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

Disruptionware V: Malicious Cyber Actors Attack a Florida Water Treatment Facility

Article By:

Jason G. Weiss

We have posted four previous articles discussing the foundation and structure of what a disruptionware attack is, how their attack matrix works, possible defenses to disruptionware attacks and industries that are very susceptible to these attacks. Disruptionware has proven over the last year that it is a growing and dangerous cyber threat to our data, our businesses and possibly our lives.

Disruptionware attacks typically involve ransomware and they aim to encrypt and hold the victim's data hostage. Such attacks are usually financially motivated, and, to date, there have fortunately been only a few known examples where the disruptionware attack has resulted in threats to health and safety or caused loss of life. When such significant collateral damage has occurred, it typically appears to have been inadvertently caused.

A recent cyberattack on a Florida water treatment plant, which has been widely reported in the media, provides a disturbing example of a probable disruptionware attack in which the malicious actors appear to have intended to use their attack to cause physical harm and, notionally, significant loss of life. Based on publicly-available information, it appears that the individual or individuals who engineered the attack on the Florida water treatment facility sought to poison the plant's water supply, which could have led to serious health repercussions and possibly death for numerous people. To the extent these types of attacks – that is, those intended to cause physical harm or death, as opposed to financial harm – become more commonplace, it would represent a serious evolution to the disruptionware threat landscape.

While the threat actors who attacked the Florida water plant apparently did not attempt to lock up or destroy the plant's networks – as is typically the case in "traditional" disruptionware attacks – there is no doubt that the attacker here intentionally penetrated the plant's critical Operational Technology (OT) network in order to gain remote access to and control over the plant's industrial control system network in order to launch their attack. Such an attack is especially dangerous because it compromises the physical infrastructure of the victim, which, in a worst-case scenario, can result in injuries or loss of life.

The recent critical infrastructure attack is yet another reminder that any business or entity can be targeted by cyber attackers, and companies should make every effort to protect their own critical

assets. Disruptionware is already a serious issue for companies, and, as the Florida water treatment attack shows, it is an evolving and increasingly dangerous threat landscape. Companies should be proactive and protect themselves from being victimized by similar critical cyber-attacks.

National Law Review, Volumess XI, Number 48