Water, Water Everywhere – But Nary a Hacker to Blame

pylos.co/2021/02/09/water-water-everywhere-but-nary-a-hacker-to-blame/

Joe

02/09/2021

Multiple entities reported an attempt to dramatically alter operational parameters at a water treatment plant in Oldsmar, Florida in the United States on 08 February 2021. The intrusion and manipulation focused on a municipally-owned treatment facility. As an item of potential coincidence, the intrusion appears to have overlapped with the American football Super Bowl located at Raymond James Stadium in Tampa Bay, Florida – approximately 13 miles away, but served by a completely separate water system. Irrespective of such tangential links, subsequent reporting from Chris Bing identified an externally-accessible Teamviewer instance as the source of the intrusion.

Once inside the network, details are scarce but apparently the entity increased levels of sodium hydroxide in the treatment system. Likely via interaction with a Human Machine Interface (HMI) through the Teamviewer connection, the intruder increased sodium hydroxide levels from 100 Parts per Million (PPM) to 11,100 PPM. Sodium hydroxide, referred to colloquially as lye, is a caustic substance that can cause burns to soft tissues or damage to the lungs when in aerosol form. While commonly used in water treatment operations, at such concentrations as attempted by the entities in this incident, the substance would be harmful to any persons coming in contact with the tainted water. Luckily, operator monitoring of the environment caught the manipulation and mitigated the incident before any harm could result.

Yet for all the concern and mounting hype around this issue, and despite it not resulting in any known significant impact, multiple questions come to mind. Primary in the minds of many would be who is responsible, although personally I am more intrigued by *intent*. Looking at the incident as described in reporting and local press conferences, it appears that the intruder authenticated to the network while it was monitored by personnel, resulting in not only an alarm but quick action to reverse process changes which minimized impact. While we can praise operators for reversing circumstances to prevent harm, the very fact that this was possible presents some curious items for further analysis.

Principally, the lack of alteration to or denial of process visibility and control in this case is curious. As seen in previous industrial-targeting incidents, from the 2015 and 2016 Ukrainian power events to the 2017 Petro Rabigh incident, attackers needed to either remove operator visibility and control (Ukraine) or completely evade operator attention (Petro Rabigh) to even hope to achieve mission success. Alteration of process parameters combined with continued visibility and operator positive control over the environment means that any changes made through remote access can be quickly detected and reversed by engineers and staff. In the case of the Oldsmar water treatment system, operators were not only still able to monitor the environment, but still possessed positive control over operations to quickly catch and prevent any significant adverse effect – a complete and abject failure for the unknown adversary.

Plotted along a continuum of Industrial Control System (ICS) attack maturity, the Oldsmar “attack” seems both primitive and simplistic in nature. Given what limited information is currently available about the incident, the intruder appears to have leveraged an insecure or weakly-protected Teamviewer remote access instance to gain control over the system. Superficially, this would appear no different from two waves of “opportunistic access” activity against water-related systems in Israel during 2020. In these instances, intruders leveraged insecure remote access mechanisms to gain control over several water pumping or treatment systems. While such operations are concerning given adversary brazenness and lack of concern, they also are incredibly unsophisticated in nature – representing a burglar opening an unlocked door more than a thief penetrating a well-resourced security system. While we do not know the particulars of the Oldsmar system at this time, limited evidence and significant experience points to a situation similar to what occurred in Israel, where insecure systems were remotely accessible and entities simply took advantage of circumstances.

So just what the hell was the intruder thinking when they penetrated the relevant control systems? If this was in fact a state-nexus, cyber-physical disruption operation, that actor was both ignorant and incompetent in how to successfully manipulate and undermine an ICS environment. In addition to failing to address operator view and control items, discussed previously, the adversary also entered a completely outlandish value for increasing sodium hydroxide levels – increasing the presence of this chemical by a factor of over 100. While we cannot completely know how this would work within the impacted environment, experience and process awareness indicate such astronomically high values would be identified, flagged, or even mitigated by engineering controls, whether through limiting the release of sodium hydroxide to the system to prevent overloading or triggering a shutdown in response to widely anomalous values. If a state-directed or -sponsored entity is responsible for this event, they should return to their dayjob of DDoS'ing websites and similar low-capability activity, as they've clearly demonstrated a lack of fitness for industrial intrusions.

Alternatively, this intrusion may be the result of something more benign in nature although no less sinister in implication. Especially given Oldsmar's location near the stadium hosting the American football Super Bowl, probing for remotely accessible infrastructure in the general area would appear to be a tantalizing target for an ethically ambiguous researcher or similar entity. While in-depth process and infrastructure analysis would show that the stadium (and its environs) are served by a completely separate water supply, such insights are not available to someone simply browsing Shodan for open access to critical systems. In the course of such exploration, bringing up a logon page is a simple click from the infrastructure scanning services' web GUI – guessing common credentials an ethically significant but technically minor step further, provided any authentication was present on the link at all. While the following is pure speculation, the 11,000 PPM sodium hydroxide increase would seem to represent a "shot in the dark" value change as opposed to any operationally savvy actor's adjustment of values to both maximize damage while minimizing detection. Although such an action would represent a significant degree of callousness and depravity, such a nice, "round" and outrageous number also implies lack of familiarity with the system in question.

Overall, there remain many questions about this incident – but we can be fairly certain of some observations:

1. This event is clearly not on par with past, physically disruptive ICS-targeting events such as the Ukraine power incidents, the Petro Rabigh event, or Stuxnet.
2. Based on available information and observations, this event appears to align more with opportunistic subversion of weakly-protected remote access mechanisms to gain entry to the victim network.
3. Although deeply concerning, the lack of attempts to hide, mask, or otherwise obfuscate operations within the ICS environment not only led to rapid operator intervention to mitigate the incident, but also betrays a significant immaturity and lack of technical understanding on the part of the adversary.

Although concerning for the simple fact that some unknown entity attempted to manipulate the supply of a potentially noxious, corrosive chemical in a community's water supply, the actual details as they are known right now indicate this was hardly a sophisticated or well-planned incident. In the absence of clarifying evidence, this incident appears more aligned with the opportunistic intrusions into Israeli water systems than any other well-planned and thought-out manipulation to industrial control systems for damaging effect.

However – it is worth noting that despite the lack of technical sophistication or even likely basic understanding of the compromised network, some unknown entity still attempted this operation. This observation on its own is deeply concerning and far more significant than the limited technical details of the event in question. That unknown, technically immature entities would not only access a water treatment system remotely but then interact with its controls for chemical dispersal is highly problematic. While our “primary concerns” in critical infrastructure defense will remain sophisticated state-sponsored entities such as Sandworm for the foreseeable future, events such as those which took place at Oldsmar show that there are a number of other, less mature but nonetheless quite concerning entities also probing this space. While their efforts may be lacking or laughable depending on perspective, their intent remains an item of immediate worry – and an item emphasizing that critical infrastructure asset owners and operators must take these threats (even the least competent) seriously.