

CYBER SECURITY FOR CRITICAL INFRASTRUCTURE

Or: “how to break into a nuclear
power station for fun & profit”

Dr. Richard Gold (CSSA)

<richard.gold@gmail.com>

(@Cisco, but representing myself)

<https://twitter.com/Phreaklets>

DEFINITION OF TERMS

- ▶ Cyber Security
 - ▶ As opposed to physical security like gates, fences, locks, guards, etc.
 - ▶ Network & host security
- ▶ Critical infrastructure
 - ▶ Power grid
 - ▶ Water supply
 - ▶ Oil & Gas pipelines
 - ▶ Chemical factories (some)
 - ▶ Refineries
- ▶ IT networks (aka Enterprise networks: Windows, Linux, etc.)
- ▶ ICS networks (aka SCADA systems: PLCs, RTUs, etc.)

CRITICAL INFRASTRUCTURES



WHAT MAKES CS FOR CI NOTEWORTHY?

- ▶ In IT networks, C-I-A is the norm in terms of priority
 1. Confidentiality
 2. Integrity
 3. Availability
- ▶ In ICS networks, it's reversed to A-I-C
 1. Availability
 2. Integrity
 3. Confidentiality
- ▶ Loosely translated: “nobody cares about cyber security” 😊

IT GETS WORSE...

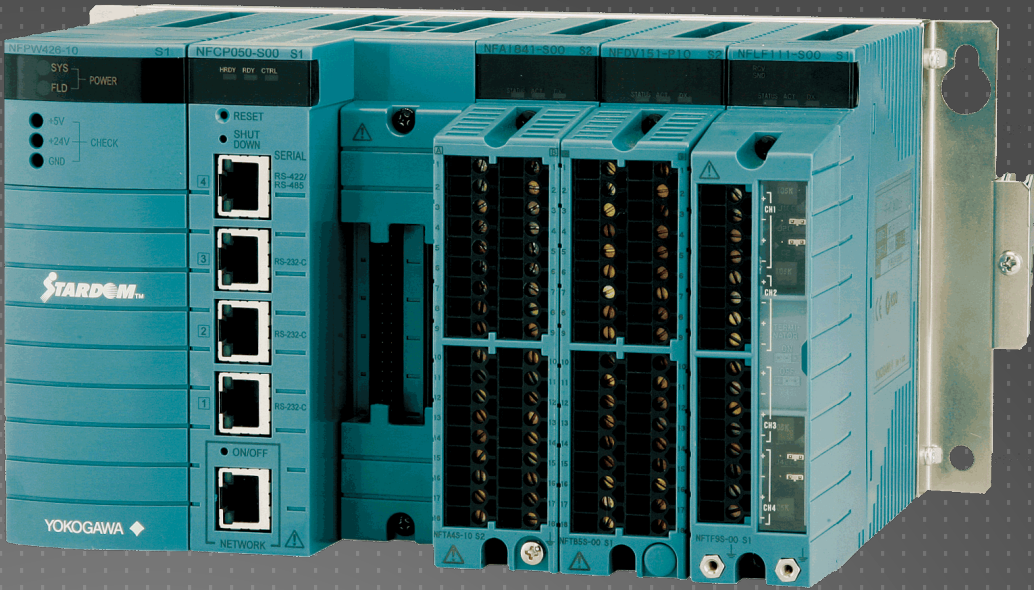
- ▶ “What’s a patch?”
 - ▶ Dedicated hardware (PLCs, RTUs, etc.) & OS are pretty esoteric compared to W/LinTel
 - ▶ Until recently patches weren’t even available...
 - ▶ ...even if they are available, typically not applied (~30% coverage)
 - ▶ If Desktop OS required (HMI) often locked to a specific OS & patch level (WinXP SP1!)
- ▶ “What’s a firewall/IDS/AV?”
 - ▶ Typical argument against using standard IT tools is that ICS networks are “airgapped”
 - ▶ Most standard IT security solutions have no idea about ICS vulnerabilities
- ▶ “What’s protocol security?”
 - ▶ Most ICS field protocols (Modbus, DNP3, IEC 61850, IEC 104, etc.) were originally serial protocols wrangled over TCP/IP
 - ▶ No notion of authentication, authorization, but is being retrofitted...

A MENAGERIE OF DEVICES: PLC, RTU, IED, ...

YOKUGAWA



SIEMENS



ABB



OUR ICS SYSTEM IS AIRGAPPED!



AIRGAPS AND UNICORNS

- ▶ “What’s perimeter security?”
- ▶ Airgaps possible in the past, not realistic anymore
- ▶ How do you get the data out of the ICS system into your ERP?
- ▶ Transfer of updates?
- ▶ Many attack vectors:
 - ▶ USB sticks (Stuxnet)
 - ▶ Ultrasonic/acoustic (BadBIOS?)
 - ▶ Modems (default password, if there is one at all)
 - ▶ Ethernet connected to IT network (abandoned or forgotten)
 - ▶ Proprietary wireless links vulnerable due to bad crypto (RFComms @ S4xI3)
 - ▶ Wifi (WEP networks still abound)

ASIDE: WIFI SECURITY

- ▶ WPA2 PSK
 - ▶ Capture the 4 way handshake with aircrack-ng
 - ▶ Feed it into (GPU enabled) HashCat and a good wordlist
- ▶ WPA2 Enterprise
 - ▶ Create a fake AP with hostapd
 - ▶ Capture credentials with FreeRADIUS-WPE
 - ▶ Feed into John the Ripper (many cores) and a good wordlist
 - ▶ Mobile devices in particular do the certificate handling insecurely (Defcon 21)
- ▶ BYOD policies can really help you in this area
- ▶ Lather, rinse, repeat...

FEATURES NOT EXPLOITS

- ▶ Many attacks use exploits, like 0days, to break into a system
 - ▶ Also, stolen credentials
- ▶ These can be patched with a code fix within a reasonable timeframe
- ▶ Going after features, typically exploiting trust, is much more potent
- ▶ Much harder to defend against, require architectural or cultural changes
- ▶ Examples are essential services that require privileged access
 - ▶ Bug reporting system
 - ▶ Log files
 - ▶ Customer billing system
 - ▶ Compliance systems
 - ▶ Enterprise Resource Planning systems

SO YOU WANT TO PWN A NUCLEAR POWER STATION?

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering your tracks

Compromising the supply chain/partner sites are also good choices!

Most real-world attacks are cyber espionage-related, not sabotage like Stuxnet...

STUXNET (V0.5 & V1)

י כ ו ת ר ו מ ת י ד כ כ י א ל פ נ ו י ה ו ה א ל ה י כ ת א
ה ו א י נ נ ב ה מ ת ב ו נ ה ל ו ח כ מ ו י ש כ י ל ו ז א ת י ב
כ ר א ר ש ב ע ו י ק מ א ב י מ ל כ פ י כ ל ש ר צ ב א ו ו י
י ב א א ל י ה ו ת ה ר ל ו ו ת ק מ ו ת ל כ ו ת ס ר
ש פ י מ ו י ע ש ו ג מ ה מ ח ר ט מ י מ צ ר י מ ב ל
ק ר ס י מ ו ה ב א ת ש מ ה מ ב י ת ל פ ר כ ת א ת א
ה ו ה ב י א א ת ק ר ב נ ו א ש ר ח ט ע ש ר ת ה
ע ת ת ס פ ר ו ח מ ש י מ י ו ס ו ה ק ר ב ת מ מ נ ח
א ת ה ש ו מ י מ י מ ע ת ה נ פ ש ו י ב ש ה א י נ כ
ג ש ו ה ק ר ב ת מ ע ל ה ל י ה ו ה ר י ח נ י ח ח פ
פ ל ל פ נ י ה ו ה א ת א ר ב ע י מ ה י ו מ ו א ת
ה ו ב ק צ פ ג ד ל ו י ש ל כ מ א ל א ר צ א ח ר ת כ
ו י ב א ו ש נ י ה מ ל א כ י מ ד מ ה ב ע ר ב ו ל
ע ק ב ב נ י ו ר א ל ה ת ל ד ו ת ע ש ו ה ו א א ד ו
ב ה כ ב ש ר ו ה י א מ ל א י א מ י נ ו ל כ ו ל
ו א ו ת ה ו י א ת ה כ נ ע נ י ו א ת ה ח ת י מ ל פ נ י כ ל א
א ש ר ע ל ה א ש א ש ר ע ל ה מ ז ב ח ו ה ר ב ו ה כ ר ע י מ
מ ו ר נ ת ת י א ת פ נ י ב נ פ ש ה ה ו ה ה כ ר ת י א ת ו מ ק
ה ו ש ל מ י מ ע ש ר י מ ו א ר ב ה פ ר י מ א י ל מ ש ש י מ
נ ה ו א פ ר י מ ב נ י מ נ ה ל מ כ י ר מ ש פ ח ת ה מ כ י
ר י ב י ד ו ז ק ה ו י נ י ה ו ה א ו ת ו מ פ ת י מ ג ד
ה י כ מ ר ל ע ש ו ת א ת כ ל מ צ ו ת י ו ו ח ק ת י ו א ש
ה ד ה ו ה א ל י ו ל א מ ר ל א י י ר ש כ ז ה כ י א מ א
י ג מ א ת ה ש ל י ש י ג מ א ת כ ל ה ה ל כ י מ א ח ר י ה ע ד
נ י ס ו ת ו ל א מ ר כ ה ת א מ ר ו ל י ו פ א נ א ש א נ א פ



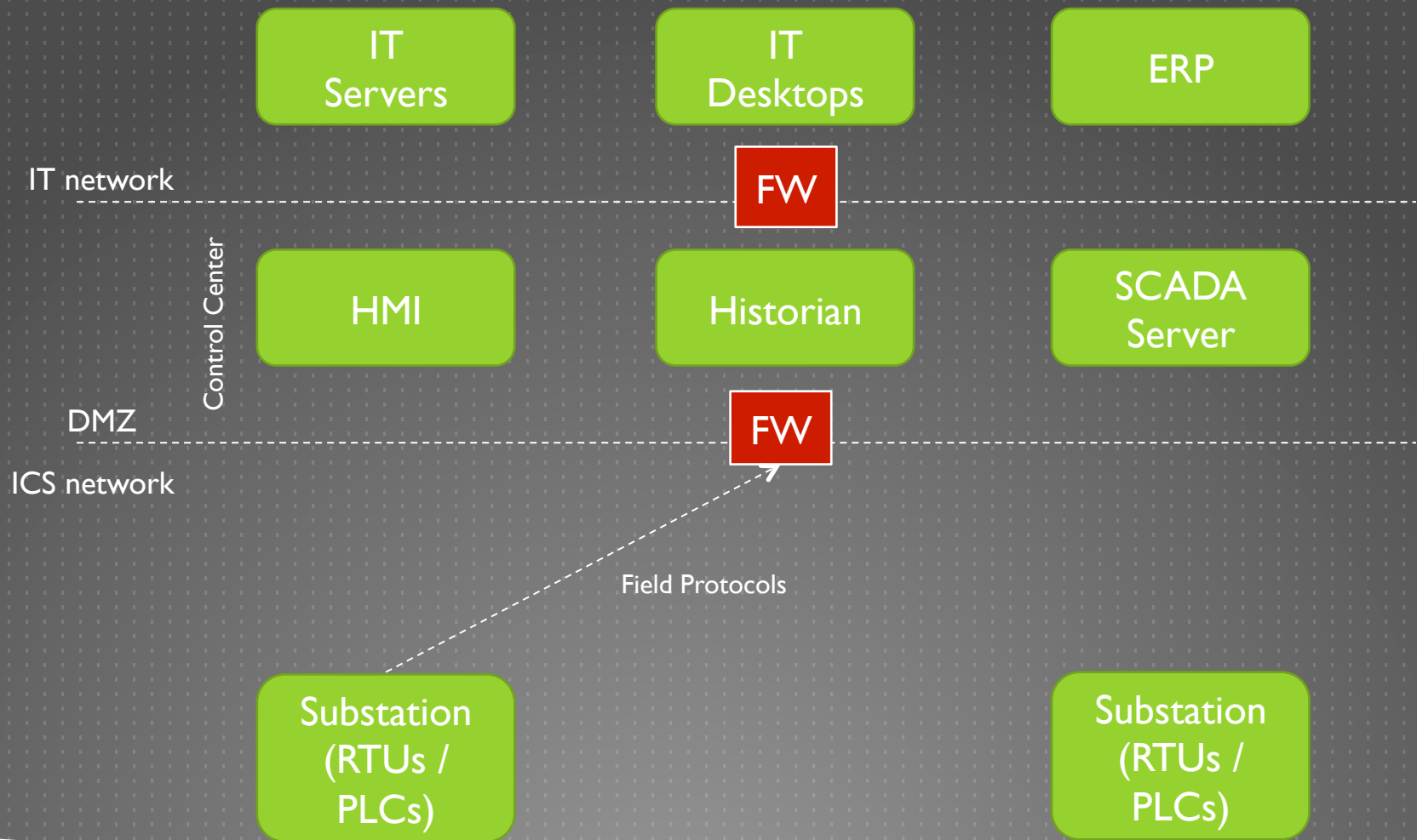
STUXNET VIRUS (WORM)
ATTACK ON IRAN



Term	Translation	Skip	Start	End
סְטֻקְסֵט	STUXNET	-120048	Genesis Ch 50 V 17 Letter 11	Exodus Ch 7 V 11 Letter 37
וִירֻס	Virus	-30013	Deuteronomy Ch 29 V 27 Letter 33	Leviticus Ch 23 V 16 Letter 19
אִירָן	Iran	30009	Exodus Ch 26 V 33 Letter 41	Numbers Ch 11 V 6 Letter 8
מְחַשֵּׁב	Computer	30010	Numbers Ch 26 V 28 Letter 24	Genesis Ch 15 V 4 Letter 6
תְּשֻׁעָה	(5)771/2010	-30010	-Deuteronomy Ch 6 V 22 Letter 3	Leviticus Ch 20 V 6 Letter 56
חֲסֵמֶלֶי	electric	30013	Numbers Ch 7 V 88 Letter 9	Genesis Ch 15 V 4 Letter 8
אָטוֹם	Atom	-60027	Leviticus Ch 5 V 11 Letter 51	Deuteronomy Ch 12 V 18 Letter 4
חֲרֻטְמֵי	Secret Arts	1	Exodus Ch 7 V 11 Letter 35	Exodus Ch 7 V 11 Letter 39

The ELS reference is 30012 characters between rows.
The matrix starts at Deuteronomy Ch 12 V 17 Letter 70 and ends at Genesis Ch 50 V 17 Letter 20.
The matrix spans 720318 characters of the surface text.
The matrix has 25 rows, is 30 columns wide and contains a total of 750 characters.

TYPICAL POWER GRID LAYOUT



RECONNAISSANCE

- ▶ Google
 - ▶ Huge amounts of OSINT information widely available
 - ▶ Brochures, presentations, white papers, manuals, ...
- ▶ Social networks (linkedin, facebook)
 - ▶ Who works where & does what
- ▶ Maltego
 - ▶ Transforms to discover & correlate emails, phone numbers, network infrastructure
- ▶ Foca
 - ▶ Search for networks/hosts, documents, analyze metadata
- ▶ Shodan HQ
 - ▶ Searches for Internet-connected machines, captures banners
 - ▶ ICS equipment like Modbus/RTUs & bridges routinely found

RECONNAISSANCE

The screenshot shows the FOCA Free 3.2 application window. The left sidebar displays a tree view of the 'Test Project' with categories like Network, Clients, Servers, Domains, Roles, Vulnerabilities, Metadata, Documents (1/140), and Metadata Summary. The main area features a search engine selection panel (Google, Bing, Exalead) and an 'Extensions' list (doc, ppt, pps, xls, docx, pptx, ppsx, xlsx, sxw, sxc, sxi, odt). Below this is a table of search results with columns for Id, Type, URL, Download status, Download Date, Size, and Actions. A context menu is open over the table, showing options like Download, Download All, Stop All Downloads, Delete, Delete All, Extract Metadata, Extract All Metadata, and Analyze Metadata.

Id	Type	URL	Download	Download Date	Size	Actions
0	pptx	\\psf\Home\Desktop\DigitalLifeDeck.pptx	●	10/27/2012 1:09:31...	2.94 MB	Download
1	doc	http://www.wwt.com/products_services/documents/CC...	●	10/27/2012 1:09:32...	384 KB	Download All
2	doc	http://www.wwt.com/missouri/docs/eep.doc	●	10/27/2012 1:09:32...	28.5 KB	Stop All Downloads
3	doc	http://www.wwt.com/products_services/documents/CC...	●	10/27/2012 1:09:33...	397 KB	Delete
4	doc	http://www.wwt.com/products_services/documents/Go...	●	10/27/2012 1:09:36...	364.5 KB	Delete All
5	doc	http://www.wwt.com/products_services/documents/DC...	●	10/27/2012 1:09:34...	365 KB	Extract Metadata
6	doc	https://www.wwt.com/p...ents/C...	●	10/27/2012 1:09:35...	366.5 KB	Extract All Metadata
7	xls	http://www.wwt.com/markets/federal/NIH1E.xls	●	10/27/2012 1:09:36...	120.5 KB	Analyze Metadata
8	xls	http://www.wwt.com/federal/images/NIH2.xls	●	10/27/2012 1:09:37...	370.5 KB	
9	xls	http://www.wwt.com/markets/federal/NIH3.xls	●	10/27/2012 1:09:37...	104 KB	
10	xls	http://www.wwt.com/federal/images/NIH1C.xls	●	10/27/2012 1:09:39...	636.5 KB	

Services	
HTTP	273
HTTP Alternate	4
NetBIOS	2
Top Countries	
Japan	116
Germany	48
Czech Republic	47

IRMC S2@iRMCA825EB - ServerView®; iRMC S2 Redirecting ... (Fw: 5.09A/SDR: 3.09)
 182.48.26.66
 SAKURA Internet Inc.
 Added on 29.09.2013
 ● Osaka

HTTP/1.0 302 Found
 Date: Sun, 29 Sep 2013 20:05:16 GMT
 Server: ServerView Remote Management iRMC S2 Webserver
 Connection: close
 Cache-Control: no-cache
 Pragma: no-cache
 Location: https://182.48.26.66:8929/
 Content-Type: text/html
 Transfer-Encoding: chunked

SCANNING

- ▶ Nmap! 😊
 - ▶ Look for ICS protocols connected to the Internet
 - ▶ Port 502 for Modbus, Port 20000 for DNP3, etc.
 - ▶ Look for exposed Windows services (CIFS/SMB, etc.)
 - ▶ Look for vulnerable network services
 - ▶ Telnet, SNMP, (T)FTP,...
- ▶ OpenVAS, Nessus, etc.
 - ▶ Vulnerability scanners with some ICS vulns
 - ▶ Look for HMIs or PLCs with default passwords

OPENVAS / GSD

Greenbone Security Desktop

File Task View Settings Extras Help

Dashboard

Vulnerabilities

High: 106
Medium: 27
Low: 47

Scan Tasks

High: 2
Medium: 2
Low: 1
None: 1

Top 5 Tasks

- Deep Scan Windows 105
- Conficker Search 1
- Nightly Scan 1
- Quick Scan Linux 1
- IT-Grundschutz Scan 8

Trends

0 0 2 0 0 4

Task Overview

Total	6
Running	0
Progress	1
Done	5
New	0
Error	0

Resources Overview

Targets	14
Scan Configs	8
Schedules	1
Escalators	2
Credentials	2
Agents	0
Overrides	0
Notes	0

Performance

Size: Width: 697 px Height: 268 px

System load

1 min	0.00	Min.	0.18	Avg.	1.01	Max.	0.99	Last
5 min	0.00	Min.	0.17	Avg.	0.46	Max.	0.15	Last
15 min	0.00	Min.	0.13	Avg.	0.30	Max.	0.13	Last

Greenbone Security Manager

Tasks

Name	Status	Reports	First	Last	Threat	Trend
Quick Scan Linux	Done	2	Jun 15 2010	Jun 15 2010	Medium	→
Conficker Search	Done	1	Jun 15 2010	Jun 15 2010	High	
IT-Grundschutz Scan	Done	1	Jun 15 2010	Jun 15 2010	Low	
Deep Scan Linux	Stopped at 23%	0			None	
Nightly Scan	Done	102	Jun 16 2010	Apr 5 2011	Medium	→
Deep Scan Windows	Done	105	Jun 15 2010	Jun 15 2010	High	→

Report Deep Scan Windows (Tue Jun 15 09:12:22 2010)

Results 1 - 100 of 130

Filtered results 1-100 as CPE

High (CVSS: 9.3)
NVT: Microsoft Windows Indeo Codec Multiple Vulnerabilities (OID: 1.3.6.1.4.1.25623)

[Add Note](#)
[Add Override](#)

Overview: This host is insatlled with Microsoft Windows Indeo codec and p...
Multiple Vulnerability
Vulnerability Insight:
The multiple Flaws are due to:
- An error in the Indeo4l codec when processing a specific size within the 'movi' record of a IV4l stream can be exploited to cause a heap-based bu...
- An error in the Indeo4l codec when decompressing a video stream can be exploited to cause a stack-based buffer overflow.

Tasks Deep Scan Windows

- New
- Delete
- Start
- Stop
- Details
- Refresh

Tasks Targets

Logged in as: demo

Refresh Interval: manual

GAINING ACCESS

- ▶ **Direct approach**
 - ▶ Fire up Metasploit and go after the discovered vulns directly over the Internet
 - ▶ Exploits available for both ICS & IT systems
- ▶ **Indirect approach**
 - ▶ (Spear) Phishing campaign based on intel gathered from social network analysis
 - ▶ Fake email from colleague or collaborator or boss
 - ▶ Malicious link, watering hole attack, PDF or Office exploit, etc. targeting systems administrators or engineers
 - ▶ Once in the IT network, you'll be able to find a way into the ICS network somehow...
- ▶ **Semi-direct**
 - ▶ Get in range of a target wireless network and go in that way

GAINING ACCESS

```
msf > search scada  
[*] Searching loaded modules for pattern 'scada'...
```

Exploits

=====

Name	Disclosure Date	Rank	Description
windows/scada/realwin	2008-09-26	great	DATA RealWin SCADA Server Buffer Overflow
windows/scada/realwin_scpc_initialize	2010-10-15	great	DATA RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow
windows/scada/realwin_scpc_initialize_rf	2010-10-15	great	DATA RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow

```
msf > █
```

Results

Just over 25% of the highly targeted recipients fell victim to the spear phishing and clicked on the link. If their browsers were missing security patches or the attacker had an 0-day, the computer would be compromised. An attacker could load a keystroke logger and or other programs and gain whatever access that computer or user had to the ICS.

The money slide in the presentation was the job titles of those that clicked on the link:

- Control System Supervisor
- Automation Technician
- Equipment Diagnostics Lead
- Instrument Technician
- Senior VP of Operations and Maintenance

MAINTAINING ACCESS

- ▶ Remote Access Trojan (RAT) or Botnet
 - ▶ Many available, some open source(!)
 - ▶ Poison Ivy, Zeus, Andorrat
 - ▶ Lots of functionality like mic & webcam access, document retrieval
 - ▶ How do you extract GBs of data without anyone noticing?
 - ▶ How do you process GBs of mostly worthless data?
- ▶ Install your own backdoor
 - ▶ SSH on a high port on some abandoned Linux box
 - ▶ Man in the browser (BEEF project)
 - ▶ DNS tunnelling? 😊

MAINTAINING ACCESS

The screenshot displays a remote control interface with several components:

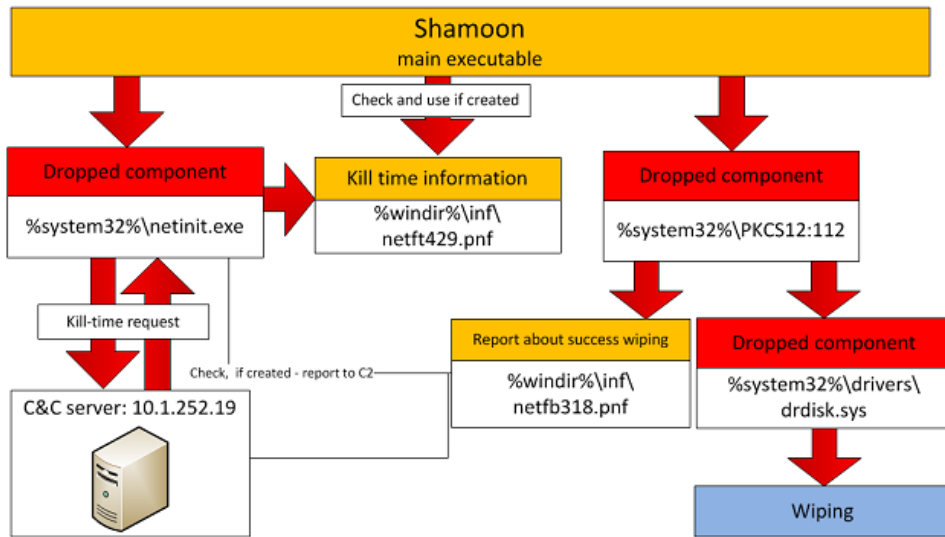
- Calendar:** A calendar for the year 2012, showing the month of April. The date 20th is highlighted.
- Web Browser:** A window titled "Hotmail" showing an email from "iexplore.exe" with the subject "Sign in to Yahoo!". The email content includes the text "Dear Mazen," and a request to change a return date from 22nd April to 26 April or 27th.
- Hooked Browsers:** A tool window showing a list of hooked browsers. The "Online Browsers" section is expanded, showing a folder for "192.168.175.1" containing a browser instance.
- Command Window:** A window titled "Getting Started" with tabs for "Details", "Logs", "Commands", and "Requester". The "Commands" tab is active, showing a list of modules with columns for "id" and "date".

The interface also includes a sidebar with various management tools such as "Information", "Managers", "Surveillance", "Network", and "Tools".

COVERING YOUR TRACKS

- ▶ Log doctoring
 - ▶ Both desktop & server OS types
 - ▶ Doctor the logs of the ICS hardware?
 - ▶ For advanced agents only!
- ▶ Nuclear option
 - ▶ Wipe the MBR (Shamoon attack on Aramco)
 - ▶ Wipe the MBR & disk volumes (South Korea attacks)

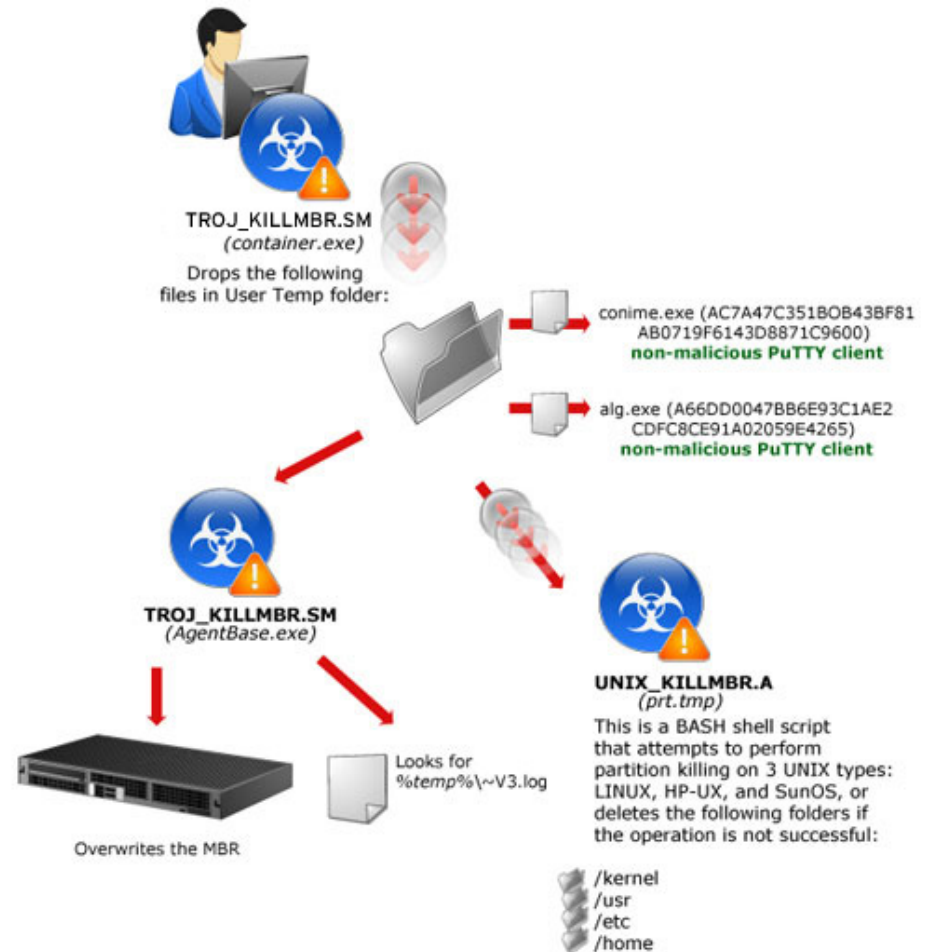
COVERING YOUR TRACKS



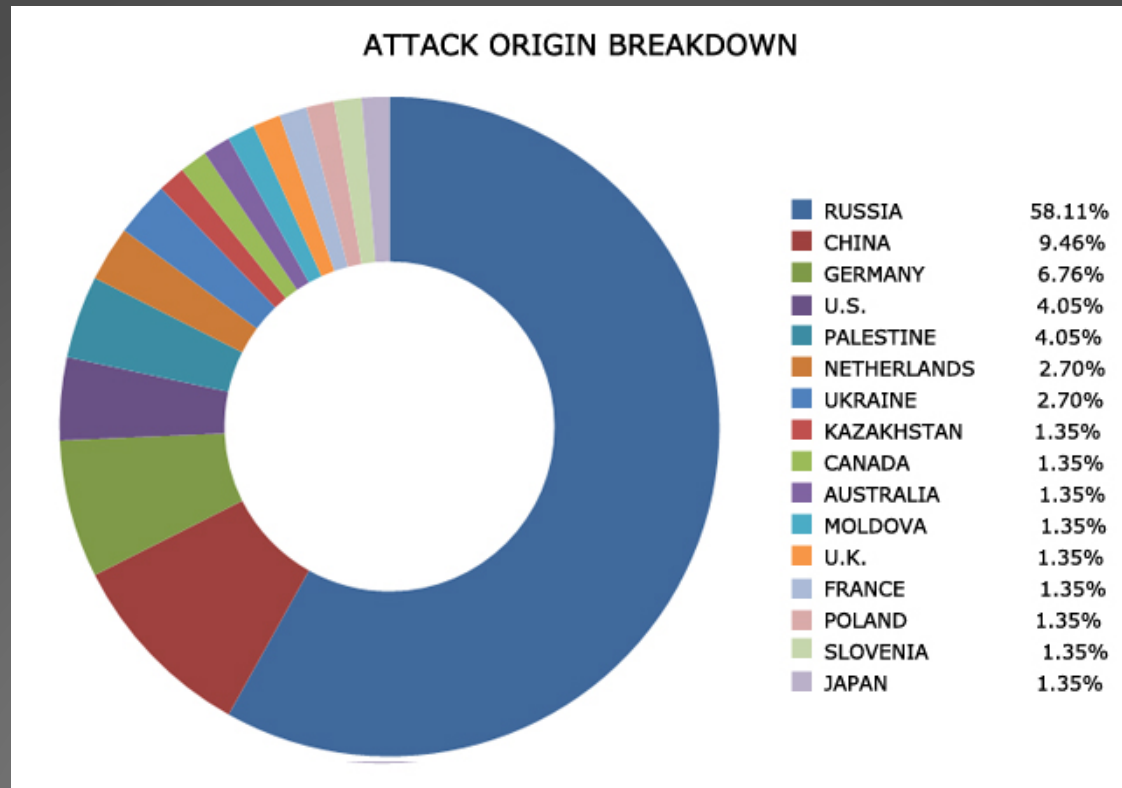
© 2012 Kaspersky Lab ZAO. All Rights Reserved.

Shamoon

South Korean Wiper



ARE ATTACKS AGAINST CI FOR REAL?



The SCADA that cried Wolf

IS THERE ANY HOPE? 😊

- ▶ After Stuxnet, the interest in CS for CI increased dramatically (from 0!)
- ▶ Companies offer DPI firewalls, “bump in the wire” & data diodes for ICS
 - ▶ Industrial Defender, Tofino
- ▶ ICS honeypots
 - ▶ Digital Bond, conpot
 - ▶ Currently deployed as part of Peer Energy Cloud project
- ▶ ICS signatures for Snort IDS available
- ▶ Pen-testing firms offer ICS-specific services
- ▶ Standards like NERC CIP mandate CS, ICS-CERT supports these standards
- ▶ Lots (but not all!) of ICS systems are at least in private networks

CONCLUSIONS

- ▶ CS for CI was typically neglected due to radically different priorities for ICS
 - ▶ “Do you have a spare hot swap nuclear power station to test that patch on?”
- ▶ Stuxnet was a big wake up call but it was more a “movie plot threat” for 99.9% of ICS operators, current attacks focus more on industrial espionage
- ▶ No patches, no patches applied, no technical compensating controls, insecure protocols (if you can connect, you can pwn), no security engineering mindset
- ▶ Breaking in to an ICS network is relatively straightforward due to the plethora of options available to the attacker
 - ▶ Currently very few attacks due to obscure nature of ICS, but don't expect this to last...
- ▶ Situation is improving but sloooooooooowly...