

RESPONDING TO RANSOMWARE IN INDUSTRIAL CONTROL SYSTEM ENVIRONMENTS

SETH ENOKA
PRINCIPAL INDUSTRIAL INCIDENT
RESPONSE CONSULTANT, DRAGOS

INTENTIONAL VS UNINTENTIONAL

WHAT'S THE DIFFERENCE?

Intentional ransomware:

- + Demonstrates ICS-specific capabilities
- + e.g. ICS ports and protocols
- + Capable of impacting production

Unintentional ransomware:

- + Lands in OT, doesn't care about OT
- + 8/10 OT infections come from IT



A BRIEF HISTORY OF RANSOMWARE AFFECTING ICS

WHEN

JUNE 2017

RANSOMWARE USED

NOTPETYA

ESTIMATED COST OF ATTACK

\$300 – 400 MILLION

NotPetya Ransomware Attack Cost Shipping Giant Maersk

Over **Shipping company Maersk says June cyberattack could cost it up to \$300**

Lee Mathews
Observing, poi

million

PUBLISHED WED, AUG 16 20



Jordan Novet
@JORDANNOVET

Shipping Company Maersk Says NotPetya Cyberattack Could Cost Up to \$300M



EDITORIAL STAFF

AUG 16, 2017 |

LATEST SECURITY NEWS

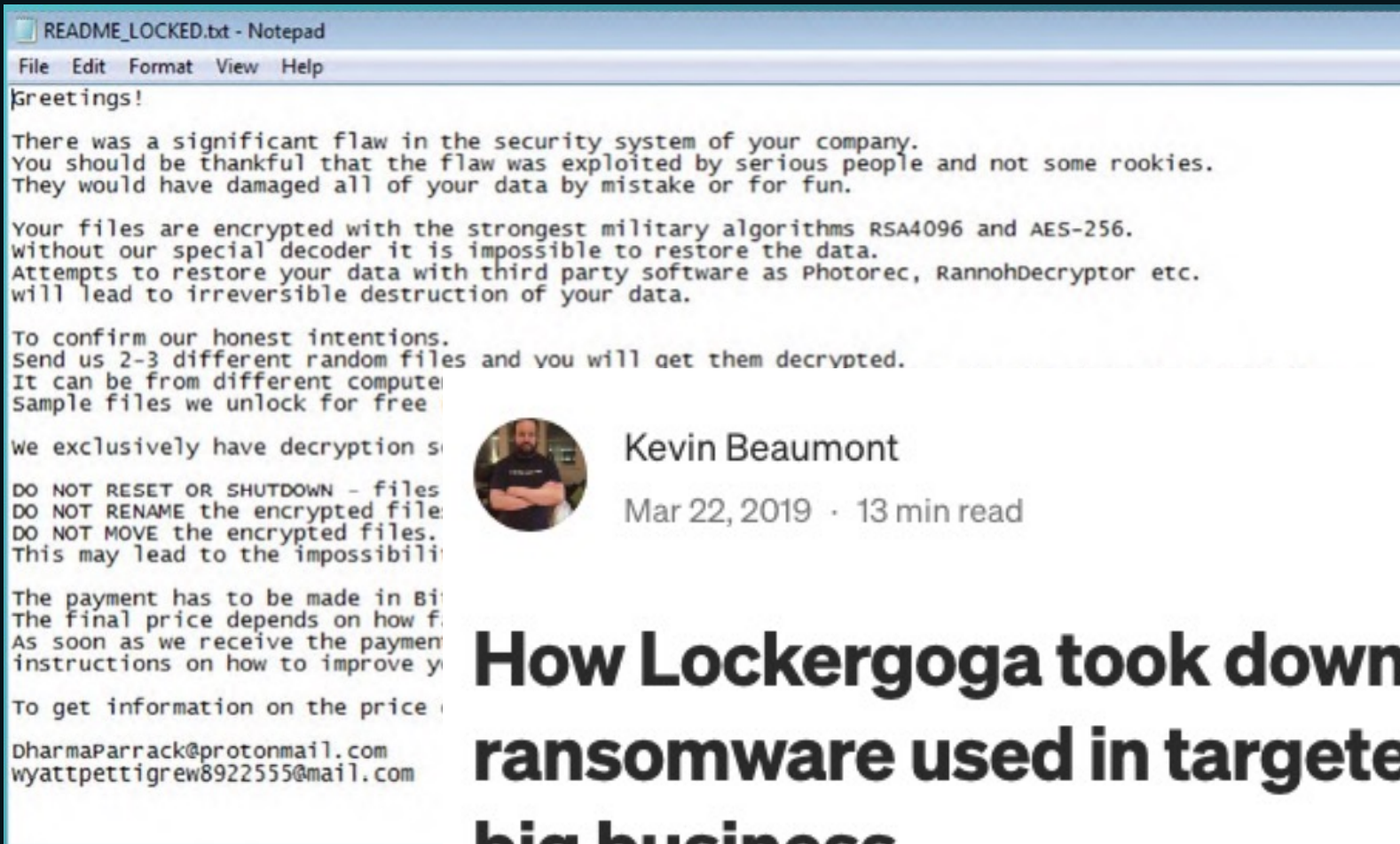
NORSK HYDRO


Hydro

WHEN
MARCH 2019

RANSOMWARE USED
LOCKERGOGA

ESTIMATED COST OF ATTACK
550 – 560 MILLION kr



README_LOCKED.txt - Notepad
File Edit Format View Help

Greetings!

There was a significant flaw in the security system of your company. You should be thankful that the flaw was exploited by serious people and not some rookies. They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256. without our special decoder it is impossible to restore the data. Attempts to restore your data with third party software as Photorec, RannohDecryptor etc. will lead to irreversible destruction of your data.

To confirm our honest intentions. Send us 2-3 different random files and you will get them decrypted. It can be from different computer. Sample files we unlock for free

we exclusively have decryption software

DO NOT RESET OR SHUTDOWN - files
DO NOT RENAME the encrypted files
DO NOT MOVE the encrypted files.
This may lead to the impossibility

The payment has to be made in Bitcoin
The final price depends on how many files
As soon as we receive the payment we will send you instructions on how to improve your system

To get information on the price of the decryption software contact us at

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com



Kevin Beaumont

Mar 22, 2019 · 13 min read



How Lockergoga took down Hydro — ransomware used in targeted attacks aimed at big business

EKANS

WHEN

JANUARY 2020

VICTIMS

FRESENIUS GROUP, HONDA,
ENEL GROUP

IMPACT

INDUSTRIAL ENVIRONMENTS

137313 **5** EKANS ransomware binary identified via signature. MARK AS READ

DETECTION INFORMATION

WHAT HAPPENED:
EKANS ransomware binary identified via signature.

OCCURRED AT: 05/10/22, 05:37 UTC **LAST SEEN:** 05/10/22, 05:37 UTC

COUNT: 1 **STATE:** UNRESOLVED

DETECTED BY: EKANS Ransomware Binary **SOURCE:** 9ae59ea0-d0bd-11ec-acc0-0a56ec842977

DETECTION QUAD: Indicator **ZONES:** IDMZ, Control Center

ACTIVITY GROUP: N/A **ICS CYBER KILLCHAIN STEP:** Stage 1 - Act on Objectives, Stage 2 - Execute ICS Attack, ...

MITRE ATT&CK FOR ICS TACTIC
[Impair Process Control](#)

MITRE ATT&CK FOR ICS TECHNIQUE
[T0881: Service Stop](#)

MITRE ATT&CK FOR ICS TACTIC
[Impact](#)

MITRE ATT&CK FOR ICS TECHNIQUE
[T0813: Denial Of Control](#)

MITRE ATT&CK FOR ICS TACTIC
[Impact](#)

MITRE ATT&CK FOR ICS TECHNIQUE
[T0815: Denial Of View](#)

MITRE ATT&CK FOR ICS TACTIC
[Impact](#)

MITRE ATT&CK FOR ICS TECHNIQUE
[T0829: Loss Of View](#)

QUERY-FOCUSED DATASETS: No Applicable Query-Focused Datasets

NOTIFICATION RECORD: No Associated Record

PLAYBOOKS: No Associated Playbooks

NOTIFICATION COMPONENTS: [View in Kibana](#)

ASSOCIATED ASSETS

View	Type	ID	Name	D...
VIEW	Asset	17	Asset 17 10.10.100.51	src
VIEW	Asset	78	Asset 78 172.18.0.4	dst

COMMUNICATIONS SUMMARY

Asset 10.10.100.51 (00:0c:29:e7:f3:30, IDMZ-INTERMEDIATE1, localhost) connected to Asset localhost 172.18.0.4 (00:0c:29:f5:b0:23, CC-EWKS1) via HTTP.

Detecte...	Protocol	Source A...	Source P...	Destinati...	D...
05/10/22, 0...	HTTP	10.10.100.51	50017	172.18.0.4	80

[PREV](#) [CLOSE](#) [CREATE A RULE](#) [CREATE CASE](#) [NEXT](#)



PRODUCTS & SERVICES

EKANS Ransomware and ICS Operations

Feb 3, 2020 | Blog, Industry News



COLONIAL PIPELINE



COLONIAL PIPELINE CO.

WHEN

MAY 2021

RANSOMWARE USED

DARKSIDE

ESTIMATED COST OF ATTACK

\$5 MILLION

ZDNet



MENU



US

Colonial Pipeline attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.



By Charlie Osborne for Zer

The real-world consequences highlighted this week with due to ransomware.

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

By William Turton and Kartikay Mehrotra

5 June 2021 at 03:58 GMT+8

JBS FOODS

JBS FOODS®

WHEN
MAY 2021

RANSOMWARE USED
REVIL

ESTIMATED COST OF ATTACK
\$11 MILLION

CNN BUSINESS

LIVE TV @ ☰

What the JBS cyberattack means for meat supply

By [Danielle Wiener-Bronner](#) and [Angus Watson](#), [CNN](#)

[Business](#)

Updated 9:59 PM ET, Wed June 2, 2021

NOW PLAYING

WH: Cyberattack on JBS likely from Russia

CNNBusiness



ABC RURAL

JBS Foods pays \$14.2 million ransom to end cyber attack on its global operations

ABC Rural / By [David Claughton](#) and [Nikolai Beilharz](#)

Posted Thu 10 Jun 2021 at 8:58am, updated Thu 10 Jun 2021 at 11:04am

HUMAN-OPERATED RANSOMWARE

CRIMINAL ECOSYSTEMS & COMMON ATTACK VECTORS

- + Initial access vendors
- + Ransomware authors & tool creators
- + Ransomware 'affiliates'
- + Act like APTs, but less advanced, more determined

- + Use RDP
- + Abuse Domain trust between IT and OT
- + Acquire access from darkweb sources





PREPARE & DETECT

PREPARE & DETECT

PEOPLE



TRAIN YOUR SMES

both in corporate and OT



DESIGNATE

incident commanders and site champions



ENGINEERING TROUBLE TICKETS

get security personnel involved in them



BUILD RELATIONSHIPS

with your vendors and other third parties



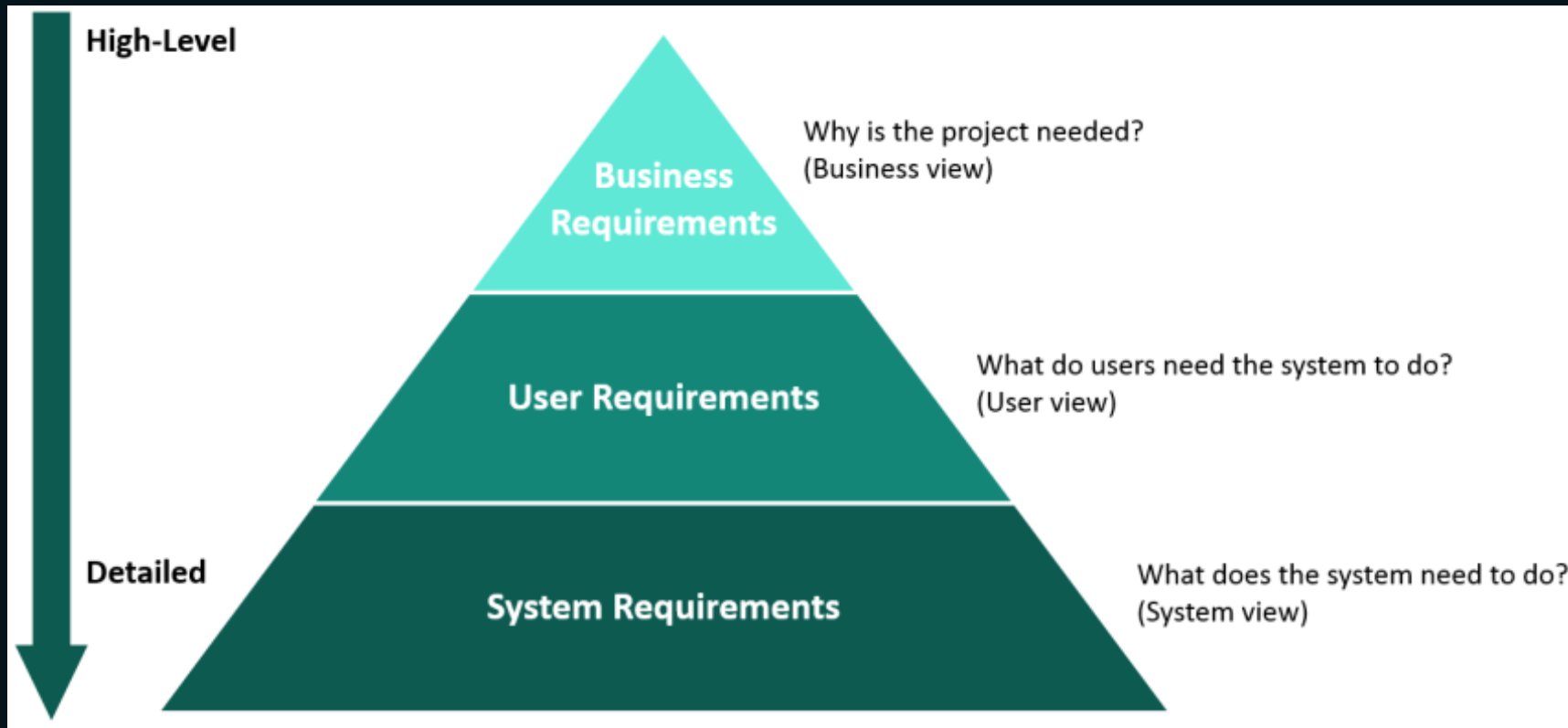
INCLUDE ALL RELEVANT STAKEHOLDERS

in your incident response planning

PREPARE & DETECT

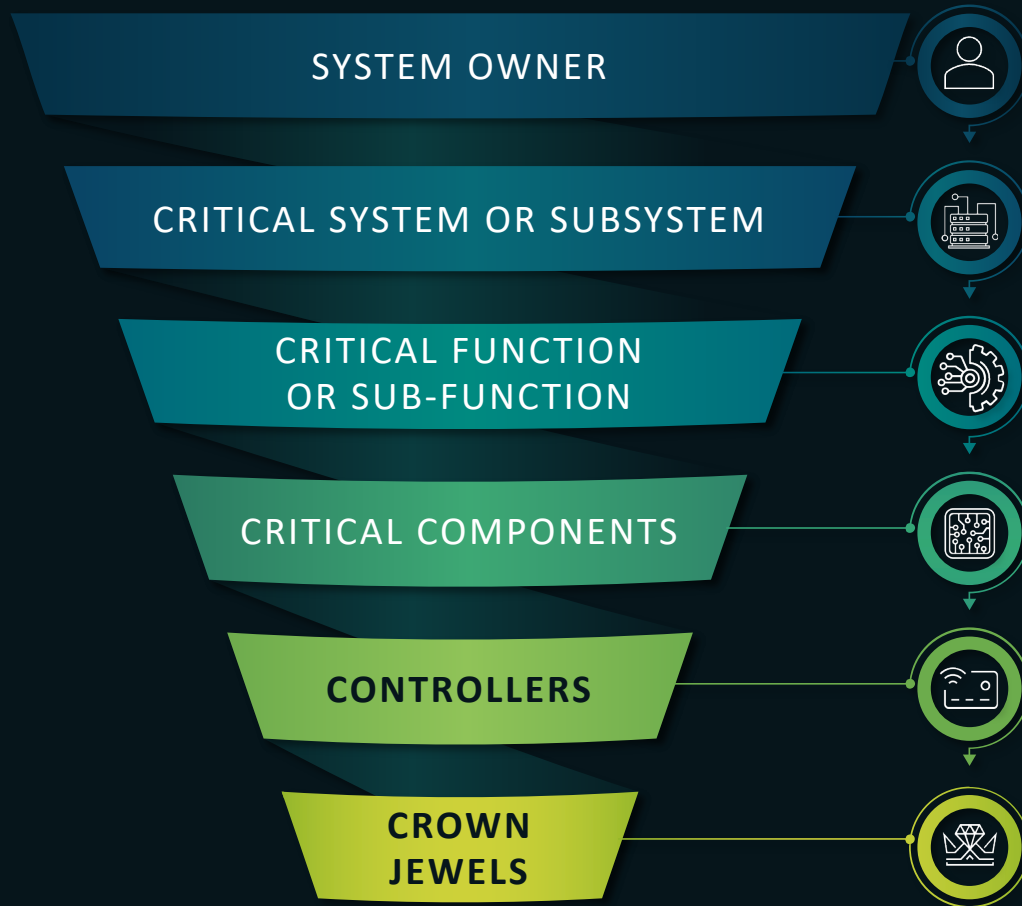
PROCESS

- + Gather security requirements and perform due diligence early



PREPARE & DETECT

PROCESS: CROWN JEWELS ANALYSIS



WHAT:

- “**Crown Jewels Analysis**” is the process of identifying an (ICS) environment’s most critical assets

WHY:

- We, as defenders, have limited resources
- CJA enables us to prioritise where to focus defenses and response activities
- Support cybersecurity exercises and data collection for incident response, threat hunting, and other activities

PREPARE & DETECT

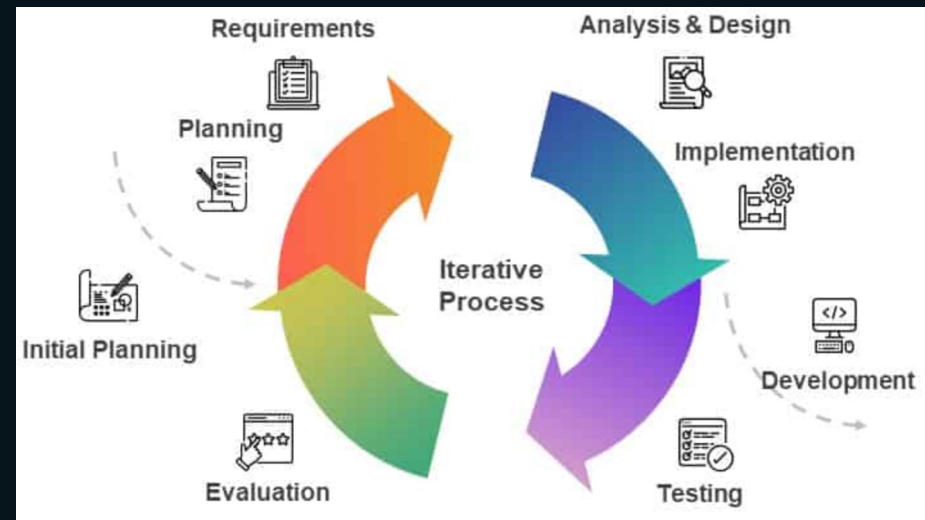
PROCESS: COLLECTION MANAGEMENT FRAMEWORK

Site	Segment / Level	Asset	Data Type	Kill Chain Phases	Data Storage Location	Data Retention	Follow-On Collection
All	DMZ	VPN Concentrator	Access Logs	Reconnaissance, Command and Control, Delivery	Enterprise SIEM	2 Years	Local Firewall Logs
	DMZ	Firewall	Firewall Logs	Reconnaissance, Command and Control, Delivery	Enterprise SIEM	180 Days	Firewall Ruleset
	DMZ	Jump Host	Windows Event Logs	Reconnaissance, Command and Control, Delivery	Enterprise Log Server	1 Year	Registry
Alpha Facility	Supervisory Network Alpha	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	OT Log Server	60 Days	Historian Logs, Registry
	Supervisory Network Alpha	Dragos Platform	Notifications	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Dragos Platform	1 Year	Known Good Baseline Comparison
	Supervisory Network Alpha	EWS	Windows Event Logs		Local Host	30 Days	Registry, Memory, MFT
	Control Network Alpha	RTUs	Syslog	Installation, Actions, on Objectives	OT Log Server	90 Days	Controller Logic
	Control Network Alpha	HMIs	Windows Event Logs	Installation, Actions, on Objectives	Local Host	15 Days	Registry, Memory, MFT
Bravo Facility	Supervisory Network Bravo	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	OT Log Server	60 Days	Historian Logs, Registry
	Supervisory Network Bravo	EWS	Windows Event Logs	Exploitation, Installation, Actions on Objectives	Local Host	4 Years	Registry, Memory, MFT
	Supervisory Network Bravo	Snort IDS	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	OT Log Server	90 Days	Ruleset
	Control Network Bravo	RTUs	Security Events	Installation, Actions, on Objectives	Dragos Platform	1 Year	Controller Logic
	Control Network Bravo	HMIs	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	Local Host	7 Days	Registry, Memory, MFT
	Control Network Bravo	Snort IDS	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	OT Log Server	90 Days	Ruleset
Charlie Facility	Supervisory Network Charlie	Historian	Windows Event Logs	Exploitation, Installation, Actions on Objectives	Local Host	15 Days	Historian Logs, Registry
	Supervisory Network Charlie	EWS	Windows Event Logs	Installation, Actions, on Objectives	Local Host	10 Years	Registry, Memory, MFT
	Supervisory Network Charlie	Snort IDS	Alerts	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	OT Log Server	90 Days	Ruleset
	Control Network Charle	PLCs	Internal Logging	Installation, Actions, on Objectives	Local Host	7 Days	Controller Logic
	Control Network Charle	HMIs	Windows Event Logs	Installation, Exploitation, Actions, on Objectives	Local Host	7 Days	Registry, Memory, MFT

PREPARE & DETECT

PROCESS

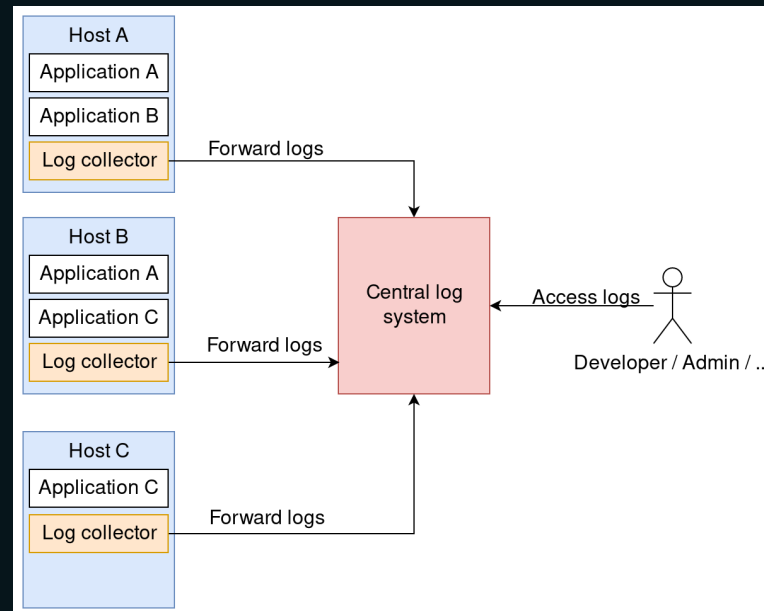
- + Backups, backups, backups
- + Comprehensive IRP documents **specific to OT**
- + Exercise your IRP with TTXs, and iterate



PREPARE & DETECT

TECHNOLOGY

- + High-fidelity sensors
- + Capable of capturing, collating, alerting and notifying, enable IR
- + Centralise and aggregate endpoint logs and network traffic



FIVE CRITICAL CONTROLS

FOR WORLD-CLASS OT CYBERSECURITY



DEFENSIBLE ARCHITECTURE



MONITORING AND DETECTION



REMOTE ACCESS AUTHENTICATION



KEY VULN MANAGEMENT



ICS INCIDENT RESPONSE PLAN

PREPARE & DETECT

TECHNOLOGY

- + Utilise public available data to augment internal collections



PREPARE & DETECT

TECHNOLOGY

First Name	Surname	Name	E-Mail	Telephone		
J				Electric.com	01	
A				er-electric.com	07	
D				der-Electric.com	01	
M				ctric.com	07	
S				neider-Electric.com	01	
J				-electric.com	01	
H				ctric.com	07	
P				er-Electric.com	01	
S				lectric.com	07	
K				Electric.com	07	
C				ctric.com	07	
O				neider-electric.com	07	
D				Electric.com	01	
N				-electric.com	07	
M				r-electric.com	01	
C				ectric.com	01	
N				ic.com	07	
A				neider-Electric.com	01	
D				er-Electric.com	01	
M				er-Electric.com	01	
B				er-Electric.com	01	
C				der-Electric.com	01	
E				Electric.com	01	
J				lectric.com	01	
D				er-Electric.com	01	
V				-electric.com	07	
B				schneider-electric.com	07	
A				neider-Electric.com	01	
T				Electric.com	01	
G				-Electric.com	07	
R				er-Electric.com	01	
I				r-Electric.com	07	
D				neider-Electric.com	01	

PREPARE & DETECT

TECHNOLOGY

- + Monitor and investigate non-standard connections
- + Implement application control
- + Patch applications and OSs, but consider the relative risk
- + Implement user application hardening
- + Restrict and tightly control and monitor elevated privileges
- + Implement MFA on all remote access methods





RESPONSE STRATEGY

RESPONSE STRATEGY

CONTAIN

- + To pay or not to pay...
 - + Be aware of known ransomware decryptors
 - + Consider restoring from backup, at least for mission critical data
 - + Exercise your backup procedures *before* an incident occurs
 - + Gain familiarity with living off the land techniques
 - + Understand lateral movement
 - + Know when elevated privileges are used and why
-

RESPONSE STRATEGY

ERADICATE & RECOVER

- + When escalating an event to an incident
 - + Priority 1: safety, of humans, then facility
 - + Priority 2: availability and reliability of operations
 - + Follow your IRP
 - + Scope affected assets
 - + Collect relevant evidence
 - + Analyse collected evidence, adjust response as necessary
 - + Remove the adversary and prevent re-infection
-

RESPONSE STRATEGY

POST-INCIDENT

- + Lessons learned/after action
 - + Short- and long-term goals and remediation
 - + Iterate and improve procedures
-

RECOMMENDATIONS

KEY TAKEAWAYS

- + Malware has increased in the last 5 years, will continue to do so
- + OT \neq IT: develop OT-specific IR documentation and processes
- + Defensible architecture and monitoring at 2+ kill chain phases
- + Develop and exercise rapid IR plans for common scenarios
- + Implement and validate a robust backup strategy
- + MFA all the things



ADDITIONAL RESOURCES

- [HTTPS://HUB.DRAGOS.COM/HUBFS/WHITEPAPERS/RANSOMWAR
E%20IN%20ICS%20ENVIRONMENTS%20-
%20DRAGOS%202020.PDF?UTM_REFERRER=HTTPS%3A%2F%2FW
WW.DRAGOS.COM%2F](https://hub.dragos.com/hubfs/whitepapers/ransomware%20in%20ics%20environments%20-%20dragos%202020.pdf?utm_referrer=https%3a%2f%2fwww.dragos.com%2f)
 - [HTTPS://WWW.YOUTUBE.COM/WATCH?V=W7C6DFRXYAQ](https://www.youtube.com/watch?v=W7C6DFRXYAQ)
 - [HTTPS://WWW.DRAGOS.COM/BLOG/DRAGOS-2021-INDUSTRIAL-
CYBERSECURITY-YEAR-IN-REVIEW-SUMMARY/](https://www.dragos.com/blog/dragos-2021-industrial-cybersecurity-year-in-review-summary/)
 - [HTTPS://WWW.YOUTUBE.COM/C/DRAGOSINC/ICS/CYBERSECURITY
/SEARCH?QUERY=RANSOMWARE](https://www.youtube.com/c/dragosinc/ics/cybersecurity/search?query=ransomware)
 - [HTTPS://WWW.CONTROLENG.COM/ARTICLES/HOW-TO-PROTECT-
OT-ICS-SYSTEMS-FROM-RANSOMWARE-ATTACKS/](https://www.controleng.com/articles/how-to-protect-ot-ics-systems-from-ransomware-attacks/)
-

ADDITIONAL RESOURCES

- [HTTPS://WWW.CYBERTALK.ORG/2021/06/15/RANSOMWARE-ATTACKS-ON-INDUSTRIAL-CONTROL-SYSTEMS-2021/](https://www.cybertalk.org/2021/06/15/ransomware-attacks-on-industrial-control-systems-2021/)
 - [HTTPS://WWW.ZDNET.COM/ARTICLE/RANSOMWARE-GANGS-ARE-TAKING-AIM-AT-SOFT-TARGET-INDUSTRIAL-CONTROL-SYSTEMS/](https://www.zdnet.com/article/ransomware-gangs-are-taking-aim-at-soft-target-industrial-control-systems/)
 - [HTTPS://WWW.SECURITYWEEK.COM/KASPERSKY-SEES-RISE-RANSOMWARE-ATTACKS-ICS-DEVICES-DEVELOPED-COUNTRIES](https://www.securityweek.com/kaspersky-sees-rise-ransomware-attacks-ics-devices-developed-countries)
 - [HTTPS://WWW.FIREEYE.COM/CONTENT/DAM/FIREEYE-WWW/PRODUCTS/PDFS/WP-TOP-20-CYBERATTACKS.PDF](https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf)
 - [HTTPS://WWW.BLACKHILLSINFOSEC.COM/WEBCAST-INTRO-TO-RANSOMWARE-AND-INDUSTRIAL-CONTROL-SYSTEMS-ICS/](https://www.blackhillsinfosec.com/webcast-intro-to-ransomware-and-industrial-control-systems-ics/)
-

ADDITIONAL RESOURCES

- [HTTPS://WWW.DRAGOS.COM/BLOG/INDUSTRY-NEWS/PROJECT-MIMICS-STAGE-ONE/](https://www.dragos.com/blog/industry-news/project-mimics-stage-one/)
 - [HTTPS://WWW.SANS.ORG/PRESENTATIONS/E-MIMICS---EXTENDED-MALWARE-IN-MODERN-ICS/](https://www.sans.org/presentations/e-mimics---extended-malware-in-modern-ics/)
 - [HTTPS://WWW.SANS.ORG/WHITE-PAPERS/36297/?MSC=BLOG-ICS-LIBRARY](https://www.sans.org/white-papers/36297/?MSC=BLOG-ICS-LIBRARY)
 - [HTTPS://ARCHIVE.F-SECURE.COM/WEBLOG/ARCHIVES/00002718.HTML](https://archive.f-secure.com/weblog/archives/00002718.html)
 - [HTTPS://WWW.DRAGOS.COM/BLOG/INDUSTRY-NEWS/EKANS-RANSOMWARE-MISCONCEPTIONS-AND-MISUNDERSTANDINGS/](https://www.dragos.com/blog/industry-news/ekans-ransomware-misconceptions-and-misunderstandings/)
-

ADDITIONAL RESOURCES

- [HTTPS://PORTSWIGGER.NET/DAILY-SWIG/WHEN-THE-SCREENS-WENT-BLACK-HOW-NOTPETYA-TAUGHT-MAERSK-TO-RELY-ON-RESILIENCE-NOT-LUCK-TO-MITIGATE-FUTURE-CYBER-ATTACKS](https://portswigger.net/daily-swig/when-the-screens-went-black-how-notpetya-taught-maersk-to-rely-on-resilience-not-luck-to-mitigate-future-cyber-attacks)

The background is a dark, industrial scene, possibly a refinery or power plant, with various structures and pipes. A dark blue rectangular overlay is centered on the image, containing the text "THANK YOU" in a light green, sans-serif font. The text is enclosed within a thin white rectangular border.

THANK YOU

SENOKA@DRAGOS.COM