

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

DRAFT V0.1.3

APT-29
(MITRE ATT&CK)

Focused Attack
on Company XYZ

No

Opportunistic

Yes

Cyber Kill Chain

No

Insider
Source/Intel/Leak

Yes

No

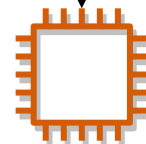
DLP, SAAS App
Inspection, UBA, Honey Pot, Honey Token, Web
Traffic Analysis,
IPS/IDS, SIEM.

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

SSRF IMDS V1

Recon AWS
Credential Access



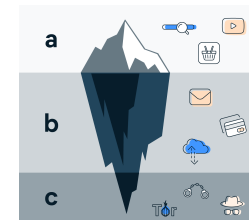
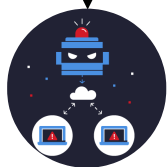
S3 Bucket

Exfiltrate S3 Data.

Leak to Public

Ransom Data

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



NIST IR

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