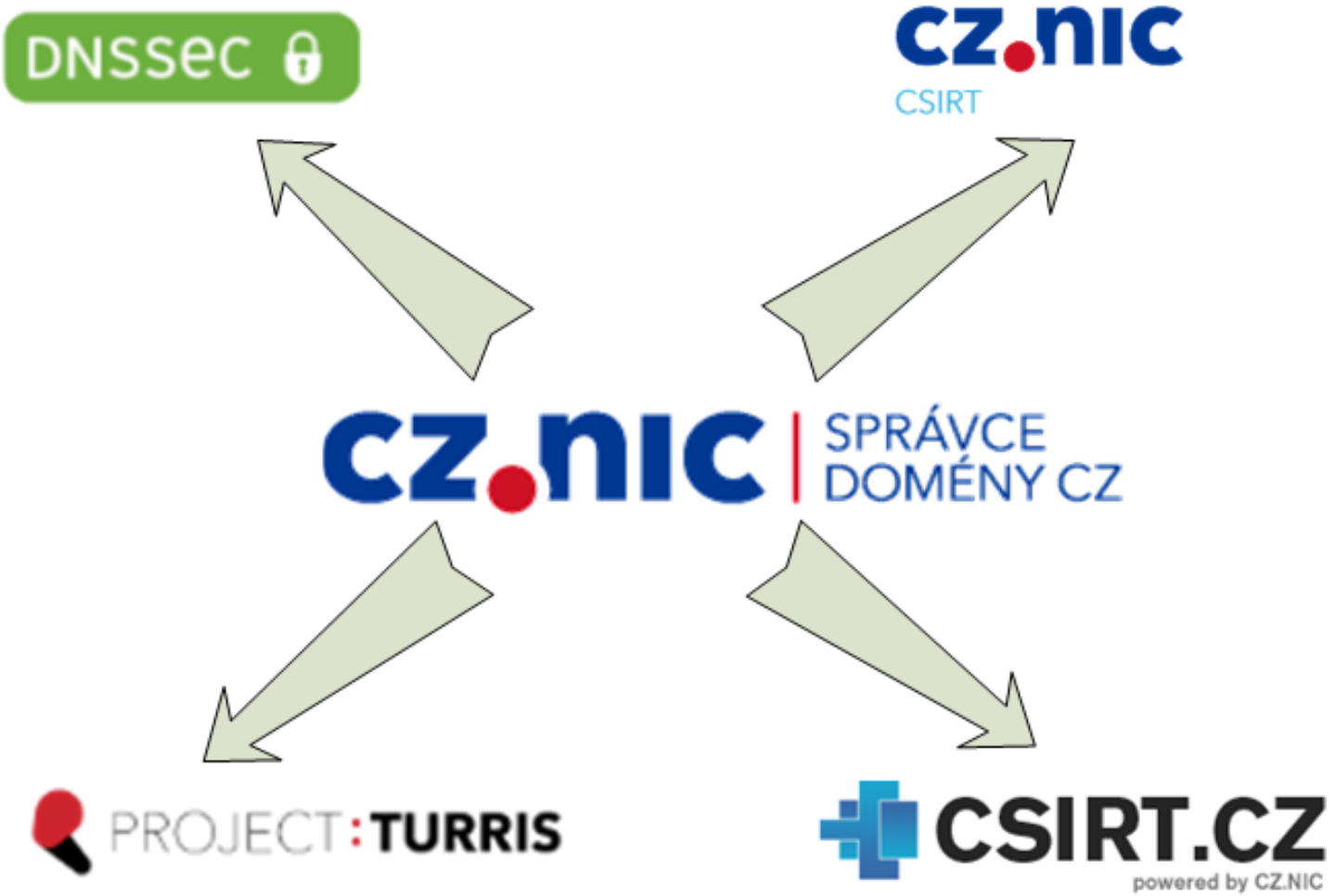
Bezpečnostní rizika chytrých spotřebičů a Internetu věcí

Poznatky z digitální hranice routerů Turris

Patrick Zandl • patrick.zandl@nic.cz • 20.4.2017

CZ.NIC | SPRÁVCE DOMÉNY CZ

Aktivity zaměřené na bezpečnost



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?*

Internet věcí a 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

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.*

Co je mi do zabezpečení kamery nebo elektroměru

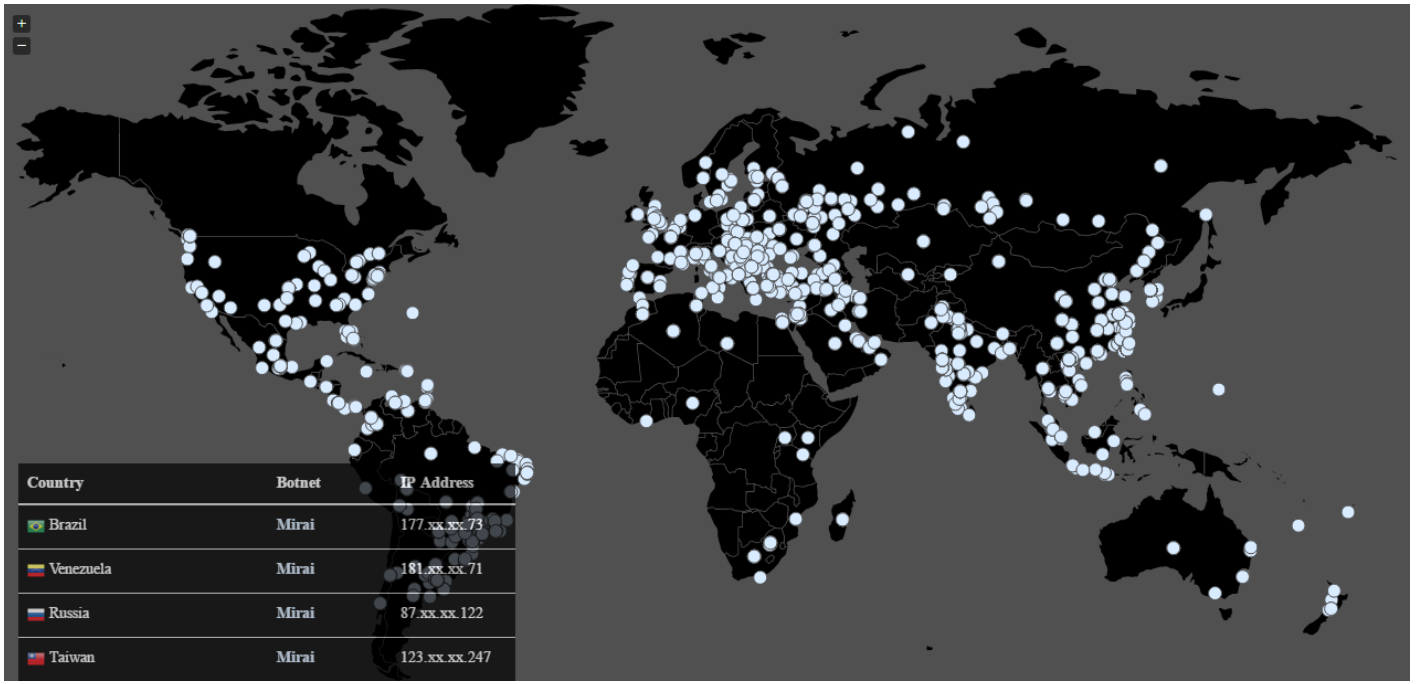
- Terčem jste ihned po připojení na internet
  - Než si vás najde scanner, trvá to málo desítek minut od připojení
  - Rychle se dostanete do databází napadnutelných
- Je to jako s viry: fungujete pomalu, divně, ostatní vás nemají rádi
  - ISP, vyhledávače i další poskytovatelé služeb postupně odstavují podezřelé sítě, případně je upozorňují na problémy.
  - Máte kvalitativní problémy se základními službami
- Vaše data jsou použita a zneužita
  - A vaše síť je monitorována, když se v ní objeví něco cenného, bude to použito. Často ani nejste schopni domyslet, jak.
- Útočník je již ve vaší síti a s tím lze mnoho podniknout
  - Například napadnout jiná zařízení v ní, která nejsou jinak přístupná.

Tak například kamery…

- Ty levné na AliExpress stojí pár dolarů a jsou tak jednoduché na provoz. Jen je zapojíte a už jedou, konfigurace netřeba.
- U řady z nich není možné změnit heslo nebo jsou zde použita defaultní hesla.
- Častou funkcí jsou „bezpečnostní snímky“ z kamery získatelné kýmkoliv bez hesla.
- Honeypot tvářící se jako kamera registruje pokusy o průnik v řádu desítek minut, pokusy o stažení snímků bez autorizace v řádu dne, když se „kamera“ dostane do správných databází.
- Kamera může sloužit k DDoS útokům (MIRAI) nebo infikovat další zařízení.
- Rozšiřují se databáze zranitelných zařízení, tak vás dostanou.

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



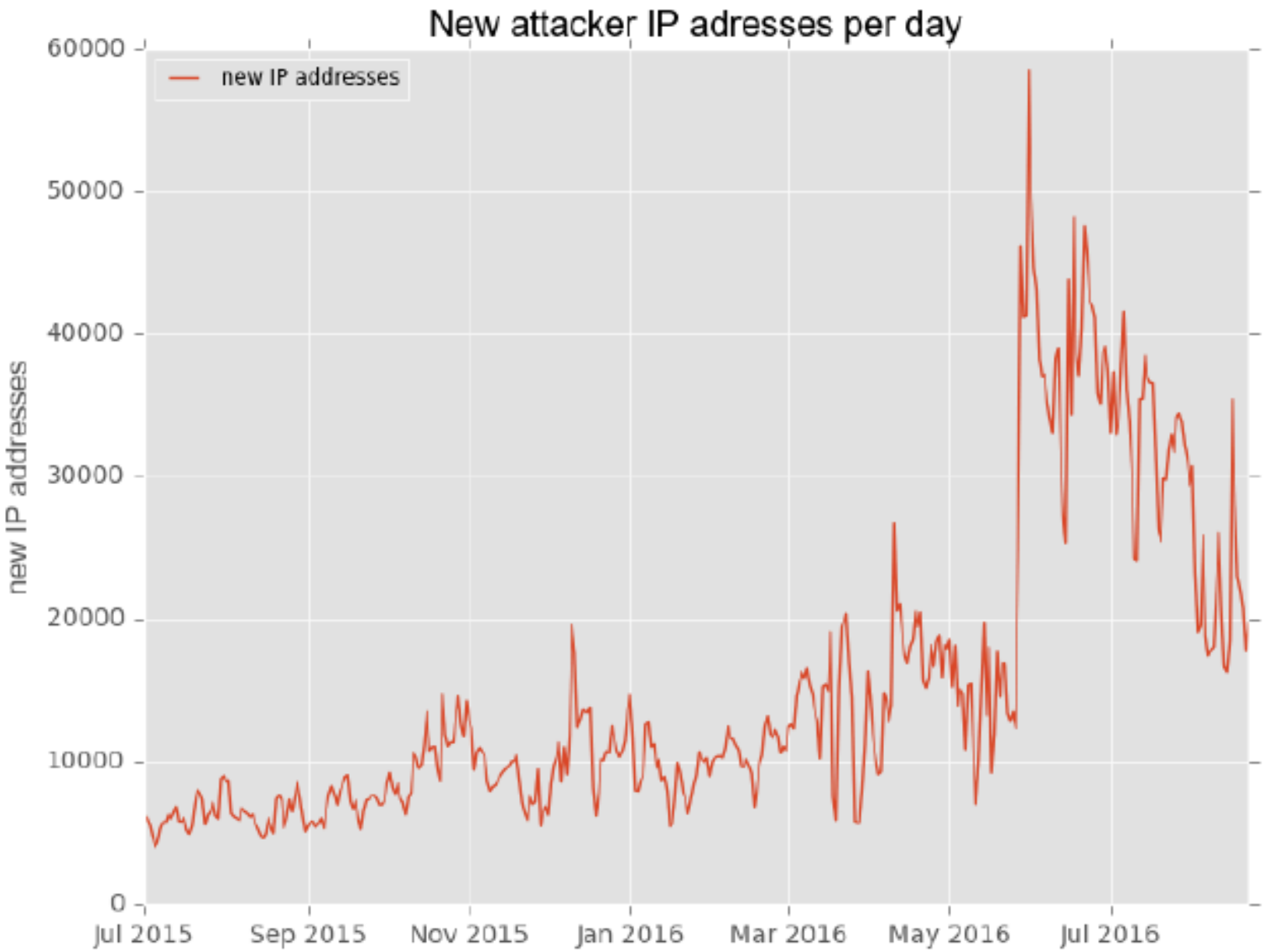
Jak funguje botnet MIRAI

- 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

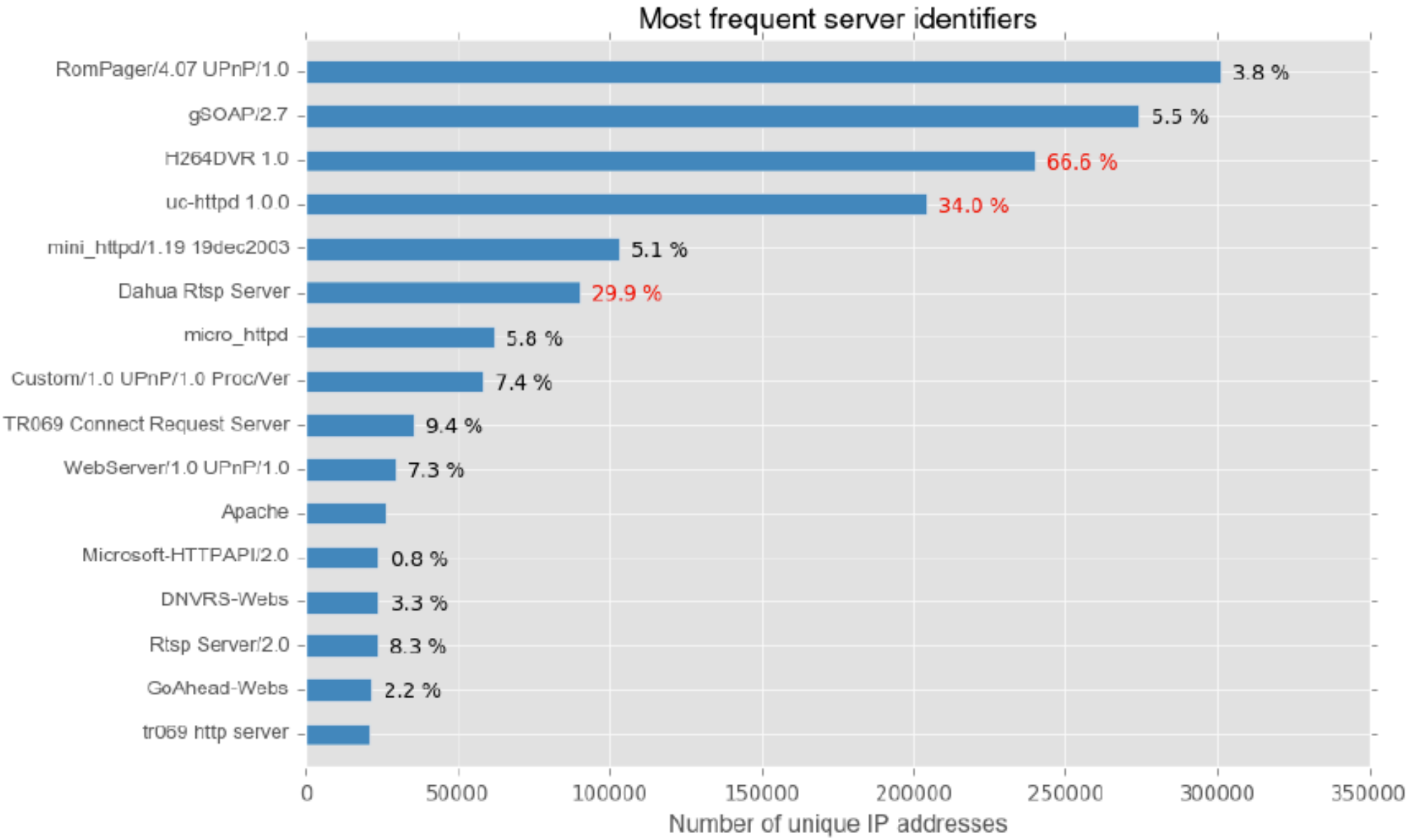
root/xc3511	root/vizxv	root/admin
admin/admin	root/888888	root/xmhdipc
root/default	root/juantech	root/123456
root/54321	support/support	root/(none)
admin/password	root/root	root/12345
user/user	admin/(none)	root/pass
admin/admin1234	root/1111	admin/smcadmin
admin/1111	root/666666	root/password
root/1234	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.

A jakou rychlost MIRAI nabral?



Penetrace MIRAI v jednotlivých produktech



Nejde o marginální problém

- Botnetům typu MIRAI se nelze nyní efektivně bránit na straně napadeného
- Přes 1,2 milionu útočících zařízení
- „Konecept“ okamžitě okopírovaly další skupiny a záhy přišly podobné útoky (SOAP)
- U některých produktů byly nakaženy dvě třetiny zařízení
- Rozsah škod nikdy nebyl a nebude přesně zjištěn, řada posledních průniků může a nemusí s úspěchem MIRAI souviset.
- Nakažená zařízení dále útočí, není mezi nimi koordinace
- Dříve nebo později je uvidíme v našem honeypotu
- **https://amihacked.turris.cz**

Otázky?

Děkuji za pozornost

Patrick Zandl • patrick.zandl@nic.cz •