An Executive Summary of

The Rise of Disruptionware

A Cyber-Physical Threat to Operational Technology Environments

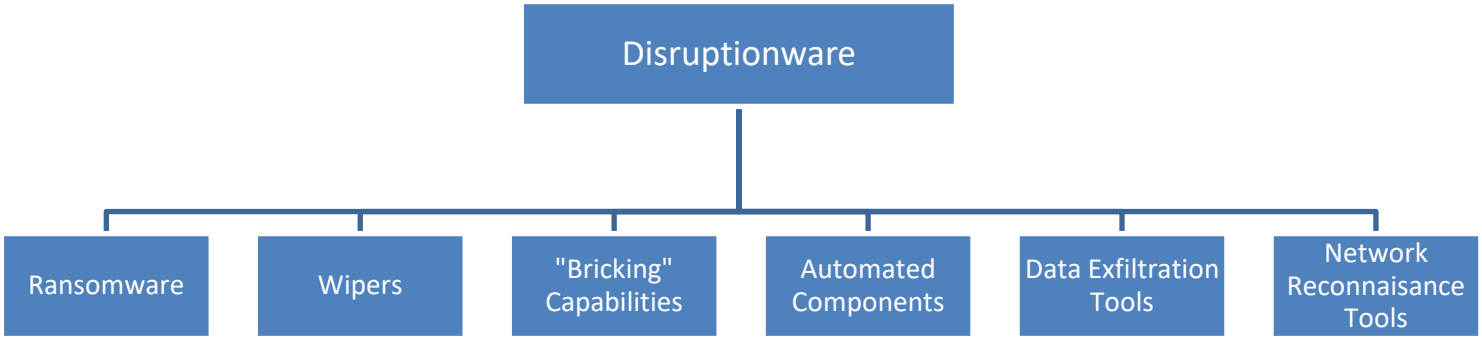
by Ryan Brichant, ICIT Fellow & Global CTO, Critical Infrastructure Cybersecurity, Forescout and Parham Eftekhari, Executive Director, ICIT

Link to Full Report

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