Published on *The National Law Review* https://www.natlawreview.com

Emerging Cyber-Security Threats for 2020: The Rise of Disruptionware and High-Impact Ransomware Attacks

Article By:

Jason G. Weiss

Disruptionware is defined by the Institute for Critical Infrastructure Technology (ICIT) as a new and "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." New forms of disruptionware can be a more crippling form of cyber-attack than other more "garden-variety" malware and ransomware attacks. This is the case since, as the ICIT notes, disruptionware not only attempts to encrypt and deny users access to their data, but works as a "layered attack" designed to "disrupt operations and production in manufacturing or industrial environments (as well as infrastructure) in order to achieve some other strategic goal."

Disruptionware has "consumed" many traditional cyber-attacks, making them part of the disruptioware "toolkit." These techniques include cyber-attacks such as ransomware, "wipers," "bricking capabilities," automated components, data exfiltration tools and network reconnaissance tools. (See ICIT report for further definitions.) Today, the rise of disruptionware is a new and even more chaotic form of cyber warfare attack – it not only attempts to encrypt and deny users access to their data, but disruptionware works to "disrupt operations and production in manufacturing or industrial environments (as well as infrastructure) in order to achieve some other strategic goal."

Additionally, generalized forms of ransomware attacks – designed to block access to the victim's computer systems until money is paid – are continuing to represent a more prevalent threat to government agencies, healthcare providers and educational institutions. Ransomware was so destructive on its own that the FBI recently issued a Public Service Announcement (PSA) warning about such "high-impact" attacks on critical private and public sector institutions. Underscoring the FBI's announcement, another publication has noted the rise of ransomware attacks since the beginning of 2019 finding that there have been at least 621 reported successful ransomware attacks against U.S.-based corporations. Of these attacks, at least 491 were targeted against healthcare providers, while another 68 of the attacks were directed at county and municipal institutions, and 62 of the attacks were focused on school districts.

According to the FBI, hospitals and health care institutions are the primary targets of these high-impact ransomware attacks because of the critical role they play in providing lifesaving services, and the fact that these institutions usually do not have the luxury of taking time to restore backups in order to get their networks working again and running safely and securing after an attack. Above and

beyond the costs associated with paying the ransom and restoring computer networks and systems, ransomware attacks on hospitals and health care providers have proven especially damaging because they affect the ability of the targeted healthcare providers to deliver critical health care services to patients. Perhaps even more disturbingly, many of the victim companies reported losing data even when they paid the ransom demanded by the hackers. Nevertheless, according to the blog "knowbe4," it was predicted that ransomware payments alone by victim companies will have exceeded $11.5 billion in 2019 – representing an increase of almost 30% over the approximately $8 billion paid in 2018.

Along with the rise of disruptionware and high-impact ransomware, hackers are also now using new and diverse techniques to launch multiple forms of cyber-attacks including, among other things, an increased use of new Remote Desktop Protocol (RDP) attacks, as well as leveraging various software vulnerabilities to infect organizations through backdoor channels. Unfortunately, few businesses are hardening their IT infrastructure against these new types of extremely damaging cyber-attacks. RDP attacks are becoming far more common because of the simplicity of many users' login credentials, while companies are not doing enough to "whitelist" exclusively acceptable computer software and applications to prevent security holes caused by numerous software vulnerabilities in unsecured and sometimes untested software applications.

The FBI's PSA serves as a warning to businesses that they should have a plan in place to respond efficiently and appropriately in the event of high impact ransomware and disruptionware attacks. Such plans should include, among other things, clear designations of responsible individuals (both inside and outside the company), procedures for contacting law enforcement, and the business having a firm understanding of what their data is as well as a good understanding of its importance in the overall business plan. Finally, businesses need a current and workable Disaster Recovery Plan for getting the organization up and running again as quickly as possible if there is a cyber-attack. Businesses would be wise to review how their systems are backed up, as reliable and readily accessible backups are often critical in allowing ransomware or disruptionware victims to try and resume normal business operations as quickly as possible.

National Law Review, Volumess X, Number 23