LIGHTS OUT – CYBER ATTACK ON UKRAINE POWER GRID

Daniel Su & Patrick Tedeschi

A well coordinated attack on 3 power stations in the Ukraine left over 225K without power.

INFORMATION GATHERING

Multi-Stage attack and a high level of coordination indicate reconnaissance went on for at least 6 months

INITIAL ACCESS

Spear Phishing targeted at specific employees with a spoofed email address from the government. Used BlackEnergy 3 malware

PRIVILEGED ACCESS

Discovered VPN which opened direct communication with the adversary by connecting to the Industrial Control System (ICS). Remote access to SCADA Interface

DATA COLLECTION

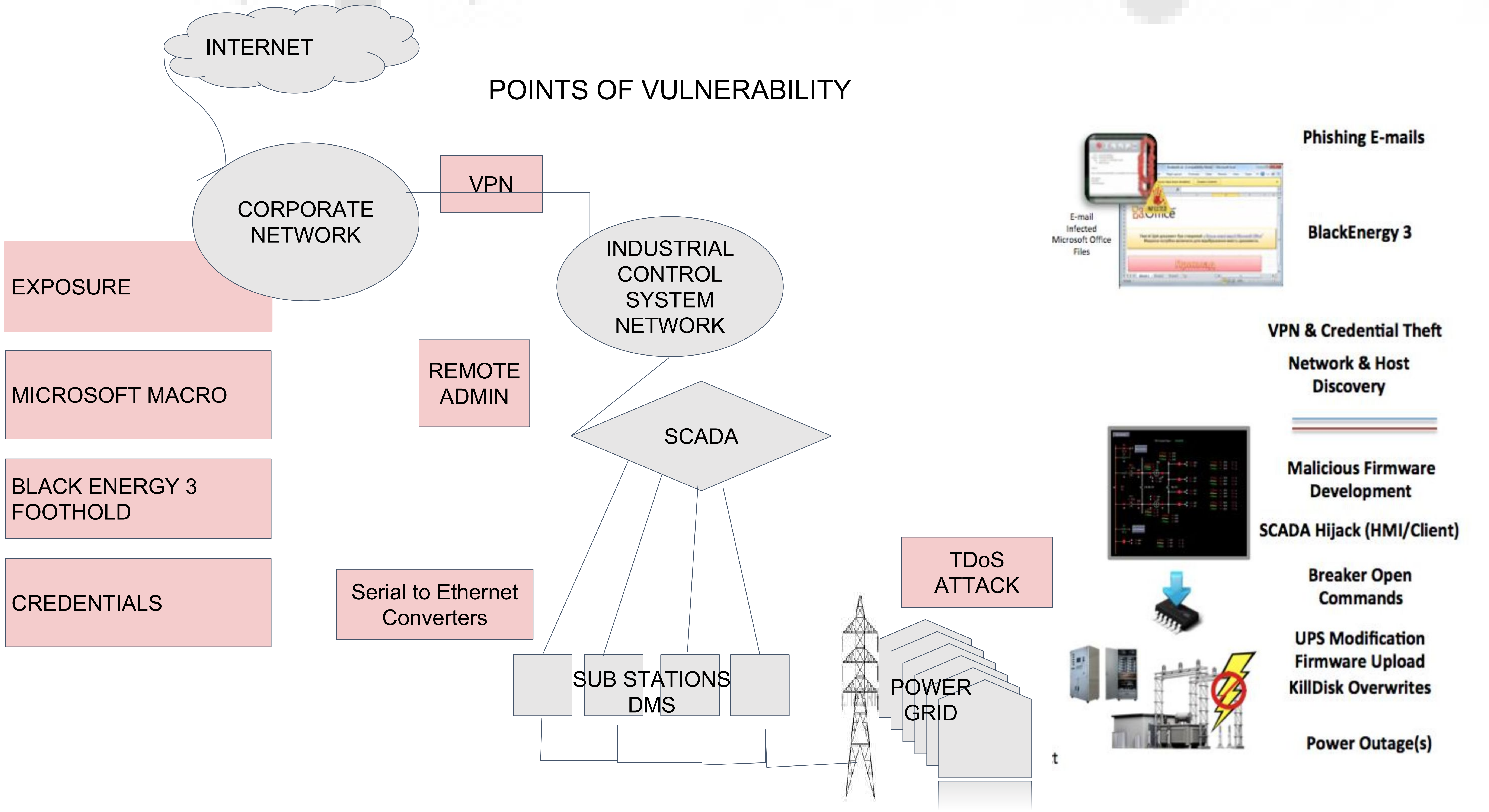
Identified VPN between Corporate Network and ICS. Afterwards, mapped out ICS network and tested malware on Serial-to-Ethernet devices

MAINTAIN ACCESS

Backdoor inside business network makes consistent access into ICS possible

COVER TRACKS / EXECUTE

Malicious firmware uploaded to Serial-to-Ethernet devices. Provided manipulation of commands from the SCADA network to the substation control systems



INTERNET

POINTS OF VULNERABILITY

CORPORATE NETWORK

VPN

INDUSTRIAL CONTROL SYSTEM NETWORK

EXPOSURE

MICROSOFT MACRO

REMOTE ADMIN

SCADA

BLACK ENERGY 3 FOOTHOLD

CREDENTIALS

Serial to Ethernet Converters

TDoS ATTACK

SUB STATIONS DMS

POWER GRID

t

Phishing E-mails

E-mail Infected Microsoft Office Files

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery

Malicious Firmware Development

SCADA Hijack (HMI/Client)

Breaker Open Commands

UPS Modification

Firmware Upload

KillDisk Overwrites

Power Outage(s)

Compromised Security Principles

1. Separation of Privilege: Lack of 2-factor Authentication
2. Authentication: Credentials Impersonated
3. Non-repudiation: Unable to identical Hackers
4. Complete Mediation: Microsoft Vulnerability
5. Confidentiality: System infiltrated and researched thoroughly
6. Integrity: Killdisk Uploaded
7. Availability: Access between SCADA and Substations compromised

UNC
DEPARTMENT OF COMPUTER SCIENCE