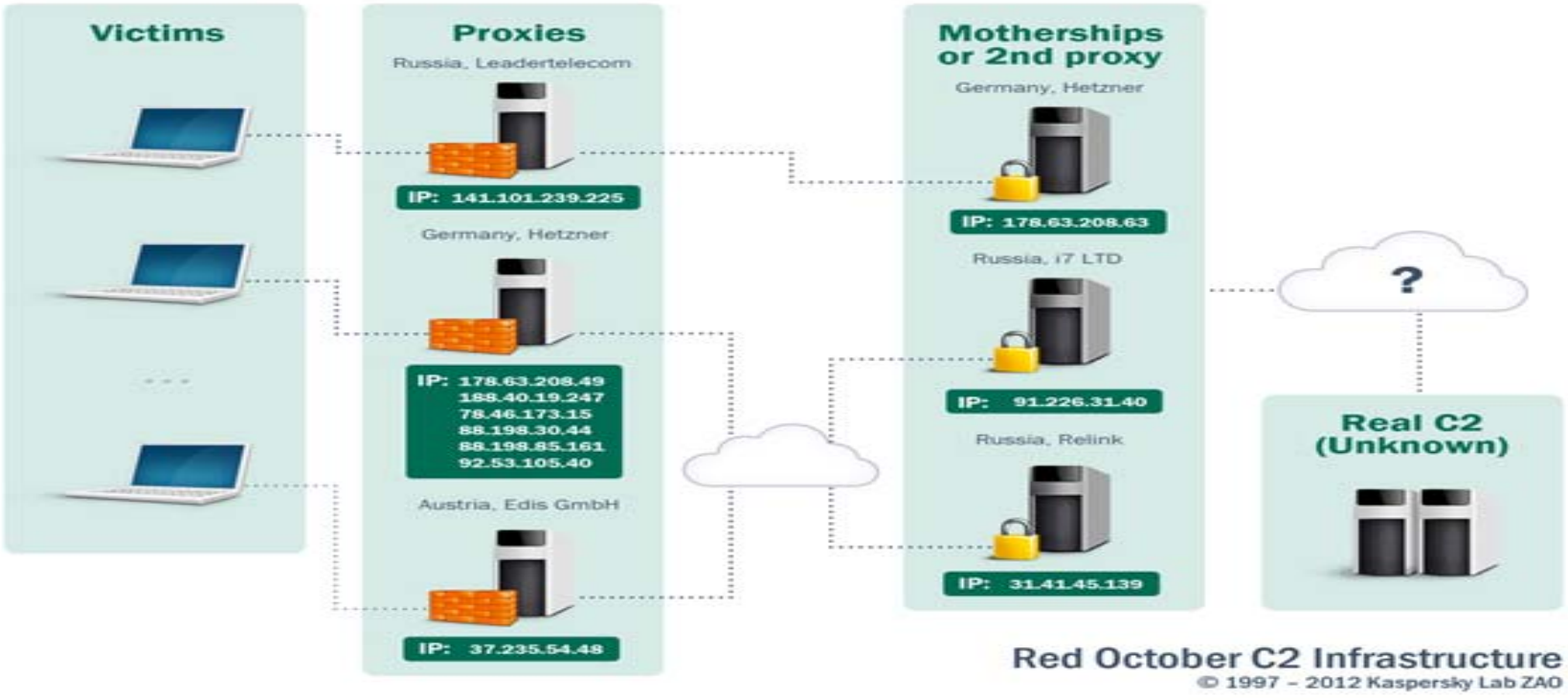
IP	Date	Confirmed malicious	Country	ISP
31.41.45.139	Oct-12	Yes, mini-mothership	Russia	Relink Ltd.
91.226.31.40	Oct-12	Yes, mini-mothership	Russia	i7 Ltd
178.63.208.63	Oct-12	Yes, mini-mothership	Germany	Nuremberg Hetzner Online Ag

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A7 „Red October“ attacks

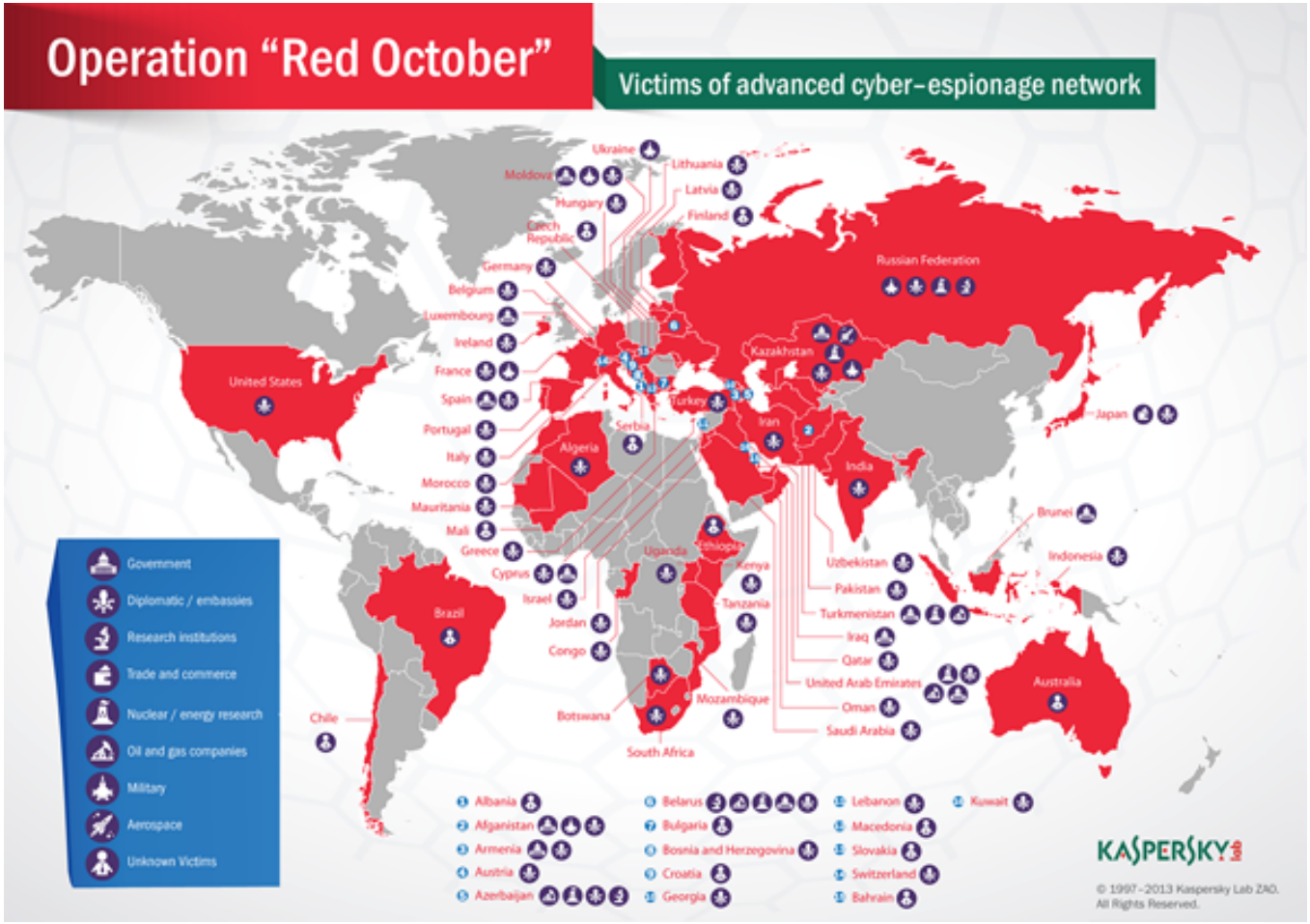
“It should be noted that the **"last modified" field** of the pages **points to the same date: Tue, 21 Feb 2012 09:00:41 GMT**. This is important and probably indicates that the three known mini-motherships are probably just proxies themselves, pointing to the same top level "mothership" server.

“Diagram of the C&C infrastructure as of November 2012:



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.3 A8 „Red October“ attacks: Worldwide Victims



2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A1 „Russian Underground 101 Attack Services“

Survey of cybercriminal underground/hacker activities:

TrendMicro 2012:

→ **Information collected from online forums (antichat.ru, xeka.ru, carding-cc.com) and services used by Russian cybercriminals, as well as articles written by hackers on their activities, the computer threats they create, and the kind of information they post on forums' shopping sites.**

→ **“The fraudsters consider the Internet a playing field. It has many vulnerable sites and a great deal of unprotected data. While “protected” data do exist, the places they are stored in can still be hacked. Some cybercriminals shared their experience in hacking; generating traffic; and writing code for Trojans, exploits, and other malware via online articles. “**

→ **Extracted from this paper: Selected list of criminal services**

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A2 „Russian Underground 101 Attack Services“

1) Crypter Prices

Basic statistical crypter	US$10–30
Stub crypter with various add-ons	US$30–80
Polymorphic crypter	US$100+

2) Dedicated Server Prices

Dedicated server	US$0.50–1
Powerful server	US$10–20

Bulletproof-hosting service/virtual dedicated server US$15–250 per month

Bulletproof-hosting service with DDoS protection,
a 1Gb Internet connection, and other extra features US$2,000 per month

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A3 „Russian Underground 101 Attack Services“

4) Pay-per-Install Service Prices

Offering download services is a widespread practice. In this **business model**, a **customer provides the malicious file for a service provider to distribute**. Download services are usually offered based on the target country.

Country	Price per 1,000 Downloads
Australia (AU)	US$300–550
Great Britain (UK)	US$220–300
Italy (IT)	US$200–350
New Zealand (NZ)	US$200–250
Spain (ES), Germany (DE), or France (FR)	US$170–250
United States (US)	US$100–150
Global mix	US$12–15
European mix	US$80
Russia (RU)	US$100

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A4 „Russian Underground 101 Attack Services“

5) Different types of DDoS attack: UDP/TCP/TCP SYN/ICMP flood attacks, Smurf attacks, ICMP flood attacks

1-day DDoS service	US$30–70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A5 „Russian Underground 101 Attack Services“

6) Spamming services: (toolkit ZeuS)

Cheap email spamming service	US$10 per 1,000,000 emails
Expensive email spamming service using a customer database	US$50–500 per 50,000–1,000,000 emails
SMS spamming service	US$3–150 per 100–10,000 text messages
ICQ spamming service	US$3–20 per 50,000–1,000,000 messages
1-hour ICQ flooding service	US$2
24-hour ICQ flooding service	US$30
Email flooding service	US$3 for 1,000 emails
1-hour call flooding service (e.g. take call center services down)	US$2–5
1-day call flooding service	US$20–50
1-week call flooding service	US$100
SMS flooding service	US$15 for 1,000 text messages
Vkontante.ru account database	US$5–10 for 500 accounts
Mail.ru address database	US$1.30–19.47 per 100–5,000 addresses
Yandex.ru address database	US$7–500 per 1,000–100,000 addresses
Skype SMS spamming tool	US$40
Email spamming/flooding tool	US$30

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A6 „Russian Underground 101 Attack Services“

7) Botnet Prices

Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per update

8) Security Software Checking Prices

1-time security software checking	US$0.15–0.20
1-week subscription	US$10
1-month subscription	US$25–30

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A7 „Russian Underground 101 Attack Services“

9) Rootkit Prices

Linux rootkit that replaces ls, find, grep, and other commands US$500

Windows rootkit that operates at the driver level and that allows the download of specially assembled drivers US$292

10) Hacking Service Prices

The **most popular email domains** cybercriminals hack in Russia are **Mail.ru**, **Yandex.ru, and Rambler.ru**. Social networks, **Vkontakte and Odnoklassniki**, are also popular targets. Services and tools for **hacking Gmail, Hotmail, and Yahoo! Mail** are also somewhat **available but at premium prices**. Offerings for **hacking ICQ, Skype, Twitter, and Facebook accounts** as well as other services are not very popular but may also be found.

Mail.ru, Yandex.ru, and Rambler.ru accounts US$16–97

Vkontakte and Odnoklassniki known accounts (no guarantees) US$97–130

Vkontakte and Odnoklassniki unknown accounts (no guarantees) US$325+

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.4 A8 „Russian Underground 101 Attack Services“

14) Exploit prices:

Exploit bundle rental:	24 hours	1 week	1 month
	US$25	US$125	US$400

Styx Sploit Pack rental (Java/AdobeAcrobat/FlashPlayer) US$3,000 per month

Phoenix Exploits Kit v. 2.3.12 (for IE6 and others) US$2,200 per domain

Less popular and less effective bundle US$25+

SQL exploit for a site with 50,000 visitors a day US$100

Exploit bundle crypting service:	1-time	1-month subscription (5 times)
	US$50	US$150

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.5 A1 Attack „APT1“ reported by Mandiant

→ During 2012 and early 2013, several **attacks on media** (US newspapers), **enterprises** (EADS, Thyssen-Krupp) **and government agencies** were **publicly reported**.

Btw: Mandiant had published a **first report in January 2010**, describing their observations about **related attacks since 2004**, which Mandiant also traced to Chinese origins.

On **February 18, 2013**, **Mandiant** (a US-based IT security company) **published a report** (with some evidence) **about the attack´s blueprint „APT1“** which was publicly quoted extensively esp. concerning the suspected Chinese origin.

→ Mandiant reported **„evidence” linking APT1 to China’s 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s** (GSD) 3rd Department (Military Cover Designator 61398)

→ According to Mandiant, **APT1 conducted “economic espionage since 2006 against 141 victims across multiple industries”, using “more than 40 APT1 malware families” and an “extensive attack infrastructure.”**

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.5 A2 Attack „APT1“ reported by Mandiant

Mandiant´s key findings:

→ “APT1 has systematically **stolen hundreds of terabytes of data** from **at least 141 organizations**.

→ “APT1 focuses on **compromising organizations across a broad range of industries in English-speaking countries**.

→ “APT1 maintains an **extensive infrastructure** of computer systems **around the world**.

→ “In **over 97%** of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, **APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language**.

→ “The size of APT1’s infrastructure implies a **large organization with at least dozens, but potentially hundreds of human operators**.

→ “In an effort to underscore that there are **actual individuals behind the keyboard**, Mandiant is revealing **three person**as that are associated with APT1 activity.

→ “Mandiant is releasing **more than 3,000 indicators** to bolster defenses against aPt1 operations.

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.5 A3 Attack „APT1“ reported by Mandiant

Mandiant´s key findings (continued):

→ “… we have analyzed the group’s **intrusions against nearly 150 victims over seven years**. … we tracked APT1 back **to four large networks in Shanghai**, two of which are allocated directly to the Pudong New Area.

→ “ … analysed … **substantial amount of APT1’s attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures**).

→ “Mandiant **continues to track dozens of APT groups around the world** …. We refer to **this group as “APT1” and it is one of more than 20 APT groups with origins in China**. APT1 is a **single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen”.**

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.5 A4 Attack „APT1“ reported by Mandiant

Mandiant´s caveat:

“However, we admit there is one other unlikely possibility:

A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398’s gates, performing tasks similar to Unit 61398’s known mission.”

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.5 A5 Attack „APT1“ reported by Mandiant: Comments

Jeffrey Carr: „Mandiant AT1 Report has Critical Analytic Flaws“:

→ **Mission area**: „Besides China, Russia, France, Israel and other countries steal IP from English-speaking organizations and their scientific priorities frequently parallel the high level topics of China´s 5 year plans.“

Speaker´s comment: Laws in China, Russia, France, Israel, USA and other countries require that security agencies „acquire“ foreign information to support their countries national development!

→ **Tools, Tactics, Procedures:** „There are over 30 nations standing up military commands which run „military-grade computer network operations.“

→ **Scale of operations:** „Many hacker groups worldwide have dozens of members. Organised crime families known to be engaging in IP theft in many parts of the world have thousands of members. Many nation states of thousands of members in their cyber militias or cyber warfare commands.“

→ **Expertise of personnell:** „Most military and intelligence agencies worldwide have English-language speaking members. Russian Security Services and Ministry of Defense recruit and train personnell in Russian universities. Many other countries have similar relationships between their military organization and their educational institutions.“

2) A Survey of Attacks on Enterprises & Industrial Infrastructures

2.5 A6 Attack „APT1“ reported by Mandiant / Comments

Jeffrey Carr: „Mandiant APT1 Report has Critical Analytic Flaws“ (cont.)

→ **Location:** „The Pudong New Area in Shanghai is China´s financial and commercial hub. In 2010 it had an estimated 5,044,430 inhabitants, of whom 2.1 million are newcomers from other provincies or cities in China. It´gross domestic product amounts to 370 billion RMB (US $53,98 billion). It has 1.3 million square meters of prime office space and a Disney theme park is under construction.

Foreign investment in Pudong New Area was over US$ 5 billion in 2009 and over 11,000 new domestic-funded enterprises were registered that year.

Based upon population size and business development in Pudong New Area, the number of options for IP net block assignments are clearly far more numerous than just belonging to Unit 61396“

3) Inherent Risks, CounterPolicies, Perspectives

3.A1 At the Origin of Cyberattacks: Inherent Risks:

A „secure IT“ would start with „secure design“, continue with „secure implementation“ and further for a „secure life cycle“

Many causes allow attackers to get criminal access to IT systems:

- **IT usage: user behaviour often risk-unaware (BYOD)**
- **Insecure IT administration: error-prone adminb overload**
- **Insecure IT maintenance (installation, updating)**
- **Insecure IT implementation: software full of flasw, esp. „exploits“**

BUT MOST ESSENTIAL:

Unsufficient (or no) security in paradigms, concepts and design of contemporary IT systemss, esp. including essential protocols:

- **e.g. communication: IP**
- **e.g. description: HTTP**
- **e.g. operating systems: performaance over security**

3) Inherent Risks, CounterPolicies, Perspectives
3.A2 At the Origin of Cyberattacks: Inherent Risks:

Example 1: IP: when communication protocols were designed, no security (identification, authentication, protection of transfer and content) was „required“, as those few communication partners knew/trusted another.

→As billions of users and processes use „IP (v4)“, criminals may misuse IP weaknesses (adress spoofing, intercepting and sniffing messages, take-over communication, sending mass mails: SPAM, dDoS etc).

Example 2: HTTP: when the physicist conceived and deisgned HTTP/HTML, he thought of classifying and accessing information in Physics libraries. Consequently, he didnot include any requirement for assuring that html presriptions followed ANY security principle (ID/AUTH etc).

→Now, billions of users and processes use HTTP/HTML without protective measures.

3) Inherent Risks, CounterPolicies, Perspectives

3.A3 At the Origin of Cyberattacks: Inherent Risks:

Example 3: Missing Security concepts in Operating systems: many security principles (e.g. controlled access to important processes and ressources in gatekeepers at 16 rings around a secure kernel) were regarded as „performance problems“ when 2 IT experts (Ritchie and Thompson) developed their minimal operating system, later known as UNIX:

MULTICS minus security = UNIX!

Regrettably, all major contempory Operating Systems (multi-billions of which control important IT operations in each second on this planet and beyond!) have NO INHERENT SECURITY as in MULTICS!

3) Inherent Risks, CounterPolicies, Perspectives

3.B1Counterpolicies: Options:

Option 1: Secure I&C Technologies: Unfortunately, this is an „academic“ advice as some such systems work under HEAVY restrictions. Indeed, NO such systems are available for daily work !

Option 2: At least: reduce risks by avoiding highly insecure and attack-provocing IT technologies such as: smartphones (BYoD), public clouds, ..

and use filters and monitors (e.g. Intrusion Detection systems)

BTW: NEVER PATCH a running system without extensive prior tests!

Option 3: Learn to live/work under threats. Save carefully current valuable work, use cryptomethods to protect valuable information. In case of serious attacks, close your system against any network communication. Be always prepared for immediate recovery.

Option 3A: Some experts (esp. in governments) believe that „attack is the best protection“. BUT: counterattackers are NOT BETTER than attackers!

3) Inherent Risks, CounterPolicies, Perspectives

3.3 Perspectives:

With the deployment of Cloud services esp. in critical applications, such as smart grids for electricity, logistics, traffic control, financial transactions and control of distributed production, both the probability of new , serios weaknesses and related attacks as well as the impact of outages will UNAVOIDIBLY grow!

Moreover, the tendency to interconnected operation and work as well as the developing tendency towards a „ShareConomy“ with the superior goal of sharing of as many kinds of ressources and processes as possible will enlarge risks and damages significantly.

In the absence of Secure/Safe systems, and with further growing complexity, there is no hope to contain the risks from CyberSpace.

DONE!

Thank you for your interest!

Any questions, PLS?