



Bezpečnost lokální sítě

Co v Turrisu chystáme

Michal Hrušecký • michal.hrusecky@nic.cz

Bezpečnost lokální sítě a Turris 2013



Co chtít od bezpečného routeru

- bezpečnostní aktualizace
- důvěryhodnost - nedělá co nechci
- firewall
- opensource
- root account
- možná přehled o provozu
- možná IDS



Historie projektu Turris - 2013

Výzkumný a bezpečnostní projekt

- bezpečnostní sondy pro domácnosti
- uměli i routovat a dělat spoustu dalšího
- staly se oblíbené
- dodnes dostávají aktualizace
- dodnes dostatečně výkonné aby byly relevantní

⇒ CZ.NIC začal vyrábět routery



Bezpečnost zvenku

Turris Sentinel

- znáte útočníky
- máte dynamický firewall
- šance na napadení služby zvenku je malá

Co ale donesená/zakoupená zařízení?

Ne každé zařízení je jako Turris

- nedostupné aktualizace
- {bloat,spy}ware od výrobce



Pakoň - monitoring provozu

- sleduje kam se různá zařízení připojují
- sleduje lidi na straně LAN
- všechna data skladuje lokálně
- jména serverů z DNS a TLS
 - dávají větší smysl

Results

▼ Date	↕ Duration	↕ Client	↕ Hostname	↕ Port	↕ Sent	↕ Received
2018-12-05 11:59:34	00:00:00	d8:58:d7:00:b3:22 🔍	project.turris.cz 🔍 ↗	https	988 B	4.08 KiB
2018-12-05 11:38:19	00:00:02	d4:f4:6f:a1:4a:ac 🔍	www.evernote.com 🔍 ↗	https	2.75 KiB	25.58 KiB
2018-12-05 11:38:18	00:00:01	d4:f4:6f:a1:4a:ac 🔍	evernote.com 🔍 ↗	https	1.57 KiB	4.88 KiB
— 2018-12-05 11:18:22	00:01:32	7a:c0:16:b8:6d:c7 🔍	google.com 🔍 ↗	https	4.31 KiB	10.45 KiB
2018-12-05 11:18:22	00:00:41	7a:c0:16:b8:6d:c7 🔍	google.com 🔍 ↗	https	2.77 KiB	5.09 KiB
2018-12-05 11:19:54	00:00:00	7a:c0:16:b8:6d:c7 🔍	google.com 🔍 ↗	https	1.54 KiB	5.36 KiB
2018-12-05 11:18:02	00:02:16	7a:c0:16:b8:6d:c7 🔍	109.230.199.119 🔍	22067/tcp	2.64 KiB	2.53 KiB



Pakoň - under the hood

Suricata

- sbírá data o DNS a TLS
- dokáže dodávat i statistiky o flow
 - v rámci optimalizace jsme přešli na conntrack

SQLite

- ukládá data
 - jedna v RAM jedna v storage
 - agregace a přeláví dat mezi "bucketsy"



Problémy

- UI pouze ve Forisu (který zabíjíme)
- Suricata je trochu overkill
 - rychlá, ale vezme si nějakou RAM
 - spousta závislostí
 - speciální konfigurák pro Pakoně
 - nové verze závisí na Rustu
 - Rust není v OpenWrt



Budoucnost

- vlastní UI
 - aktuálně podobné tomu ve Forisu
 - CSV export navíc
 - bude časem hezčí
- nahrazení Suricaty
 - už teď používáme contrack
 - nahradíme získávání dat jednoúčelovým programem



Pakoň - využití

Sledování zařízení

- připojuje se zařízení jen tam kam má?
- posílá rozumné množství dat?
- posílá data jen když má?
- použitelné pro IoT
- méně už pro mobily a PC



Morče - integrace IDS

- zapne IDS nad provozem
- aktualizuje sady pravidel
- generuje notifikace pokud narazí na problém

Notifications

!

October 3, 2021 1:55 PM

Security alert from host Widle to 10.0.0.1:80
ET TROJAN OSX/WireLurker User-agent (globalupdate)

!

October 3, 2021 1:55 PM

Security alert from host Widle to 10.0.0.1:80
ET TROJAN NSIS/TrojanDownloader.Agent.NZK CnC Actiity M2



Morče - under the hood

Snort 3

- C++ only
- Má LUA API

Morče

- spouštěcí script pro Snort se správou pravidel
- Lua plugin pro Snort
- volání Turris API na generování upozornění
- SQLite na ukládání dat



Budoucnost?

- sloučit Pakoňe a Morče
 - možná vymyslet rozumný jméno
- rozšíření IDS na IPS
- Turris Sentinel i mimo routery
 - testovací provoz s ISP



Děkuji za pozornost

