



**JULY 2020**

# **WEAPONS OF MASS DISRUPTION**

---

## **An Assessment of the Threat Disruptionware Poses to Energy Sector Continuity**

Authored By:  
Drew Spaniel, Lead Researcher, ICIT  
Joyce Hunter, Executive Director, ICIT &  
Former Deputy CIO for Policy and Planning, USDA

## Contents

Introduction .....	1
What is Disruptionware? .....	2
Disruptionware Poses a Significant Threat to the Energy Sector .....	3
Mitigation and Remediation Recommendations.....	3
Have an Incident-Response Plan.....	4
Test Your Systems .....	4
Inventory Network Assets.....	4
Ensure Redundancy .....	4
Define Cyber Leadership Roles and Responsibilities .....	4
Utilize Network Segmentation Where Possible.....	4
Increase Network Visibility .....	5
Backup Critical Assets .....	5
Patch Systems Regularly .....	5
Implement Application Whitelisting and Software Restriction Policies.....	5
Disable Macro Scripts Where Possible .....	5
Warn Users About Potential Phishing Emails .....	6
Limit Internet Exposure .....	6
Apply the Principles of Least Privilege and Network Segmentation .....	6
Secure Network Protocols .....	6
Monitor and Audit User Activity .....	6
Disable SMB Where Possible .....	6
Secure Remote Desktop Protocol Wherever Possible.....	6
Manage Third Parties through Service-Level Agreements and Security Auditing .....	7
Participate in Cybersecurity Information Sharing Programs and Organizations.....	7
Conclusion.....	7
Appendix: Resources to Combat Disruptionware .....	8
Additional Guidance: .....	8

## Introduction

Previously, cyberattacks resulting in the targeted disruption of electricity to a geographic region were either hypothetical or featured sophisticated malware, such as Black Energy. Now, digital adversaries are adapting their tools, tactics, and procedures to threaten critical energy sector operational technology (OT) with less sophisticated, commercially available malware such as ransomware. This guide outlines this emerging threat, provides recommendations for mitigation and remediation, and details additional guidance.

On February 18, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert (AA20-049A) warning the energy sector about the threat ransomware posed to pipeline operations. A cyber attacker had compromised the information technology (IT) network of a natural gas compression facility, laterally infecting their operational technology (OT) with ransomware believed to have been specifically designed and deployed to disrupt operations. CISA detailed the attack:

*The threat actor then deployed commodity ransomware to Encrypt Data for Impact [T1486] on both networks. Specific assets experiencing a Loss of Availability [T826] on the OT network included human machine interfaces (HMIs), data historians, and polling servers. Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial Loss of View [T829] for human operators. The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations. Although the victim's emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations. This lasted approximately two days, resulting in a Loss of Productivity and Revenue [T828], after which normal operations resumed.*

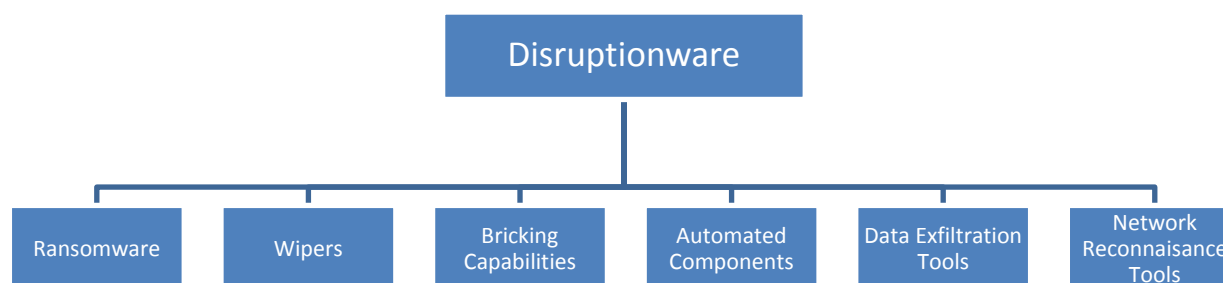
In this case, the attacker succeeded because the victim lacked robust segmentation between its IT and OT networks, thereby allowing the adversary to traverse the IT-OT boundary and disable Windows-based assets on both networks with a commodity ransomware. In this instance, the attacker's choice of Windows-specific ransomware restricted their ability to compromise the programmable logic controllers (PLCs) necessary to directly read and manipulate physical processes at the facility. If the attacker was more sophisticated or had deployed a more versatile malware platform, the impact could have been significantly worse. Instead, the victim, who lacked a cyber incident response plan, physically shut down their systems for an extended period.

In September 2019, ICIT and Forescout coined the term *disruptionware* to characterize this variety of malware and warned of the potential evolutions that could occur if the threat was left unchecked. Just a few months later, the threat is rapidly evolving in earnest due to organizations' vulnerable cybersecurity postures amidst the COVID-19 pandemic. The February 2020 attack against energy sector infrastructure could set an alarming precedent for cyberattacks intent on targeted disruption. If energy sector operators do not evolve their security postures to respond to the threat, the impacts could prove dire.

## What is Disruptionware?

Disruptionware is an emerging category of malware designed to suspend operations within the victim organization through the compromise of the availability, integrity, and confidentiality of the data, systems, and networks belonging to the target. In general, the adversaries' goal is disrupting business continuity as a means of effecting extortion, reputational harm, socio-economic or geopolitical leverage, or other targeted outcomes. Typical components of disruptionware attacks specific to OT environments are depicted in the figure below:

**Figure 1: Typical Components of Disruptionware**



*Common components of a disruptionware toolkit in the context of OT environments*

Potential components of a disruptionware platform include, but are not limited to:

1. **Ransomware:** By weaponizing encryption, attackers can render a system or data inaccessible either indefinitely or until ransom demands are met.
2. **Wipers:** Wiper malware deletes all data stored on a device and requires system administrators to either reboot the device or restore it from backups.
3. **Bricking Capabilities:** Permanent Denial of Service (PDoS) malware strategically misconfigures hardware, firmware, or software settings to cause irreparable corruption or physical destruction of a system.
4. **Automated Components:** Botnets and other automated components can be used to leech resources, relay malicious traffic, or overwhelm a network with inbound traffic in a distributed denial of service (DDoS) attack.
5. **Data Exfiltration Tools:** While other attack vectors are consuming the attention and resources of the victim's incident response team, an adversary may exfiltrate and publish employee data, trade secrets, or other sensitive information in an attempt to generate a negative PR response, disrupt employee focus, or otherwise tax the human resources of the organization.
6. **Network Reconnaissance Tools:** Remote Access Trojans (RATs), keyloggers, network mapping tools, and other applications can be used to identify and spread malware to mission-critical assets.

Disruptionware is particularly devastating when it sequesters mission-critical systems, OT environments, and legacy systems that lack redundancy. Ransomware is currently the most

common disruptionware component, with incidents such as the LockerGoga ransomware campaign demonstrating that even unsophisticated malware has the capacity to suspend daily operations whether or not the victim pays the ransom.

As detailed in *The Rise of Disruptionware* report from September 2019, factors contributing to the risk disruptionware poses to OT infrastructure include:

- Dependency on remote access over manual maintenance
- Network expansion and drift
- Unsecured industrial internet-of-things sensors and devices
- Vulnerable third and fourth-party networks

## **Disruptionware Poses a Significant Threat to the Energy Sector**

The nation's socioeconomic survival depends on a complex electricity grid. Homes and business depend on an assortment of power generation plants, distribution facilities, and transport mechanisms to deliver energy. Unfortunately, the United States' energy sector is an intricate amalgamation of interwoven networks with antiquated legacy systems resulting in an interconnected, under-protected, semi-modern technology where momentary outages disrupt daily life and sustained outages jeopardize lives.

The electric grid and the supporting energy-production infrastructure are built to be flexible, reliable, and economically competitive. The system is flexible due to a diversification of energy production resources and a location-based optimization of energy facilities. In other words, coal-fueled facilities are used in regions with plentiful coal supplies while wind power supports regions with strong wind currents. Reliability is achieved through a large transmission network that allows operators to route energy between distant cities in times of need. Finally, the American electric grid relies on a variety of generation facilities that compete to offer the most affordable rates to consumers. Unfortunately, cybersecurity was not one of the three founding principles of the American energy distribution network. All of the power generation facilities, transmission networks, distribution nodes, network operations, and consumer endpoints that interconnect to form the energy sector are susceptible to disruptionware attacks.

## **Mitigation and Remediation Recommendations**

Falling victim to a disruptionware campaign can have devastating consequences for an organization. The following is a list of high-level recommendations intended to act as a guide to evaluating an organization's general preparedness and resiliency to this growing threat. We suggest using this as the starting point for a more detailed discussion with security experts as each item is nuanced and the ideal solution for you will vary based on your environment and current security structure.

## **Have an Incident-Response Plan**

Stakeholders should collaborate to develop an incident-response plan, including what to do during a ransomware event. This plan should consider the full range of potential impacts that cyberattacks pose, including loss or manipulation of view, loss or manipulation of control, and loss of safety. In particular, response playbooks should identify criteria to distinguish between events requiring deliberate operational shutdown versus low-risk events that allow for operations to continue.

## **Test Your Systems**

How long can you afford to have downtime due to targeted disruption? Simulating downtime and system shutdowns will enable you to measure how quickly you can revert to failover communication and backup systems. Conducting drills to ensure that personnel know how to respond to emerging threats will give your employees confidence, as will practicing using alternate control systems, including manual operation, while assuming degraded electronic communications. Giving employees decision-making experience via tabletop exercises that incorporate loss of visibility and control scenarios will enable you to capture lessons learned and document them in emergency response playbooks.

## **Inventory Network Assets**

Inventorying all assets on every network and classifying them by OS, type of device, and function will increase visibility into the network and help identify critical assets, detect rogue devices, develop incident-response plans, and formulate schedules for patches and updates.

## **Ensure Redundancy**

Identifying points of failure, both technical and human, will increase operational visibility. Developing and testing emergency response playbooks ensures there are redundant channels that allow visibility into operations when one channel is compromised. Implementing redundant communication capabilities between geographically separated facilities responsible for the operation of a single asset will ensure that coordination and communication continue across all such facilities in the event of an incident.

## **Define Cyber Leadership Roles and Responsibilities**

To be prepared for an attack, identify the security roles and responsibilities of all C-level executives, especially the CIO, CISO, CSO, and CRO. If those individuals are not available, the playbook should identify alternative decision makers.

## **Utilize Network Segmentation Where Possible**

Implementing robust network segmentation between IT and OT networks will limit the ability of adversaries to pivot to the OT network if the IT network is compromised. Defining a demilitarized zone that eliminates unregulated communication between the IT and OT networks further secures both systems.

Additionally, organizing OT assets into logical zones by considering criticality, consequence, and operational necessity allows acceptable communication conduits to be established between



zones. Deploying security controls to filter network traffic and monitor communications between each zone can prohibit industrial control system (ICS) protocols from traversing the IT network.

### **Increase Network Visibility**

Take the time to leverage tools and services that increase visibility into networks and systems. Using multiple tools and services to identify and mitigate vulnerabilities can also monitor for threats infiltrating the network.

### **Backup Critical Assets**

No matter the situation, it is always a good idea to have a redundant system that saves multiple iterations of backups and stores them offline. That way, if the most recent set of backups includes encrypted or infected files it is still possible to restore the information. Routinely testing your backups for data integrity ensures you can recover your data intact.

### **Patch Systems Regularly**

One of the most critical steps to a secure network is keeping all systems patched, including hardware, mobile devices, operating systems, software, applications, cloud locations, and content management systems (CMS). If possible, use a centralized patch management system. Monitoring current events and information sharing hubs keeps systems secure against emerging threats. For instance, ensuring that patch MS17-010 (CVE-2017-0147) is applied to all systems protects against Server Message Block (SMB) exploitation via Eternal Blue. Additionally, be sure to use antivirus and antispam applications on all devices. Enabling regular system and network scans with antimalware applications and configuring them to automatically update signatures will help you spot problems quickly. Implementing an antispam solution to stop phishing emails from reaching the network will limit opportunities for users to download malware onto your network.

### **Implement Application Whitelisting and Software Restriction Policies**

Though it may not be possible or practical in OT environments, application whitelists and software restriction policies (SRPs) can prevent the execution of programs in common ransomware locations, such as temporary folders. IT systems that are networked with OT systems should be protected to limit lateral adversarial movement. Requiring firewall validation for inbound and outbound traffic prevents malicious traffic from entering the network and detects suspicious traffic requests leaving the network.

### **Disable Macro Scripts Where Possible**

Many malware programs enter the network as malicious attachments that exploit macro vulnerabilities. To limit risk, consider disabling macro scripts on relevant applications or employing alternative solutions. For instance, Office Viewer software can be used to open Microsoft Office files transmitted via email instead of using the full office suite applications.

## **Warn Users About Potential Phishing Emails**

A simple warning banner on all emails from external sources can help remind users of the dangers of clicking on links and opening attachments.

## **Limit Internet Exposure**

Consider using a proxy server for Internet access and installing an ad-blocker on that server. Do your best to restrict access to common ransomware entry points, such as personal email accounts and social networking websites. When possible, segment networks, disable unused ports, and monitor and restrict access to ports that cannot be disabled.

## **Apply the Principles of Least Privilege and Network Segmentation**

Categorize and separate data based on organizational value and, where possible, implement virtual environments with physical and logical separation of networks and data. Applying the principle of least privilege and the zero-trust paradigm will minimize risk.

## **Secure Network Protocols**

Increasing security controls for all network protocols that could allow lateral movement within a network limits the spread of malware. This includes disabling and blocking all insecure network protocols such as telnet, FTP, and HTTP. Enforcing the adoption of https, the latest version of ssh/TLS, and other secure protocols will help keep your organization secure.

## **Monitor and Audit User Activity**

Audit for unauthorized access attempts, known as brute forcing, and the use of common penetration testing tools, such as Metasploit.

## **Disable SMB Where Possible**

The more you can restrict the use of SMB, the better off you will be. Start by disabling SMBv1 on all systems and only utilize SMBv2 or SMBv3 after appropriate testing. Decrease your risk by disabling the use of SMB port 445 between endpoints and restricting SMB to communication between endpoints and file servers. Always limit and audit files accessible via SMB shares and do not forget to patch the Windows MS17-010 (CVE-2017-0147) vulnerability commonly leveraged in malicious attacks.

## **Secure Remote Desktop Protocol Wherever Possible**

Assess the need to have RDP port 3389 open on systems and, if required, whitelist connections to specific trusted hosts. After cloud environments are set up on your network, verify that RDP ports were not accidentally re-enabled, unless required for business purposes. For any cloud environment already installed, verify that your network is adhering to best practices, as defined by the cloud service provider. Any system which needs to have an open RDP port should be placed behind a firewall and require a user VPN. Additionally, you should perform regular checks to ensure the RDP port is not open to the public internet.



## **Manage Third Parties through Service-Level Agreements and Security Auditing**

Evaluating and monitoring third parties that have remote access into your organization's network limits the potential for lateral spread from their networks. Ensuring business partners are equally as diligent with their cybersecurity could save you significant trouble in the future.

## **Participate in Cybersecurity Information Sharing Programs and Organizations**

By participating in information sharing hubs and publications, you can be part of the first line of preemptive defense against emerging threats.

## **Conclusion**

Disruption attacks on energy sector infrastructure is not a purely hypothetical threat. Ever since Ukraine was targeted with the Black Energy malware and that same malware was discovered on major US networks, the sector has been primed to guard against the eventuality of a sophisticated cyberattack, launched from a advanced persistent threat actor, focused on a targeted outcome of localized disruption. However, the emergence of disruptionware is more troubling because the malware is neither overly sophisticated nor proprietary. These targeted ransomware attacks can be launched by low level adversaries and the malware can be either purchased individually or as part of a platform on dark web markets and forums. If the sector does not modernize its systems and evolve its security posture, attacks focused on targeted disruption could replace ransomware campaigns against healthcare organizations as the "low hanging fruit" among cybercriminals and sophisticated threat actors alike.

## Appendix: Resources to Combat Disruptionware

The following is a list of publicly available resources which offer tools, frameworks, and guidance to help organizations combat disruptionware.

- [The No More Ransom Project](#): The *No More Ransom* website is an initiative by McAfee, Europol's European Cybercrime Centre, and the National High Tech Crime Unit of the Netherlands' police. Their goal is to help victims of ransomware retrieve their encrypted data without having to pay the criminals. They offer free ransomware decryption and other tools.
- [NIST Cybersecurity Framework](#): The framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Its prioritized, flexible, and cost-effective approach helps promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.
- [OWASP Cyber Defense Matrix](#): This was created to help security practitioners mature their security programs. It does this by building, managing, and operating a security program that captures use cases and their implementations.
- [CIS Controls](#): This is a list of technical controls and best practice configurations that can be applied to any environment. Their focus is on hardening technical infrastructure to reduce risk and increase resiliency. It does not address risk analysis or management like the NIST Cybersecurity Framework.

### Additional Guidance:

- [CISA Ransomware One-Pager and Technical Document](#) (CISA, 2019)
- [CISA Insights: Ransomware Outbreak](#) (CISA, 2019)
- [Pipeline Cybersecurity Initiative](#) (CISA, 2018)
- [CISA Webinar: Combating Ransomware](#) (CISA, 2018)
- [Framework for Improving Critical Infrastructure Cybersecurity](#) (NIST, 2018)
- [Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events](#) (NIST, 2018)
- [Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events](#) (NIST, 2018)
- [Pipeline Security Guidelines](#) (TSA, 2018)
- [NIST SP 800-11: Data Integrity: Recovering from Ransomware and Other Destructive Events](#) (NIST, 2017)
- [Guide to Industrial Control Systems \(ICS\) Security](#) (NIST, 2015)
- [Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model](#) (DOE, 2014)