

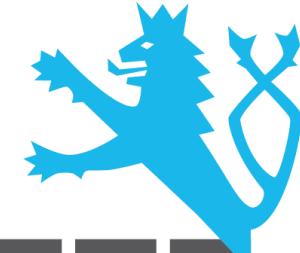
10100101011010100010110100101101  
10101000110100101101101001001011010  
10101000110100101101101001001101001010



# Sdílení informací public-private o zranitelnostech, hrozbách a incidentech

Pavel Titěra

GovCERT.CZ  
NCKB  
NBÚ



nckb

Národní centrum  
kybernetické  
bezpečnosti

10100101011010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

# CO SDÍLET

- Sdílení informací
  - Kybernetické incidenty
  - Aktuální zranitelnosti, hrozby, IoC, apod.
  - Analýzy
  - Externí spolupráce při řešení incidentů
- Sdílení nástrojů, technických schopností
- Sdílení zkušeností - společná kybernetická cvičení
- Vzdělávání
- Stáže



1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

# NÁRODNÍ CVIČENÍ

- Strategic Decision Making Course & Exercise on Cyber Crisis Management
  - 16. - 18. června 2015 (Praha)
  - Cílem table-top cvičení: prověřit komunikaci a spolupráci
- Cyber Czech 2015
  - 6.-7. října 2015 (Brno)
  - Technicky zaměřené - Red/Blue týmy
  - 20 osob (5 týmů)
  - Fiktivní scénář
  - Cílem chránit svěřené systémy před kyber. útoky, kopírovat postupy podle zákona č. 181 Sb. o KB



1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

## ZDROJE INFORMACÍ

---

- Veřejně dostupné
  - Informační zdroje lidsky čitelné (RSS, weby, twitter, fóra)
  - Strojově zpracovávané zdroje
- Uzavřené skupiny, komunity
  - Diskusní fóra
  - Mailing listy
- AV společnosti a bezp. týmy
  - Zprávy
  - Analýzy
- Placené zdroje
- Naše vlastní systémy (Honeypoty, sondy)

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101



## KONZULTAČNÍ ČINNOST

---

- SCADA/ICS systémy
- Forenzní analýza
- Analýza malware
- Penetrační testování
- Virtualizované prostředí a cloudová řešení
- Sítová bezpečnost
- Operační systémy Windows a UNIXového typu
- Databázové systémy
- Bezpečné programování

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101

## S KÝM SDÍLET

---

- V rámci ČR
  - Constituency
  - CSIRT.CZ
  - CIRC MO
  - CSIRT-MU, CSIRT-VUT
  - Další CERT týmy
  - Veřejnost
- Mimo ČR
  - Zahraniční CERT týmy
  - Jižní Korea
  - USA
  - Izrael
- Komunita CERT týmů
  - FIRST (Forum of Incident Response and Security Teams)
  - TF-CSIRT (Task Force zastřešená GÉANT, dříve TERENA)
    - Trusted Introducer

10100101011010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

## ČESKÉ CERT/CSIRT TÝMY

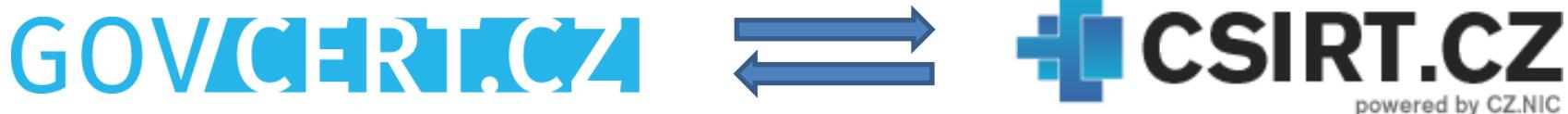
- 2CCSIRT Listed (since 2014)
- ACTIVE24-CSIRT Listed (since 2012)
- ALEF-CSIRT Listed (since 2015)
- CASABLANCA.CZ-CSIRT Listed (since 2014)
- CDT-CERT Listed (since 2014)
- CESNET-CERTS Accredited (since 2008)
- Coolhousing CSIRT Listed (since 2014)
- CSIRT Merit Listed (since 2015)
- CSIRT-MU Accredited (since 2011)
- CSIRT-VUT Listed (since 2014)
- CSIRT.CZ Accredited (since 2011)
- CSOB-Group-CSIRT Listed (since 2014)
- CZ.NIC-CSIRT Accredited (since 2010)
- DIAL-CERT Listed (since 2013)
- FORPSI-CSIRT Listed (since 2015)
- GOVCERT.CZ Accredited (since 2014)
- ISPA CSIRT Listed (since 2015)
- KAORA-CSIRT Listed (since 2015)
- O2.cz CERT Listed (since 2014)
- SEBET Listed (since 2014)
- SEZNAM.CZ-CSIRT Listed (since 2013)
- WEB4U-CSIRT Listed (since 2015)



101001010110101010001011010010110110100101101  
1010100011010010110110100100101101010101010  
1010100011010010110110110110100100110100101010

## SPOLUPRÁCE S NÁRODNÍM CERT

- CSIRT.CZ provozovaný sdružením CZ.NIC
  - Národní CERT tým
  - Koordinační role
  - Plní funkci poslední instance
- NCKB je Point of contact pro ČR v oblasti IT Security
- Předávání incidentů spadajících do pole působnosti druhého týmu



## OMEZENÍ SDÍLENÍ DAT

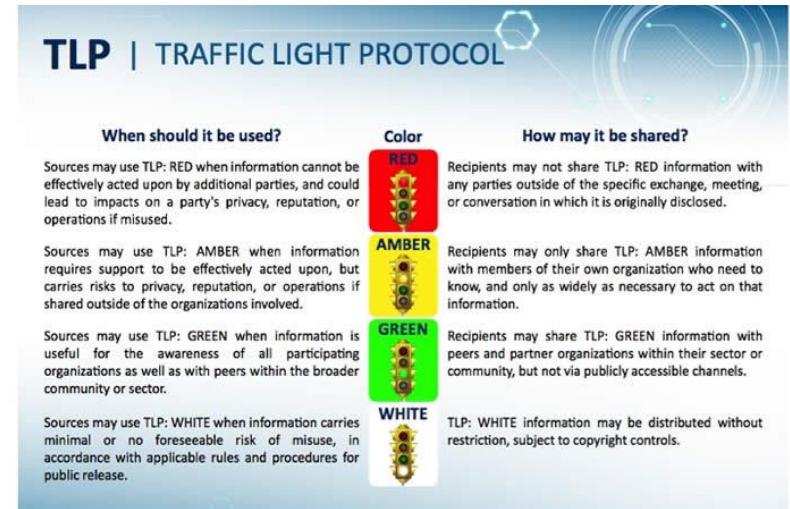
---

- Základní princip „need to know“
- Směrem k CERT týmu
  - Citlivá data (např. data o klientech) mohou být anonymizovaná
  - Součástí formuláře hlášení KBI
- Směrem od CERT týmu
  - Pouze se spolupracujícími CERT týmy,
  - Pokud je povoleno (viz formulář KBI, NDA, TLP,...)
  - Citlivá data vyjmuta/anonymizována

10100101011010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

# PROTOKOL TLP

- Traffic Light Protocol
- De facto standard
- Definuje míru sdílení informace
- 4 úrovně:
  - RED („face to face“)
  - AMBER („need to know“, v rámci organizace)
  - GREEN (komunita)
  - WHITE (veřejné)



1010010101101010100010110100101101  
10101000110100101101101001001011010  
101010001101001011010110100100110100101

# KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

---

- E-mail
  - [cert.incident@govcert.cz](mailto:cert.incident@govcert.cz) – řešení incidentů, formulář
  - [cert@govcert.cz](mailto:cert@govcert.cz) – konzultace, informativní
- Web <http://govcert.cz>
  - Aktuality
  - Zranitelnosti
  - Měsíční bulletin
  - Legislativa, dokumenty

# PROJEKT

## Automatizace sdílení dat o incidentech

- spolupráce s O2

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:annotation>
        <xs:documentation xml:lang="cz">Schema definuje formular pro hlaseni kybernetickeho bezpecnostniho incidentu GovCERT.CZ</xs:documentation>
        <xs:appinfo>
            <version>0.1</version>
        </xs:appinfo>
    </xs:annotation>
    <!-- Zakladni Typy -->

    <xs:simpleType name="STmiraOchranyInformace">
        <xs:annotation>
            <xs:documentation xml:lang="cz">Osobní - seznam příjemců (v rámci úřadu)</xs:documentation>
            <xs:documentation xml:lang="cz">Omezená distribuce (v rámci komunity)</xs:documentation>
            <xs:documentation xml:lang="cz">Neomezeno (veřejně)</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:normalizedString">
            <xs:enumeration value="Osobni" />
            <xs:enumeration value="Omezena" />
            <xs:enumeration value="Neomezeno" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="STtlp">
        <xs:annotation>
            <xs:documentation xml:lang="cz">TLP - Traffic Light Protocol</xs:documentation>
            <xs:documentation xml:lang="cz">zdroj: https://www.us-cert.gov/tlp</xs:documentation>
            <!-- Plyn vypis polozek -->
            <xs:documentation xml:lang="cz">RED When should it be used?- Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</xs:documentation>
            <xs:documentation xml:lang="cz">RED How may it be shared?- Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</xs:documentation>
            <xs:documentation xml:lang="cz">AMBER When should it be used?- Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</xs:documentation>
            <xs:documentation xml:lang="cz">AMBER How may it be shared?- Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.</xs:documentation>
            <xs:documentation xml:lang="cz">GREEN When should it be used?- Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</xs:documentation>
            <xs:documentation xml:lang="cz">GREEN How may it be shared?- Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.</xs:documentation>
            <xs:documentation xml:lang="cz">WHITE When should it be used?- Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</xs:documentation>
            <xs:documentation xml:lang="cz">WHITE How may it be shared?- TLP: WHITE information may be distributed without restriction, subject to copyright controls.</xs:documentation> ...
        </xs:annotation>
    </xs:simpleType>

```

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

## KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

---

- E-mail
  - [cert.incident@govcert.cz](mailto:cert.incident@govcert.cz) – řešení incidentů, formulář
  - [cert@govcert.cz](mailto:cert@govcert.cz) – konzultace, informativní
- Web <http://govcert.cz>
  - Aktuality
  - Zranitelnosti
  - Měsíční bulletin
  - Legislativa, dokumenty

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101

# WEBOVÉ STRÁNKY



The screenshot shows the homepage of the NCKB website. At the top, there is a navigation bar with links to "Mapa serveru", "Textová verze", and "English". Below the navigation bar is the NCKB logo, which consists of a grid of blue circles and the text "národní centrum kybernetické bezpečnosti". The main menu below the logo includes "ÚVOD", "VLÁDNÍ CERT", "RKB", "INFORMAČNÍ SERVIS", "LEGISLATIVA", "KII / VIS", "ODKAZY", and "KONTAKTY". The "ÚVOD" button is highlighted with a red background. The main content area features a section titled "Co je NCKB" with text about the establishment of the agency. Another section, "Aktuální hrozba", discusses a threat to mobile devices running Android 5. A link to "Další hrozby" is provided. The "Aktuality" section mentions the selection of NCKB as the national CERT operator by NBÚ. A link to "Další aktuality" is also present. Logos for TI (Trusted Introducer) and CERT are displayed at the bottom.

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

# WEBOVÉ STRÁNKY



The screenshot shows the homepage of the nckb website. At the top, there is a navigation bar with links to "Úvod", "VLÁDNÍ CERT", "RKB", "INFORMAČNÍ SERVIS" (which is highlighted in yellow), "LEGISLATIVA", "KII / VIS", "ODKAZY", and "KONTAKTY". Below the navigation bar is a sidebar with a list of links under the heading "Zranitelnosti": "Akce a události", "Publikace", "Strategie a Akční plán", "Pracovní příležitosti", "RSS", "Informace CSIRT.CZ", and "Výkladový slovník". The main content area features a large graphic of a lion holding a sword, with the text "národní centrum kybernetické bezpečnosti" and the nckb logo. The page title "Zranitelnosti" is displayed above a list of news items from 2015, each with a link to the full article.

## Zranitelnosti

- 17.09.2015 [Android 5 – zranitelnost uzamčení obrazovky mobilních zařízení](#)
- 04.09.2015 [Kritická zranitelnost Keychain v Apple Mac OS X](#)
- 27.08.2015 [iOS - zranitelnost Ins0mnia](#)
- 18.08.2015 [Nová zranitelnost nultého dne v OS X 10.10.5](#)
- 14.08.2015 [DYLD - zranitelnost nultého dne v OS X opravena](#)
- 31.07.2015 [Nová zranitelnost služby Mediaserver v OS Android](#)
- 21.07.2015 [Zranitelnost v aplikaci AirDroid pro vzdálenou správu mobilních zařízení](#)
- 14.07.2015 [Adobe Flash Player – kritické zranitelnosti nultého dne](#)
- 07.07.2015 [CMS Orchard – perzistentní XSS zranitelnost](#)
- 24.06.2015 [Společnost ESET vydala důležitou aktualizaci, která ošetřuje vážnou zranitelnost](#)
- 18.06.2015 [Chyba služby overlayfs v Ubuntu umožňuje lokální escalaci práv](#)
- 10.06.2015 [Zranitelnost v e-mailové aplikaci iOS.](#)
- 01.06.2015 [Apple - zranitelnost nultého dne ve starších zařízeních Mac umožňuje rootkit injection.](#)
- 28.05.2015 [Android - zranitelnost frameworku Apache Cordova](#)
- 22.05.2015 [Logjam - nová zranitelnost v TLS protokolu](#)
- 14.05.2015 [VENOM - zranitelnost ve virtualizovaném prostředí](#)
- 06.05.2015 [Fortinet FortiAnalyzer a FortiManager - XSS zranitelnost](#)
- 29.04.2015 [WordPress - kritická XSS zranitelnost nultého dne](#)

1010010101101010100010110100101101  
10101000110100101101101001001011010  
101010001101001011010110100100110100101010

# ZRANITELNOSTI

## POODLE - zranitelnost využívá SSL 3.0 protokol

17. 10. 2014

Pracovníci Google odhalili závažnou chybu v zabezpečení šifrované komunikace, kterou označili POODLE (Padding Oracle On Downgraded Legacy Encryption). Přestože je protokol SSL 3.0 již téměř 15 let starý a je dávno nahrazen novější verzi protokolu TLS, je stále využíván z hlediska kompatibility v mnoha webových službách k ochraně komunikace mezi uživatelem a internetovou stránkou. K tomuto zabezpečení starým SSL dochází, pokud z nějakého důvodu nelze navázat spojení pomocí nového protokolu TLS.

### Charakteristika zranitelnosti

Útočník v pozici „man-in-the-middle“ může záměrně vynutit sestavení spojení tak, aby byl využíván pro zabezpečenou komunikaci starší SSL 3.0 protokol. Šifrování v SSL 3.0 využívá buď proudovou šifru RC4, nebo blokovou šifru v CBC módu, které svými vlastnostmi umožňují útočníkovi získat některá přenášená data.

### Postižené systémy

Všechny systémy, které umožňují používat (neblokuji) protokol SSL 3.0 pro zabezpečenou komunikaci.

### Dopad zranitelnosti

Chyba umožňuje útočníkovi získat informace uživatelů, jako například přihlašovací údaje k různým službám z obsahu cookies.

### Řešení

Zakázat používání SSL 3.0 protokolu. Využívat nejnovější verze protokolu TLS.

### CVE

CVE-2014-3566

### Odkazy

<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.troyhunt.com/2014/10/everything-you-need-to-know-about.html>  
<http://googleonlinesecurity.blogspot.de/2014/10/this-poodle-bites-exploiting-ssl-30.html>  
<http://securityaffairs.co/wordpress/29254/security/ssl-3-0-poodle.html>

101001010110101010100010110100101101  
101010001101001011011010010010110101010  
101010001101001011010110100100110100101010

# WEBOVÉ STRÁNKY



Úvodní stránka | Mapa serveru | Textová verze | English |  |

**národní centrum kybernetické bezpečnosti**

**ÚVOD** **VLÁDNÍ CERT** **RKB** **INFORMAČNÍ SERVIS** **LEGISLATIVA** **KII / VIS** **ODKAZY** **KONTAKTY**

Zranitelnosti

Akce a události

**Publikace**

Strategie a Akční plán

Pracovní příležitosti

RSS

Informace CSIRT.CZ

Výkladový slovník

Úvodní stránka » Informační servis » Publikace

## Publikace

- » [Bezpečnostní incidenty srpen 2015](#)
- » [Bezpečnostní incidenty červenec 2015](#)
- » [Bezpečnostní incidenty červen 2015](#)
- » [Bezpečnostní incidenty květen 2015](#)
- » [Zpráva o stavu kybernetické bezpečnosti České republiky 2014](#)
- » [Bezpečnostní incidenty duben 2015](#)
- » [Bezpečnostní incidenty březen 2015](#)
- » [Bezpečnostní incidenty únor 2015](#)
- » [Bezpečnostní incidenty leden 2015](#)
- » [Bezpečnostní incidenty prosinec 2014](#)
- » [Bezpečnostní incidenty listopad 2014](#)
- » [Bezpečnostní incidenty říjen 2014](#)
- » [Bezpečnostní incidenty září 2014](#)
- » [Bezpečnostní incidenty srpen 2014](#)
- » [Bezpečnostní incidenty červenec 2014](#)
- » [Bezpečnostní incidenty červen 2014](#)
- » [Bezpečnostní incidenty květen 2014](#)
- » [Zpráva o stavu kybernetické bezpečnosti ČR - 2013](#)



nckb

10100101011010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

# NOVÉ WEBOVÉ STRÁNKY



nckb

## NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI

ÚVOD VLÁDNÍ CERT RKB INFORMAČNÍ SERVIS KII / VIS LEGISLATIVA ODKAZY KONTAKTY

ZRANITELNOSTI AKCE A UDÁLOSTI PUBLIKACE STRATEGIE A AKČNÍ PLÁN PRACOVNÍ PŘÍLEŽITOSTI RSS INFORMACE CSIRT.CZ VÝKLADOVÝ SLOVNÍK

### ZRANITELNOSTI

- 14.07.2015 [Adobe Flash Player – kritické zranitelnosti nultého dne](#)  
07.07.2015 [CMS Orchard – persistentní XSS zranitelnost](#)  
24.06.2015 [Společnost ESET vydala důležitou aktualizaci, která ošetřuje vážnou zranitelnost](#)  
18.06.2015 [Chyba služby overlays v Ubuntu umožňuje lokální eskalaci práv](#)  
10.06.2015 [Zranitelnost v e-mailové aplikaci iOS.](#)  
01.06.2015 [Apple - zranitelnost nultého dne ve starších zařízeních Mac umožňuje rootkit injection.](#)  
28.05.2015 [Android - zranitelnost frameworku Apache Cordova](#)  
22.05.2015 [Logjam - nová zranitelnost v TLS protokolu](#)  
14.05.2015 [VENOM - zranitelnost ve virtualizovaném prostředí](#)  
06.05.2015 [Fortinet FortiAnalyzer a FortiManager - XSS zranitelnost](#)  
29.04.2015 [WordPress - kritická XSS zranitelnost nultého dne](#)  
21.04.2015 [WordPress - XSS zranitelnost postihuje mnoho pluginů](#)  
13.04.2015 [Darwin Nuke - zranitelnost v operačních systémech OS X a iOS](#)  
07.04.2015 [Schneider Electric VAMPSET – chyba umožňující spuštění libovolného kódu](#)  
02.04.2015 [MongoDB - oprava chyby umožňující vzdálené odmítnutí služby](#)  
23.03.2015 [Zranitelnost IP telefonů Cisco řady Small Business umožňuje odposlech hovorů](#)  
19.03.2015 [OpenSSL – oprava 14 zranitelností SSL/TLS](#)  
11.03.2015 [FREAK – Společnosti Apple a Microsoft vydaly opravy zranitelnosti](#)

### AKTUÁLNÍ HROZBY

#### Adobe Flash Player - kritické zranitelnosti nultého dne

Na základě uniklých informací z databázi kompromitované italské firmy Hacking Team objevili bezpečnostní analytici ze společnosti Trend Micro a Fire Eye dvě kritické zranitelnosti ...

Další hrozby

### AKTUALITY

#### Národní bezpečnostní úřad mění vizuální styl

Národní bezpečnostní úřad a některé jeho organizační celky přechází od 1. 7. 2015 na nový vizuální styl ...

Další aktuality

NBÚ FAQ Mapa webu Prohlášení o přístupnosti Textová verze Nahoru



1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101

# NEVEŘEJNÉ WEBOVÉ STRÁNKY

- Pouze pro uzavřenou skupinu uživatelů
- DMZ
  - Přístup přes VPN
- Navíc
  - Data ke stažení
  - Podrobnější analýzy (malware,...)
  - Generované reporty
  - E-learning
  - Diskusní fórum

1010010101101010100010110100101101  
10101000110100101101101001001011010  
101010001101001011010110100100110100101

# KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

- Twitter @GOVCERT\_CZ



The screenshot shows the Twitter profile page for @GOVCERT\_CZ. The header features the NCKB logo and the text "Oficiálním zdrojem informací jsou stránky GovCERT.CZ". Below the header, the bio reads "The official source of information is website GovCERT.CZ". The profile has 56 tweets, 10 following, and 114 followers. The timeline displays two recent tweets from GovCERT.CZ:

- Měsíční souhrn bezpečnostních incidentů za srpen 2015.** [govcert.cz/cs/informaci-...](http://govcert.cz/cs/informaci-...)
- Zranitelnost uzamčení obrazovky mobilních zařízení s OS Android 5.** [govcert.cz/cs/informaci-...](http://govcert.cz/cs/informaci-...)

The sidebar includes a "Who to follow" section with suggestions like "Anonymous", "HackRead", and "Thorsten Benner".

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101

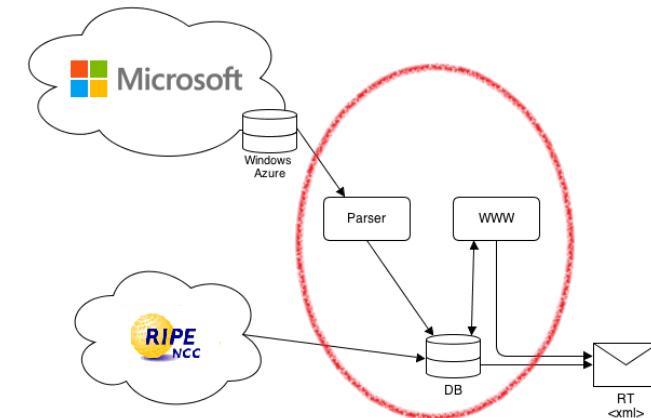
# KOORDINAČNÍ CENTRUM PRO ČESKÉ BEZP. TÝMY

- Videokonferenční kolaborační platforma
  - V případě rozsáhlých incidentů
  - Virtuální videokonferenční místnost
  - Práce nad sdílenými dokumenty
  - Kompatibilita



## BOTNET FEED

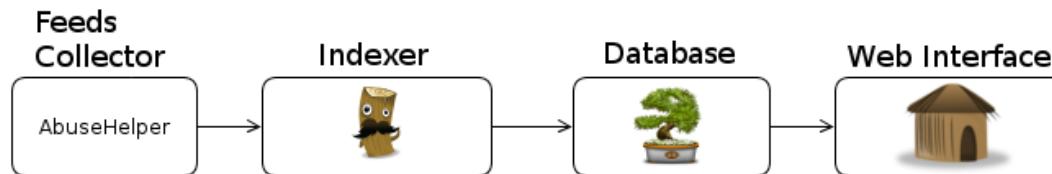
- Data od MS Digital Crimes Unit
- Komunikace směrem od strojů k C&C serverům botnetů
  - Potenciálně nakažené PC
- Conficker, Zeus, ZeroAccess
- Strojově zpracovávané
  - 250 tisíc záznamů denně
- Agregace dat
- NCKB dostává data pro ČR
  - Jedinná organizace v ČR
  - Data předáváme dále



1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

## Projekty IHAP a MDM

- **Incident Handling Automation Project**
- **Malicious Domain Manager**
- Zpracování a standardizace dat
- Ukládání v databázi, zobrazení a práce s událostmi
- celkem získaných dat – 223 450 událostí za měsíc:
  - brute-force (105 776), phishing (97 332), exploit (176), trojan (14)
- celkem získaných dat týkajících se ČR – 685 událostí



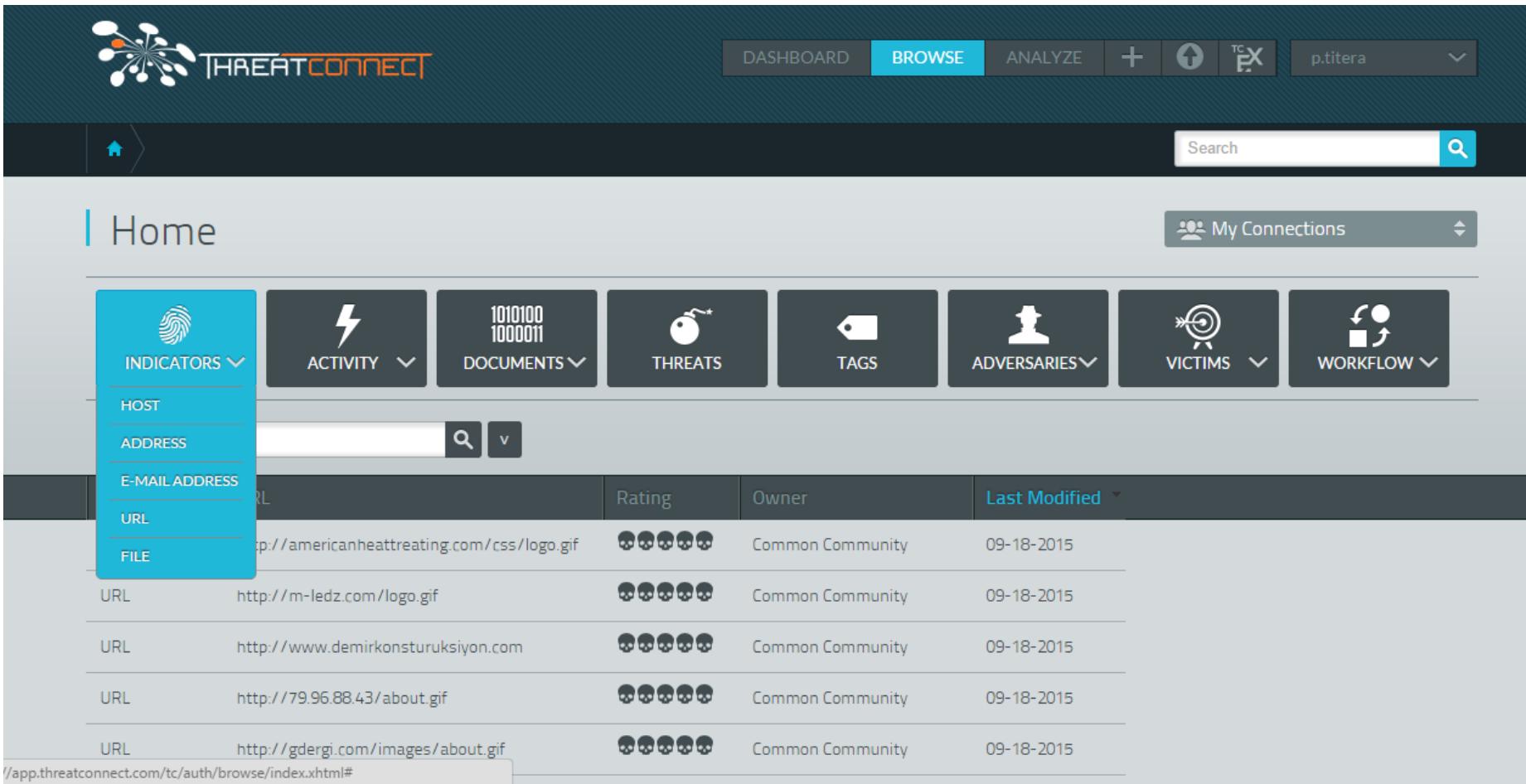
1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

## KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

- Neveřejné komunikační kanály:
  - Diskusní fóra
    - Pro komunikaci s odborníky z bezpečnostních týmů
    - Konzultace
  - Platformy pro sdílení dat, IoC, informací o APT
    - „need to share“
    - CTI (CERT-EU)
    - THREATCONNECT (NATO)
- Počítačové sítě pro klasifikované informace:
  - CRONOS - spojení s členy NATO do stupně Tajné
  - ACID - spojení s Francií do stupně Důvěrné
  - VEGA - spojení s PČR do stupně Důvěrné

1010010101101010100010110100101101  
10101000110100101101101001001011010  
1010100011010010110110100100110100101010

# PLATFORMA THREATCONNECT



The screenshot shows the ThreatConnect platform interface. At the top, there is a navigation bar with the ThreatConnect logo, a search bar, and several buttons: DASHBOARD (gray), BROWSE (blue), ANALYZE, a plus sign, a upload icon, and a TC EX icon. To the right of the buttons is a user profile with the name "p.titera" and a dropdown arrow. Below the navigation bar is a secondary header with a home icon, a search bar containing "Search" and a magnifying glass icon, and a "My Connections" button with a dropdown arrow.

The main content area is titled "Home". On the left, there is a sidebar with a tree icon and a dropdown menu for "INDICATORS" which includes "HOST", "ADDRESS", "E-MAIL ADDRESS", "URL", and "FILE". The "FILE" option is currently selected and highlighted in blue. Next to the sidebar are eight large buttons: ACTIVITY, DOCUMENTS, THREATS, TAGS, ADVERSARIES, VICTIMS, and WORKFLOW. Below these buttons is a search bar with a magnifying glass icon and a dropdown arrow.

The main table area displays a list of indicators. The columns are: URL, Rating, Owner, and Last Modified. The table contains five rows of data:

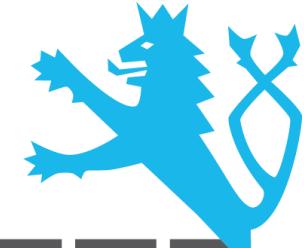
URL	Rating	Owner	Last Modified
http://americanheattreating.com/css/logo.gif	💀💀💀💀	Common Community	09-18-2015
http://m-ledz.com/logo.gif	💀💀💀💀	Common Community	09-18-2015
http://www.demirkonsturuksiyon.com	💀💀💀💀	Common Community	09-18-2015
http://79.96.88.43/about.gif	💀💀💀💀	Common Community	09-18-2015
http://gdergi.com/images/about.gif	💀💀💀💀	Common Community	09-18-2015
/app.threatconnect.com/tc/auth/browse/index.xhtml#	💀💀💀💀	Common Community	09-18-2015

10100101011010100010110100101101  
10101000110100101101101001001011010  
10101000110100101101101001001101001010



**Děkuji za pozornost.**

**Otzky?**



**nckb**

Národní centrum  
kybernetické  
bezpečnosti