Responding to Incidents: Fighting Trickery with Planning

Varun Kukreja
Senior Program Manager,
Cyber Security
Middle East, Turkey and Africa
GIAC GSTRT, CISSP, CCSP, CISA, ITIL, ISO 27LA, ISO 20LA
Art of War and Cyber Security Today

Art of War (512BC)

• “If you know the enemy and know yourself, you need not fear the result of a hundred battles”

• “All war is based on deception”

• “If your enemy is secure at all points, be prepared for him. If he is in superior strength, evade him”

Now (2020)

• What was true then, is true NOW! Only the terms have changed

• Knowing your own weaknesses, vulnerabilities and risks may not be enough, it is essential to understand the trends of security and risk management

• Deception is often used by adversaries as well as defenders

• Not all attacks are worth persuading, sometimes deterrence or evasion is better
Rise of Security Incidents and History

1903
Nevil Maskelyne disrupts John Ambrose Fleming’s demonstration by sending insulting Morse Code message through the auditorium’s projector.

1941
The Enigma machine cracked by British Cryptologists.

1980s
- NY Times describe the term Hacker
- Ian Murphy is convicted as the first felon for breaking into AT&T Computers
- Trojan horse is coined
- First National Bank of Chicago is subjected to a 70M USD computer theft

1990s
- First virus created
- 10M USD siphoned from Citibank transferred to multiple accounts in the world
- Hackers alter US DOJ, CIA and Air Force Websites

2000s
- ILOVEYOU Worm introduced
- DOS Attacks emerge
- Anonymous formed
- Turkish hacker iSKORPiTX hacks 21,549 websites
- FBI finds 1M botnet victims
- Google reveals IP theft

2010s
- Stuxnet attack on Iran Nuclear facility
- Bank of America breach – 85,000 Credit cards affected
- PlayStation Network, 77M PII Leak
- Bangladeshi hacker defaces 700,000 websites
- Yahoo Leak – 3B Records
- Facebook data breach – 540M Accounts
- EasyJet – 2020 – 9M accounts – 18B Pound Liability
Shift in TTPs

- Targeted Attacks
- Continued Phishing
- Persistent Attacks
- Weakest Link Compromise
- Zero Days Reliance
- Advanced Intelligence
What is Cyber Kill Chain

Developed by Lockheed Martin

Developed as part of the Intelligence driven defense model for identification and prevention of cyber intrusions activity

Helps understand and combat ransomware, security breaches and Advanced Persistent Threats (APTs)
Cyber Kill Chain - Explained

- Reconnaissance
- Exploitation
- Intrusion
- Privilege Escalation
- Lateral Movement
- Obfuscation
- Exfiltration
- Denial of Service
Planning Response

Post Incident Analysis

Preparation

Containment, Eradication and Recovery

Detection

Analysis
Summary

Remember, All warfare is Deception
Don’t Firefight, Plan for them
Perform Threat Modeling
Leverage Advanced Technology
Plan for Deterrence