CAPER

Center for Advanced Power Engineering Research

2017 Summer Research Planning Workshop

Detecting Cyber Attacks before the Attack

Presented By: Jeff Hahn

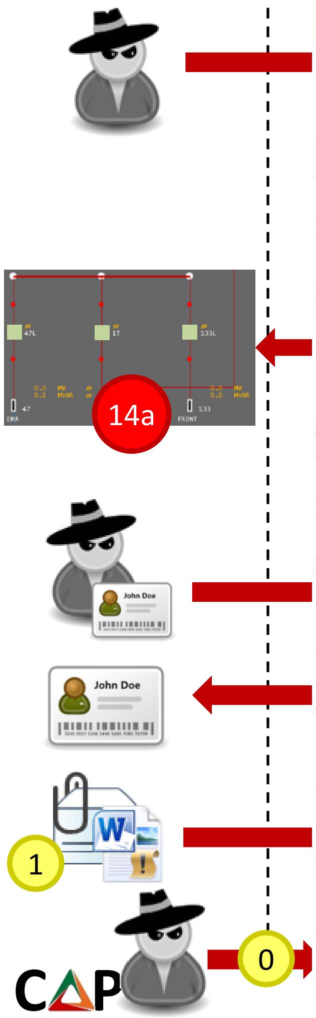
Let’s define a Cyber-Attack

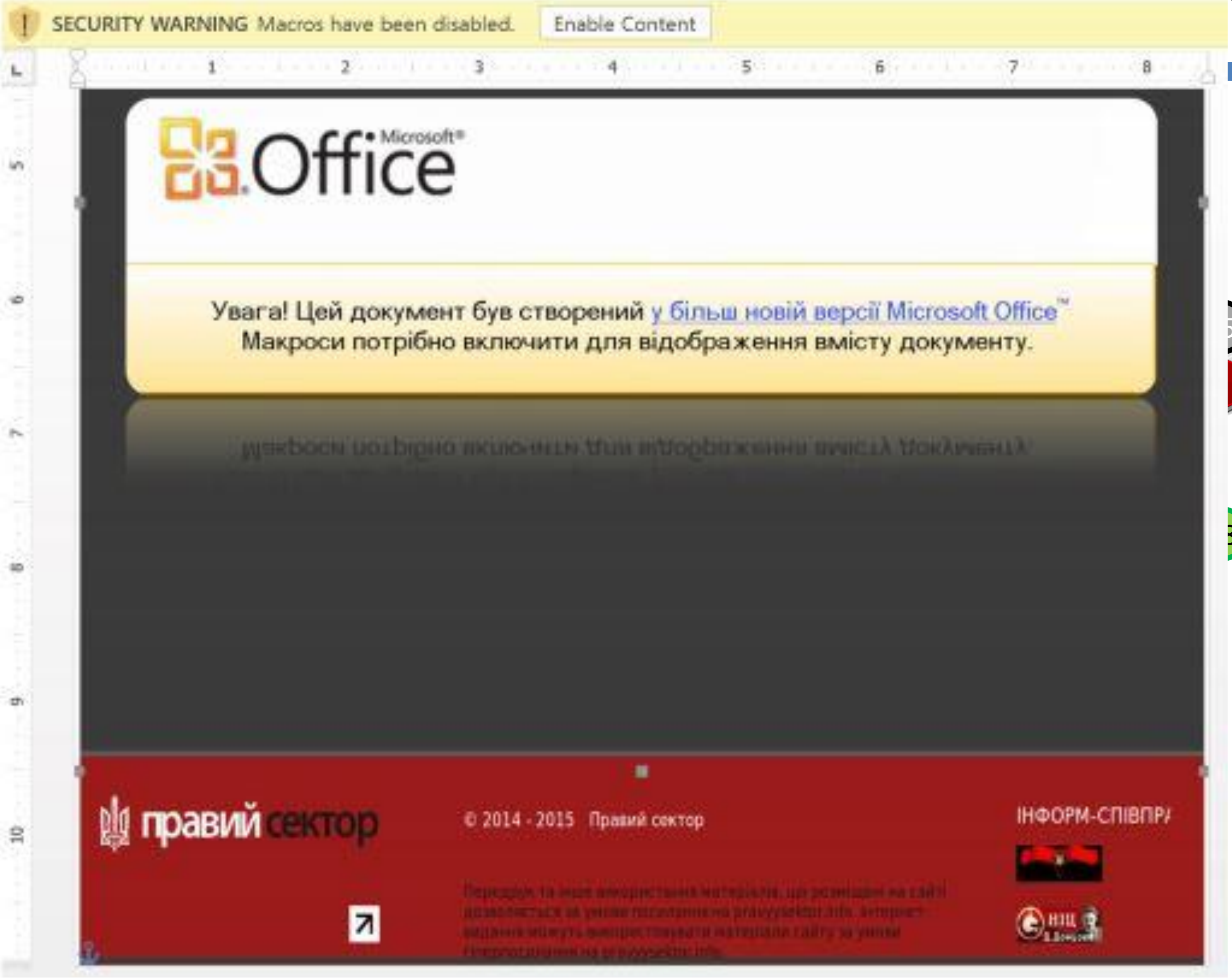
- Intrusion ≠ Cyber-Attack
  - Intrusion or exploitation of a computer precedes attack. The purpose is to gather information.
  - Cyber-Attack is the blow, the physical affect to modify, degrade or destroy.

Ukraine Power Outages - Summary

When	**December 2015,**	**December 2016**
What	Cyber-attack against Distribution Systems. Started with phishing campaign	Cyber-attack against Transmission System & other key infrastructure Started with a phishing campaign
Consequence	3 regional Oblenergos (utilities) 225,000 customers 1 – 6 hrs **Remote control lost for months	1 Utility in Kiev, Ukraine 230,000 customers 1 hr
Why	Speculation: “Someone, or various individuals, may be using the country as a testbed for refining attacks on critical infrastructure, attacks that could be used across the world.” Unsubstantiated – many believe it is due to geopolitics in the region	
How	See next slide ☺	CrashOverride

Attackers' Location | Public Internet | Business Network | Control System DMZ | Control System | Substation/Field | Consumer





SECURITY WARNING Macros have been disabled.

Увага! Цей документ був створений у більш новій версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документу.

Chart & animation created by Matt Yourek, Security Architect at GE Grid Solutions, Software Solutions

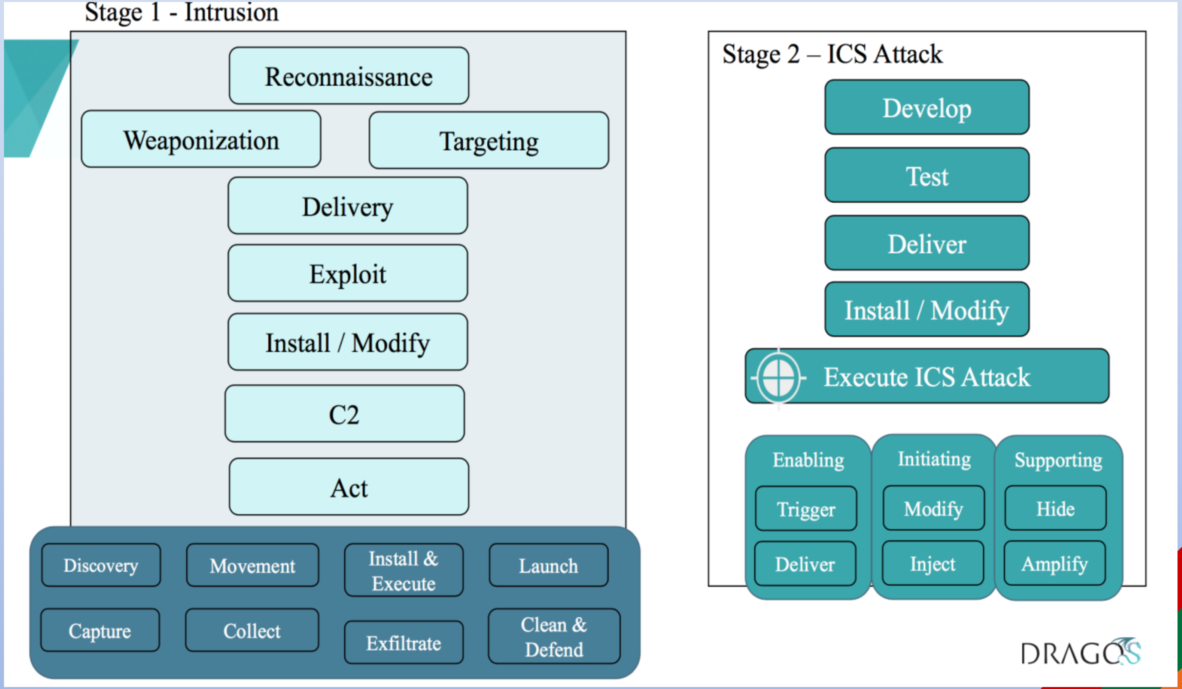
Lessons Learned from 2015 Ukraine Attack

Lessons:

- Initial intrusion occurred 8-9 months before Cyber Attack
- The purpose of Black Energy 3, was to gain and maintain access, and gather information.
- The Cyber-Attack used capabilities of the system against itself.
    - Allowed remote control of the DMS enabled the attackers to open breakers
    - KillDisk & malicious firmware uploads were allowed by the products and system. This delayed remote control restoration and created economic and resource issues.
- Look for abnormal network traffic during the attackers investigation stage

2016 Ukraine Attack - CrashOverride

- CrashOverRide is the 2nd half of a targeted cyber-attack
  - Stage 1: Intrusion
  - Stage 2: ICS Attack



CAPER

CrashOverride

This Malware was designed to:

- Understand and codify the knowledge of the industrial process to disrupt operations
- Scans with OPC protocol to help it map the environment and select its targets
- Target the libraries and configuration files of HMIs to understand the environment further and leverage HMIs to connect to Internet-connected locations when possible (Smi
  - Uses ICS protocols (IEC 101, IEC 104, IEC61850, OPC)
- Used understanding grid operations and leveraging the systems against themselves
  - Issues valid commands directly to RTUs (using ICS protocols)
- Includes Wiper to cover tracks and delay recovery

Appears to be targeting Europe/Asia; But could be modified to US systems

Defending against CrashOverride

- NOT effective:
  - Air gapped networks
  - Unidirectional firewalls
  - Anti-virus
  - Passive defenses
  - Architectural changes
- Effective:
  - Anomaly detection
  - Whitelisting
  - Recovery plans (including manual operation)

How to find CrashOverride type attacks?

- Disrupt the ‘Kill chain’
  - Find the attacker during the reconnaissance phase
- Step #1: Product/Network Protection
  - Properly configured firewall
  - Anti-Virus / Whitelisting app
  - User/Patch Management
  - Segmentation Architecture
  - Etc.
- Step #2: Network anomaly detection
  - SCADA systems are predictable and repeatable
  - Learn the difference between good network traffic and bad (non-normal) network traffic
  - Correlate events

Anomaly Intrusion Detection Systems

- There are many COTS IDS & SIEM systems:
  - Which ones work?
  - Which ones are easy to use?
  - Which ones are effective?
- Need a ‘consumer reports’ type review
  - Validation of feature claims vs reality
  - Industrial experience (customer review)
  - Etc.

Thanks !

CAPER