



Bezpečnost a routery Turris

Miroslav Hanák, Michal Hrušecký
miroslav.hanak@turris.com, michal.hrusecky@turris.com



Historie projektu Turris - 2013

Výzkumný a bezpečnostní projekt

- vyrobeny bezpečnostní sondy pro domácnosti
 - PPC, 2G RAM, USB, GBit síť
 - opensource, root account, ...
 - mimochodem i router
- rozdány po republice
- UX pro otrlé
- automatické aktualizace



Co se sbíralo

- firewall log "zvenku"
- různé pasti na útočníky
- anonymizované statistiky o provozu
 - charakter provozu "zevnitř"
 - různé "pingy"



První výsledky

- velmi oblíbené mezi geeky
- cizinci je chtěli taky domů
- poznat něco z provozu zevnitř ven je těžké
 - nemáme-li kontext
 - nemáme-li obsah
 - mít obsah je problém
- co přichází "z venku" dává zajímavé výsledky



Pokračování - Turris Omnia

- má vše a ještě víc
 - armv7, 2G RAM, 5GHz AC, SFP, ...
- Indiegogo kampaň
- opt-in sbírání dat
- uzrálé a propracované UI



Pokračování - HaaS

- házet útočníkům klacky pod nohy je super
- osamostatnění nejzábavnější části
- Honeypot as a Service
- forwarduje útočníka do honeypotu
 - útočník je na serveru CZ.NIC
 - uživateli nic nehrozí
 - záznam jeho marného snažení je k dispozici

<https://haas.nic.cz>



Ultimátní router pro Geeky - MOX

- modulární, armv8, 1G RAM
- doplnění nabídky Omnie
- mnoho možností
- těžko uchopitelné pro negeeky



A co běžní uživatelé? Shield!

- pro běžné lidi
- zjednodušené UI
- firewall i sběr dat zapnut
- aktualizace zapnuty
- jasný cíl



Shield detailněji

- OpenVPN client/server
- zjednodučený reForis
- HW vychází z Turris MOX
- **Turris Sentinel**

