




Whitepaper

HOW TO PREPARE FOR & RESPOND TO RANSOMWARE IN OPERATIONAL TECHNOLOGY (OT) ENVIRONMENTS

August 2022

Seth Enoka

Principal Industrial Incident Responder
Global Services | Dragos, Inc.

 info@dragos.com


 [@DragosInc](https://twitter.com/DragosInc)

TABLE OF CONTENTS

Overview 1

Key Takeaways and Recommendations 2

A Brief History of Ransomware Affecting Industrial Control Systems (ICS) 3

 Maersk..... 3

 Norsk Hydro 3

 Colonial Pipeline..... 4

 JBS Foods..... 4

 EKANS..... 4

Preparation and Detection Strategy 5

 People..... 5

 Process..... 5

 Technology..... 6

Response Strategy..... 8

 Contain, Eradicate, and Recover 8


 Post-Incident..... 9


In Conclusion 9

References 10

KEY TAKEAWAYS AND RECOMMENDATIONS

- Malware and ransomware attacks against ICS environments have increased significantly in the last five years.
- OT mission, impact, and consequences are not the same as IT, and IT-focused plans cannot simply be reused in OT; incident response plans (IRPs) and playbooks must be ICS-specific, and must be tested, exercised, and validated to be effective.
- Defensible architecture, including network segmentation between IT and OT, is required to prevent cross-zone ransomware spread.
- ICS network monitoring can aid in threat detection across multiple phases of the ICS Cyber Kill Chain and provide detailed logs/forensic evidence that simplifies investigations.^{4,5}
- Rapid containment plans must be in place to protect core systems (i.e. minimal viable operations) in the event of an incident in adjacent networks. These plans should be exercised early to prevent impact to crown jewel assets. A clear understanding of impacts to auxiliary systems (such as Enterprise Resource Planning or other business reporting systems) must be pre-established and communications plans implemented to notify impacted stakeholders when containment plans are activated.
- Resilient, validated backup and restoration procedures and the use of gold images must be considered for mitigation and remediation of ransomware.
- Multi-factor authentication must be implemented for all methods of remote access into the OT environment.





OT security platform provides visibility into assets, network, vulnerabilities, and threats

Largest, most experienced team of industrial cybersecurity specialists

500+ employees, 300+ global customers, HQ in Hanover, MD, USA

A BRIEF HISTORY OF RANSOMWARE AFFECTING INDUSTRIAL CONTROL SYSTEMS (ICS)

Targeted intrusions for gaining long-term access and collecting data about industrial control systems (ICS) are becoming much more frequent. Many of these attacks are about understanding the network and preparing for future activities without causing any immediate impact. The most recent Dragos Year in Review⁶ report shows that the ransomware groups Lockbit 2.0 and Conti were responsible for more than half of the observed ransomware attacks in industrial environments in 2021, and that these instances resulted in actions on objectives. These attacks have been observed in almost every industrial vertical, primarily targeting small to medium-sized organizations in manufacturing.



MAERSK

WHEN

JUNE 2017

RANSOMWARE USED

NOTPETYA

ESTIMATED COST OF ATTACK

\$300 – 400 MILLION

MAERSK

In June 2017, Maersk, the global shipping conglomerate, suffered an attack utilising NotPetya, affecting 574 offices in 130 countries, that affected their entire Active Directory infrastructure.⁷ Luckily for Maersk, a lone Domain Controller was offline at the time of the attack, allowing them to restore operations. Although the outage lasted less than two weeks, the company lost an estimated 300 to 400 million dollars as a result of the attack.



Hydro

WHEN

MARCH 2019

RANSOMWARE USED

LOCKERGOGA

ESTIMATED COST OF ATTACK

550 – 560 MILLION kr

NORSK HYDRO

LockerGoga⁸ was used against Norsk Hydro, a 35,000 person aluminium and renewable energy company headquartered in Norway, in March 2019. The attack resulted in a significant operational impact on the company's aluminium production operations. Although Norsk was able to return to minimum viable operation soon after the attack, they lost between 550 and 560 million Norwegian kroner as a result of the incident.



COLONIAL PIPELINE CO.

WHEN

MAY 2021

RANSOMWARE USED

DARKSIDE

ESTIMATED COST OF ATTACK

\$5 MILLION

COLONIAL PIPELINE

Responsible for almost half of America’s oil pipeline, Colonial Pipeline⁹ suffered a Darkside ransomware incident in May of 2021. The incident primarily affected the billing infrastructure in the enterprise environment, although the OT network was shut down to prevent the infection from spreading and causing more significant consequences to operations. The company paid the ransom within hours of the attack being identified and investigated, but eventually restored their environment from backups due to the slow performance of the decryption tool, validating the need for effective backup and restore procedures.

JBS FOODS®

WHEN

MAY 2021

RANSOMWARE USED

REvil

ESTIMATED COST OF ATTACK

\$11 MILLION

JBS FOOD

Another global organisation with more than 150 industrial plants worldwide providing 20 percent of meat supplies globally, JBS had to shut down operations in Australia, the US, and Canada as a result of a REvil ransomware attack in late May 2021. 10,000 employees were affected, and the company paid an 11 million dollar ransom in Bitcoin.

WHEN

JANUARY 2020

VICTIMS

FRESENIUS GROUP, HONDA, ENEL GROUP

IMPACT

INDUSTRIAL ENVIRONMENTS

EKANS

Originally discovered in January 2020, EKANS¹⁰ ransomware has attempted or caused disruptions to Fresenius Group, Honda, and Enel Group. This malware variant has some capability related to impacting industrial environments, specifically process kill functionality related to ICS data historians and other endpoints. However, these capabilities have been observed to be relatively simple and unintentional. Nevertheless, asset owners and operators should be aware of this actor and the possibility of operational impact in their ICS environments.

PREPARATION AND DETECTION STRATEGY

To effectively prepare for and detect ransomware in industrial environments, consider factors across people, processes, and technology.

PEOPLE

People include your IT and OT personnel, asset owners and operators, vendors, and other stakeholders within the OT environment:

- **To identify ransomware incidents and respond appropriately, your stakeholders require training:** in some cases, IT and OT teams at an organisation haven't met before, or there's a lack of trust between the two teams, so ensure these two teams understand each other's roles and responsibilities, that OT understand the security risks associated with their systems and processes, and that IT understand the downstream effects of their security decisions.
- **Appoint incident commanders and site champions before an incident occurs:** these people will be your last line of defense and your early warning system. They know what normal looks like and can easily identify when things go awry. Training these first responders in incident and evidence handling provides an excellent return on investment in terms of incident identification, recovery, and root cause analysis (RCA).
- **Involve security personnel in engineering trouble tickets:** when operators identify issues, your security team should be involved in their resolution, enabling them to perform threat hunting to verify whether the root cause of a shut down or other interruption was the result of something intentional or accidental.
- **Involve your vendors and any third-party consultants in your incident response planning:** vendors and consultants are valuable resources in containing a ransomware infection once identified, performing RCA, returning your environment to a known-good or certified state, and recommending how to prevent similar incidents in future.

PROCESS

Visibility and knowledge of your environment are paramount to success in detecting and responding to ransomware:

- **Gather security requirements and perform security due diligence as early as possible in site commissioning:** determining security requirements early in the process enables you to implement better security controls early in the project. It's much more difficult to retroactively implement security controls in a site that's already online than it is before commissioning. In sites that are already running, perform architecture reviews, compromise assessments, and threat hunts during scheduled improvement projects to identify gaps that could be remedied tactically or strategically.
- **Understand the assets in your environment and what they do:** document your assets and create baselines against which you can compare current activity to identify suspicious activity.

- **Perform a Crown Jewels Analysis:**¹¹ identify critical assets and implement endpoint and network management, monitoring, and network segmentation, particularly between IT and OT zones, around those assets, systems, and processes to detect and respond to incidents. It's important to know and understand how to rapidly contain potential incidents while maintaining minimum viable operations at a site so that operations can be restored even while remediation activities are ongoing.
- **Create a Collection Management Framework (CMF):** A CMF¹² contains information on available data sources, their retention periods, and how data might be applied during security monitoring, incident response, or threat hunting. Formalize and document your understanding of available data and how to collect or access it. Then, exercise your documentation by performing a threat hunt to identify any malicious activity already ongoing in your network.
- **Create, verify, and test backups and gold images:** having robust backup and restoration plans for data and systems based on operational risk and business needs will drastically reduce your mean time to recover during a ransomware incident. For example, data required:
 - **To get back online:** system images and data, gold images
 - **To restore recent operations or operational state:** recent program changes, operating controller logic for PLCs and other devices
 - **For business functions to continue:** usage data, energy generation and usage data, billing data
- **Ensure you have a comprehensive incident response plan (IRP) and playbooks specifically designed for response in your OT environment:**¹³ most organizations develop an IT IRP, then either forego an OT IRP, or try to overlay the IT IRP on the OT environment.

The technologies, architecture, roles, responsibilities, and consequences in an OT environment are very different to those in an IT environment. Make sure your OT IRP reflects these differences.

Once you've created your IRP, it must be exercised, tested, and validated before an incident occurs. Outside of experiencing an incident, the best way to do this is a tabletop exercise, where you simulate an incident and discuss with the stakeholders how the IRP would be executed in that scenario. Likewise, testing your forensic collection tools and techniques is a significant consideration, and can be accomplished during maintenance shutdowns or otherwise in concert with your operational personnel. These processes can then be folded into future tabletop exercises.

Lastly, your IRP is iterative. After any incident, real or simulated, update your IRP with lessons learned or additional information that would have been useful during the exercise which was either unavailable or difficult to access or obtain.

TECHNOLOGY

It's important to build your toolkit before an incident occurs. Trying to push licensing or other purchases through procurement during an incident is a nightmare. Whatever solution you choose, it must have high-fidelity sensors and be capable of not only capturing and collating data, but alerting and notifying analysts to potentially malicious activity and must enable effective incident response.

Regardless of which solution you choose, ensure that your technology stack addresses and enables the five key security controls for an ICS cybersecurity program:¹⁴ defensible architecture, monitoring, remote access authentication (both internal and external), key vulnerability management, and an ICS incident response plan.

- **Centralize and aggregate endpoint logs and network traffic:** collect network and endpoint logs and evidence in a central location for retrospective analysis and to prevent tampering by a determined adversary.
- **Utilise publicly available datasets to augment your internal evidence collection and identify additional attack vectors:** services like Shodan, VirusTotal, Censys, and others, can provide you with telemetry about both your internal and external attack surfaces, vulnerabilities, and potential for compromise. Make use of these services and their APIs, but also be sure not to disclose sensitive information.

For example, search *hashes* against VirusTotal but don't upload *executables* — anything uploaded to VirusTotal becomes public.

- **Monitor and investigate non-standard connections:** communication to remote sites and facilities over cellular routers, for example; these might not be evident in known IP ranges, but can allow adversaries to pivot to internal networks.
- **Implement application control:** restrict the use of executables, software libraries, scripts, etc. on endpoints.
- **Patch applications and operating systems:** application and operating system patches, updates, and/or vendor mitigations for security vulnerabilities should be applied in a timely manner and on a regular schedule.
- **Implement user application hardening:** restrict users from running applications or application features which pose a legitimate risk to the organisation, such as java, advertising, and add-ons or extensions in web browsers.
- **Restrict administrative privileges:** privileged access to systems and applications, and administrator level accounts must be limited as much as possible, and must be regularly reviewed and managed in line with the principle of least privilege
- **Implement multi-factor authentication:** wherever possible, 2FA/MFA must be used to authenticate users accessing critical or sensitive data and systems, and for any methods of remote access.

RESPONSE STRATEGY

In addition to the preparation and identification steps already discussed, be prepared with a strategy to respond when ransomware eventually does land in your network.

CONTAIN, ERADICATE, AND RECOVER

How you contain the incident and whether you choose to pay the ransom or not will largely depend on your corporate policies and procedures, but also how well you were able to prepare for the incident with the right mitigating controls:

- It pays to be aware of any known decryptors for common ransomware and adversary groups, but also that any decryptor, even those provided by the adversary, may be very slow to restore data.
- It's not uncommon for organisations affected by ransomware to restore from backup simply because doing so is faster than using the relevant decryption tool; you'll likely need to weigh the cost of restoring versus decrypting particularly critical or sensitive data, so ensure this consideration is a part of your IRP.
- Additionally, backup and restoration procedures must be exercised and validated before an incident occurs; your disaster recovery plan is the most effective way of dealing with the aftermath of a ransomware event.

Be sure to have people on your team familiar with and trained to investigate and identify common living-off-the-land attacks where adversaries use tools that already exist in the environment to achieve actions on objectives:

- This could include tools such as Microsoft PowerShell, vendor tools used to manage industrial control systems and endpoints, or authorised remote access tools such as remote desktop and VPN connections; further examples can be found here: <https://lolbas-project.github.io/>.
- Be aware of and look for common lateral movement techniques, such as RDP, VNC, PSTOOLS, and potentially unauthorised or 'temporary' methods or remote access such as TeamViewer¹⁵ and AnyDesk.
- Log and monitor privilege escalation within your environment, both successful and unsuccessful, authorized and unauthorized.
- Familiarity with common command and control tools and tactics is beneficial, as is how to identify this within endpoint logs and network traffic to detect and remediate an incident in progress.

If you believe you've identified an incident, ensure you prioritise safety, availability, and reliability of operations:

- Scope the incident by identifying the sites and assets affected.
- Collect relevant evidence and data, then isolate affected devices as much as possible to prevent the spread of the infection (in line with your pre-defined response playbooks).

- Analyse the collected evidence and data and adjust the scope and response efforts as necessary
- Once the infection has been mitigated, try to identify the root cause to prevent secondary and tertiary infections, and begin remediation and recovery of the environment and restoration of operations.

POST-INCIDENT

After closing the incident:

- Complete a lessons-learned or after action exercise, with a view to identifying tactical and strategic (i.e. short- and long-term) improvements to processes and defenses to prevent recurrence, and to improve your incident response procedures.
- Update your backup and restore procedures and any gold images, configuration files, logical and physical network configurations as necessary.

IN CONCLUSION

There's a significant increase in ransomware attacks and overall incidents evident in industrial environments. Asset owners and operators, as well as other stakeholders in industrial sectors, must take preventative action to mitigate or remediate the risks associated with these tools, tactics, and procedures.

Understand the assets in your networks and what they're doing. Create defensible architectures where possible and use mitigating controls elsewhere. Implement monitoring and detection strategies that cover several phases of the ICS Cyber Kill Chain¹⁶ to detect and respond to events and incidents as they happen. Finally, perform post-incident activities and iterate your incident response plans and procedures as new information becomes available.

REFERENCES

1. <https://www.dragos.com/blog/industry-news/project-mimics-stage-one/>
2. <https://www.sans.org/presentations/e-mimics---extended-malware-in-modern-ics/>
3. <https://www.dragos.com/blog/dragos-2021-industrial-cybersecurity-year-in-review-summary/>
4. <https://www.sans.org/white-papers/36297/?msc=blog-ics-library>
5. <https://hub.dragos.com/guide/5-critical-controls>
6. <https://www.dragos.com/year-in-review/>
7. <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>
8. <https://www.cybertalk.org/2021/06/15/ransomware-attacks-on-industrial-control-systems-2021/>
9. <https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/>
10. <https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/>
11. <https://www.dragos.com/resource/crown-jewel-analysis-electric-power-distribution-example/>
12. <https://www.dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/>
13. <https://www.dragos.com/resource/preparing-for-incident-handling-and-response-in-ics/>
14. <https://www.dragos.com/year-in-review/>
15. <https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/>
16. <https://www.sans.org/white-papers/36297/?msc=blog-ics-library>

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

**TO LEARN MORE
ABOUT DRAGOS AND
OUR TECHNOLOGY,
SERVICES, AND THREAT
INTELLIGENCE FOR
THE INDUSTRIAL
COMMUNITY,
PLEASE VISIT
www.dragos.com.**



THANK YOU