Projekt Turris

Bezpečnost uživatelských zařízení

Michal Hrušecký • michal.hrusecky@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

KKTS před deseti lety

KKTS - dnes

- prosazuje se optika
  - pomalu ubývá DSL
- 1 GBit začíná být málo
- ISP řeší víc než jen cenu
  - bezpečnost
  - dostatečný výkon
  - aby zařízení vydrželo - TCO

Co chtít od bezpečného routeru

- bezpečnostní aktualizace
- důvěryhodnost - nedělá co nechci
- firewall
- možná opensource
- možná 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 relevatní

⇒ CZ.NIC začal vyrábět routery

Bezpečnostní sonda - zdroje dat

- firewall logy z venku
- opt-in minipoty
  - předstíá telnet/webserver/mail server, …
  - požádá o login
  - zařízne spojení
- HaaS

Bezpečnostní sonda - výstupy

- posíláme CSIRT
- pouštíme automatické algoritmy
- zkoušíme vyvíjet nové a lepší algoritmy
- aktualizujeme lidem firewall
- publikujeme data
  - https://view.sentinel.turris.cz

Sentinel View

Pakoň - monitoring provozu

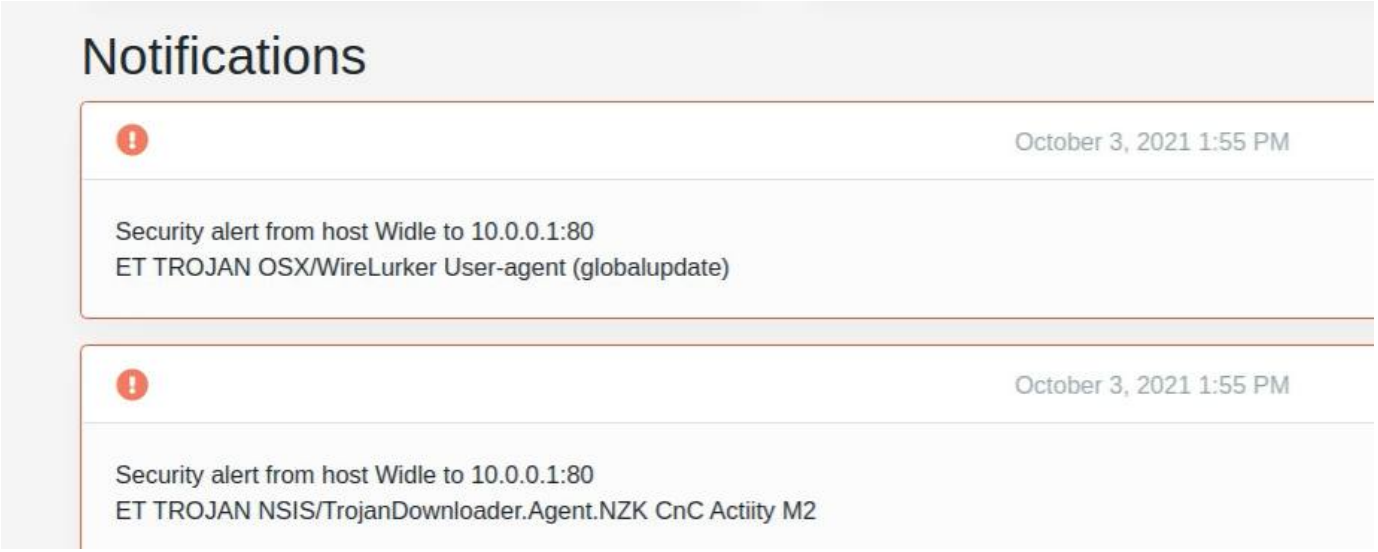
- sleduje kam se různá zařízení připojují
- sleduje lidi na straně LAN
- všechna data skladuje lokálně
- jména serverů z DNS a TLS
  - dávají větší smysl

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

Morče - integrace IDS

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



Budoucnost?

- rychlejší HW
- propracovanější integrace IDS
- rozšíření IDS na IPS
  - snadné UI pro psaní pravidel?
- Turris Sentinel i mimo routery
  - testovací provoz s ISP

Děkuji za pozornost

http://www.turris.cz

http://view.sentinel.turris.cz

http://haas.nic.cz