sentryo

Cyber Security for the **Industrial Internet**

Detection of Cyberattacks in Critical Infrastructures

Sentryo HQ | 66 Bd Niels Bohr CS 52132 69603 Lyon-Villeurbanne - France
+33 970 469 694 | contact@sentryo.net | www.sentryo.net

Company Overview

- **Incorporated:** June 2014
- **Headquarters:** Lyon - France
- **Venture capital** backed by UK/FR funds
- Target **Industrial corporations:** Energy, Process Industries, Manufacturing, Transportation
- Offices: **France/Germany**
- Partners: **USA, LATAM, South Asia, Middle East**

Awards

BMW TechDate **Winner** - June 2016

CISCO Acceleration **Prize** - June 2016

Lauréat Concours Mondial de l'Innovation CMI - June 2016

Winner Innovation Prize Monaco Cybersecurity Show October 2015

IIOT Cybersecurity startup of the year McRock Capital Symposium - May 2017

OT SECURITY IS NOT IT SECURITY BUT...

IT risks are sources of **fraud**, **privacy & data** leaks, **financial** losses

OT & IIoT risks are sources of **health**, **safety** and **environmental** casualties.

SENTRYO THREAT INTELLIGENCE

THREAT INTELLIGENCE REPORT published by the Sentryo Security Labs in September 2017
Preface by Vytautas Butrimas, Energy Cybersecurity Expert at NATO Energy Security Center of Excellence

Available for download on: sentryo.net

&

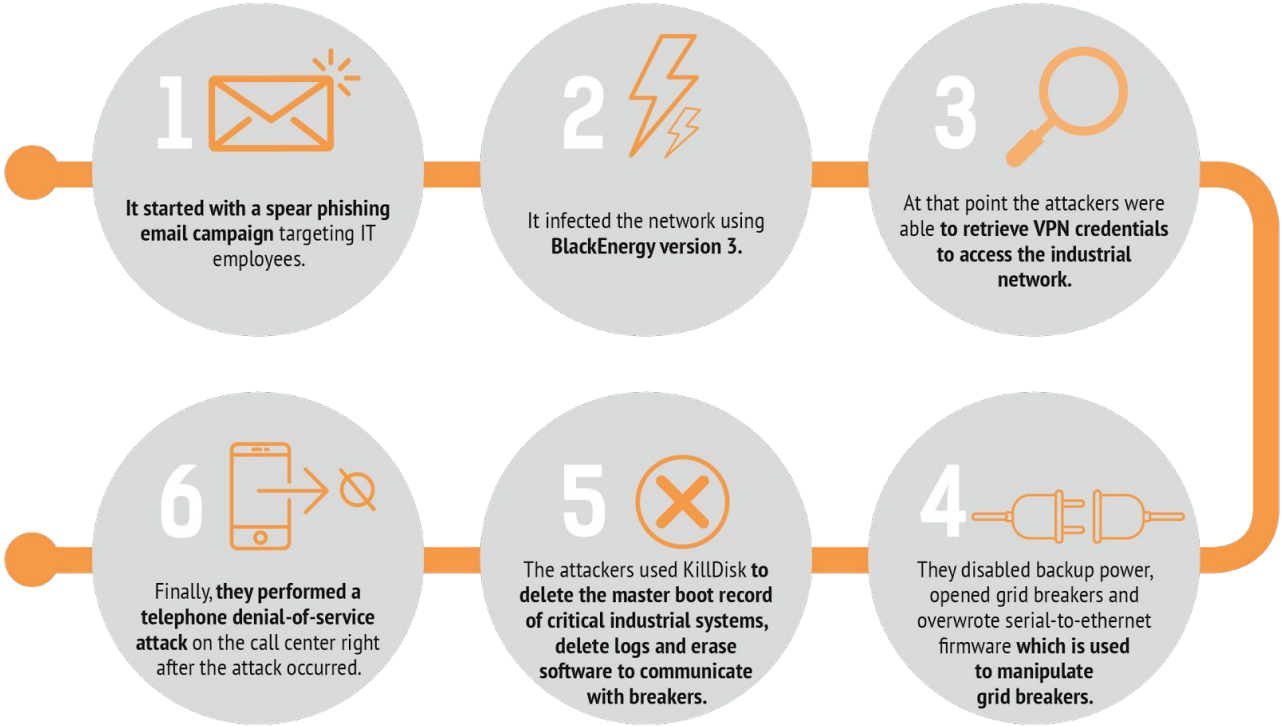
ANALYSIS using IEC 62443 published in the ISA March-April 2017 InTech magazine (International Society of Automation)

Available for download on: isa-france.org

2015 INCIDENT:

- **Simultaneous cyberattacks on three electricity distribution centers supplying electricity to all of western Ukraine:**
  - Several hours of power outages
  - From 80.000 to 1.4 million customers impacted
- **Hacking techniques to support and amplify the cyberattack:**
  - Stop or slow down operations during the power restore processes
- **Denial-of-service attack on the call center:**
  - Impossibility to call power operators

2015 INCIDENT: POTENTIAL SCENARIO

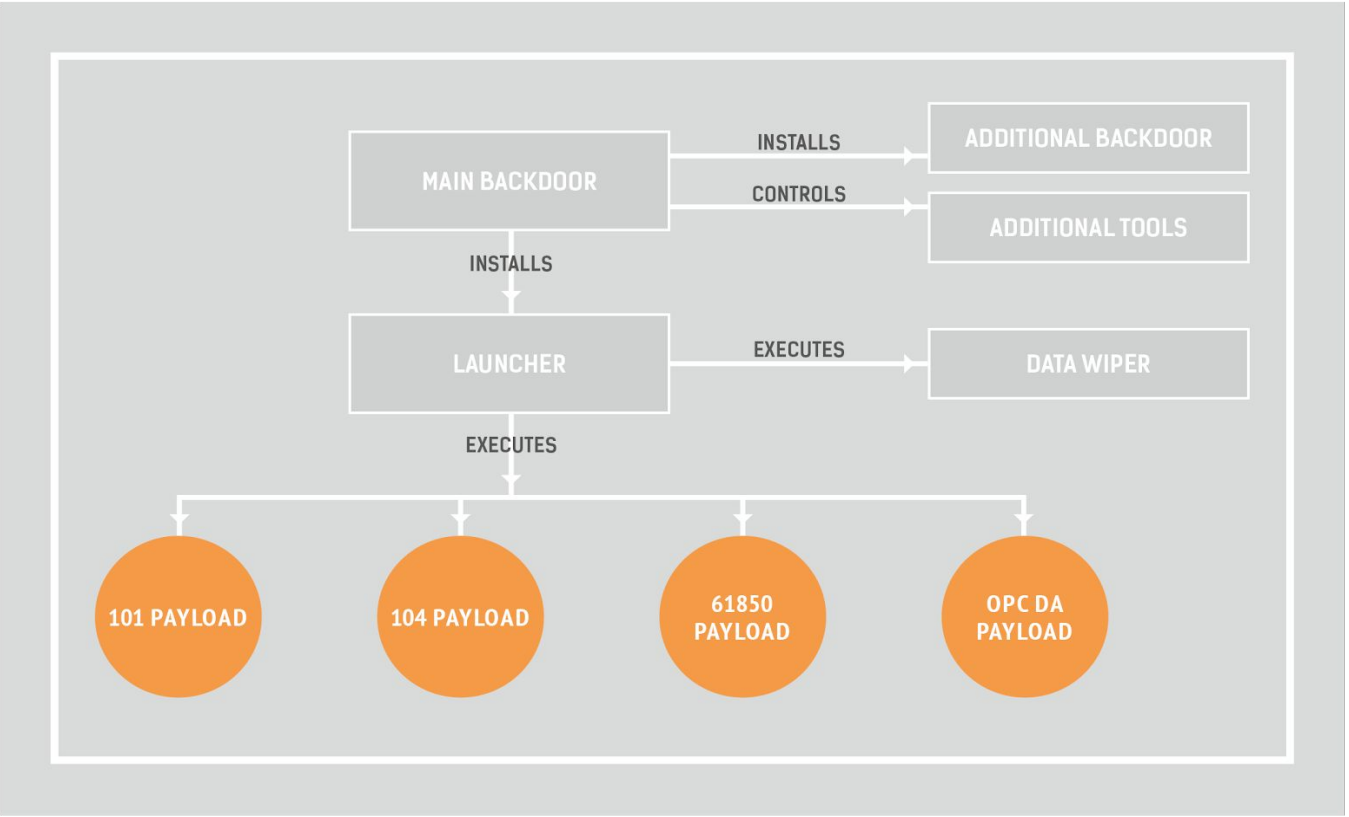


2016 INCIDENT:

- **Second cyberattack on another ukrainian grid company:**
  - Multiple blackouts in the Ukrainian capital Kiev
  - A complete power loss for the northern part of Kiev and the surrounding region

- **Less than 1 hour of power outages:**
  - Experts of the grid company were on site 30 minutes after the outage and fixed the situation with a manual procedure.

2017: AN UPGRADE OF MALWARE



2017: AN UPGRADE OF MALWARE

INDUSTROYER / CRASHOVERRIDE

=> The first OT malware designed specifically to attack electric grids.

This malware supports **4 different industrial protocols**	This malware embedded **4 different components**
• IEC 60870-5-101 (aka IEC 101) • IEC 60870-5-104 (aka IEC 104) • IEC 61850 • OLE for Process Control Data Access (OPC DA)	• Two backdoors (C&C through HTTPS) • A launcher • A wiper • Four differents payloads corresponding to four different industrial protocols

THE KILL CHAIN AND THE MALWARE IMPACT

Phase 1 PREPARATION	1. **Reconnaissance** => harvesting for email; industrial protocol used and target proxy configuration 2. **Weaponization** => development of the malware including the dropper, industrial payloads, the backdoor the wiper and the C&C server
Phase 2 INTRUSION	3. **Delivery** => probably an email with a link or an attachment to the dropper 4. **Exploitation** => find and exploit a vulnerability on the victim's computer to be able to install the malware 5. **Installation** => install the malware as a non-critical Windows service program and install a new malicious Microsoft Notepad program
Phase 3 ACTIVE BREACH	6. **Command & Control** (C&C OR C2) => communicate regularly with the C&C 7. **Actions & Objectives** => scan the network using embedded payloads and configuration files ; detect any breaker; turn it off and use the wiper.

SENTRYO ICS CYBERVISION

ICS CyberVision

is a network monitoring and threat intelligence platform that provides cyber-resilience for Industrial Control Systems (ICS) and SCADA networks

ICS CYBERVISION DETECTION

Environment	Communications	Process
Instant & Automatic visibility of all industrial components, logical connections and weaknesses	Track all type of communications and commands exchanged between all components	Monitor all the components, behaviors, processes and configurations

Raise alarm when first malicious actions are detected

ICS CYBERVISION DETECTION

Environment	Communications	Process
Mapping of components and monitor all new equipments added to this map	DPI engine dedicated to ICS protocols Tracks all changes in type of communications (control, admin…)	Machine and deep learning algorithms to detect any changes or anomaly in industrial process

Sentryo developed technologies

ICS CYBERVISION IN THE ENERGY SECTOR

ICS CyberVision detects weak signals enabling the local team to stop the attacks

- Detection of **unknown connections** to a remote Internet website
- Detection of any **new connections** to a remote Internet website and also **new and strange behaviours** on the OT networks
- Detection of the **disappearance of TCP connections** between SCADA stations and PLCs/ RTUs
- **Analyse of IEC 101 flows** and **detection of orders** to open up the breaker and to switch off power and trace down the hackers to particular infected machines
- Identification of **potentially affected devices** in the network.

Thank you