Introduction to Advanced Persistent Threats

Email from John Carter to Fellow IT Team

Potential Cyber Threat Actors responsible for the attack impacting Nexora Dynamics

APT - Sophisticated Cyebr Attackers that operate golablly each with their own targets tools and motivations

Four Groups: APT 33 - Elfin Originating from Iran Focuses on Sectors like Energy, aerospace, petrochemcials, and manufacturing Main motivation is Espionage and disruption of critical infastructure, particular interest in middle east and the western world Attack Vectors: Spear Phishing (Highly Targeted Emails that exploit vulnerabiliteis in attachements or links putting malware directly on the victims systems.) Powershell based malware to enable persistent backdoors into victims systems. Credential Harvesting and Lateral Movement Once inside use tools to steal credentials and move laterally. Known to deploy destructive wiper malware APT 28 - Fancy Bear Russia Based Group Targeting government entities, political organizations, media outlets, and defense contractors Attack Vectors: Spear Phishing Credential Theft Use social engineering to steal credentials to high profile accounts Toolkit of sophisticated malware Espionage, Remote Access, C2 Infastructure Politically Motivated
APT 34 - OilRig Iran Linked group Targets financial Sector, telecommunications, government agencies, and energy firms Emphasis on middle eastern companies, and their allies. Attack Vectors: Phishing Use social engineering tactics to compromise networks Credential Harvesting Gather user credentails WEb based Exploits and VPN attacks Exploit vulnerabilites in web applications and vpns to gain access to internal systems. Allows them to remain hidden while they gather intelligence Custom Backdoors and Scanning Tools Used to maintain access Also known for their lateral movement capabilities Find high value targets Espionage, Survillence, long term footholds in network APT 29 - Cozy Bear Russian Linked Group Known for is stealthy focus on government agencies, dimplocatic institutions, and think tanks High rofile espionage campaigns aimed at gathering intelligence from werstern targets Attack Vecotrs: Sohpicsticated Speat Phishing Deploy Advanced Malware, through attachments or cloud services, Supply Chain Attacks Infiltrate Third party vendors to reach tehir targets Custom malware and advanced persistence

Invade detection and maintain longterm access Living Off the Land Techniques CLoud servies and legitimate software to blend in with network traffic Difficult to detect thier activiteis

---

Revision #1

Created 2025-11-25 17:45:50 UTC by David Rizzo

Updated 2025-11-25 17:46:21 UTC by David Rizzo