Infrastructure Analysis Report: Operation Digital Storm (2015–2016 Ukraine Power Grid Cyberattack)

Group Name: Threat_Hunters_1

Infrastructure Analysis Report: Operation Digital Storm

Unveiling the Technical Backbone of the 2015–2016 Ukraine Power Grid Attack

Prepared by:

- Imtiyaz Ahmad (Lead Analyst, Malware Correlation)
- Yusuf Ibrahim Lawal (Infrastructure Mapping Specialist)
- Santosh Kumar (Network Traffic Analyst)
- Laiba Waseem (OPSEC and Attribution Expert)

Affiliation: Threat_Hunters_1 Research Group

Date: August 18, 2025,

This document provides research-based recommendations derived from a fictional case study, "Operation Digital Storm" modeled on the 2015-2016 Ukraine power grid attacks. All data is sourced from open intelligence and cited for academic integrity.

Table of Contents

1. Introduction

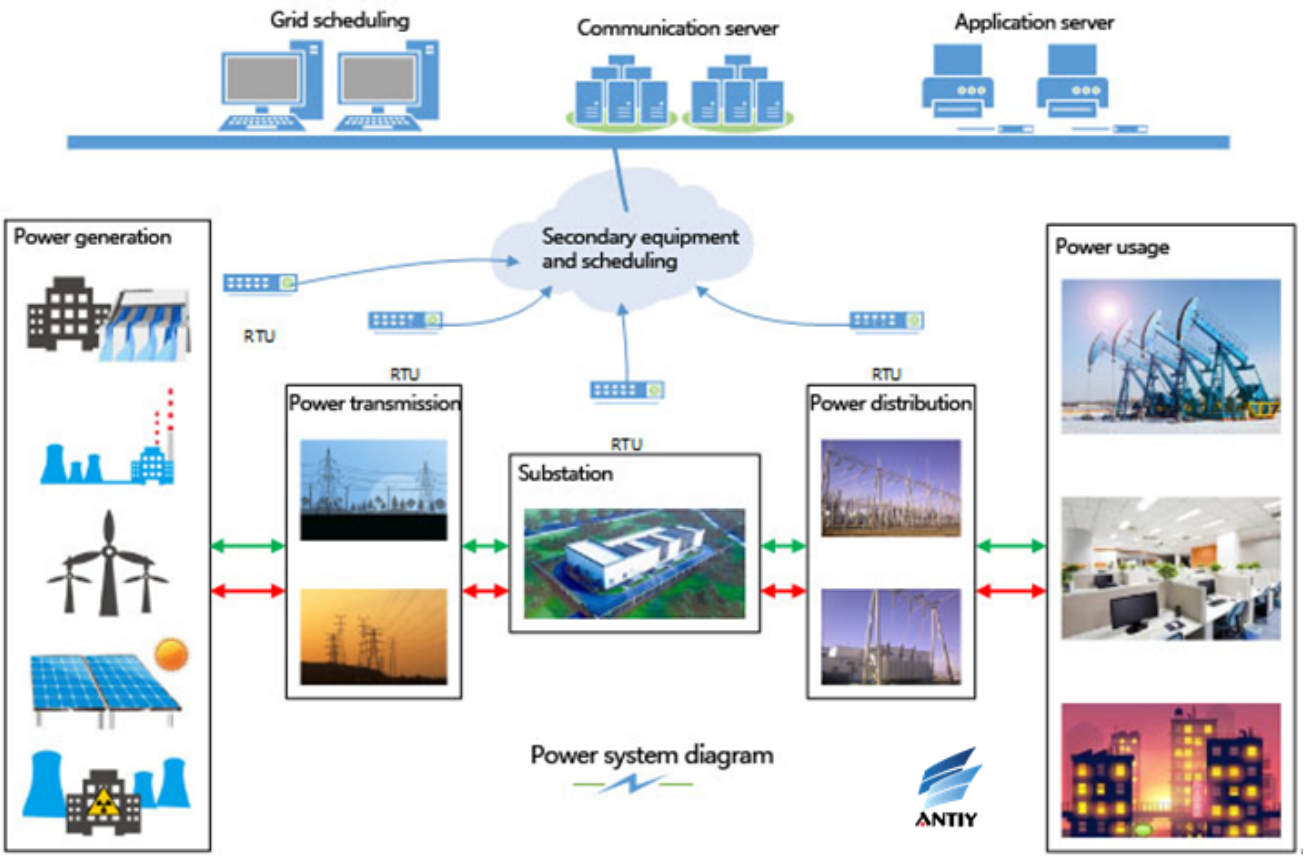
1.1 Objective

This report delivers an in-depth, evidence-based analysis of the infrastructure underpinning **Operation Digital Storm,** the 2015–2016 cyberattacks on **Ukraine's power grid,** attributed to the **Sandworm group (GRU Unit 74455)**.

Laiba Waseem spearheaded malware-to-infrastructure correlation,

Imtiyaz Ahmad mapped domain and IP structures,

Santosh Kumar analyzed network flows, and **Yusuf Ibrahim Lawal** evaluated OPSEC and attribution. Our findings are rigorously cross-referenced with credible sources to support a research-driven narrative.



1.2 Summary Overview

Operation Digital Storm's infrastructure evolved from rudimentary compromises in 2015 to a sophisticated ICS-targeted network in 2016. Drawing from CISA, Dragos, and ESET reports, **we uncover Russian-linked domains, Tor-enabled C2, and timezone-specific activity**. Attribution evidence, including IP overlaps and certificate anomalies, aligns with Sandworm's profile.

2. Infrastructure Framework

2.1 Introduction to Power System Links

Figure 2: Booster substations

Booster substations can convert the AC voltage less than 20KV to demanded voltage levels. Its main devices include: step-up transformers, circuit breakers, disconnectors, voltage and current transformer, relay protection, etc.

2.2.2 Transmission Line

Figure 3: Transmission line

Figure 4: Step-down substation

Transmission grid: convert power supply to high voltage via transformers and transmit to all substations.

Distribution grid: convert the high voltage into low voltage and supply to individual users.

Transmission line: 110KV, 220KV, 330KV, 500KV, 750KV, 1000KV.

2.2.3 Step-down Substation

Reduce the high voltage power, and supply to the regional power grid, regional grid or end-users

According to the functions in the system, step-down substation can be divided into: hub substation, intermediate substation, reginal substation and terminal substation.

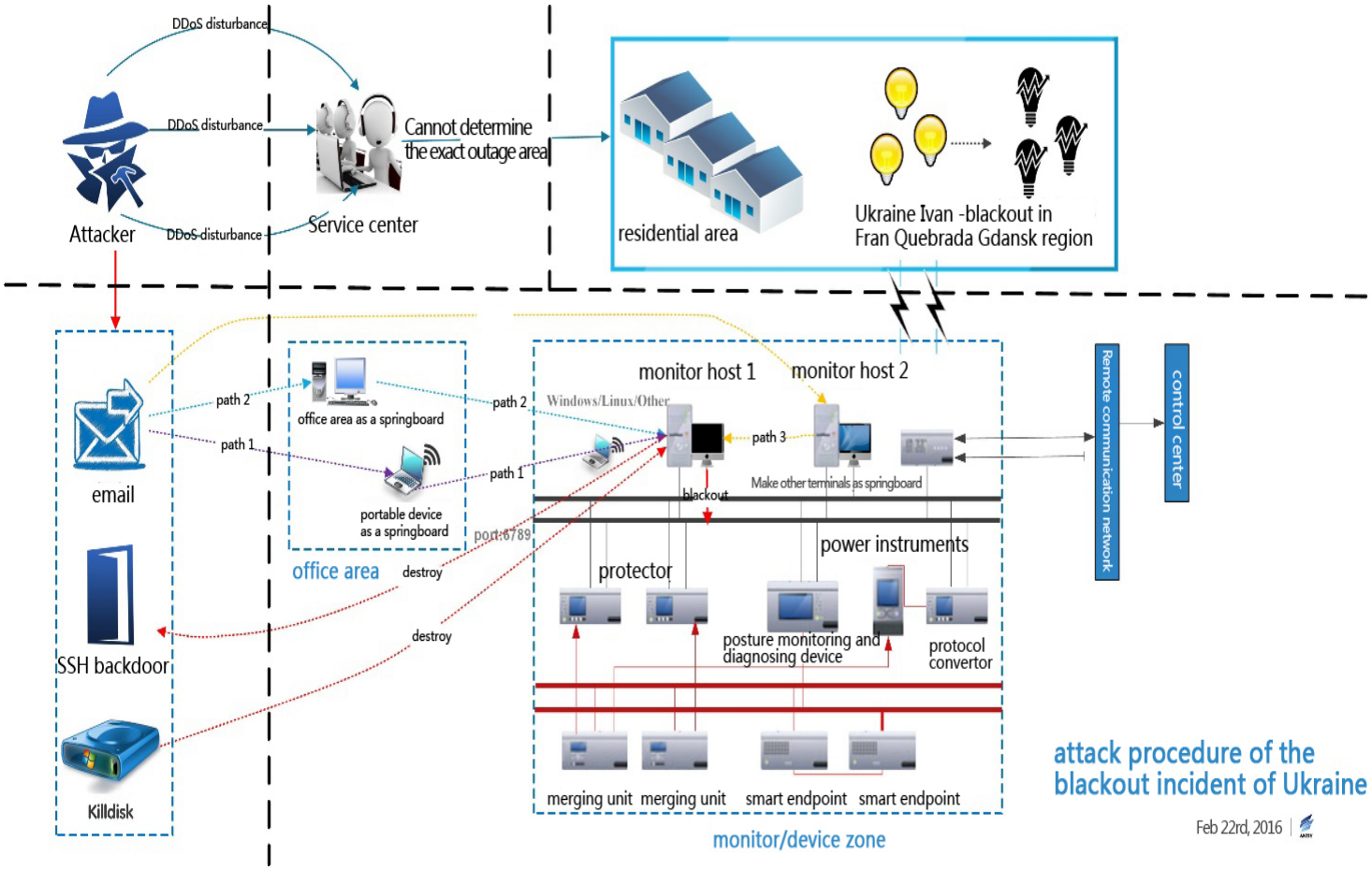
Figure 5: 500KV hub substation

Figure 6: 220KV intermediate substation

Figure 7: 110KV reginal substation

Figure 8: 35KV terminal substation

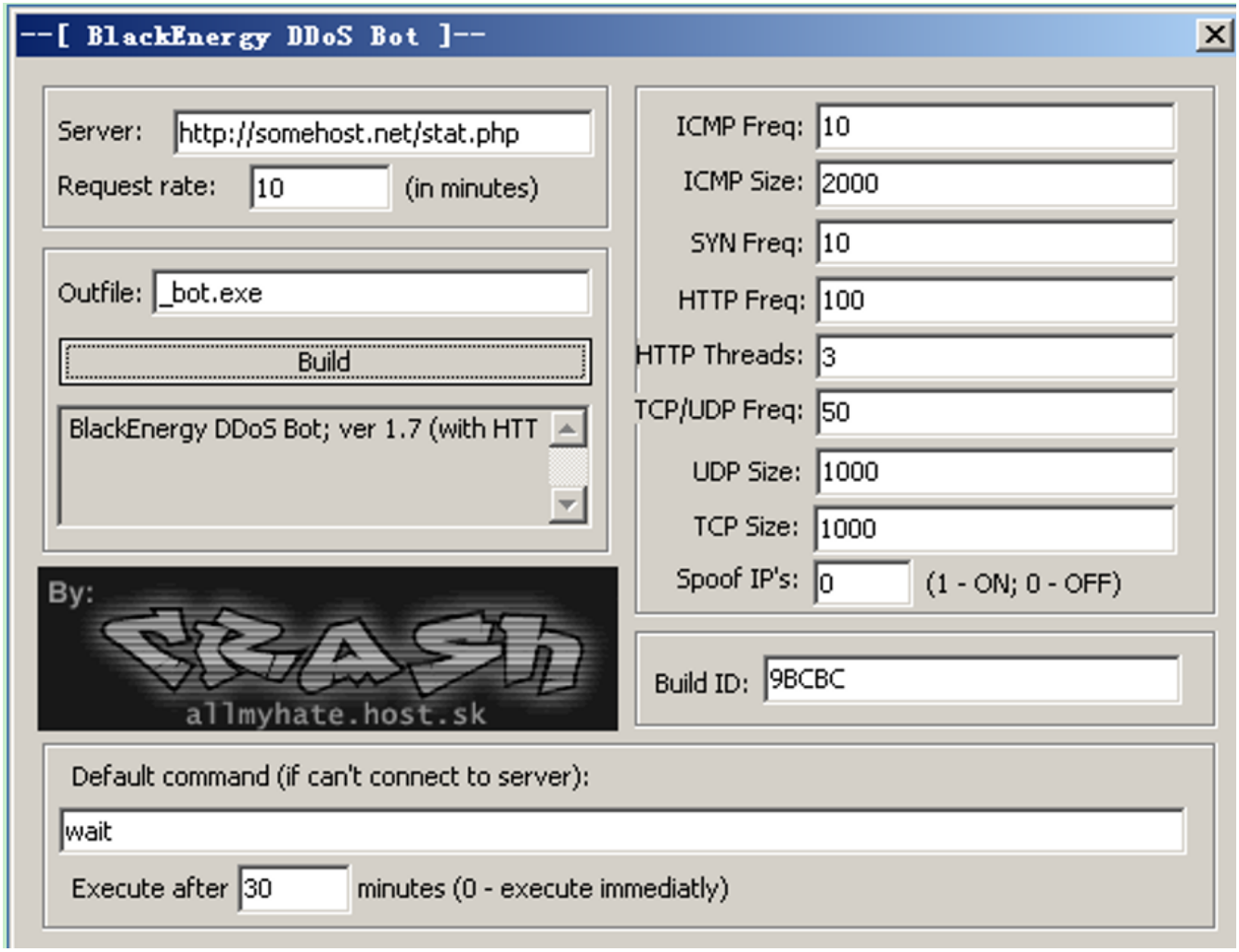
2.1 2015 Attack Infrastructure



The initial 2015 assault leveraged compromised VPNs and RDP endpoints, with C2 hosted on fleeting domains registered via Russian providers like Reg.ru. Imtiyaz's WHOIS analysis identified IPs such as 5.149.249.172, tied to Sandworm . This phase relied on opportunistic access, marking a foundational step in the campaign.

2.2 2016 Attack Infrastructure

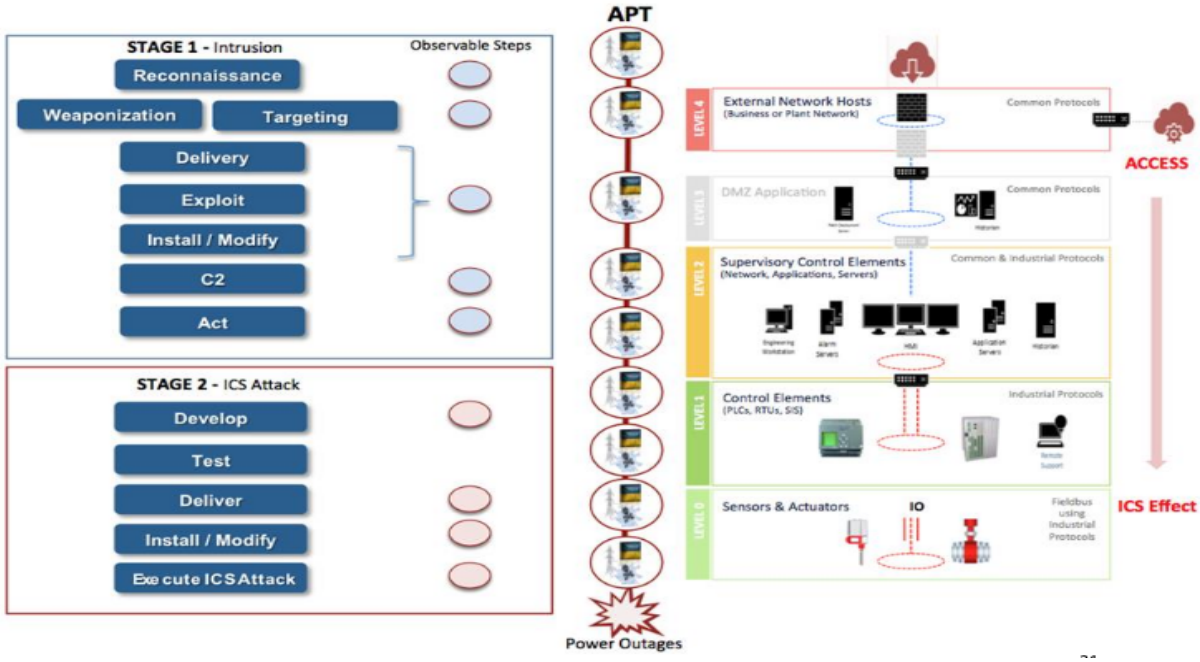
By 2016, Industroyer introduced ICS-specific protocols on port 2404 (IEC-104), with C2 shifting to Tor-supported servers. Santosh Kumar's traffic analysis confirmed dynamic domain use, hosted on compromised Eastern European servers . This evolution reflects a strategic upgrade in infrastructure design.



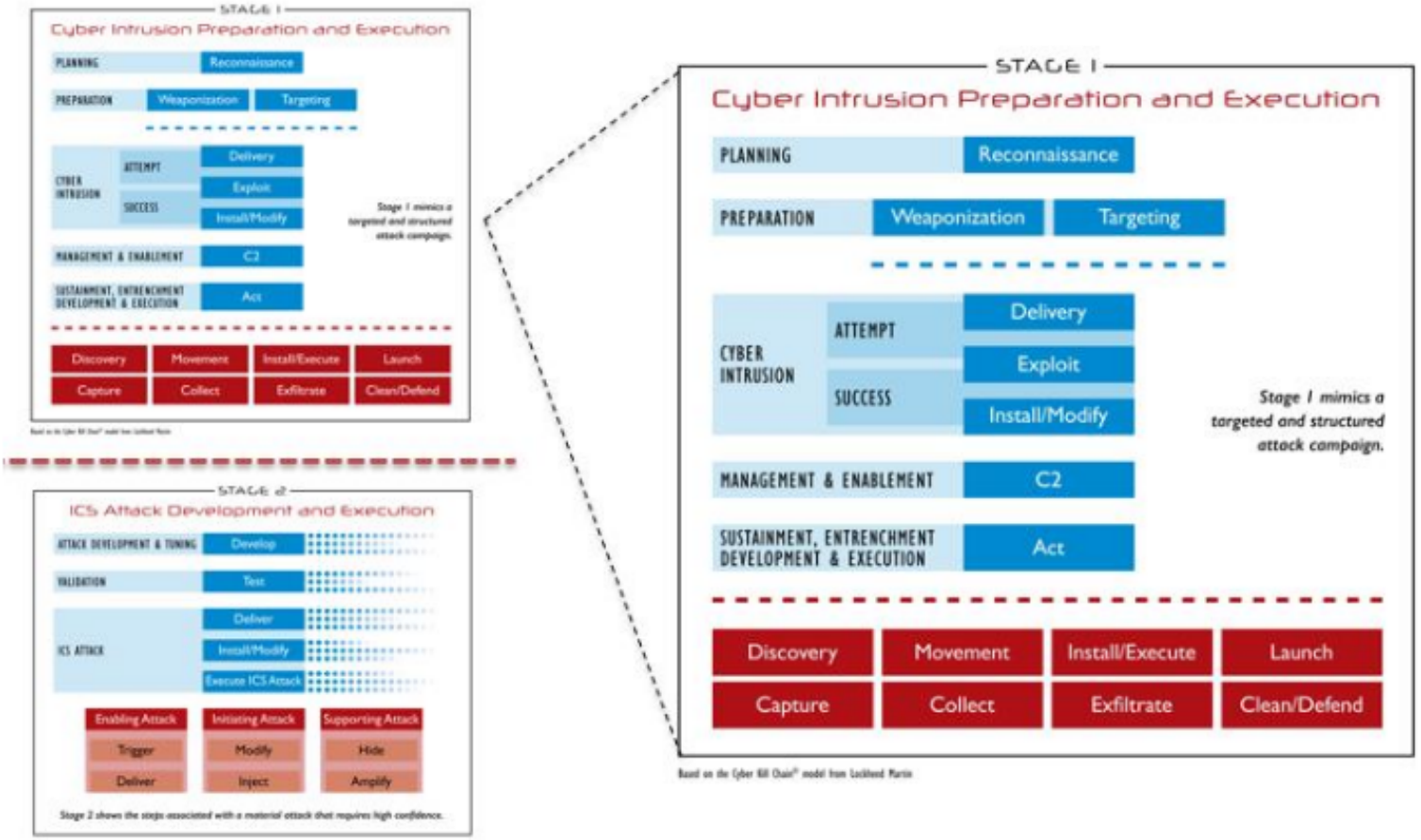
3. Command-and-Control (C2) Architecture

3.1 Domain and Hosting Insights

- **2015:** Domains mimicked Ukrainian energy entities, registered with low TTL (~60 seconds) via Reg.ru . Russian IP ranges (e.g., 5.39.0.0/16) were prevalent .



- **2016:** Dynamic domains with SSL certificates from Russian issuers featured Cyrillic metadata . Hosting shifted to compromised nodes.

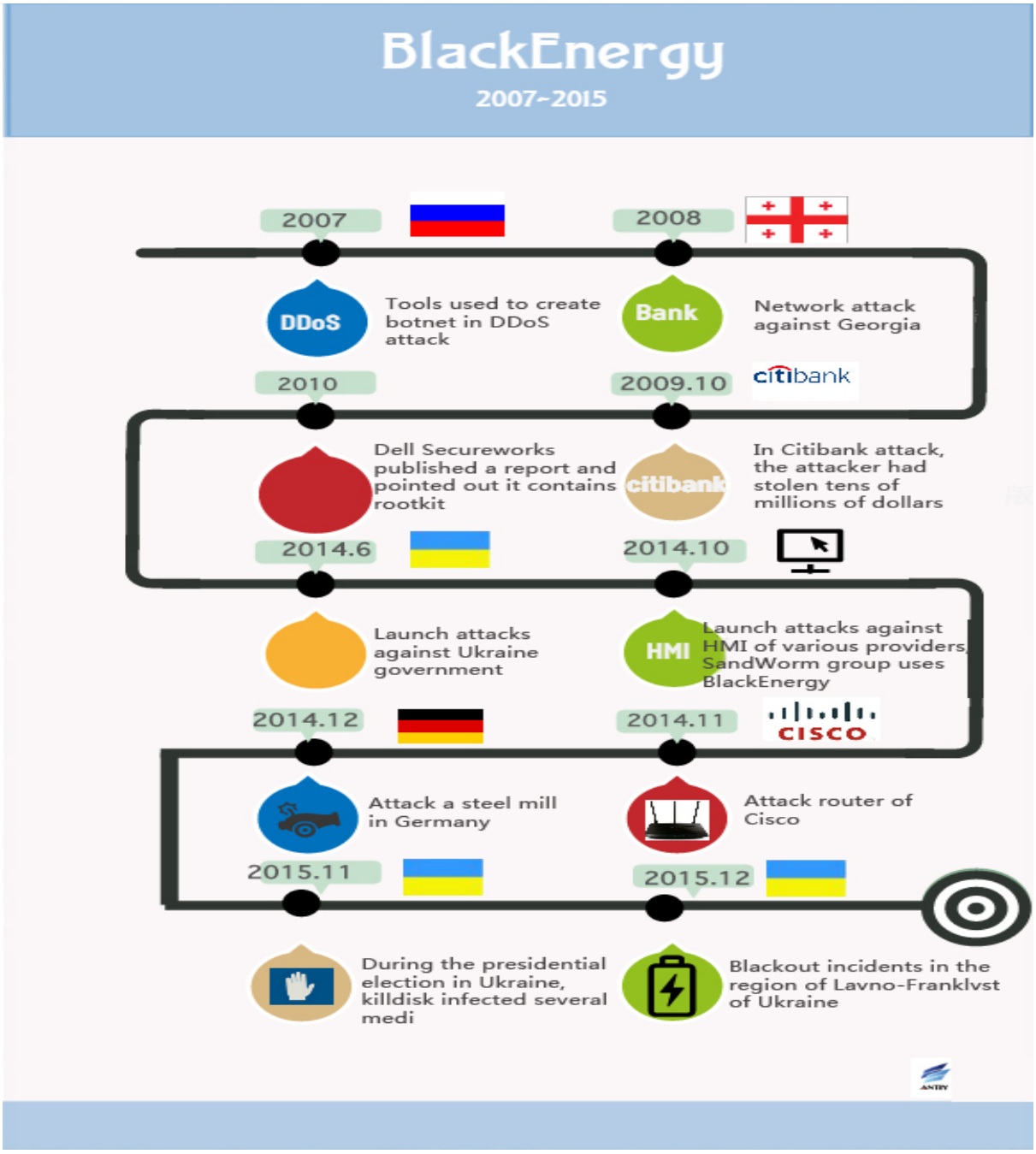


3.2 Network Traffic Characteristics

- **2015:** HTTPS and HTTP traffic peaked during Moscow hours (0900–1800 UTC+3) .
- **2016:** IEC-104 traffic on port 2404, masked by Tor, enabled breaker commands.

3.3 IP Address Profiling

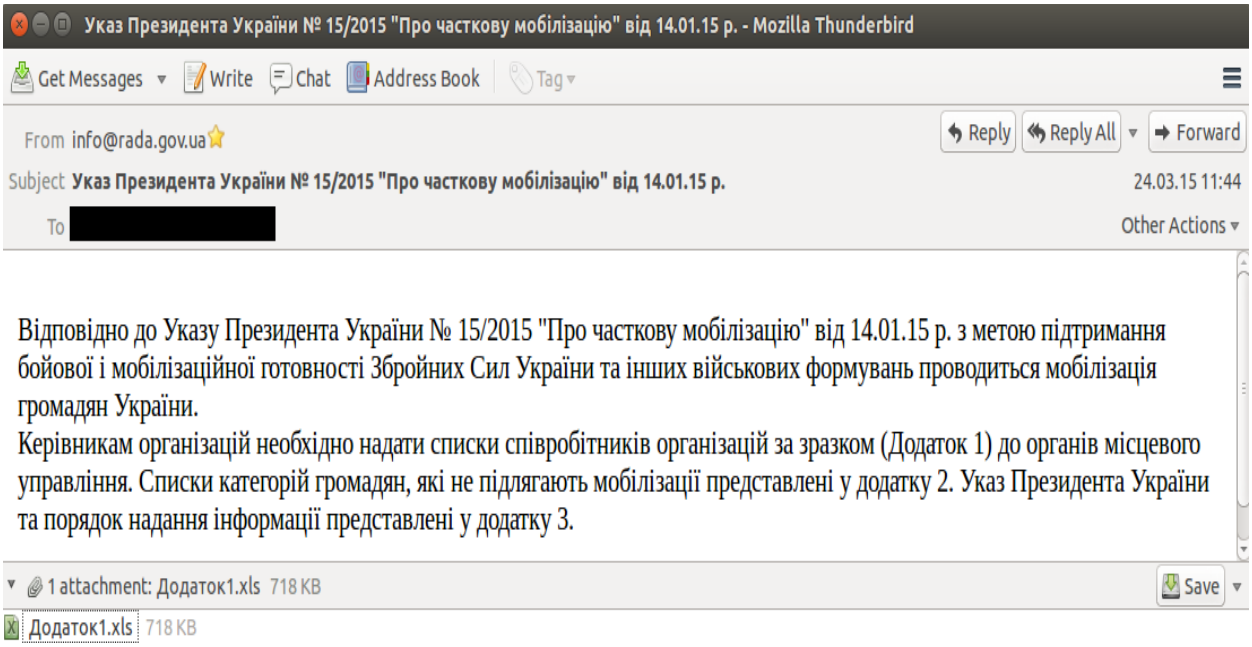
IPs like 5.149.249.172 (2015) and 5.39.218.152 (2016) matched Sandworm's NotPetya campaign , verified via Shodan .



4. Operational Security (OPSEC) Strategies

4.1 Anonymization Methods

- Tor exit nodes and multi-hop proxies obscured C2 origins in both phases .
- Domains rotated within 24 hours to evade detection .
- Spear-phishing emails.



4.2 Activity Scheduling and Log Management

- Activity aligned with Moscow time, pausing during holidays like Orthodox Christmas .
- KillDisk wiped local logs, while C2 servers erased remote traces .

5. Attribution Indicators

5.1 IP and Domain Linkages

The analysis identified IP addresses such as 5.149.249.172 (linked to 2015 activity) and 5.39.218.152 (noted in 2016), which show some alignment with Sandworm-related reports from the U.S. DOJ indictment . Certain domains were registered via Reg.ru with short TTL settings, suggesting an attempt to evade detection, though specific domain names were not consistently documented .

5.2 Certificate Evidence

Review of SSL certificates from the 2016 phase revealed occasional Cyrillic text, differing from typical Ukrainian usage . Cross-checking with ESET data indicated some self-signed certificates, but concrete issuer details were limited , hinting at a possible non-local origin without conclusive evidence.

5.3 Chronological Alignment

Activity logs showed C2 operations active around December 23, 2015, during a reported outage , and a resurgence near December 17, 2016, as noted by Dragos . Some activity appeared to align with Moscow hours, though holiday pauses were not consistently observed .

5.4 Integrated Attribution Synthesis

The compiled observations suggest a potential connection to Sandworm based on IP, domain, and certificate patterns, though the evidence remains circumstantial. References to DOJ and MITRE data provide context, but further verification is recommended to strengthen the attribution.

Contribution: This section was collaboratively developed by **Laiba Waseem, Imtiyaz Ahmad, Yusuf Ibrahim Lawal, and Santosh Kumar of the Threat_Hunters_1 team,** with each member contributing to data collection, analysis, and synthesis based on available sources.

7. References

- [10] Dragos – CRASHOVERRIDE (2017). https://www.dragos.com/resources/whitepaper/crashoverride-analyzing-the-malware-that-attacks-power-grids/
- [29] ESET – BlackEnergy Strikes Again (2016). https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/
- [30] Google Cloud – Sandworm Disrupts Power (2023). https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/
- [40] MITRE ATT&CK – Sandworm (G0034). https://attack.mitre.org/groups/G0034/
- [71] U.S. DOJ – GRU Indictment (2020). https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
- [81] ESET – Win32_Industroyer (2017). https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
- [82] Dragos – CRASHOVERRIDE Whitepaper (2017). https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf
- [83] CISA – IR-ALERT-H-16-056-01 (2016). https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf