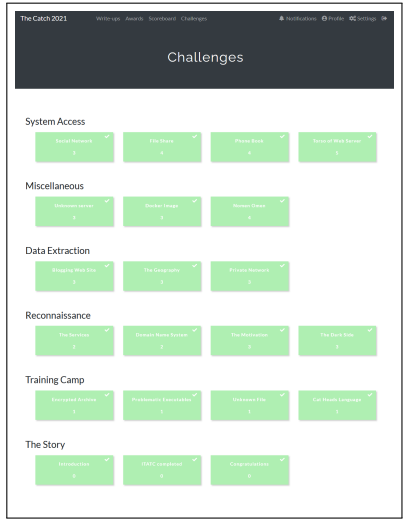
The Catch backstage

Aleš Padrta

Forenzní laboratoř CESNET

The Catch

- Vzdělávací soutěž
- Říjen = Evropský měsíc kybernetické bezpečnosti
- https://thecatch.cesnet.cz



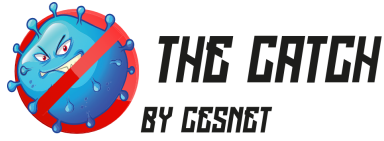
Trocha historie

- 2017 – začátek roku
  - Radovan Igliar: „CESNET by měl zábavně vzdělávat veřejnost“
- 2017 – červen
  - Aleš Padrta, Andrea Kropáčová
  - Diskuse v kavárně (Strasbourg)
  - Zábavné vzdělávání $\Rightarrow$ capture the flag
- 2017 – červenec
  - Příprava soutěže – Forenzní laboratoř CESNET
  - Výběr názvu – Radovan Igliar
- 2017 – říjen
  - První ročník **The Catch**

Trocha historie

The Catch

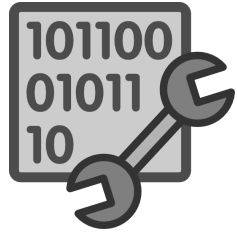
Catch the QuBit



The Catch
by TREND MICRO & cesnet

Nastavení soutěže

- Zábavné vzdělávání
  - Výborný nápad
  - Jak realizovat?
- Požadavky
  - Pro (odbornou) veřejnost
  - Procvičení mozkových závitů
  - Rozšíření obzorů
  - Naučení/oprášení postupů
- Oblasti ke vzdělávání
  - Kyberbezpečnost
  - Schopnosti realizačního týmu



Příprava úloh

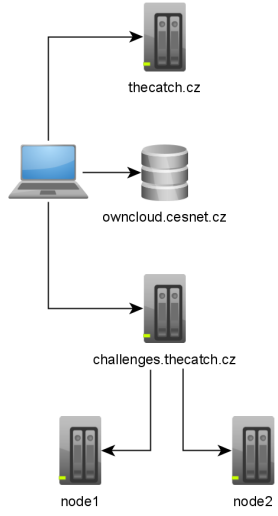
- Základní princip úlohy
  - Inspirace praxí
  - Zajímavé vlastnosti souborů
  - Zajímavé nástroje / použití
  - Zajímavé algoritmy
  - Obecné principy
- Pedagogický efekt
  - Analýza problému
  - Potřebné znalosti (motivace k získání)
  - Ovládnutí problematiky
- Umístění flagu
- Předpokládané řešení
  - Pohled účastníka
  - Nasměrování (zadání, nápovědy)
- Obtížnost
  - Bodové ohodnocení 1–5
  - Potřebné znalosti
  - Potřebný čas/práce
- Zapojení do tématu soutěže
  - Kreativní chvilka

Příprava n-tého ročníku The Catch

- Konec října
  - Konec The Catch $n - 1$
- Listopad
  - Vyhodnocení průběhu
  - Vyhodnocení dotazníků
- Od prosince
  - Sběr nápadů na úlohy
- Od ledna
  - Implementace úloh (volný čas)
- Červen
  - Revize stavu
  - Zjištění mezer v úlohách
- Červenec, srpen
  - Doplnění úloh
  - Jednotící prvek
- Září
  - Příprava nasazení
  - Výroba odměn
  - Promo aktivity
- Říjen
  - Doladění drobností
  - Zahájení soutěže
  - Dohled nad průběhem
  - Konec The Catch n

Technické zázemí

- Postupný vývoj
- Hlavní web soutěže
  - Zadání úloh
  - CTFd
- Soubory ke stažení
  - Samostatný server
  - Owncloud
- On-line úlohy
  - Docker + GitLab CI
  - Dva uzly
  - Load balancing (nginx)



Monitoring

- Průběžné sledování
  - Icinga
  - Detekce + odstranění problémů
  - Vylepšení pro příště
- Analýzy
  - Databáze CTFd
  - Logy
- Automatizované zpracování dat
  - Průběžné reporty
  - Tabulky a přehledy
  - Grafy

Report o stavu – Thecatchbot

thecatchbot BOT 06:00

```
Celkový přehled

  866 registrováno
  396 opsalo flag v introduction
  340 vyřešilo aspoň jednu bodovanou úlohu
  293 získalo důvěru archeologů a už kutá na místě vykopávek
  228 vyřešilo aspoň jednu úlohu na místě vykopávek
  35 vyřešilo všechny úlohy
```

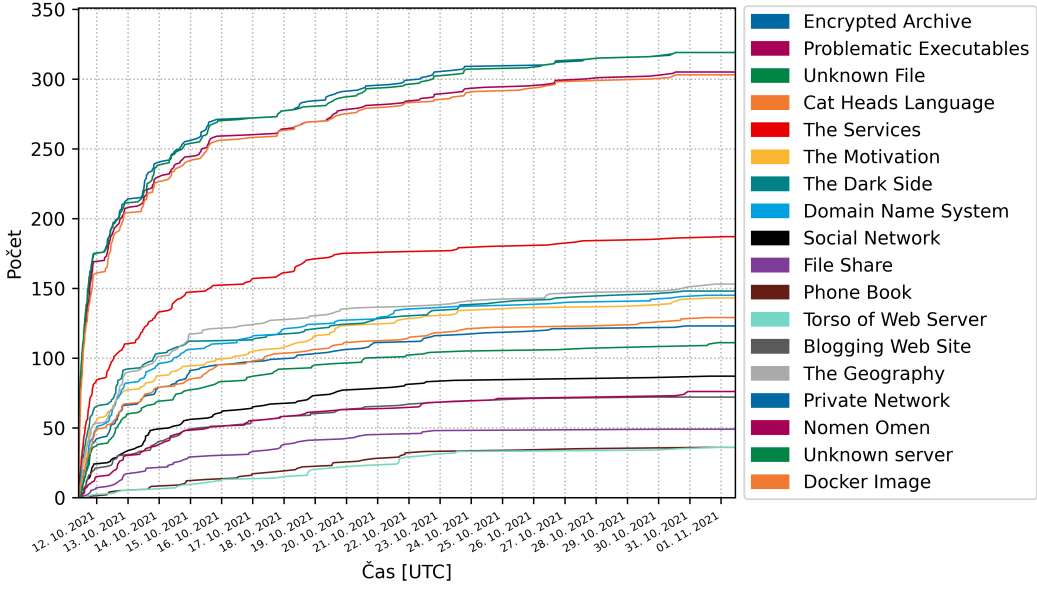
Pokusy o zneužívání botnetem

T **thecatchbot** BOT 19:00

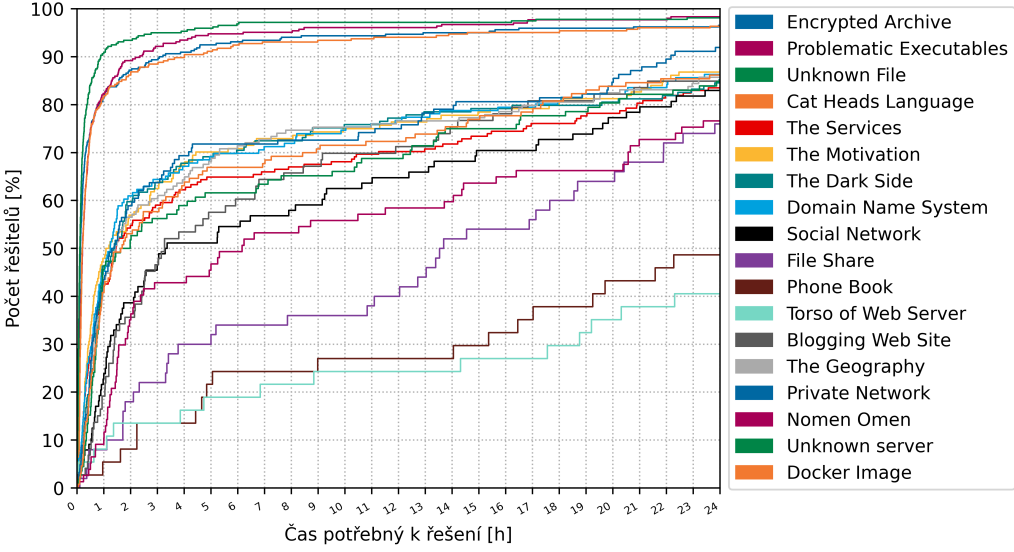
```
New registrations (honeypot)

  Date, E-mail, Team Name
  2022-01-18 17:02:47.549925, hedfam@gmail.com, Jaketrip
  2022-01-18 17:10:29.533334, martinbnvds@gmail.com, ahjc.irfquiemia
  2022-01-18 17:11:39.174006, haigner@sonic.net, Biaemi
  2022-01-18 17:12:41.818953, nourcan_ademova@hotmail.com, Kristina
  2022-01-18 17:13:29.118650, basenlaw@gmail.com, fylhyz
  2022-01-18 17:20:51.014916, rmtierney@comcast.net, nfhfcquiemia
  2022-01-18 17:34:40.730474, adryancazares3@gmail.com, nikulya
  2022-01-18 17:45:36.488515, stones177@hotmail.com, mitryukha
  2022-01-18 17:52:53.357073, lkamian@aol.com, lila
  2022-01-18 17:56:54.757315, charissay9@gmail.com, Taunerquiemia
```

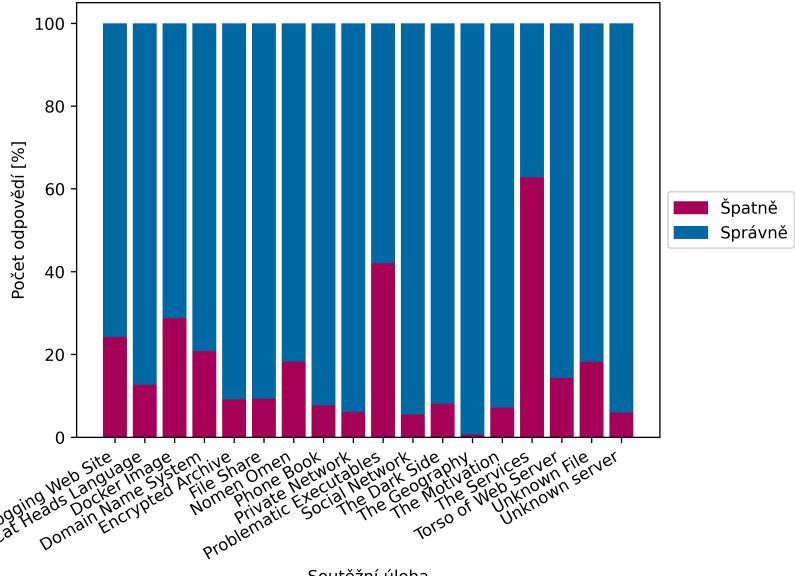
Počty správných řešení v čase



Doba potřebná k vyřešení



Chybně zadané odpovědi

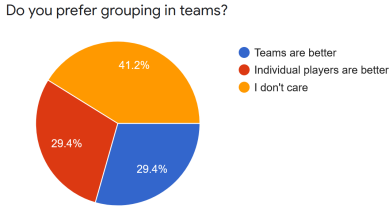


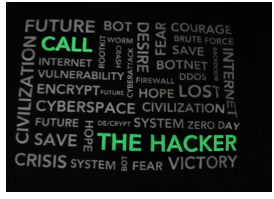
Postupný vývoj a vylepšování

- Opisování flagů
  - Alternativní cesta
  - Smyslupný text (`flag{WISE-NICE-DEAR-CATS}`)
- Obtížnost pro každého
  - Akademie – začínající experti
  - Ostatní úlohy – podle zkušeností
- Vyšší rozmanitost úloh
  - On-line úlohy
  - Více autorů = více nápadů

Postupný vývoj a vylepšování

- Zpětná vazba od účastníků
  - Write-ups (popis řešení)
  - Dotazník spokojenosti
  - Samostatně zaslané nápady
- Odměny pro řešitele
  - Prvních *N* řešitelů
  - První vyřešení úlohy
  - *M* nejlepších write-upů
- Zvažujeme VPN pro on-line úlohy





Děkuji za pozornost

cesnet