I am a …

traffic control center

civil defense siren

smart grid

space station

steel mill

power plant

supertanker

death star

gas pipeline

sewage plant

wind power station

I am …

a power plant

associate professor

a smart grid

First contact with IT security in 1988

Computer security degree in 2004, business degree in 2009

Strong industrial background from nearly 9 yrs at Siemens

Founder and former head of Siemens Hack-Proof Products Program and Siemens ProductCERT

Founder of Limes Security in 2012

Associate Professor (University of Applied Sciences St.Pölten)

“Thomas Brandstetter”

I am …

a power plant

researcher

a smart grid

Started Software & Security Engineering in 1999

Developed flightdata analysis software from around 2002

member of the honeynet project

Activist for anonymization technology

No industrial background prior to conpot

Researcher (University of Applied Sciences St.Pölten)

“Daniel Haslinger”

RECAPITULATION

In 2010, the world was considered a much less hostile one

The internet was known to have security issues, but the industrial automation world considered itself to be somewhat peaceful, due to:

- The success of process/discrete automation engineers shielding their systems from enterprise IT
- The belief that the automation systems were mostly isolated or even airgapped
- Nobody outside automation would (care to) understand its inner, quite often proprietary workings

RECAPITULATION

what was Stuxnet?

- A major, professionally developed cyber security threat
- Targeted automation systems with specific configurations
- Received notable public attention due to
- the usage of 4 0-day vulnerabilities
- multiple infection/persistence vectors
- its abilities to inflict physical damage through cyber operation manipulations
- its political “cyber-warfare” aftertaste

RECAPITULATION

Stuxnet showed that regular IT attack know-how applies to ICS too

Many researchers tried to find ICS software

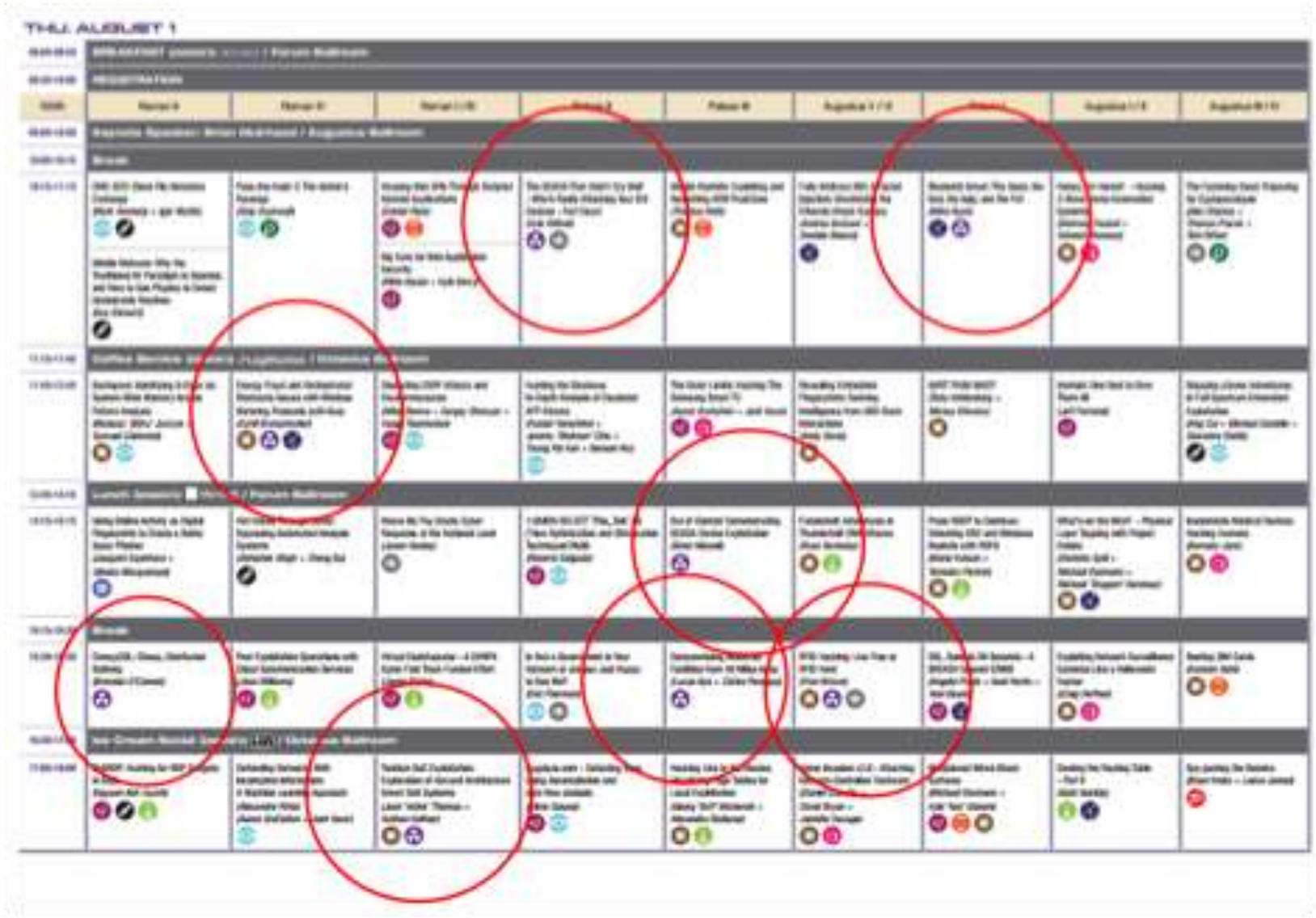
Copycats: Public disclosures of vulnerabilities were followed up by others

RECAPITULATION

Industrial security presentations are “mainstream”

BlackHat 2013:

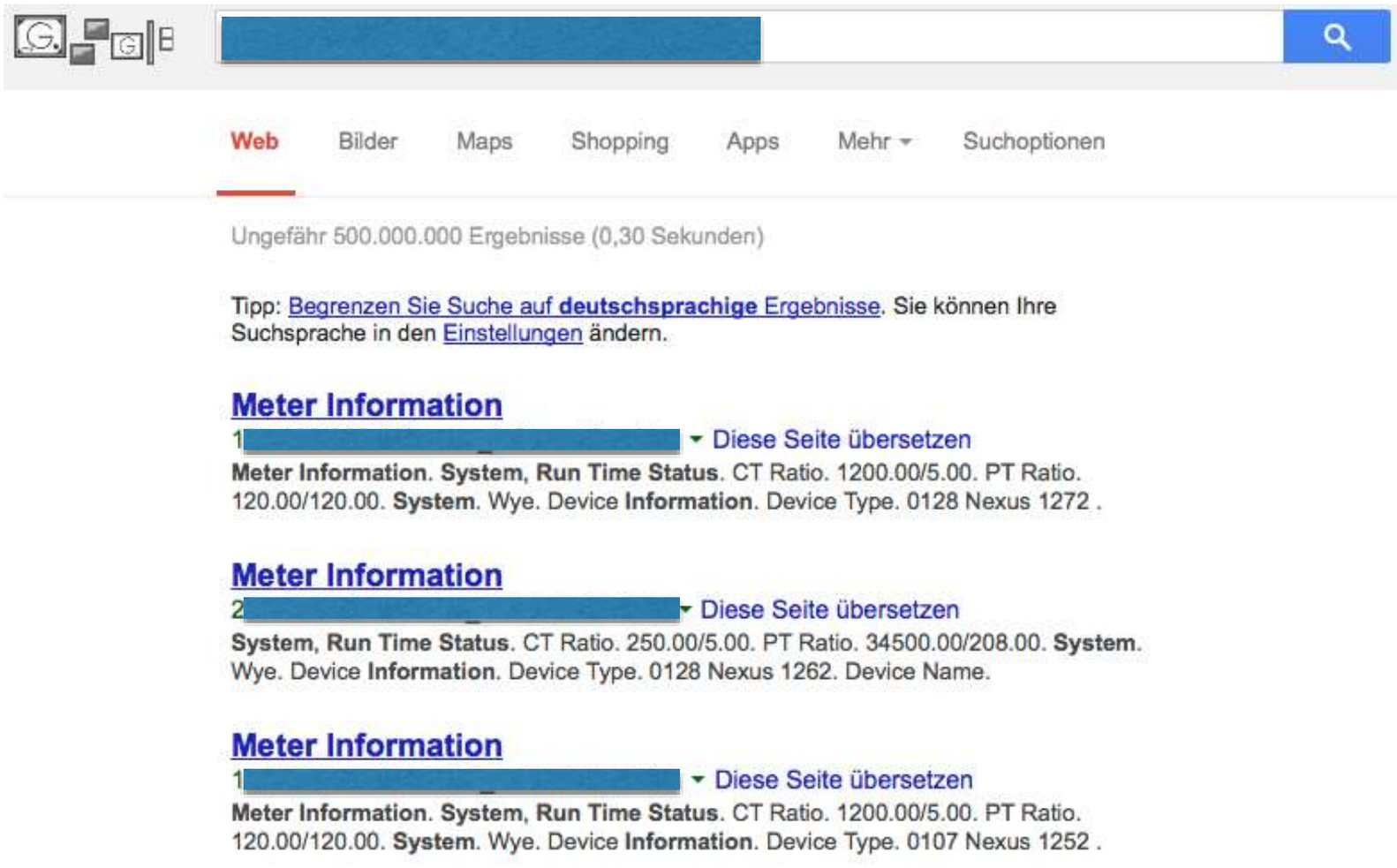
Number of SCADA security talks:



RECAPITULATION

ICS (recon) tools are getting stronger …

The security community shows strong interest in (ab)using SHODANHQ, Google and other search engines for finding ICS systems connected to the internet



RECAPITULATION

…even politically motivated hacks are “mainstream”

In the last decade, politically motivated/funded hacking was rare

- Estonia, and ???

In 2013, many publications document offensive operations or cyber units of nations such as

- China (e.g. APT1 through Mandiant report)
- USA (through their “tailored access operations”)
- UK
- Russia (Since early September)
- Middle-East (e.g. Syrian Electronic Army)

This ends speculations on existens of offensive operations

Nation-state level attackers have a strong interest in identifying foreign ICS systems…

So, how do we learn who is attacking us?

HONEYPOTS

Abstract definition:

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource." (Lance Spitzner)

Concrete definition:

"A honeypot is a fictitious vulnerable IT system used for the purpose of being attacked, probed, exploited and compromised."

Honeypots are real or emulated vulnerable systems ready to be attacked.

HONEYPOTS

Traps set to detect, deflect and counteract attempts at unauthorized use of information systems.

Valueable systems that can be used as surveillance and early-warning tool.

Used for monitoring, detecting and analyzing attacks

HONEYPOTS

Primary value of honeypots is to collect information.

This information is used to better identify and study attacks

May lure an attacker away from real systems, buying time during incident response

So, why not mixing the honeypot concept with industrial control systems?

Recent Publications

Trend Micro Incorporated:

release of a research paper 2013:

“Who’s really attacking your ICS Equipment”

“Where do attacks come from?”

Recent Publications

Trend Micro Incorporated:

release of a research paper 2013:

“Who’s really attacking your ICS Equipment”

USA GB LAOS CHINA NETHERLANDS

JAPAN BRAZIL POLAND RUSSIA VIETNAM

PALESTINIAN TERRITORIES NORTH KOREA CHILE

Products

DIGITAL BOND SCADA Honeywall

for high-interaction scenarios, to be put in front of real PLCs and similar equipment.

DIONAEA

used for ICS by some researchers - often to emulate a single protocol to be observed.

HoneyD

very widespread, but minimalistic approaches to protocol emulation.

Difficulties

<LOGGING mode=“egoistic”>

data collected by countless researchers that operate (ICS related) honeypots is dispersed!

valuable information may be lost because of different logging formats and targets

Difficulties

<OPERATING mode=“expert”>

honeypots are often hard to set up, parameterizing them is a tough and complex job

many companies would run honeypots, but they don’t know how …

THE HONEYNET PROJECT

“An open source industrial control honeypot”

CONPOT

CONPOT

Easy to use

In future, ready-to-use templates of common ICS hardware allow easy setup …

Flexible

some products do not “behave” the way they should according to protocols - so we must be flexible …

Co-op mode included!

attack data can be transmitted to HPFRIENDS, a “social” platform where you can store and retrieve attack information…

CONPOT

HTTP

HTTP 0.9 / 1.0 / 1.1 support
including several transfer encodings, status msgs and selective backproxying, coordinated dynamic response

SNMP

SNMP v1, v2c, v3 support
including read / write / next / bulk and coordinated dynamic response

CONPOT

MODBUS

Modbus TCP implementation,

allowing to define multiple slaves (e.g. sensors, motors, etc.)

s7comm

The s7 protocol, provided over “ISO on TCP”
being able to respond to SSL/SZL requests for fingerprinting

CONPOT

all those protocols

are allowed to misbehave … :-)

are rate limited in case they go berserk (SNMP traffic amps)

are tarpitted (to emulate slow devices)

are almost complete protocol stacks

CONPOT

Written in python…

Easy to understand, easy to extend, PEP-8 compliant, unit-tested and documented

…and very humble

Conpot will happily run on low performance commodity hardware, e.g. an Raspberry Pi or AWS micro instances, .. your smartphone (?)

CONPOT

use the source, Luke!

Everything we do is available on github

http://conpot.org

http://github.com/glastopf/conpot

we <3 contributions and rich pull requests :)

CONPOT

... let's watch a short ad we created for conpot ...

FIN

— Audience testing slide —

If they do not clap yet,
blame it on the audience …