

September 2019



THE RISE OF DISRUPTIONWARE

A Cyber-Physical Threat to Operational Technology Environments

Authored By:

Ryan Brichant, ICIT Fellow & Global CTO, Critical
Infrastructure Cybersecurity, Forescout

Parham Eftekhari, Executive Director, ICIT

ICIT | Institute for Critical
Infrastructure Technology

The Cybersecurity Think Tank



FORESCOUT

The Rise of Disruptionware

A Cyber-Physical Threat to Operational Technology Environments

September 2019

The authors would like to thank the following experts for their contributions to this paper:

- Elisa Costante, Sr. Director, Industrial and OT Technology Innovation, Forescout
- Jerry Davis, ICIT Fellow & V.P. and Global Chief Security Officer, Lam Research
- Alex Eisen, Security Researcher, Forescout
- Drew Spaniel, Lead Researcher, ICIT

Copyright 2019 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

Contents

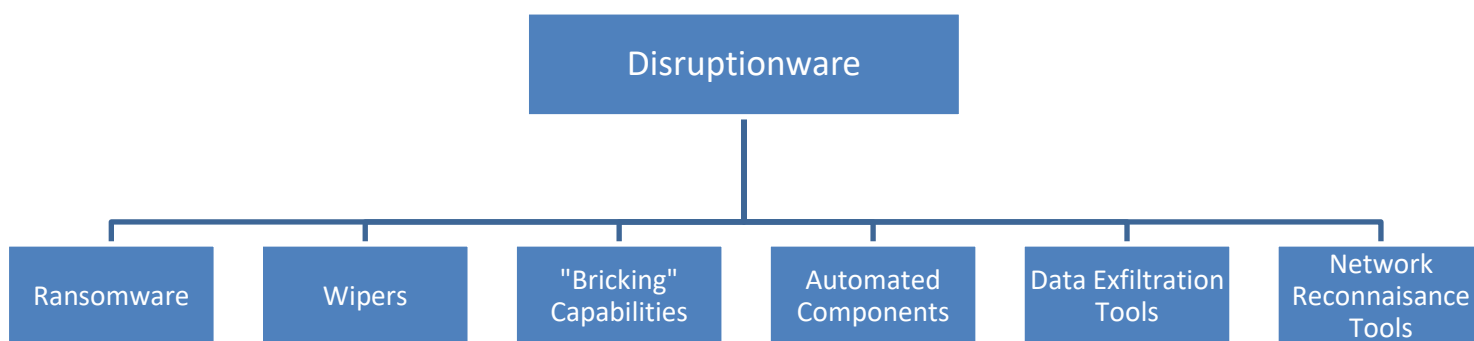
Executive Summary	3
Disruptionware: The Weaponization of Disruption Through Malware	5
What is Disruptionware?	6
Ransomware is at the Core of the Disruptionware Evolutionary Trend	8
Variants of Ransomware	9
Responding to Ransomware Depends on an Organization's Preparedness.....	10
What Else Could Go Wrong?	11
Factors Contributing to the Increasing OT Risk Landscape	11
Remote Access vs. Cost-Prohibitive Manual Maintenance	11
Network Expansion and Drift	12
Industrial Internet of Things Sensors and their Risk	12
Vulnerable Third and Fourth-Party Networks.....	12
Recommendations to Improve Resiliency	12
Develop a Plan.....	12
Assess and Monitor Your Network	13
Practice Strong Cyber Hygiene.....	13
Implement Strong Controls.....	14
Resources to Combat Disruptionware	15
Conclusion.....	15
Sources	16

Executive Summary

Disruptionware is an emerging category of malware designed to suspend operations within a victim organization through the compromise of the availability, integrity, and confidentiality of the systems, networks, and data belonging to the target.

This trend, identified by ICIT and Forescout researchers, sees adversaries disrupting business continuity and poses an existential threat to critical infrastructure operators. Disruptionware attacks introduce risk into the environment by degrading or halting manufacturing processes, damaging reputations, extorting money from victims, or other targeted outcomes. Typical components in disruptionware attacks specific to OT environments are depicted in the figure below:

Typical Components in Disruptionware



The diagram above depicts some common components of a disruptionware toolkit in the context of OT environments

For OT environments, disruptionware is particularly devastating when it sequesters mission-critical systems 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 bring businesses to a halt.

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

To improve resiliency against disruptionware attacks, organizations should consider the following categories of action:

1. Develop a Plan

- Implement security-by-design
- Have an incident response plan
- Define leadership roles and responsibilities during an attack
- Backup critical assets
- Test your systems
- Participate in cybersecurity information sharing programs and organizations

2. Assess & Monitor Your Network

- Inventory network assets
- Increase network visibility
- Monitor and audit user activity

3. Practice Strong Cyber Hygiene

- Regularly patch systems
- Disable macro scripts where possible
- Limit internet exposure
- Disable secure server message block where possible
- Manage third parties through service-level agreements and security auditing
- Warn users about phishing emails

4. Implement Strong Controls

- Apply the principles of least privilege and network segmentation
- Secure network protocols
- Implement application whitelisting and software restriction policies
- Secure remote desktop protocol access wherever possible

The following publicly available resources are available to help organizations combat disruptionware:

- [The No More Ransom Project](#)
- [NIST Cybersecurity Framework](#)
- [OWASP Cyber Defense Matrix](#)
- [CIS Controls](#)

Disruptionware: The Weaponization of Disruption Through Malware

The year 2019 will be remembered as the year disruptionware emerged as the preferred methodology for attackers to wreak havoc on our nation's critical infrastructure. Cunning adversaries now target the operational technology (OT) environments of critical infrastructure firms with cyberattacks tailored towards disruption of business continuity or, in some cases, physical outcomes. By encrypting, locking, or wiping systems or data essential for business continuity, organizations are forced to either pay the demanded ransom or face the harsh reality of needing to replace systems, suspend operations, or revert to failover systems until continuity can be restored.

Researchers at ICIT and Forescout refer to this evolving attack paradigm as disruptionware. Others have more narrowly categorized the emerging threat as a permanent denial of service attack (PDoS) [1] [2]. Technical specifics of the malware or attack vector aside, the adversary's strategy relies on disruption to business continuity as a means of halting manufacturing, extortion, damaging reputations, gaining socioeconomic or geopolitical leverage, or other targeted outcomes. Targeted disruption can take many forms, such as corrupting systems, spamming clients, or denying access to critical assets or services.

The risk that disruptionware poses to business and technical leaders cannot be understated. According to ICIT Fellow and V.P. and Global Chief Security Officer at Lam Research, Jerry Davis, "For those of us in critical manufacturing environments, we shudder to think about the cascading effect that Disruptionware can have within any sector of our Value Chain eco-system. In those segments where Operational Technology (OT) is a key and pervasive manufacturing service, Disruptionware poses an existential threat to any business that does not have proper cyber controls in place to reduce the disruption, degradation or total destruction of its business operations."

Because the potential layers of an attack are vast and only limited by the imagination, willpower, and resources of the adversary, this publication will instead focus on a more limited scope: the risk that disruptionware poses to OT environments. Gartner defines operational technology as "[the] hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations." OT components and applications are utilized in manufacturing plants, oil and gas facilities, mining operations, and some smart city technology. Examples of common OT components include PLCs (programmable logic controllers), SCADA (supervisory control and data acquisition) systems, DC (distributed control) systems, and CNC (computer numerical control) systems.

Over time, as with any malware, less sophisticated hackers mirror the tools, tactics, and procedures of advanced threats. The evolution of disruptionware is the natural development of a decade of trendsetting attacks from nation-state advanced persistent threat (APT) actors. In 2010, the Stuxnet malware was believed to have caused significant damage to the SCADA systems supporting Iran's nuclear program [3] [4]. In 2013, the BlackEnergy malware was leveraged to disrupt the Ukrainian electric grid temporarily [5]. More recently, in December 2017, it was revealed that the Triton malware had disrupted the safety systems of an unidentified power station in the Middle East [6] [7]. Each of the aforementioned malware were developed and deployed by APT actors that were intent on disrupting the operations of

their targets rather than focusing on the more typical motivations of data exfiltration or financial gain. Today, disruptionware has become an even more significant threat to critical infrastructure, as tools have been developed beyond the BrickerBot malware and botnets of the past decade and are now easily accessible by script kiddies and cybercriminals around the world. For example, the LockerGoga attacks resulted in tens of millions of reported losses and the June 2019 Silex attacks left thousands of Internet of things (IoT) devices inoperable [8] [9].

Recent ransomware attacks, such as the LockerGoga infections that impacted the French engineering consulting firm Altran, the Norwegian aluminum manufacturer Norsk Hydro, and US chemical companies Hexion and Momentive, did not used to be the purview of operators of industrial control systems (ICS). As facilities become more interconnected, IT and ICS infrastructures cannot be considered separately. Critical OT assets must be secured against IT-focused malware that can be launched from point-and-click applications by adversaries across the globe. These targeted cyberattacks require very little technical sophistication, making them low-risk with potentially high-rewards. Norsk Hydro suffered \$40 million in losses after switching to manual operations while its systems were restored and the ransomware infection was removed. Unfortunately, many firms that rely on automated systems, such as manufacturing plants, cannot efficiently or safely operate manually [10]. Disruptionware attacks inflict digital and, in some cases, physical impact on critical infrastructure operations at plants and manufacturing facilities.

Disruptionware has the potential to cause a number of highly impactful risk scenarios to materialize within organizations including that can bring down a business unit or an entire company for hours, days, or weeks. In this publication, Forescout and the Institute for Critical Infrastructure Technology (ICIT) chose to focus specifically on the threat disruptionware poses to OT operations, even unsophisticated ransomware like LockerGoga, and on recommending holistic security solutions such as planning for and implementing security-by-design controls, developing an incident response plan, increasing device visibility across the converged IT/OT environment, segmenting networks according to least privilege and least access principles, and layering security controls. This publication will not delve into the motivation or attribution parameters of specific threat actors or focus on other variants of disruptionware.

What is Disruptionware?

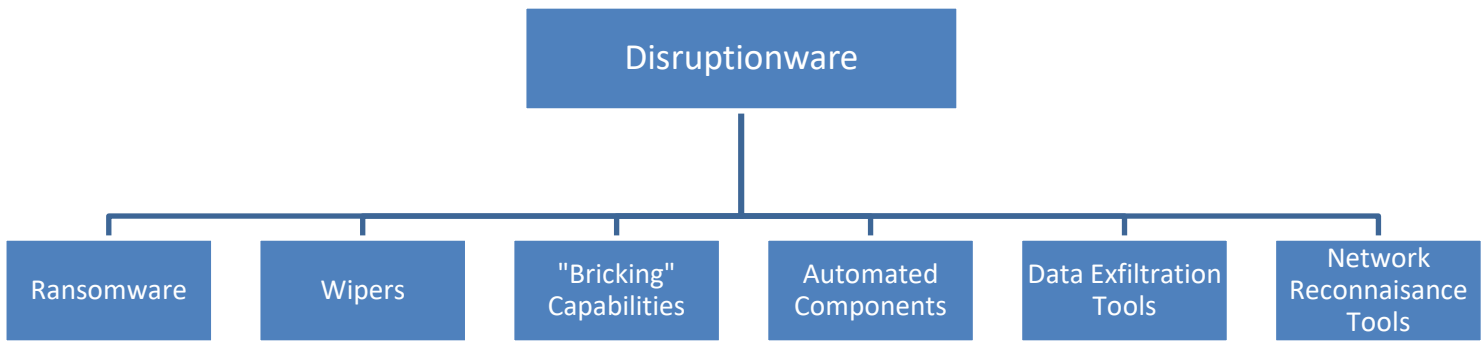
Disruptionware is a category of malware designed to suspend operations within a victim organization through the compromise of the availability, integrity, and confidentiality of the systems, networks, and data belonging to the target.

Ransomware is one of many tried and tested tools in a catalog of disruptionware mechanisms that are employed in layered attacks by adversaries of varying degrees of sophistication. In OT environments, the primary objective in using ransomware may not be to collect a ransom payment. Instead, the attacker may intend to disrupt operations and production in manufacturing or industrial environments in order to achieve some other strategic goal.

In the context of this paper, which is focused on OT operations, some common components of a disruptionware toolkit 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** – 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 overwhelm a network with inbound traffic in a distributed denial of service attack, leech resources, or relay malicious traffic.
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 , keyloggers, network mapping tools, and other applications can be used to identify and spread malware to mission-critical assets.

Typical Components in Disruptionware



The diagram above depicts some common components of a disruptionware toolkit in the context of OT environments

Notable disruptionware attacks have garnered significant media attention recently and will continue to do so in the foreseeable future, as disparate vectors such as ransomware, botnets, wiper tools, and other components continue to converge into accessible point-and-click malware platforms. For instance, in March 2019, Norsk Hydro, one of the largest aluminum producers in the world, disclosed that some of their systems had been infected by the LockerGoga ransomware, affecting their operations worldwide. Norsk Hydro is involved in all parts of the aluminum manufacturing process, from refining to manufacturing products for construction and industry. Disruption of any stage of its supply chain can significantly impact multiple sectors. Norsk declined to pay the ransom and instead engaged its incident response

procedures and reverted to backup and redundancy infrastructure. Nevertheless, a week after the attack, it estimated its losses at \$40 million despite reporting a full recovery.

Other victims of LockerGoga, such as the US chemical companies Hexion and Momentive, were not as fortunate and were forced to replace systems infected with LockerGoga [10] [11]. Norsk Hydro's \$40 million estimated loss is relatively small in comparison to the \$100 million loss Spanish food distributor Mondelez suffered, or the \$300 million Danish shipping firm Maersk reported losing after the 2017 NotPetya ransomware attack [12].

Despite its lack of sophistication, most disruptionware is devastating to critical infrastructure firms because it has a high rate of successful compromise, requires little to no continued adversarial effort, consumes the target's resources, disrupts daily operations, and may spread down the supply chain. Consequently, the integration of disruptionware into adversarial campaigns is attractive to threat actors ranging from script kiddies to nation-state sponsored threats.

Consider a situation where encrypting the OT network of a US steel manufacturer could result in a lucrative contract being awarded to a Russian firm, or where wiping the systems and backup servers of a tech startup provides a Chinese firm with a technological advantage. This type of corporate espionage is already occurring. If BlackEnergy, LockerGoga, GermanWiper, and other prolific malware are indicative of the evolution of the threat landscape, then APT groups, such as the Russian sponsored Sandworm APT or Cybercrime FIN6 APT, have already incorporated disruptionware into their digital arsenals and are actively evolving the capabilities of the malware to impact critical infrastructures [13] [14] [15].

The traditional Information Security principles, known as the Confidentiality, Integrity and Availability paradigm, or the CIA triad, is inverted in OT and ICS environments. Instead, security priorities are often organized as follows:

1. Safety/Resilience
2. Availability
3. Integrity
4. Confidentiality
5. Privacy

This inversion of the paradigm that IT practitioners follow makes OT environments especially vulnerable to ransomware attacks if they have not specifically prepared for such a threat. Since they focus their limited IT budgets on patching and maintenance, they are essentially trading secure data to ensure continuous daily operation. Moreover, these systems are especially vulnerable to targeted disruptionware attacks because the desired outcome of a disruptionware attack is compromised safety, suspended operations, or critical systems rendered unavailable. In short, disruptionware was designed to be the antithesis of secure OT and ICS environments.

Ransomware is at the Core of the Disruptionware Evolutionary Trend

Today, ransomware is by far the most ubiquitous variant of disruptionware in use by threat actors of every level of sophistication due to its accessibility, availability, and versatility.

Ransomware is the malicious weaponization of encryption to deny access to a system, device, or file until a ransom is paid or, on rare occasions, until the victim manages to regain access to the system or network. Victims are typically given the options of paying the ransom, reverting to redundancy and backup servers if they were not infected, attempting to employ a decryption tool or services such as from sites such as NoMoreRansom.org, or accepting the loss of the encrypted system.

Though experts advise against paying the ransom, in some instances, the downtime necessary to revert to backup systems may cost significantly more than the amount demanded. In other cases, the operational downtime, especially in sectors that demand business continuity, such as manufacturing, utilities or healthcare, could result in millions of dollars in lost productivity, loss of critical services, loss of trust with customers, or even loss of life. In many OT environments, failover systems may not exist or be readily available. It is also important to note that in many instances, the threat actor who delivered the ransomware is not the developer of the malware and may not be able to support decryption of the file or system.

Ransomware is not the simplest form of disruptionware to develop; many botnets, wiper tools, and PDoS tools are simpler to design, deploy, and operate. However, due to its point-and-click deployment platform design and its ease of adoption, many adversaries are incorporating capabilities such as wiper components into basic ransomware toolkits. For instance, shortly after the attack on Norsk Hydro, Palo Alto Network's Unit 42 reported that the developers behind LockerGoga were actively incorporating additional capabilities into the malware variants and Cisco Talos reported that the malware featured wiper capabilities [16].

Ransomware is by no means the most dangerous form of disruptionware, but it is the most ubiquitous and often the most successful; in fact, last year new ransomware samples increased an estimated 118% [17]. Adversarial campaigns can be targeted attacks against specific firms, semi-targeted attacks against a category of victims, or as a widespread attack with no particular target. Ransomware can proliferate via botnets, act as brickware, include wiper capabilities, be a profitable and distracting attack for an experienced threat actor, or be leveraged as a strategic tool in an espionage or ransom campaign. Whatever the goal, ransomware began the evolution of the malware category because many of the adversaries developing and deploying disruptionware begin with ransomware as their foundation.

Variants of Ransomware

Variants of ransomware can be categorized into encryption driven derivatives, known as crypto-ransomware, wiper variants that erase data, or locker ransomware that blocks access to vital data and files. The risk each of these variants introduces into OT environments is essentially the same; operators are locked out of mission critical systems and operations cease until systems can be restored.

Ransomware may be further categorized as either opportunistic or strategic according to its infection vector and targets. Opportunistic ransomware is designed to infect as many victims as possible. Once access to the system or files is blocked, the ransomware demands a ransom in order to unlock the files. The majority of opportunistic ransomware is propagated through user-initiated actions such as clicking on a malicious link in a spam email or visiting a compromised website. More rarely, ransomware infects computers through malvertising. A few variants of

opportunistic ransomware spread via Server Message Block (SMB) vulnerabilities and use the Eternal Blue tool. In part, due to the widespread victim pool and the unpredictability of the success of the attack, opportunistic ransomware frequently makes small ransom demands ranging from a few hundred to a few thousand dollars [18].

Strategic ransomware is predicated on extortion. The ransom amount will often vary based on the adversary's assessment of the victim's ability and need to pay. Ransoms for these targeted attacks scale according to the access of the attacker, size of the victim organization, and value of the data. Typical ransoms range from a few thousand to tens of thousands of dollars [18].

Responding to Ransomware Depends on an Organization's Preparedness

Regardless of the categorization of the ransomware, the result of the infection is often the same: business comes to a grinding halt due to the inaccessibility of OT systems. The decision business and IT leaders are faced with is, "What do we do now?"

Forescout, ICIT, and most other security organizations recommend that organizations never pay a ransom. Instead, the recommendation is to spend that money on preparing for potential incidents by creating redundancies, backing up systems, doing proper incident response and business continuity planning, and conducting regular cyber war-gaming exercises. The incident response plans should specify which stakeholders to include in key decision making, ranging from C-level executives, to facility and operations managers, PR, legal, cyber insurance firms, and law enforcement. The steps of the incident response plan should be clearly communicated to senior leaders, legal, communications, technical staff, and all other relevant personnel. If personnel are only vaguely familiar with the incident response plan, then their reactions may be stunted, and the delay could allow the malware to have a larger impact than it would otherwise. Instead, incident response plans should be routinely tested through gamification exercises [19].

When an incident occurs, organizations should typically do the following:

- Evaluate whether they have redundant systems or recent backups and assess how long it would take to recommence operations from those assets.
- Ascertain whether they should attempt to decrypt the data themselves or hire a third-party to do so. Many ransomware programs have decryption keys released online and, if the attacker did not change the default key, it is possible to use the online key to retrieve the data.
- Consult their cyber insurance policies to see if they cover ransomware attacks or matters of cyber extortion.

In some instances, companies, cities, and utilities may ultimately decide to pay the ransom because they lack backups of their data, their redundancy systems were compromised, or other lapses caused by inadequate preparation. For others, paying the ransom is a financial cost-saving decision centered on a fear of disruption. Consider the March 22, 2018 ransomware attack that hit the City of Atlanta. It impacted nearly 4,000 of the city's computers, networks, and workstations, resulting in an estimated \$17 million in damages. Chris Duvall, senior director at The Chertoff Group, which provides security and risk management advisory services, said, "If we look at Atlanta and how much it has cost to replace systems and applications, we see there is a financial incentive to sweep an attack under the rug and move on."

However, it is essential to remember that paying the ransom does not guarantee an organization will regain access to its data as not all cyberthreat actors will respond to payments, and some variants of malware are unable to decrypt files or may have deleted them [18]. Further, by paying the ransom, the victim is demonstrating to the attacker, and to aspiring threats, that ransomware attacks are lucrative and may be particularly profitable against the victim organization or others in the sector.

Despite recent news of ransom payments being made, particularly at the local government level, the public continues to stand by the ‘no pay’ mantra. A resolution at the US Conference of Mayors in early July 2019, which estimated that at least 170 county, city, and state governments had suffered a ransomware attack since 2013, bound more than 1,400 officials in their commitment to not paying the ransoms that enforce cybercriminal behavior.

What Else Could Go Wrong?

Ransomware is now more than just an unsophisticated cybercrime attack vector. While the victim is deciding whether or not to pay the ransom, the adversary retains access to the system, allowing them to install backdoors, remote access Trojans, or other malware that can facilitate future attacks or provide access-as-a-service to other attackers. For example, sophisticated ransomware might include components that laterally infect networked systems and eventually spread onto third-party networks. In contrast, unsophisticated ransomware could include flaws in the code that prevents full data decryption even with a decryption key. Another variant includes the capability to lock cloud-based backups during persistent synchronization, while another targets IoT devices. Additionally, emerging ransomware, such as variants of GermanWiper profiled in August 2019, preclude the possibility of paying the ransom to recover encrypted data. While the victim is presented with a ransom note demanding bitcoins, the data cannot be recovered because, instead of encrypting the information, the malware destroys the data by overwriting it with zeroes and ones. At the time of writing, GermanWiper has only infected businesses in Germany via malicious job application attachments; however, there is no current technical or non-technical barrier that would prevent an attacker from leveraging similar capabilities against OT environments [20] [21].

Factors Contributing to the Increasing OT Risk Landscape

According to researchers at Forescout, “...expect the convergence of IT and Operational OT [to], yet again, make ICS and OT systems primary targets for exploit” [23]. Disruptionware campaigns are expected to increase in success, as they are evolving faster than organizations with OT networks are successfully defending themselves. The next sections will discuss the factors which contribute to this trend.

Remote Access vs. Cost-Prohibitive Manual Maintenance

For many firms, manual maintenance is deemed too expensive compared to remote access solutions, especially if the systems are located overseas. Maintaining a dedicated staff on-site to patch, update, and repair a system is considered too costly in comparison to cheaper remote access or automated alternatives. Adversaries leverage the remote desktop protocol (RDP) ports, generally TCP 3389 and UDP 3389, that are often used for remote maintenance, to install malware onto networks or laterally infect additional devices.

Even after serious threats are discovered that exploit vulnerabilities in remote access protocols, companies are slow to mitigate the immediate risk. For example, despite months of warning, as of July 2, 2019, 805,665 systems remain vulnerable to the BlueKeep RDP exploit, with an estimated 105,170 systems located in the United States [22]. BlueKeep (CVE-2019-0708), is a remotely executable vulnerability in RDPs in older versions of Windows that enables attackers to assume complete control of vulnerable systems and steal or destroy the data on them. Microsoft described the vulnerability as “wormable” because leveraging it allows the malware to spread autonomously from one vulnerable system to another in much the same fashion as WannaCry did worldwide in 2017 [22].

Network Expansion and Drift

Over time, if networks are not properly monitored, enumerated, and audited, rogue and unregistered devices may creep onto the network. Any such devices which are not secured by the information security team may be leveraged as unsecured access points for targeted malware such as disruptionware.

Industrial Internet of Things Sensors and their Risk

As IT and OT environments converge and become more automated, manufacturing environments are becoming increasingly reliant on industrial IoT sensors and devices which may be unsecured due to a lack of layered security by design, default administrative credentials, or a plethora of other vulnerabilities.

Vulnerable Third and Fourth-Party Networks

Outsourced operations and services often rely on connections to third-party or even fourth-party networks, which may already be infected with malware that can laterally navigate onto critical assets.

Recommendations to Improve Resiliency

As evidenced by the examples referenced in this paper, 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 for the reader to evaluate their 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 has many nuances and specifics and will vary based on your environment and organization.

Develop a Plan

1. **Implement Security-by-Design** – At the core of every organization’s culture should be the principals engrained in NIST SP 800-160 which improve software and hardware resiliency by following a development process that includes continuous testing, responsible coding practices, and adherence to security best practices.
2. **Have an Incident Response Plan** - Stakeholders should collaborate to develop an incident response plan that includes what to do during a ransomware event.
3. **Define Cyber Leadership Roles and Responsibilities:** To be prepared for an attack, identify the security roles and responsibilities of C-level executives such as the CIO, CISO, CSO, and CRO.

4. **Backup Critical Assets:** No matter the situation, it is always a good idea to use a redundancy system that allows multiple iterations of the backups to be saved and stored offline, in case the most recent set of backups includes encrypted or infected files. Routinely test backups for data integrity to ensure you can recover intact data from them.
5. **Test Your Systems:** How long can you afford to have downtime due to targeted disruption? Simulate downtime and system shutdowns to measure how quickly you can revert to failover communication and backup systems. Conduct drills to ensure that personnel know how to respond to emerging threats.
6. **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.

Assess and Monitor Your Network

1. **Inventory Network Assets:** Inventory all assets on every network, classifying them by operating system, type of device, and function. Increasing visibility into the network helps to identify critical assets, detect rogue devices, formulate patching and updating schedules, and develop incident response plans.
2. **Increase Network Visibility:** Take the time to leverage tools and services that increase visibility into networks and systems to identify and mitigate vulnerabilities as well as monitor for any threats infiltrating the network.
3. **Monitor and Audit User Activity:** Audit for unauthorized access attempts, brute forcing, and the use of common penetration testing tools, such as Metasploit.

Practice Strong Cyber Hygiene

1. **Regularly Patch Systems:** Keeping all systems patched, including hardware, mobile devices, operating systems, software, applications, and cloud locations and content management systems can be one of the most critical steps to a secure network. If possible, use a centralized patch management system. Monitor current events and information sharing hubs to keep systems secure against emerging threats. For instance, ensure that patch MS17-010 (CVE-2017-0147) is applied to all systems to protect against SMB exploitation via Eternal Blue. Additionally, be sure to use antivirus and antispyware applications on all devices. Enable regular system and network scans with antimalware applications and configure them to automatically update signatures. Implementing an antispyware solution to stop phishing emails from reaching the network will help prevent users from downloading malware onto your network.
2. **Disable Macro Scripts Where Possible:** Many malware enter the network as malicious attachments that exploit macro vulnerabilities. To limit risk to the organization, 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 full office suite applications.
3. **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. Segment

networks and systems when possible. You should also disable unused ports and monitor and restrict access to ports that cannot be disabled.

4. **Disable Secure Server Message Block 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. Disable the use of SMB, port 445, between endpoints. Where possible, restrict SMB to communication between endpoints and file servers to decrease your risk of infection. Always limit and audit files accessible via SMB shares. Do not forget to patch the Windows MS17-010 (CVE-2017-0147) vulnerability commonly leveraged in malicious attacks.
5. **Manage Third Parties through Service-Level Agreements and Security Auditing:** Vet and monitor third parties who have remote access into your organization's network, as well as your connections to other networks, to ensure everyone connected to your network is as equally diligent with their cybersecurity as you are.
6. **Warn Users About Potential Phishing Emails:** A simple warning banner for all emails from external sources can help remind users of the dangers of clicking on links and opening attachments.

Implement Strong Controls

1. **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. Apply the principle of least privilege and the zero-trust paradigm to minimize risk.
2. **Secure Network Protocols:** Increase security controls for all network protocols that could allow for lateral movement within a network. Disable and block all insecure network protocols such as telnet/FTP/HTTP. Enforce the adoption of https, the latest version of ssh/TLS and other secure protocols.
3. **Implement Application Whitelisting and Software Restriction Policies (SRP):** Though it may not always be possible or practical in OT environments, application whitelists and 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 by limiting lateral adversarial movement. Require firewall validation for inbound and outbound traffic to prevent malicious traffic from entering the network and to detect or halt suspicious traffic requests leaving the network.
4. **Secure Remote Desktop Protocol (RDP) 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 a business purpose. 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 users to VPN. Additionally, you should perform regular checks to ensure the RDP port is not open to the public Internet.

Resources to Combat Disruptionware

The following is a list of publicly available resources which offer tools, frameworks, and guidance to help organizations combat disruptionware. ForeScout and ICIT encourage you to explore these resources. We also thank these organizations for their work:

- [The No More Ransom Project](#) – This initiative from the National High Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre, and McAfee helps 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 organize security technologies by helping 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](#) – A list of technical controls and best practice configurations that can be applied to any environment, this is solely focused on hardening technical infrastructure to reduce risk and increase resiliency. It does not address risk analysis or management like the NIST Cybersecurity Framework.

Conclusion

Organizations with extensive OT networks must act immediately to secure their combined IT and OT networks against the emerging ransomware threat before a single incident metastasizes into a global epidemic. Once enough adversaries adopt disruptionware variants that have proven successful in the public theater, such as LockerGoga, the evolution of threats against manufacturing and other OT heavy environments will escalate. Remember, disruptionware in the form of ransomware, or any other malware tool, is about more than just preventing access to systems and data. It is about suspending operations, disrupting continuity, and crippling the business’s ability to engage in operations, gather resources, and disseminate deliverables. In other words, productivity is the real target.

LockerGoga infections resulted in millions of dollars in losses despite it being an unsophisticated piece of malware. Other threats such as the GandCrab ransomware claim to have earned the developers as much as \$2 billion even after the FBI released the master decryption keys [24] [25]. Once more sophisticated adversaries such as the FIN6 APT evolve the code, or if nation-state sponsored threats such as the Sandworm APT mimic the attack vector with a more sophisticated malware, critical infrastructure firms may not be able to recover from the deluge of threats to their operations. In the interest of national security, policymakers, federal agency leaders, and private sector stakeholders should not delay, but instead, rush to address this emerging threat.

Sources

- [1] "BrickerBot Permanent Denial-of-Service Attack (Update A) | CISA", *Us-cert.gov*, 2019. [Online]. Available: <https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-102-01A>. [Accessed: 09-Aug- 2019].
- [2] "BrickerBot Results in PDoS Attacks (Permanent Denial of Service Attack)", *Security.radware.com*, 2017. [Online]. Available: <https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/>. [Accessed: 09- Aug- 2019].
- [3] "Monitoring Industrial Control Systems to Improve Operations and Security", *Forescout.com*, 2019. [Online]. Available: <https://www.forescout.com/company/resources/monitoring-industrial-control-systems-to-improve-operations-and-security/>. [Accessed: 30- Aug- 2019].
- [4] J. Fruhlinger, "What is Stuxnet, who created it and how does it work?", *CSO Online*, 2019. [Online]. Available: <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html>. [Accessed: 30- Aug- 2019].
- [5] L. Barba, "Greyenergy: The Latest Advanced Persistent Threat to ICS Security - Forescout", *Forescout*, 2018. [Online]. Available: <https://www.forescout.com/company/blog/greyenergy-the-latest-advanced-persistent-threat-to-ics-security/>. [Accessed: 30- Aug- 2019].
- [6] W. Dixon, "How the TRITON Malware Highlights the Need for Tighter OT/IT Collaboration - Forescout", *Forescout*, 2017. [Online]. Available: <https://www.forescout.com/company/blog/triton-malware-highlights-need-tighter-otit-collaboration/>. [Accessed: 30- Aug- 2019].
- [7] T. Nuth, "Malware Keynotes: 4 ICS Cybersecurity Lessons Learned from 2017 - Forescout", *Forescout*, 2018. [Online]. Available: <https://www.forescout.com/company/blog/malware-keynotes-4-ics-cybersecurity-lessons-learned-from-2017/>. [Accessed: 30- Aug- 2019].
- [8] "What You Need to Know About the LockerGoga Ransomware - Security News - Trend Micro USA", *Trendmicro.com*, 2019. [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/>. [Accessed: 30- Aug- 2019].
- [9] R. Abel, "Silex bricks 2,000 plus IoT devices, 14-year-old author has bigger plans for botnet", *Scmagazineuk.com*, 2019. [Online]. Available: <https://www.scmagazineuk.com/silex-bricks-2000-plus-iot-devices-14-year-old-author-bigger-plans-botnet/article/1589112>. [Accessed: 30-Aug- 2019].
- [10] B. Workentin, "Cyber Is Becoming Physical: Ransomware Attack Hits Aluminum Producer Norsk Hydro - Forescout", *Forescout*, 2019. [Online]. Available: <https://www.forescout.com/company/blog/cyber-is-becoming-physical-ransomware-attack-hits-aluminum-producer-norsk-hydro/>. [Accessed: 09- Aug- 2019].
- [11] L. Franceschi-Bicchierai, "Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers'", *Vice*, 2019. [Online]. Available: https://www.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers. [Accessed: 09- Aug- 2019].
- [12] C. Cimpanu, "Norsk Hydro ransomware incident losses reach \$40 million after one week | ZDNet", *ZDNet*, 2019. [Online]. Available: <https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week/>. [Accessed: 09- Aug- 2019].
- [13] P. Paganini, "FIN6 group starts using LockerGoga and Ryuk Ransomware", *Security Affairs*, 2019. [Online]. Available: <https://securityaffairs.co/wordpress/83448/apt/fin6-lockergoga-ryuk-ransomware.html>. [Accessed: 09- Aug- 2019].

- [14] I. Ilascu, "FIN6 Group Diversifies Activity, Uses LockerGoga and Ryuk Ransomware", *BleepingComputer*, 2019. [Online]. Available: <https://www.bleepingcomputer.com/news/security/fin6-group-diversifies-activity-uses-lockergoga-and-ryuk-ransomware/>. [Accessed: 09- Aug- 2019].
- [15] J. Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks", *FireEye*, 2016. [Online]. Available: <https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html>. [Accessed: 09- Aug- 2019].
- [16] L. O'Donnell, "LockerGoga: The Newest Industrial Ransomware Threat", *Threatpost.com*, 2019. [Online]. Available: <https://threatpost.com/lockergoga-ransomware-norsk-hydro-wiper/143181/>. [Accessed: 09- Aug- 2019].
- [17] "New ransomware grows 118% as cybercriminals adopt fresh tactics and code innovations - Help Net Security", *Help Net Security*, 2019. [Online]. Available: <https://www.helpnetsecurity.com/2019/08/29/new-ransomware/>. [Accessed: 30- Aug- 2019].
- [18] "MS-ISAC Security Primer - Ransomware - CIS", *CIS*, 2019. [Online]. Available: <https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware/>. [Accessed: 09- Aug- 2019].
- [19] K. Zurkus, "To Pay or Not To Pay? That Is the (Ransomware) Question", *Dark Reading*, 2019. [Online]. Available: [https://www.darkreading.com/edge/theedge/to-pay-or-not-to-pay-that-is-the-\(ransomware\)-question/b/d-id/1335174](https://www.darkreading.com/edge/theedge/to-pay-or-not-to-pay-that-is-the-(ransomware)-question/b/d-id/1335174). [Accessed: 09- Aug- 2019].
- [20] I. Ilascu, "GermanWiper Ransomware Erases Data, Still Asks for Ransom", *BleepingComputer*, 2019. [Online]. Available: <https://www.bleepingcomputer.com/news/security/germanwiper-ransomware-erases-data-still-asks-for-ransom/>. [Accessed: 09- Aug- 2019].
- [21] C. Cimpanu, "GermanWiper ransomware hits Germany hard, destroys files, asks for ransom | ZDNet", *ZDNet*, 2019. [Online]. Available: <https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/>. [Accessed: 09- Aug- 2019].
- [22] J. Vajayan, "800K Systems Still Vulnerable to BlueKeep", *Dark Reading*, 2019. [Online]. Available: <https://www.darkreading.com/vulnerabilities---threats/800k-systems-still-vulnerable-to-bluekeep/d/d-id/1335286>. [Accessed: 09- Aug- 2019].
- [23] C. Proffitt, "BlueKeep: Havoc on the Horizon Rapid Response: BlueKeep (CVE-2019-0708) - Forescout", *Forescout*, 2019. [Online]. Available: <https://www.forescout.com/company/blog/bluekeep-havoc-on-the-horizon/>. [Accessed: 09- Aug- 2019].
- [24] L. Abrams, "GandCrab Ransomware Shutting Down After Claiming to Earn \$2 Billion", *BleepingComputer*, 2019. [Online]. Available: <https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-2-billion/>. [Accessed: 09- Aug- 2019].
- [25] L. Abrams, "FBI Releases Master Decryption Keys for GandCrab Ransomware", *BleepingComputer*, 2019. [Online]. Available: <https://www.bleepingcomputer.com/news/security/fbi-releases-master-decryption-keys-for-gandcrab-ransomware/>. [Accessed: 09- Aug- 2019].