

TRISIS Malware

Analysis of Safety System Targeted Malware

DRAGO 



Dragos Inc.
www.dragos.com
version 1.20171213

Executive Summary

In mid-November 2017, the Dragos, Inc. team discovered ICS-tailored malware deployed against at least one victim in the Middle East. The team identifies this malware as TRISIS because it targets Schneider Electric's Triconex safety instrumented system (SIS) enabling the replacement of logic in final control elements. TRISIS is highly targeted and likely does not pose an immediate threat to other Schneider Electric customers, let alone other SIS products. Importantly, the malware leverages no inherent vulnerability in Schneider Electric products. However, this capability, methodology, and tradecraft in this very specific event may now be replicated by other adversaries and thus represents an addition to industrial asset owner and operators' threat models.

Why Are We Publishing This?

The Dragos team notified our ICS WorldView customers immediately after validating the malicious nature of the software. Following that notification, the team sent a notification to the U.S. Department of Homeland Security, Department of Energy, Electric Sector Information Sharing Analysis Center (E-ISAC), and partners. We broadcasted to our customers and partners that we would not be releasing a public report until the information became public through other channels. It is Dragos' approach around industrial threats to never be the first to identify new threats publicly; infrastructure security is a highly sensitive matter and the more time the infrastructure community has to address new challenges without increased public attention is ideal. Dragos' focus is on keeping customers informed and ideally keeping sensitive information out of the public where the narrative can be quickly lost and sensationalized. However, once information about threats or new capabilities are made public, it is Dragos' approach to follow-up with public reports that capture the nuance to avoid hype while reinforcing lessons learned and advice to the industry.

Key Take-Aways

- The malware targets Schneider Electric's Triconex safety instrumented system (SIS) thus the name choice of TRISIS for the malware.
- TRISIS has been deployed against at least one victim.
- The victim identified so far is in the Middle East, and currently, there is no intelligence to support that there are victims outside of the Middle East.
- The Triconex line of safety systems are leveraged in numerous industries - however, each SIS is unique and to understand process implications would require specific knowledge of the process. This means that this is not a highly scalable attack that could be easily deployed across numerous victims without significant additional work.
- The Triconex SIS Controller was configured with the physical keyswitch in 'program mode' during operation. If the controller is placed in Run mode (program changes not permitted), arbitrary changes in logic are not possible substantially reducing the likelihood of manipulation.
- Although the attack is not highly scalable, the tradecraft displayed is now available as a blueprint to other adversaries looking to target SIS and represents an escalation in the type of attacks seen to date as it is specifically designed to target the safety function of the process.
- Compromising the security of an SIS does not necessarily compromise the safety of the system. Safety engineering is a highly specific skill set and adheres to numerous standards and approaches to ensure that a process has a specific safety level. As long as the SIS performs its safety function the compromising of its security does not represent a danger as long as it fails safe.
- It is not currently known what exactly the safety implications of TRISIS would be. Logic changes on the final control element implies that there could be risk to the safety as set points could be changed for when the safety system would or would not take control of the process in an unsafe condition

SIS Background

Safety systems are those control systems, often identified as Safety Instrumented Systems (SIS), maintaining safe conditions if other failures occur. It is not currently known what the specific safety implications of TRISIS would be in a production environment. However, alterations to logic on the final control element imply that there could be a risk to operational safety. Set points on the remainder of the process control system could be changed to conditions that would result in the process shifting to an unsafe condition. While TRISIS appears to be focused, ICS owners and operators should view this event as an expansion of ICS asset targeting to previously-untargeted SIS equipment. Although many aspects of TRISIS are unique for the environment and technology targeted, the general methodology provides an example for ICS defenders to utilize when future, subsequent SIS-targeted operations emerge.

Safety controllers are designed to provide robust safety for critical processes. Typically, safety controllers are deployed to provide life-saving stopping logic. These may include mechanisms to stop rotating machinery when a dangerous condition is detected, or stop inflow or heating of gasses when a dangerous temperature, pressure, or other potentially life-threatening condition exists. Safety controllers operate independently of normal process control logic systems and are focused on detecting and preventing dangerous physical events. Safety controllers are most often connected to actuators which will make it impossible for normal process control systems to continue operating. This is by design since the normal process control system's continued operation would feed into the life-threatening situation that has been detected.

Safety controllers are generally a type of programmable logic controller (PLC). They allow engineers to configure logic, typically in [IEC-61131](#) logic. While on their face they are similar to PLCs, safety controllers have a higher standard of design, construction, and deployment. They are designed to be more accurate and less prone to failure. Both the hardware and the software for these controllers must be designed and built to the Safety Integrity Level (SIL) blanket of standards ([IEC-61508](#)). This includes the use of error correcting memories and redundant components and design that favors failing an operation safety over continuing operations. Each SIS is deployed for specific process requirements after a process hazard analysis (PHA) identifies the needs for a specific industrial environment. In this way, the systems are unique in their implementation even when the vendor technology remains the same.

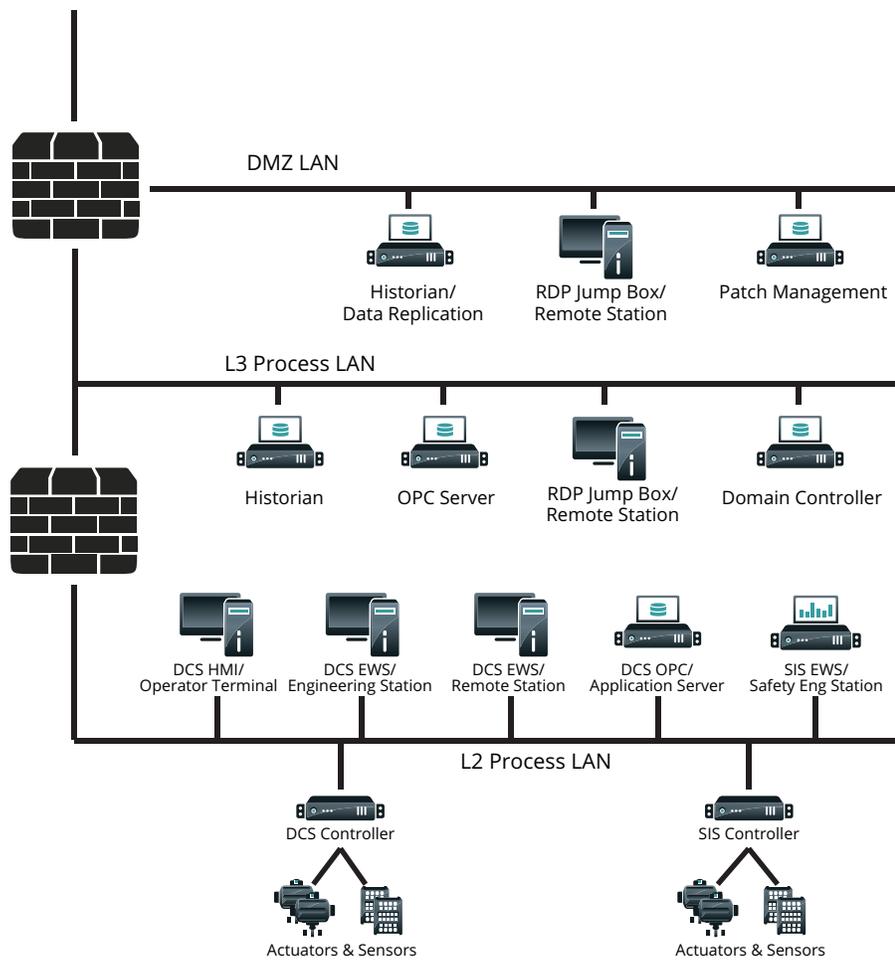
Safety controller components have more flexibility than a typical PLC. A safety controller's output cards will usually have a firmware, and a configuration, which allows the output card to fail into a safe state should the main processors fail entirely. This may even include failing outputs to a known-safe state in the event that the safety controller loses power.

Many safety controllers offer redundancy, in the form of redundant processor modules. In the case of the Triconex system, the controller utilizes three separate processor modules. The modules all run the same logic, and each module is given a vote on the output of its logic function blocks on each cycle. If one of the modules offers a different set of outputs from the other two, that module is considered faulted and is automatically removed from service. This prevents a module that is experiencing an issue such as an internal transient or bit-flip from causing an improper safety decision.

TLP: WHITE information may be distributed without restriction

Safety controller architecture has been debated in the industry. Many end users opt to use the same control LAN for both systems. LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) has identified¹ three distinct integration strategies of SIS with control systems networks. In the case of attacks such as TRISIS, these architectures can be reduced to two, as the security implications of two identified architectures remain the same. End users decide the level of risk that they are willing to accept with their safety system, and use this to determine how tightly they couple their safety system with their DCS (Distributed Control System). A tightly-coupled architecture, shown in figure 1, can provide cost savings, since data from an SIS controller may be incorporated into general operator HMI systems. In addition, network wiring and support is shared between the systems. Sensors data may also be shared, in both directions, between the normal process controllers and the SIS controllers. However, a downside to such an architecture is that attacker who gains access to the Control LAN systems may attack the SIS directly.

Figure 1: Typical (Insecure) SIS integration



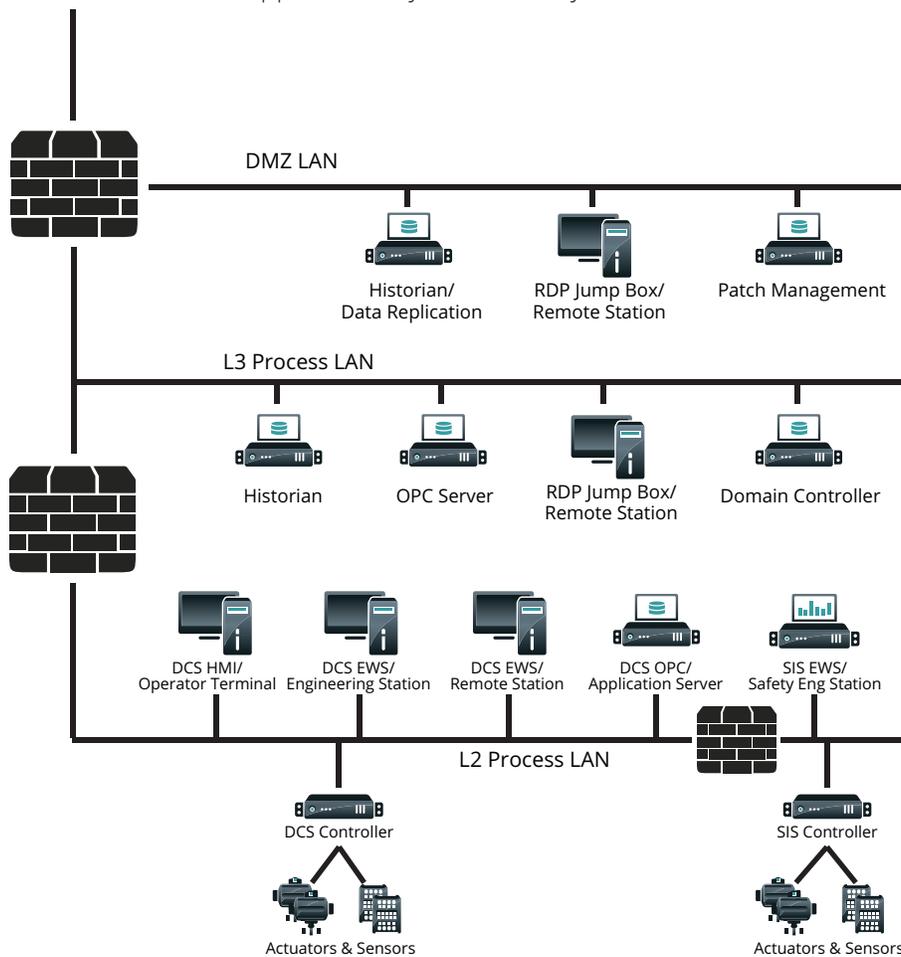
¹ Cyber Security Implications of SIS Integration with Control Networks

<https://www.automationfederation.org/filestore/af/logiic/LOGIIC%20SIS%20REPORT%20for%20ISA%20August%2025%202011%20mod%20jan%202013.pdf>

TLP: WHITE information may be distributed without restriction

This architecture can be especially dangerous when combined with engineering remote access. A common practice at many sites is to allow access to the process control network to engineers via the Remote Desktop Protocol. The engineer will most frequently use their corporate workstation to access an RDP jump box inside of the process control DMZ. From there, the engineering may RDP to either the L3 or L2 process LAN. Compromise of this process, either through an infected corporate workstation or theft of the engineer's credentials, can give an attacker access to the L2 engineering systems. In the case of a tightly integrated DCS and SIS, the attacker then has access to all services of the SIS, including the programming service. The attacker may also be able to gain access to the SIS Engineering Station and gain a better understanding of how the SIS is programmed.

Figure 2: Architecture with application-layer 'Read-Only' firewall between L2 and SIS LAN



TLP: WHITE information may be distributed without restriction

Alternate architectures have been suggested. Many security-conscious asset owners will instrument their SIS Controller with a 'read-only' application-layer firewall as shown in figure 2. These firewalls typically support protocols such as Modbus/TCP or OPC and are specifically designed to prevent the assertion of safety outputs from the process LAN. These firewalls will also prevent access to the proprietary configuration services of the SIS, closing that avenue of attack. Placing both the SIS Engineering Workstation (EWS) and SIS Controllers on the secure side of this firewall will prevent easy access to the SIS programming protocols. In this architecture, an attacker who gains access to the L2 LAN will not be able to impact the safety system, unless the attacker also identifies a weakness in the firewall protecting the SIS from the rest of the L2 Process LAN. A downside of this architecture is that an engineer will need to physically access the SIS workstation to make changes to the safety programming. However, SIS programming changes should be much less frequent than normal DCS updates.

Other methods use data diodes or completely separate safety networks which provide data to the DCS via a DC Controller add-on card. These mechanisms further increase security, although in the case of a completely separate safety network, prevent end users from using potentially valuable safety sensor data for ordinary process control.

A potential attack on SIS can have multiple implications. Two that immediately come to mind and represent most-likely targets include the following scenarios:

Attack Scenario #1: Plant Shutdown

The most likely and operationally easy impact scenario from SIS manipulation or attack is a plant shutdown – and not necessarily due to follow-on physical damage as the result of SIS alteration. There are two general methods of achieving an operational 'mission kill' without physically impacting any element of the target environment:

1. Create operational uncertainty. By altering an SIS where some noticeable effect is produced, even if only recognizing a configuration change or tripping a safety fault where no corresponding physical condition is observed, doubt is introduced into operations as to safety system accuracy and reliability. While the problem is investigated and troubleshooting takes place, operations will likely be significantly reduced if not outright stopped.
2. Trip safety 'fail-safes' to halt operations. Changing underlying logic to enter safety-preserving conditions during normal operations can trip SIS-managed equipment to enter 'fail-safe' modes when such conditions are not actually present. This will lead to a likely halt or stop to the affected process, and likely bring about a much longer shutdown as this scenario rapidly transitions to the item outlined in no. 1 above due to extensive troubleshooting.

Some level of general and plant-specific knowledge is required in order to execute this attack, but the level of knowledge is not as extensive as more fine-toothed, subtle changes to SIS configuration. Simply introducing any noticeable change in the system – which may, through unintended follow-on effects, result in a much more serious issue – results at least in case #1. A slightly more refined approach focusing on specific logic and devices managed can be used to create case #2. Alternatively, an adversary can attempt to leverage insecure authentication to pull existing configuration information from the SIS and simply reverse values to cause safety faults where none exist.

Attack Scenario #2: Unsafe Physical State

Likely the most obvious and assumed attack scenario is creating an unsafe physical condition within the target environment resulting in physical damage to the environment. While this may be the most obvious conceptual attack, the requirements for actually executing make this scenario significantly more difficult – and thus less likely in reality – than scenario #1.

Ensuring an SIS alteration results in physical damage or destruction requires knowledge of the underlying physical processes and controls managed by the targeted SIS. More specifically, knowledge of specific process points where removing a logical fail-safe at the SIS will result in an uncontrolled, damaging physical state – with no complementary physical safety fail-safe in place to prevent damage. The amount of knowledge required specific to the SIS and process installation targeted is significant, and likely not possible to obtain through purely network espionage means. If even possible, the amount of time, effort, and resources required to: obtain necessary environment information; develop and design software tailored to the target environment; and finally, to maintain access and avoid detection throughout these steps all require a lengthy, highly skilled intrusion.

While the above is certainly not impossible – in many ways, it is analogous to the efforts required to launch [CRASHOVERRIDE](#) – the combined requirements make this a less-likely scenario attainable only by highly-skilled, well-resourced adversaries with lengthy timelines. Typical operations safety layering, where SIS forms only part (albeit a large one) in overall safety management, should work to mitigate the worst-case damage a destruction scenario in most instances.



SIS Defense Status

In theory, SIS equipment is isolated from other operations within the ICS environment, and network connectivity is either extremely limited or non-existent. In practice, operational and convenience concerns often result in more connectivity with other ICS devices than ideal, or that ICS operators may even be aware of. An operator may choose to connect a safety controller to their wider plant network in order to retrieve data from the controller to facilitate business intelligence and process control information gathering. This carries the risk that the safety controller may be affected by malicious network activity, or accessible to an intruder that has penetrated the ICS network.

Safety controllers generally have the same security profile as a standard PLC. Controller projects offer password protection; however, projects typically contain two backdoor accounts by default that the user has no control over. While suboptimal from a security perspective, such accounts are vital to ensure administrator-level access and control over the device in an emergency situation. A reverse engineer with moderate skill may uncover these accounts and use them to gain unauthorized access to the project and to the safety controller.

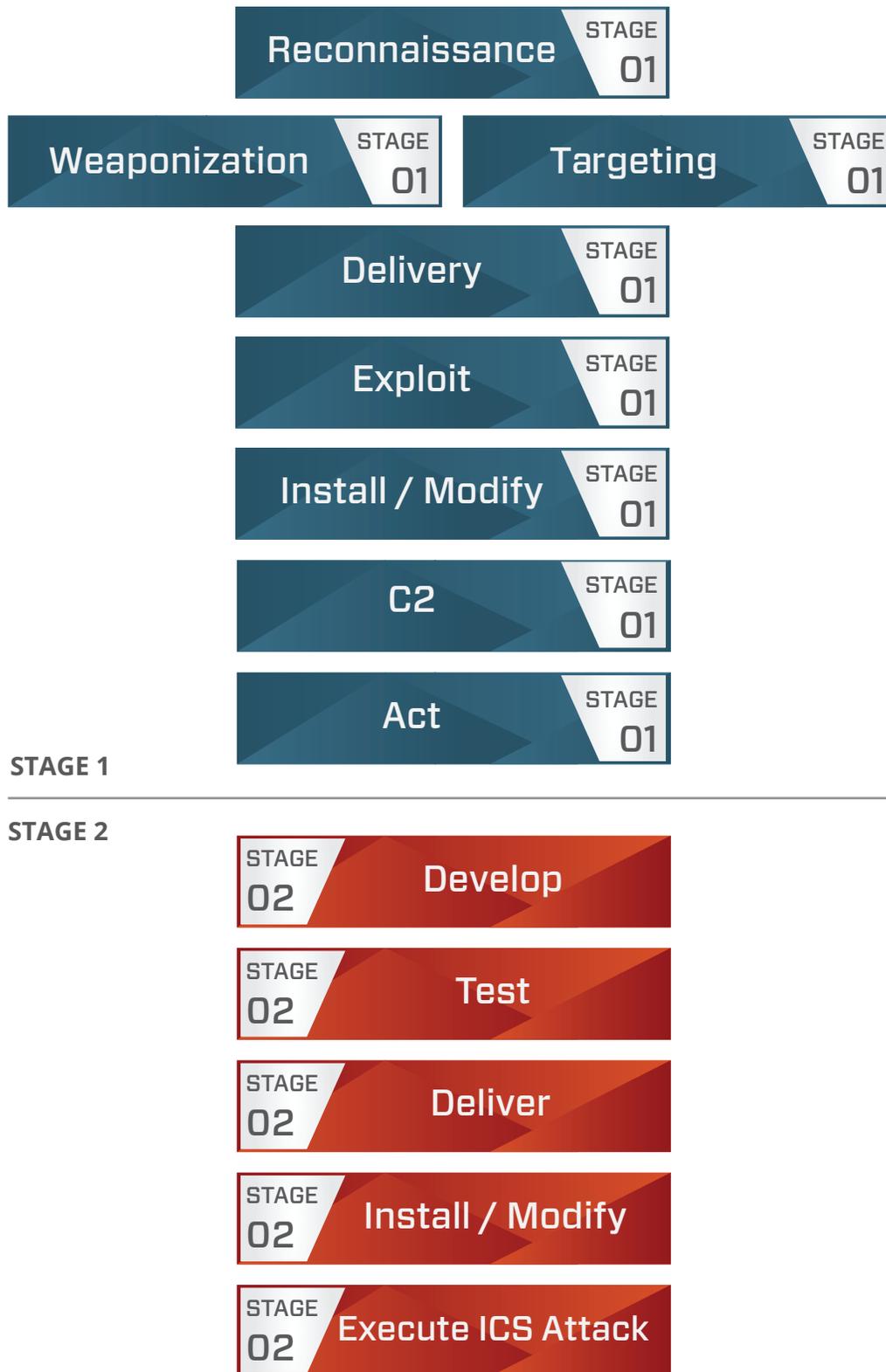
While common to many SIS devices, the newer versions of Schneider Electric's Triconex units are not susceptible to this attack. The older controller (which was deployed at the victim site) is protected by following the deployment recommendations, listed below, to prevent arbitrary changes in SIS functionality via a physical control. Newer model controllers removed the backdoor accounts entirely and added X.509 mutual authentication to the controllers.

Examining SIS devices generally, backdoor accounts cannot typically be disabled due to the operational need for the reasons outlined above. SIS network isolation is critical in preventing abuse of this feature in vulnerable devices it is appropriate to monitor connections to such systems more so than blocking activity without an understanding of the impact.

TRISIS Capabilities

TRISIS is a Stage 2 ICS Attack capability, as defined by the ICS Cyber Kill Chain as shown in figure 3. Given its design and assessed use, TRISIS has no role or applicability to IT environments and is a focused ICS effects tool. As a result, TRISIS' use and deployment requires that an adversary has already achieved success in Stage 1 of the ICS Cyber Kill Chain and either compromised the business IT network or has identified an alternative means of accessing the ICS network. Once in position, the adversary can deploy TRISIS on its target: an SIS device.

Figure 3: ICS Cyber Kill-Chain



TRISIS is a compiled Python script using the publicly-available 'py2exe' compiler. This allows TRISIS to execute in an environment without Python installed natively, which would be the case in most ICS environments and especially in SIS equipment. The script aims to change the underlying logic on a target SIS – in this case, a Schneider Electric Triconex device. Subsequent code analysis indicated the script is designed to target Triconex 3008 processor modules specifically. The executable takes its target as a command-line argument passed to it on execution. The implications of this are specifically in targeting at run-time, unless called through an additional script, and based on a review of the code, limiting TRISIS to impacting a single target per execution.

The core logic alteration functionality works through a combination of four binaries that are uploaded to the target SIS:

- Two embedded binary payloads within the compiled Python script.
- Two additional, external binaries that are specifically referenced by name within the script but located in separate files.

Dragos analysis indicates that the embedded items are used to prepare and load the external modules, which contain the replacement logic. As part of a general attack flow, an adversary would need to take the following steps to deploy and execute TRISIS as shown in figure 4 on the next page.



Completion of Stage 1 of the ICS Cyber Kill Chain:

Identify and gain access to a system able to communicate with target SIS.

Stage 2 Develop:

Identify target SIS type and develop TRISIS with replacement logic and loader

Stage 2 Test:

Ensure TRISIS works as intended, likely off network in the adversary environment

Stage 2 Deliver:

Transfer TRISIS to the SIS which contains the 'loader' module for the new logic and support binaries that provide the new logic

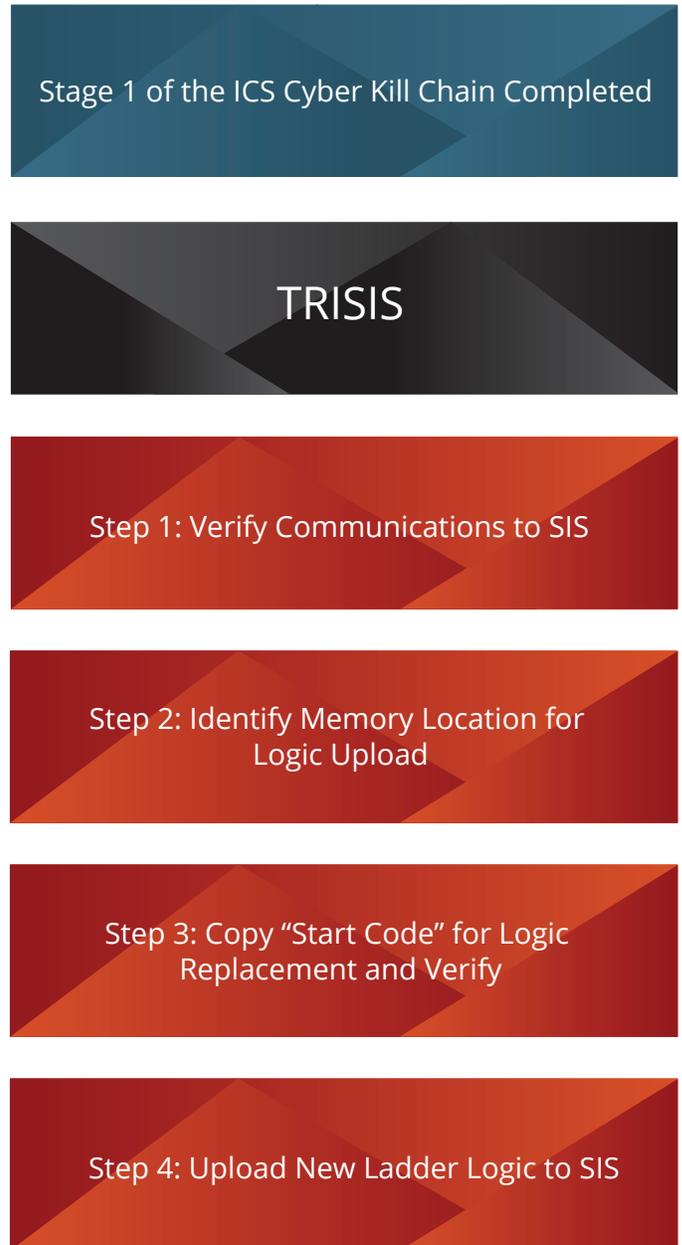
Stage 2 Install/Modify:

Upon running the TRISIS executable, disguised as Triconex software for analyzing SIS logs, the malicious software utilizes the embedded binary files to identify the appropriate location in memory on the controller for logic replacement and uploads the 'initializing code' (4-byte sequence)

Stage 2 Execute ICS Attack:

TRISIS verifies the success of the previous step and then uploads new ladder logic to SIS

Figure 4: TRISIS Attack Flow



TLP: WHITE information may be distributed without restriction

Based on the description above, TRISIS itself represents a facilitating capability or framework for the actual ladder logic change that has the potential, as outlined in the scenarios above, to alter the environment. As such, TRISIS itself could be repurposed to deliver alternative payloads to either deliver different logic files (the external binaries uploaded by TRISIS to the target SIS) or to utilize differently embedded binaries to target different SIS types entirely. While both are quite plausible, the work involved would be significant and represents the largest amount of effort and required resources for TRISIS efficacy: ensuring that the embedded binaries identify the correct portion of SIS memory for replacement ladder logic upload, and then developing appropriate ladder logic for the target system. Neither of these is trivial, and make scaling or spreading this attack to other environments – and potentially the same Triconex devices but in different installations – extremely difficult.

Dragos was not provided with the external binaries used in the TRISIS attack, and we are therefore unable to determine what precise impact would result on the victim SIS. Nonetheless, any modification to SIS in an operational environment represents a significant risk and potential for damage or even loss of life. The precise attack path is also unknown at this time, but based upon available information and functionality of TRISIS, the target SIS must be network accessible from a device the adversary was able to compromise and establish reasonably persistent command and control over. As a result, TRISIS activity – from initial installation through periodic control followed by ultimate payload delivery – represents multiple steps across Stages 1 and 2 of the ICS Cyber Kill Chain.

While TRISIS as a Python program allows for some level of flexibility in that different modules could be referenced or included to provide different effects, as an attack vector such alterations are difficult to execute in practice for the reasons outlined above. As such, TRISIS is a very focused, target-specific malware that would not be capable of delivering equivalent effects in another environment without significant modification.

An additional point to emphasize is that no real vulnerability or exploit is utilized by TRISIS. Rather, TRISIS functionality depends upon understanding how Triconex SIS devices function and specifics about the process environment. With a full understanding of these items, the adversary then must design and deploy ladder logic to create the desired impact on the target SIS.

Implications

TRISIS represents, in several ways, 'game-changing' impact for the defense of ICS networks. While previously identified in theoretical attack scenarios, targeting SIS equipment specifically represents a dangerous evolution within ICS computer network attacks. Potential impacts include equipment damage, system downtime, and potentially loss of life. Given these implications, it is important to ensure nuance in how the industry responds and communicates about this attack.

First, adversaries are becoming bolder, and an attack on an SIS is a considerable step forward in causing harm. This requires the industry to continue its focus on reliability and safety by pursuing appropriate and measured steps towards securing industrial processes. Information technology security best practices are not necessarily appropriate to such situations and an ICS, and a mission-focused approach must be taken into consideration of secondary effects.

Second, the attack of an SIS cannot be taken lightly but should not be met with hype and fear. Eventually, information about this attack will leak to the media and public community. At that point, those in the industrial security community can have a nuanced conversation noting that this attack is not a highly scalable attack that has immediate repercussions to the community. Or simply stated, the public nor government should invoke fear. The industrial asset owner, operator, and vendor community have had a significant dedication to safety and reliability, and now it is obvious that the community is taking steps forward in security. Dragos cautions the community not to use this attack to further other causes as the impact of hype can be far-reaching and crippling. TRISIS is a learning moment to push for more security but in a proper and measured way.

Third, this attack does have implications for all industrial asset owners and operators that leverage SIS. The fact that Schneider Electric's Triconex was targeted should have no bearing on how defenders respond to this case. This was a clear attack on the community. There can be no victim blaming or product shaming that is reasonable nor will it make the community better. The implication is that adversaries are targeting SIS and defenders must live in this reality presented adapting as appropriate to ensure safety and reliability of the operations our society depend upon.

Defending Against TRISIS

SIS system implementation should begin with relevant vendor recommendations. The recommendations surrounding methods on network isolation are especially critical to preserving SIS autonomy. In the case of TRISIS, Schneider Electric has provided the following recommendations for Triconex Controllers

- Safety systems should always be deployed on isolated networks.
- Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment, or the safety network.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All Tristation terminals (Triconex programming software) should be kept in locked cabinets and should never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network such as CDs, USB drives, etc. should be scanned before use in the Tristation terminals or any node connected to this network.
- Laptops that have connected to any other network besides the safety network should never be allowed to connect to the safety network without proper sanitation. Proper sanitation includes checking for changes to the system not simply running anti-virus software against it (in the case of TRISIS no major anti-virus vendor detected it at the time of its use).
- Operator stations should be configured to display an alarm whenever the Tricon key switch is in the “Program Mode.”

It is important to understand that TRISIS represents only the second stage of the ICS Cyber Kill Chain. This report does not infer or suggest what stage 1 of the attack may be and instead focuses on what has been confirmed through capability analysis. This puts defenders in the position of not stopping activities prior to impact but during or after the SIS impact. Keep in mind there is a wide range of defenses to detect and stop the attacker prior to exposing human safety and equipment during stage 1 and earlier stage 2 phases.

Stage 2 ICS Attack: Delivery

TRISIS requires being executed from a host that can directly communicate with the SIS controller(s). In figure 1 cited above any host on L2: Process LAN can serve this purpose. This allows more options for the attacker and greater scope of what needs to be defended. Delivery of TRISIS to any one of these hosts may be accomplished through network transfer or USB/media transfer.

- Strong architecture can deter, delay or detect adversarial actions as they deliver TRISIS from another network to a host that can communicate to the SIS environment. This is traditional network concepts of segmentation through firewalls, dual factor authentication of interactive access, etc.
- Once architectural foundations are in place, both active and passive defenses are needed. Automated log collection, passive network collection provides the basis of information needed for forensic analysis after an event while strong tailoring of firewalls may limit/prevent delivery or minimally serve as a triggering event for defenses to investigate and respond.

Stage 2 ICS Attack: Install/Modification

Once TRISIS resides on a host that has direct access, it is now in a dormant state until either the attacker or unwitting user executes the binary. Once the TRISIS package is on the host, there are several options for the defenders to stop or detect it proactively.

- If the network architecture were already revised to limit what hosts can communicate to the SIS, then the number of hosts that can successfully run TRISIS against SIS has already been reduced. Again, this limits the attacker's options while allowing more focused security controls. Strong mechanisms to limit removable media can be considered- both technical (USB whitelisting or outright disabling of USB ports) or administrative (enforcing scanning of a USB drive prior to usage in production equipment) are valuable. Strong filesystem permissions or execution whitelisting technology become much easier to implement for engineering workstations or hosts that have access to communicate with SIS.
- Reliance on traditional signature-based detection (antivirus) is not sufficient. At the time of discovery, TRISIS was undetected by all antivirus engines. Instead, a more proactive approach is required. For instance, Worldview customers were provided Yara signatures to identify TRISIS. Those signatures also detect any binary compiled with py2exe as any such tool within an ICS or SIS environment is an outlier and immediately suspect.
- Additional proactive baselining can also occur. Hosts such as engineering workstations are often not well managed. They generally are not part of Active Directory and have the option of running a wide range of agents. However, baselining of known files, applications, services, USB insertions, and user accounts can find deviations that could detect TRISIS files on the system. This can offer assurances of the limited number of hosts that can communicate to the SIS.

Stage 2 ICS Attack: Execute

The execution of the TRISIS attack can be broken down into two components: the launch of the process on the host and the network communications from the compromised host to the SIS controller(s).

Architecturally limiting the TRISIS executable to run on the host via execution and/or hampering its ability to communicate to the controllers via windows host firewall would stop any impact.

Additionally, proactive detection – such as identifying when a host is communicating with an SIS controller can serve as an alarm. Even with strong architectures, misconfigurations occur that may allow a host that shouldn't have access to an SIS to communicate to it. Such alarms, even if they fail to stop an attack, are vital to understanding and isolating the cause of the attack.

SIS environments can be some of the most defensible systems. They are largely simplistic and static- usually the most static of any ICS environment. However, good architecture, passive defenses, and active defenses are key to understand when an attack is in progress and how to repel when the attackers use novel techniques. There is no such thing as an undetectable or unpreventable cyber attack, and as defenders, it should be a priority to secure and monitor the safety systems responsible for protecting human life, the environment, and the physical processes.

Dragos applies expert human intelligence and behavioral analytics to redefine industrial control system (ICS) cybersecurity. Its industry-first, ICS/OT cybersecurity ecosystem provides control systems operators with unprecedented situational awareness over their environments, with comprehensive threat intelligence, detection, and response capabilities. Dragos' solutions include the Dragos Platform, providing ICS/OT-specific threat detection and response; Dragos Threat Operations Center, providing ICS compromise assessment, threat hunting, and incident response services; and Dragos WorldView, providing global, ICS-specific threat intelligence. Headquartered in metropolitan Washington DC, Dragos' team of ICS cybersecurity experts are practitioners who've lived the problems the industry faces hailing from across the U.S. Intelligence Community to private sector industrial companies.

FAQ

Who Did It?

Achieving a level of confidence on attribution is not as difficult as often positioned. However, achieving a high confidence of attribution can be incredibly difficult without access to a significant set of data or a long period of historical analysis across numerous intrusions into victim environments. Infrastructure attacks are often geopolitically sensitive topics that can carry real considerations between states. In addition, there is little to no value in true attribution (state, agency, or operator identity) to defense teams. In many cases, attribution can actually negatively affect defense teams. Due to the lack of value to defenders and the ramifications of incorrect attribution Dragos does not comment publicly on attribution.

Is TRISIS a Big Deal?

TRISIS is the fifth ever publicly known ICS-tailored malware following STUXNET, HAVEX, BLACKENERGY2, and CRASHOVERRIDE. It is the first ever publicly known ICS-tailored malware to target safety instrumented systems. For these reasons, it is of significant importance to the ICS community, and it should be analyzed fully to capture lessons learned. The malware is not capable of scalable and long-term disruptions or destruction nor should there be any hype about the ability to leverage this malware all around the community. Attacks on an industrial process that are as specific in nature as TRISIS are considerably difficult to repurpose against other sites although the tradecraft does reveal a blueprint to adversaries to replicate the effort. However, because SIS are specifically designed and deployed to ensure the safety of the process, environment, and human life an assault on one of these systems is bold and unsettling. While fear and hype are not appropriate in this situation, this is absolutely an escalation in the types of attacks we see against ICS and should not be taken lightly.

Could This Attack Lead to Loss of Life?

Yes. BUT, not easily nor likely directly. Just because a safety system's security is compromised does not mean it's safety function is. A system can still fail-safe, and it has performed its function. However, TRISIS has the capability to change the logic on the final control element and thus could reasonably be leveraged to change set points that would be required for keeping the process in a safe condition. TRISIS would likely not directly lead to an unsafe condition but through its modifying of a system could deny the intended safety functionality when it is needed. Dragos has no intelligence to support any such event occurred in the victim environment to compromise safety when it was needed.

What are the Indicators of Compromise?

Dragos supplied Yara rules to our ICS WorldView customers to help defenders scope their environments for this or similar malware. However, indicators of compromise (IOCs) are not appropriate in most cases for industrial threats and capabilities. Technical data is often not similar in adversary capabilities between victims. Defenders should instead focus on defense recommendations and the adversary tradecraft and techniques.

I Do Not Use Triconex Should I Care About TRISIS?

Vendors targeted in specific malware implementations such as Schneider Electric with TRISIS are victims. The malware was not designed because Triconex was a good choice for this attack; the malware would have been designed because the intended victim was using Triconex. If the victim was leveraging a different type of SIS, it is reasonable to conclude the malware would have targeted a different vendor. Therefore, defenders should instead focus on monitoring their environments and being aware of how they have SIS configured if it's deployed according to best practices, and the ability to respond if there was an issue detected with the SIS. The Triconex connection is specific to this malware, but the lessons learned apply to anyone using safety systems.

What Questions Should Executives Ask?

Executives should ask, and thus their security teams should anticipate these questions, questions such as: Do we have an SIS and if so where and what type(s)? If we needed to collect data from the environment or validate the system has not been modified could we? If the SIS is disrupted is there a cybersecurity component to the processes in place to determine root cause analysis and if an attack has occurred? Do we have an incident response plan that factors in the loss of the SIS even if it does not immediately lead to an unsafe situation? Is our SIS properly segmented off of the network and if not what monitoring do we have in place to ensure it is not impacted?

I Want to Speak on or Write About Safety Instrumented System Security What Should I Know?

Please ensure you talk to a certified safety engineer. The security of SIS is important, but safety engineering is a very specific skillset. What seems feasible and nuanced from security professionals may not fully represent the reality of the situation. I.e., please avoid sensationalist writing on the subject by including both security and an engineering input. There have been presentations and topics at information security conferences on safety systems before that impress generalist audiences but are known to the community to be inaccurate or simplistic; fantastic research but not holistic in how it is often implemented or discussed. What that translates into is the "what is possible in a given scenario" should have an expert on the threat and an expert on the SIS speaking.