





Top Cyber Attacks

Campaign / Threat Name	Time	Detected by	Methods
DUQU 2.0	2015	KA\$PER\$KY\$	Topology Recon + Credential Theft
Epic Turla	2014 – Today	KA\$PER\$KY∄ + ØSymantec.	Topology Recon
SAMAS Ransomware	2015 – Today	Microsoft + (intel)	Topology Recon
Poseidon APT	2015 – Today	KA\$PER\$KY\$	Topology Recon
Carbanak APT	2014 – Today	Kaspersky± + 👿 fox it	Topology Recon + Credential Theft
Regin	2014 – Today	KA\$PER\$KY\$	Topology Recon
APT29	2015	 FireEye 	Topology Recon
APT28	2015	 FireEye 	Credential Theft
Shell_Crew	2014	RSĄ.	Credential Theft
Target & Other POS attacks	2014 – 2015	Post Damage Detection	Credential Theft
Operation Ke3chang	2014	र्⇔FireEye	Topology Recon + Credential Theft
Hurricane Panda	2014	CROWDSTRIKE	Credential Theft
IceFog APT	2013 Company	KASPERSKYŝ confidential and proprietary	Credential Theft

THE EXPANDED CYBER KILL CHAIN MODEL

LEGACY CYBER KILL CHAIN						
External Reconnaissance	Weaponization	Delivery	External Exploitation	Installation	Command & Control	Actions on Objectives

Post Compromise

	INTERNAL KILL CHAIN				
	Internal	Internal	Ent. Privilege	Lateral	Target
1	Reconnaissance	Exploitation	Escalation	Movement	Manipulation

Target Achieved

TARGET MANIPULATION KILL CHAIN					
Target Reconnaissance	Target Exploitation	Weaponization	Installation	Execution	