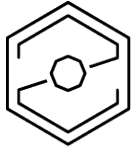


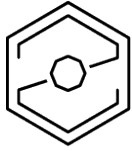
Countermeasures

Reconnaissance	<ul style="list-style-type: none">• Attack Surface Monitoring• external recon• know what you have
Weaponizing	<ul style="list-style-type: none">• NIL
Delivery + Exploit	<ul style="list-style-type: none">• Patch patch patch• Minimize Attack-Surface, make it harder for the attacker• no Low-Hanging-Fruits
Installation vertical Movement	<ul style="list-style-type: none">• Real DMZ for external facing• Proxies• Defense-In-Depth-best-practices• HIDS & NIDS• network-separation• application whitelists• restrict workstation to workstation communication (contains ransomware/outbreak, AD)• HoneyPots & Cloaking
C&C	<ul style="list-style-type: none">• Firewall all outgoing• proxy all outgoing• HIDS & NIDS• Whitelist accepted Destinations• HoneyPots & Cloaking
DataExfil	<ul style="list-style-type: none">• See C&C



Actions per Actor

Actor	Recon	Weaponizing + Delivery	Exploit + Installation	C&C + Objectives
Botnet-Infection [1]	Scan or all targets	Known exploits	Exploitation and bot-drop	bot-operation
Direct Attack / APT [2]	Stealth, OSINT	0days, Custom made by identified targets	Single-shot + beachhead	Critical databreach
James Bond	Like APT			
Malicious Insider	Not needed	Not needed	Not needed	Databreach or chaos
Ransomware	Scans and bruteforce	Known exploits, sometimes 0days, > 24hrs	Implant and beachhead	Dataexfil and exncryption
Skiddos, Politics	Scans and bruteforce	Known exploits, old	Sometimes, mostly look around	+look around



Explanations:

[1]

- Cryptotrojan
- Mal/Spam – Bots
- DDoS-Bots

[2]

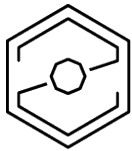
- StateActors
- Competitors
- HighProfile - Hacking

[3]

- an attack from within the datacenter (other machine hacked first) or
- something that was not initially directed towards you, but ended on one of your systems by mistake or chance

Scores:

- A – highly likely
- B – most likely
- C – possible
- D – not likely
- E - impossible



CyberKillChain / ATTACK-Matrix

Detectionpossibilities by Actors

Actor	Automation	Noisyness	Artefacts	Documented	IOCs
Botnet-Infection [1]	high	high	many	yes	many
Direct Attack / APT [2]	med/low	med/low	luck	sometimes	some
James Bond	low	low	luck	no	no
Malicious Insider	low	low/med	some	no	no
Ransomware	high	med	some	yes	many
Skiddos	low	high	some	sometimes	some
Bad Luck	?	?	?	?	?
By-catch [3]	?	?	?	?	?