**Cyber-Influence Operation Analysis:**

**Background, Documentation, and Modelling of Cyber and Disinformation Components.**

# GRU 2015 Campaign: “Ukrainian electricity grid disruption, BlackEnergy malware”.

## Summary

On the 23rd of December 2015, the Sandworm cyberwarfare unit of the GRU, activated a synchronised malicious remote operation of breakers at three regional electric power distribution companies. This rendered approximately 225,00 Ukrainian residents without power for up to six hours. When power was restored, the companies performed under constrained operations. The computer systems were hacked initially through spearphishing emails. BlackEnergy malware was used to steal user credentials, perform reconnaissance activities, and was then likely used to disrupt the transmission and distribution substation within the Ukrainian power grid. KillDisk was used at the conclusion of the operation to delete computer event logs and other files and render the infected computers inoperable.

## Timeline and Context

Power outages were caused by remote cyber intrusions at three regional electric power distribution companies impacting approximately 225,000 customers. Each of the three attacks occurred within 30 minutes of each other, where remote operation of the breakers was conducted by multiple external humans. At the They used either existing remote administration tools at the OS level or remote industrial control system client software via virtual private network connections.

* The BlackEnergy malware was delivered via a spearphishing campaign. Malicious MS Word and Excel files are attached to the emails. Employees that open the attachment and enable macros execute the installation of the malware.
* BlackEnergy facilitates the installation of additional malware plugins and tools. Credential harvesting and network discovery functions are conducted. From here, valid credentials with administrator privileges are secured. Additional KillDisk malware is delivered to the network. Lateral movement within the network leads to the compromise of telephone communications and data centre servers.
  + An outage is scheduled for the backup power services at related telephone communications server and data centre servers.
* After the setup, threat actors use native remote access services in conjunction with valid credentials to trip the breakers at the three power distribution companies. This disrupts the power supply to approximately 225,000 customers.
  + Soon after disrupting the power, the KillDisk malware erases selected files on target systems and corrupts the boot record, rendering systems inoperable.
  + Threat actors conduct a denial-of-service attack on the telephone call centre at one of the power distributors. Simultaneously, the scheduled outage for the backup power occurs. This denies opportunities for the customers to gain clarity on the situation.

We understand that the GRU looks to take advantage of the tense climate surrounding the Russo-Ukrainian War. Driving perceptions of asymmetric warfare exploits vulnerabilities in the target audience by creating fear and undermining confidence in government services and security.

## Frameworks

### ATT&CK Framework

* **TA0043: Reconnaissance**
  + T1589 Gather Victim Identity Information
    - T1589.002 Email Addresses
    - T1589.003 Employee Names
  + T1590 Gather Victim Network Information
  + T1593 Search Open Websites/Domains
* **TA0042 Resource Development**
  + T1583 Acquire Infrastructure
    - T1583.003 Virtual Private Server
      * Valid credentials are used to interact directly with the client application for the document management system server via a VPN.
  + T1585 Establish Accounts
    - T1585.001 Email Accounts
  + T1588 Obtain Capabilities
    - T1588.001 Malware
      * BlackEnergy 3 malware used. Malicious plugins and malware such as KillDisk later uploaded.
    - T1588.002 Tool
      * Automated IP-based call generators used to conduct a denial-of-service attack.
  + T1608 Stage Capabilities
    - T1608.001 Upload Malware
* **TA0001 Initial Access**
  + T1133 External Remote Services
    - Threat actors installed a modified Dropbear SSH client as the backdoor.
  + T1566 Phishing
    - T1566.001 Spearphishing Attachment
  + T1078 Valid Accounts
    - Threat actors used valid accounts to escalate privileges, move laterally, and establish persistence.
* **TA0002 Execution**
  + T1059 Command and Scripting Interpreter
    - T1059.005 Visual Basic
      * Threat actors installed a VBA script that dropped the primary BlackEnergy implant for executing some malware and the default file used to determine folder displays on Windows machines.
  + T1204 User Execution
    - T1204.002 Malicious File
* **TA0003 Persistence**
  + T1136 Create Account
    - T1136.002 Domain Account
      * Threat actors exploited position on network to create privileged domain accounts. These were used for further exploitation and lateral movement.
  + T1133 External Remote Services
    - The modified Dropbear SSH backdoor.
  + T1078 Valid Accounts
* **TA0004 Privilege Escalation**
  + T1055 Process Injection
    - Threat actors loaded BlackEnergy 3 into svchost.exe, which then launched iexplore.exe for their command and control server.
  + T1078 Valid Accounts
* **TA0005 Defense Evasion**
  + T1070 Indicator Removal
    - T1070.001 Clear Windows Event Logs
  + T1562 Impair Defenses
    - T1562.001 Disable or Modify Tool
      * Threat actors modified in-registry internet settings to lower security.
  + T1070 Indicator Removal
    - T1070.004 File Deletion
  + T1112 Modify Registry
    - Before starting the malware required to communicate with their command and control servers, threat actors lowered internet security levels.
  + T1055 Process Injection
  + T1218 System Binary Proxy Execution
    - T1218.011 Rundll32
  + T1078 Valid Accounts
* **TA0006 Credential Access**
  + T1056 Input Capture
    - T1056.001 Keylogging
      * Account credentials were gathered via a BlackEnergy keylogger plugin.
    - T1040 Network Sniffing
      * Threat actors used BlackEnergy plugins/modules to perform network sniffing. This was used to sniff and capture more credentials being sent over the network between the local LAN and the power grid's industrial controls systems.
* **TA0007 Discovery**
  + T1087 Account Discovery
  + T1040 Network Sniffing
  + T1135 Network Share Discovery
    - KillDisk will attempt to enumerate mapped network shares to later attempt to wipe all files on those shares.
  + T1018 Remote System Discovery
    - Threat actors remotely discover systems over LAN connections. Operational technology systems were visible from the IT network as well, giving the actors the ability to discover operational assets.
* **TA008 Lateral Movement**
  + T1570 Lateral Tool Transfer
    - The threat actors moved their tools laterally within the corporate network and between the ICS and corporate network.
* **TA0009 Collection**
  + T1056 Input Capture
    - T1056.001 Keylogging
* **TA0011 Command and Control**
  + T1071 Application Layer Protocol
    - T1071.001 Web Protocols
      * BlackEnergy enabled communication between compromised hots and their CC servers via HTTP post requests.
  + T1105 Ingress Tool Transfer
    - Threat actors pushed additional malicious tools onto the infected system via BlackEnergy. Used to steal user credentials, move laterally, and destroy data.
* **TA0040 Impact**
  + T1485 Data Destruction
    - Scheduled KillDisk execution erases master boot records and deletes system log data.
  + T1498 Network Denial of Service
    - Threat actors initiate DoS attack on telephone call centre to prevent customers from gaining clarity on the power outage.
  + T1529 System Shutdown/Reboot
    - Previously scheduled backup power outage disrupts power to the telephone communications server and targeted data centre servers.
  + T1490 Inhibit System Recovery
    - Threat actors overwrote the serial-to-ethernet communication device gateways with custom firmware to make systems either disabled, shutdown, and/or unrecoverable.
    - The malicious updates render the converters inoperable, and sever connections between the control centre and the substations.
    - KillDisk rendered devices that were necessary for remote recovery unusable, including at least one RTU.

### DISARM Framework

* **PLAN**
  + TA01: Plan Strategy
    - T0073: Determine Target Audiences
    - T0074: Determine Strategic Ends
  + TA02: Plan objectives
    - T0078: Dismay
    - T0079: Divide
  + TA13: Target Audience Analysis
    - T0081: Identify Social and Technical Vulnerabilities
* **PREPARE**
  + TA14: Develop Narratives
    - T0068: Respond to Breaking News Event or Active Crisis
* **EXECUTE**
  + TA18: Drive Online Harms
    - T0123: Control Information Environment through Offensive Cyberspace Operations
  + TA11: Persist in the Information Environment
    - T0129: Conceal Operational Activity
      * T0129.003: Break Association with Content
      * T0129.006: Deny Involvement
    - T0130: Conceal Infrastructure
      * T0130.004: Use Cryptocurrency
      * T0130.005: Obfuscate Payment
* **ASSESS**
  + TA12: Assess Effectiveness
    - T0132: Measure Performance
      * T0132.003: View Focused
    - T0133: Measure Effectiveness
      * T0133.003: Awareness
      * T0133.004: Knowledge
      * T0133.005: Action/attitude
    - T0134: Measure Effectiveness Indicators (or KPIs)
      * T0134.002: Social media engagement

## Resources

*BlackEnergy, Software S0089 | MITRE ATT&CK®*. Available at: <https://attack.mitre.org/software/S0089/>

SANS ICS, (2016), Analysis of the Cyber Attack on the Ukrainian Power Grid. Available at: <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>

*2015 Ukraine Electric Power Attack*, *2015 Ukraine Electric Power Attack, Campaign C0028 | MITRE ATT&CK®*. Available at: <https://attack.mitre.org/campaigns/C0028/>

*Cyber-Attack Against Ukrainian Critical Infrastructure: CISA* (2021) *Cybersecurity and Infrastructure Security Agency CISA*. Available at: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>

*Special Section: Ukrainian power grids cyberattack - ISA* (2017) *isa.org*. Available at: <https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack>

Booz | Allen | Hamilton, (2019). When the Lights Went Out. A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure. Available at: <https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>

U.S. Department of Justice (2018) United States of America v. Yuriy Sergeyevich Andreienko [and 5 Others], Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. Available at: <https://www.justice.gov/opa/press-release/file/1328521/dl>

McLellan, C. *How hackers attacked Ukraine’s power grid: Implications for Industrial IoT security* (2016) *ZDNET*. Available at: <https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/>