Ukraine Power Grid Cyber Attack

Guy Barnhart-Magen
@Akamai, December 2019

@barnhartguy


Hi
I’m Guy
@barnhartguy

Who am I?

Father of two, hacker

BSidesTLV chairman and CTF Lead
(Lucky to speak at many conferences)

Today: Cyber Security Consultant

Before: Intel, Cisco and a couple of Startups

- Security of ML
- OS Hardening
- Crypto
- Embedded Security

@barnhartguy

@barnhartguy

DISCLAIMER

personal story

my own experience (~3 years ago)

Opinions are my own, some guesswork involved

BACKGROUND

Why is it interesting?

- Attack took place on December 23rd, 2015
- First “public” cyber attack
  - And a successful one at that
- Interesting aspects to the attack:
  - Multiple Stages
  - Multiple Groups

WHAT WILL WE COVER?

- Background
- Attack layout
- Anecdotes
- Then attack #2 happened (not covered in this talk)
- Then “WannaCry” and “Petya” happened
- There was much rejoicing

WHY IS THIS INTERESTING?

First large scale attack on a utility, discussed in public
Attack caused critical infrastructure to fail
This could have been much worse that it was

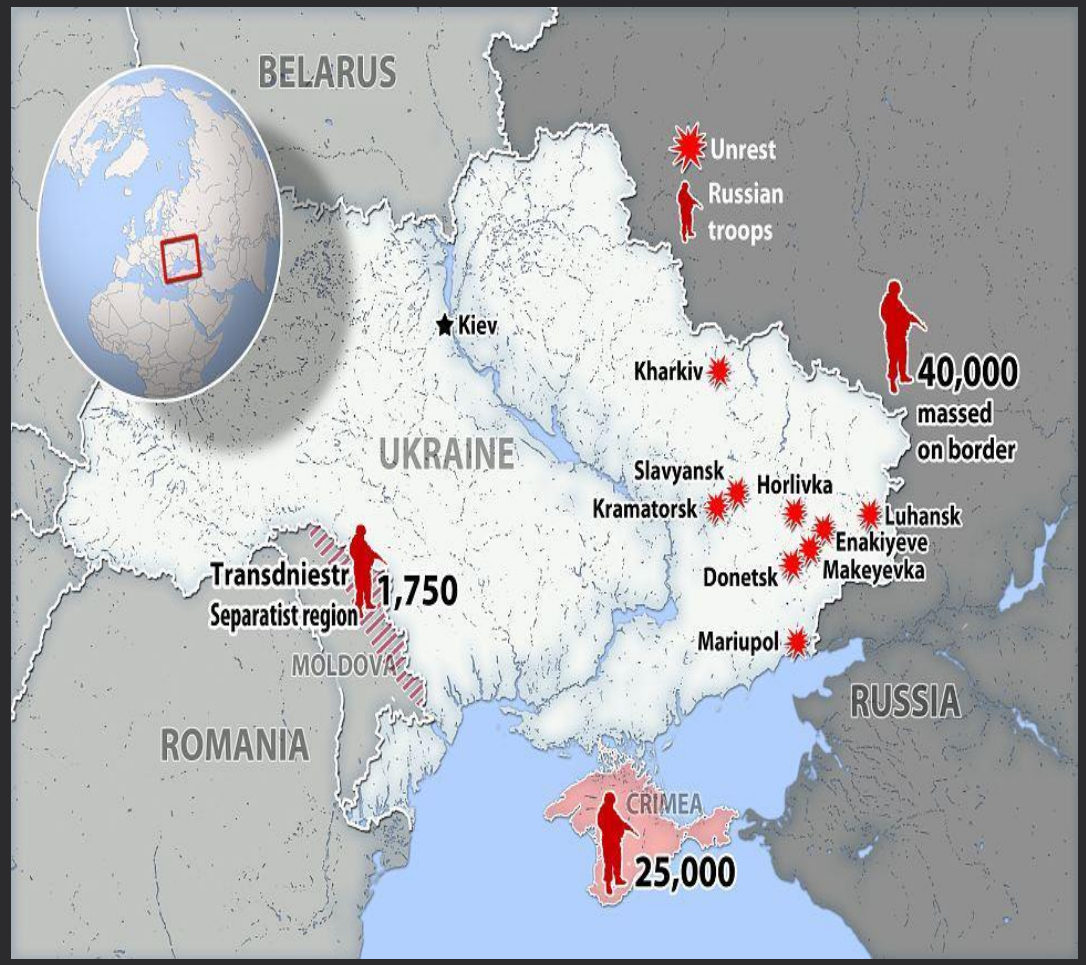
Probably a warning shot – not a full out attack

WHAT WILL WE COVER?

- The attack focused on 3 power utilities in the transport segment
- Over 250,000 people affected
- December 2015, winter, Ukraine
- Holiday – less people in the office
- Multi team/phased attack

SCOPE
Who? What? Where?

- Three transmission companies affected
- ~73 MWh, 0.015% of daily consumption
- Most customers had power restored in under 7 hours
  - Although no power in soviet winter is harsh
- Attributed to Russian hacking team “Sandworm”

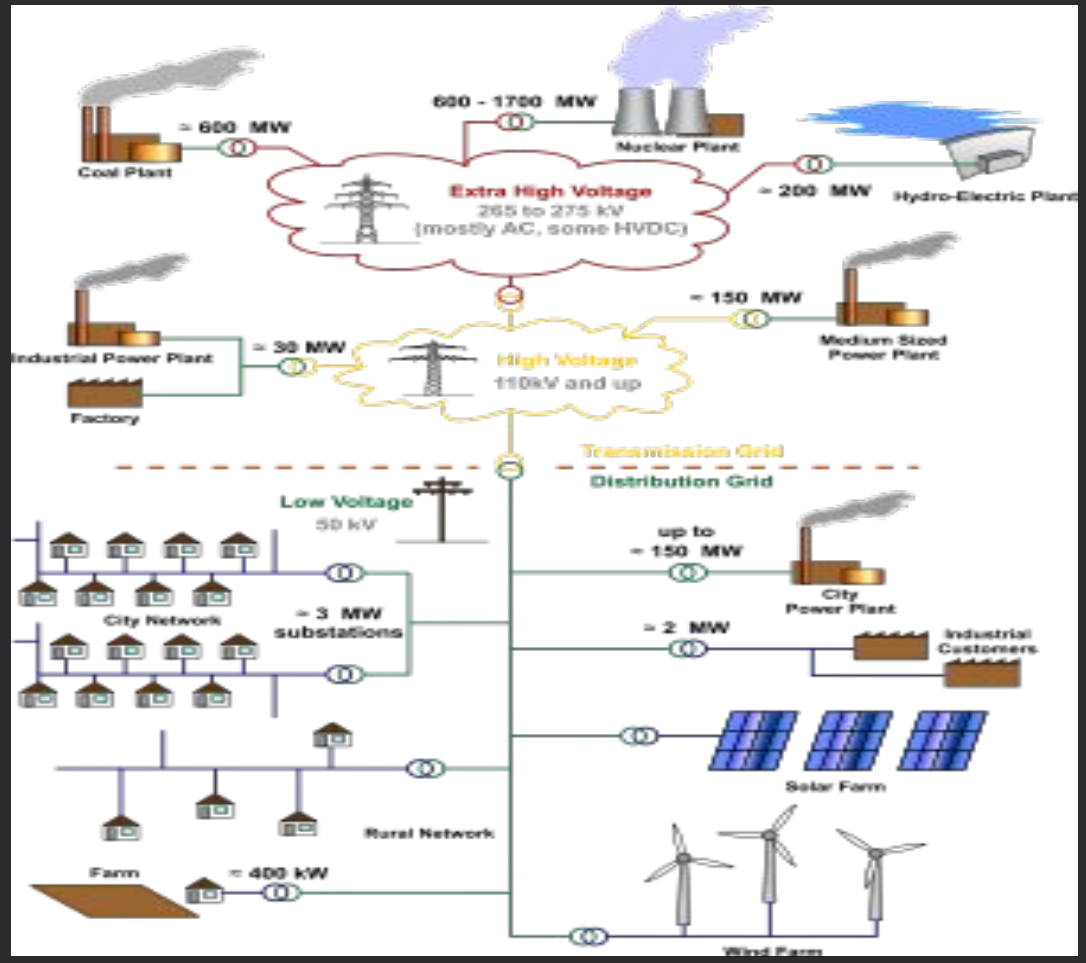


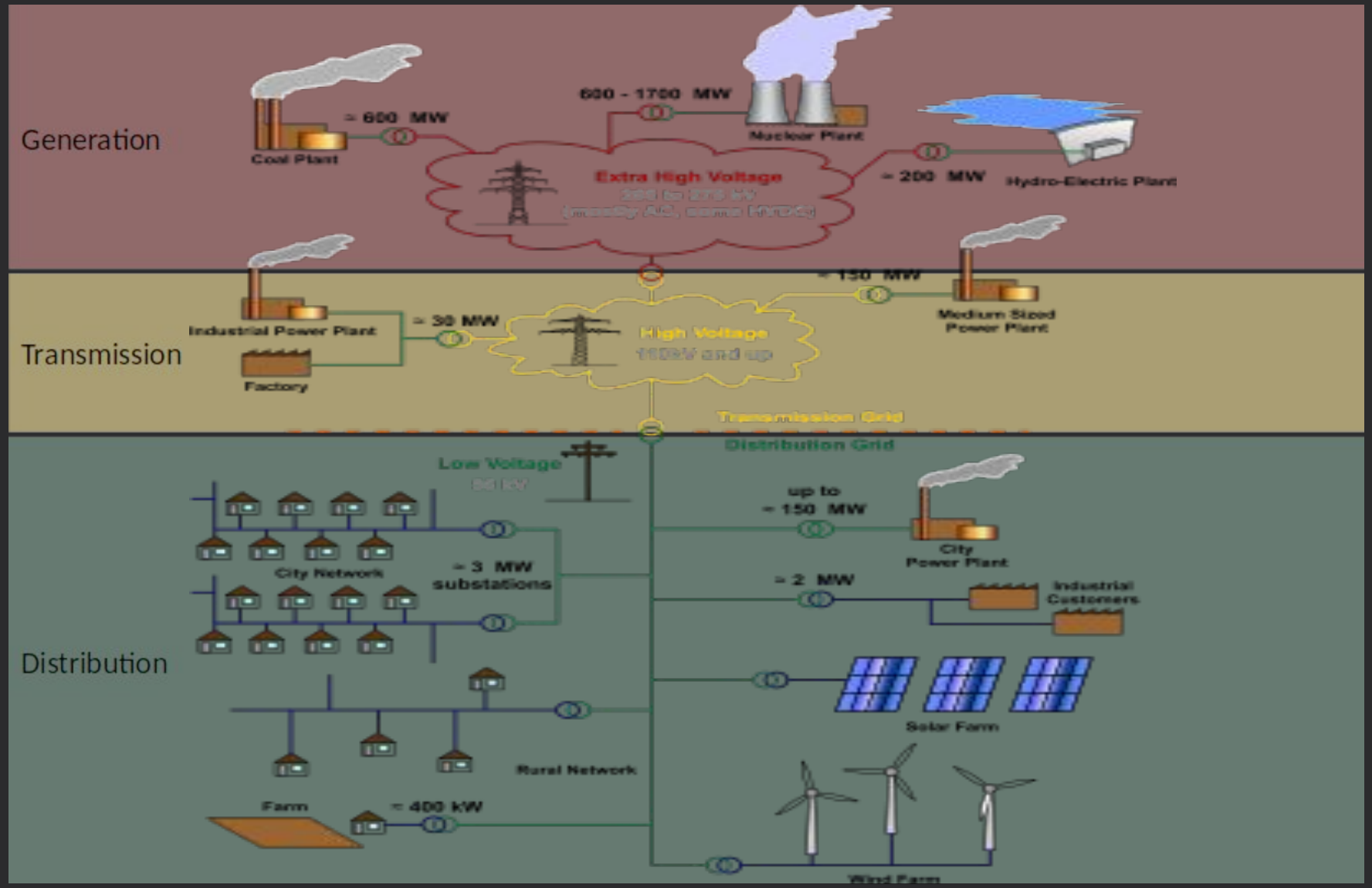

BELARUS
Unrest
Russian troops
Kiev
Kharkiv
40,000
massed on border
UKRAINE
Slavyansk
Horlivka
Kramatorsk
Luhansk
Enakiyeve
Makeyevka
Donetsk
Mariupol
Transdniestr
Separatist region
1,750
MOLDOVA
ROMANIA
RUSSIA
CRIMEA
25,000

POWER GRID

Some Fundamentals

- Generation
- Transmission
- Distribution
- Consumers
  - Industrial
  - Commercial
  - Private





Operational Technology (OT)
vs. Information Technology (IT)

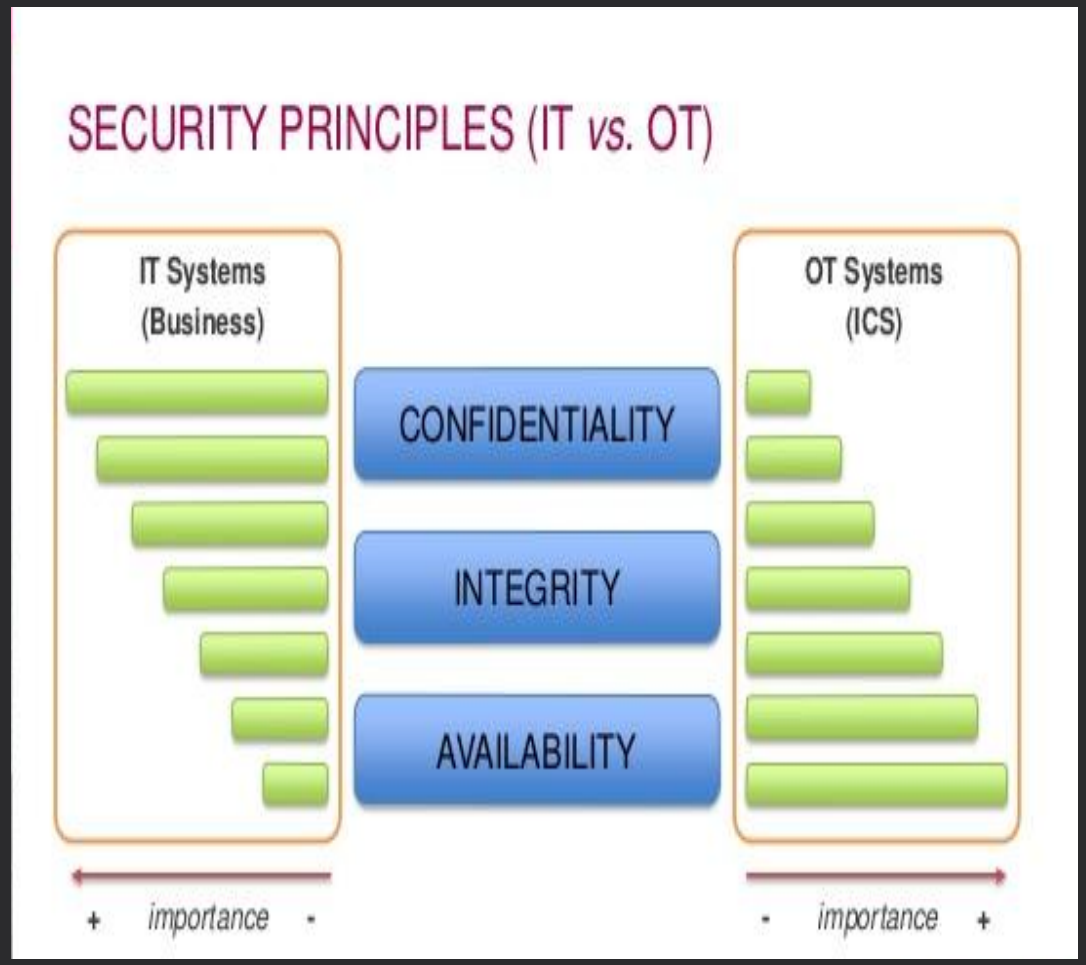
- Different emphasis in the industrial world
- Robustness, ruggedness most important
- Trusted technologies for more than 50 years
- New equipment, old technology
- IT introduced hybrid systems
  - A lot of converters, gateways
  - Most data thrown away

- This is IIoT

OT Security Emphasis

Why can't they measure up?

- Security is often bolted-on after the fact
- Almost security at the edge
  - Also no monitoring, upgrades, patches, etc.
- Monetary values of a different order of magnitude
  - Cost of equipment
  - Cost of failure, maintenance
- Running production overrules security every time
- Security teams care, have little influence



EXAMPLE

RS232 to Ethernet Converters

- Used to connect OT equipment to gateways
  - These gateways connect to IT at some stage
- They are built to be:
  - Robust
  - Idiot proof
  - Upgradable
- They do not have “security”
  - The most advanced have username and password
    - Hardcoded ☹
- This is by design! (see “idiot proof” above)

@barnhartguy

Attack Stages

Rough outline, ~9 months in total

01 MARCH 2015

02 MAY 2015

03 DECEMBER 2015

04 MARCH 2016

Stage 1
Spear phishing

- There was an active plan to privatize the Ukrainian power grid companies
  - This was already taking place
- Managers in the companies received emails containing malicious links from official functionaries (who were hacked separately)
- The hackers silently explored the network, establishing various footholds

Stage 2

Network layout and planning

- The attackers studied the network well
- Special attention:
  - Admin credentials
  - Phone infrastructure
  - UPS infrastructure
  - Backup internet access (ISDN lines, etc.)
- Infrastructure prepared for attack
- Attackers went dormant

Stage 3
The Attack!

- Trigger was political, mostly
- Multiple parties attacking simultaneously
  - IT Team
  - OT Team
  - Telephony Team

First Step

Plan your execution, Execute your plan

- The data center UPSs were put into scheduled maintenance mode
  - Shutdown at +4h
- This is unmonitored
  - Who should get alerts on scheduled maintenance?
- Note: the UPSs are still operational at this time

First Step

Plan your execution, Execute your plan

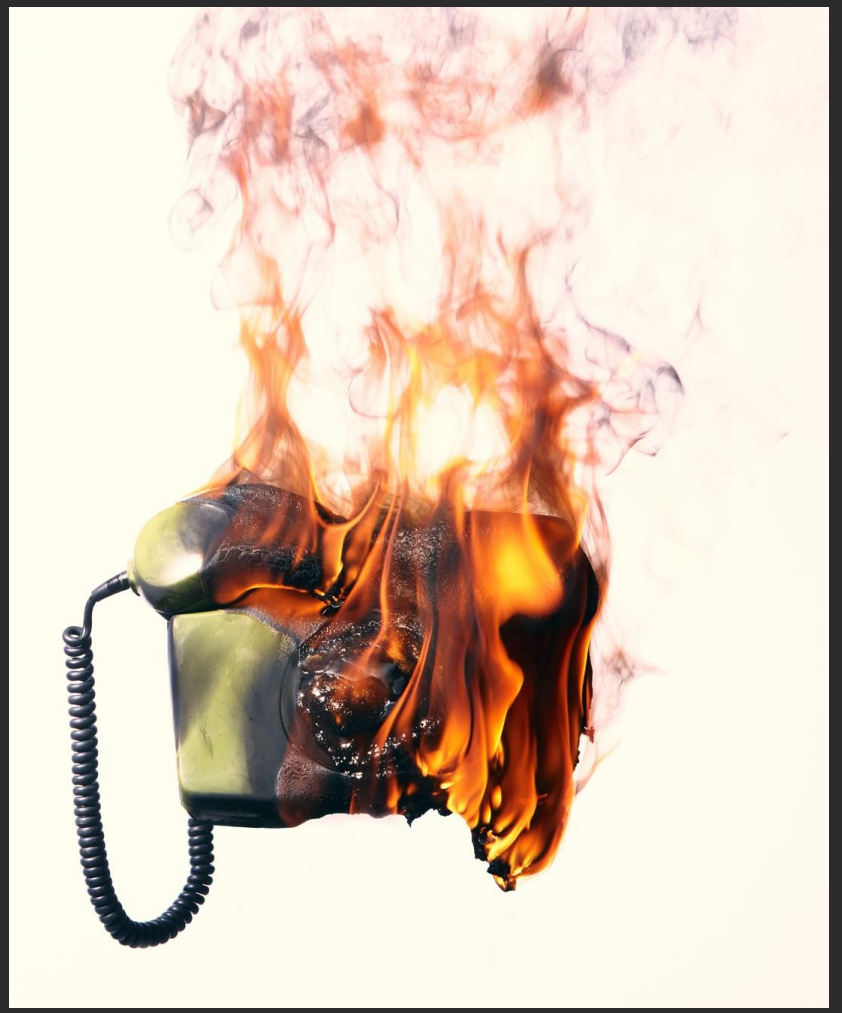
- Used pre-harvested credentials to replace all relevant passwords
- Took over C&C stations
- VNC lockout

First Step

Additional Shenanigans

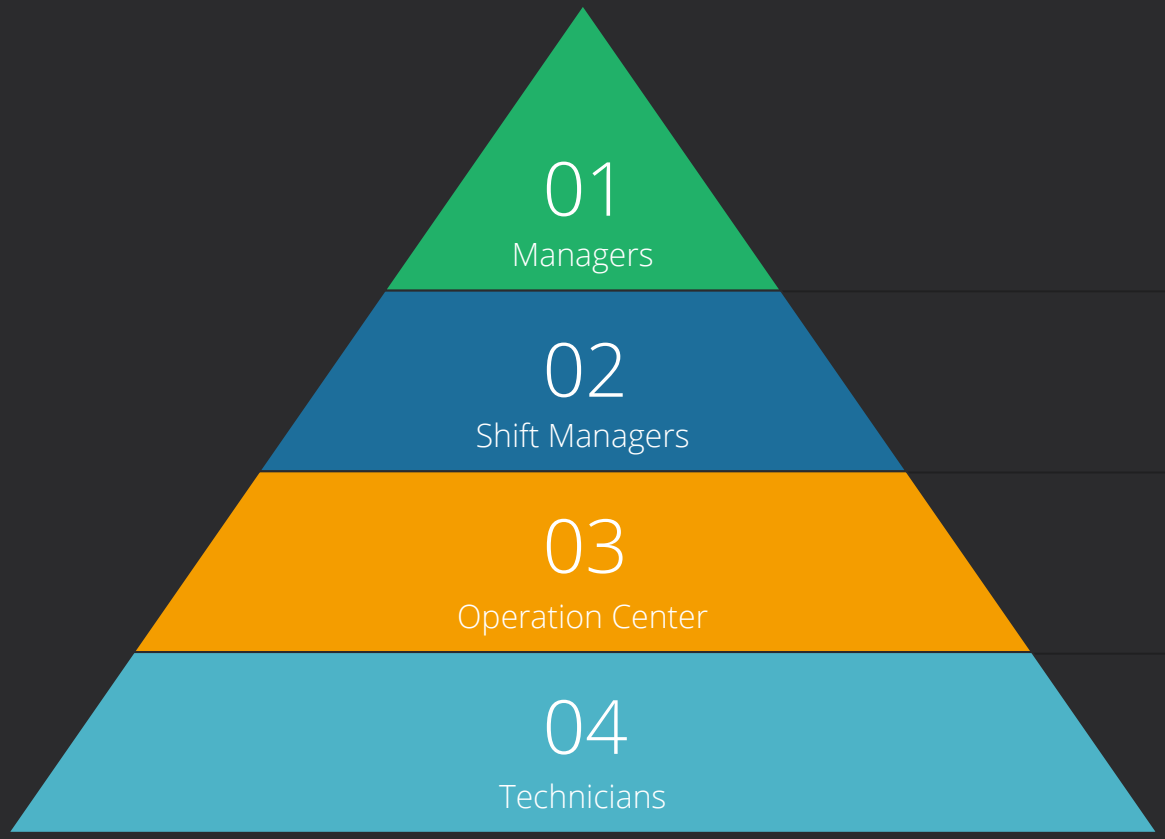
- Telephony Denial of Service
  - No one can call in to the offices
  - Specifically the operation center
- Preventing customers from complaining?

- Not really against customers (as reported in the media)
- Break connection between central control (NOC) and operators at the sub-stations
- No coordinated response



First Step

TDOS is fun they said...



Managers need to make decisions

Decisions are limited to people present in the building

Operation teams are locked out of most computers, cannot call technicians

Technicians cannot communicate with operation center, get commands

Second Step

All your C&C now belongs to us

+1h

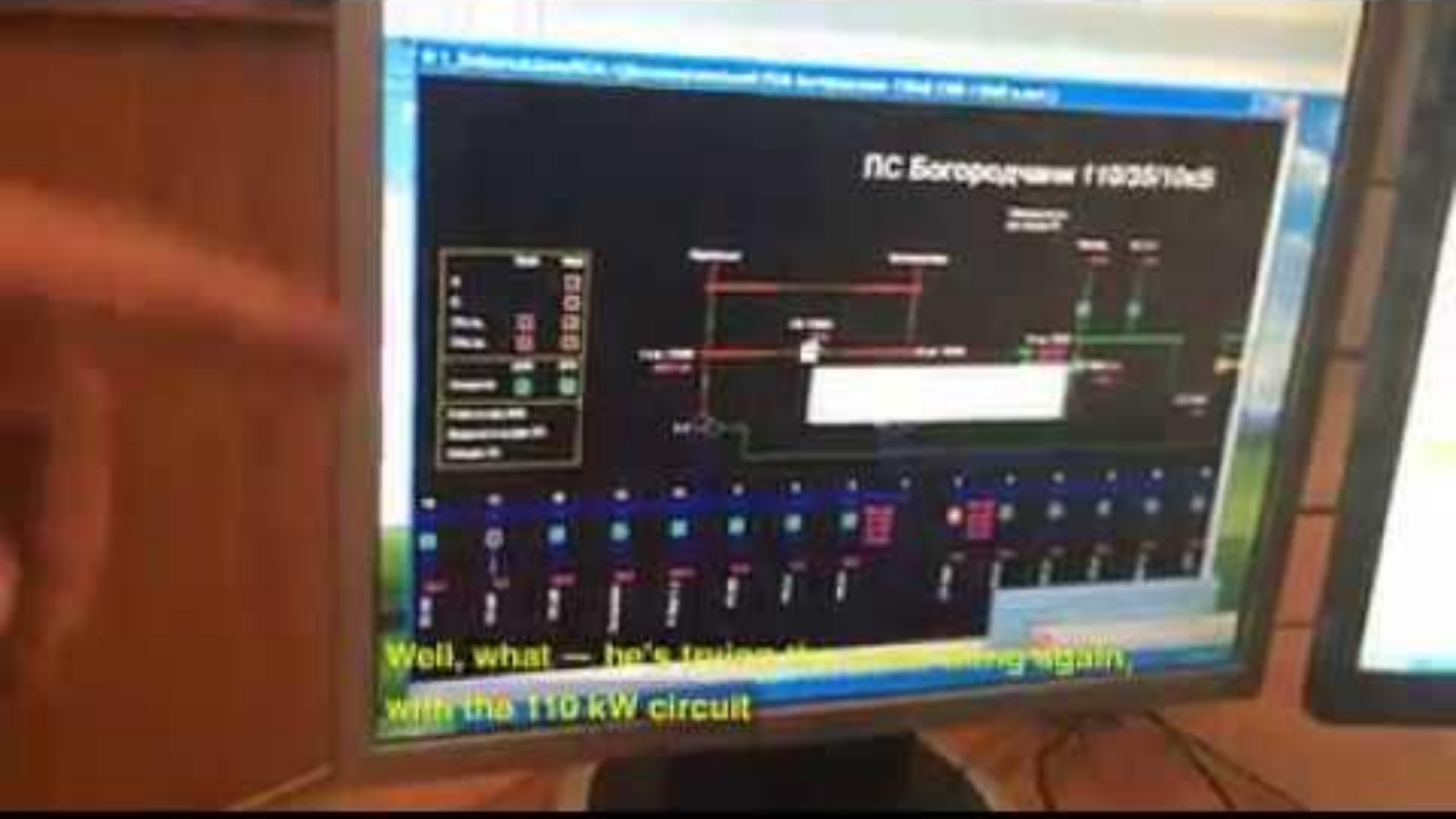
- Using admin credentials, change admin passwords
- Lock VNC sessions to view only
- Take over C&C workstations

@barnhartguy

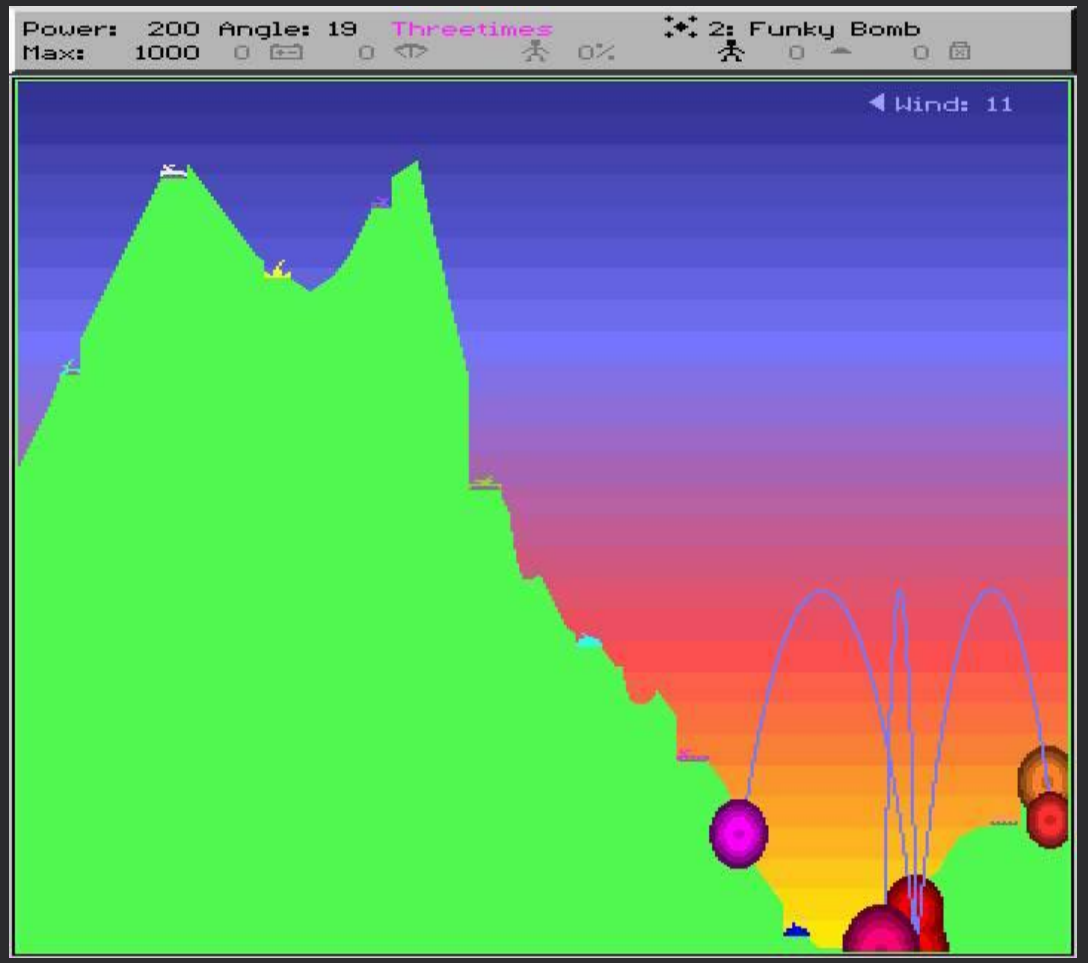
Third Step

Who guards the guards?

- Turning off circuit breakers
- Taking gateways offline
- Shutting down equipment
  - These are legitimate commands coming from the C&C!


ПС Богородичная
Well, what — he's
with the 110 kW circuit

Scorched Earth: Making this more than a “cyber attack”



@barnhartguy

Stage 4

Scorched Earth: Making this more than a “cyber attack”

- Sending firmware updates to OT control units
  - Targeting over 50,000 units, mostly RS232-Ethernet converters
  - Not actually firmware but garbage
- Result: Bricking the devices
- Outcome: now everything is manual

Stage 4

Scorched Earth: Making this more than a “cyber attack”

- Remember the UPS?
- Now its turning off
- SOC has no more power

@barnhartguy

Anecdotes

@barnhartguy

KILL SWITCH?

- The attackers knew their network better than them
- The SOC tried shutting down the routers (both of them)
- The attacker had a backup route through the ADSL backup
- The SOC didn’t know about the ADSL backup…

3 COMPANIES, REMEMBER?

- 2 of these companies had their C&C station taken over
- At the 3rd company – they couldn't take over the C&C station
- Technical difficulties

Solution? They spun up their own instance of a C&C station in one of the servers

MALWARE

- A lot of discussion around the “Black Energy” malware
- Was it such an important part of the plan?
- My guess – not so much
- They could accomplish the same goals with TELNET

GOVERNMENT REGULATORS

- The Ukraine regulator was working hard on privatizing the power grid companies
- This was a major move that was supposed to happen early 2016

PHISHING, yes - phishing

- Around march 2015 the attackers used a government regulator mail server to phish the transmission company
- They got in through the email
- Scoped the network, hunted for credentials
- Stayed dormant for many months

REDUCED DAMAGE

- They didn’t understand the grid
- A lot of damage could have been done through deliberate shutdown of specific switches

STROKE OF LUCK

- The main reason the recovery was so fast was that they had a large number of skilled manual labor at hand
- Remember – they were all supposed to be fired and replaced with automation systems (yes, the pawned ones)
- Although power was recovered – the automation system was not
- The vendor didn’t have a hardened version – the best he could supply was hard coded passwords

SECURITY ISSUES

Well, who should we blame?

SECURITY ISSUES
Well, who should we blame?

- OT networks are rarely monitored
- IT networks are somewhat monitored
  - Does this help against a skilled adversary
  - Most alerts go unnoticed in the noise
- There was no immediate disaster recovery plan
  - Immediate response was improvised
- TDOS is an issue that should be planned for
  - What other assumptions are we making?
- What systems can you trust? Should you trust?
  - Think of stuxnet

@barnhartguy