# Turris Omnia: jak lovit hackery

**ISSS 2017**

**Patrick Zandl • patrick.zandl@nic.cz • 4.4.4444**

# Situace na internetu je horší, než kdy dříve

- Co jsme se o bezpečnosti naučili před deseti lety, je dnes pasé.
- Neustálé školení administrátorů nikdo nezvládá (není čas)
- Každý systém tvrdí, že je bezpečný (jinak by se neprodal)
- Cenných dat je online stále více (cílit na ně je tedy snadnější)
- Zranitelností se denně publikuje několik desítek
- Jejich náprava trvá často i roky (díra je otevřena dlouho)
- Bezpečnost je „kritériem slibu“, nikoliv „kritériem realizace“
- Uživatelé zabezpečení systémů vlastně bezmezně věří
- A ujišťování o rostoucím zabezpečení vede k menší ostražitosti

# Internet věcí je nová všudypřítomná výzva pro bezpečnost

- Internet věcí (IoT) začíná být všude
- IoT je připojené programovatelné zařízení s omezenými rozhraními
- Liší se od M2M komunikace mnohem větší variabilitou, možnostmi sběru a vyhodocení dat i správy
- To přináší dosud netušené možnosti, ale také bezpečnostní výzvy
- Výpočetní kapacita typického IoT zařízení odpovídá 15 let starému počítači
- Kvůli ceně se tlačí mimo jiné na velikost paměti, což se projevuje na úrovni použitých bezpečnostních konceptů a pohodlí zabezpečení.
- V roce 2016 bylo na světě kolem 5 miliard IoT zařízení

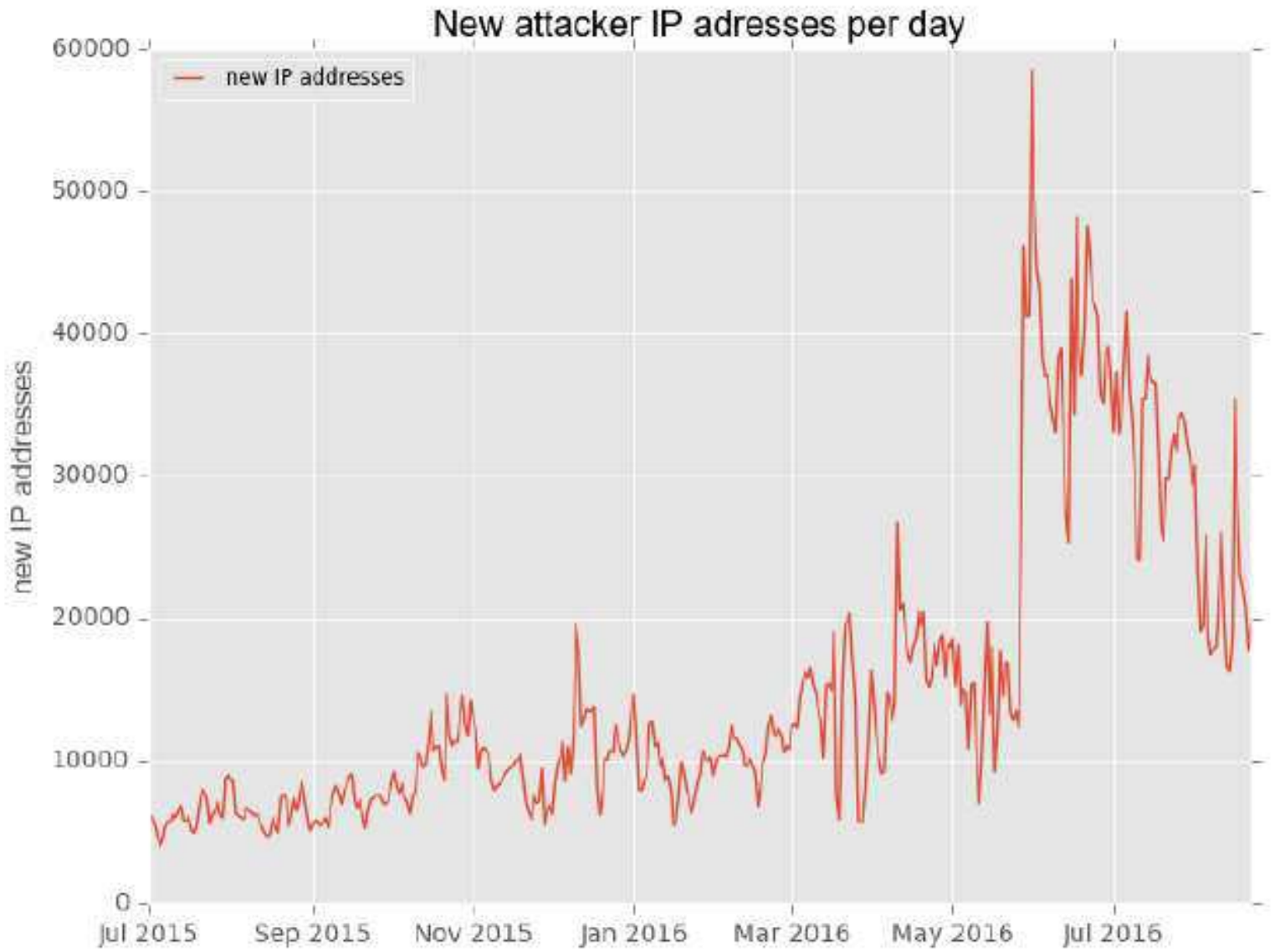
PROJECT:TURRIS

- Vytvoření sítě zabezpečených routerů
  - vlastní HW i SW
  - security updates, grey listy, …
  - webové rozhraní pro uživatele
    - statistiky, nastavení, vlastní honeypoty, …
- Aktuálně tisíce uživatelů
- Výstupy z turrisů slouží jako jeden ze vstupů dat pro CSIRT.CZ tým
- A také k zabezpečení ostatních routerů

# Koncept „superbezpečného“ routeru

- *Je open source*
  - *Protože každý si může projít zdrojové kódy a ověřit si, zda data jsou posílána tam, kam je slíbeno a ne jinam.*
- *Je aktuální (online aktualizace)*
  - *Protože se tak co nejrychleji zavírají publikované chyby do systému.*
- *Je adaptabilní na útoky bez zásahu administrátora*
  - *Protože jen tak není třeba admina stále školit.*
  - *Adaptabilní kolaborativní firewall sbírá data o útocích*
  - *Ta analyzuje řídící pracoviště Turrisu*
  - *Následně jsou automaticky aktualizována pravidla pro firewall*
  - *Reakční doba typicky do deseti minut*
- *Filosofická otázka: Když může být superprémiové kočičí žrádlo, může být i router superbezpečný?*

# Příklad naší práce: botnet MIRAI



# Projekt Turris: tři roky ochrany digitální hranice

- Útok nemá v řadě případů konkrétní motiv. Až později útočník zjišťuje, co cenného získal a jak to může zhodnotit.
- Množí se ale i cílené útoky v rámci konkurenčního či politického boje, s tím roste panika a také ostudy „false positive“.
- Projekt Turris se o „digitální hranici“ stará čtvrtým rokem.
- **Nyní chceme poskytnout routery Turris Omnia českým úřadům, školám a státním institucím.**
- Podmínky účasti se právě finalizují, projekt se rozběhne na podzim.
- Nechte nám vizitku na stánku, kontaktujeme vás…
- Nebo napište na patrick.zandl@nic.cz ...


# Otázky?

# Děkuji za pozornost

**Patrick Zandl • patrick.zandl@nic.cz •**

# Praktický příklad: botnet MIRAI

- Skládá se z milionů „chytrých“ zařízení
  - CCTV kamery, online DVR, routery
- Zdroj masivních DDoS útoků
  - 600 Gbps a více s velmi kvalitní celoplošnou distribucí provozu
- Celosvětově rozšířený

# Bezpečnostní problémy a rizika Internetu věcí

- Kompromitace dat
  - Cílem je získání konkrétních dat ze zařízení
  - Ty lze zpeněžit nebo použít pro další útoky (slovníky hesel aj.)
- Kompromitace k útok proti infrastruktuře
  - Napadené zařízení lze použít k vnějším útokům typu DDoS
  - Nebo jako nejrůznější SPAM a fake-news relay.
- Kompromitace k útok proti prvku
  - Zařízení bude použito k dalším útokům dovnitř chráněné sítě
- *A samozřejmě kombinace, protože cokoliv cenného se hodí zpeněžit, hackeři se škatulkováním typu útoku nezdržují.*

# Jak funguje botnet MIRAI

- Zkouší se připojit Telnetem na porty 23 a 2323
- Testuje malý slovník kombinací přihlašovacích jmen a hesel
- Po úspěšném přínku se spustí malware
  - Ten zabije proces obsluhující Telnet (znemožní dálkovou nápravu)
  - Malware se neukládá, je pouze rezidentní (ztíží odhalení)
- Nakažené zařízení okamžitě napadá další a šíří se
  - K tomu přispěla doporučení výrobců kamer portforwardovat port 23
  - Defaultní či jednoduché kombinace hesel

| | | |
|---|---|---|
| root/xc3511 | root/vizxv | root/admin |
| admin/admin | root/888888 | root/xmhdipc |
| root/default | root/juantech | root/123456 |
| root/54321 | support/support | root/(none) |
| admin/password | root/root | root/12345 |
| user/user | admin/(none) | root/pass |
| admin/admin1234 | root/1111 | admin/smcadmin |
| admin/1111 | root/666666 | root/password |
| root/1234 | root/klv123 | Administrator/admin |
| service/service | supervisor/supervisor | guest/guest |
| guest/12345 | guest/12345 | admin1/password |
| administrator/1234 | 666666/666666 | 888888/888888 |
| ubnt/ubnt | root/klv1234 | root/Zte521 |
| root/hi3518 | root/jvbzd | root/anko |
| root/zlxx. | root/7ujMko0vizxv | root/7ujMko0admin |
| root/system | root/ikwb | root/dreambox |
| root/user | root/realtek | root/00000000 |
| admin/1111111 | admin/1234 | admin/12345 |
| admin/54321 | admin/123456 | admin/7ujMko0admin |
| admin/1234 | admin/pass | admin/meinsm |
| tech/tech | mother/fu[redacted]r | |

Mirai's built-in password dictionary.

# Penetrace MIRAI v jednotlivých produktech