# Acronyms

|  |  |
| --- | --- |
| PG | Power Generation |
| ET | Electric Transmission |
| OT | Operational Technology |
| DMZ | Demilitarized Zone (Networking) |
| LAN | Local Area Network |
| SCADA | Supervisory Control and Data Acquisition |
| FIN (Abbr) | Financial |
| IT | Information Technology |
| HR | Human Sources |

# Day 1 – Lockbit 3.0 Ransomware

COA: Encrypt specific subnets associated with mission essential functions to disrupt power transmission and/or power generation.

Motivation: Lockbit 3.0 is financially motivated to disrupt, degrade, or destroy critical infrastructure targets for patriotic mission and for profit.

Storyline: The kremlin is leveraging cyber-criminal actors, especially ransomware, to directly support a campaign to destroy, disrupt, or degrade U.S. Critical Infrastructure. This will almost certainly impact the U.S. response to Russia’s advances on Ukraine. If successful, this campaign would shift the public support away from direct intervention in the Russo-Ukraine conflict, instead focusing on resolving internal civilian infrastructure issues caused as a result of this campaign.

Requirements:

* Subnets must have Windows Servers or Clients

Qualifying Subnets for Consideration:

* OT Network (10.0.9.0/24)
  + PRO: Has a network VPN connection to the Tactical Microgrid.
  + PRO: Degradation/destruction would result in denying the co-op the ability to control their PG/ET infrastructure. This could result in downstream damage to equipment, or failure to deliver power.
* ENGINEERING LAN (10.0.8.0/24)
  + PRO: Has a network VPN connection to the OT network
  + PRO: Likely a Windows machine
  + PRO: Likely running Windows 7 or older.
  + PRO: Degradation/destruction would result in the inability to control the OT network.
  + CON: Likely difficult to get initial access.
* DMZ LAN (10.0.10.0/24)
  + PRO: Already exposed to the Internet
  + PRO: Contains the company mail server.
  + CON: May be difficult to conduct lateral movement.
* FIN LAN (10.0.7.0/24)
  + PRO: Likely Windows machines
  + PRO: Impacting the primary purpose of the business: “To make money”, by degrading the secondary mission: “Deliver power”.
  + PRO: Initial access may be easier to achieve than other LAN segments.
  + PRO: Could be running Windows 11 or 10.
  + CON: Encrypting the FIN LAN does not disrupt power delivery as a direct result; however, the COOP may decide to disable power delivery.
  + CON: FIN network may not be internal or may be more isolated than other LANs, making it a less-than-ideal candidate for initial access.
  + Impact: Can cause reputational harm and loss of profitability.
* Infra (10.0.1.0/24)
  + PRO: Disruption is highly likely to disrupt business operations
  + PRO: Mail server is highly likely to contain sensitive information about business operations
  + PRO: File server and Sharepoint are likely to contain back-ups of configs for OT and IT equipment (especially networking in regards to IT)
  + CON: Likely not a good initial access candidate
  + CON: Likely very difficult target for lateral movement
* HR LAN (10.0.2.0/24)
  + PRO: Contains a lot of sensitive information. Good single point of information for exfiltration.
  + PRO: Employee data can provide targeting information for the coop.
  + PRO: HR and payroll is a mission essential function, as it keeps employees at work.
  + PRO: Initial access would likely be easy to achieve.
  + PRO: Likely Windows network. Probably uses Windows 11.
  + CON: In order to meaningfully impact payroll functions, HR functions would need to be disrupted for approximately 1 week or more.
  + CON: Degradation/destruction is not likely to result in immediate impact to PG/ET operations.
* IT Network LAN (10.0.6.0/24)
  + PRO: Degradation/destruction of enterprise business services are highly likely to degrade future business operations
  + CON: Degradation/destruction is not likely to result in immediate impact to PG/ET operations.
* User LAN (10.0.3.0/24)
  + PRO: Potential easy target for initial access.
  + CON: Disruption is unlikely to damage business operations
  + CON: May not be ideal for lateral movement.