Identifikácia fáz útoku v počítačovej sieti

Bc. Marek Dorko

Vedúci práce: doc. RNDr. JUDr. Pavol Sokol, PhD.

Konzultant: RNDr. Tomáš Bajtoš

ÚINF

17. 5. 2023

Motivácia

- V súčasnosti počítačové systémy hrajú dôležitú úlohu
- Útočníci vyvíjajú nové techniky a nástroje
  - Exfiltrácia údajov
  - Informácie o kreditných kartách
- Zložité útoky – viackrokové/viacfázové
- APT skupiny
- Detekcia týchto fáz

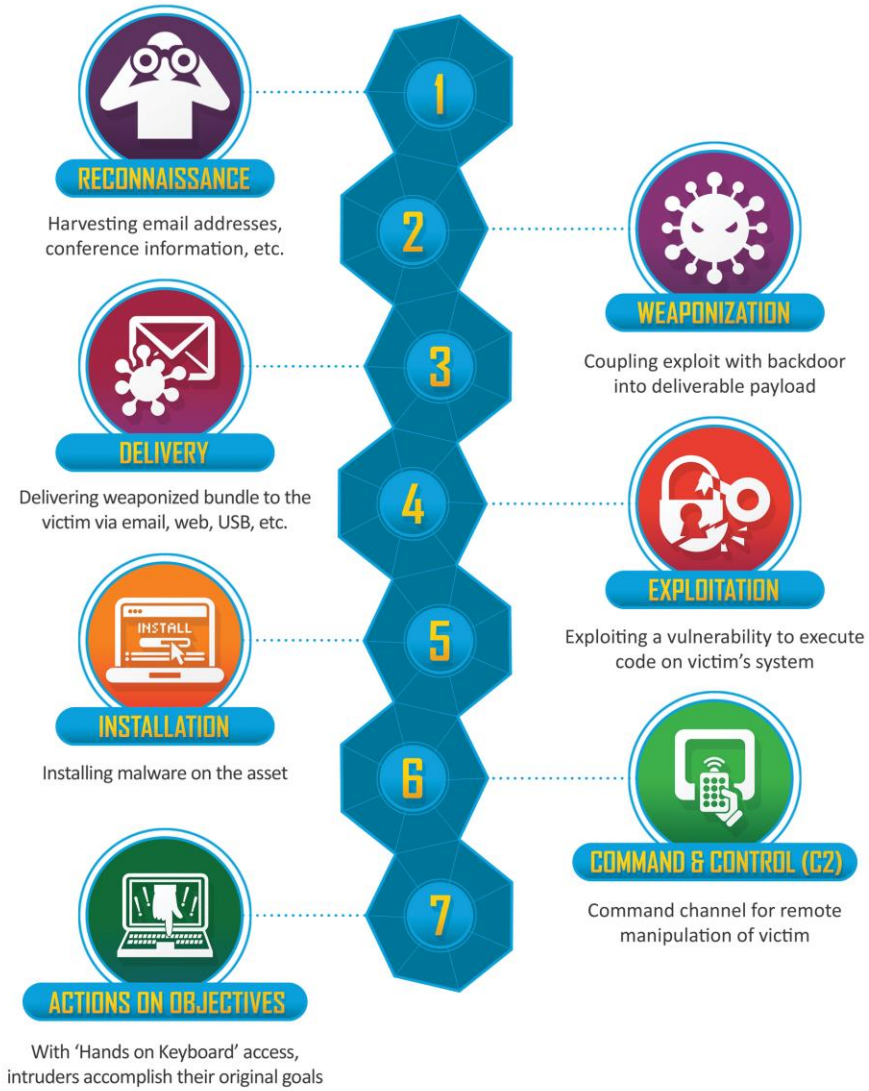
APT skupina

- APT
  - Advanced – cielené
  - Persistent – mesiace, roky
  - Threat – schopnosti, možnosti
- Zoskupenie útočníkov (štátne organizácie)
  - Cielené, sofistikované útoky voči vládnym organizáciám, korporáciám...
  - Pokročilé nástroje a techniky

Modely životného cyklu útokov

The cyber kill chain

- Vyvinutý spoločnosťou Lockheed Martin
- Kroky útočníka od prípravy až po naplnenie cieľov

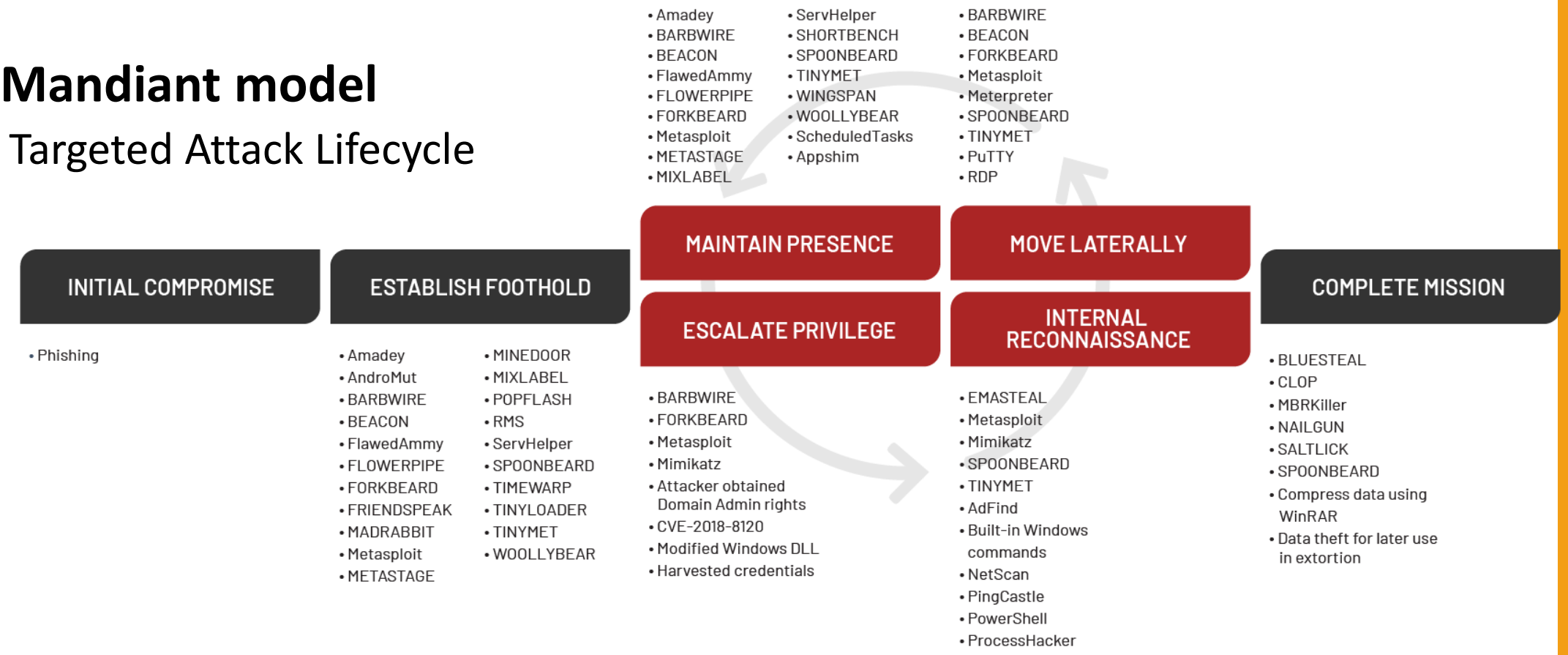


https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Modely životného cyklu útokov

The Mandiant model

- Targeted Attack Lifecycle

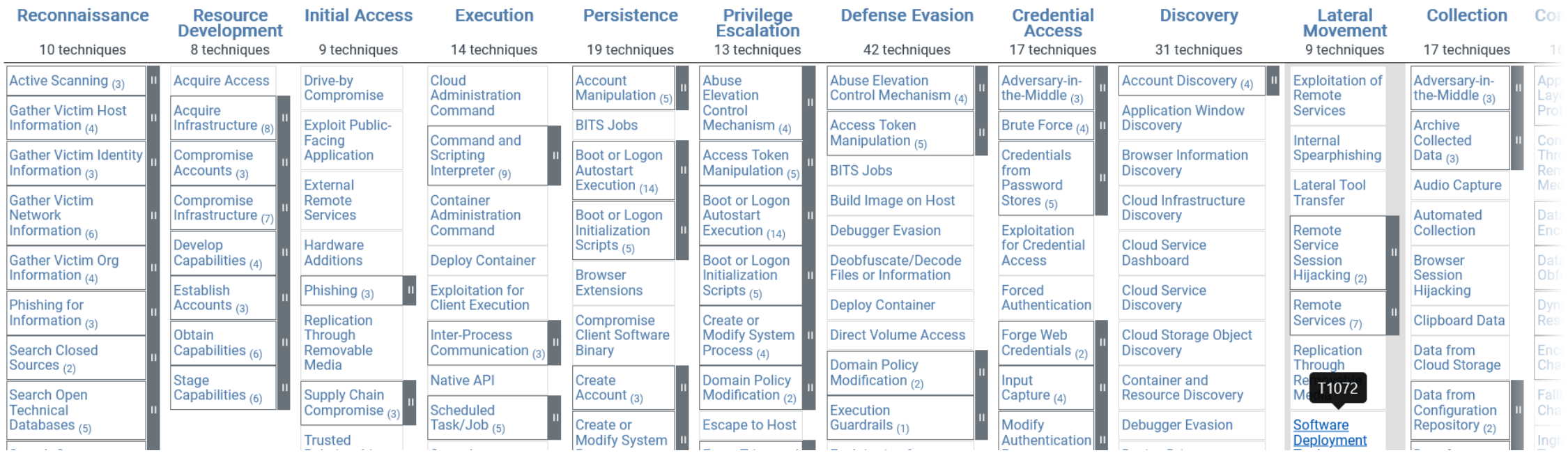


https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

Modely životného cyklu útokov

MITRE ATT&CK

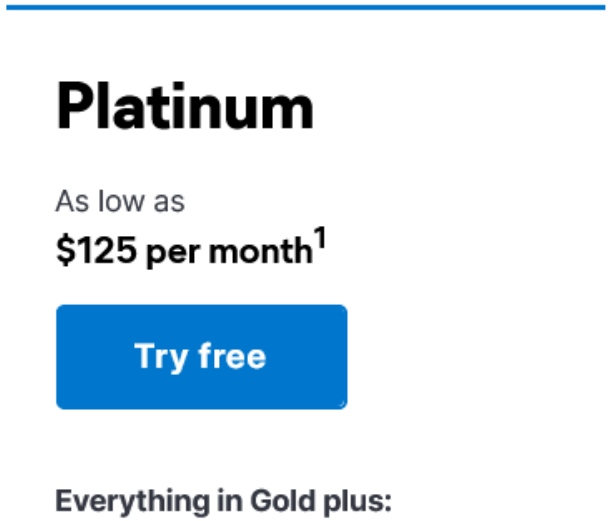
- **A**dversarial **T**actics, **T**echniques **and** **C**ommon **K**nowledge



https://attack.mitre.org/#

ELK stack

- ELK
  - Elasticsearch – vyhľadávací nástroj
  - Logstash – nástroj na príjem údajov z rôznych zdrojov
  - Kibana – nástroj na vizualizáciu údajov, analýzy logov a časových radov
- Machine learning modul
- Platinum balík
  - Hľadanie anomálií, outliers
  - Predikcia



Prehľad podobných prác

- Cyber Attacks Detection Using Open Source ELK Stack
  - Dáta z koncových zariadení aj sieťovej prevádzky
  - VirusTotal
  - GeoIP – geolokačné informácie
  - Integrácia ELK stack s MISP (Malware Information Sharing Platform)
  - ML algoritmy v Elastic stack – anomálie v sieťovej prevádzke

Prehľad podobných prác

- Developing an Adaptive Threat Hunting Solution: The Elasticsearch Stack
  - Diplomová práca
  - Unsupervised ML – hľadanie anomálií
  - Vykonané útoky na základe Mandiant modelu a vyhodnotené v ELK stack

Ďalšie články

- Detection of advanced persistent threat using machine-learning correlation analysis
  - Systém MLAPT, presne a rýchlo odhalí a predpovedá APT útoky

- Analysis of hidden Markov model learning algorithms for the detection and prediction of multi-stage network attacks

Najbližšie kroky

- články
- Elasticsearch na lokálnom stroji
- pozrieť sa bližšie na dataset

Ďakujem za pozornosť.