ROLE CERT/CSIRT v NÁRODNÍ BEZPEČNOSTI

Národní úřad
pro kybernetickou
a informační bezpečnost

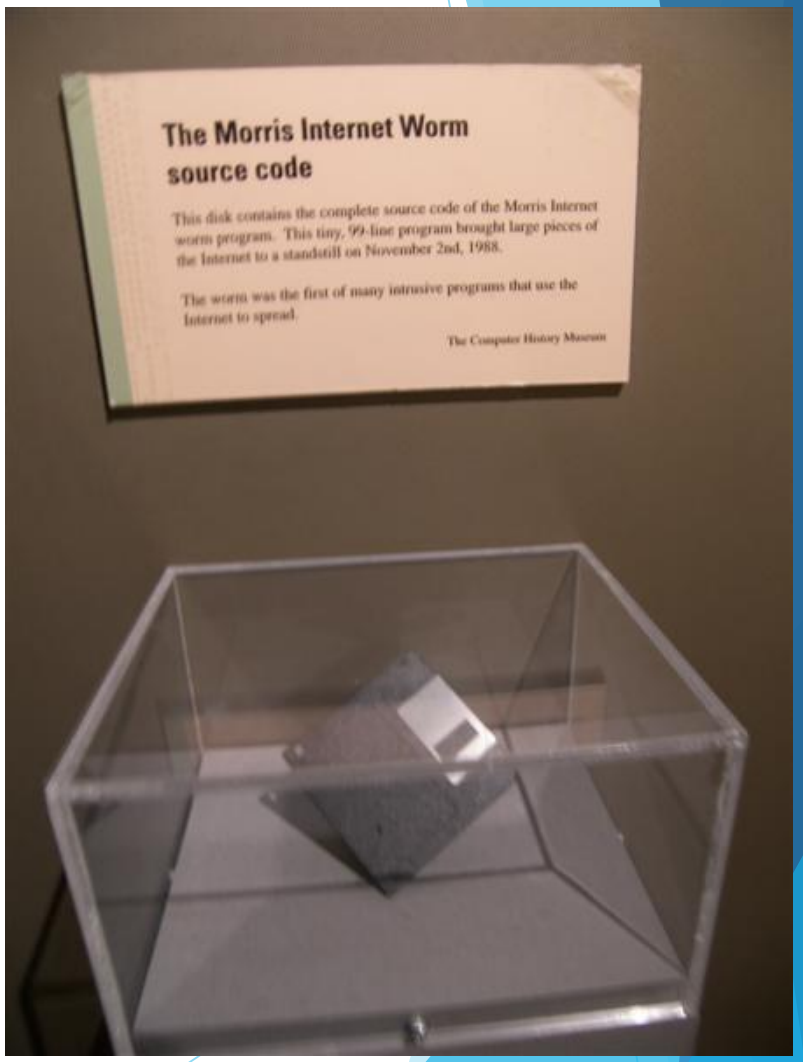
HISTORIE

- 1988 – Morrisův červ
- Autor: Robert T. Morris
- Červ aktivován ze stanice v MIT
- Zranitelnost v Unix / ovlivněn celý internet (až 10% stanic nakaženo)
- Motiv: ?
- Usvědčen dle 1986 computer Fraud and Abuse Act
- Trest: community service, pokuta, 3 roky probace


Virus

HISTORIE

- Vznik PS
  (MIT, Berkeley, Purdue, …)
- Institucionalizace řešení kybernetických bezpečnostních incidentů
  → The CERT® Coordination Center (CERT®/CC)
- CERT®/CC, jakožto pionýr – stále funguje pod Carnegie Mellon University (TM „CERT“)
- V Evropě SURFnet-CERT (1992)




Thug Life

CERT/CSIRT

- Dalšími názvy, s kterými se můžeme setkat jsou například:
  - 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
- V každém státě na vrcholové úrovni nějaký CERT/CSIRT

Rozsah činnosti pracoviště CERT/CSIRT

- V rámci určení pracovního rámce každého pracoviště CERT/CSIRT jsou vždy nejzásadnější tyto tři otázky, které dále definují rozsah činnosti CERT/CSIRT :
  1. Jaké má CERT/CSIRT poslání? (základní principy, strategické cíle, úkoly a priority, …)
  2. Jaká je CERT/CSIRT constituency? (pole působnosti)
  3. Jaké je organizační zakotvení CERT/CSIRT? (definice pozice v rámci interní/externí organizační struktury a systému krizového řízení)

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)

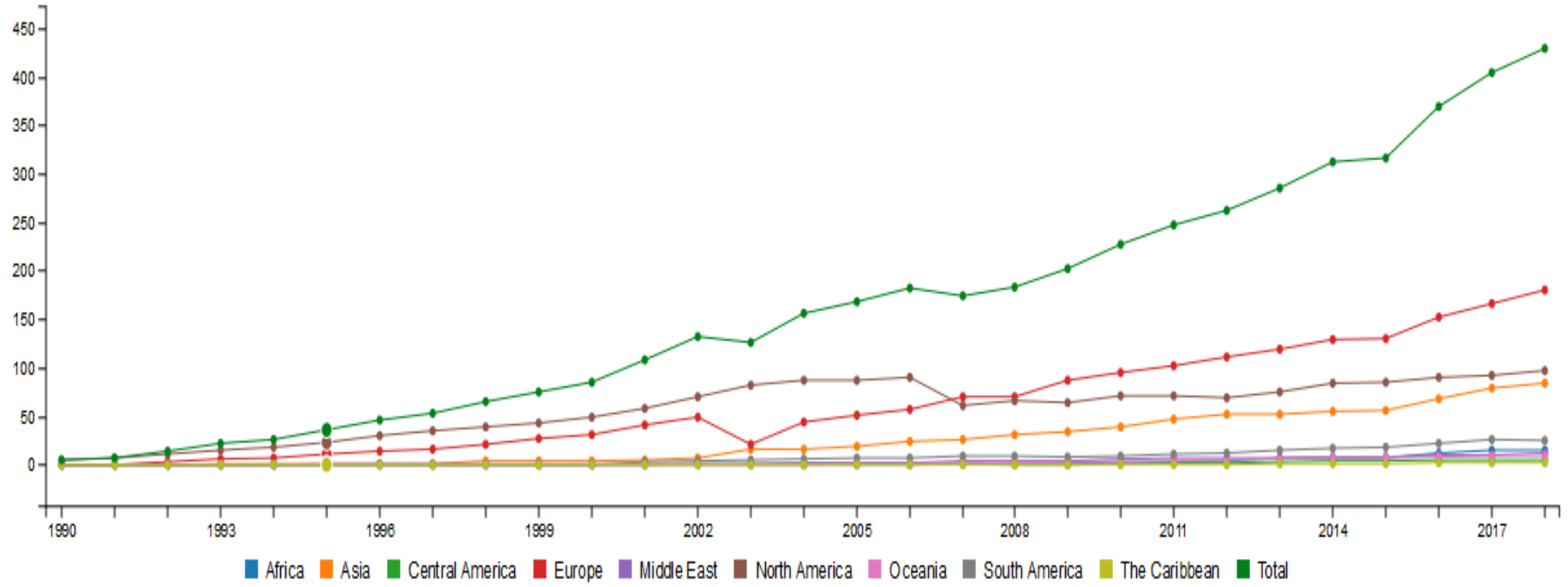
TYPY CERT/CSIRT

- **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)
- …

FIRST

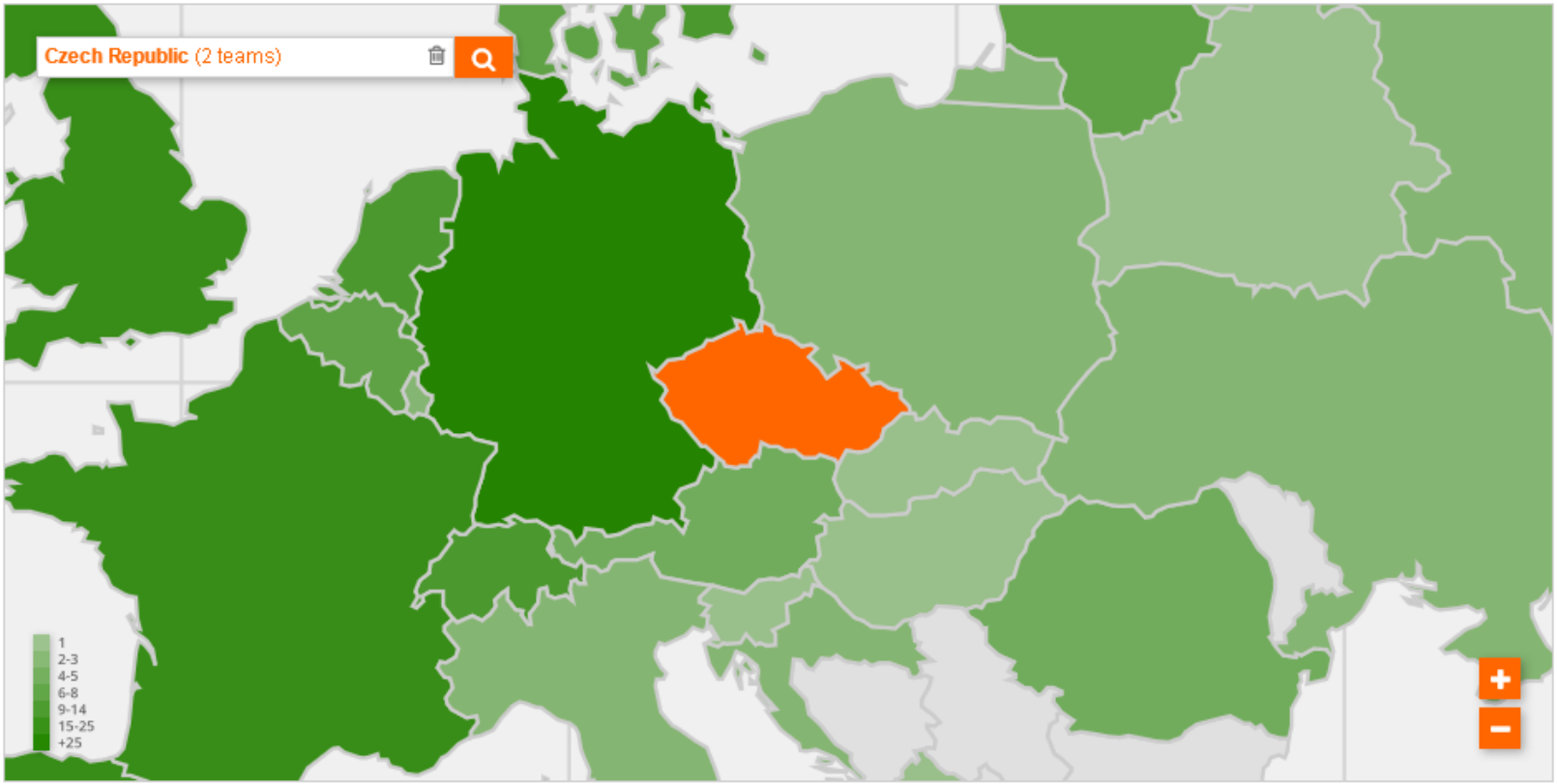
- Založeno 1990
- Forum for Incident Response and Security Teams
- Sdružuje CERT komunitu na globální úrovni
- Hlavním cílem: sdílení informací a zkušeností mezi CERT pracovišti a pomoc při rozsáhlých kybernetických bezpečnostních incidentech
- Aktuálně přes 350 členů
- Status: member

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, …

TI-GÉANT

Czech Republic

ALEF-CSIRT	Accredited (since 14 Nov 2016)
CESNET-CERTS	Accredited (since 27 Jan 2008)
CSIRT-MU	Certified (since 05 Dec 2016)
CSIRT.CZ	Certification Candidate (since 10 Dec 2017)
CZ.NIC-CSIRT	Accredited (since 26 Aug 2010)
GOVCERT.CZ	Accredited (since 21 Aug 2014)
SOCA	Accredited (since 10 Feb 2017)

2CCSIRT	Listed (since: 15 Sep 2014)
ACTIVE24-CSIRT	Listed (since: 09 Feb 2012)
ALEF-CSIRT	Accredited (since: 14 Nov 2016)
AVENTA CSIRT	Listing Candidate (since 04 Oct 2018)
CASABLANCA.CZ-CSIRT	Listed (since: 08 Mar 2014)
CDTCERT	Listed (since: 16 Jul 2014)
CESNETCERTS	Accredited (since: 27 Jan 2008)
CETIN CSIRT	Listed (since: 31 Mar 2017)
Coolhousing CSIRT	Listed (since: 17 Sep 2014)
CRA CSIRT	Listed (since: 09 Nov 2016)
CS-CSIRT	Listed (since: 11 Mar 2016)
CSIRT CSAS	Listed (since: 04 Jul 2018)
CSIRT Merit	Listed (since: 25 Mar 2015)
CSIRT OU	Listed (since: 04 Jul 2018)
CSIRT-MU	Certified (since 05 Dec 2016)
CSIRT-SPCSS	Listed (since: 26 Jun 2018)
CSIRT-VUT	Listed (since: 20 May 2014)
CSIRT.CZ	Certification Candidate (since 10 Dec 2017)
CSOB-Group-CSIRT	Listed (since: 29 Oct 2014)
CZ.NIC-CSIRT	Accredited (since: 26 Aug 2010)
DIAL-CSIRT	Listed (since: 16 Dec 2013)
ELAT CSIRT	Listed (since: 03 May 2018)
FORPSI-CSIRT	Listed (since: 19 Jul 2015)
GOVCERT.CZ	Accredited (since: 21 Aug 2014)
ISPA CSIRT	Listed (since: 13 Aug 2015)
KADRA-CSIRT	Listed (since: 04 Mar 2015)
KBM CSIRT	Listed (since: 13 Dec 2017)
KERNUN CSIRT	Listed (since: 09 Oct 2017)
MASTER.CZ-CSIRT	Listed (since: 12 Dec 2017)
NIXCZ-CSIRT	Listed (since: 13 Dec 2017)
O2.cz CERT	Listed (since: 01 Jan 2014)
SEBET	Listed (since: 25 Oct 2014)
SEZNAM.CZ-CSIRT	Listed (since: 18 Oct 2013)
SOC-Corpus	Accreditation Candidate (since: 13 Aug 2018)
SOC365 CSIRT	Listed (since: 15 May 2018)
SOCA	Accredited (since: 10 Feb 2017)
TMCZ CSIRT	Listed (since: 08 Aug 2016)
TPS-CSIRT	Listed (since: 15 Mar 2017)
VSHOSTING-CSIRT	Listed (since: 21 Jul 2017)
WEB4U-CSIRT	Listed (since: 19 Jul 2015)

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


Kaliningrad
RUSSIA
Vilnius
Gdańsk
Rostock
Hamburg
Berlin
Amsterdam
Poznań
Warsaw
Brest
NETHERLANDS
Hannover
Elbe
GERMANY
POLAND
Wrocław
Leipzig
Brussels
Bonn
Kraków
Vistula
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
Vistula
L'viv
Frankfurt
Luxembourg
Paris
LUX.
Stuttgart
CSIRT.SK
Budapest
CERT-FR
Munich
CERT.at
Graz
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
SWITZ.
LIECH.
Bern
Geneva
Pécs
si·cert
Lyon
Milan
Zagreb
Danube


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


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


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

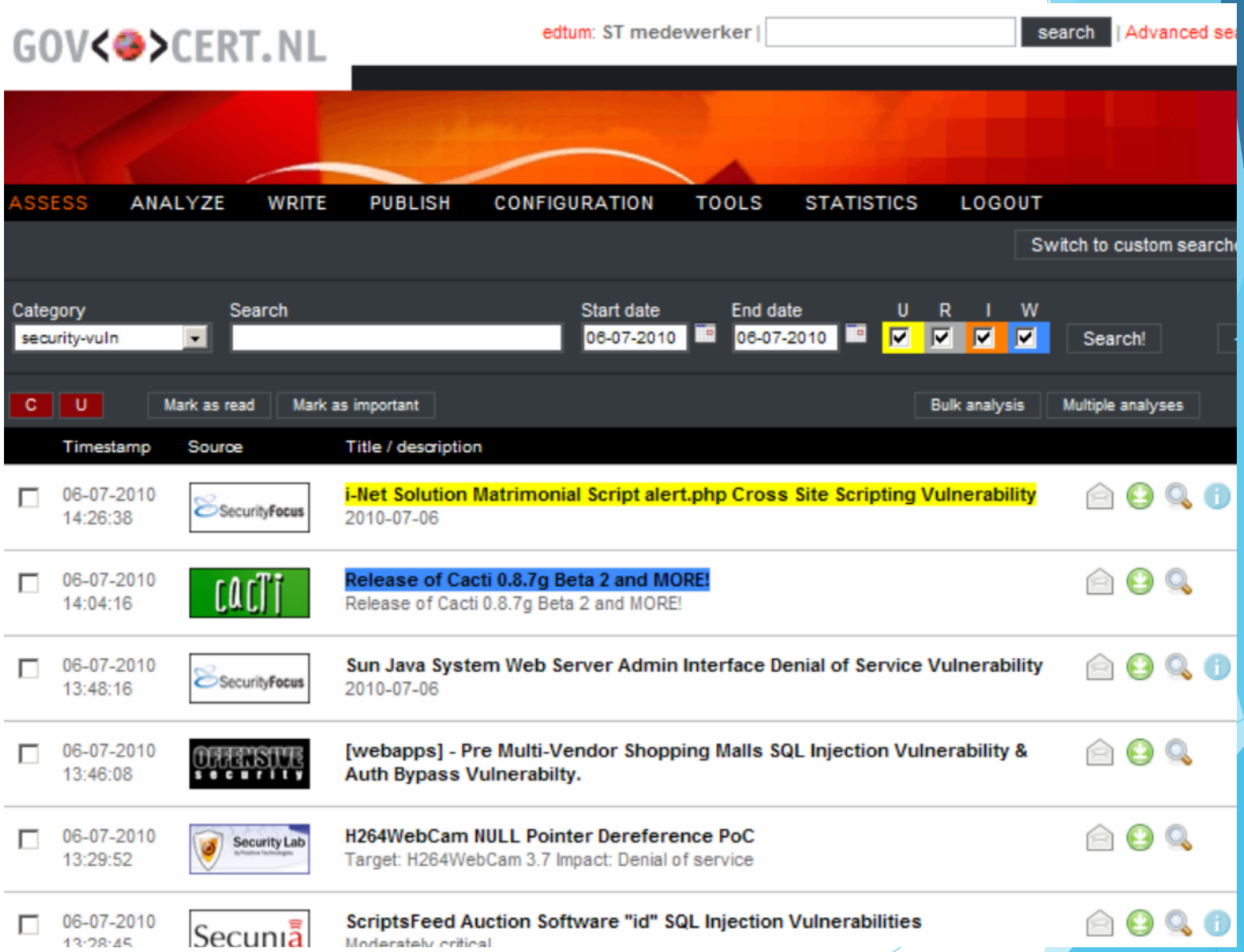

Gdańsk
Hamburg
Berlin
Amsterdam
NETHERLANDS
Poznań
Warsaw
Brest
CERT Bund
CERT.PL
Wrocław
Leipzig
Kraków
CERT.be
L'viv
Luxembourg
Paris
LUX.
CSIRT.SK
Budapest
CERT-FR
Munich
CERT.at
SWITZ.
Graz
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT
Pécs
Geneva
Bern
si·cert
Lyon
Milan
Danube
Zagreb

CERT/CSIRT – činnosti a aktivity

- **Reaktivní služby:** základní element činnosti všech CERT. Tyto služby jsou spouštěny skrze detekovanou/nahlášenou bezpečnostní událost/incident (incident handling, vydávání varování, zvládání zranitelností, manipulace s artefakty, …)
- **Proaktivní služby:** Tyto služby poskytují pomoc a informace za účelem připravit, chránit a zabezpečit systémy v constituency. CERT tak proaktivně přispívá ke snížení počtu incidentů v budoucnu (vývoj bezpečnostních nástrojů, IDS, proaktivní šíření informací, bezpečnostní audity, …)
- **Management kvality bezpečnosti:** služby, které rozšiřují stávající, již zavedené služby / přidaná hodnota (poradenství, analýza rizik, certifikace, vzdělávání/školení, …)

Kultura CERT 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
- Důvěra („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

- 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


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.

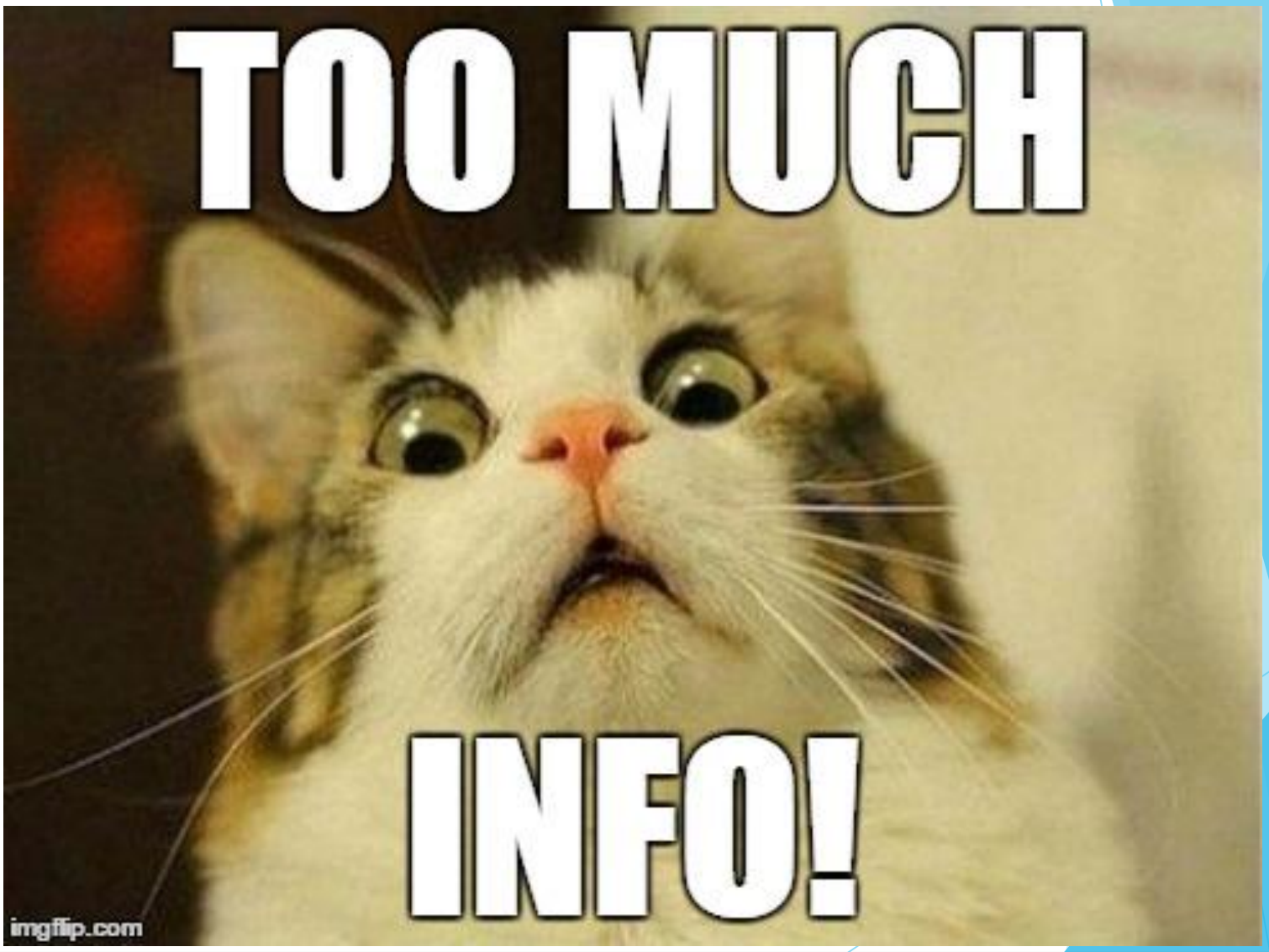
Co se sdílí?

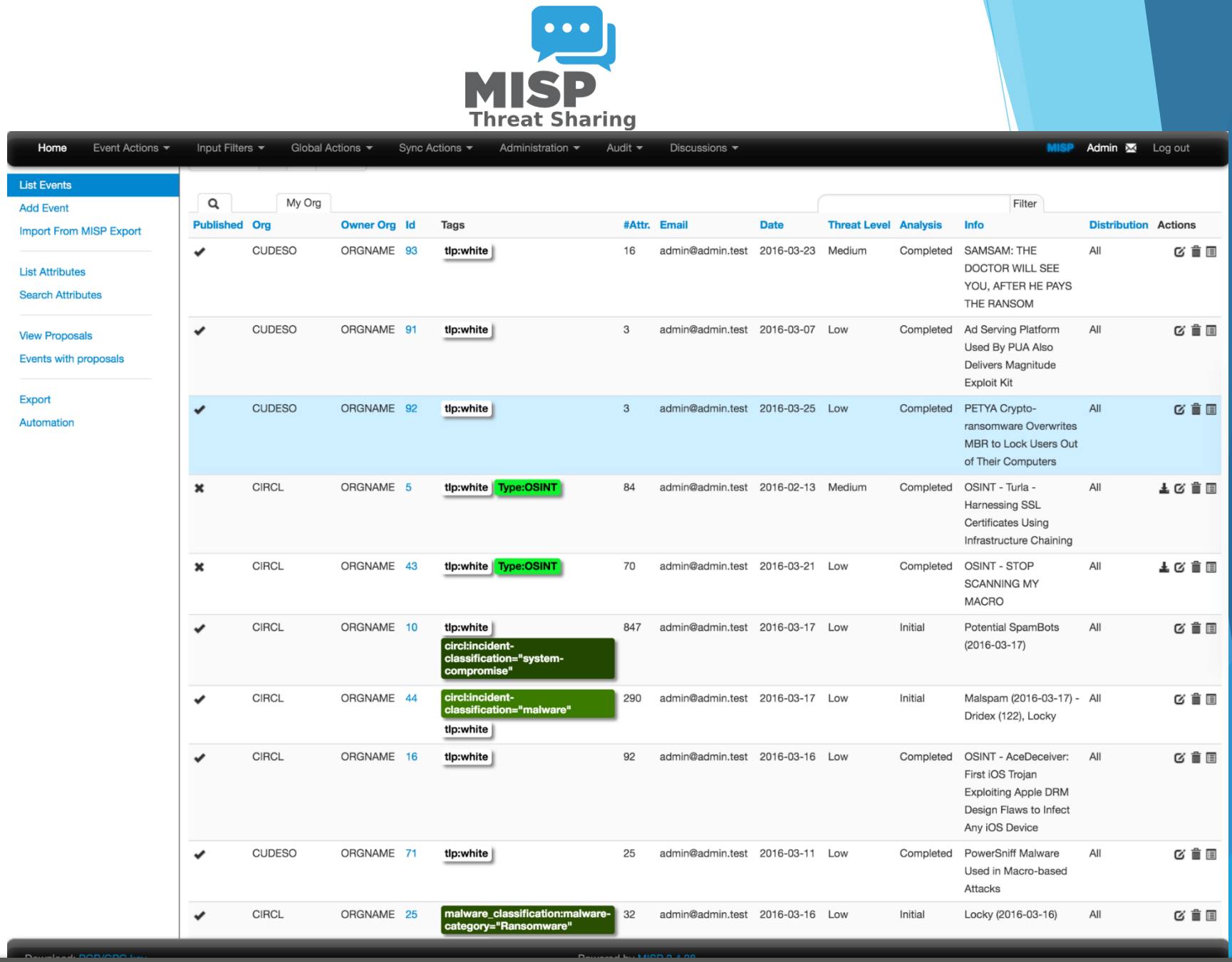
- Indikátory kompromitace (IoCs): virové signatury, škodlivé IP adresy, malware soubory, URL, doménové jména
- Kontextové informace např. o malware kampaních, informace o modu operandi útočníků,
- Případové studie a reporty o incidentech,
- Varování o možných či potenciálních obětech útoku,
- Dešifrovací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

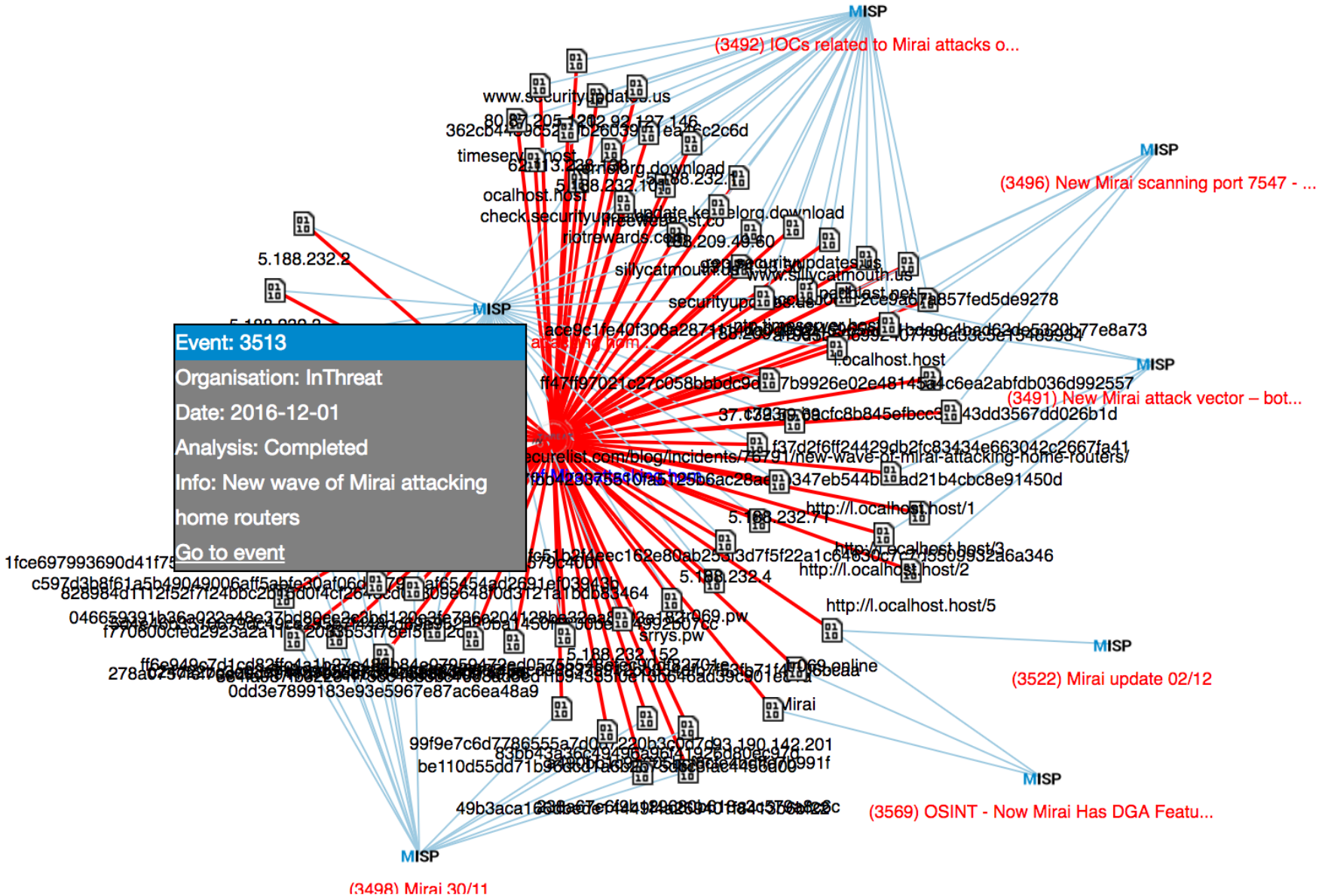
https://www.phishtank.com/

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...
www.securityupdates.us
80.87.205.12
92.127.146
362cb4
timeserver.host
5.188.232.10
ocalhost.host
check.securityupdates.us
riotrewards.com
188.209.49.50
5.188.232.2
MISP
Event: 3513
Organisation: InThreat
Date: 2016-12-01
Analysis: Completed
Info: New wave of Mirai attacking
home routers
Go to event
MISP
(3496) New Mirai scanning port 7547 - ...
www.sillycatmouth.us
MISP
(3491) New Mirai attack vector – bot...
l.ocalhost.host
http://l.ocalhost.host/1
http://l.ocalhost.host/3
http://l.ocalhost.host/2
http://l.ocalhost.host/5
srrys.pw
5.188.232.152
MISP
(3522) Mirai update 02/12
Mirai
99f9e7c6d7786555a7d0
93.190.142.201
be110d55dd71
MISP
(3569) OSINT - Now Mirai Has DGA Featu...
MISP
(3498) Mirai 30/11

Stát vs. CERT/kybernetická bezpečnost

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

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

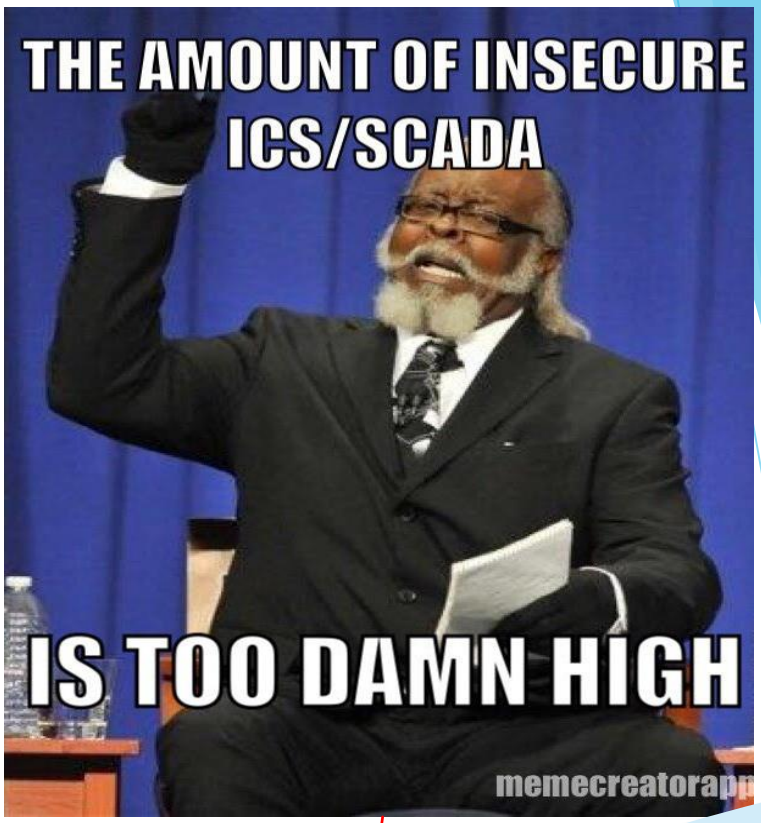
ICS/SCADA cyber security

< 2011

2011

Ted'

ICS/SCADA
cyber security



< 2011

2011
OMG
STUXNET

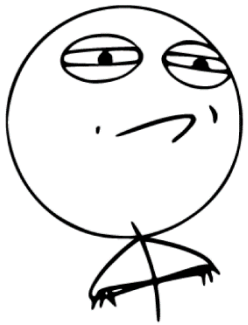
Ted'

Stát vs. CERT/kybernetická bezpečnost

- Rozšíření ve dvou směrech:
  Vertikálním: od expertní úrovně k úrovni politické
  Horizontálním: z USA a dalších pár vyspělých evropských zemí do téměř všech ostatních států světa
- Nejnovější trend: řešit kybernetickou bezpečnost skrze strategicko-vojenskou optiku (aktivní protiopatření, kybernetická obrana, kybernetické zastrašování, …)

Vybrané výzvy: CERT jako politický aktér

- Povaha CERT komunity akademická vs. fungování státního aparátu
- Národní/vládní CERT musí nacházet ideální rovnováhu mezi fungováním v rámci CERT komunity a plněním politických cílů a povinností
- Národní/vládní CERT mají specifickou „netechnickou“ agendu
- Nové výzvy….



Vybrané výzvy: Sdílení informací a vzájemná důvěra

- Otázka odpovědnosti / poškození reputace / důvěry constituency
- Vnitrostátní právní předpisy (např. zákony o datové lokalizaci)
- 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

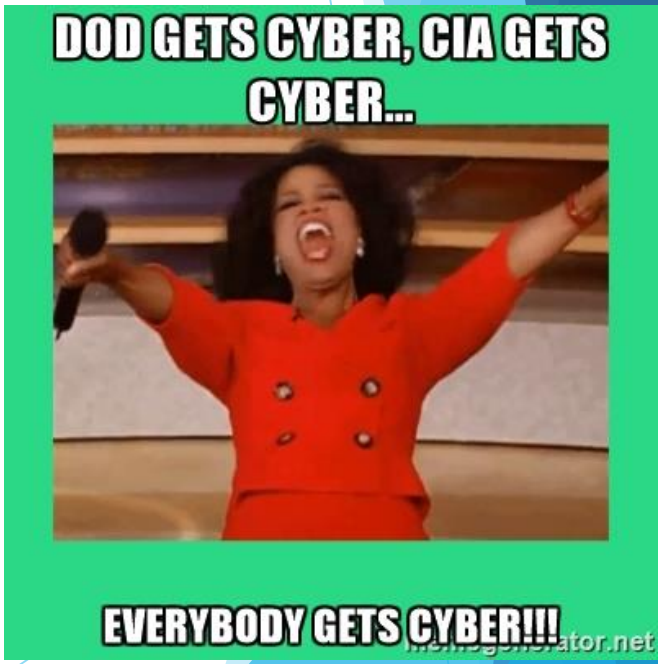
Vybrané výzvy: Komercionalizace kybernetické bezpečnosti

- 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

Vybrané výzvy: Rostoucí CERT komunita / politizace kybernetické bezpečnosti

- Status národní/vládní CERT sebou nese mnoho zodpovědnosti, ale také benefitů (zejména lepší přístup k finančním prostředkům, citlivým informacím, …)
- Resorty/instituce mohou usilovat o převzetí agendy / vstup aktérů, kteří nejsou a nemají být součástí CERT komunity
- Volby mohou mít zásadní vliv na směřování a rozvoj CERT
  → hrozba rozkladu celého konceptu kybernetické bezpečnosti v zemi během pár dní
- CERT obětí politického boje – negativně působí na bezpečnostní situaci nejen na národní, ale i na mezinárodní úrovni



Vybrané výzvy: Pozice CERT v systému zajišťování národní bezpečnosti

Russian GOV CERT

- Rozdílné vnímání kybernetické bezpečnosti a kybernetických hrozeb
- GOV-CERT.RU is tasked with information security and making *"recommendations on how to neutralize relevant information security threats,"* which include the use of information and communications technology to interfere *"with the internal affairs of the sovereign state, [and] violation of public order,"*
- Může vést k porušování lidských práv, svobody slova, apod.

→ ostatní CERT se mohou vyhýbat sdílení informací, spolupráci

Vybrané výzvy: Kyberprostor jako nová operační (vojenská) doména

- Aktivnější role státu v kyberprostoru / používání aktivních prostředků a nástrojů:
  - Zajišťování kybernetické obrany v reálném čase (schopnost reagovat efektivně a dostatečně rychle)
  - Schopnost aktivní identifikace a rekognoskace nepřítele v kyberprostoru (spočívá v lokálním i vzdáleném shromažďování informací, tj. zisk logů či dat ze síťového provozu; OSINT; monitoring zranitelností, aj.)
  - Schopnost provádět odvetné (tzv. hacking back) i preemptivní kybernetické útoky (např. nasazení malware, modifikace síťového provozu, provádění DoS/DDoS útoků proti útočníkovi, apod.)
- Nedotýká se přímo CERT, ale má vliv na efektivitu jeho práci / sdílení informací, důvěru, apod. = jaká role v KO?

ROLE STÁTU V ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI

Kybernetická obrana

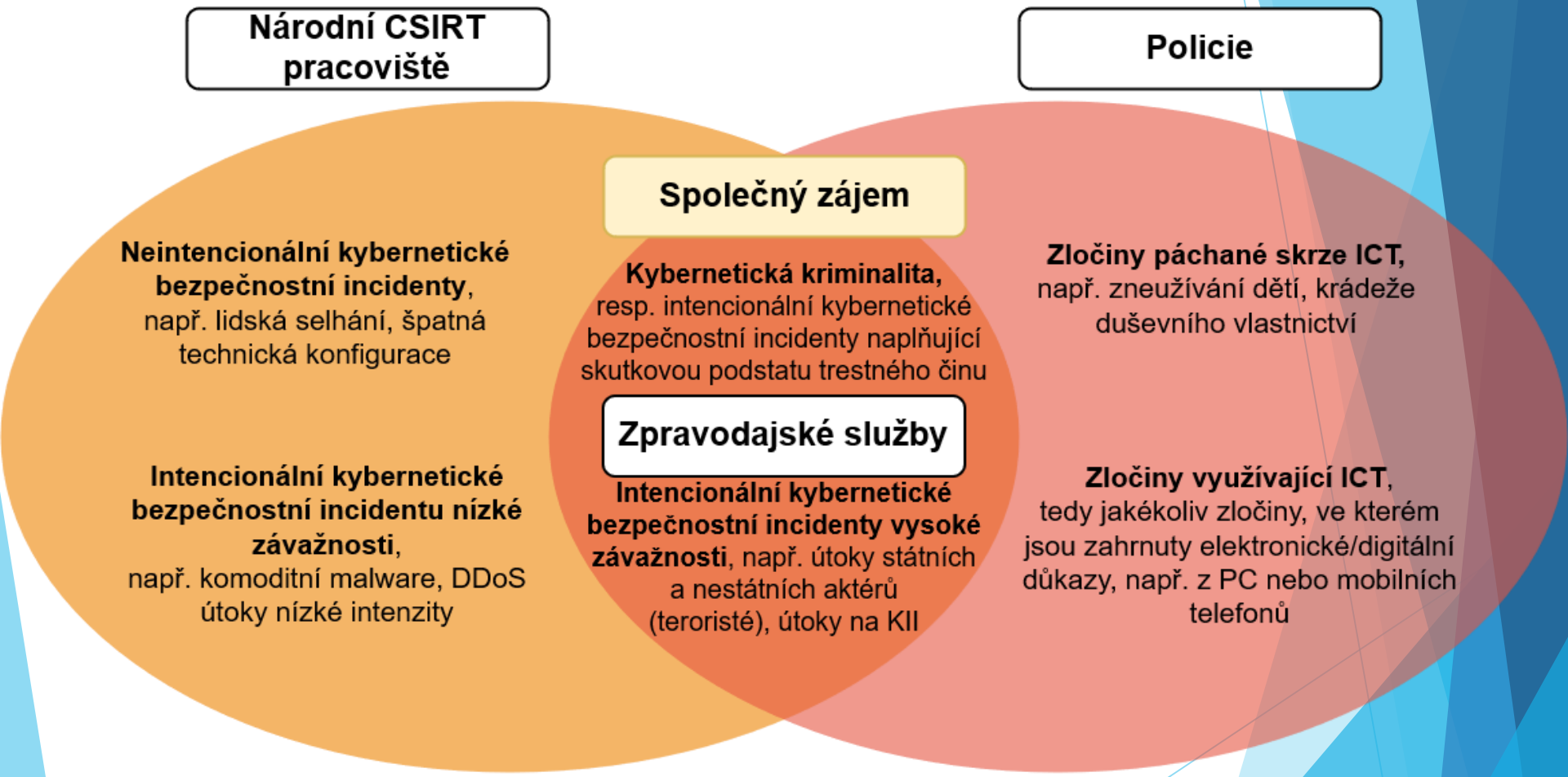
Ochrana KII

Kybernetická kriminalita

Působení zpravodajských služeb

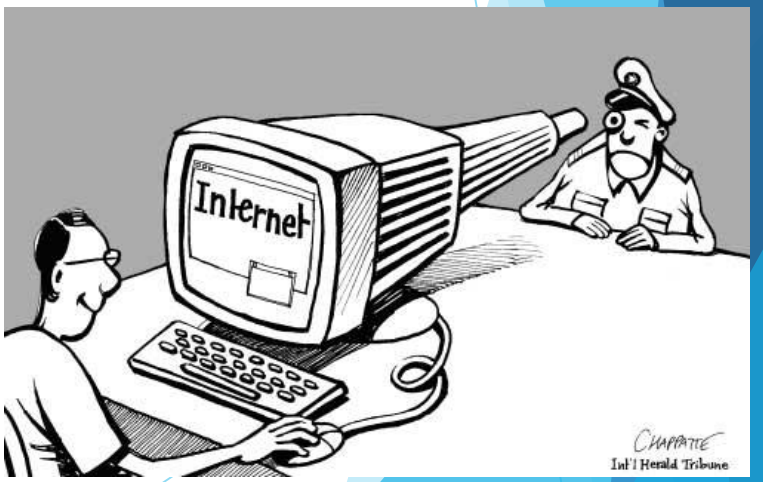
KYBERNETICKÁ BEZPEČNOST STÁTU

Národní CERT vs. zpravodajské služby a policie



Národní CERT vs. zpravodajské služby a policie

- Společný cíl: zabezpečení kyberprostoru
- Rozdílný mandát / úroveň expertízy
- **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



June 2010

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.

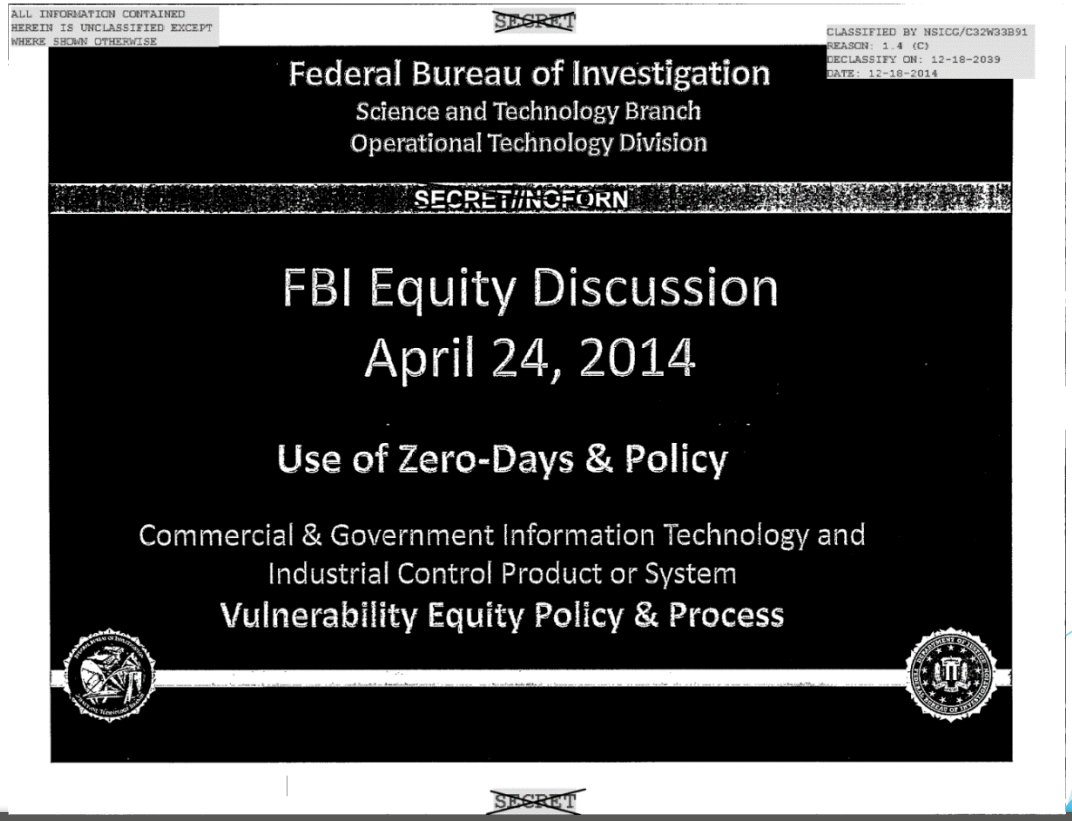
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Národní CERT vs. zpravodajské služby a policie

- Národní/vládní CERT – obnova systému, odstranění zranitelností/snižování rizik
  - ***Ochrana své constituency je esenciálním úkolem CERT/CSIRT***
- LE – sběr důkazů, přisouzení útoků a stíhání zločinců
- IA – přisouzení útoků, sběr/analýza infa ohledně národní bezpečnosti (vojenská, zahraniční politika)
- **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?

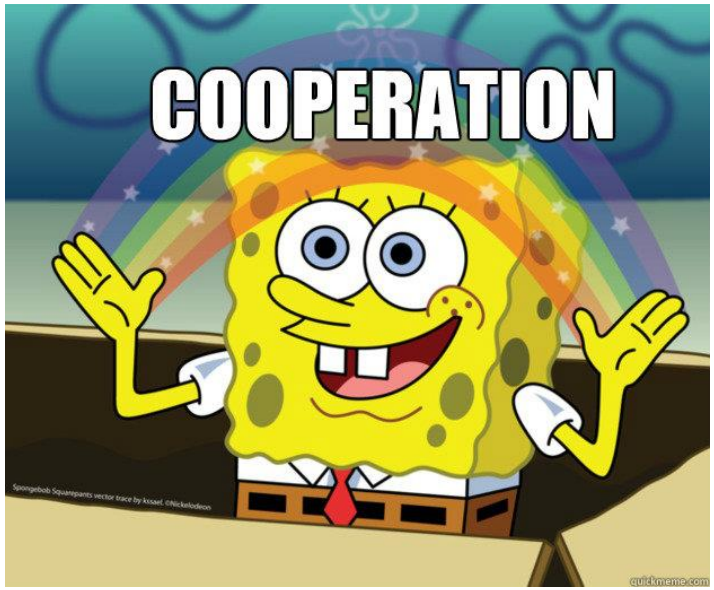
Národní CERT vs. zpravodajské služby a policie

- **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



Historie CERT komunity v ČR

- 2004 – vznik CESNET-CERTS:
  1. oficiálně konstituovaný CERT tým v ČR
- 2007 – CSIRT.CZ byl vybudován v rámci grantu
  „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“
  (2007 – 2010: financováno MVČR)
  - **Řešitelé (výherci výběrového řízení):**
    - Matematicko-fyzikální fakulta UK
    - Právnická fakulta UK
    - Fakulta sociálních věd UK
    - České vysoké učení technické
    - **CESNET**
    - NESS
- Cílem vybudování modelového pracoviště typu CSIRT a ověření schopnosti spolupráce provozovatelů sítí a služeb v ČR při řešení bezpečnostních incidentů

Historie CERT komunity v ČR / zapojení státu

- 2007 – po vybudování nezbytného technické a organizačního zázemí došlo za podpory týmu CESNET-CERTS k akceptaci týmu CSIRT.CZ světovou komunitou (Trusted Introducer)
- → CSIRT.CZ začal v ČR suplovat chybějící vrcholový (národní/vládní) CERT tým
- Formální existence vrcholového týmu se ukázala být nutná
- 2010 – MVČR podepsalo se sdružením CZ.NIC Memorandum → **zřízen oficiálně Národní CSIRT (CSIRT.CZ)**
- 2010 – vláda ČR schválila usnesení č. 205 o řešení problematiky kybernetické bezpečnosti a ustanovila **MVČR gestorem** kybernetické bezpečnosti **(zřízení CERT plánováno)**
- 2011 – vláda ČR schválila usnesení č. 781 jímž ustavila **NBÚ gestorem** kybernetické bezpečnosti **(vznik GovCERT.CZ), …**

CERT komunita v ČR: aktuální stav

- TOP úroveň: Národní CSIRT.CZ / vládní GovCERT.CZ
- 40 CERT/CSIRT v ČR (vysoký počet)
- Důvody:
  - Dlouhodobá podpora a osvěta komunity ve vytváření CERT/CSIRT (např. semináře a kurzy CZ.NIC akademie)
  - Pomoc a podpora zejména u constituency GovCERT.CZ
  - Projekt Fénix (NIX.CZ, smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity.)

FENIX

PROČ VSTOUPIT

- Stanete se součástí týmu, jehož členové určují trendy v oblasti síťové bezpečnosti
- Ukážete, že vám bezpečnost vašich zákazníků není lhostejná
- Zapojíte se do unikátního projektu, který oceňuje odborná část internetové komunity

PODMÍNKY PRO VSTUP

ORGANIZAČNÍ

- Aktivní účast na pracovních skupinách/hlasování v rámci projektu FENIX
- 24/7 dohledové středisko
- CERT/CSIRT tým s patřičným statusem
- Implementace vnitřních procesů pro řešení incidentů
- A další (dokument v PDF)

TECHNICKÉ

- Plně redundantní přípojky do nejméně dvou uzlů NIX.CZ
- Síť využívá protokolů IPv4 a IPv6
- Domény podepsané pomocí technologie DNSSEC
- Zapojení do systému RTBH filteringu
- Využívá Route Serveru provozovaného v rámci projektu FENIX
- A další (dokument v PDF)

DOPORUČENÍ

- Získání doporučení od dvou stávajících členů
- Předložení prohlášení o splnění všech technických a organizačních podmínek
- A další (dokument v PDF)

FENIX

PROČ VSTOUPIT

- Stanete se součástí týmu, jehož členové určují trendy v oblasti síťové bezpečnosti
- Ukážete, že vám bezpečnost vašich zákazníků není lhostejná
- Zapojíte se do unikátního projektu, který oceňuje odborná část internetové komunity

PODMÍNKY PRO VSTUP

ORGANIZAČNÍ

- Aktivní účast na pracovních skupinách/hlasování v rámci projektu FENIX
- 24/7 dohledové středisko
- CERT/CSIRT tým s patřičným statusem
- Implementace vnitřních procesů pro řešení incidentů
- A další (dokument v PDF)

TECHNICKÉ

- Plně redundantní přípojky do nejméně dvou uzlů NIX.CZ
- Síť využívá protokolů IPv4 a IPv6
- Domény podepsané pomocí technologie DNSSEC
- Zapojení do systému RTBH filteringu
- Využívá Route Serveru provozovaného v rámci projektu FENIX
- A další (dokument v PDF)

DOPORUČENÍ

- Získání doporučení od dvou stávajících členů
- Předložení prohlášení o splnění všech technických a organizačních podmínek
- A další (dokument v PDF)

Případová studie: GovCERT.CZ

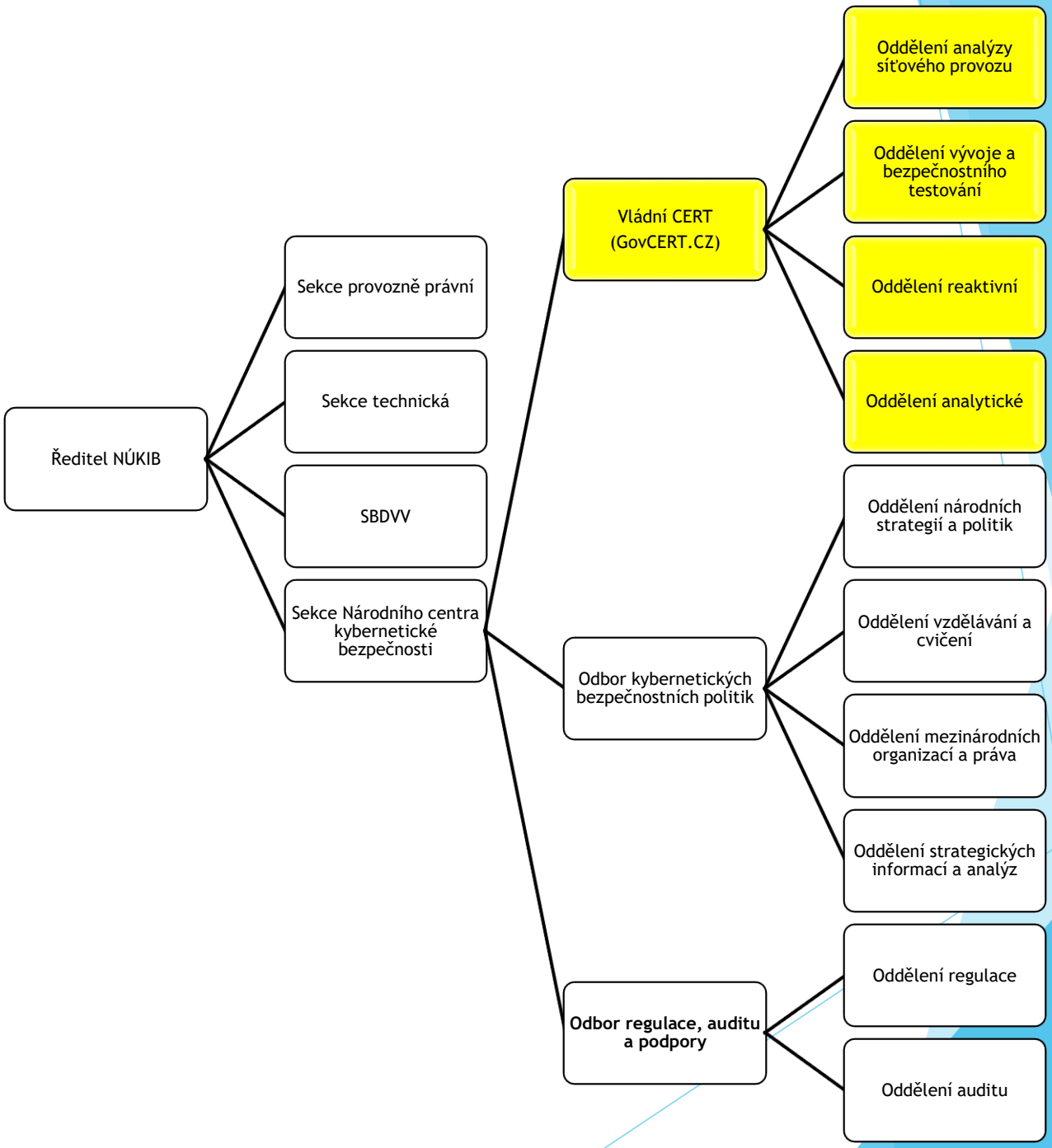
1) Poslání?
2) Constituency?
3) Organizační zakotvení?
4) Rozsah poskytovaných služeb?

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)

Organizační zakotvení

- **Zakotvení:** NÚKIB / OKBP+ORAP
- **Struktura týmu:**
  - Zpracování incidentů
  - Vývoj a bezpečnostní testování
  - Síťová bezpečnost
  - Analytická skupina

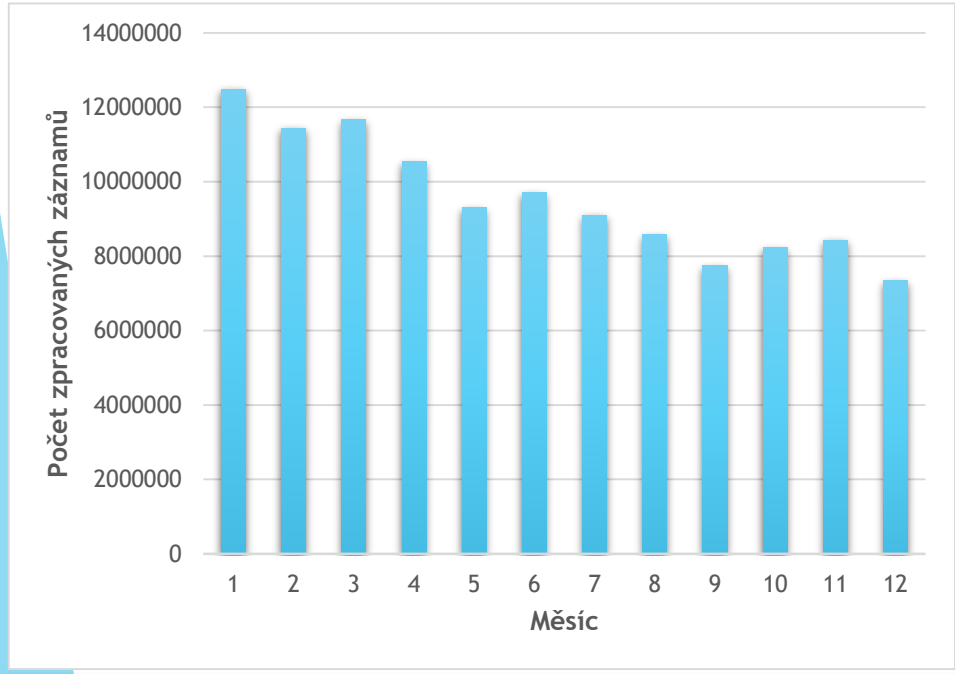

Ředitel NÚKIB
Sekce provozně právní
Sekce technická
SBDVV
Sekce Národního centra kybernetické bezpečnosti
Vládní CERT (GovCERT.CZ)
Oddělení analýzy síťového provozu
Oddělení vývoje a bezpečnostního testování
Oddělení reaktivní
Oddělení analytické
Odbor kybernetických bezpečnostních politik
Oddělení národních strategií a politik
Oddělení vzdělávání a cvičení
Oddělení mezinárodních organizací a práva
Oddělení strategických informací a analýz
Odbor regulace, auditu a podpory
Oddělení regulace
Oddělení auditu

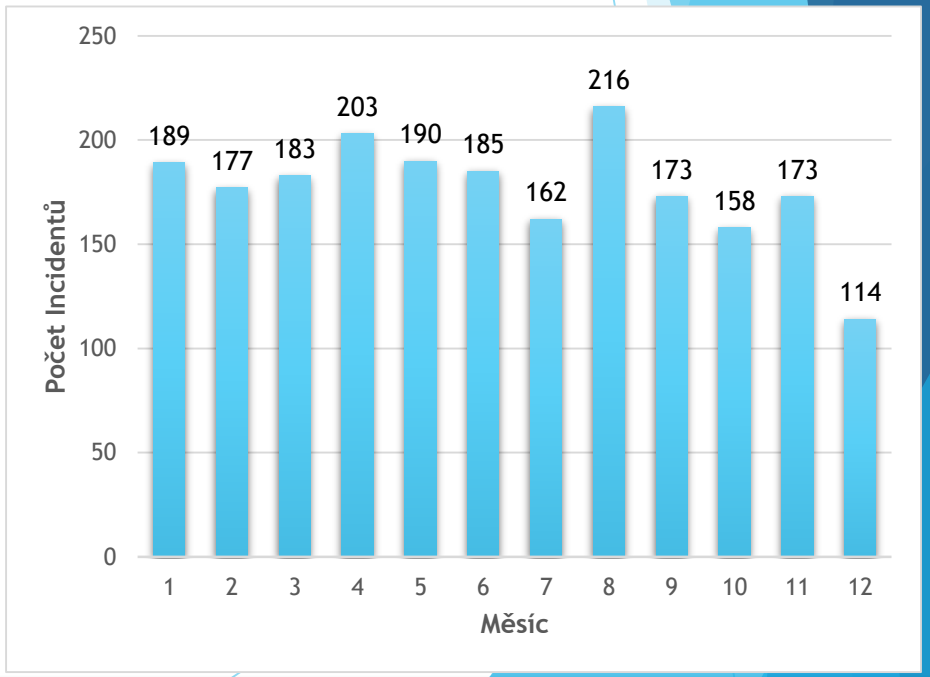
Oblasti zaměření

- **SCADA/ICS systémy**
- **Penetrační testování**
- **Forenzní úkoly**
- **Analýza malware a reverzní inženýrství**
- Virtuální prostředí a cloudová řešení
- Bezpečný vývoj a databázové systémy
- UNIXové systémy
- Windows systémy
- Síťová bezpečnost a analýza síťového provozu
- Honeypoty

Zpracování incidentů

- Hlášené incidenty přibližně 30 měsíčně
- Stabilní trend





Aktuální situace

- Rozsáhlé phishingové kampaně
- Velké množství škodlivého kódu, převážně ransomware
- Špionážní malware
- Rozložení typů incidentů zůstává stejné

Odstranit zprávu po čtení! Spam ×

polit-pgs-prez@fss.muni.cz
komu: polit-pgs-prez

Proč je tato zpráva ve spamu? Podobá se zprávám, které byly dříve označeny jako spam.

Nejde o spam

Ahoj!
Jsem členem mezinárodní hackerské skupiny.

Jak jste asi pravděpodobně uhodli, váš účet z domény@domain.com byl napaden, protože Poslal jsem vám e-mail z vašeho účtu.

V období od 5. července 2018 do 21. září 2018 jste byli infikováni virem, který jste vytvořili, prostřednictvím navštívených webových stránek pro dospělé.
Zatím máme přístup k vašim vzkazům, účtům sociálních médií a poslům.
Máme však úplné skládky těchto dat.

Jsme si vědomi svých malých a velkých tajemství ... jo, máte je.
Zaznamenali jsme a zaznamenávali vaše akce na pornografických webových stránkách. Váš vkus je tak divný, víte ..

Ale klíčovou věcí je, že jsme někdy zaznamenali vás s vaší webovou kamerou a synchronizovali nahrávky s tím, co jste sledovali!
Myslím, že nemáte zájem ukázat toto video svým přátelům, příbuzným a vašemu intimnímu ...

Přeneste 250$ do naší Bitcoin peněženky: 139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ
Garantuji, že po tom budeme smazat všechny vaše "data": D

Po přečtení této zprávy se spustí časovač. Máte 48 hodin na zaplacení výše uvedené částky.

Vaše údaje budou vymazány po převodu peněz.
V opačném případě budou všechny vaše záznamy a videozáznamy automaticky zaslány všem vašim kontaktům, které jsou na vašem zařízení nalezeny v okamžiku infekce.

Měli byste vždy myslet na vaši bezpečnost. Doufáme, že vás tento případ naučí udržovat tajemství.

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

Aktuální projekty

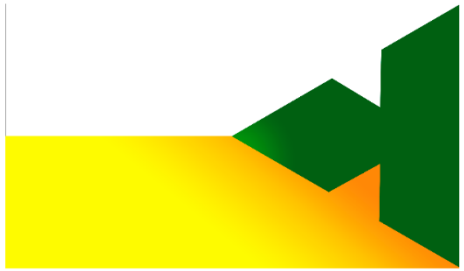
- Forenzní laboratoř
- Laboratoř škodlivého kódu
- Skenování zranitelností (OWASP)
- Penetrační testování
- ICS / SCADA laboratoř
- Budování scrubbing centra
- Koordinační centrum pro české bezpečnostní týmy
- Organizace a účast na národních i mezinárodních cvičeních kybernetické bezpečnosti

Cyber Czech 2016 / 2017

- Technické národní cvičení v kyberbezpečnosti
- Národní centrum kybernetické bezpečnosti ve spolupráci s Masarykovou univerzitou
- Red/blue tým cvičení s více než 60 účastníky
- Každý tým odpovědný za virtuální prostředí s více než 20 stanicemi a servery
- Komponenty hodnocení:
  - Automatické skórování dostupnosti
  - Negativní ohodnocení za úspěšný útok provedený red týmem
  - Udržení prostředí použitelného pro práci pro koncové uživatele
  - Sdílení informací a spolupráce s ostatními blue týmy
  - Spolupráce a komunikace se zástupci médií
  - Právní scénář

Cyber Czech 2016 / 2017

Cyber Czech 2016 / 2017



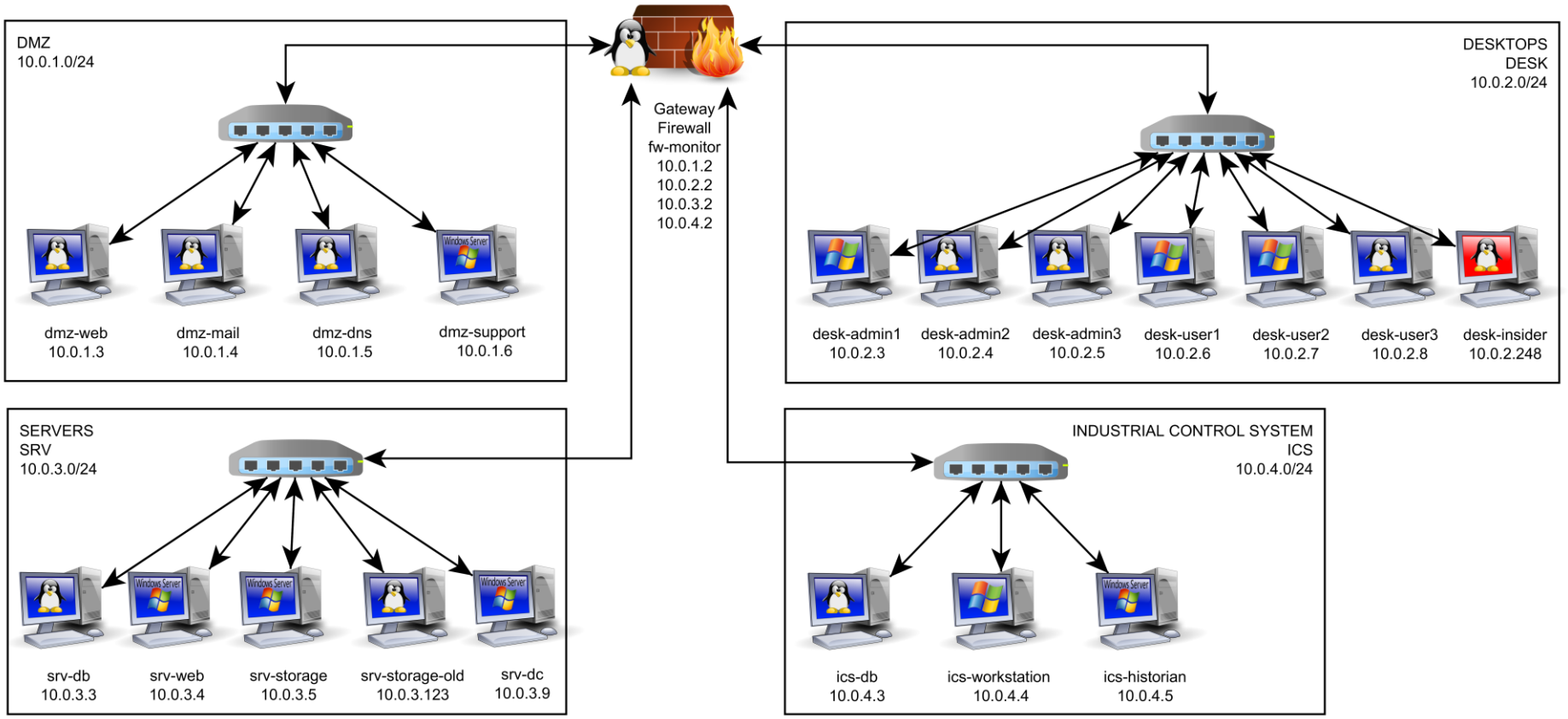
Pilsneria

Sauronia

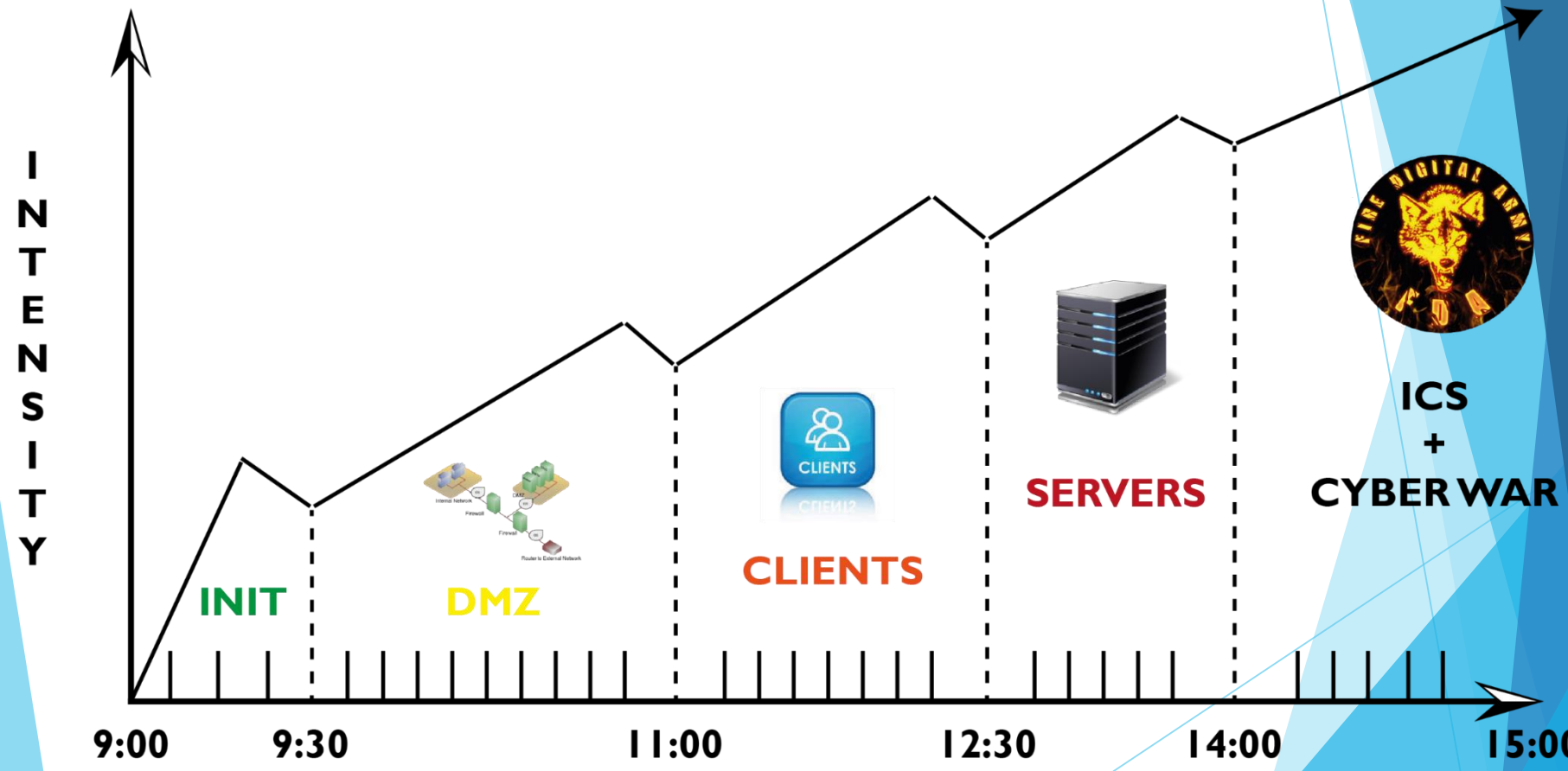
RAP

RAILWAY ADMINISTRATION OF PILSNERIA

Cyber Czech 2016 / 2017



Cyber Czech 2016 / 2017



Cyber Czech 2016 / 2017

Děkuji za pozornost!

Roman Pačka

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