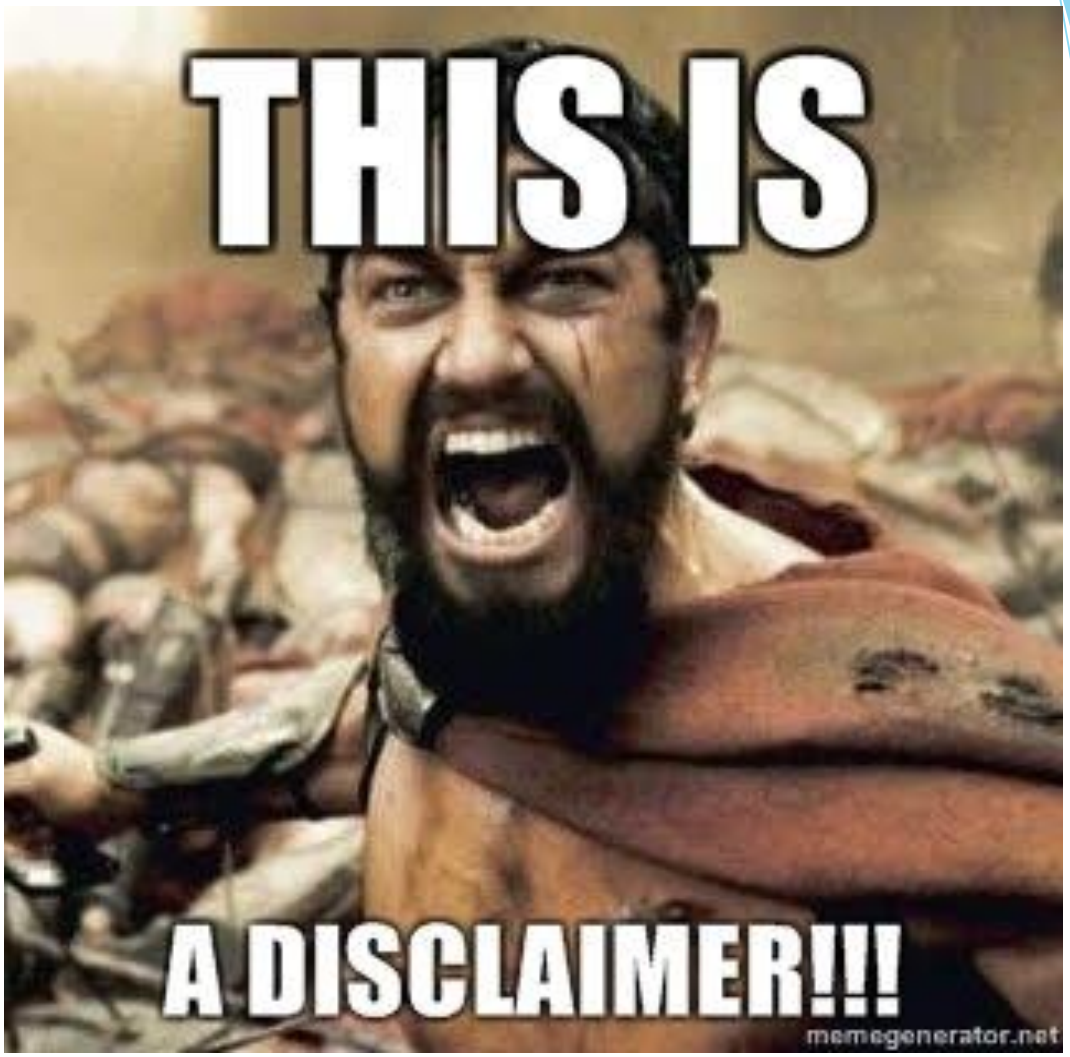
Mezinárodní spolupráce v boji proti kybernetickým hrozbám

Národní úřad
pro kybernetickou
a informační bezpečnost



DISCLAIMER: Názory prezentované v této přednášce jsou výhradně názory autora a nemusí nutně reprezentovat stanoviska a názory NÚKIB, potažmo NCKB.

KYBERNETICKÉ HROZBY

Kybernetická kriminalita

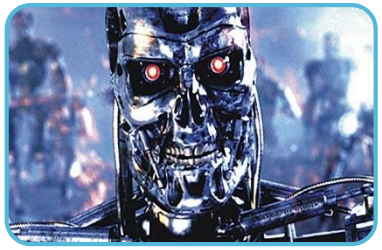
- Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat

Kybernetický terorismus

- Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.

Kybernetická špionáž

- Užití/zneužití ICT s cílem získat citlivé informace bez souhlasu jeho držitele/majitele. Provádí ji státní i nestátní aktéři za účelem získání strategické, ekonomické, politické,
nebo vojenské převahy.



Kybernetická válka

- Národní stát (či skupiny podporované státem) cílí na sítě a systémy jiného státu za účelem jejich zničení či narušení, způsobení škody, extrakce/zničení citlivých informací, narušení bojeschopnosti, apod. Útoky provádí především specializované vojenské/zpravodajské jednotky.

Proč je nutná mezinárodní spolupráce?

- Relativní nezávislost kyberprostoru na geografických/policy hranicích
- Většina kybernetických bezpečnostních incidentů má přeshraniční/mezinárodní povahu
- Problematika vymáhání práva v kyberprostoru

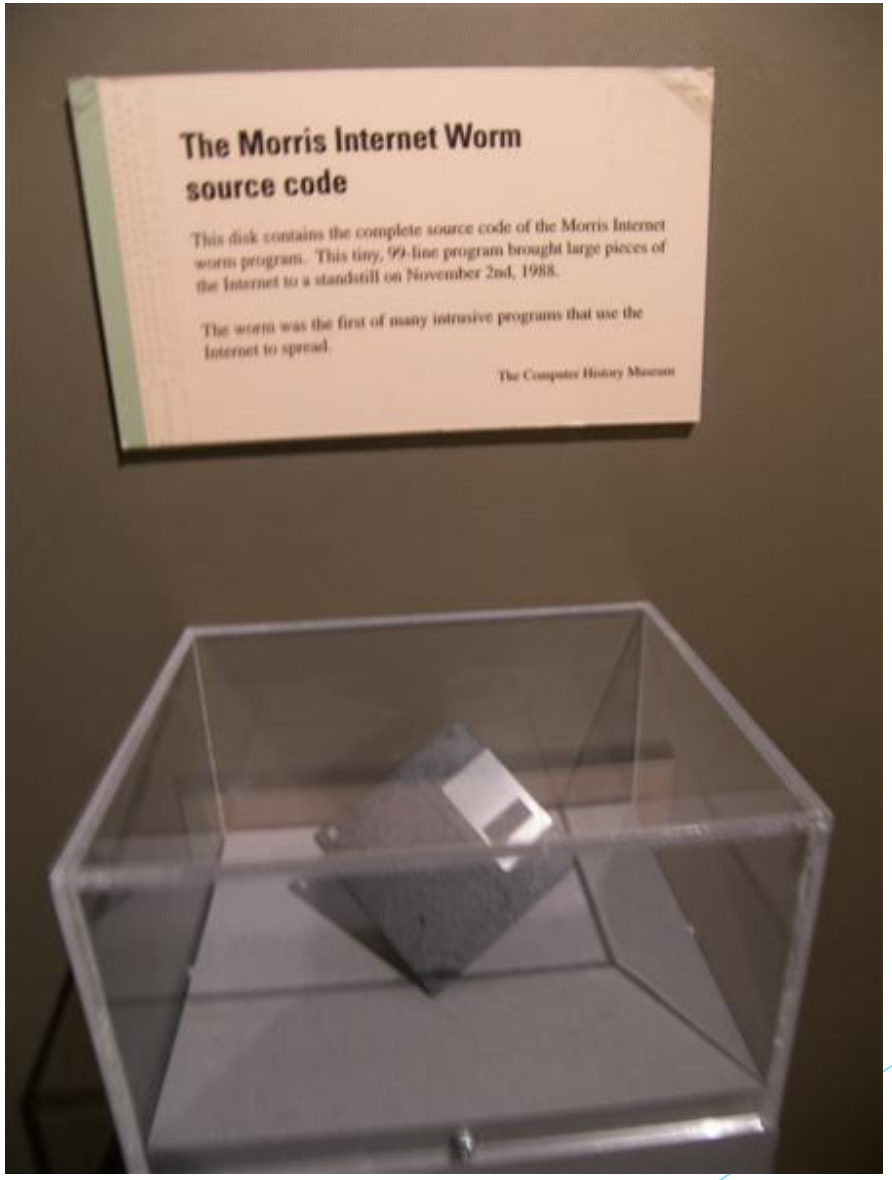
Mezinárodní spolupráce

- Mnoho úrovní: přeshraniční, regionální, mezinárodní, …
- Mnoho dimenzí: kyberkriminalita, kyberterorismus, incident response, …
- Mnoho druhů: sdílení dat a informací, memoranda, konvence, …
- Mnoho aktérů: mezinárodní organizace, vlády/stát, soukromý sektor, akademie, …

Historie spolupráce v kybernetické bezpečnosti: 1988 - Morris worm


Virus


Thug Life


The Morris Internet Worm
source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
The Computer History Museum

GOVCERT.CZ

CERT/CSIRT

- Další názvy, s kterými se můžeme setkat jsou např.:
  - IRT (Incident Response Team),
  - CIRT (Computer Incident Response Team),
  - SERT (Security Emergency Response Team),
  - CIRC (Computer Incident Response Centre)
  - a další
- Všechny spojuje zvládání a řešení kybernetických bezpečnostních incidentů – incident handling/response
- V každém státě na vrcholové úrovni min. 1 TOP-level CERT/CSIRT

TYPY CERT/CSIRT

- **Národní/vládní** (GovCERT.CZ, SingCERT)
- **Regionální** (TF-CSIRT, AfricaCERT)
- **Sektorový** (ICS-CERT)
- **Akademický** (CESNET-CERTS)
- **Vojenský** (Centrum CIRC)
- **Interní** (ACTIVE24-CSIRT, CSOB-Group-CSIRT)
- **Koordinační** (GovCERT.CZ, US-CERT)
- **Produktové** (Cisco PSIRT, Adobe PSIRT)
- **Byznys / Poskytovatelé incident handling** (Team Cymru, Nixu, Mandiant)
- …

Constituency

- Pole působnosti – Soubor subjektů, kvůli kterým byl CERT/CSIRT vytvořen/komu poskytuje a nabízí služby
- *Constituency* může být jak neomezená, kdy CERT/CSIRT poskytuje služby komukoliv, nebo omezená (ve většině případů), kdy poskytuje své služby jen vybrané, úzké komunitě
- Může být však obtížné přehledně a jednoduše definovat constituency
- **RFC 2350 standard** (základní info o možnostech kontaktování, odpovědnosti a nabízených službách)

GOVCERT.CZ

- veřejné instituce a kritická informační infrastruktura v České republice

- celá Česká republika, tzn. všichni uživatelé a všechny sítě provozované v České republice se nachází ve sféře vlivu CSIRT.CZ

CSIRT-MU

- Constituency bezpečnostního týmu Masarykovy univerzity CSIRT-MU může být definována:
  - „univerzitní síť Masarykovy univerzity“
  - skrze doménu „*.muni.cz“ (tj. fss.muni.cz; ff.muni.cz; apod.)
  - a skrze rozsah IP adres (všechny IPv4 adresy z rozsahu 147.251.0.0/16, všechny IPv6 adresy z rozsahu 2001:718:801::/48)

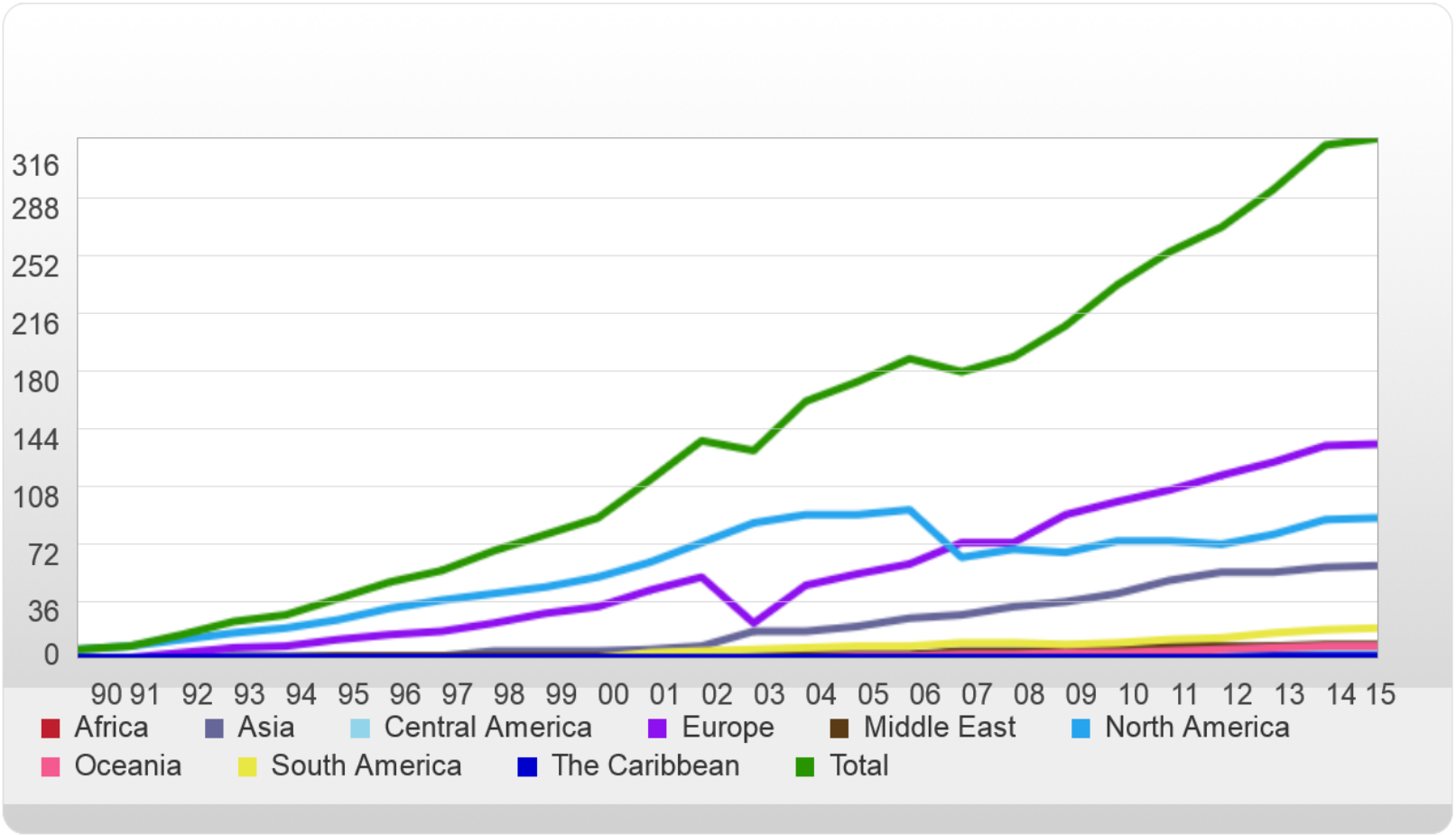
CERT/CSIRT – činnosti a aktivity

- Důležitá je kooperace a důvěra se svou constituency a ostatními CERT/CSIRT
- **Esenciální součástí zvládání a řešení kybernetických bezpečnostních incidentů** + další služby (ovlivňuje finanční prostředky, technologické vybavení a lidský kapitál)
- CERT/CC vytvořil základní klasifikaci CERT služeb, která by měla sloužit k větší konzistenci a srovnatelnosti popisu CERT služeb

FIRST

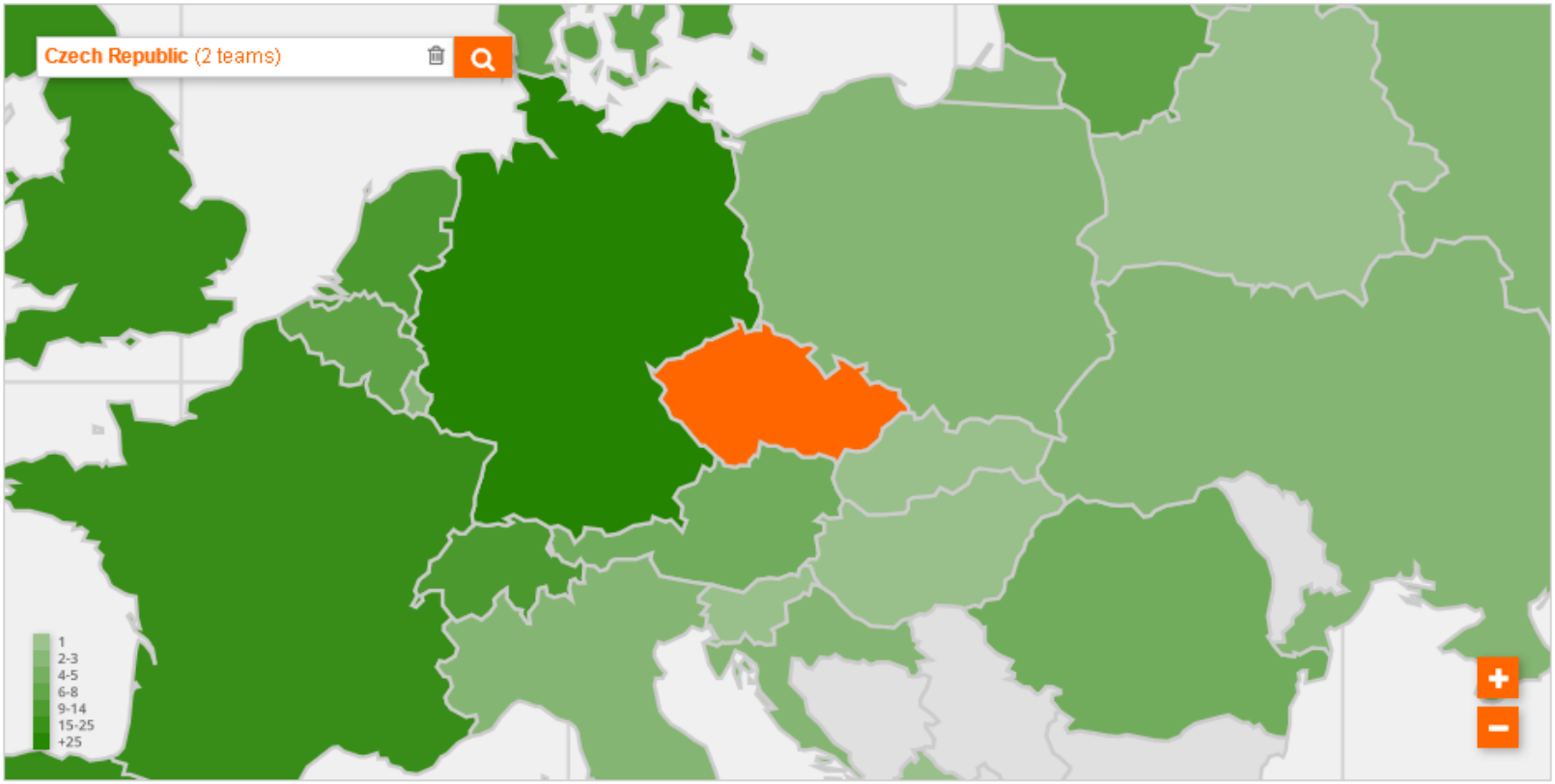
- Založeno 1990
- Forum for Incident Response and Security Teams
- Sdružuje CERT komunitu na globální úrovni
- Hlavním cílem: sdílení informací a zkušeností mezi CERT pracovišti a pomoc při rozsáhlých kybernetických bezpečnostních incidentech
- Aktuálně stovky členů
- Status: member

FIRST members growth by year*



(*) The statistic measurement method and regional breakdown changed in 2007.

Members around the world



Search results for: **Czech Republic** *(2 teams)*

Team name	Official Team name	Country
CSIRT.CZ	The Czech National CSIRT	
GovCERT.CZ	Government CERT of the Czech Republic	

FIRST follows the International Olympic Committee (IOC) country name listings. [credits]

TI-GÉANT

- 2000 – založena evropská komunita CERT/CSIRT týmů za účelem řešení společných potřeb a budování infrastruktury, která by poskytovala důležitou podporu všem bezpečnostním týmům, zaměřeným na řešení a řízení bezpečnostních incidentů
- Pro akreditované / certifikované týmy jsou k dispozici služby, které jim umožní efektivněji spolupracovat a účinněji si vyměňovat informace

TI-GÉANT

- Status:
  - Listed (splnění základních požadavků)
  - Accredited (náročnější proces – standardní stupeň)
  - Certified (pouze malá část týmů / potvrzení vysoké vyspělosti týmu)
- TRANSITS / TF-CSIRT meetings
- Další regionální platformy: AfricaCERT, APNIC, …

Czech Republic

CESNET-CERTS	Accredited (since 27 Jan 2008)
CSIRT-MU	Certification Candidate (since 26 Nov 2015)
CSIRT.CZ	Accredited (since 13 Oct 2011)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)
GOVCERT.CZ	Accredited (since 21 Aug 2014)

Czech Republic

2CCSIRT	Listed (since 15 Sep 2014)
ACTIVE24-CSIRT	Listed (since 09 Feb 2012)
ALEF-CSIRT	Accreditation Candidate (since 08 Sep 2016)
CASABLANCA.CZ-CSIRT	Listed (since 08 Mar 2014)
CDT-CERT	Listed (since 16 Jul 2014)
CESNET-CERTS	Accredited (since 27 Jan 2008)
Coolhousing CSIRT	Listed (since 17 Sep 2014)
CS-CSIRT	Listed (since 11 Mar 2016)
CSIRT Merit	Listed (since 25 Mar 2015)
CSIRT-MU	Certification Candidate (since 26 Nov 2015)
CSIRT-VUT	Listed (since 20 May 2014)
CSIRT.CZ	Accredited (since 13 Oct 2011)
CSOB-Group-CSIRT	Listed (since 29 Oct 2014)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)
DIAL-CERT	Listed (since 16 Dec 2013)
FORPSI-CSIRT	Listed (since 19 Jul 2015)
GOVCERT.CZ	Accredited (since 21 Aug 2014)
ISPA CSIRT	Listed (since 13 Aug 2015)
KAORA-CSIRT	Listed (since 04 Mar 2015)
O2.cz CERT	Listed (since 01 Jan 2014)
SEBET	Listed (since 25 Oct 2014)
SEZNAM.CZ-CSIRT	Listed (since 18 Oct 2013)
SOCA	Listed (since 04 May 2016)
TMCZ CSIRT	Listed (since 08 Aug 2016)
WEB4U-CSIRT	Listed (since 19 Jul 2015)


Kaliningrad
RUSSIA
Vilnius
Gdańsk
Rostock
Hamburg
Berlin
Amsterdam
Poznań
Warsaw
Brest
NETHERLANDS
Hannover
Elbe
GERMANY
POLAND
Wrocław
Leipzig
Brussels
Bonn
Vistula
Kraków
L'viv
BELGIUM
Frankfurt
Luxembourg
Paris
LUX.
SLOVAKIA
Stuttgart
Bratislava
Strasbourg
Vienna
Budapest
Munich
AUSTRIA
HUNGARY
SWITZ.
LIECH.
Graz
Bern
Pécs
Geneva
Ljubljana
SLOVENIA
Zagreb
Danube
Lyon
Milan


Kaliningrad
RUSSIA
Gdańsk
Rostock
Hamburg
Berlin
Amsterdam
NETHERLANDS
CERT Bund
Poznań
Warsaw
Brest
CERT.PL
GERMANY
Wrocław
Leipzig
Bonn
CERT.be
Kraków
Frankfurt
Luxembourg
LUX.
Paris
CSIRT.SK
Stuttgart
Budapest
CERT-FR
Munich
CERT.at
Graz
SWITZ.
LIECH.
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
Pécs
Geneva
Bern
si·cert
Lyon
Milan
Zagreb
Danube


HACKED
CERT Bund
CERT.PL
CERT.be
CERT-FR
CSIRT.SK
CERT.at
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
si-cert
Kaliningrad
RUSSIA
Gdańsk
Hamburg
Amsterdam
NETHERLANDS
GERMANY
Poznań
Warsaw
Brest
Wrocław
Kraków
Bonn
Frankfurt
Luxembourg
LUX.
Paris
Stuttgart
Munich
Budapest
Graz
SWITZ.
LIECH.
Bern
Geneva
Lyon
Milan
Pécs
Zagreb
Danube
L'viv


HACKED
CERT Bund
CERT.PL
CERT.be
CSIRT.SK
CERT-FR
CERT.at
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
si·cert
Hamburg
Amsterdam
NETHERLANDS
GERMANY
Bonn
Frankfurt
Luxembourg
LUX.
Paris
Stuttgart
Munich
SWITZ.
Bern
Geneva
Lyon
Milan
Poznań
Warsaw
Brest
Wrocław
Kraków
L'viv
Budapest
Graz
Pécs
Zagreb
Danube

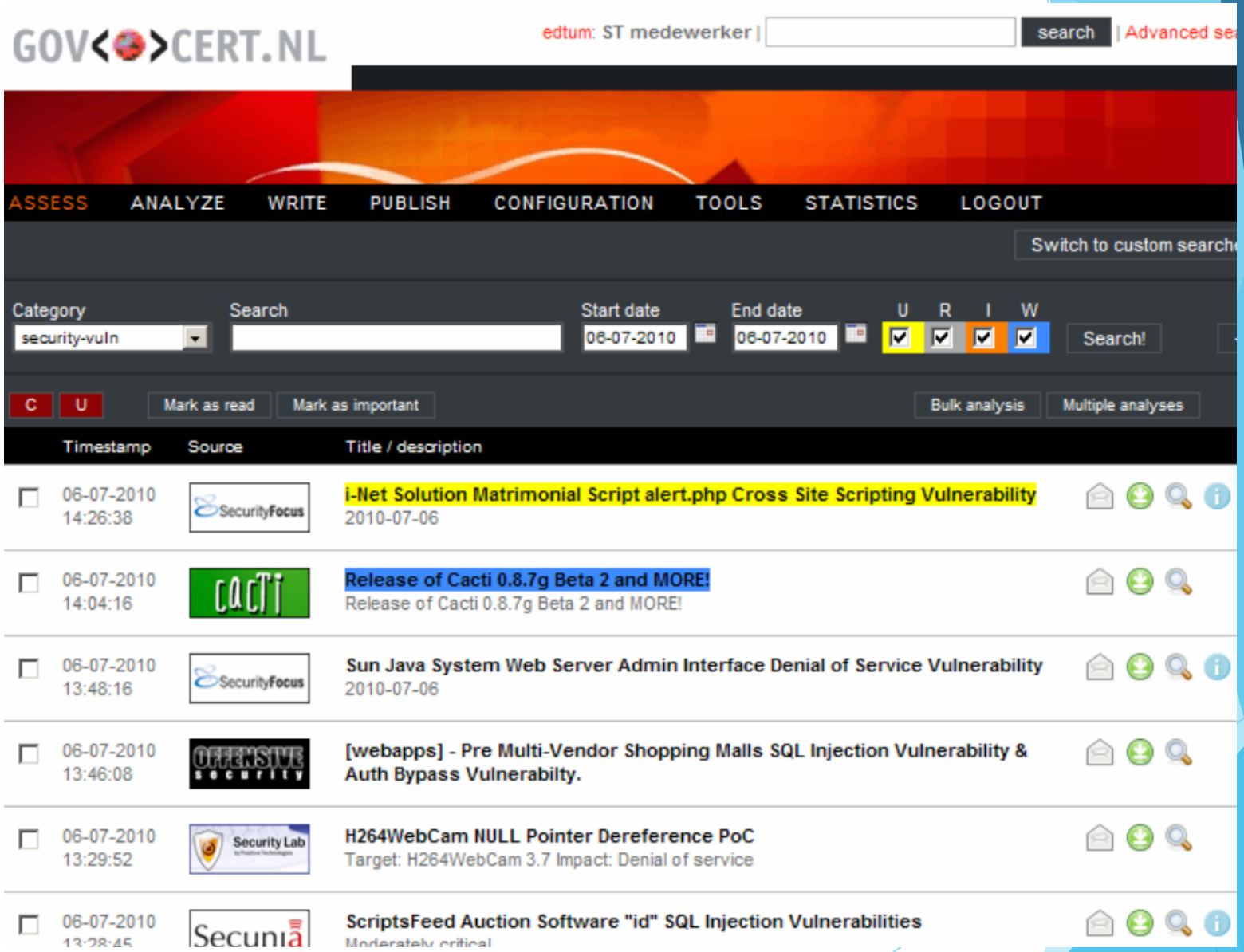

HACKED
CERT Bund
CERT.PL
CERT.be
CSIRT.SK
CERT-FR
CERT.at
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
si·cert
Hamburg
Amsterdam
NETHERLANDS
Poznań
Warsaw
Brest
Wrocław
Kraków
L'viv
Luxembourg
LUX.
Paris
Munich
Budapest
Graz
Pécs
Zagreb
Danube
SWITZ.
LIECH.
Bern
Geneva
Lyon
Milan


Hamburg
Berlin
Amsterdam
NETHERLANDS
Poznań
Warsaw
Brest
Wrocław
Leipzig
Kraków
L'viv
Luxembourg
Paris
LUX.
Munich
Budapest
Graz
Geneva
Bern
Lyon
Milan
Pécs
Danube
Zagreb
CERT Bund
CERT.PL
CERT.be
CSIRT.SK
CERT-FR
CERT.at
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
si·cert


Gdańsk
Hamburg
Berlin
Amsterdam
NETHERLANDS
Poznań
Warsaw
Brest
CERT Bund
CERT.PL
Wrocław
Leipzig
Kraków
Vistula
L'viv
CERT.be
Luxembourg
Paris
LUX.
CSIRT.SK
Budapest
CERT-FR
Munich
CERT.at
Graz
SWITZ.
LIECH.
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
Pécs
Geneva
Bern
si·cert
Lyon
Milan
Zagreb
Danube

Kultura CERT/CSIRT komunity

- CERT/CC jako pionýr a prapůvodce komunity
- Celá komunita sdílí několik klíčových principů, které pramení ze společného přesvědčení, chápání a pohledu na kybernetickou bezpečnost
- Důležitost vzájemné komunikace a především důvěry mezi členy, jako důležité prerekvizity k účinné a úspěšné spolupráci
- Problém navyšování důvěry/spolupráce („Hlava 22“):
  - Nezbytnost – iniciuje kooperaci s možným pozitivním výsledkem
  - Trusted introducer – založeno na dobrých vztazích mezi členy (využíváno např. v FIRST, TF-CSIRT)
  - Příležitost – vytváří vazby mezi členy / zapojování se do chodu komunity (např. vývoj bezp. nástrojů)


GOV CERT.NL
edtum: ST medewerker |
search
| Advanced se
ASSESS
ANALYZE
WRITE
PUBLISH
CONFIGURATION
TOOLS
STATISTICS
LOGOUT
Switch to custom search
Category
security-vuln
Search
Start date
06-07-2010
End date
06-07-2010
U
R
I
W
Search!
C
U
Mark as read
Mark as important
Bulk analysis
Multiple analyses
Timestamp
Source
Title / description
06-07-2010 14:26:38
SecurityFocus
i-Net Solution Matrimonial Script alert.php Cross Site Scripting Vulnerability
2010-07-06
06-07-2010 14:04:16
cacti
Release of Cacti 0.8.7g Beta 2 and MORE!
Release of Cacti 0.8.7g Beta 2 and MORE!
06-07-2010 13:48:16
SecurityFocus
Sun Java System Web Server Admin Interface Denial of Service Vulnerability
2010-07-06
06-07-2010 13:46:08
OFFENSIVE security
[webapps] - Pre Multi-Vendor Shopping Malls SQL Injection Vulnerability & Auth Bypass Vulnerabilty.
06-07-2010 13:29:52
Security Lab
H264WebCam NULL Pointer Dereference PoC
Target: H264WebCam 3.7 Impact: Denial of service
06-07-2010
Secunia
ScriptsFeed Auction Software "id" SQL Injection Vulnerabilities
Moderately critical

Sdílení informací a dat

Sdílení informací a dat

- Nejrůznější informace a data od dalších CSIRT, AV společností, ISP, a dalších partnerů
- Feedy/fóra:
  Malc0de; Malware Domain List; Shadowserver; Zone-H; Phishtank; Abuse.ch, …

ABUSE.ch


shadowserver
Hide ⇓ Home
Edit
HomePage
Shadowserver
Mission
Updated
Terms of Service
New
Privacy
Standards and
Guidelines
Organizations
Blog
Calendar
Future Goals
Jobs and Contributions
Press
Security Organizations
News Articles
Blogs and Forums
Misc
Presentations
Chronological
Operations Status
Knowledge Base
Technology in Use
Botnets
Botnet Detection
Honeypots
eFraud
Malware
Whitepapers
Definitions
Links
Mission
Introduction
The Shadowserver Foundation is continually seeking to provide timely and relevant information to the security community at large. We also seek to increase our level of research and investigation into the activity we discover. As such, we list our goals and plans for the next six to twelve months:
Goals
Investigate and contribute to new technologies in botnet control.
Develop and deploy new methods for harvesting malware and studying its behavior.
Develop and utilize additional techniques for gathering and analyzing botnet data and network flows.
Work more closely with ISPs, Hosting and DNS providers in the identification and mitigation of botnets and malware propagation.
Increase our collaboration with other key security organizations and researchers to share discoveries and analysis.
Develop and release whitepapers and reports based on our research.
Further develop our website to provide information and reports to the interested public.
Participate in future security conferences and workgroups.
Increase our communication with the public through irc, mailing lists, and the website.

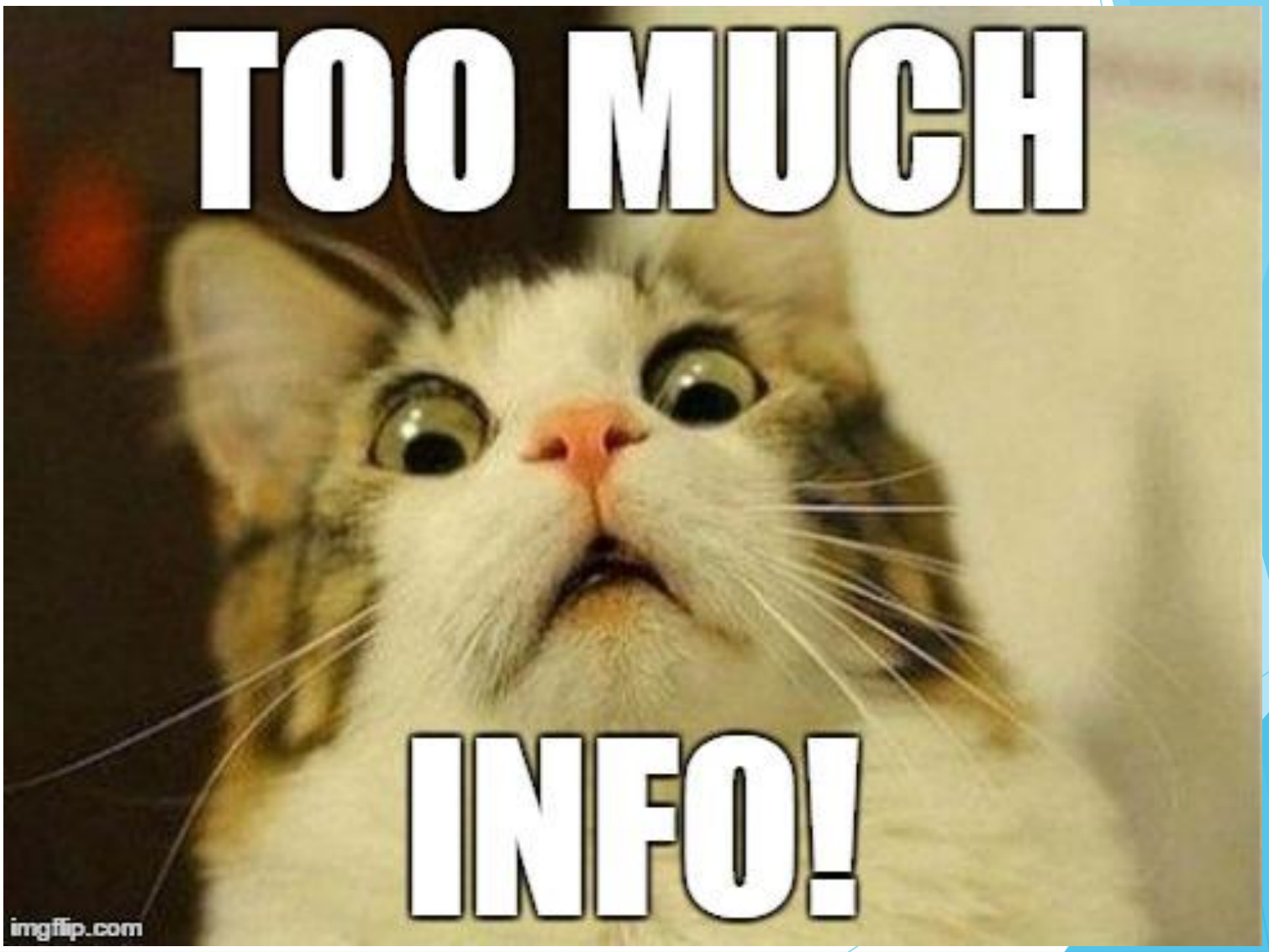
Co se sdílí?

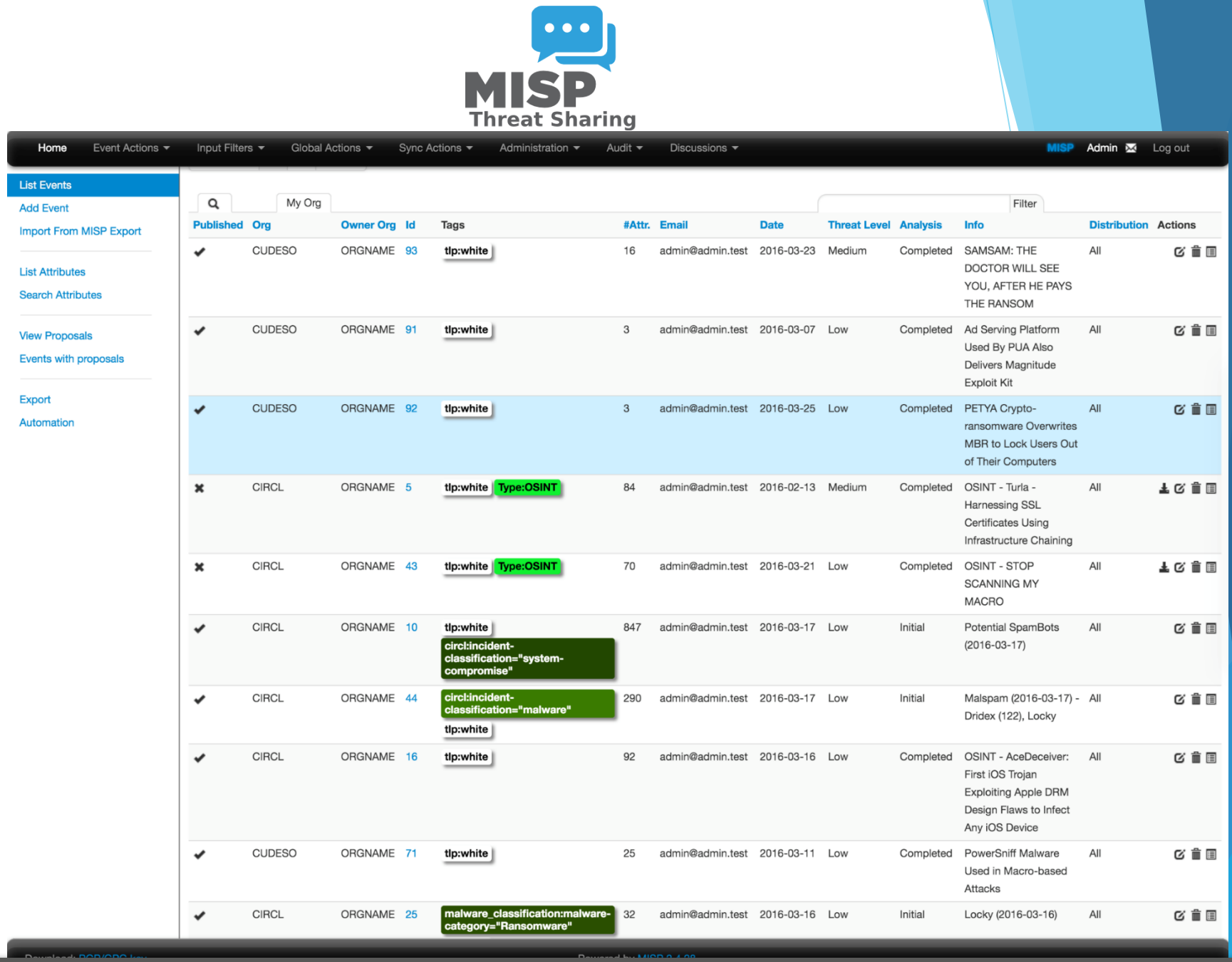
- Indikátory kompromitace (IoCs): virové signatury, škodlivé IP adresy, malware soubory, URL, doménové jména
- Kontextové informace např. o malware kampaních, informace o modu operandi útočníků,
- Případové studie a reporty o incidentech,
- Varování o možných či potenciálních obětech útoku,
- Dešifrovací klíče u ransomware útoků,
- Detaily zájmových účtů na sociálních sítích a další

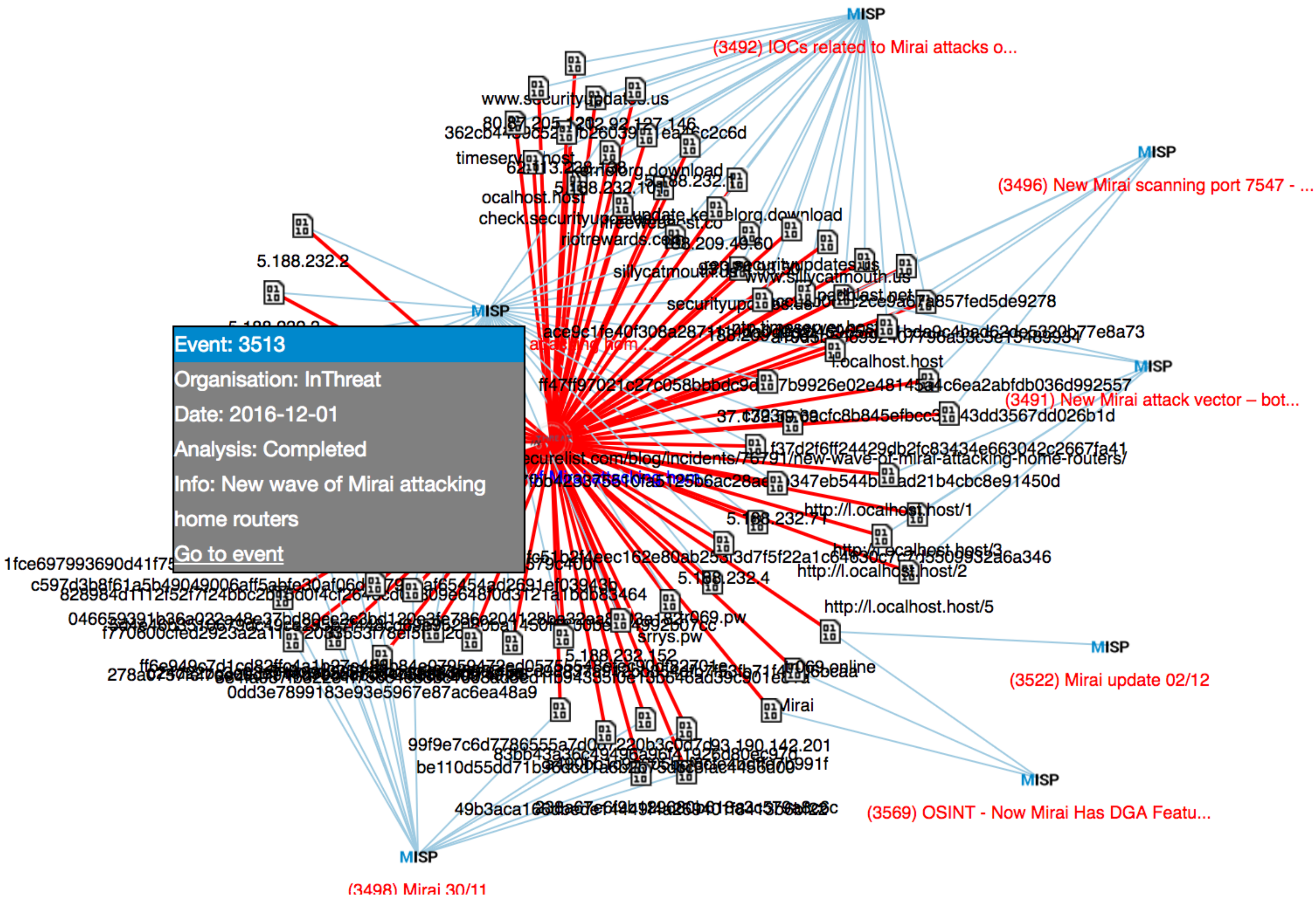
https://www.phishtank.com/

http://www.malwaredomainlist.com/mdl.php

Jak a kolik se toho sdílí?




MISP
Threat Sharing
Home
Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
MISP
Admin
Log out
List Events
Add Event
Import From MISP Export
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation
My Org
Filter
Published
Org
Owner Org
Id
Tags
#Attr.
Email
Date
Threat Level
Analysis
Info
Distribution
Actions
CUDESO ORGNAME 93 tlp:white 16 admin@admin.test 2016-03-23 Medium Completed SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM All
CUDESO ORGNAME 91 tlp:white 3 admin@admin.test 2016-03-07 Low Completed Ad Serving Platform Used By PUA Also Delivers Magnitude Exploit Kit All
CUDESO ORGNAME 92 tlp:white 3 admin@admin.test 2016-03-25 Low Completed PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers All
CIRCL ORGNAME 5 tlp:white Type:OSINT 84 admin@admin.test 2016-02-13 Medium Completed OSINT - Turla - Harnessing SSL Certificates Using Infrastructure Chaining All
CIRCL ORGNAME 43 tlp:white Type:OSINT 70 admin@admin.test 2016-03-21 Low Completed OSINT - STOP SCANNING MY MACRO All
CIRCL ORGNAME 10 tlp:white circl:incident-classification="system-compromise" 847 admin@admin.test 2016-03-17 Low Initial Potential SpamBots (2016-03-17) All
CIRCL ORGNAME 44 circl:incident-classification="malware" tlp:white 290 admin@admin.test 2016-03-17 Low Initial Malspam (2016-03-17) - Dridex (122), Locky All
CIRCL ORGNAME 16 tlp:white 92 admin@admin.test 2016-03-16 Low Completed OSINT - AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device All
CUDESO ORGNAME 71 tlp:white 25 admin@admin.test 2016-03-11 Low Completed PowerSniff Malware Used in Macro-based Attacks All
CIRCL ORGNAME 25 malware_classification:malware-category="Ransomware" 32 admin@admin.test 2016-03-16 Low Initial Locky (2016-03-16) All


MISP
(3492) IOCs related to Mirai attacks o...
MISP
(3496) New Mirai scanning port 7547 - ...
MISP
(3491) New Mirai attack vector – bot...
MISP
(3522) Mirai update 02/12
MISP
(3569) OSINT - Now Mirai Has DGA Featu...
MISP
(3498) Mirai 30/11
MISP
Event: 3513
Organisation: InThreat
Date: 2016-12-01
Analysis: Completed
Info: New wave of Mirai attacking home routers
Go to event
5.188.232.2
l.ocalhost.host
http://l.ocalhost.host/1
http://l.ocalhost.host/2
http://l.ocalhost.host/5
5.188.232.4
Mirai
srrys.pw
f37d2f6ff24429db2fc83434e663042c2667fa41
0dd3e7899183e93e5967e87ac6ea48a9

Problémy sdílení informací a vzájemné důvěry

- Otázka odpovědnosti / poškození reputace / důvěry constituency
- Vnitrostátní právní předpisy (např. zákony o datové lokalizaci, GDPR)
- Čína, Vietnam, Írán, Rusko X Austrálie, Kanada
- Různé důvody/politické cíle:
  - od zajištění ochrany osobních údajů svých občanů
  - až k ochraně státní suverenity
  - či podpoře růstu domácí digitální ekonomiky

Stát vs. CERT/kybernetická bezpečnost

- V posledních několika letech téma kybernetické bezpečnosti katapultováno z uzavřeného prostředí technických expertů až na politické výsluní
  - Vertikální/horizontální

- Virus Stuxnet / nárust kyberkriminality/ kyberšpionážní kampaně / Estonsko 2007 / 11. září 2001 → Politizace / sekuritizace tématu

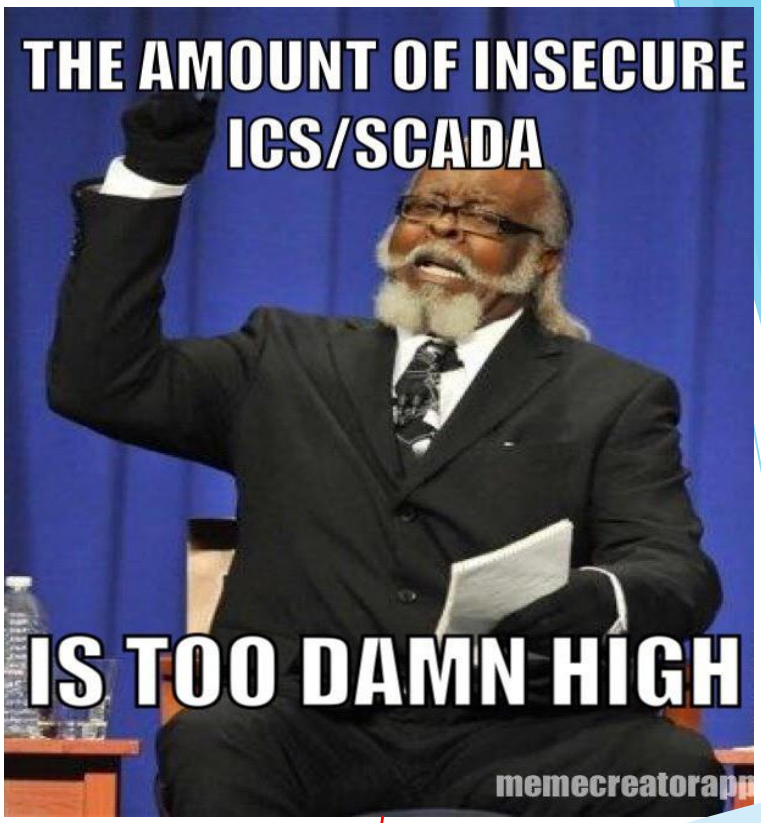
ICS/SCADA cyber security

< 2011

2011

Ted'

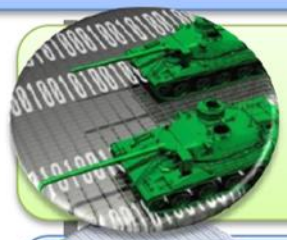
ICS/SCADA cyber security



- < 2011
- 2011 OMG STUXNET
- Ted'

KYBERNETICKÁ BEZPEČNOST STÁTU

Působení zpravodajských služeb



Kybernetická obrana

Kybernetická kriminalita

Kybernetická bezpečnost
(KB KII, VIS, Incident Handling,…)

čas

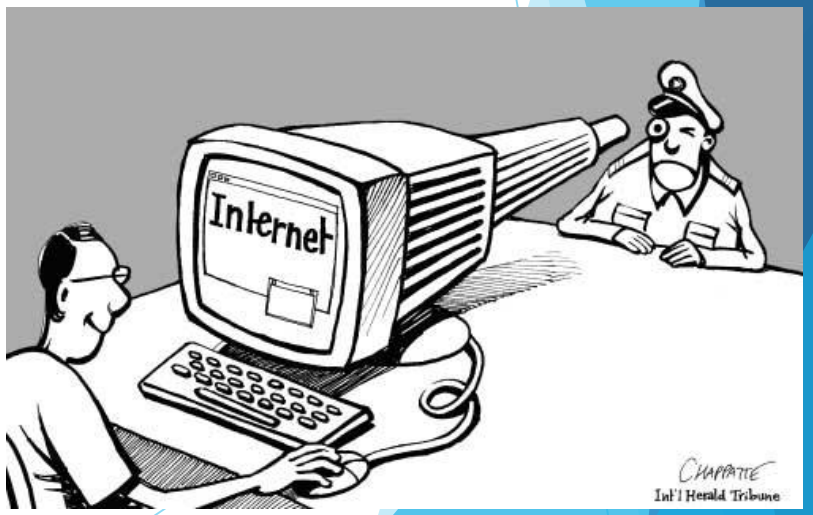
Kybernetický
bezpečnostní incident

proaktivní oblast

reaktivní oblast

Národní CERT vs. zpravodajské služby a policie

- **Společný cíl: zabezpečení kyberprostoru**
- Rozdílná mise / mandát / úroveň expertízy / pohled na KB
- **Národní/vládní CERT: hlavní priorita** – ochrana IS a KS/infrastruktury před zranitelnostmi/útoky
- **LE/IA: hlavní priorita** – redukovat počet hrozeb/fokus na aktéry; vnímání kybernetické bezpečnosti jako záležitost fyzické a národní bezpečnosti



Národní CERT vs. zpravodajské služby a policie

- **Řešení incidentu vs. využití incidentu**
  - Problematický vztah některých LE/IA s některými vendory
  - Blízký vztah CERT a LE/IA může podrýt důvěru CERT
  - Spory pramení z nepochopení poslání a kultury CERT komunity
  - Jak naložit se 0-day zranitelnostmi?

Komercionalizace kybernetické bezpečnosti

- Komodifikace a kumulace zranitelností (zero-days vulnerabilities)
- Zdroj financí např. pro soukromé firmy (nákup/vyhledávání)
- Podporuje konkurenční prostředí (paradoxně nenavyšuje kyberbezp.)
- Případ NSA / státem kupované zranitelnosti?
- Negativně působí na spolupráci v CERT komunitě

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

SID today

(U) Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets

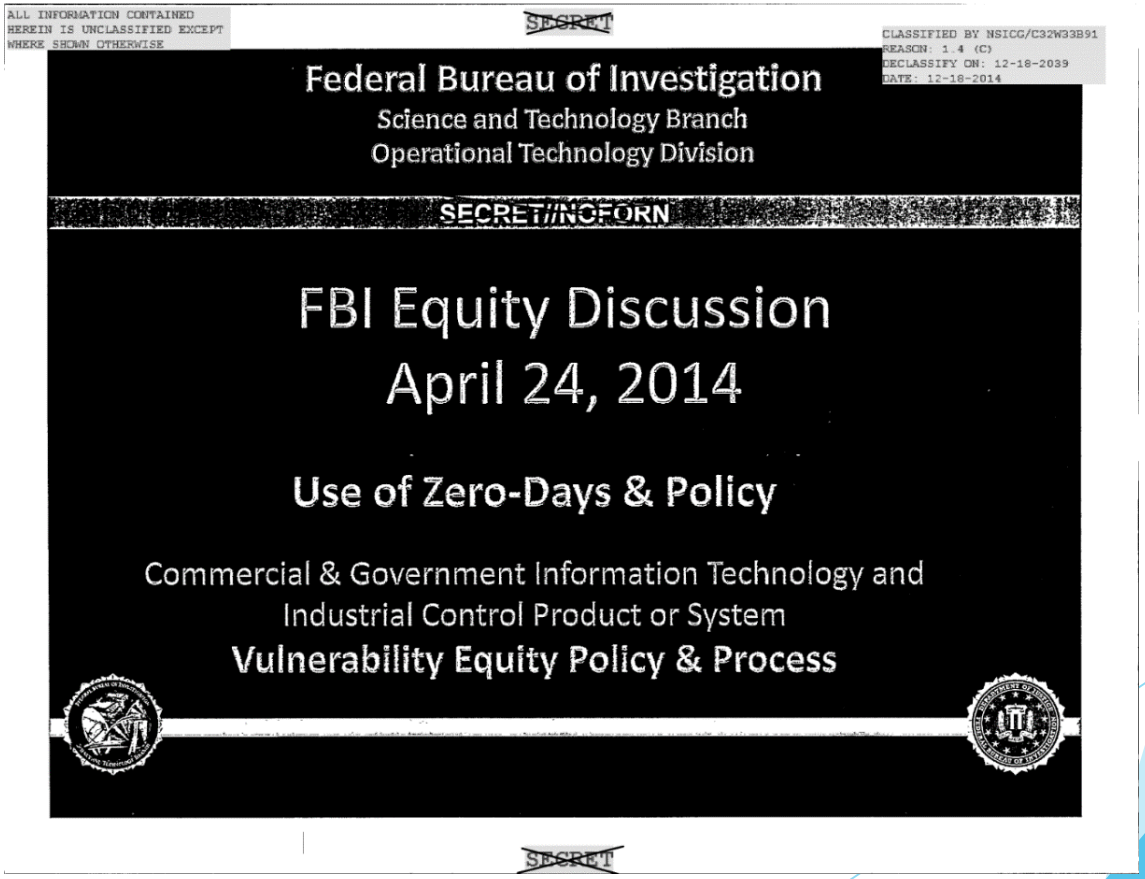
By: (U//FOUO) [redacted], Chief, Access and Target Development (S3261)

(TS//SI//NF) Not all SIGINT tradecraft involves accessing signals and networks from thousands of miles away… In fact, sometimes it is very hands-on (literally!). Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are ***intercepted***. Next, they are ***redirected to a secret location*** where Tailored Access Operations/Access Operations (AO – S326) employees, with the support of the Remote Operations Center (S321), enable the ***installation of beacon implants*** directly into our targets' electronic devices. These devices are then re-packaged and ***placed back into transit*** to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO.

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

- **Případ FBI (FOIA)** – posouzení obecně kybernetické bezpečnosti, zabezpečení informací, rozvědné a kontrarozvědné aktivity, vymáhání práva, vojenské ofenzivní operace a ochrana kritické infrastruktury

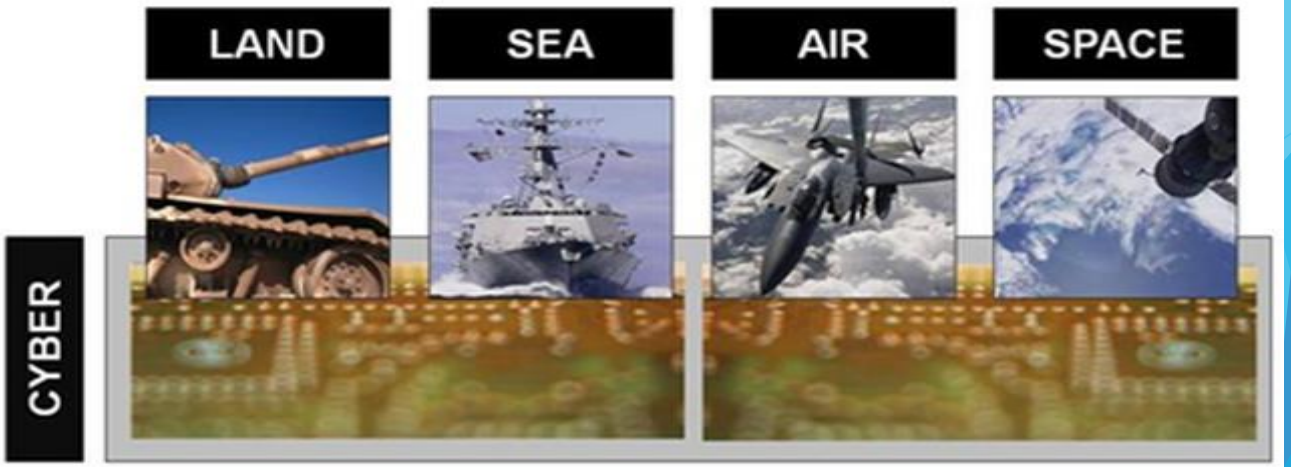


Národní CERT vs. zpravodajské služby a policie

- Výhody spolupráce:
  - Efektivnější řešení a koordinace incidentů
  - Kontextualizace kybernetických útoků / incidentů
  - Odstrašení nepřátel / útočníků

Národní CERT vs. vojenské složky

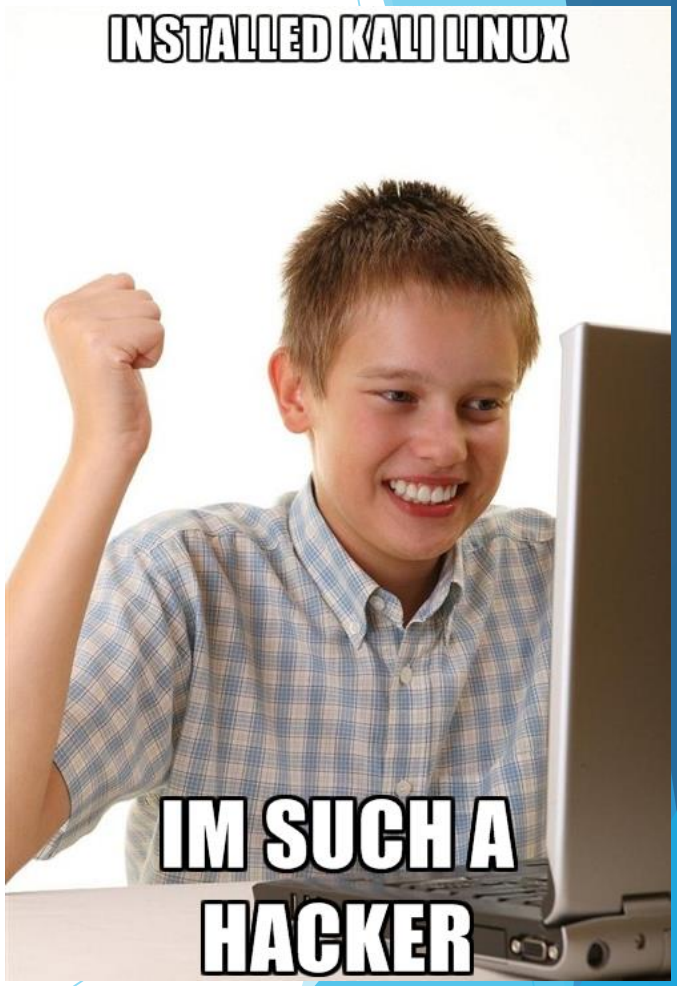
- Dříve neexistence enormní nutnosti spolupráce (civilního a vojenského sektoru)
- Omezeno na spolupráci v CERT komunitě
- NATO summit 2014, 2016 + narůstající závislost na kyberprostoru a kritičnost jeho selhání



Národní CERT vs. vojenské složky

- Vnější vs. vnitřní bezpečnost
- Kybernetická obrana vs. bezpečnost
- Atribuce?

???



ČT24

KOMUNÁLNÍ VOLBY | VOLBY V KRAJSKÝCH MĚSTECH | SENÁTNÍ VOLBY | DOMÁCÍ | SVĚT | RE

Nizozemsko viní Rusy z pokusu o hackerský útok na Organizaci pro zákaz chemických zbraní

AKTUALIZOVÁNO Před hodinou

Nizozemsko ve čtvrtek obvinilo Ruskou federaci z pokusu o hackerský útok na Organizaci pro zákaz chemických zbraní (OPCW). Ministryně obrany Ank Bijleveldová uvedla, že její země po rozkrytí operace na svém území vyhostila čtyři ruské agenty. Ti byli zadrženi 13. dubna, řekl podle agentury Reuters šéf nizozemské vojenské rozvědky Onno Eichelsheim. Ministryně zároveň oznámila, že Nizozemsko si předvolalo ruského velvyslance.

Národní CERT vs. vojenské složky

- Role CSIRT/CERT?

Kybernetická obrana			
Situace	Válka / Ozbrojený konflikt		
		Mírový stav	
Technika kybernetické obrany	Kybernetické síťové operace / nasazení kybernetických zbraní	Aktivní kybernetická obrana / hack back	Defenzivní kybernetická obrana / fortifikace

Národní CERT vs. vojenské složky

- Role CSIRT/CERT?

Kybernetická obrana			
Situace	Válka / Ozbrojený konflikt		
		Mírový stav	
Technika kybernetické obrany	Kybernetické síťové operace / nasazení kybernetických zbraní	Aktivní kybernetická obrana / hack back	Defenzivní kybernetická obrana / fortifikace

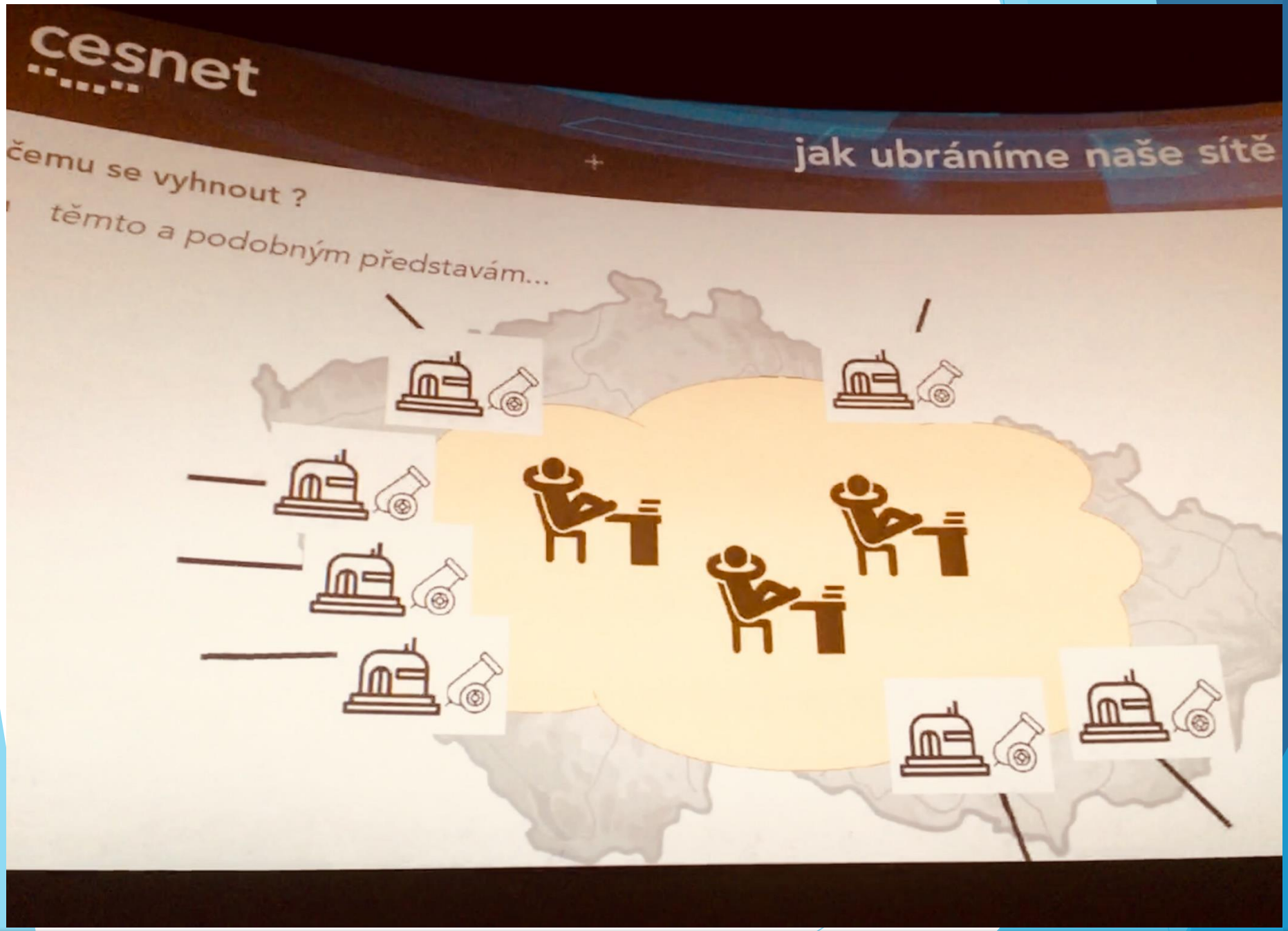
Národní CERT vs. vojenské složky

- Role CSIRT/CERT?

Typ	Popis	Příklady
Vojenská CSIRT pracoviště	- Zajišťování kybernetické bezpečnosti vojenských systémů a sítí - Detekce a řešení incidentů spolu s kontinuálním navyšování robustnosti a odolnosti vojenské infrastruktury	Centrum-CIRC FR-MIL-CERT
Vojenské jednotky kybernetické obrany	- Zajišťování kybernetické obrany státu - Nasazování ofenzivních kapacit v kyberprostoru k defenzivním i ofenzivním účelům	USCYBERCOM Defense Cyber Command (DCC)

Národní CERT vs. vojenské složky

- Válčení je stále považováno za exkluzivní vojenskou záležitost X velká závislost na civilním sektoru
- „Vábení“ tradičního myšlení / aplikace na kyberprostor problematická (role doktrín?)
- Spolupráce při defenzivní a ofenzivní části kybernetické obrany?
- Zapojení do CERT komunity? (CSIRT.MIL.SK)


cesnet
jak ubráníme naše sítě
čemu se vyhnout ?
těmto a podobným představám...

Mezinárodní spolupráce: ČR

Mezinárodní spolupráce: ČR

Strategičtí partneři

- U.S. – Federal Bureau of Investigation, US Department of Homeland Security, Department of Defense, Microsoft, Cisco Systems a další
- South Korea – intelligence community
- Israel – Ministry of Defense Security Authority (MalMab), National Cyber Bureau, CyberGym

Cyber attaché – US, (Israel), Brussels (EU/NATO)

Mezinárodní spolupráce: ČR

Cyber attachés

- Prohlubování vztahů a bilaterální spolupráce se strategickými partnery – the U.S. and Israel
- Zisk lepšího přehledu o diskuzi v otázkách kybernetické bezpečnosti – NATO/EU instituce
- Snadnější prosazování národních priorit v zahraničí a lepší koordinace aktivit jednotlivých úřadů/resortů v lybernetické bezpečnosti a spjatých oblastech

Příklad spolupráce s USA

- Pravidelné sdílení analytických výstupů / informací a dat s vybranými subjekty/agenturami
- Provádění TTX pro USCYBERCOM, NATO ACT, Norfolk and U. S. academia and think tanks
- Pravidelné návštěvy a bilaterální jednání s vybranými subjekty/agenturami
- Lekce: např. George C. Marshall Center - European Center for Security Studies (Program on Cyber Security Studies – PCSS), U.S. Congress

GovCERT.CZ

Poslání a Constituency

- **Poslání:** Přispívat k navyšování ochrany a zabezpečení KII a státních orgánů, respektive pomoci jim účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat kroky k jejich řešení a účinně jim předcházet.
- **Constituency:** veřejný sektor a kritická informační infrastruktura
- **Typ:** Vládní/Koordinační tým (nejedná se o interní typ)

Detekce incidentů

- Nasazení síťových sond
- Nasazení honeypotů
- Analýza indikátorů kompromitace a dalších veřejně dostupných dat

- Systém včasného varování

Zdroje informací / spolupráce

- Novinky, studie, diskuzní fóra / OSINT
- Analýzy AV společností, CERT týmů a dalších partnerů
- Microsoft‘s Cyber Threat Intelligence Program
- Strojově zpracovávané zdroje (IoC)
  - Shadowserver, Phishtank, MalwareDomainList, …
  - Zejména identifikace infekce / špatné konfigurace
- Sondy, honeypoty

Sdílení informací

- Informace o zranitelnostech
- Informace o možných hrozbách
- Shrnutí nedávných útoků a hrozeb
- Agregovaná strojově zpracovávaná data, zranitelnosti
- Ad-hoc analýzy v případě potřeby
- Komunitní webový portál
  - Agregovaný report z dostupných zdrojů (Shadowserver, Microsoft, atd.)
  - Informace o probíhajících útocích, incidentech
  - Privátní fórum pro bezpečnostní týmy a další zainteresované organizace

Tweets 381 | Following 142 | Followers 1,156 | Likes 27

Follow

GovCERT.CZ

@GOVCERT_CZ

National Cyber Security Center (NCSC) / National Cyber and Information Security Agency (NCISA) / e-mail contact: nckb@nukib.cz

Brno

govcert.cz

Joined November 2014

95 Photos and videos

Tweets | Tweets & replies | Media

GovCERT.CZ @GOVCERT_CZ · 23h

Do cvičení #cyberczech zbývá 14 dní. Přípravy jsou v plném proudu. Autentičnost nesmí být podceněna. Děkujeme Hasičskému muzeu Kočí za propůjčení exponátů. @csirtmu

Roman Pačka

mail: r.packa@nukib.cz / 333252@mail.muni.cz
web: www.govcert.cz
twitter: @GOVCERT_CZ