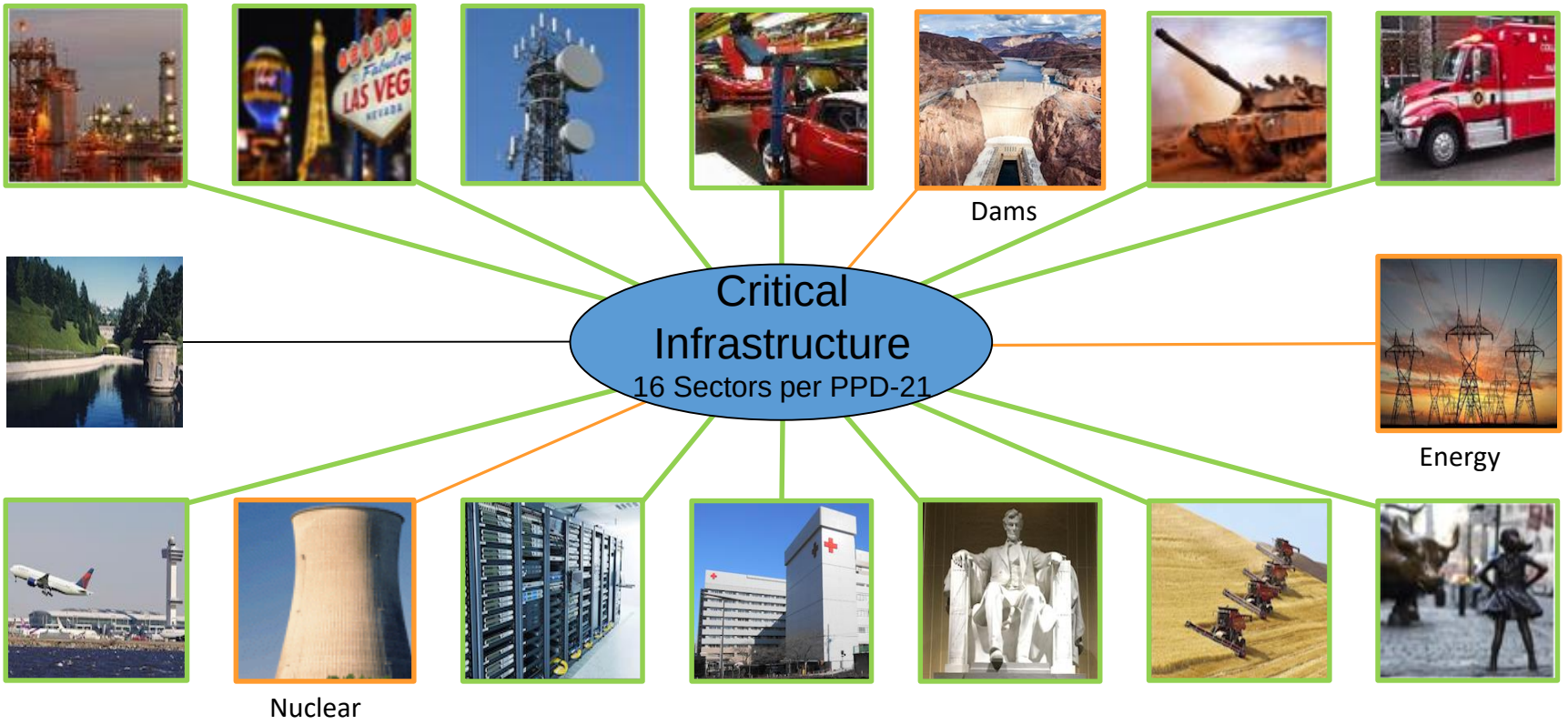
NCCIC | NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

LITTLE ARC-FLASH:
HOW DIGITAL ATTACKS CAN CAUSE PHYSICAL RAMIFICATIONS

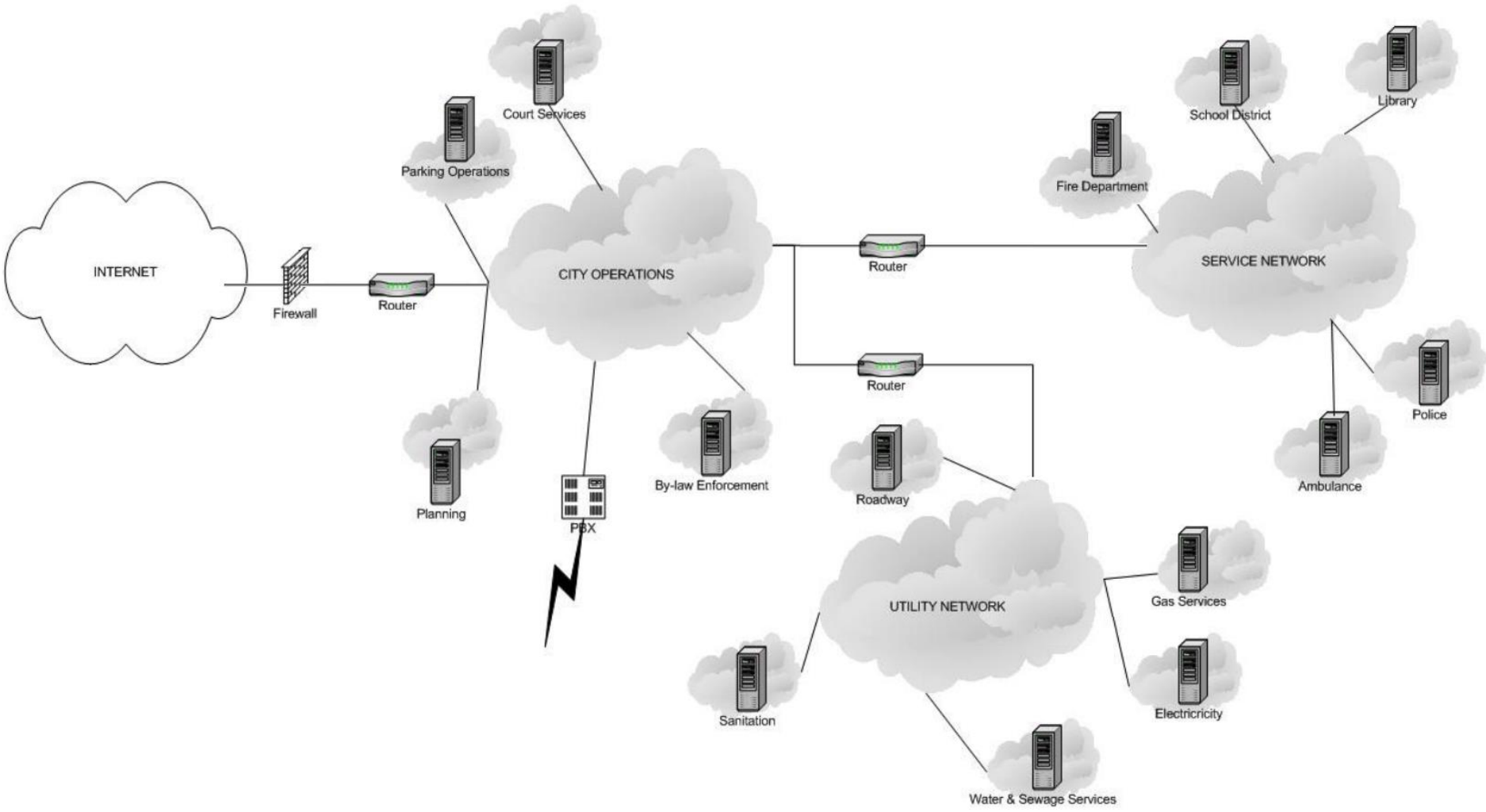
7/18/2019

NCCIC

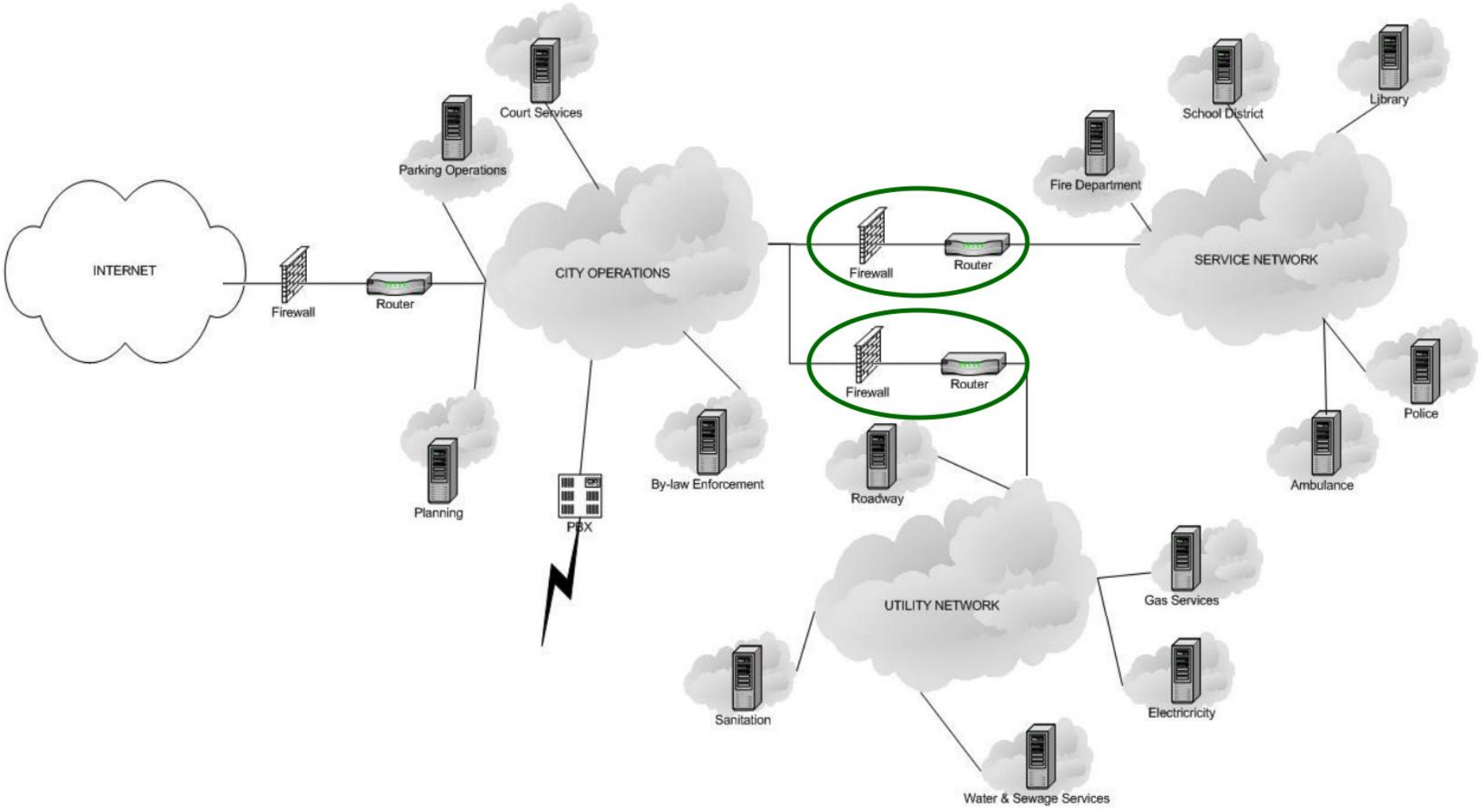
Critical Infrastructure Sectors



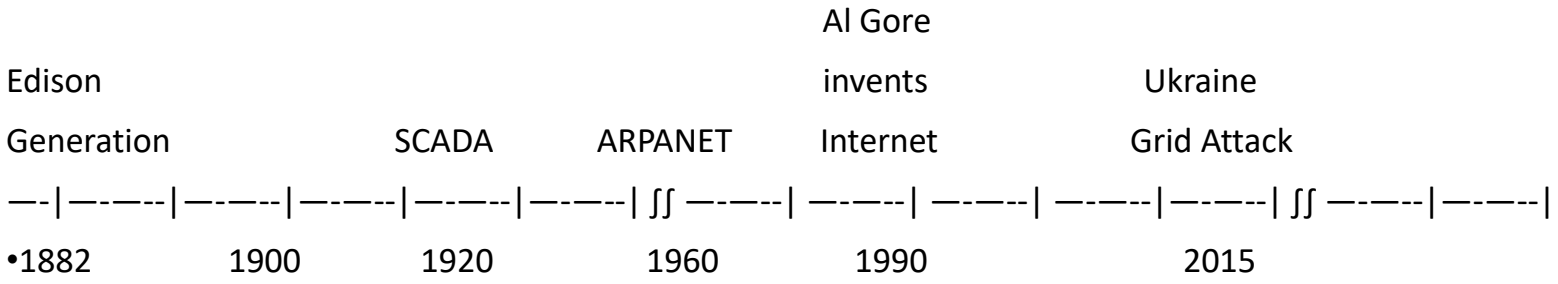
Flat Networks Pose Significant Risk



Isolated Networks are the First Mitigation



Moving into the Present



From the Perspective of an Attacker

How to Approach the Target?

- Reconnaissance
  - Opensource research

- Gain access to the network through any workstation
  - Each employee has access to some level of sensitive information
    - Email, applications and logistics all provide new insights to the inner workings of the organization

- Elevate access through either an exploit or credential harvesting
  - Zero day exploits are rarely used or needed

How to Approach the Target?

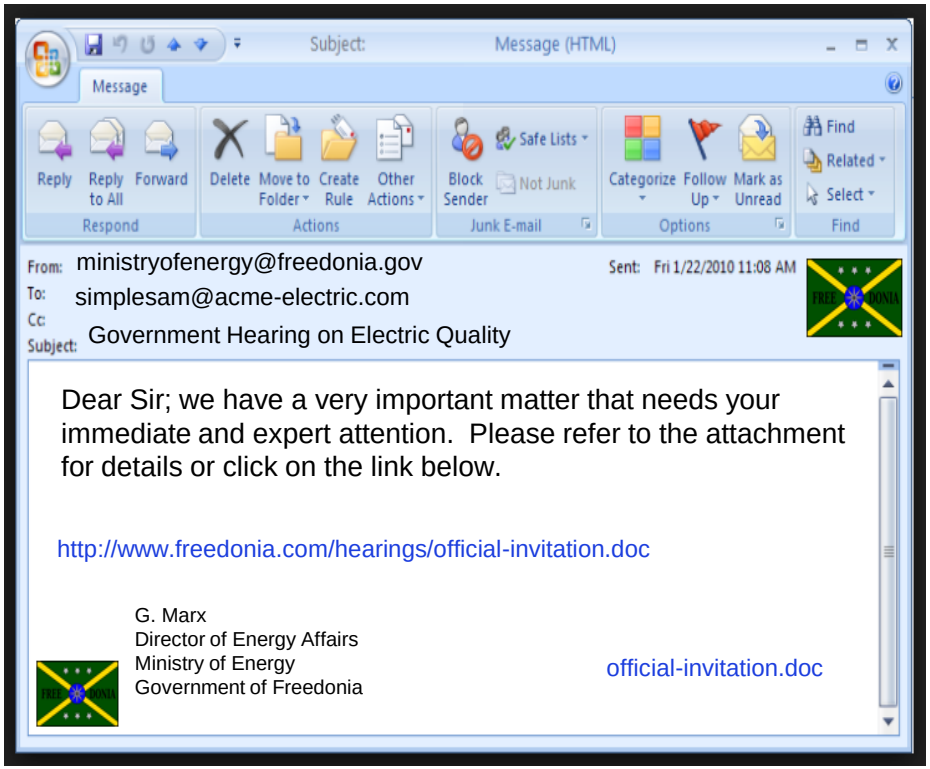
- Determine how and when to cause a certain outcome
    - This process may take considerable time
        - Gathering intel can be a lengthy process, and time between initial intrusion and taking action will make post-mortem analysis more difficult
        - Understanding the system and how to disrupt it or cause a cyber-physical consequence
- Timing depends on desired effect
    - Holiday? Weekend? Weekday?

- Strike when there is a lack of visibility or when a larger impact can occur

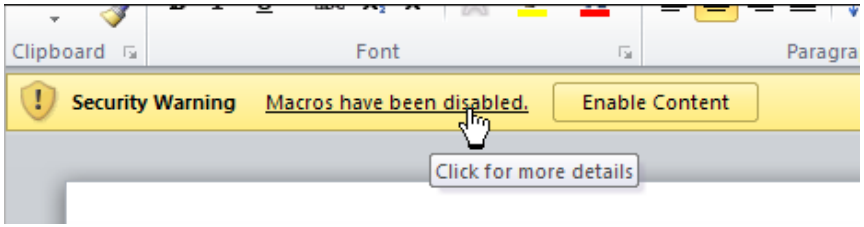
Approach A: Spear Phishing

- Pros:
- Very little time investment for the attacker
- Exceedingly high likelihood to be effective
    - People get used to repetition
- Cons:
- Could expose the attack effort if someone investigates

BlackEnergy



- An official invite from the government!
- The ministry of energy asked for my help!

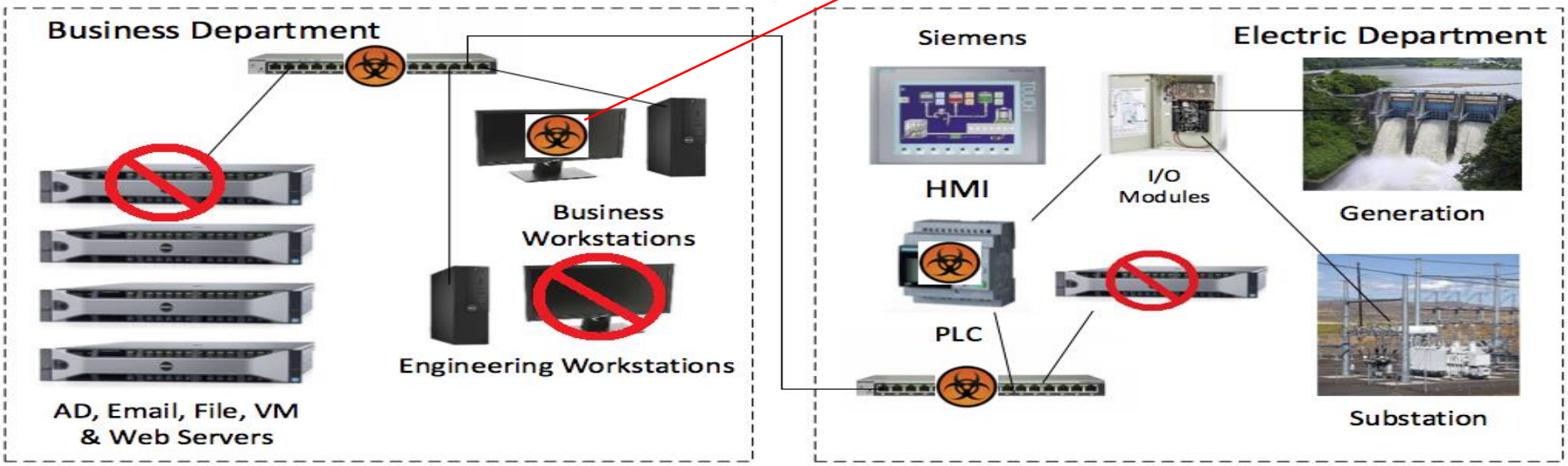


It is definitely official alright, its got the seal in the email and everything.

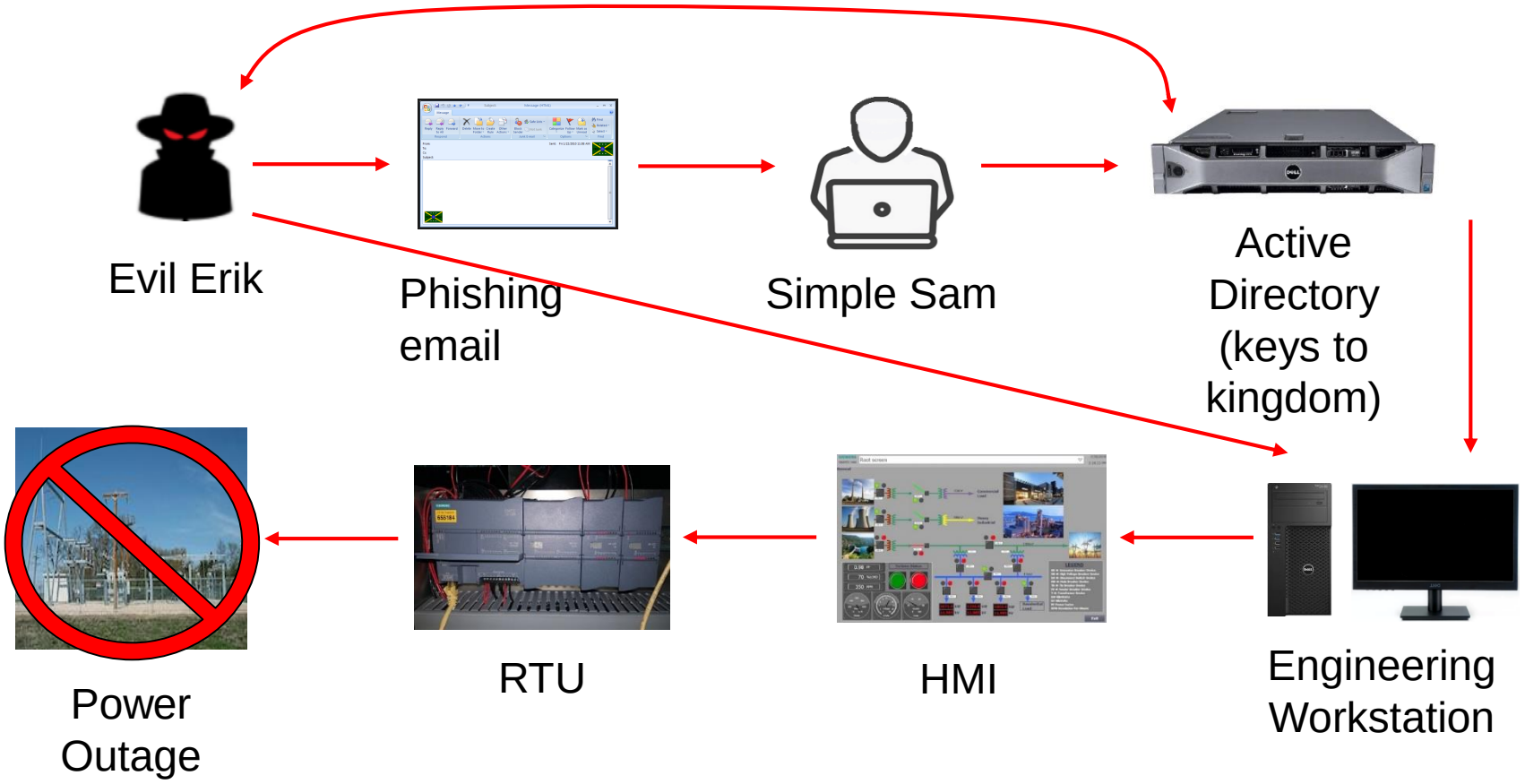
I better enable macros to view, it must be incredibly important.

BlackEnergy

- Multiple infection vectors
- Macros enabled in a Word document
- HMI software vulnerabilities
- Variants targeted routers
- Destructive: Overwrite files and hard drives



BlackEnergy Timeline



Approach B: Watering Hole

- Pros:
- Much more difficult to discover
- May provide elevated access immediately
  - Much more reliable for segmented networks
- Cons:
- Requires upfront effort to compromise third party
  - Operation could be derailed if discovered early
- Difficult to control timeframe

Havex

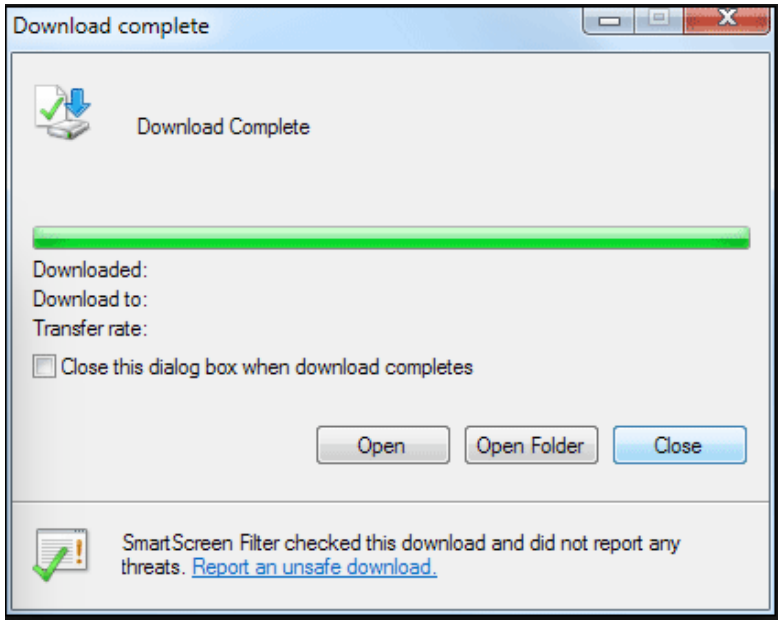
- Its time to patch! Let's get the latest updates from our trusted vendor.

Checkums

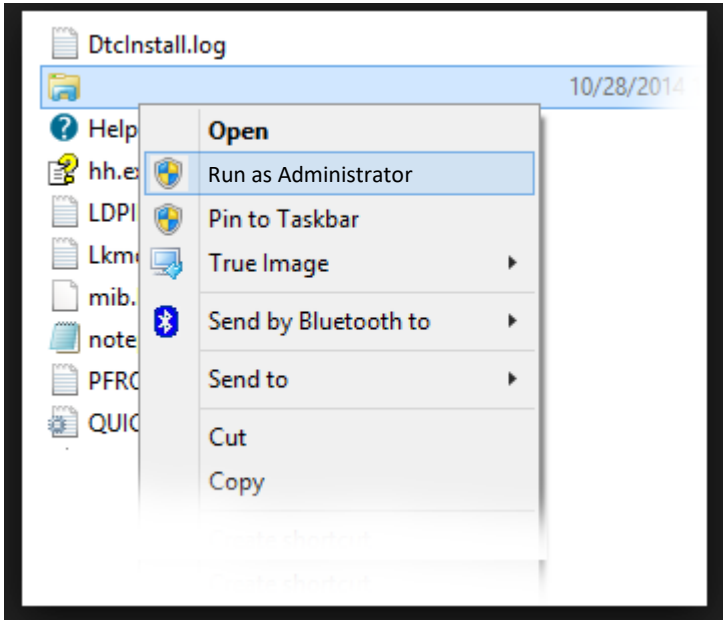
md5	42fc5859322ca48798651db3a77e2748
LM	fb19972931b97724e3ffaf3a65f0dbd1
NTLM	31d6cfe0d16ae931b73c59d7e0c089c0
sha1	b02e34bdbab0ef4da9e034c9c2c8d6412abac8bf
sha256	fe8fa4daa404ebb3bd6df4c20650a1c94ee686d0fe624aa4cda3fe7d1282ce32

I wonder what this gobbledygook is for?

Havex

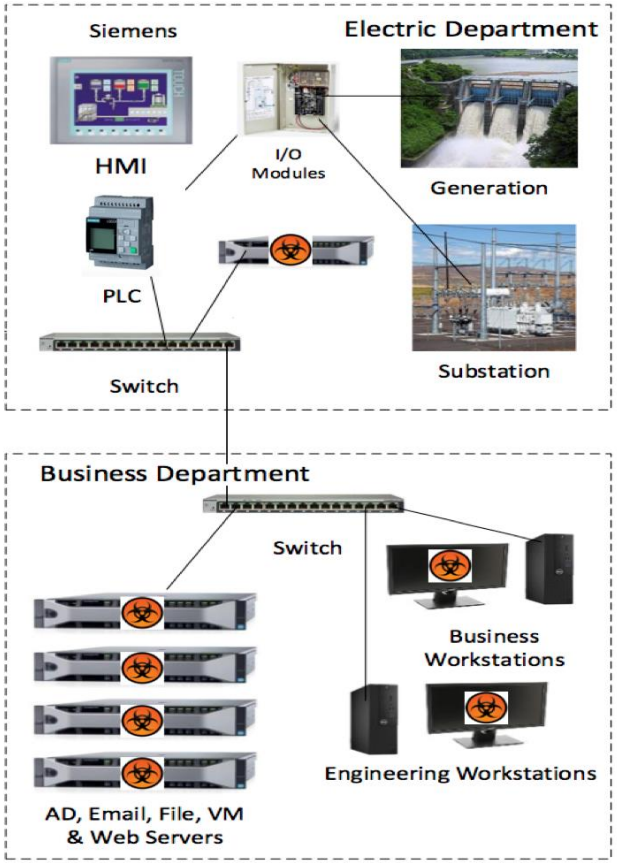


I don't remember the last update taking that long to download. Hmmm… and this patch seems to be a weird size?



However, I'm really busy today, I need to get this installed ASAP.

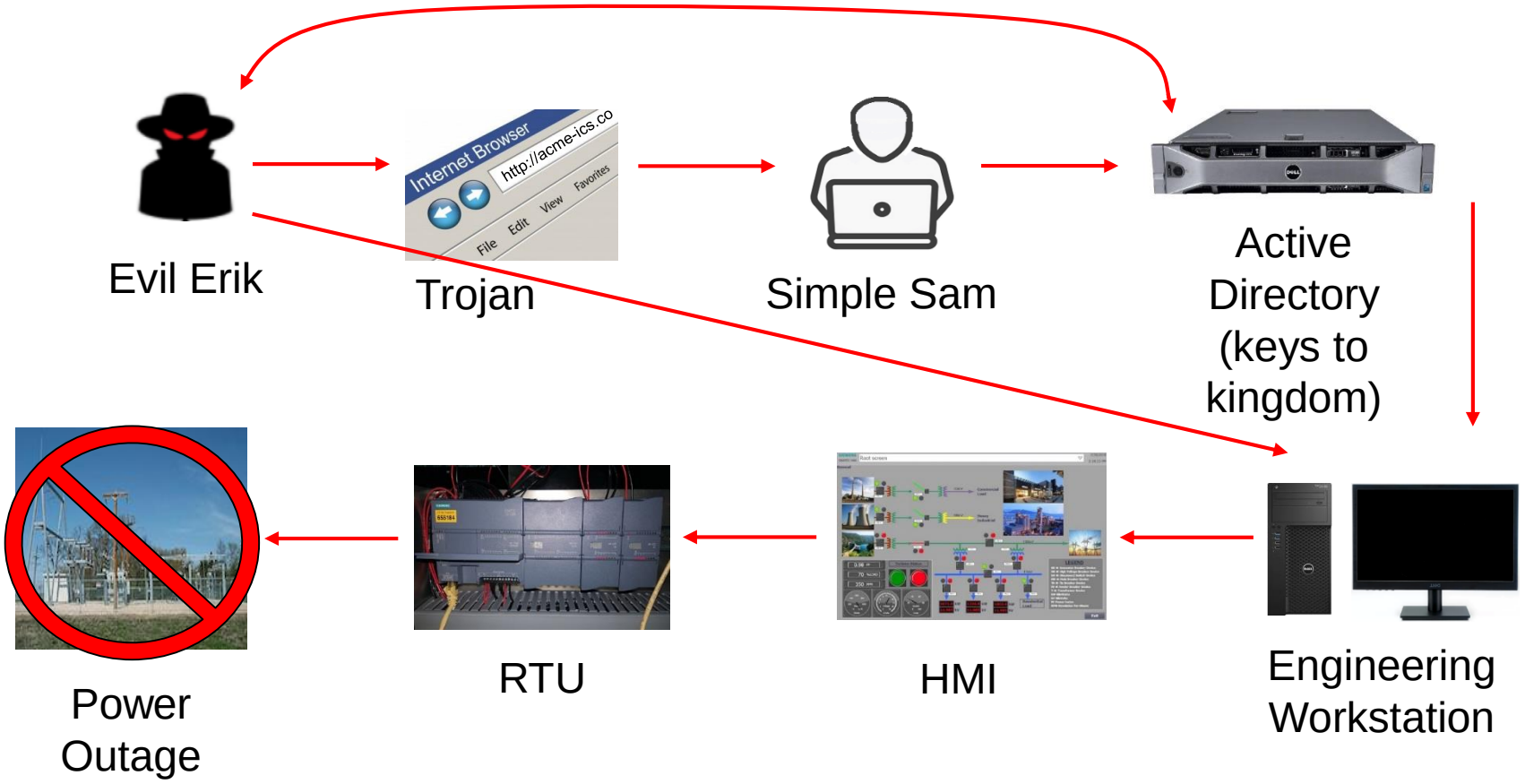
Havex



As a result of running Trojan-ized software, systems have been infected with a Remote Access Trojan (RAT).

Your ICS details are now being gathered by a Black Hat from anywhere in the world and operation continuity is at risk.

Havex Timeline



So what?

- Many different techniques to gain initial access to a victim network
- Often insufficient security in place at utilities due to need for remote access
- Similar threat landscape is seen across all sectors

Little Arc-Flash (LAF)

- All components of LAF are functional industrial control system equipment commonly seen in the field

- Attacker utilizes a common phishing strategy to gain initial access to the corporate environment

- Active Directory manipulated by the attacker to gain execution on engineer workstation

DEMO

Aftermath

- Recovery
  - Returning to a known good state can be exceedingly difficult after the fact
- Avoid becoming a victim
  - Auditing and proactive monitoring of infrastructure changes is vital to the ongoing process
- Plan for the day things go wrong
  - Proactive approaches are key, but all the planning in the world will not protect against a sufficiently motivated attacker
  - Know your ‘worst case’ scenario, and how you would respond to a compromise

NCCIC