

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

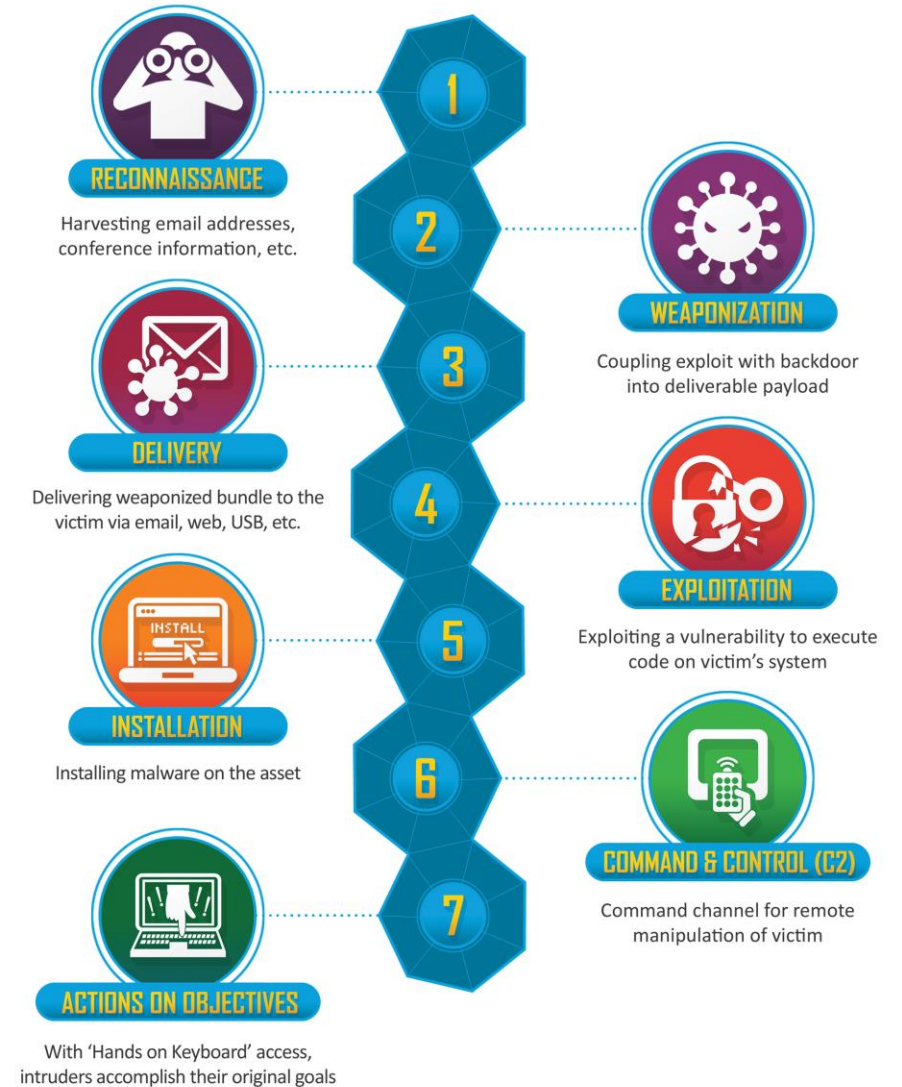
APT skupina

- 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

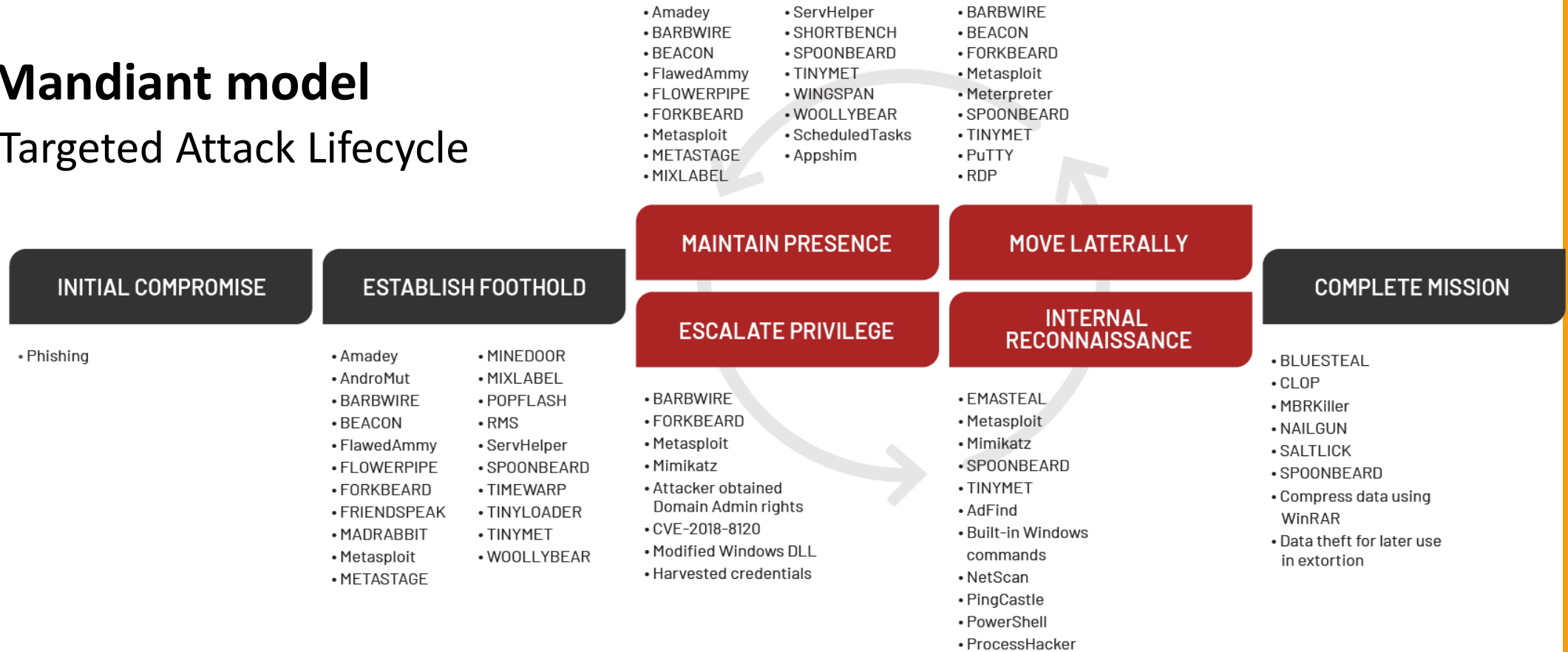
- Vyvinutý spoločnosťou Lockheed Martin
- Kroky útočníka od prípravy až po naplnenie cieľov



Modely životného cyklu útokov

The Mandiant model

- Targeted Attack Lifecycle



Modely životného cyklu útokov

MITRE ATT&CK

- Adversarial Tactics, Techniques and Common Knowledge

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Communication 16 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	App Layer Protection
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Command and Control
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Remote Services
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encrypted
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking	Data Obfuscated
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Remote Media	Clipboard Data	Dynamic Resource Discovery
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment	Data from Cloud Storage	Encrypted Channels
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted	Scheduled Task/Job (5)	Create or Modify System	Escape to Host	Direct Volume Access	Modify Authentication	Container and Resource Discovery		Data from Configuration Repository (2)	Fallible Channels
						Domain Policy Modification (2)		Debugger Evasion			Ingress

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

Platinum

As low as

\$125 per month¹

[Try free](#)

Everything in Gold plus:

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.