

# Proaktivní informování o bezpečnostních incidentech

CZ.NIC z.s.p.o.  
Michal Prokop / [michal.prokop@nic.cz](mailto:michal.prokop@nic.cz)  
09. 06. 2011



Národní CSIRT České republiky



Interní bezpečnostní tým CZ.NIC

# CZ.NIC-CSIRT

- Založen 2008
- Status „akreditovaný“ u TI
- Interní bezpečnostní tým CZ.NIC
  - řešení interních bezpečnostních incidentů
  - právo zrušit delegaci domény při ohrožení (mezi)národní bezpečnosti (na 1 měsíc)
  - škodlivý obsah (malware, viry), phishing, řídicí centrum botnetu
  - Neřešíme tímto způsobem spamy, ochranné známky, autorská práva apod.

# Databáze hrozeb v doméně .cz

## Co nás k tomu vedlo?

- Zvýšení bezpečnosti internetového prostředí
- Snaha minimalizovat množství napadených domén .cz

## Jak toho dosáhnout?

- Vytvoření vlastní databáze domén .cz z veřejně dostupných databází domén obsahujících škodlivý obsah
- Zasílání informací držitelům domén vedených v této databázi
- Pomoc držitelům doménových jmen v zóně cz

# CZ.NIC LABS

- CZ.NIC LABS vytvořil interní aplikaci, která informace z vybraných databází sjednocuje
- Zatím se jedná o pilotní provoz
- Hrozby:
  - malware, phishing, domény fungující jako řídicí počítače botnetů apod.
- Zdroj:
  - veřejně dostupné databáze domén hostujících škodlivý obsah
- Aplikace umožňuje CZ.NIC-CSIRT týmu kontaktování správce daných .cz domén za účelem řešení problému

# Zdroje dat pro databázi

## **Malwarepatrol** (<http://www.malware.com.br>)

- Jedná se o automatizovaný i manuální sběr dat
- Databáze aktualizována každou hodinu
- Evidované URL kontrolovány minimálně jednou denně

## **Phishtank** (<http://www.phishtank.com>)

- Provozováno společností OpenDNS
- Data převážně z mailů nahlášených od dobrovolníků
- Veškerá data jsou kontrolována manuálně

# Zdroje dat pro databázi

## Google Safe Browsing

- Data z této databáze využívají také prohlížeče Mozilla Firefox a Google Chrome
- Pomocí nástrojů google lze požádat o kontrolu URL pro urychlení odstranění domény z databáze nebezpečných webových stránek

## Manuální

- Pokud se členové CZ.NIC-CSIRT týmu dovědí o bezpečnostním incidentu jiným způsobem
- E-mail, webová aplikace, IM, apod.

# Testovací provoz

- Momentálně probíhá testování aplikace
- Nastavování procesů pro práci s incidenty
- Dva typy dat
  - kompletní URL (řeší se ihned)
  - nekompletní URL (déle trvající incidenty)
- Neřešení incidentu může mít vliv na:
  - návštěvnost dané URL
  - případná ztráta zisku
  - poškození dobrého jména

# Hlavní funkce aplikace

The screenshot displays a web application interface for monitoring threats in the .CZ domain. On the left is a navigation sidebar with various filter categories. The main content area is titled 'Seznam hrozeb v doméně .CZ' and includes a 'Stav databáze' section with statistics and a 'Nové zprávy' table.

**Nové zprávy**

- [Nové zprávy](#)
- [Nové hrozby \(443\)](#)
- [Závažné \(1\)](#)
- [Řešené \(4\)](#)
- [Řešené CSIRT \(0\)](#)
- [Není problém \(1\)](#)
- [Skryté \(0\)](#)
- [Opravené \(7\)](#)
- [Pozitivní změna bez reakce \(1\)](#)
- [Pozitivní změna s reakcí \(2\)](#)
- [Dřívější \(650\)](#)

## Seznam hrozeb v doméně .CZ

### Stav databáze

Celkový počet domén v zóně: 795818  
Aktuální počet škodlivých domén: 447

Stav databází k poslední aktualizaci (31.5.2011 06:22:58):  
.cz záznamů v Google Safebrowsing Malware: 429  
.cz záznamů v Google Safebrowsing Black: 0  
.cz záznamů v databázi Malwarepatrol: 5  
.cz záznamů v databázi Phishtank: 13

### Nové zprávy

doména	poslední změna	status	<input type="checkbox"/>
[redacted]	2011-05-17 15:47:21	pozitivní změna s reakcí	<input type="checkbox"/>
[redacted]	2011-04-26 16:50:58	řešený	<input type="checkbox"/>

- Aktuální informace z databáze včetně statistik
- Přehled posledních změn u řešených domén

# Hlavní funkce aplikace

- Detail reportované domény
- Přehled aktuálních a historických hrozeb na dané doméně
- Korespondence nabízí souhrnný přehled komunikace
- Status poukazuje na životní cyklus konkrétní domény

The screenshot displays the application interface for a domain. On the left is a sidebar with navigation links: [Nové zprávy](#), [Nové hrozby \(443\)](#), [Závažné \(1\)](#), [Řešené \(4\)](#), [Řešené CSIRT \(0\)](#), [Není problém \(1\)](#), [Skruté \(0\)](#), [Opravené \(7\)](#), [Pozitivní změna bez reakce \(1\)](#), [Pozitivní změna s reakcí \(2\)](#), and [Dřívější \(650\)](#). Below these is a search box with a 'Hledat' button and a user login section for Michal Prokop. The main content area is titled 'Detail: [redacted]' and includes a 'Vyhledávání v registru (Whois)' link. It features two tables: one for threat details with columns 'zdroj', 'uri', 'začátek hrozby', and 'ukončení manuálně přidané hrozby', and another for history with columns 'zdroj', 'uri', 'začátek hrozby', and 'konec hrozby'. Below the tables are sections for 'Korespondence' (with a 'Napsat e-mail' link) and 'Status', which includes a dropdown menu set to 'nový' and an 'Aktualizovat status a poznámku' button. The status log shows two entries: '2011-02-03 13:37:52 - status změněn z 'nový' na 'dřívější'' and '2011-02-07 09:12:17 - status změněn z 'dřívější' na 'nový''. The footer of the sidebar shows the 'cz.nic' logo and 'SPRÁVCE DOMÉNY CZ'.

# Hlavní funkce aplikace

- Možnost výběru odpovědi z přednastavených šablon a editace textu
- Přímá komunikace se službou whois
- Po odeslání e-mailu je status incidentu změněn dle uvážení řešitele

The screenshot displays the application's interface. On the left is a sidebar with a list of filters: 'Nové zprávy', 'Nové hrozby (443)', 'Závažné (1)', 'Řešené (4)', 'Řešené CSIRT (0)', 'Není problém (1)', 'Skruté (0)', and 'Opravené (7)'. Below these are buttons for 'Pozitivní změna bez reakce (1)', 'Pozitivní změna s reakcí (2)', and 'Dřívejší (650)'. At the bottom of the sidebar is a search box with a 'Hledat' button and a user profile for 'Přihlášen: Michal Prokop' with links for 'Nastavení šablon' and 'Odhlásit'. The main area is titled 'E-mail k doméně "[redacted]"'. It features a 'Šablona: Šablona 1' dropdown and a 'Nové zprávy' button. The email form includes fields for 'Příjemce:', 'Vlastníka domény lze zjistit v registru Whois.', 'Kopie (jednorázově):', 'Slepá kopie (jednorázově):', and 'Předmět: Škodlivý obsah v doméně [redacted]'. The 'Zpráva:' field contains a pre-filled message: 'Dobrý den, vaše doména [redacted] je vedena v seznamu domén hostujících škodlivý obsah. Touto zprávou vás chceme požádat o nápravu situace. Doména je evidována v těchto databázích: Od 2011-05-22 06:22:51 v databázi Phishtank: [redacted]'. The signature block reads: 'S pozdravem Michal Prokop michal.prokop@nic.cz CZ.NIC-CSIRT CZ.NIC, z.s.p.o. Americká 23 120 00 Praha 2'. The footer of the sidebar shows the 'CZ.nic' logo and 'SPRÁVCE DOMÉNY CZ'.

# Budoucnost

## Krátkodobá

- Přejít z testovacího provozu do ostrého
- Získat ze stávajících databází přesnější data

## Střednědobá

- Rozšířit sběr dat na případné další databáze

## Dlouhodobá

- Minimalizace množství infikovaných domén .cz

# Děkuji za pozornost

## Otázky ?

CZ.NIC z.s.p.o.  
Michal Prokop / [michal.prokop@nic.cz](mailto:michal.prokop@nic.cz)  
09. 06. 2011