Implications of IT Ransomware for ICS Environments

By Dragos, Inc.

Published: 2019-04-10 · Archived: 2026-04-05 18:02:31 UTC

ICS environments require reliable, available, and sound processes to ensure continued, safe production. Ransomware – malware that encrypts vital data and disrupts operations – directly impacts these goals, yet historically ICS networks were free of such software. The only example of "ICS targeting ransomware" is a proof-of-concept (or hoax, depending on perspective) from April 2017, never observed "in-the-wild." Yet since that time, ICS asset owners and operators faced several waves of ransomware (or disruptive malware masquerading as ransomware) migrating from enterprise IT to ICS environments: WannaCry; NotPetya; and BadRabbit. In each of these cases, self-propagating ("wormable") malware initially infected IT networks, but through either exploit (particularly the SMBv1-targeting MS17-010 vulnerability) or dynamic credential capture-and-reuse, spread to industrial networks producing significant impacts.

These "inadvertent" and relatively untargeted events (in many cases, actual victims were far removed from initial, intended targets based on unforeseen connectivity between organizations) continue to impact many environments. Recently, these untargeted, self-spreading events were eclipsed by more focused, targeted attacks on IT resources for ICS-operating organizations. Starting with Ryuk in 2018 and proceeding to LockerGoga in 2019, events transitioned from self-spreading, untargeted propagation to more directed, deliberate movement through victim environments. In these cases, adversaries leveraged long-term, persistent access to victim environments to enable privilege and access, using either first-stage or "loader" malware (Ryuk) or compromised legitimate services (LockerGoga) to propagate infections. More concerning still for ICS environments is an evolution in targeting: from Ryuk events targeting municipal utilities (although not spreading to actual production environments) to deliberate targeting of manufacturing environments in the case of LockerGoga.

While ransomware increasingly *impacts* ICS operations, asset owners and defenders must still understand that such malware remains IT-focused in nature and operations. For the wormable variants from 2017, this IT-centric nature is obvious, but more-recent activity such as LockerGoga blurs this distinction due to the impacts of such known events and their seemingly narrow focus on manufacturing-related organizations. Yet many commercial responses stress the "OT focus" of LockerGoga (and recent ransomware campaigns more generally), while also promising the ability to "detect LockerGoga" or whatever is the current ransomware "flavor of the moment." This second point is especially interesting and amusing, as nearly all victims will certainly detect ransomware, as it almost always delivers its "impact" (encrypting files on the victim machine) shortly after infection – thus no entity really needs a special tool to detect such software. Prevention is of course another matter entirely, yet here IT-centric solutions (such as resource-intensive Endpoint Detection and Response, or EDR, products or antivirus running in aggressive fashion against unknown or suspicious files) are either inappropriate for ICS operations or introduce additional risk (through inadvertent clean-up or quarantine of a legitimate file, for example).

Thus, although media and security researchers expended much effort analyzing WannaCry, Ryuk, LockerGoga, and other ransomware types, from an ICS security perspective the keys to defending these networks are far

removed from the ransomware itself. Rather, ICS owners and operators must focus on two enabling steps for opportunistic, ICS-impacting ransomware infections: targeting the mechanisms by which such malware enters the industrial environment; and identifying the attack surface industrial operations expose to infection through IT-centric systems supporting physical processes. Dragos previously addressed these concepts in our initial presentation on WannaCry in 2017, but given continued, and in some ways increasing, attention to the subject of ransomware's impact on ICS operations, such items are reexamined within this article.

First, when viewed through the lens of the ICS Cyber Kill Chain, ransomware represents a final effect for Stage 1 (IT-focused) operation. Focusing on ransomware detection – whether in ICS or IT environments – essentially means defenders cede much space and initiative to adversaries in executing attacks. Based on this perspective, ransomware defense depends less on final-stage mitigation (although recovery planning is vital for the inevitable successful attack), but rather on mid-stage detection and mitigation to prevent final effects on target. While understanding the "how" behind a specific piece of ransomware may be academically interesting, such analysis provides little operational value for defense. Instead, defensive resources are better spent identifying the mechanism through which an adversary can either propagate malware throughout the victim network (wormable infections) or interactively ensure widespread, targeted infection (LockerGoga).

Toward this end, the first step in defending industrial environments from ransomware (or related) infections is not to ensure something like antivirus definitions are up-to-date, but rather to understand just what features of the ICS environment make it potentially vulnerable to infection. "Breaking research" on a specific strain of ransomware is unhelpful at best and breeds a false sense of accomplishment at worst when adopting a realistic view of ICS security. Instead, the mechanisms through which an IT-based infection would propagate to ICS are most important for defense. With WannaCry, SMB links required for migrating historian data to business intelligence systems provided the IT-ICS link – in many cases allowing MS17-010-targeting exploits to migrate into control system environments; for LockerGoga, federated Active Directory installations appear to be the most-likely reason for ICS network impacts. In both cases, connectivity designed to either facilitate or improve the efficiency of normal business practice was weaponized, resulting in disruptive impact in environments otherwise reasonably isolated from enterprise IT.

Defenders must identify links between IT and ICS in advance to grasp the true threat landscape facing their processes and industrial operations. Organizations may do an excellent job in securing interactive links between networks (e.g., enforcing jump hosts or multi-factor authentication [MFA] for remote ICS network access), yet feature other operational links (to business intelligence systems, vendor licensing or remote update servers, remote diagnostics and maintenance services, or similar items) that provide adversaries with a potential ingress route to sensitive networks. Identifying these connections, then either eliminating them where possible or hardening them to the greatest extent allowed provide ICS asset owners and operators with their best, most robust options for mitigating such attacks. For example, it may be necessary to export process data via historians to business intelligence systems residing in enterprise IT – yet such a link need not be bidirectional and can certainly be monitored for and potentially limited to forbid the movement of executable code along this path.

In addition to preventing opportunistic ICS attacks through intelligent, secure architecture and design, organizations must also prepare for breach. In this sense, ICS asset owners must understand that a potentially disruptive infection remains a possibility even after the best, most robust controls are applied to networks. From this residual risk, organizations must plan for response (to reduce the scope or impact of an intrusion) and

recovery (to restore operations to a known, safe state as quickly as possible). Norsk Hydro's response to a LockerGoga infection in March 2019, captured in company-released video, provides an example of what an organization must commit to – in terms of operational pain and contingencies – to ensure continued production in the event of a widespread disruptive network intrusion reaching or impacting ICS operations.

Through these mechanisms, ICS operations can protect themselves from inadvertent or propagating infection events that take advantage of IT-ICS links to produce ICS-relevant impacts. Reacting to truly ICS-targeted ransomware may represent another problem entirely, as a sufficiently motivated (and well-resourced) adversary could pursue operations designed specifically to inflict the most amount of pain for industrial operations: manipulating firmware, encrypting project files, and eliminating access to HMIs and EWs. Yet no such operations exist at this time, and given the level of effort required (and likely law enforcement interest in response) such operations seem unrealistic for the near future. Instead, organizations must prepare for the migration of IT-centric malware to increasingly IT-enabled ICS environments, and learn to mitigate and prepare appropriately.

Unfortunately, uninformed parties will proclaim that increased IT-ICS convergence means that the extension of IT-centric security solutions will suffice to head off this threat. Yet the operational and functional differences between IT and ICS networks (including Windows-based systems in ICS that would appear to resemble enterprise IT deployments) mean that such solutions may present a mirage of defense at best and be counter-productive at worst. As noted earlier in this article, ICS-focused systems, even those that superficially resemble enterprise Windows machines, face an entirely different set of constraints from the typical IT workstation. Vendor warranty requirements, limited processing capability, uptime and throughput necessity, and older operating systems all work against simply deploying the latest EDR or related product or making typical hardening changes. Therefore, rather than expect a direct port of IT security products and best-practices, ICS asset owners and operators must recognize the constraints imposed by the operational requirements of their environment and adapt suitable solutions within these boundaries.

While ICS operators and defenders face unique challenges in protecting their networks in an increasingly connected and interdependent networking environment, such tasks are far from impossible. Scoping the attack surface in advance of events, hardening services where possible, and limiting exposure to business-critical communication pathways can all be combined to significantly reduce the likelihood or impact of opportunistic IT-focused but ICS-impacting events. Further actions, such as heightened network segmentation, traffic limitation, and building an ICS-centric business recovery and continuity plan for cyber-nexus events will further enable organizations to maintain operational resilience and make relatively quick recovery from events possible. Ultimately, organizations must begin planning and taking action now in advance of potential malicious activity to ensure robust, resilient, and defensible networks, while also realizing that IT-centric solutions and chasing the "next headline" in malware are insufficient to foster true defense.
