encode
cyber threat management

# Cyber Threat Landscape

## 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** — **Motivation**

| CI | CIA | CIA | IA | CIA | CI |
|---|---|---|---|---|---|
| Information theft/ Intel/Espionage | Reputational Damage | Political | Sabotage | Opportunist/ Entertainment/ Unspecified | Financial/ Fraud |

| Very High | High | Medium | Low | Very Low |
|---|---|---|---|---|
| (Focused) | (Committed) | (Interested) | (Curious) | (Curious) |

## 3 | Threat Actor

**Threat Actor** — **Capability**

| Full time, Qualified Expert | Trained Computer User | Average Untrained User | Minimal Experience |
|---|---|---|---|

**Threat Group**

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

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

## 4 | Attack Construction

### 4a | Reconnaissance

**OSInt**
- DNS Registration Info
- Google Hacking
- Archived Ref/Websites
- Recruitment

**Social Engineering**
- Passive
- Active

**Electronic Scanning**

### 4b | Exploit Vector/Payload Exploits

**Vulnerabilities**
- SQL Injection
- Backdoor
- Memory Leakage
- Vendors/Partners
- Remote Code Execution
- Cross Site Scripting
- Cross Site Request Forgery
- Zero Day
- Password Mngt
- Protocol Stack
- Buffer Overflow
- Physical Access
- User A/C Mngt

**Exploits**
- Spear Phishing
- RAT/Trojan
- Root Kits
- Worms/Virus
- (D)DOS
- DNS/NTP Amplification
- APT
- DNS Poisoning
- Pharming
- Session Hijacking
- Man-In-Middle

**Tools**
- Maltego
- NSlookup
- Exploit-DB.com
- Whois
- Nmap
- Google Hacking
- Shodan
- Nessus
- Metagoofil/Exiftool
- Nexpose
- Cain & Abel
- Wireshark/TCPDump
- Exploit Framework(s)
- Immunity CANVAS
- 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

### 5a | Detection Evasion

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