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" ☺

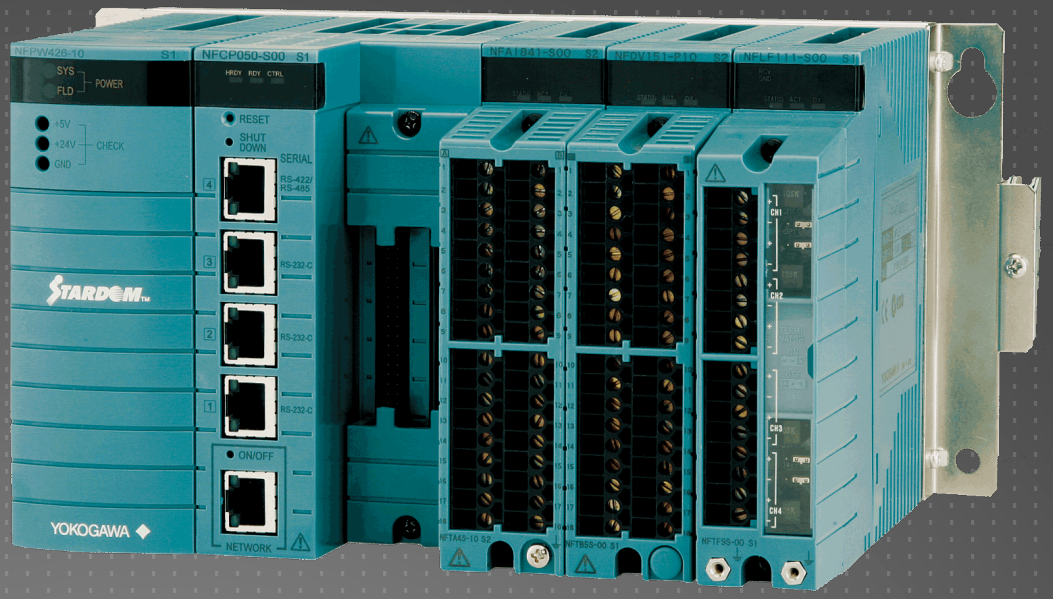
IT GETS WORSE…

- "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, …

SIEMENS

YOKUGAWA



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 @ S4x13)
  - 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 particularly 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

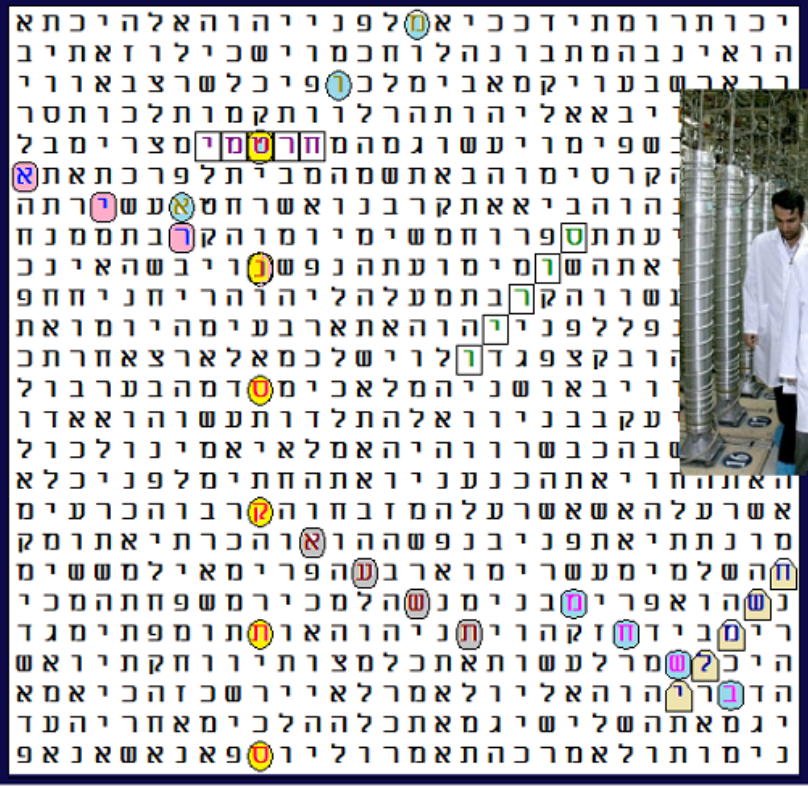
SO YOU WANT TO PWN A NUCLEAR POWER STATION?

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)

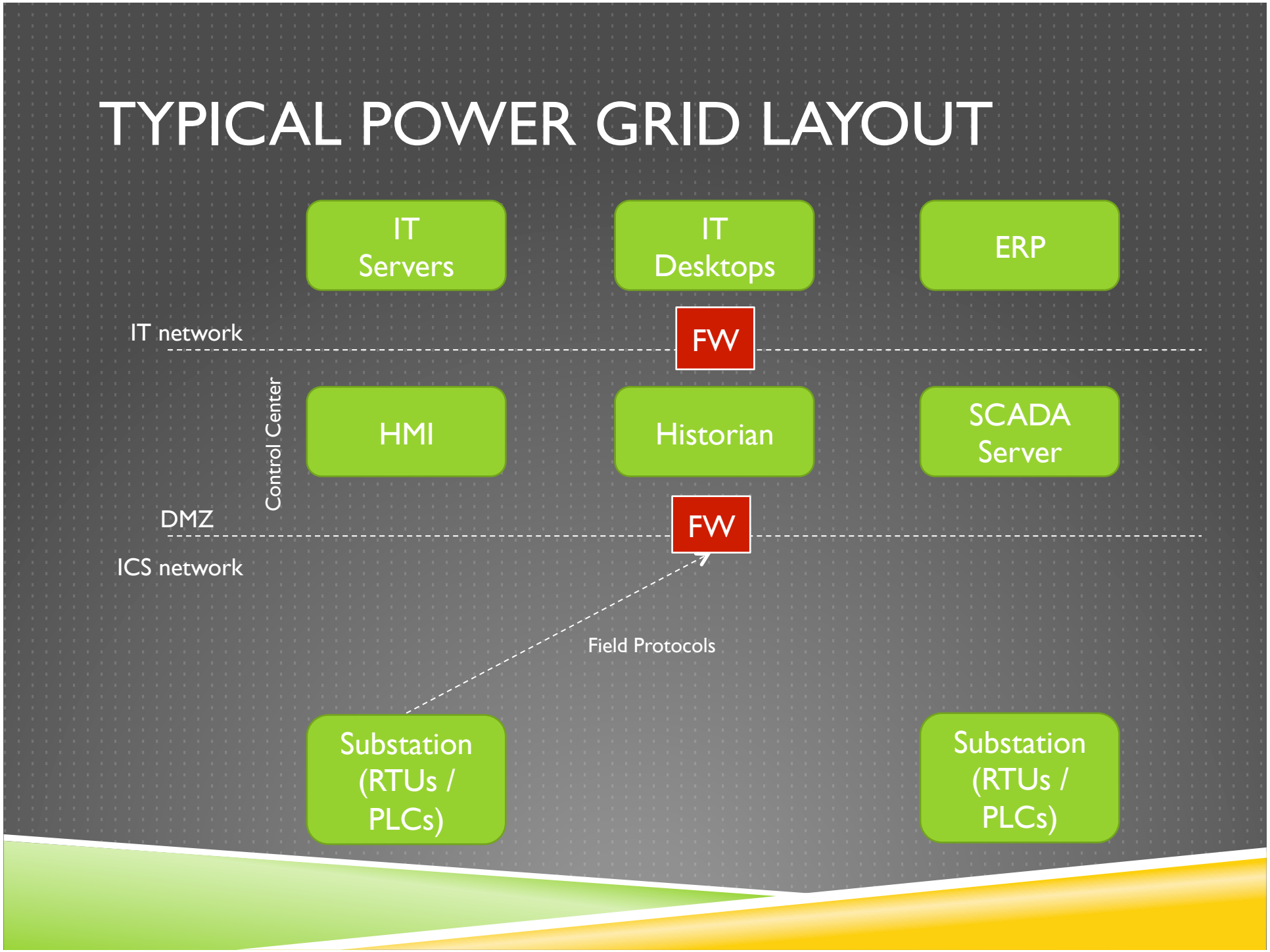


STUXNET VIRUS (WORM) ATTACK ON IRAN

Term	Translation	Skip	Start	End
סתקסנט	STUXNET	-120048	Genesis Ch 50 V 17 Letter 11	Exodus Ch 7 V 11 Letter 37
וירוס	Virus	-30013	Deuteronomy Ch 29 V 27 Letter 33	Leviticus Ch 23 V 16 Letter 19
אירן	Iran	30009	Exodus Ch 26 V 33 Letter 41	Numbers Ch 11 V 6 Letter 8
מחשב	Computer	30010	Numbers Ch 26 V 28 Letter 24	Genesis Ch 15 V 4 Letter 6
תשעא	(5)771/2010	-30010	-Deuteronomy Ch 6 V 22 Letter 3	Leviticus Ch 20 V 6 Letter 56
חשמלי	electric	30013	Numbers Ch 7 V 88 Letter 9	Genesis Ch 15 V 4 Letter 8
אטום	Atom	-60027	Leviticus Ch 5 V 11 Letter 51	Deuteronomy Ch 12 V 18 Letter 4
חרטמי	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.

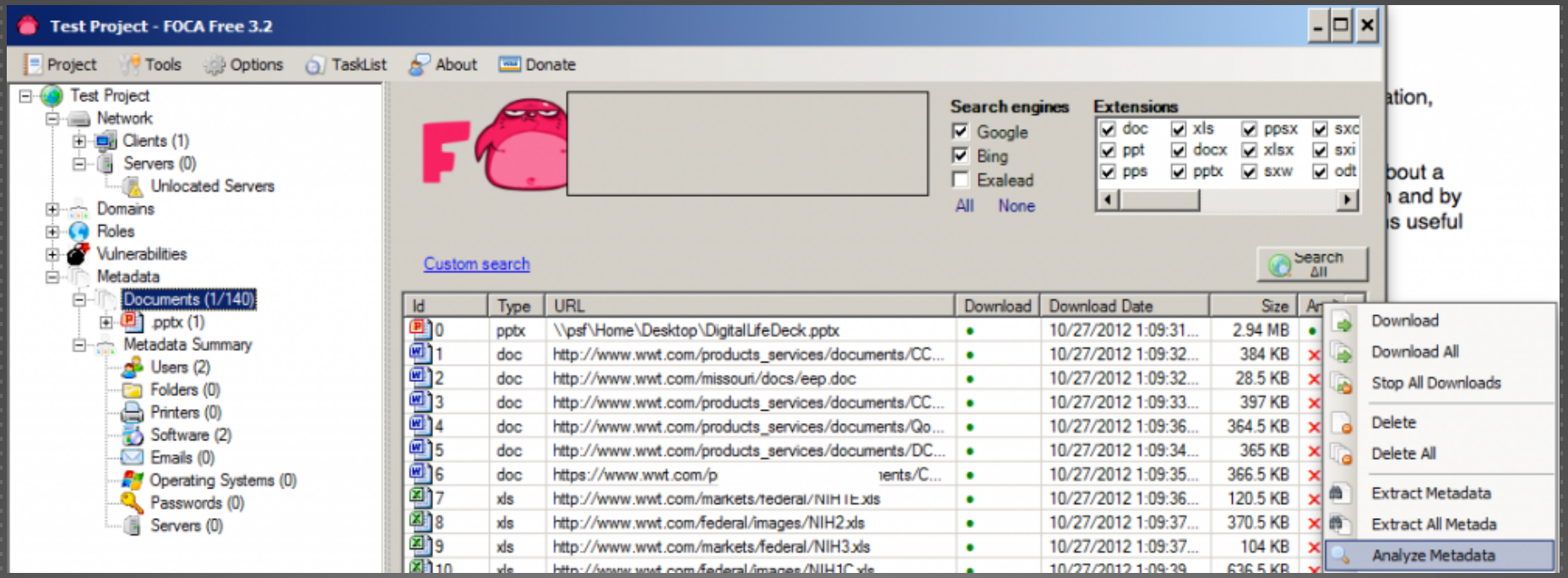
TYPICAL POWER GRID LAYOUT

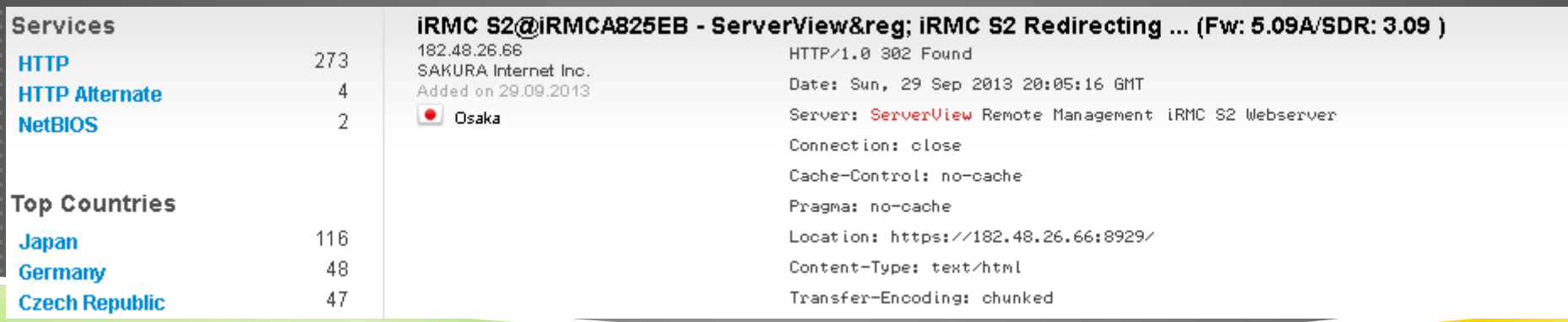


RECONNAISSANCE

- 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

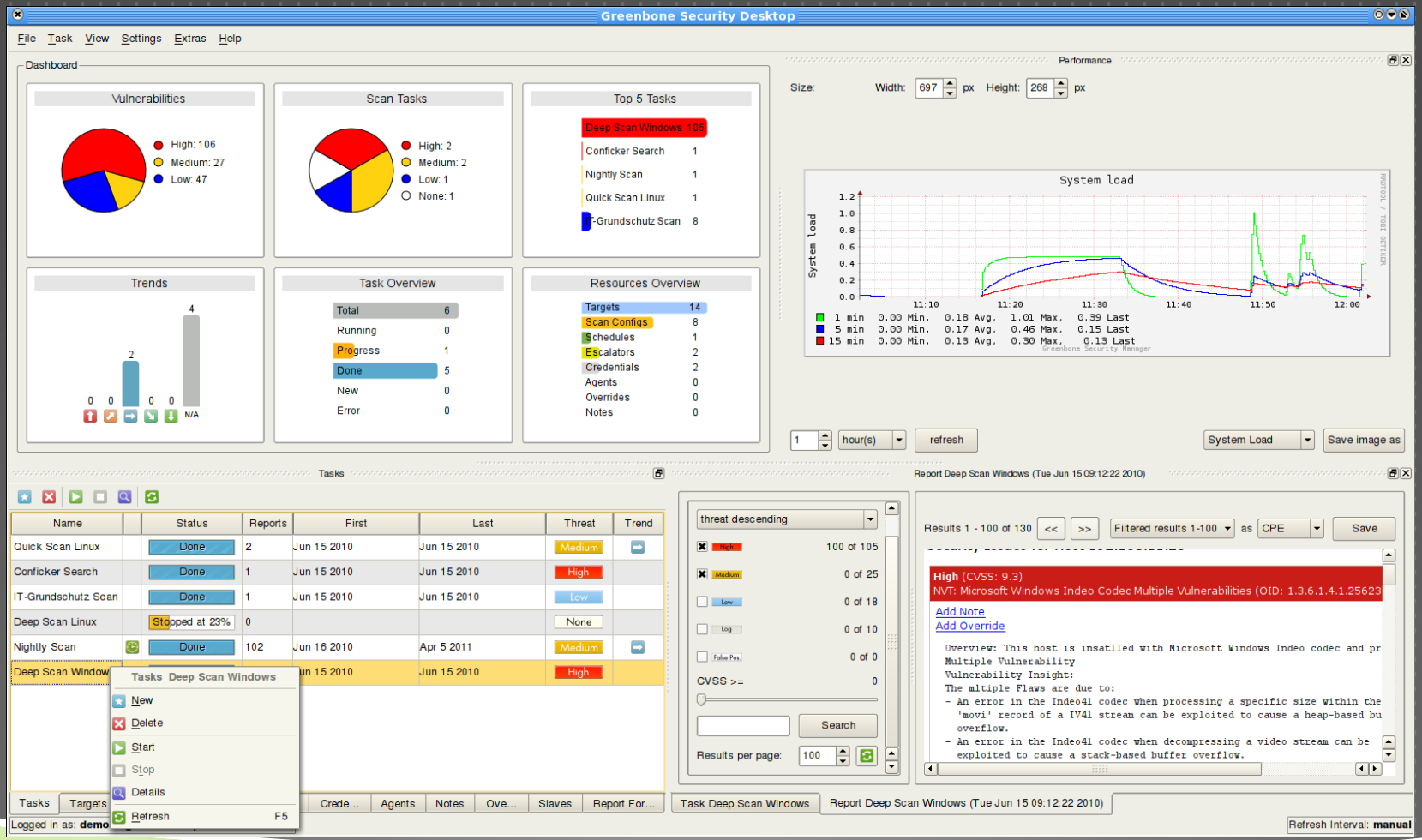




SCANNING

- 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
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, 0.39 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
refresh
System Load
Save image as
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 Window Jun 15 2010 Jun 15 2010 High
Tasks Deep Scan Windows
New
Delete
Start
Stop
Details
Refresh F5
Report Deep Scan Windows (Tue Jun 15 09:12:22 2010)
threat descending
100 of 105
0 of 25
0 of 18
0 of 10
0 of 0
CVSS >= 0
Search
Results per page: 100
Results 1 - 100 of 130
Filtered results 1-100
as CPE
Save
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 pr
Multiple Vulnerability
Vulnerability Insight:
The mltiple Flaws are due to:
- An error in the Indeo41 codec when processing a specific size within the
'movi' record of a IV41 stream can be exploited to cause a heap-based bu
overflow.
- An error in the Indeo41 codec when decompressing a video stream can be
exploited to cause a stack-based buffer overflow.
Tasks Targets Crede... Agents Notes Ove... Slaves Report For...
Task Deep Scan Windows
Report Deep Scan Windows (Tue Jun 15 09:12:22 2010)
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  DATAC RealWin SCADA Server Buffer Overflow
   windows/scada/realwin_scpc_initialize 2010-10-15       great  DATAC RealWin SCADA Server SCPC_SCPC_INITIALIZE Buffer Overflow
   windows/scada/realwin_scpc_initialize_rf  2010-10-15       great  DATAC 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.

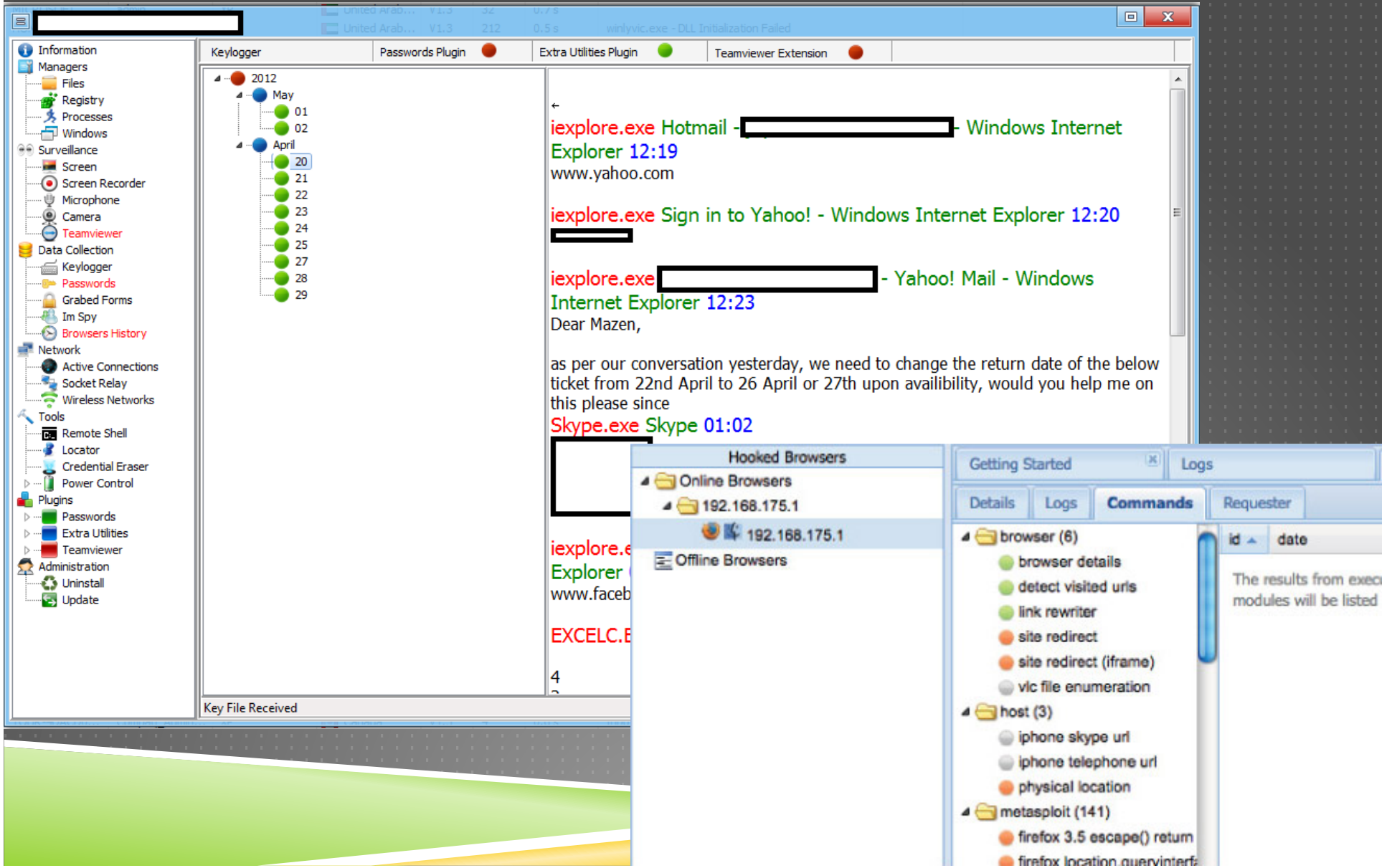
The money slide in the presentation was the job titles of those that clicked on the link:

- 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, Androrat
  - 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? ☺

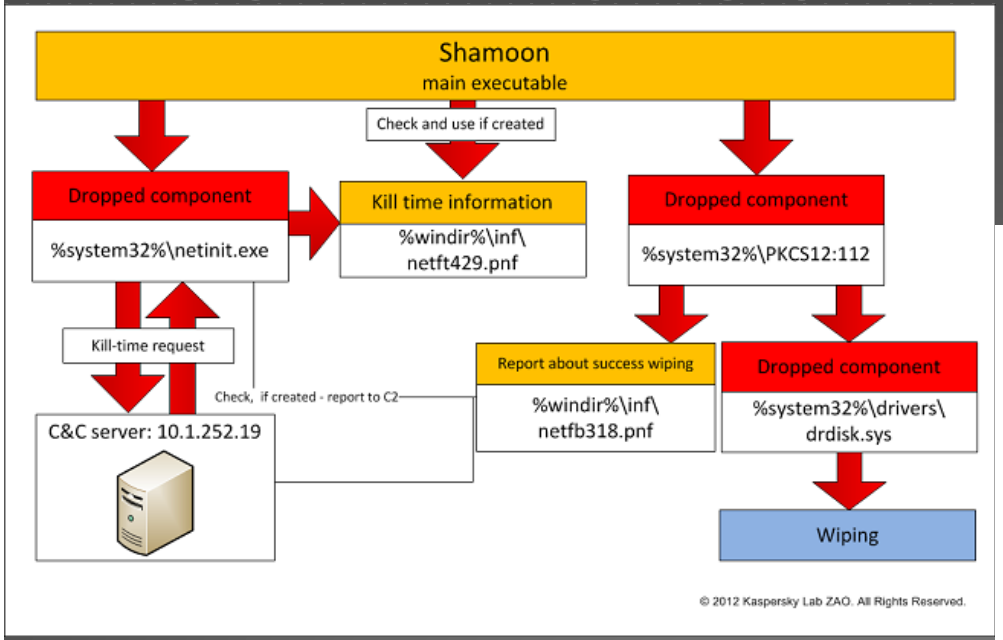
MAINTAINING ACCESS



COVERING YOUR TRACKS

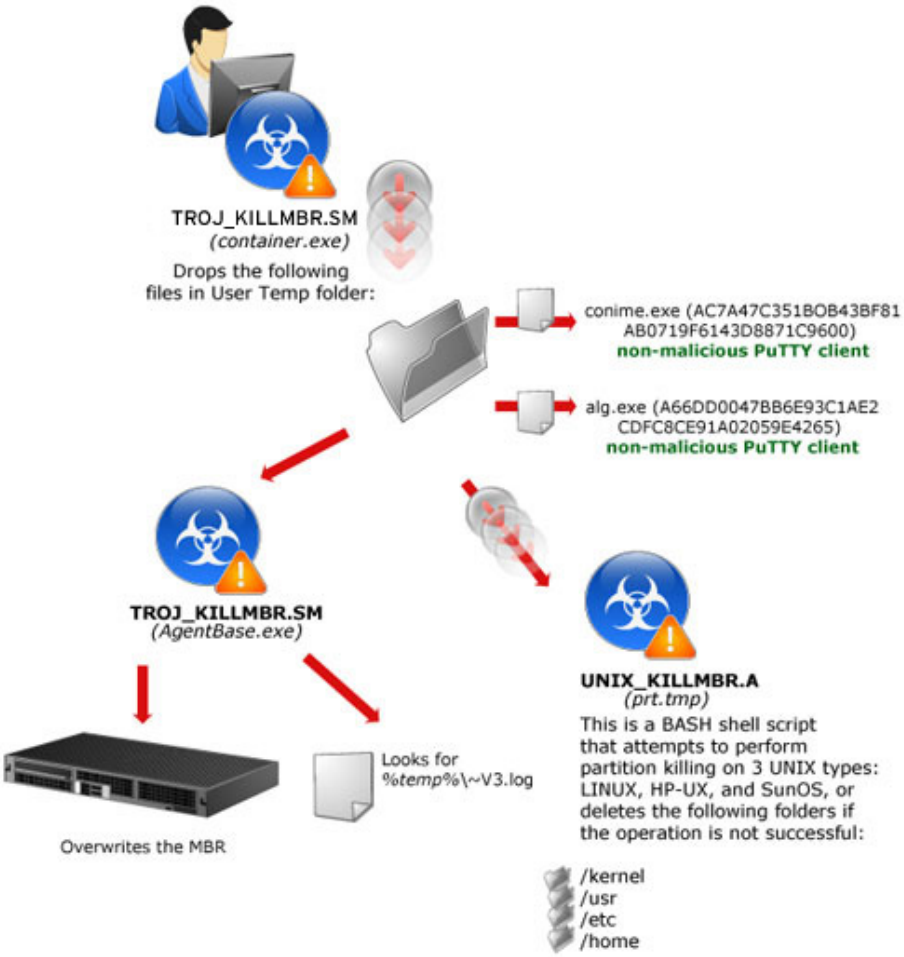
- Log doctoring
  - Both desktop & server OS types
  - Doctor the logs of the ICS hardware?
    - For advanced agents only!
- Nuclear option
  - Wipe the MBR (Shamoon attack on Aramco)
  - Wipe the MBR & disk volumes (South Korea attacks)

COVERING YOUR TRACKS

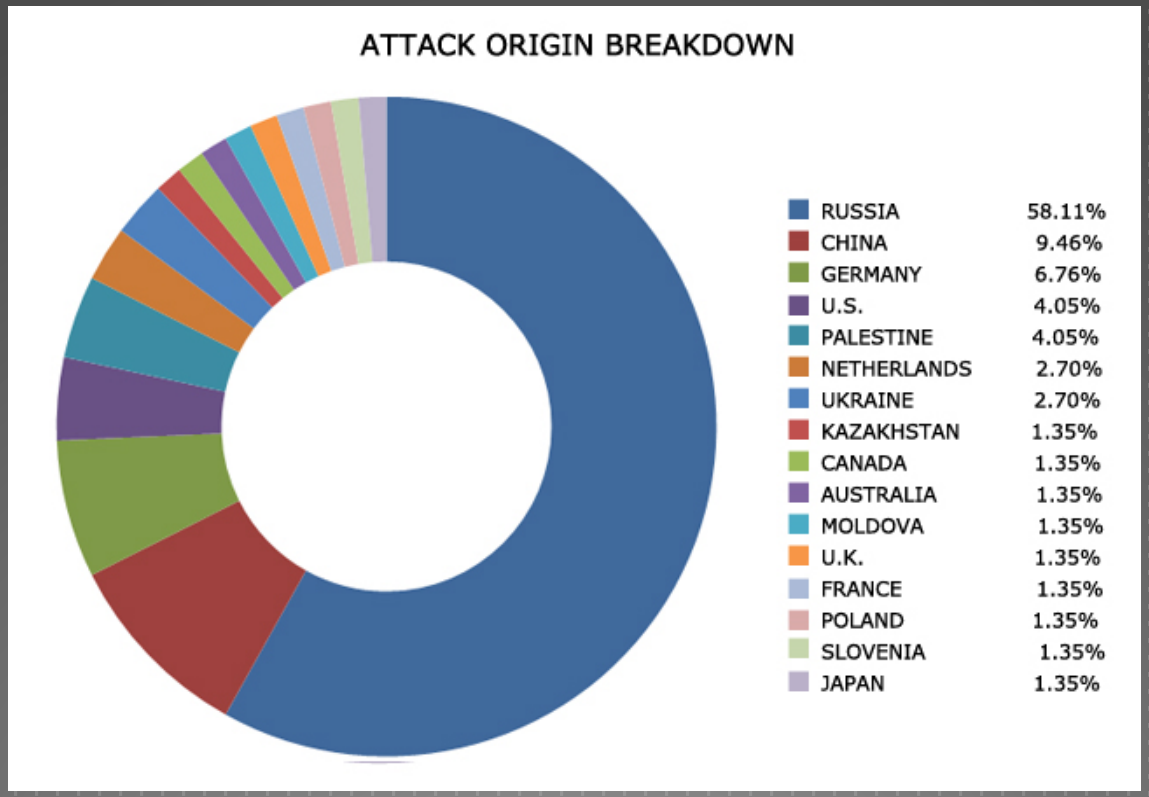


Shamoon

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 slooooooooowly…