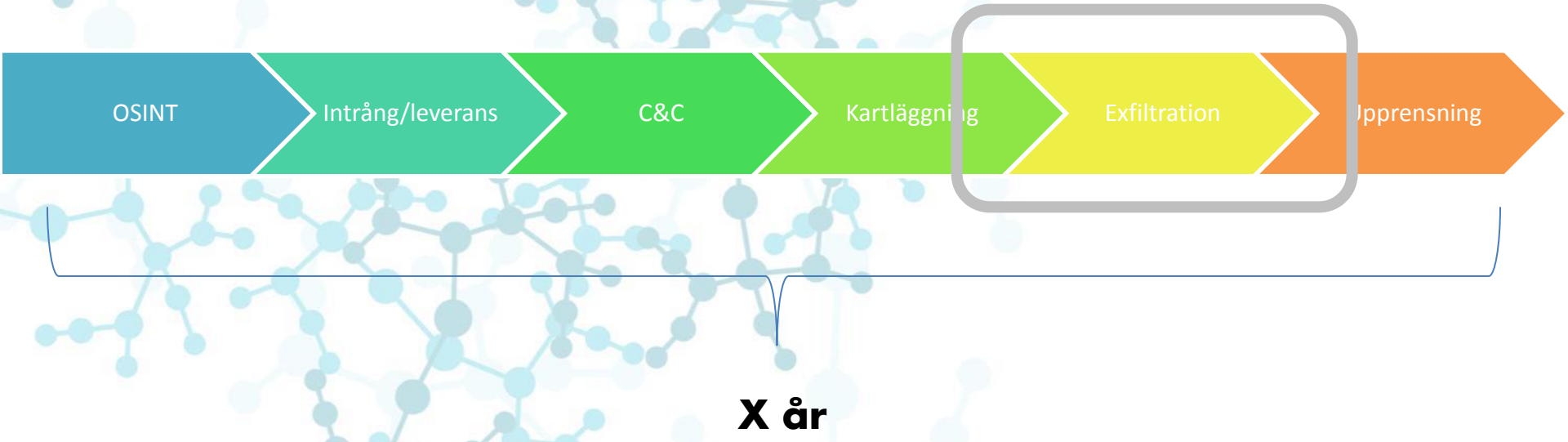
Exfiltration av data

Jonas Lejon
Kryptera.se

Internetdagarna 2014

Definition

Tidslinje


OSINT
Intrång/leverans
C&C
Kartläggning
Exfiltration
Upprensning
X år

Skadlig kod

- Axplock av skadlig kod:
  - Careto
    - Krypterade filer med .GIF
  - Flame
    - AutoCAD via SSH (puttys bibliotek)
  - FrameworkPOS
    - DNS
  - Duqu ”The mask”
    - Krypterade filer med JPG-filändelse

Flyga under radarn

- Steganografi
- Nyttja kända domäner/tjänster
  - Twitter, Dropbox
- Installerade programvaror
- Inga spår på hårddisk
- Under lång tid
- Flera destinationer
- Kryptering
- Modulärt

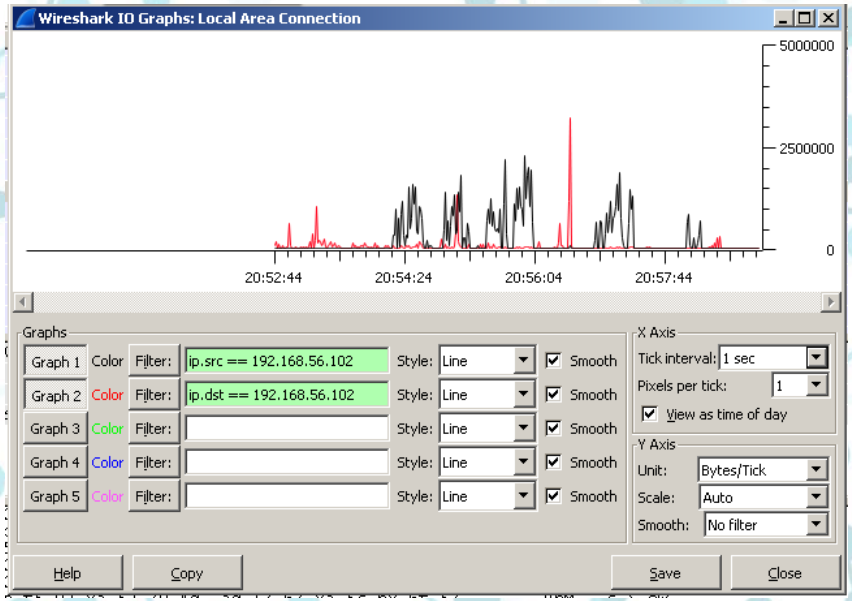
Flyga under radarn

- Situation awareness
  - Airgap
- Unikt för målsystemet
  - Sökväg till progamvara som invärde till nyckelderiveringsfunktion såsom scrypt
  - MAC
- Tor Hidden Services
  - Meek transport (domain fronting)

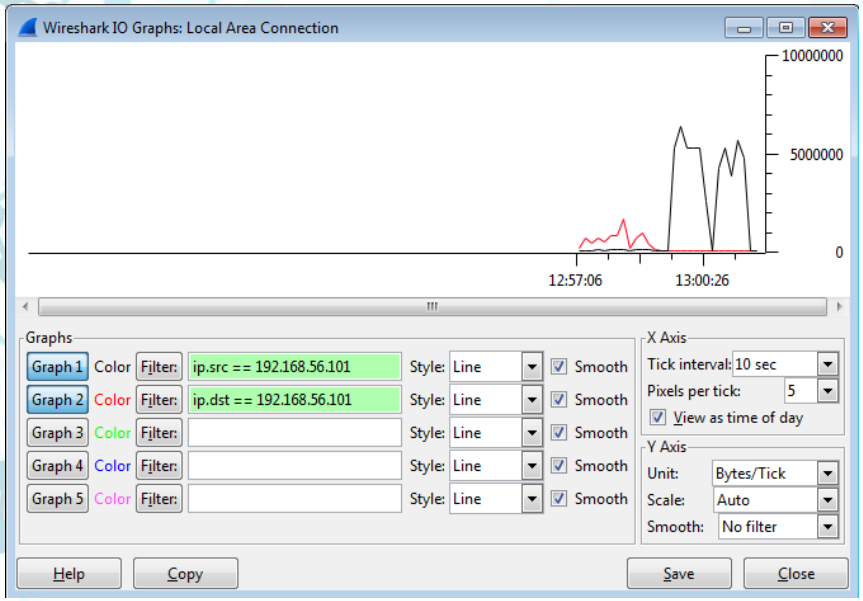
Detektion

- Ändpunkter
- Stora mängder ut/flöden
  - Argus
- Minnesforensik
- Loggning
  - Immunity El Jefe
- IOC
- Honeytokens
- Spela in nätverkstrafik (FIFO)

Exempel



Poison Ivy



Metasploit

Poison Ivy C&C

- **Snort**

```
[**] [1:2013337:4] ET TROJAN PoisonIvy.E Keepalive to CnC [**]
[Classification: A Network Trojan was Detected] [Priority: 1]
11/23-20:57:56.359548 192.168.56.102:1350 -> 192.168.56.101:3460
TCP TTL:128 TOS:0x0 ID:5990 IpLen:20 DgmLen:88 DF
***AP*** Seq: 0x3A0D73D7  Ack: 0x972356A5  Win: 0xF7D0  TcpLen: 20
[Xref => http://www.threatexpert.com/report.aspx?md5=fc414168a5b4ca074ea6e03f770659ef]

[**] [1:2013337:4] ET TROJAN PoisonIvy.E Keepalive to CnC [**]
[Classification: A Network Trojan was Detected] [Priority: 1]
11/23-20:58:50.707274 192.168.56.102:1350 -> 192.168.56.101:3460
TCP TTL:128 TOS:0x0 ID:8784 IpLen:20 DgmLen:88 DF
***AP*** Seq: 0x3A395EC7  Ack: 0x972359A5  Win: 0xFAF0  TcpLen: 20
[Xref => http://www.threatexpert.com/report.aspx?md5=fc414168a5b4ca074ea6e03f770659ef]
```

Twitter: @kryptera

https://kryptera.se
https://triop.se