Attack Tree based on Russian Cyber activity during Ukrainian War 2022. Types of targets, techniques and tactices

DRAFT V0.1.3

APT-29 (MITRE ATT&CK)

Focused Attack on Company XYZ

No

Opportunistic

Yes

Cyber Kill Chain

NIST IR

No

Insider Source/Intel/Leak

Report Findings to: Board, Employees, Clients, Regulators, Intel Sharing Platform (ISIAC)

Yes

No

DLP, SAAS App Inspection, UBA, Honey Pot, Honey Token, Web Traffic Analysis, IPS/IDS, SIEM.

Investigate the source of the leak: Malware, Ransomware, Breach, C2, Cloud Leak

Scanned Repos (Keys), Ports, Services and Data Dumps

Public AWS Secret Keys on Github Repo

EC2 Application

S3 Bucket

SSRF IMDS V1

Recon AWS Credential Access

Exfiltrate S3 Data.

Any of the Following: Ranswomware, Crypto Mining, Data Exfil, Lambda Malware, C&C Hosting, etc.

Leak to Public

Ransom Data