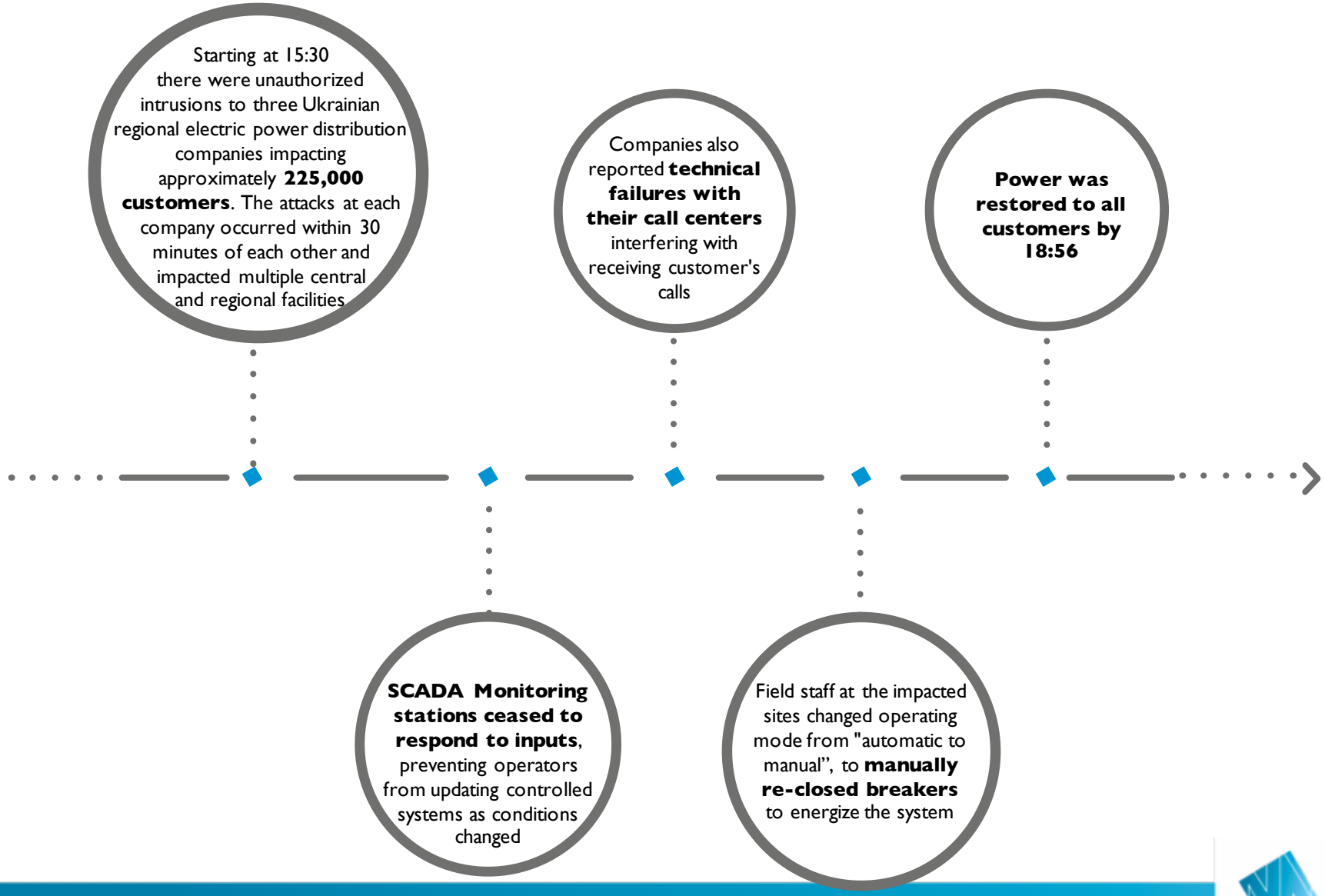
UKRAINE POWER GRID ATTACK ANALYSIS

Executive Summary

- **Hacker Attack Shuts Down the Ukraine Power Grid**, on December 23rd 2015
- The incident was caused by a **coordinated attack**
- Based on the available information, we have **analyzed the attack step by step**
- We can show you the benefits of deploying **Nozomi SCADAguardian--** the **Alerts**, the **Reactions** and the **Awareness** that would have been generated in that scenario

What's happened in Ukraine on 23rd December…



The hack on the news

CNN Money International + Markets Economy Companies Tech Autos Video stock tickers

Cyber-Safe

Scary questions in Ukraine energy grid hack

by Jose Pagliery @Jose_Pagliery

January 18, 2016: 2:37 PM ET

Social Surge - What's Trending


JetPack takes flight around Lady Liberty


There's a big sale on Puerto Rican homes


How to build a $100 million company out of mud

American investigators are traveling to Ukraine to investigate a recent electricity blackout -- perhaps the first major act of cyberwar on a civilian population.

Forbes / Security

The Little Black Boo

JAN 4, 2016 @ 12:15 PM 9,836 VIEWS

Ukraine Claims Hackers Caused Christmas Power Outage

BBC Sign in News Sport Weather Shop Earth Travel More

NEWS

Hackers caused power cut in western Ukraine - US

12 January 2016 | Technology

Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

A power cut in western Ukraine last month was caused by a type of hacking known as "spear-phishing", says the US Department of Homeland Security (DHS).

Last updated: January 5, 2016 10:37 pm

FINANCIAL TIMES

Hackers shut down Ukraine power grid

Hannah Kuchler in San Francisco and Neil Buckley in London

Share Author alerts Print Clip Comments

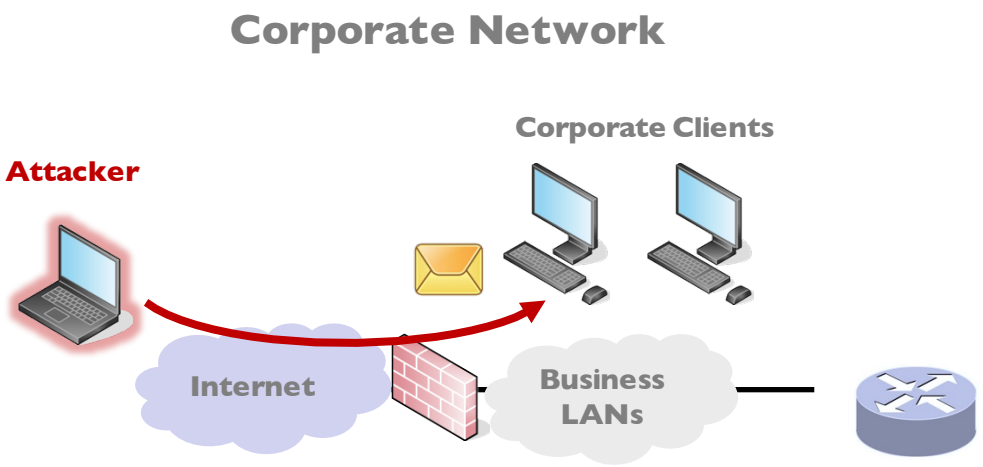
Hackers brought down the power supply to hundreds of thousands of homes in Ukraine last week, in a cyber attack believed to be the first ever to result in a power outage.

Attack Anatomy

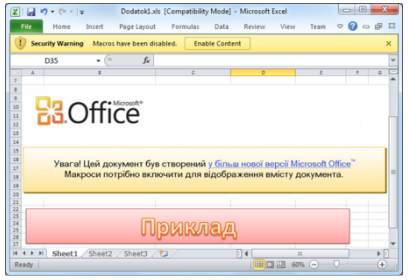
- Several sources conclude with confidence that the incident was a **coordinated intentional attack**
- The adversary initiated an intrusion into production SCADA systems using an **email attachment** to infect corporate systems and collect information on the targets
- Using this information and a new version of the **Black Energy malware**, the attackers were able to open breakers and cause the power outage
- During the outage the attackers performed actions **to prevent recovery operations**

ATTACK, STEP BY STEP

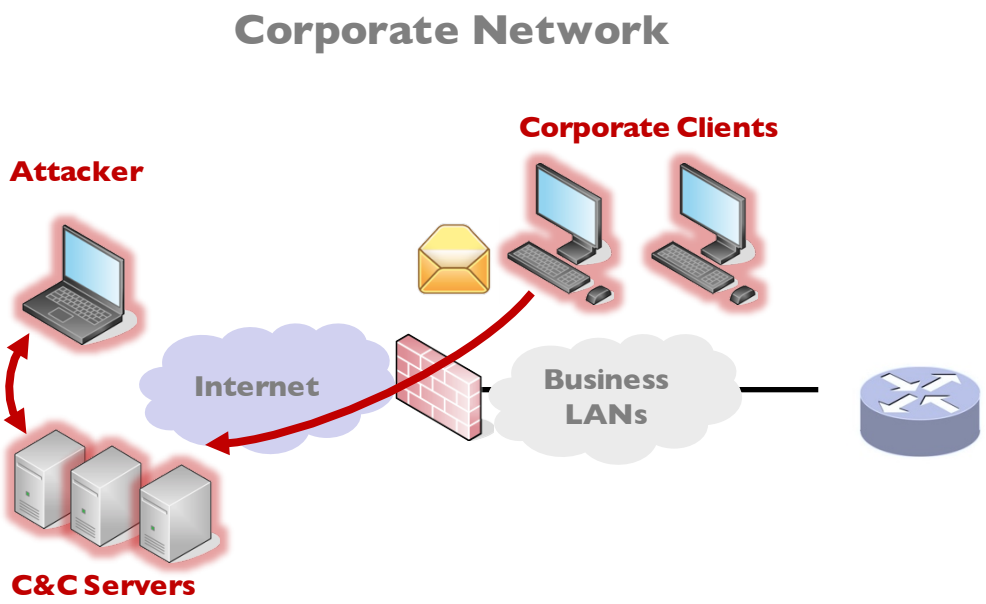
1. Spear Pishing Email



The target gets a spear-phishing email that contains an attachment with a malicious document. The attackers spoofed the sender address to appear to be one belonging to Rada (the Ukrainian parliament) and the document itself contains text trying to convince the victim to run the macro in the document

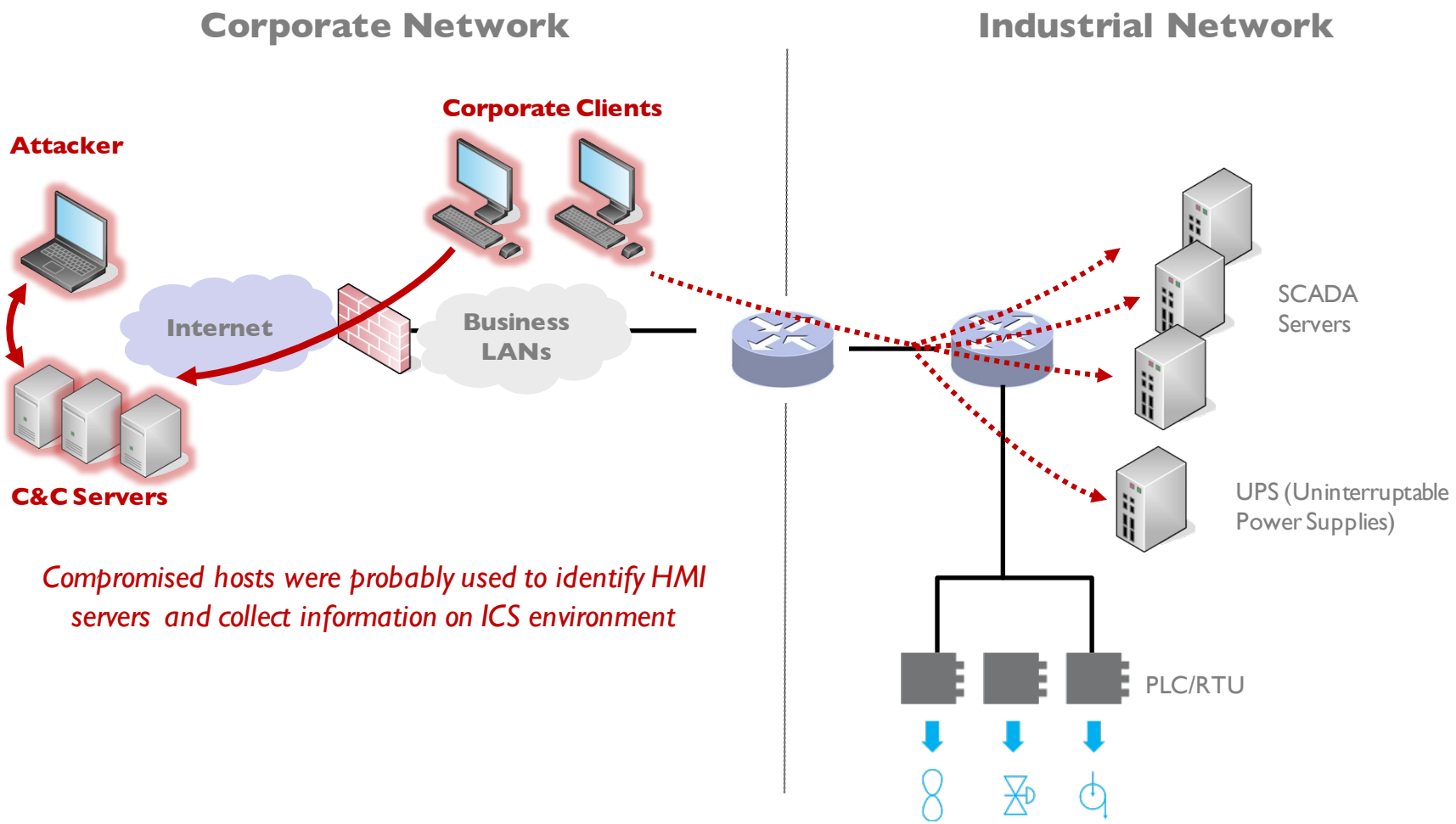


2. Information Gathering



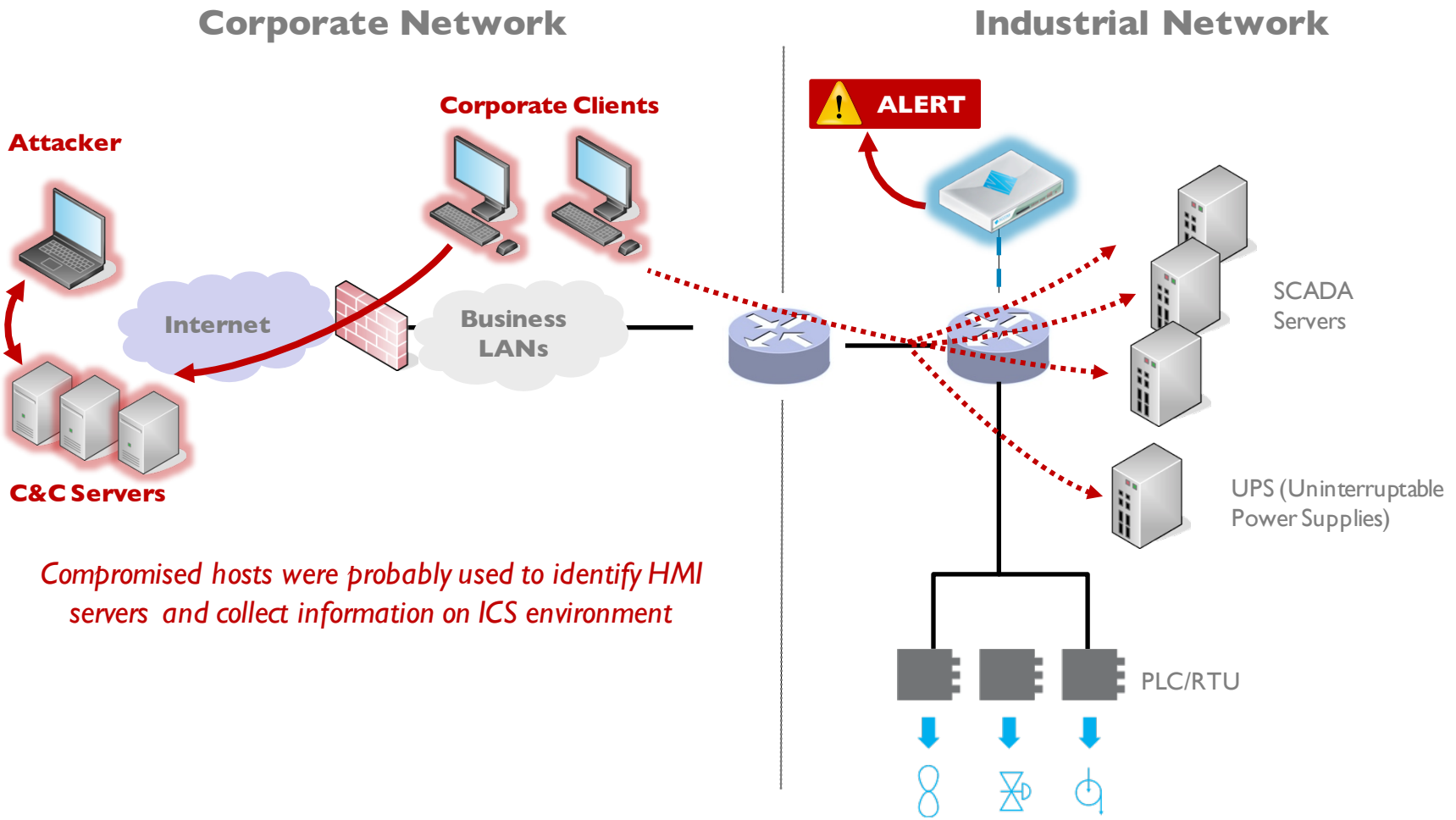
The victims, successfully tricked, executed malicious code to interact with remote Command and Control (C&C) servers. System information was sent to C&C servers, and was used by attackers to gather additional information about targets. Ultimate goal was to execute commands on the victim's hosts or to gain remote access to the target network

3. Lateral Movement



Compromised hosts were probably used to identify HMI servers and collect information on ICS environment

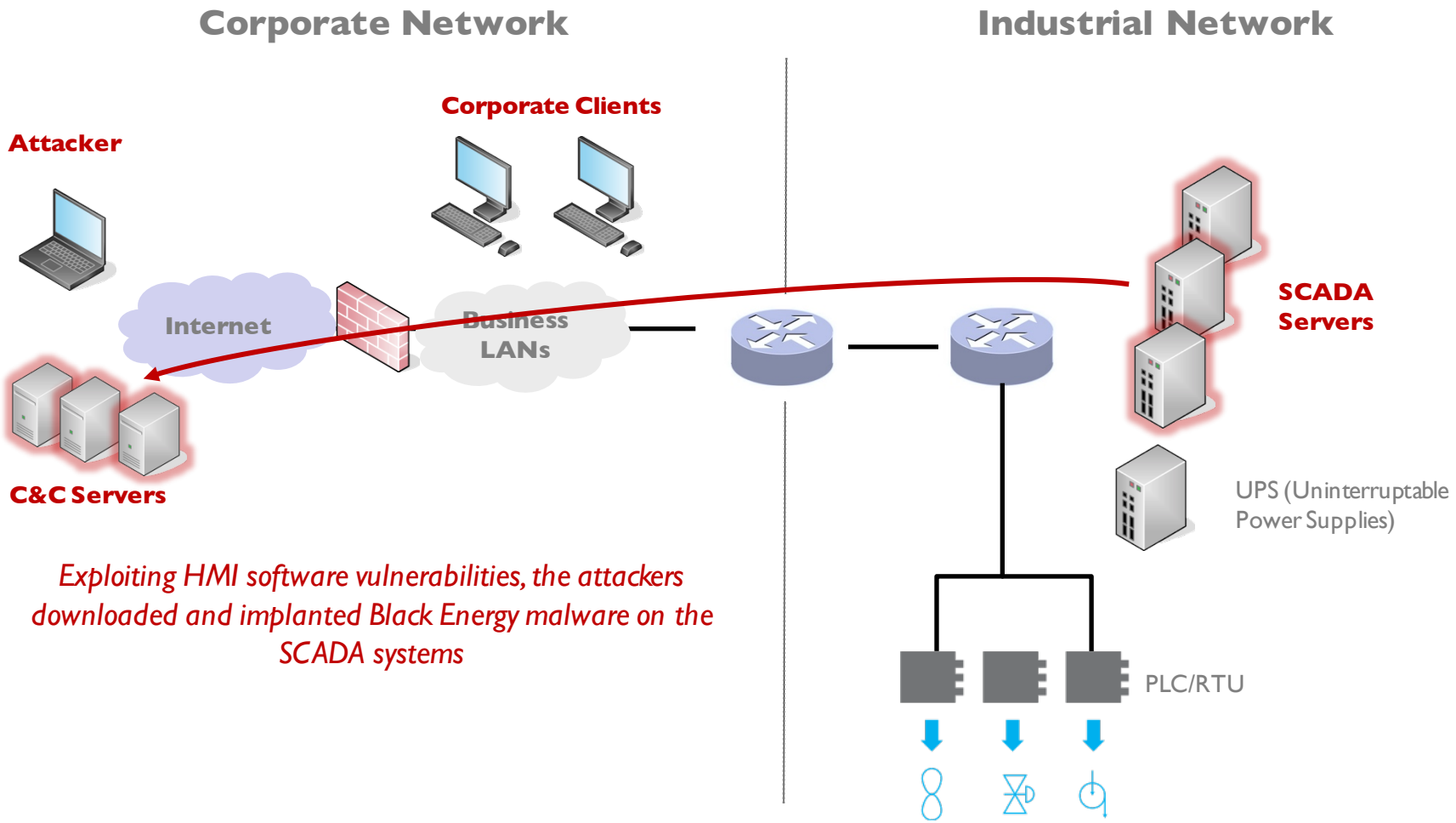
3. Lateral Movement - with NOZOMI SCADAguardian



Compromised hosts were probably used to identify HMI servers and collect information on ICS environment

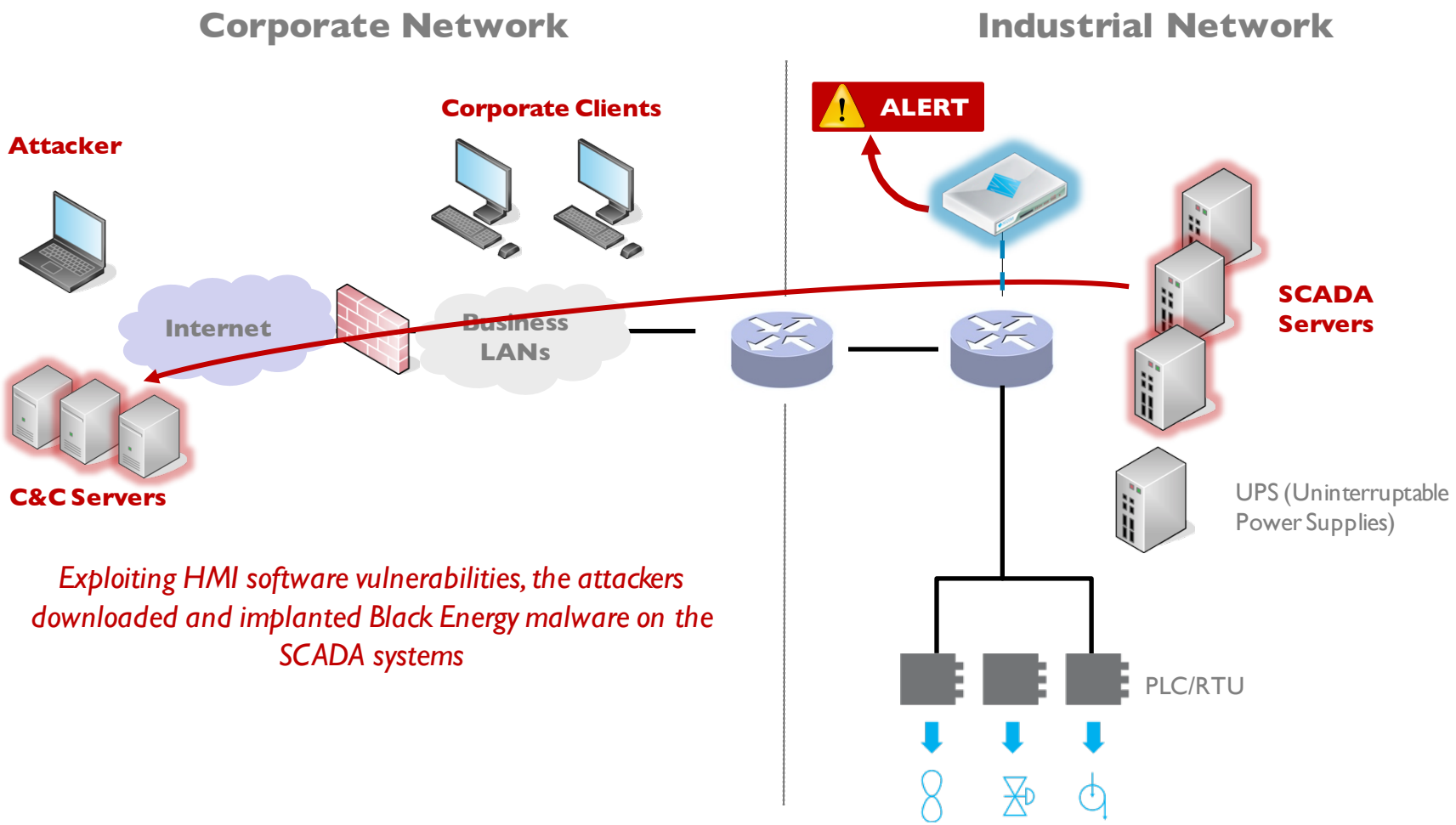
NOZOMI SCADAguardian identifies this type of reconnaissance activity, and raises alerts when they occur

4. SCADA Infiltration



Exploiting HMI software vulnerabilities, the attackers downloaded and implanted Black Energy malware on the SCADA systems

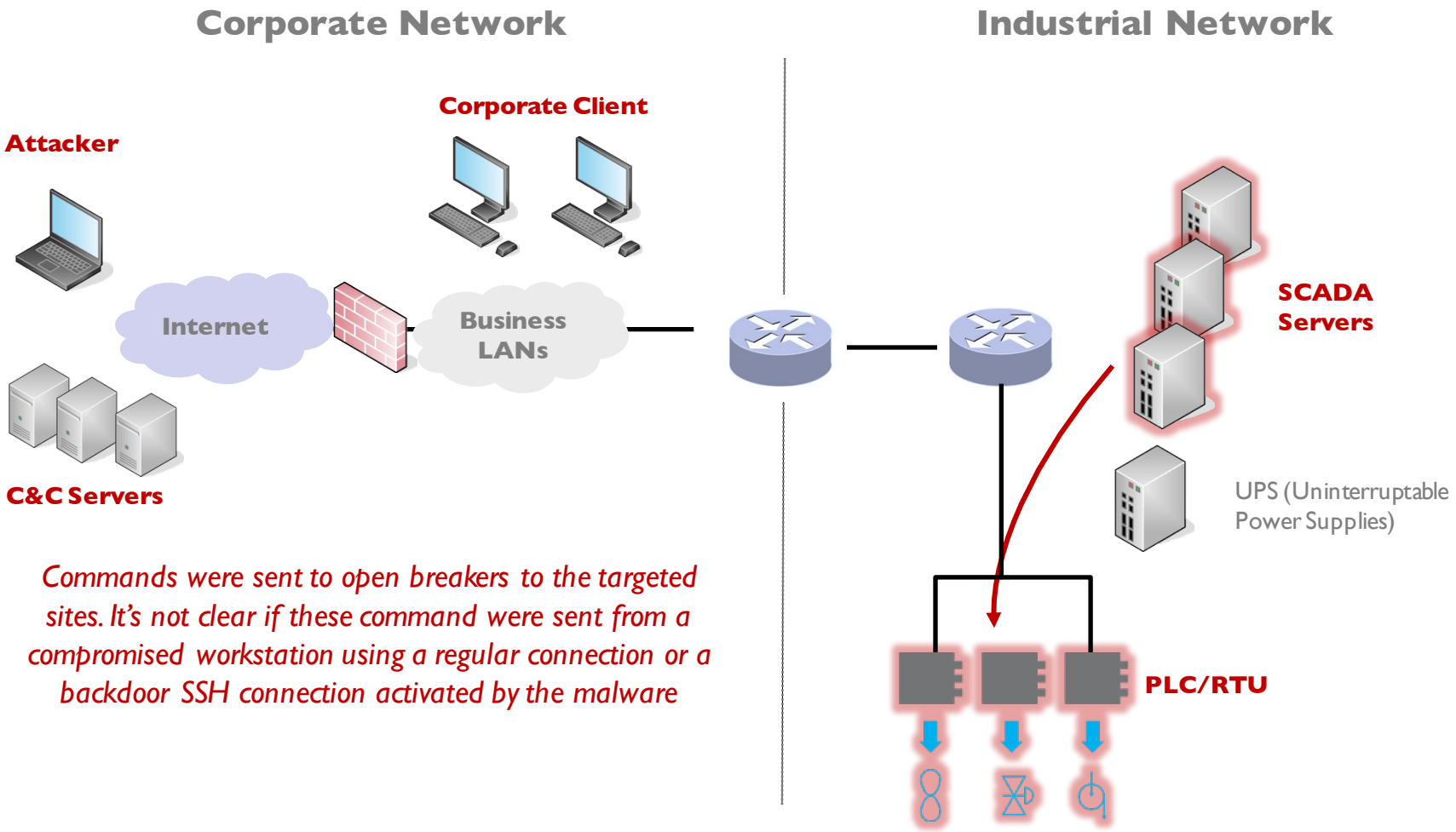
4. SCADA Infiltration - with NOZOMI SCADAguardian



Exploiting HMI software vulnerabilities, the attackers downloaded and implanted Black Energy malware on the SCADA systems

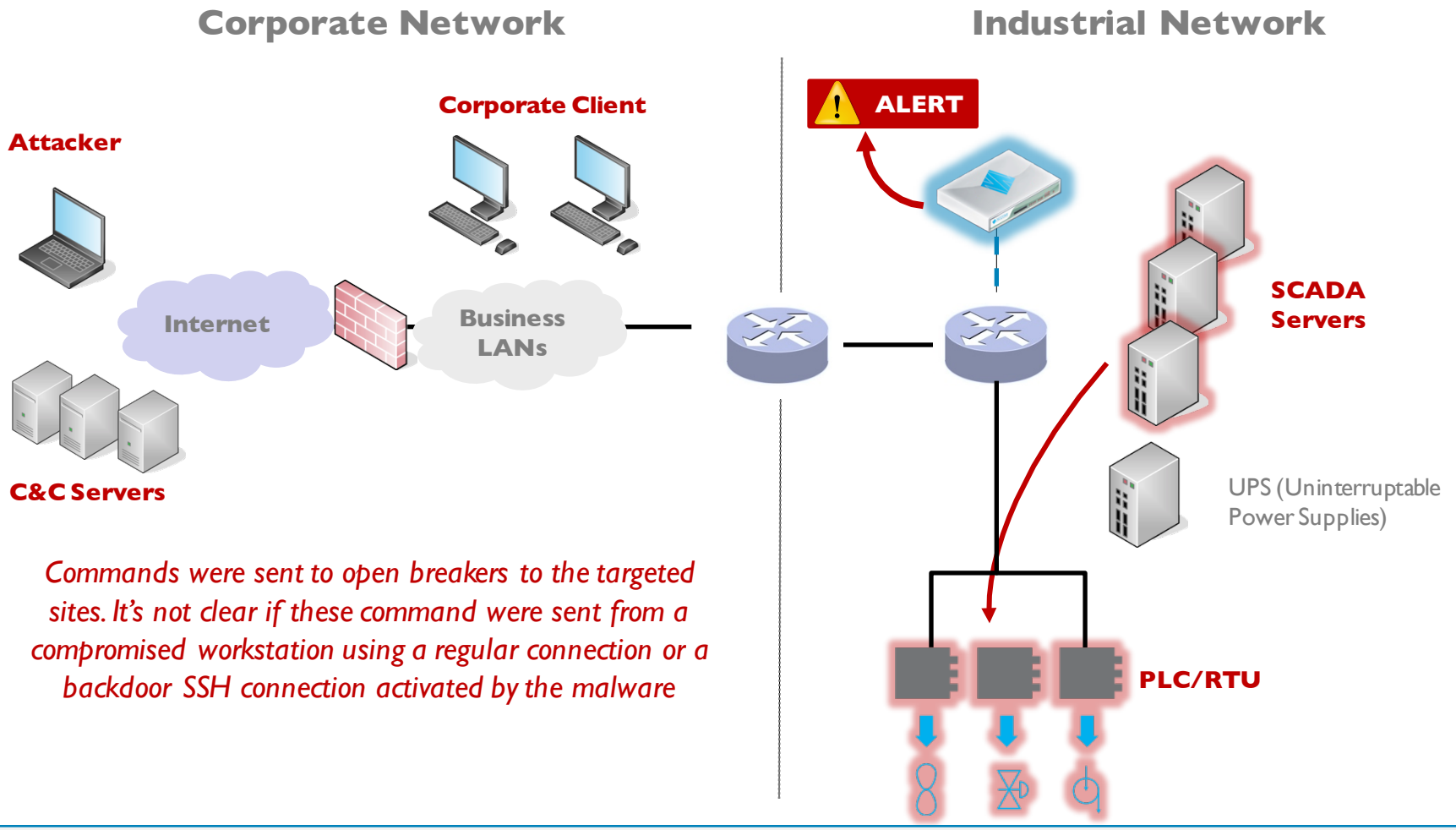
NOZOMI SCADAguardian detects abnormal and suspicious connections, like those from an industrial systems to Internet

5. Electric Outage



Commands were sent to open breakers to the targeted sites. It's not clear if these command were sent from a compromised workstation using a regular connection or a backdoor SSH connection activated by the malware

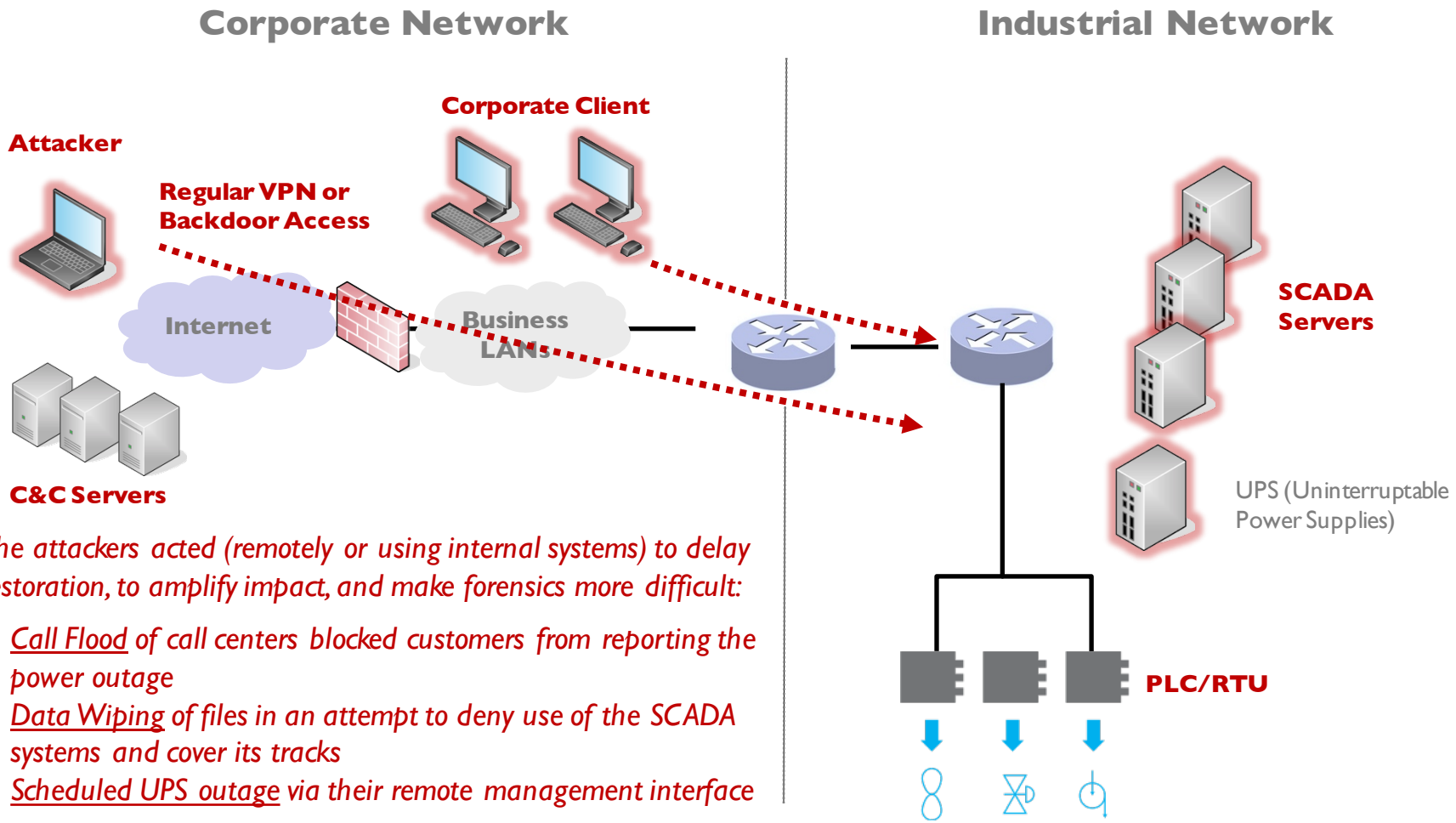
5. Electric Outage - with NOZOMI SCADAguardian



Commands were sent to open breakers to the targeted sites. It's not clear if these command were sent from a compromised workstation using a regular connection or a backdoor SSH connection activated by the malware

NOZOMI SCADAguardian monitors process commands and variables, alerting on critical or undesired conditions

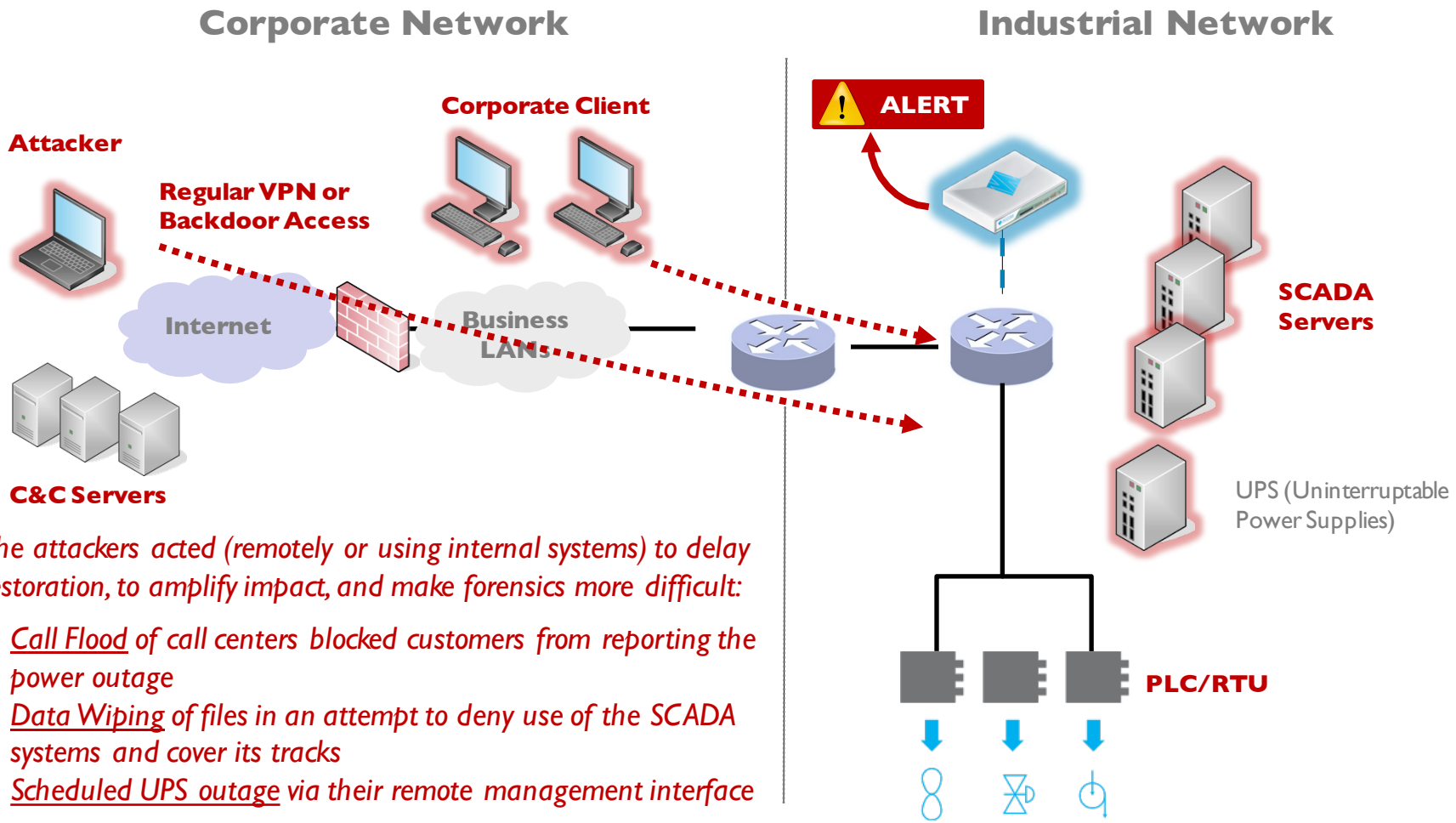
6. Actions to hinder incident response



The attackers acted (remotely or using internal systems) to delay restoration, to amplify impact, and make forensics more difficult:

- *Call Flood of call centers blocked customers from reporting the power outage*
- *Data Wiping of files in an attempt to deny use of the SCADA systems and cover its tracks*
- *Scheduled UPS outage via their remote management interface*

6. Actions to hinder incident response - NOZOMI SCADAguardian

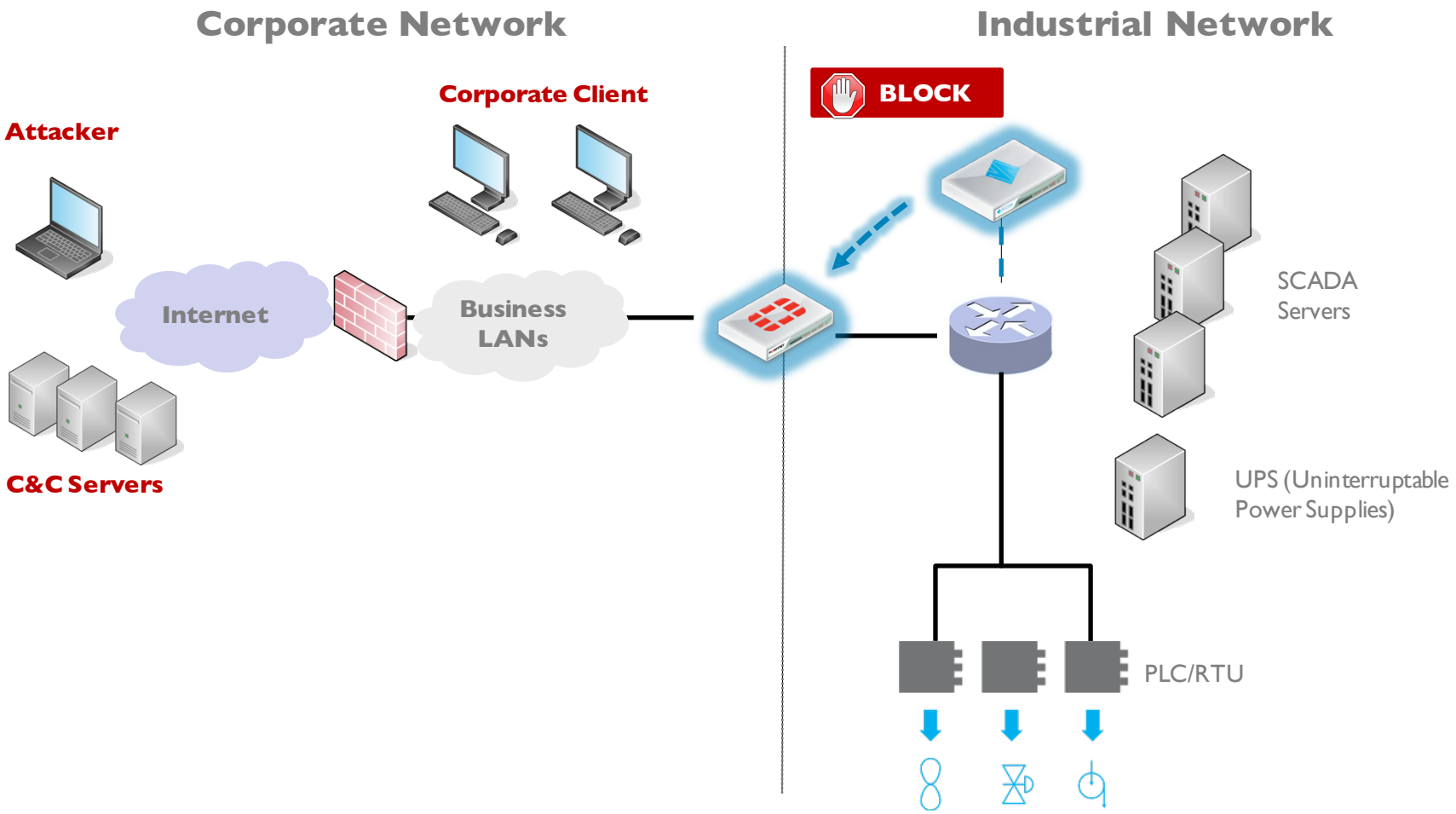


The attackers acted (remotely or using internal systems) to delay restoration, to amplify impact, and make forensics more difficult:

- *Call Flood of call centers blocked customers from reporting the power outage*
- *Data Wiping of files in an attempt to deny use of the SCADA systems and cover its tracks*
- *Scheduled UPS outage via their remote management interface*

NOZOMI SCADAguardian detects abnormal connections (internal or external), such as those generated during the power outage

Extra Benefit: Proactive response with Firewall Integration



The integration between SCADAguardian and the perimeter firewall provides additional protection against these types of attack

NOZOMI SCADAguardian Benefits Summary

- Early warning of reconnaissance activities
- Real-time alerts for SCADA infiltration
- Real-time alerts for abnormal SCADA commands
- Real-time alert for abnormal network connections
- Blocking ongoing attack via integration with perimeter firewall