8 Feb Afternoon

08 February 2020 14:26

Network Security

Attack Scenarios

Kill chain phase	Scenario	Possible use cases
Recon	Attack gathering info about targeted network enumeration/scanning activity	Host scan/ Port scan
Weaponization	Attacker obtains info, drafts emails and sends to plausible targets	
Delivery	Sends email from Gmail	Zip attachment with password in email text
	Email and attachment pass company AV protection	Suspicious file type
Compromise	Target opens email	Endpoint malware infection
Installation	.exe is executed, uses an unpatched vulnerability. Installs several files in sys_root, adds registry keys	• New Program (not whitelisted) executed • Suspicious Proxy action
C2	All C&C communication is from compromised computer(s) to C&C servers via Http during local office hours	Domain accessed with None/Pending category
Actions	Actions on Objectives (Lateral Movement/Data exfiltration/AD compromise)	• Local admin usage • Same user credentials on multiple hosts

UEBA:

- Detects:
  - Rare behaviour
  - Abnormality / Spike
  - Multi Stage phase co-relation
  - Identity Analytics
  - Access Outliers

Endpoint Security - AV

- Signature based
  - Identify the known threats by matching/comparing with hash list or file code
- Heuristic Based
  - Examining malware source code, these malicious codes are compared with known behaviours recorded in heuristic database.
- Behaviour Based
  - Capable of identifying zero day threat and uncovering the unknown threat upon execution
  - Mimikatz tool

Email Spoofing protection

- Sender policy framework (spf)
- Domain Keys identified Mail (DKIM)
- DMARC
  - Domain based message authentication, reporting, conformance

Cloud Security

- Azure AD
- Office 365
- Exchange Office
- OneDrive
- Power BI
- SharePoint
- Teams
- AWS Cloud Trail

Cloud Security - Threats

- Compromised accounts and insider threats
- Data Leakage
- Insufficient security awareness
- Malicious third part apps
- Malware
- Phishing
- Ransomware
- BYOD