

1 | Targets

CNI/Defence

Command & Control
Tactical/Strategic Intel
R&D
Personnel
Asset Inventory
.....
Systems
Sales, Mktg, Finance, HR,
Logistics, R& ad, Operations

Corporate

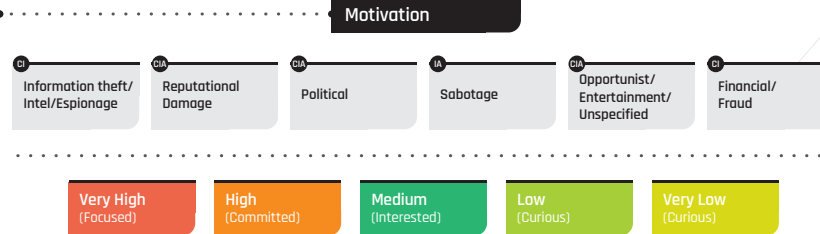
Business Data (IP)
Customer Data
Personnel Information
Config Data Host/Device
Credential Data
User Data Spreadsheets etc
.....
Systems
Sales, Mktg, Finance, HR,
Logistics, R&D, Operations

Personal

Biographic/Personal Data/ID
Banking/Credentials
Online Shopping Credentials
Social Media Credentials
.....
Systems
EUD, Host, Comms, Storage

2 | Threat Source

Threat Source



3 | Threat Actor

Threat Actor

Threat Group

Indirectly Connected (IC)	Bystander (BY)	Un-Trusteed
Physical Intruder (PI)	Person Within Range (PWR)	
Service Consumer (SC)	Service Provider (IC)	Trusteed
Shared Service Subscriber (SSS)	Normal User (BY)	
Handler (HAN)	Privileged User (PU)	

Capability

Full time, Qualified Expert	Trained Computer User	Average Untrained User	Minimal Experience
Bespoke Exploit tools + Physical attack(s)	Customise Open Source tools + physical attacks	Use popular Open Source/free tools	Deploy basic GUI based tools
Large physical, compute & net capacity	Deploy significant hardware	Small quantity of equipment	Small quantity of equipment
Several months/years	Weeks/Months	Few days/Weeks	Hours/days
			Use/access only the tools on system
			Use plug-n-play USB keyloggers
			Few hours

4 | Attack Construction

4a | Reconnaissance

OSInt	<ul style="list-style-type: none"> DNS Registration Info Google Hacking Archived Ref/Websites Recruitment
Social Engineering	<ul style="list-style-type: none"> Passive Active
Electronic Scanning	

4b | Exploit Vector/Payload Exploits

Vulnerabilities	Exploits
<ul style="list-style-type: none"> SQL Injection Backdoor Memory Leakage Vendors/Partners Remote Code Execution Cross Site Scripting Cross Site Request Forgery 	<ul style="list-style-type: none"> Zero Day Password Mngt Protocol Stack Buffer Overflow Physical Access User A/C Mngt Spear Phishing RAT/Trojan Root Kits Worms/Virus (D)DOS DNS/NTP Amplification APT DNS Poisoning Pharming Session Hijacking Man-In-Middle

Tools	<ul style="list-style-type: none"> Maltego Whois Shodan Nexpose Exploit Framework(s)
	<ul style="list-style-type: none"> NSlookup Nmap Nessus Cain & Abel Immunity CANVAS
	<ul style="list-style-type: none"> Exploit-DB.com Google Hacking Metagoofil/Exiftool Wireshark/TCPDump Low Earth Orbit Ion Cannon

5 | Attack Vectors

Channel

Social Engineering		
People	Process	Physical
Management		
Fixed	Wireless	
Optical	Physical	
User		
Fixed	Wireless	
Optical	Physical	
Partner		
Fixed	Wireless	
Optical	Physical	
Public		
Fixed	Wireless	
Optical	Physical	
Non-specific Physical		
Air	Land	Sea
Social Media		
Fixed	Wireless	Optical

Delivery

Voice	E-mail
USB	Keyboard Access
Web	Signalling
Domain User	Optical
Physical Object	

5c | Detection Evasion

Rotating Proxy hosts
Fast Flux DNS
Domain Generation
MAC Spoofing
IP Address Spoofing
Host Log Manipulations
Device Log Manipulation
Proxy
Dark Web