aramis

Stefano Rinaldi
Cyber Security Analyst

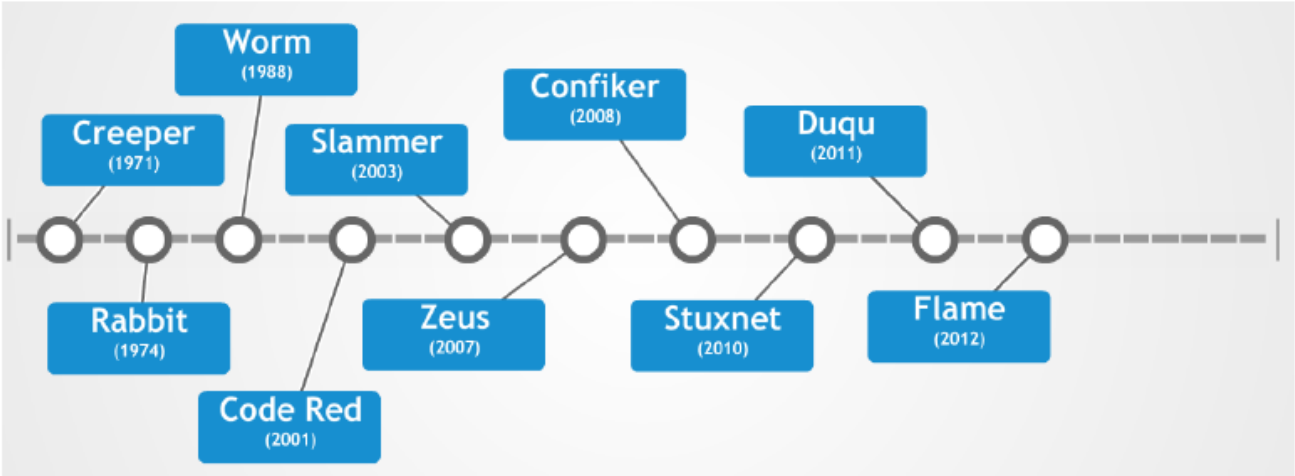
Malware: ieri, oggi e domani

aizoon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

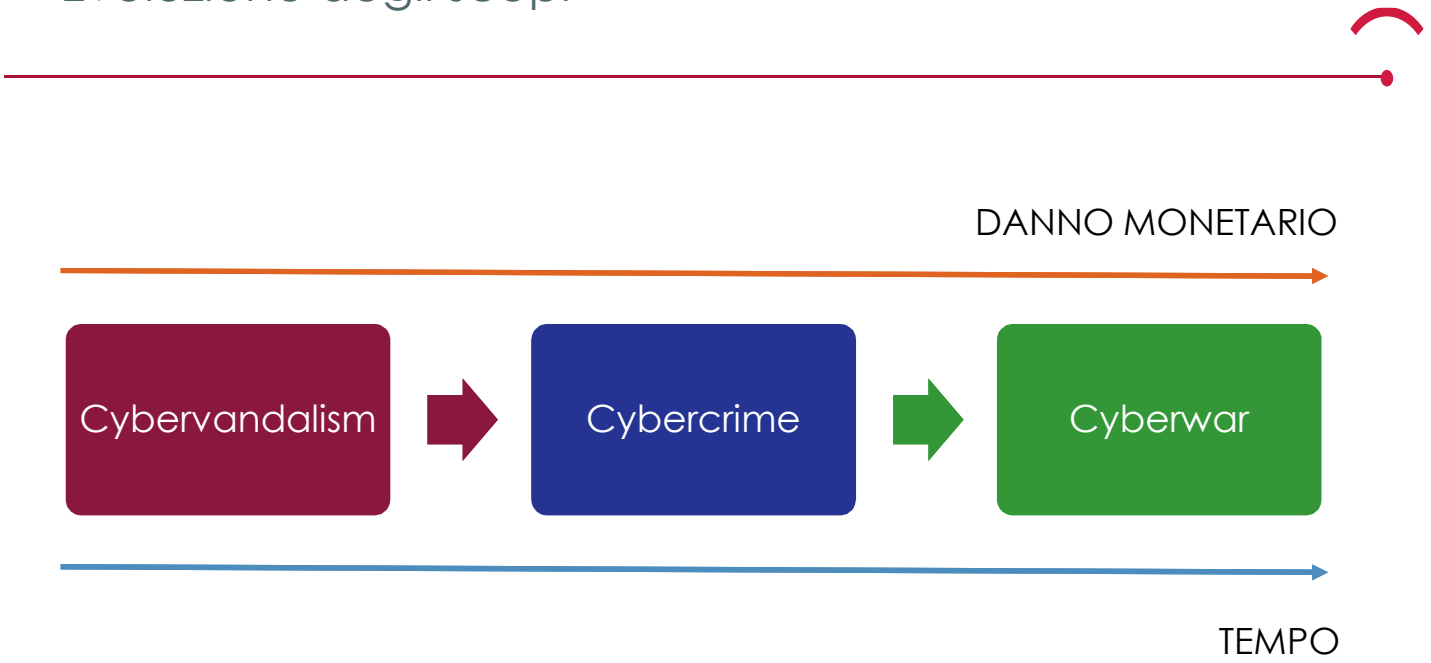
TIG – Cybertech Practical Workshop | Milano 26 Ottobre 2017

- Malware
- Next-Generation Anti-Malware
- Cyber Threat Intelligence (CTI)

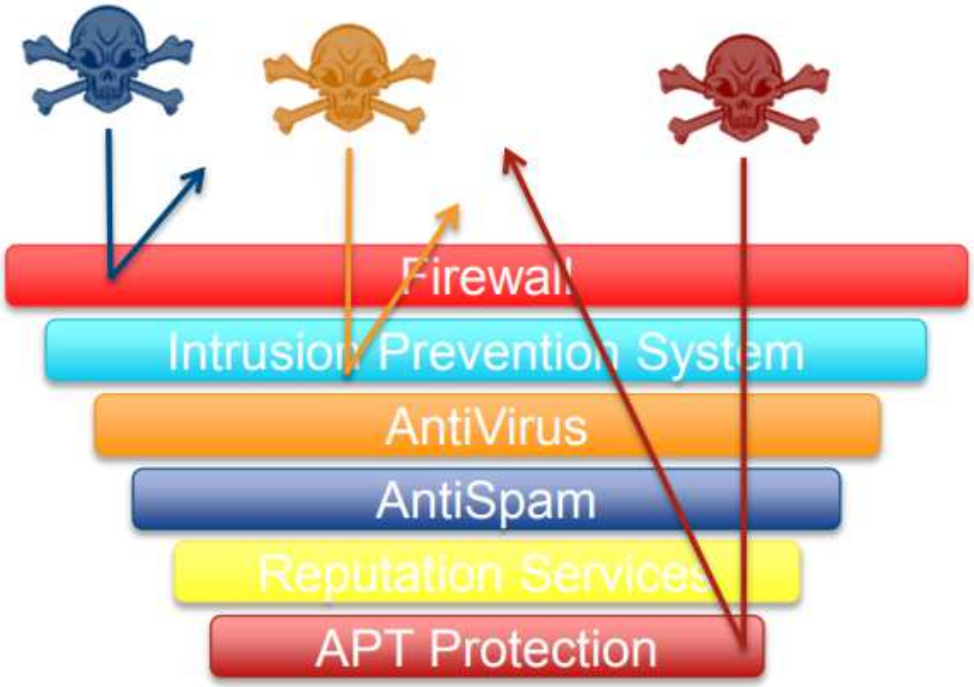
Breve storia del Malware



Evoluzione degli scopi

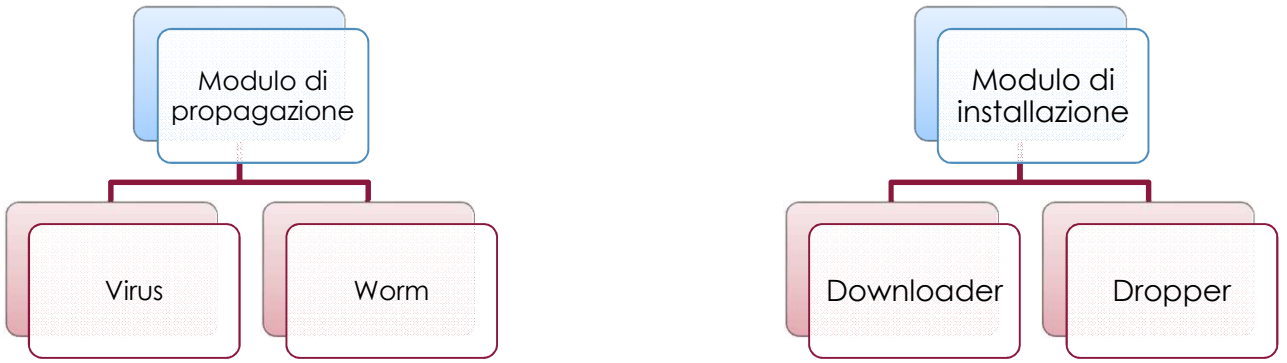


Advanced Persistent Threat (APT)

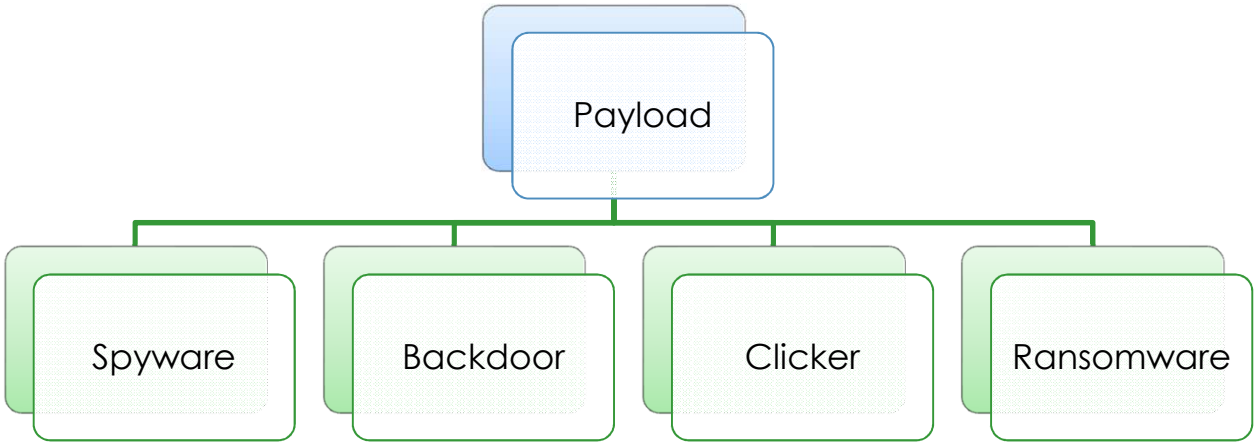


[1] WatchGuard Technologies, Inc. – Advanced Persistent Threats

Classificazione

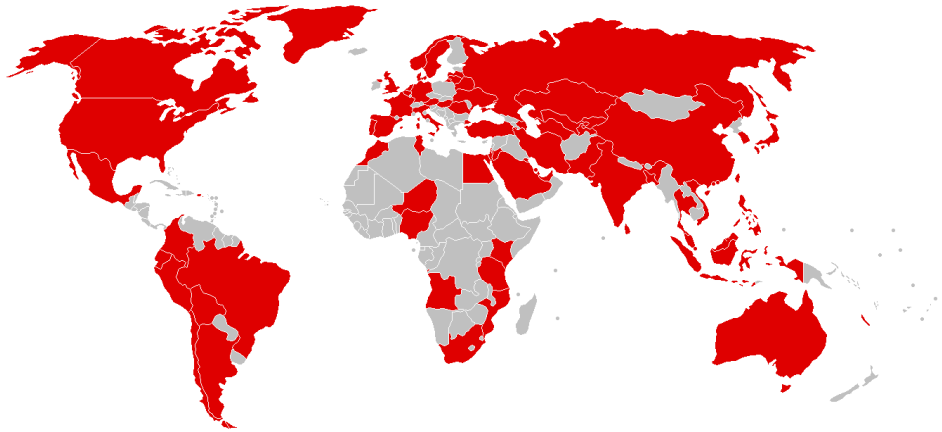


Classificazione



WannaCry Malware

- **Maggio 2017**: Malware su larga scala
- Alias: WCry, WanaCrypt, WannaCrypt, e WanaCrypt0r
  - CARO: Ransom:Win32/WannaCrypt.A!rsm
- Componenti WannaCry: Dropper, Worm, Backdoor, Ransomware



WannaCry Malware

- The Shadow Brokers (TSB)
  - Arsenale di Hacking Tools della NSA
    - EternalBlue
      - **Marzo 2017**: Patch Vulnerabilità SMB
      - **Aprile 2017**: The Shadow Brokers (TSB)
      - **Maggio 2017**: WannaCry
    - DoublePulsar

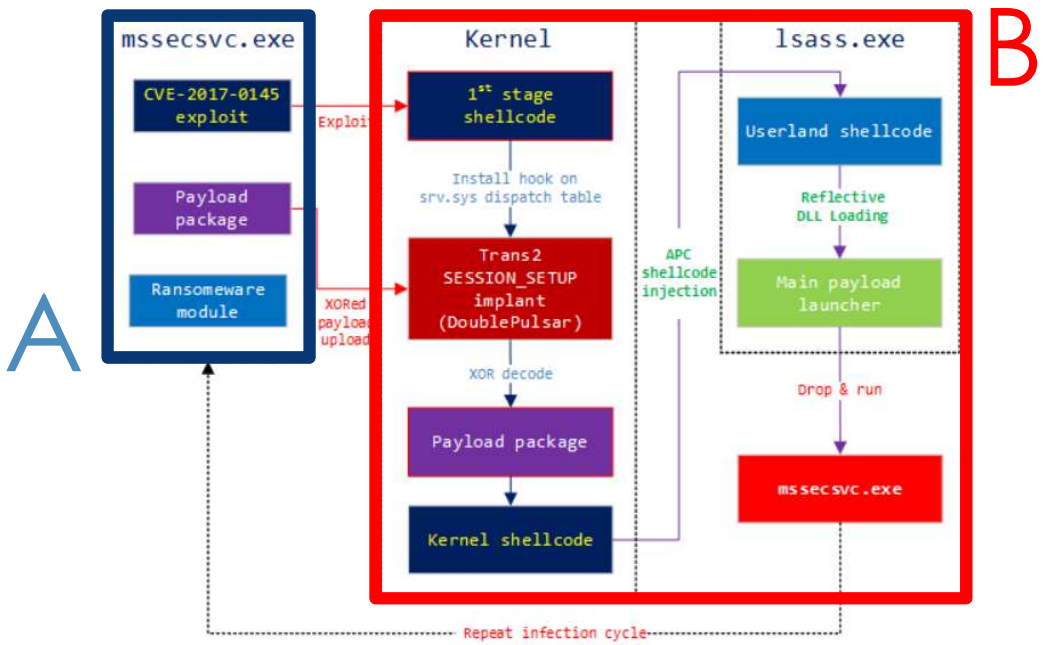
WannaCry Malware

- Componente Dropper

```
mov     esi, eax
push    0               ; lpszHeaders
push    ecx             ; http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
push    esi             ; hInternet
call    ds:InternetOpenUrlA
mov     edi, eax
push    esi             ; hInternet
mov     esi, ds:InternetCloseHandle
test    edi, edi
jnz     short exit
call    esi ; InternetCloseHandle
push    0               ; hInternet
call    esi ; InternetCloseHandle
call    dropper_main
```

WannaCry Malware

- Componente Worm

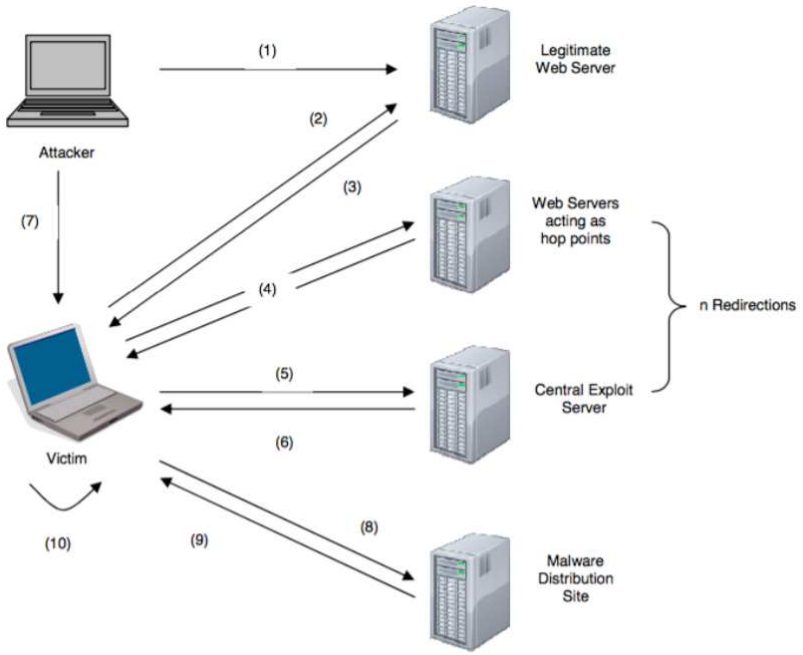


WannaCry Malware

- Componente Ransomware

WannaCry Malware

- Paziente 0 – Drive-by Download



NotPetya Malware

- **Giugno 2017**: Malware su larga scala
- Componenti del Malware: Dropper, Ransomware e Worm
- Punti in comune con WannaCry:
  - Cifratura file
  - Kill-Switch
  - Movimenti laterali mediante Exploit (EternalBlue)
- Differenze rispetto WannaCry:
  - Sovrascrittura del MBR + Cifratura MFT
  - Tecniche anti-analisi
  - Movimenti laterali mediante furto di credenziali

- Malware
- Next-Generation Anti-Malware
- Cyber Threat Intelligence (CTI)

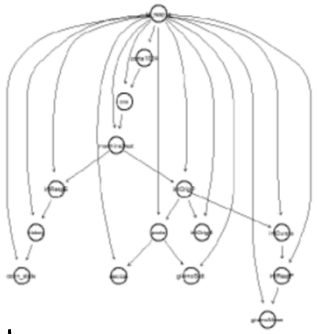
Specifiche di un Malware

Genericamente un qualsiasi sviluppatore di Malware segue alcune «specifiche tecniche» durante la realizzazione del proprio «prodotto»:

- Deve essere difficile da **individuare**;
- Deve essere **portabile**;
- Deve essere difficile da **rimuovere**;
- Deve essere **funzionale**;
- Deve essere difficile da **analizzare**;
- Deve essere **persistente**.

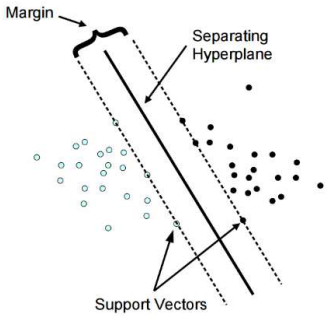
Next-Generation Anti-Malware

- Artificial Intelligence (AI) e Machine Learning (ML)
- Automated Malware Analysis (VMI)
- Cyber Threat Intelligence (CTI)



Bayesian Network

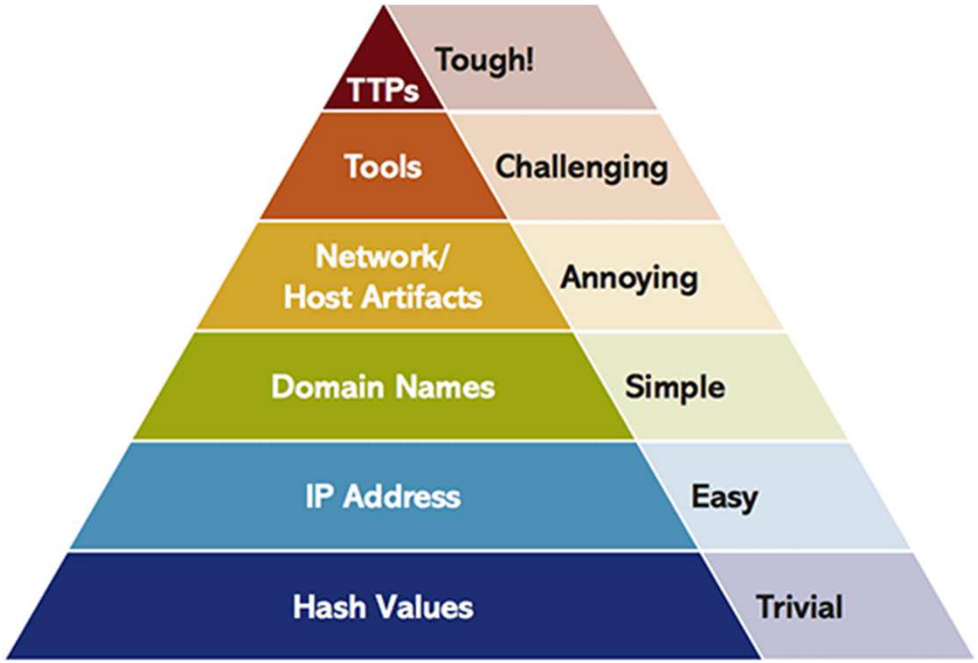
Support Vector Machine



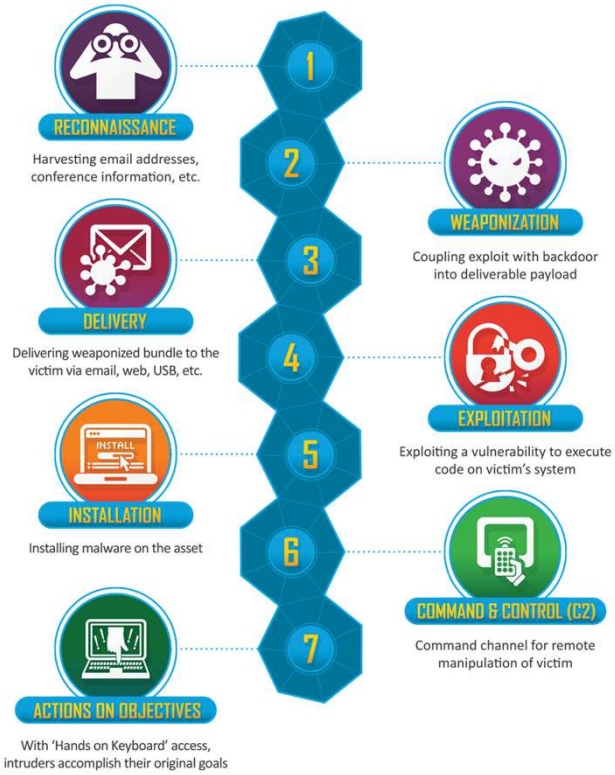
Anomaly detection

- Malware
- Next-Generation Anti-Malware
- Cyber Threat Intelligence (CTI)

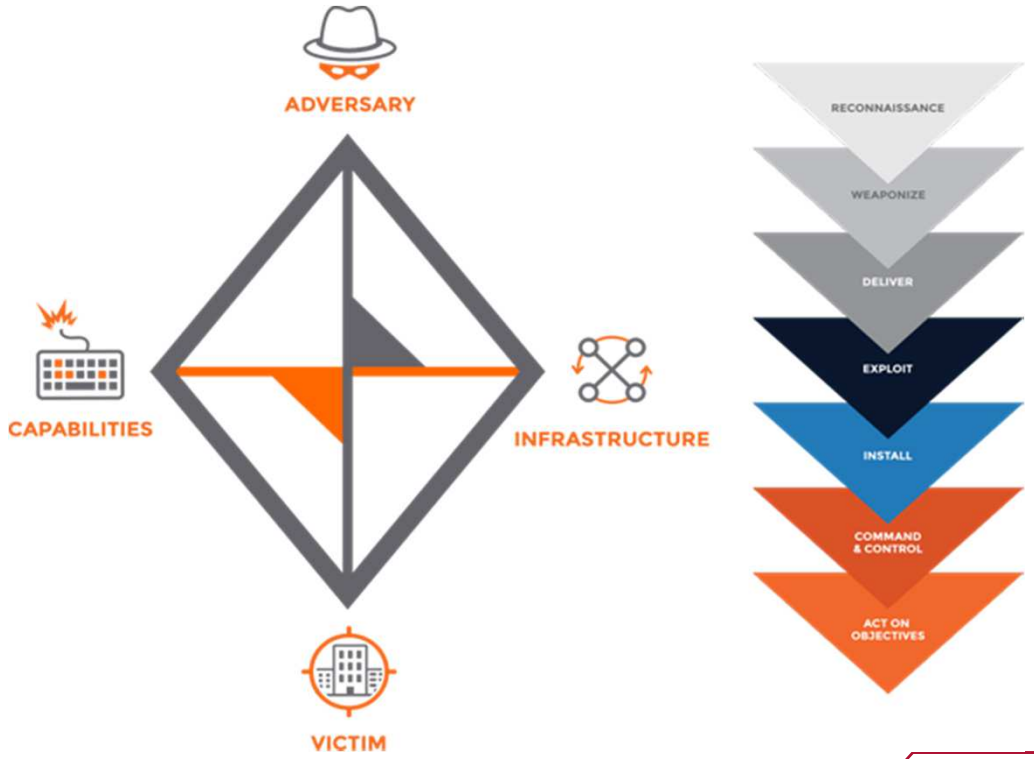
The Pyramid of Pain



The Cyber Kill Chain



The Diamond Model



aramis

GRAZIE!

Contatti:
www.aramisec.com
www.aizoongroup.com
stefano.rinaldi@aizoongroup.com

aizOon AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING