THE CYBERTHREAT HANDBOOK

**Attacker Profiles**

- **Government**
- **Political destabilisation**
- **Counter-espionage**

**Main Countries Targeted**

- **United States**
- **Israel**
- **South Korea**

**Main Sectors Targeted**

- **Business & retail**
- **Media & Pharma**
- **Digital services**

**Typical modus operandi of attackers**

- **Targeting**
- **Collection**
- **Exploitation**
- **Initial access**
- **Exfiltration**
- **Persistence**
- **Lateral movement**
- **Privilege escalation**
- **Deploy**

**Main Techniques**

- **Steal account names and passwords**
- **Exploit weaknesses**
- **Certification dumping**
- **Obfuscate and compress**
- **Obfuscate/Decode**

**Most-affected geographies**

- **Southeast Asia**
- **Europe**
- **Middle East**

**Most-impacted sectors**

- **Media**
- **Defence**
- **Government**

**Motives**

- **Financial resources**
- **Brand/reputational damage**
- **Data destruction**
- **Proselytism**

**Thales and Verint analysts**

- Identified the four major categories
- Classified approximately 60 groups of attackers and defined the "typical" modus operandi and procedures (TTPs) out of the hundreds of commonly used tactics, techniques, and procedures.

**Most common attack techniques**

- Used by more than 50% of the attackers analysed.

**Number of attacks**

- Analysis of 490 attack campaigns.
- Analysis of 56 nation states.

**Sources**

- The Cyberthreat Handbook 2019, Thales, Verint