Surviving Ransomware Attacks: Prevention and Recovery for Water and Wastewater Control Systems

Bob George

Ransomware is now the leading cybersecurity concern for most organizations[1]. The demands to restore encrypted data typically run from tens to hundreds of thousands, if not millions, of dollars[2]. Extortion via ransomware has been a threat for over a decade[3], and yet, today, rarely a week goes by that there aren't headlines identifying that yet another high-profile victim has been affected. While ransomware isn't new, the threat it poses cannot be overstated.

This article summarizes the characteristics of ransomware, how it affects organizations, why it's increasingly perceived as a direct threat to supervisory control and data acquisition (SCADA) and industrial control systems (ICS), and describes basic measures to protect against, and recover from, ransomware attacks.

Understanding Ransomware

To protect against ransomware, it's important to have a basic understanding of what it is and how it can swiftly and effectively affect entire organizations.

- In the simplest terms, ransomware is a class of malware—viruses, trojans, worms, and other cyberattacks—that encrypts accessible files, which can be all files or a specific type of file, and demands payment for a decryption key.
- Ransomware is a particularly effective method of attack. Once the malware has been introduced into a network, no external connection is required to operate or transfer data; everything occurs inside the victim's computers and networks. A single ransomware attack can simultaneously and independently attack multiple victims without consuming attacker resources.
- Pervasive and continuous network connectivity is now the norm in most organizations; networks have expanded faster than the ability to effectively manage and secure them. Poorly secured networks allow access from multiple locations, assuming that anybody on the "inside" can be trusted. It's common to find that even a user with no login can connect to a network and access large numbers of files and systems.

Ransomware has always been moderately successful in that it can rapidly discover accessible networked files and begin encrypting them before detection. What has made it more effective is the incorporation of ransomware into increasingly sophisticated attacks:

- Advanced persistent threats (APTs) are sophisticated cyberattacks that utilize multiple techniques to compromise, discover, infect, and ultimately attack a victim's systems[4]. The first APT that gained widespread public awareness was Stuxnet in 2010[5]. While, at the time, Stuxnet was considered incredibly sophisticated, the techniques it used have become commonplace and are incorporated into toolkits readily available to any would-be attacker.
- Many APT attacks can be launched when the victim simply opens a malicious webpage or a seemingly innocuous email attachment while using a vulnerable

Bob George, CISSP, is the directory of cybersecurity and network infrastructure services with Tetra Tech, headquartered in Pasadena, Calif.

[1] Dan Kobialka, "IBM Security Report: Ransomware Top Cyber Threat in 2020." IBM, 2021. https://www.ibm.com/security/data-breach/threat-intelligence (accessed Sept. 20, 2021).

[2] Steve Lasky, "A Rise in Ransomware Threatens America's Critical Infrastructure." Security Infowatch.com, 2021. https://www.securityinfowatch.com/cybersecurity/article/21228250/a-rise-in-ransomware-threatens-americas-critical-infrastructure (accessed Sept. 20, 2021).

[3] Computer Incident Advisory Capability (CIAC) Information Bulletin A-10.

[4] CISSA, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." CISSA, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a (accessed Sept. 20, 2021).

[5] ICS-CERT, "ICS-CERT – 2010 Year in Review", ICS-CERT, 2011.

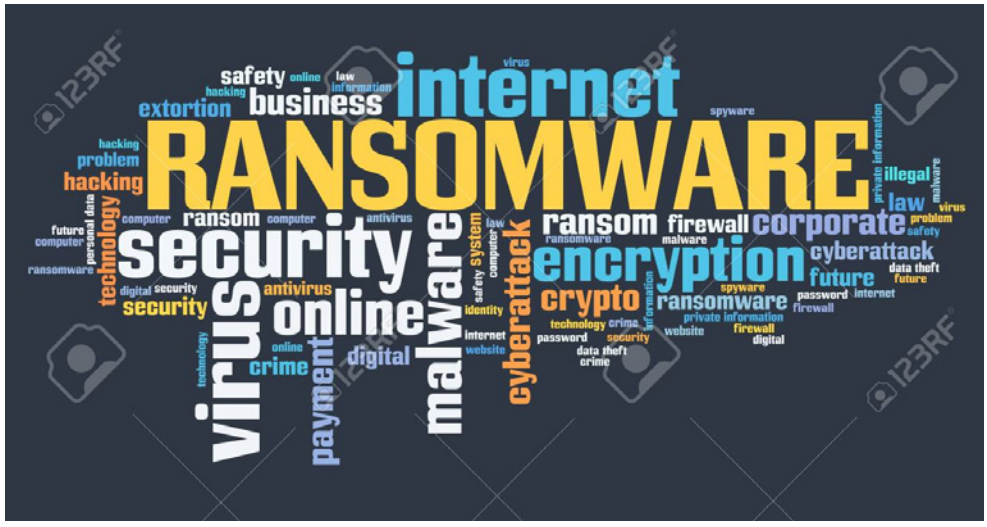
device. This initiates several attack phases, starting from initial compromise of a victim's device to discovery, intrusion, exploitation, and compromise throughout the connected network—within minutes.

- If the victim's computer is moved between networks, APT components will begin searching for vulnerable systems in the new network. While most APT attacks attempt to establish a covert communications channel back to an internet-based command-and-control server, many are fully capable of reverting a brute-force "dumb" autonomous attack mode.
- Cryptocurrencies have reduced the risk to attackers by allowing fully anonymous transfer of funds with no means of tracking transfers, or either party, in the transaction.
- Social engineering has grown increasingly effective as more nontechnical users engage with networked applications and devices daily. Techniques using email (phishing), voicemail, texting, and other communications have become increasingly adept at impersonating official communications, convincing trusted system users to effectively open the door to attackers, bypassing sophisticated network protections.
- Unlike "classic" malware, APT attacks are surreptitious. The days of an attack announcing itself are long gone and attackers go to great lengths to avoid, and in many cases, deactivate detection.

Every modern networked system is potentially vulnerable to some degree to an attack that can spread instantly and effectively throughout any connected system. Traditional models based on "insider" and "outsider" control are ineffective when trusted insiders can become unwitting agents of outsiders. Isolated systems can be attacked through inadvertent introduction of malware via support or contractor laptops. Any internal system that connects externally via email or web browser must be assumed vulnerable.

Ransomware Threats to SCADA and Industrial Control Systems

As APTs have become increasingly sophisticated, they have also become more selective. In the past, SCADA/ICS tended not to be seriously impacted, as only static



program and image files were encrypted, and these were usually backed up. This, however, is no longer true. Criminal enterprises launching APT and ransomware attacks are fully aware of the importance of SCADA/ICS and the technical details of these systems. While stored data is typically only significant from a historical perspective, attackers understand that the inability to operate critical software and devices can have devastating consequences for a utility. New generations of APTs specifically target SCADA/ICS applications, industrial networks, and control system equipment. With the long life cycles of SCADA/ICS and the difficulty of keeping these systems fully patched and protected, critical infrastructure has become a prime target for system-specific ransomware.

A ransomware attack can be more devastating than even a large-scale natural disaster. While storms, fires, flooding, and other natural events are focused in geographic areas, ransomware attacks can engulf connected systems across a much larger area. With no advance warning or preparation time, an entire system can be disabled before any response is possible.

SCADA and Control System Considerations

Simply put, if a SCADA/ICS uses internet protocol (IP)-based communications at any level, it should be assumed to be vulnerable. If an APT doesn't target a system today, it's a safe assumption that threats will emerge in the near future.

A multipronged approach needs to be adapted to protecting a system:

1. Identify the key assets—equipment, software, data, and communications—in a system and prioritize protection of the critical components.
2. Protect against and detect attacks. Traditional cyber protections, such as isolation, access control, and traffic filtering and monitoring, remain primary protections and can do much to delay and contain attacks.
3. Plan for, respond to, and recover from attacks. Resiliency is key. Assume that a system will be hit by a devastating attack and plan accordingly. Assume a system will go "lights out" and be prepared to recognize, respond, and quickly restore everything needed to resume operations.

Without knowing what's critical, effective planning is impossible. Consider the following:

- Transient, time-sensitive traffic. Are any communications essential to system operation? Is central access critical to remote system operation?
- Is any data stored on disk or in a database critical? How important is historical data? What data is required for compliance reporting?
- What programs are essential to system operation? What is required to install and operate these programs?
- What equipment is essential to system operation? What computers and network equipment must be operational?
- Are dongles, drives, removable media, or other items required for restoration at hand?

Continued on page 50

[6] U.S. DHS, "CISA Insights – Ransomware Outbreak." 2019.

Continued from page 49

- Can licensing be installed to sufficiently operate a system on a continuous basis?

Identify the time window in which each critical asset must be restored in order to avoid loss of critical data or operations.

Mitigation Strategies

The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued guidance for basic protection against ransomware attacks[6]. This guidance can be readily adapted and applied to SCADA/ICS in the form of both short-term (immediate) and long-term protections.

Short-Term Priority Mitigation

In order to prepare for a ransomware attack, every utility should verify and, where necessary, implement basic strategies for recovery.

Unsurprisingly, backups are the primary protection against long-term or unrecoverable system disruption. Given the systemwide devastation associated with ransomware attacks, however, backup strategies must encompass recovery on a scale more akin to recovery from a large-scale natural disaster than loss of a single computer or device. Time to restore is key. In most scenarios, every device must be removed from the network and only reconnected once fully wiped and reinstalled, if not replaced outright.

Other considerations include:

- "Saving money" on automated backup and recovery capabilities can literally cost an organization many times any potential savings with the first ransomware event. Recognize that ransomware and APT attacks are a pervasive and ongoing threat.
- Develop strategies for static data (computers and programs) and dynamic data (historical and compliance data).
- Develop and, more importantly, *document* standardized templates for each computer and device type.
  - Try to standardize hardware for each type of device where possible.
  - In many cases, a "gold image" for each type of computer can provide adequate backup, provided it has been tested and is updated regularly.
  - Where standardization is not possible, be prepared to develop separate images for each type of device.
- Regularly update and patch systems in accordance with the SCADA/ICS vendor's recommendations. Develop strategies for timely updates, testing, and deployment of updates and patches. Here again, standardization will greatly improve the odds of successful recovery.
- Backup, and again, *document* programs and system configurations.
- Consider adopting a "bare metal" backup and recovery strategy that allows restoration of everything on the computer, from the operating system to patches and applications, in one step. Traditional recovery by installing a new operating system, then reinstalling applications and restoring data, is inadequate when faced with the loss of every networked computer. Be sure

that such backups can be restored onto whatever hardware platform that can be acquired today. Look for solutions that can detect and restore to dissimilar hardware and can operate largely unattended when support staff is working on multiple computers simultaneously. Consider virtualization strategies to optimize disaster recovery.

- Be sure backups and snapshot images are taken frequently enough that the system can rapidly be restored to full functionality within the target restoration time window. Automate snapshots and recovery whenever possible. The cost of backup media should not limit the ability to back up critical systems and data. Acquire sufficient drives. and media or capacity. to ensure that every critical system can be backed up regularly and without intervention to the extent possible.
- Adopt a backup retention policy that will allow restoration to a point in time weeks or months back. In many cases, APT software can operate for extended periods without detection, and backups may be contaminated. Given the virulence of APT attacks, there is no acceptable level of contamination. The software must be restored to a point *before* the initial compromise.
- Consider adding equipment redundancy. While online redundant systems will typically be equally compromised during an attack, the ability to pull some equipment offline for restoration, while the system operates in a compromised mode, can significantly improve recovery times.
- Add "overlay" security technologies that can be installed and operated without significant disruption of critical production systems. Many cybersecurity solution providers may not be in business over the lifetime of a system. Avoid vendor lock-in by insisting on interoperability with established standards so that equipment can be replaced as needed.
- Develop a "secure interconnect" to provide an authorized means of transferring programs and data, and accessing SCADA/ICS from other networks when, and only if, necessary.
- Require contractors and third-party support to comply with in-house policies and procedures. Eliminate "back door" access, even by authorized support. Require that all external access (if any) use the secure interconnect.
- Test procedures. Verify the ability to restore each system to a fully operational state. Demonstrate the ability to bring back a system without accessing the original (presumed infected) equipment.
- Develop incident response plans that recognize ransomware as a systemwide threat. Incorporate system owners and operators in planning and prioritization efforts.
- Finally, pay attention. Ransomware spreads, and an attack in a utility or organization should trigger an automatic threat awareness. Engage with the Water Information Sharing and Analysis Center (WaterISAC), the only all-threats security

Continued on page 52

Continued from page 51

information source for the water and wastewater sector, and share information with other utilities in the region.

Long-Term Mitigation

Long-term mitigation requires addressing cybersecurity as a core requirement for future system expansions and upgrades. The following steps can be taken to help ensure security for a system:

- Develop a secure network architecture for future system upgrades and replacements. Allow for incremental migration from existing networks to a secure architecture in a phased manner.
- Incorporate user and device access and identity control. Control the introduction of unknown users and equipment onto the SCADA/ICS network.
- Implement robust and secure remote access, if needed.
- Develop cybersecurity policies, standards, and procedures that identify and describe authorized modes of system access and communications. Ensure that access by other means is prevented.

Summary

As ransomware continues to evolve, it's crucial to understand the threat it poses and for organizations to do everything possible to both avoid infection and prepare for recovery. Ransomware can be crippling and decryption is not always an option. The best way to avoid being exposed to ransomware—or any type of malware—is to always plan for and implement defense-in-depth:

1. Identify critical assets.
2. Protect assets by keeping operating systems and applications up to date as best as possible within SCADA system manufacturer guidelines.
3. Implement detection and alarming within and throughout sensitive networks; don't only detect at the perimeter or a single location. Ransomware outbreaks can start anywhere on a system and early detection is key.
4. Develop and test incident response plans so that staff knows how to respond when an incident occurs, regardless of when.
5. Develop and test backup and recovery plans, including the ability to recover and rebuild a system to a state weeks or months in the past.

Resources

Leading cybersecurity resources applicable to water and wastewater SCADA/ICS include:

- NIST SP 800-82 Guide to Industrial Control Systems Security
- WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- DHS CISA Cybersecurity Assessment Tool (CSET) and other services
- DHS CISA Insights – Ransomware Outbreak, Aug. 21, 2019

For more information:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is the leading cybersecurity guidance for assessment and development of a comprehensive cybersecurity program.
- The AWWA Cybersecurity Guidance and Assessment Tool is aligned with the NIST CSF and is recognized for use by water and wastewater utilities.