



# UNWEED

Active  
Attack  
Detection



J A V E L I N

**Mission:**

**Stop attackers in their tracks**



# Top Cyber Attacks

Campaign / Threat Name	Time	Detected by	Methods
DUQU 2.0	2015	KASPERSKY	Topology Recon + Credential Theft
Epic Turla	2014 – Today	KASPERSKY + Symantec	Topology Recon
SAMAS Ransomware	2015 – Today	Microsoft + intel	Topology Recon
Poseidon APT	2015 – Today	KASPERSKY	Topology Recon
Carbanak APT	2014 – Today	KASPERSKY + FOX IT	Topology Recon + Credential Theft
Regin	2014 – Today	KASPERSKY	Topology Recon
APT29	2015	FireEye	Topology Recon
APT28	2015	FireEye	Credential Theft
Shell_Crew	2014	RSA	Credential Theft
Target & Other POS attacks	2014 – 2015	Post Damage Detection	Credential Theft
Operation Ke3chang	2014	FireEye	Topology Recon + Credential Theft
Hurricane Panda	2014	CROWDSTRIKE	Credential Theft
IceFog APT	2013	KASPERSKY	Credential Theft



# THE EXPANDED CYBER KILL CHAIN MODEL

