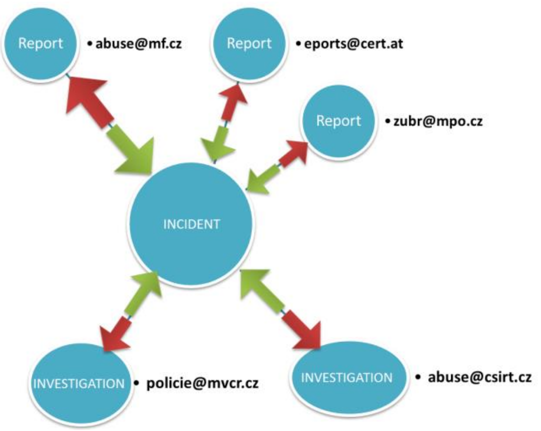
Sdílení informací public-private o zranitelnostech, hrozbách a incidentech

Pavel Titěra
GovCERT.CZ
NCKB
NBÚ

Národní centrum kybernetické bezpečnosti

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

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

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)

KONZULTAČNÍ ČINNOST

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

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

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)

TF-CSIRT
Trusted Introducer

SPOLUPRÁCE S NÁRODNÍM CERT

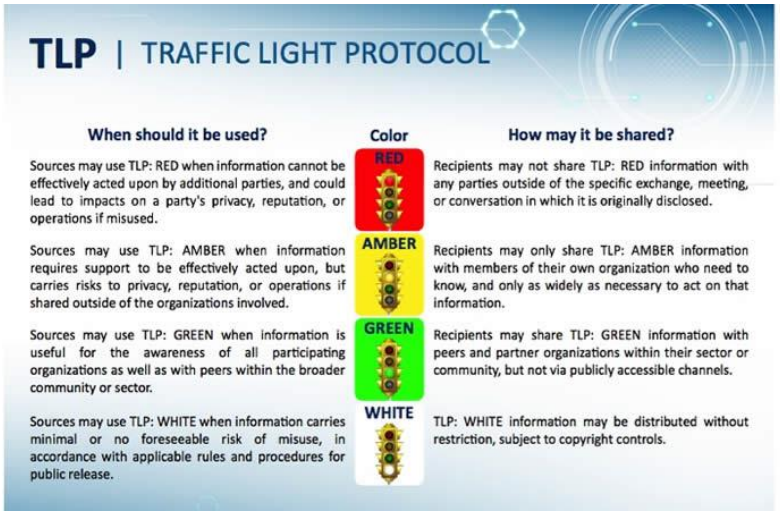
- CSIRT.CZ provozovaný sdružením CZ.NIC
  - Národní CERT tým
  - Koordinační role
  - Plní funkci poslední instance
- NCKB je Point of contact pro ČR v oblasti IT Security
- Předávání incidentů spadajících do pole působnosti druhého týmu

GOVCERT.CZ ⇄ CSIRT.CZ powered by CZ.NIC

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

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)

KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

- E-mail
  - cert.incident@govcert.cz – řešení incidentů, formulář
  - 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 (veřejné)</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>
        <!-- Plny 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> ....
```

KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

- E-mail
  - cert.incident@govcert.cz – řešení incidentů, formulář
  - cert@govcert.cz – konzultace, informativní

- Web http://govcert.cz
  - Aktuality
  - Zranitelnosti
  - Měsíční bulletin
  - Legislativa, dokumenty

WEBOVÉ STRÁNKY

WEBOVÉ STRÁNKY

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 verzí 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 (neblokují) 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

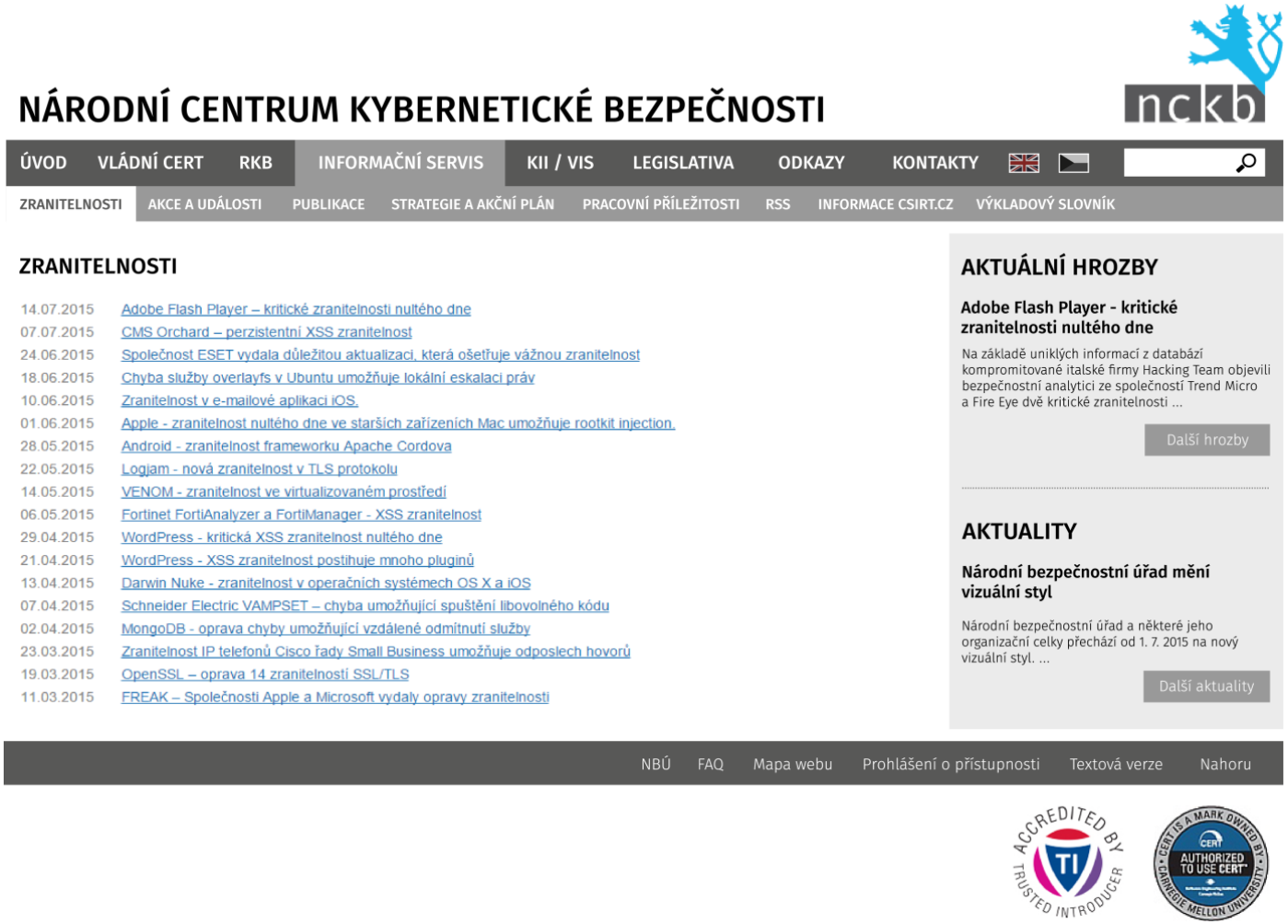
CVE-2014-3566

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

WEBOVÉ STRÁNKY

NOVÉ WEBOVÉ STRÁNKY



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

KOMUNIKAČNÍ KANÁLY PRO SDÍLENÍ DAT A INFORMACÍ

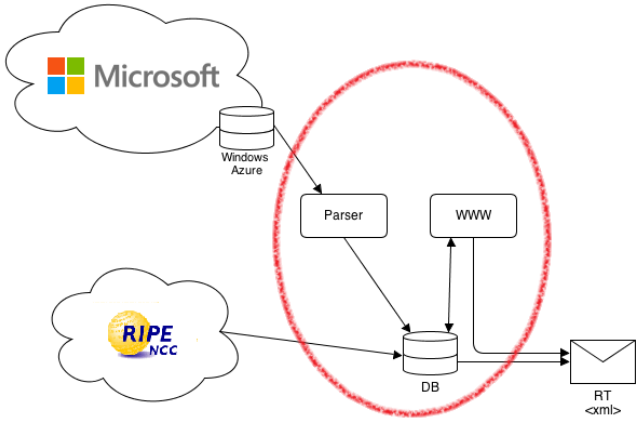
- Twitter @GOVCERT_CZ

KOORDINAČNÍ CENTRUM PRO ČESKÉ BEZP. TÝMY

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

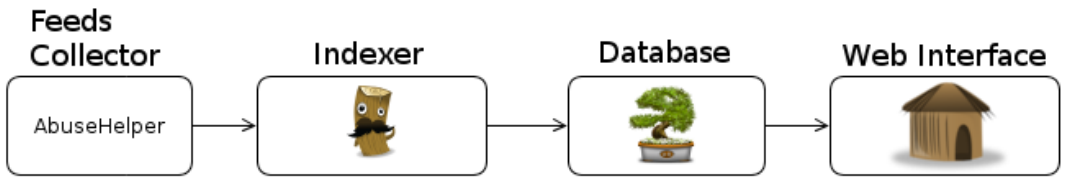
BOTNET FEED

- 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



Projekty IHAP a MDM

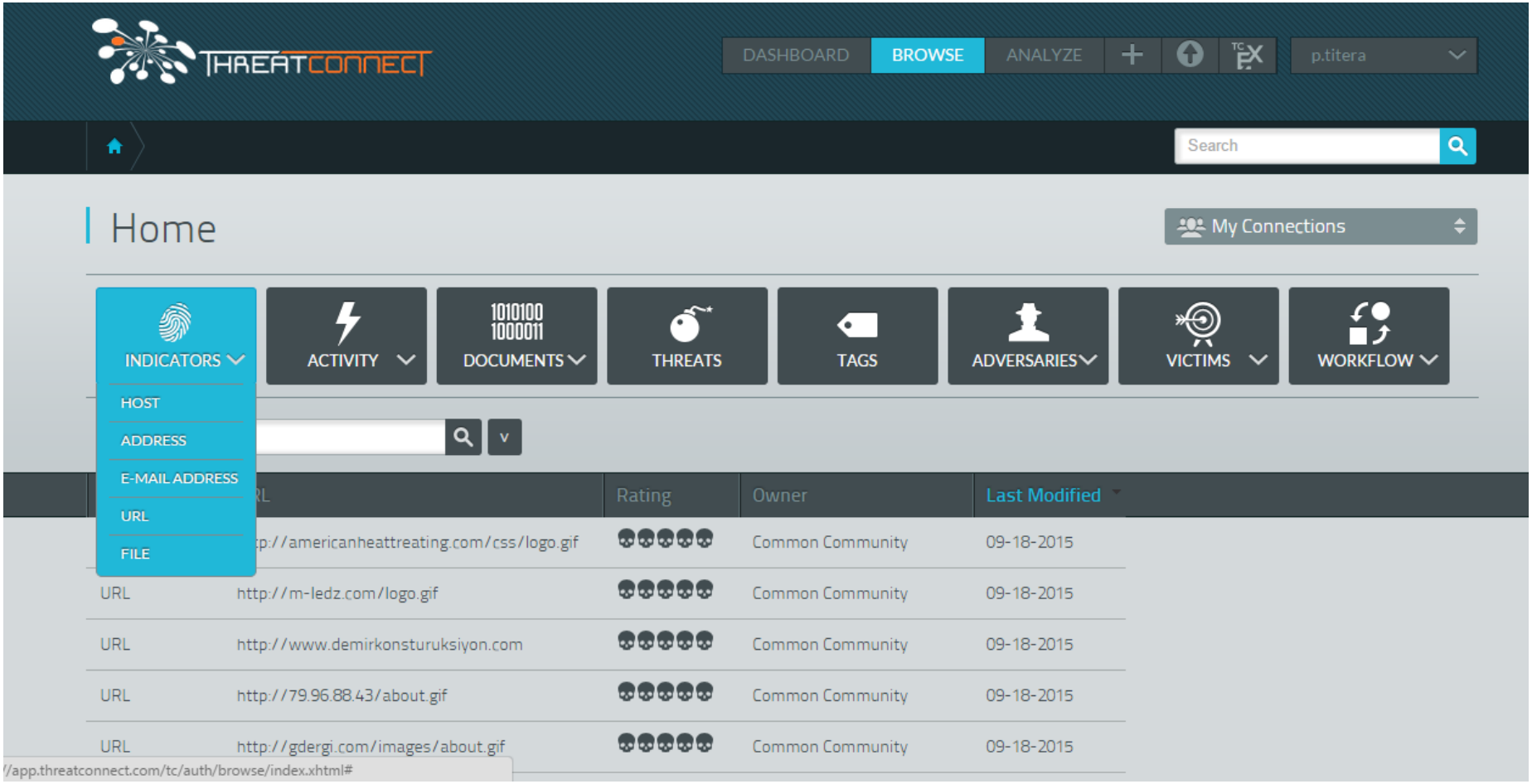
- **I**ncident **H**andling **A**utomation **P**roject
- **M**alicious **D**omain **M**anager
- Zpracování a standardizace dat
- Ukládání v databázi, zobrazení a práce s událostmi
- celkem získaných dat – 223 450 událostí za měsíc:
  - brute-force (105 776), phishing (97 332), exploit (176), trojan (14)
- celkem získaných dat týkajících se ČR – 685 událostí



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 síťě 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

PLATFORMA THREATCONNECT



Děkuji za pozornost.

Otázky?

Národní centrum kybernetické bezpečnosti