Proaktivní informování o bezpečnostních incidentech

CZ.NIC z.s.p.o.
Michal Prokop / michal.prokop@*nic.cz*
09. 06. 2011

cz nic
správce domény cz

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, řídící 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 řídící 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 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

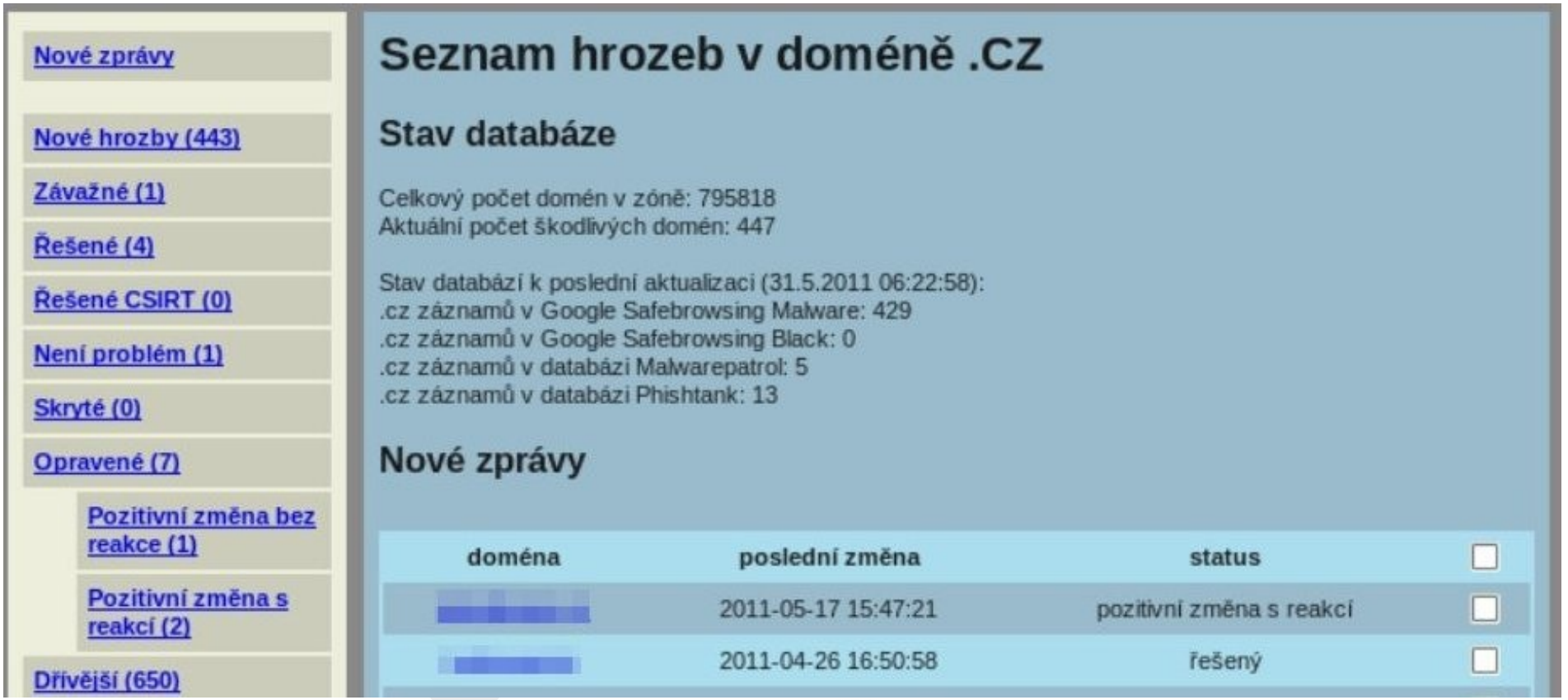
Manuální

- 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

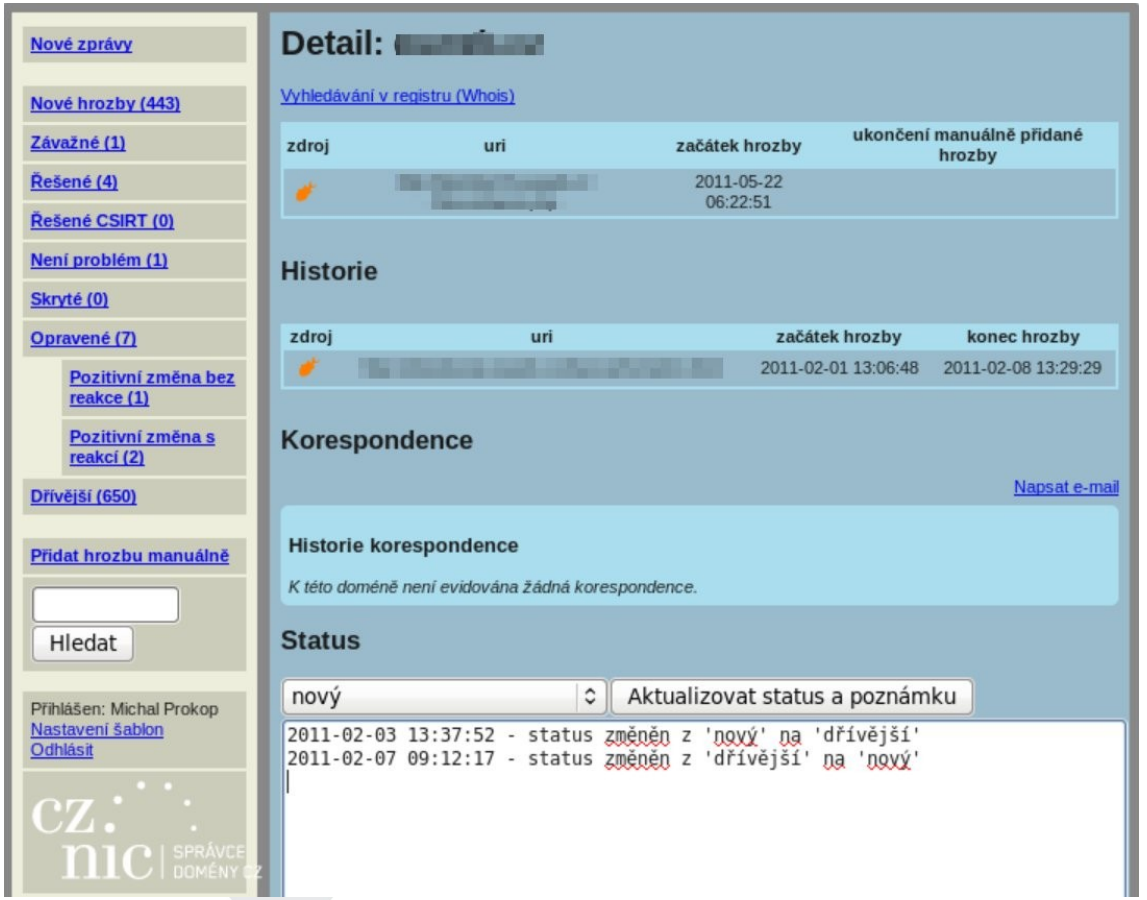
Hlavní funkce aplikace



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

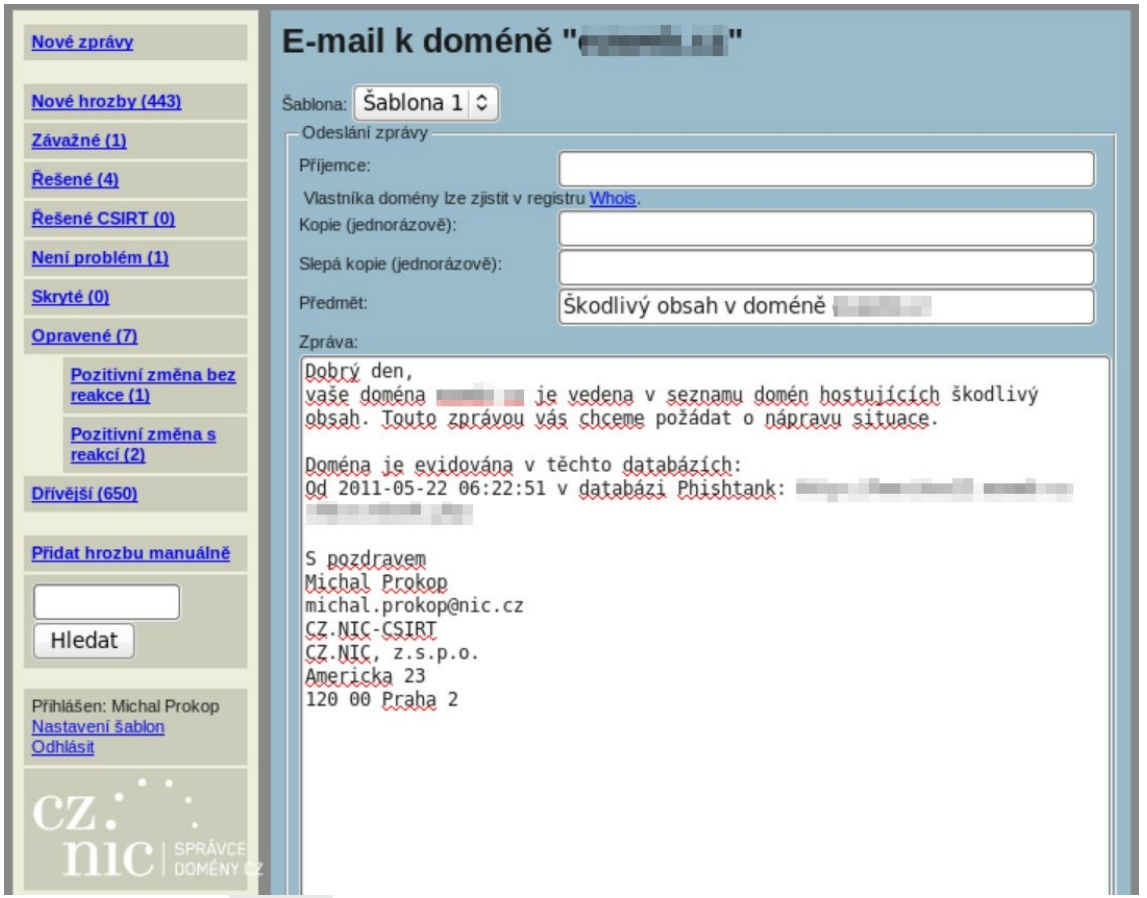
Hlavní funkce aplikace

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



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



Budoucnost

Krátkodobá

- Přechod 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*
09. 06. 2011