Turris:Sentinel

Systém sběru dat a Dynamický firewal

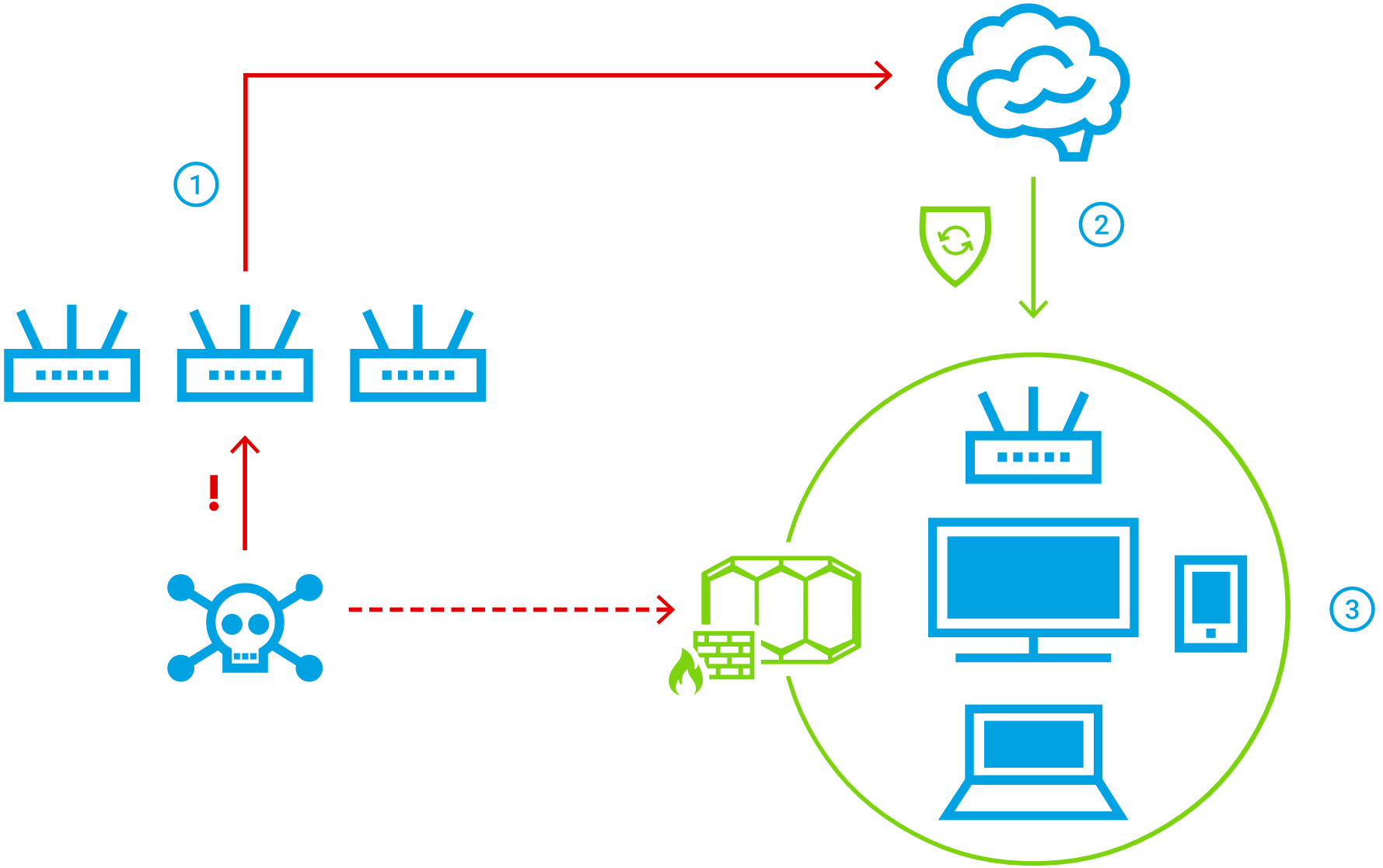
Miroslav Hanák • miroslav.hanak@turris.com

CZ.NIC | SPRÁVCE DOMÉNY CZ

Turris:Sentinel

- Nový „lepší“ systém sběru dat
- Odstranění nedostatků starého systému
- Výstupy
  - Dynamický firewall
  - Greylist
  - Statistiky

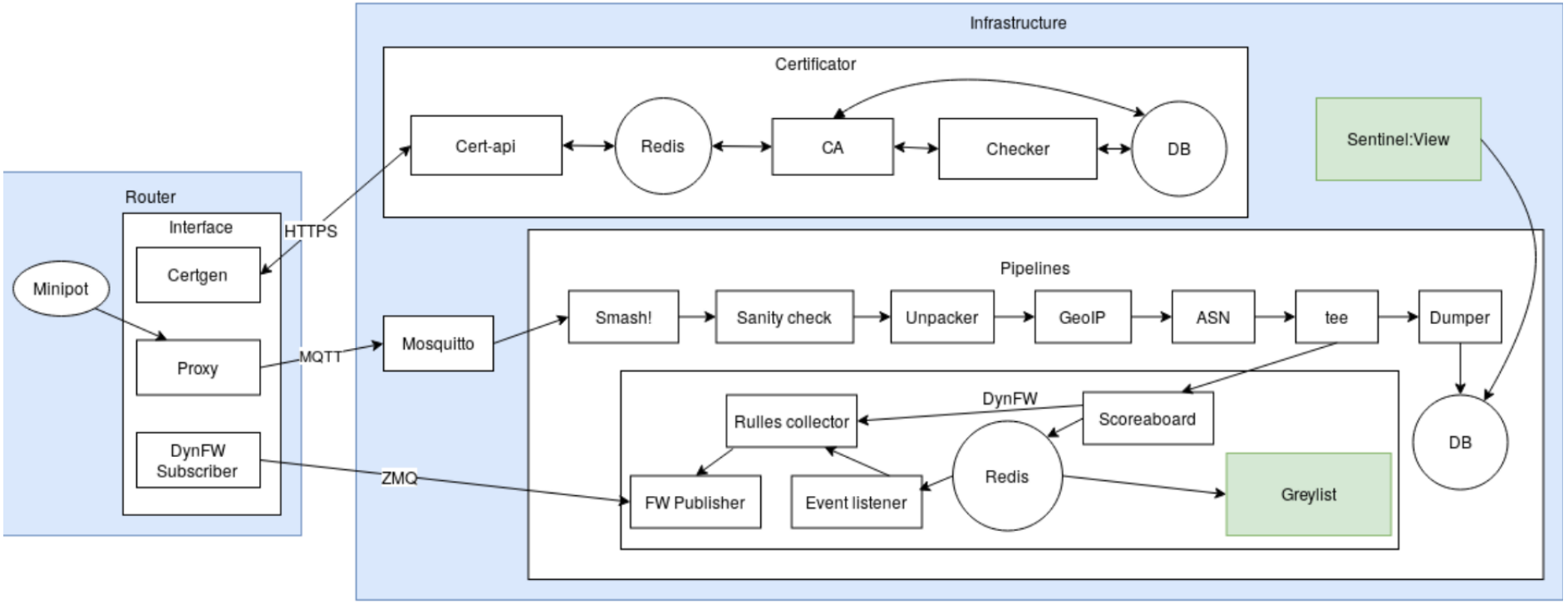
Princip



Základní přehled

- Microservice architektura
  - HW a SW škálovatelnost
- Proudové zpracování dat
  - Technologie message queues – MQTT, ZMQ
  - Realtime
- Vnější strana sítě
  - Uzká část příchozích dat z Internetu
  - Minipot

Detail


Infrastructure
Certificator
Cert-api
Redis
CA
Checker
DB
Sentinel:View
Router
Interface
Certgen
Minipot
Proxy
DynFW
Subscriber
HTTPS
MQTT
ZMQ
Mosquitto
Pipelines
Smash!
Sanity check
Unpacker
GeoIP
ASN
tee
Dumper
DynFW
Rulles collector
Scoreaboard
Redis
FW Publisher
Event listener
Greylist
DB

Minipot

- Minimální honeypot
  - Past, návnada
  - Sledování útočníkovy aktivity
    - Připojení
    - Pokus o přihlášení
- Odesílání dat do centrální DB
- HTTP, FTP, SMTP, Telnet protokoly
  - Telnet již dříve
  - HTTP, FTP, SMTP od 31.7.2020

Minipot

- Emulace nejpoužívanějších serverů
  - Omezí identifikace
  - Splynutí s okolím
  - Žádný přístup k reálnému systému
- Hlavní princip interakce s útočníky
  - Navázaní spojení
  - Neuspěšná autentikace – sběr přihlašovacích údajů
  - Ukončení spojení

HTTP minipot

- Bezestavový protokol
- Request & Response
- Sběr
  - Method
  - URL
  - User Agent header
  - Authorization header
- Žádost o Basic autentikaci

FTP, SMTP minipoty

- Stavové protokoly
- Command & Response
- Trochu složitější interakce než HTTP
- Úvodní session initialization
- Následný proces autentikace
- Sběr
  - Uživatelské jméno
  - Heslo

Telnet minipot

- Ne klasický aplikační protokol
- Vdálený přístup na CLI
- Autentikace není definována protokolem
- Dotaz na přihlašovací jméno a heslo, přihlašovací údaje = uživatelské data

Statistiky získaných dat

Počty a typy zachycených událostí

Akce	HTTP	FTP	SMTP	Telnet	Součet
Connect	713 738	596 491	9 426 192	1 100 912	11 837 333
Message	1 331 058	-	-	-	1 331 058
Login	-	539 282	7 887 771	629 885	9 056 938
Plain	-	-	1	-	1
Součet	2 044 796	1 135 773	17 313 964	1 730 797	22 225 330

Počty unikátních IP adres

	HTTP	FTP	SMTP	Telnet	Dohromady
S připojeními	53 847	4 187	3 706	100 923	147 624
Bez připojení	51 156	2 079	308	14 852	65 327
Úbytek počtu útočníků	5 %	50 %	92 %	85 %	56 %

Statistiky získaných dat

Počty unikátních přihlašovacích údajů

	HTTP	FTP	SMTP	Telnet	Dohromady
Počet unikátních usernames	9 266	71	26 111	250	32 985
Počet unikátních passwords	9 086	721	93 206	1 131	102 601

Sview

- https://view.sentinel.turris.cz/

Děkujeme za pozornost

Miroslav Hanák • **miroslav.hanak@turris.com**

Michal Hrušecký • **michal.hrusecky@turris.com**