TRISIS: Analyzing Safety System Targeting Malware

dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/

December 14, 2017

Whitepaper

By Robert M. Lee

12.14.17

Today, the Dragos, Inc. team is releasing a report titled TRISIS: Analyzing Safety System Targeted Malware. TRISIS is malware that was developed and deployed to at least one victim in the Middle East to target safety instrumented systems (SIS). Dragos, Inc. found and analyzed the malware last month and made sure our ICS WorldView customers were aware and prepared with proper defense recommendations. We did not make news of this malware public because it is in our policy not to be the first to disclose ICS targeted malware or threats. Our reasons for this revolve around the fact that releasing such information can have a blow back effect on the industrial community. ICS threats are commonly hyped up in the public and the asset owners and operators are hit with trying to deal with the consequences of that while also trying to gather how they will prepare and respond to the threat. Additionally, informing the public about the threat also reveals to the threat what we know and can help the adversary be more effective. This is a delicate balance though because there is value in informing the larger community for lessons learned and information sharing as well. This puts security vendors in a difficult choice at times where there is no right answer. Our choice though looking at the balance from our perspective is only to publicly talk about threats, even if we find them first in the community, after someone else talks about it or the information leaks to the public. This allows our reporting to focus on the “so what” factor and the nuance of the issue as well.

The key takeaways from the report and things to know about TRISIS:

- 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 which resulted in operational impact
- 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

- 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 malware must be modified for each specific victim reducing its scalability
- The Triconex SIS controller had the keyswitch in 'program mode' during the time of the attack and the SIS was connected to the operations network against best practices. In a proper configuration and with the controller placed in Run mode (program changes not permitted) the attackers would face a more difficult challenge implementing the attack. Hindsight advice is not appropriate to apply to future attacks, but it is important to always try to reduce the effectiveness of adversary attack vectors.
- Although the malware 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 skillset 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 danger as long as it fails safe.

The TRISIS malware is a very significant event for the community as the fifth ever ICS-tailored malware and the first to directly target SIS. It is a very bold attack while not technically complicated. The Dragos team intends for our report to ensure the proper nuance and recommendations to the community are captured. Our threat intelligence customers of our ICS WorldView reports can access the Dragos Intelligence Portal to get further information and technical details. We will continue to analyze and report out on this malware and its developments as well. Good luck to the community and always remember that defense is doable. If you missed the TRISIS Webinar you can watch it here.

VIEW MORE RESOURCES

Read our next whitepaper

whitepapers

CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids

Dragos, Inc.

View more whitepapers

Ready to put your insights into action?

Take the next steps and contact our team today.

CONTACT US TODAY