Bow Tie Model of Destructive Malware - ICS Historian Case Study

*By: Bryan Owen - **OSIsoft** & Lubos MIcoch - **OSIsoft***
*Dan Michaud-Soucy - **Dragos** & Josh Carlson - **Dragos***

Overview

Industrial Control System (ICS) environments are inherently hazardous based on high energy and reactive chemicals often used within them. ICS owner/operator staff have long understood the essential need to recognize the various hazards within the environment and then prioritize them with an associated mitigation strategy.

Bow Tie models put hazards directly into focus and provide a risk assessment framework to analyze causal relationships within various environments. The model helps identify relevant threats, defenses against those threats, impacts, and methods to reduce those associated impacts from creating an adverse event related to the hazard. Selecting effective barriers can reduce both the likelihood of the event and lessen the impact of the event should it take place.

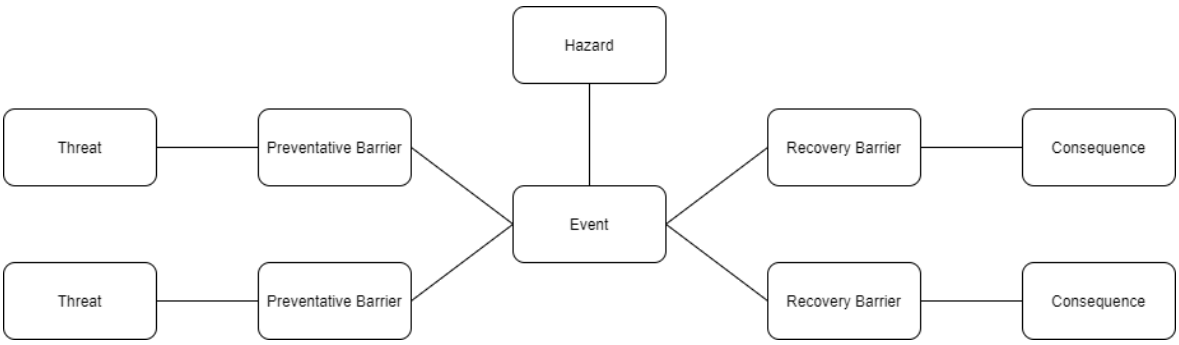
This article and the follow-up webinar describe a case study using the Bow Tie methodology for historian technology commonly found in ICS environments. We chose to focus on historian technology for our case study for two reasons. First, historian deployment is often prominent at the boundary between Stage 1 and Stage 2 ICS cyber attack. We strive to model defenses for hazards at the transition from enterprise to ICS environment. A secondary reason is that sensor data is short-lived unless recorded in a historian. Destructive attacks on historian data could result in unrecoverable losses if not well defended.

Destructive malware, specifically ransomware and wipers, have become an increasing danger that affects the entire ICS community of interest. Destructive malware is the hazard for our analysis, and a compromised historian server is the top event for this case study.

We hope the content provided in this article and the subsequent webinar will serve as a practical reference for owners/operators and others to leverage as they explore using the Bow Tie methodology. By following the techniques outlined, specific threats, impacts, and barriers are cataloged that identify reasonable steps an organization could take that lead to improvements in the system's reliability and resiliency during a risk assessment.

Sidebar: Why Bow Tie? Bow Tie methodology is 'lingua franca' for analysis of industrial hazards. Successful application to industrial control system security has received attention at ICSJWG and other forums listed in acknowledgments. This case study helps identify bridges

between Bow Tie analysis and popular ICS taxonomy, including MITRE ATT&CK for ICS and FAIR.



Methodology Overview

This case study is the collaborative effort product with analysis conducted in rapid ideation sessions where identification and the threats, consequences, and barriers constructed the basic Bow Tie. The case study analysis was informed by actual incidents (and near misses) of historian server compromise by destructive malware and related experience from subject matter experts.

Threats

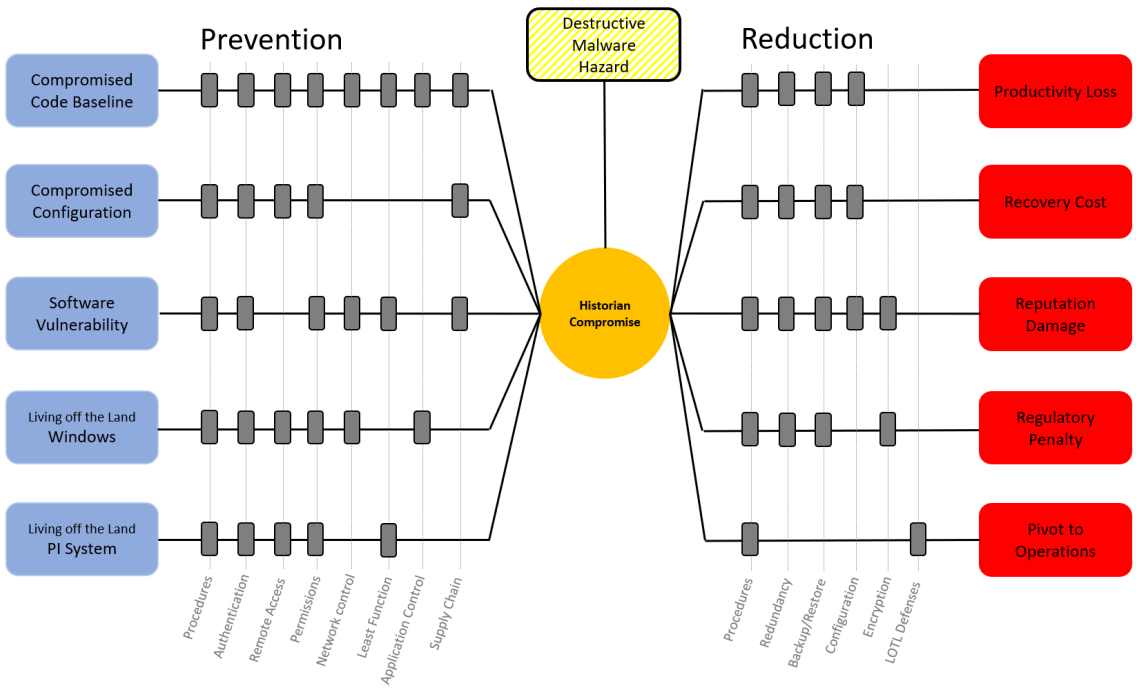
Inspiration for the threats identified in the model came from the Electric Power Research Institute Technology Assessment Methodology framework and its taxonomy for exploit objectives, particularly the execution of malware/unauthorized code (“code baseline”) and unauthorized changes to configuration (“configuration baseline”). A threat titled “vulnerability” was added to highlight barriers to help prevent potential exploitation of vulnerabilities in the underlying software separately from thwarting abuse of by design features (also known as ‘living off the land’). Living off the land threats related to the built-in operating system and historian tools & features is identified in the model.

Consequences

Factor Analysis of Information Risk (FAIR) loss model categories inform the Bow Tie model’s consequences. Two specific losses are broken out as separate categories. The first extra is loss due to payment of a ransom in a category labeled “extortion” which proved useful for identifying otherwise unique barriers. A category labeled “externality cost” was also added to highlight potential loss due to complex interdependence with other critical service providers.

Barriers

As various barriers, also known as controls, are identified, they are categorized as either; Preventative or Recovery. Preventative barriers are located on the Bow Tie diagram's left-hand side and positioned between the threat and the top event. These barriers identify opportunities for mitigating the likelihood of the event occurring at all; in other words, they must have the capability to terminate the threat sequence and not just reduce it.
Recovery barriers are located on the right-hand side of a Bow Tie diagram and positioned between the top event and a consequence. recovery barriers seek to reduce the scale of the consequence severity (impact), and possibly prevent some or all of the undesired consequences should the top event occur. Those characteristics are an essential point to understand when going through a Bow Tie analysis; recovery barriers under consideration only need to reduce the associated consequence, not necessarily stop the sequence before the consequence (impact) is fully realized.
Barriers can also be influenced by and mapped to the MITRE ATT&CK mitigations. In some cases, this mapping is straightforward: The Multi-factor Authentication preventative barrier maps directly to M1032 (Multi-factor Authentication). Other barriers map to many different types of mitigations, for example, during our analysis Access Control mapped to M1018 (User Account Management), M1026 (Privileged Account Management), M1036 (Account Use Policies), M1043 (Credential Access Protection), and several others.



Analysis Highlights

Prevention

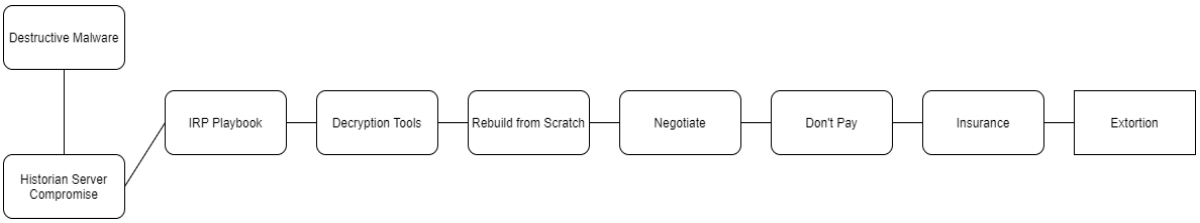
A highlight of this case study is the observation of a barrier that was found broadly applicable and useful for all identified threats and many potential consequences. The barrier involves the practice of severing network connections in response to elevated threats. Similar to how drawbridges are retracted to protect a medieval city and its citizens, understanding how and when to disconnect cyber assets from the rest of the network is a capability that is worth the effort. Having the ability to sever historian network connections aligns wells with zone and conduit requirements in ISA/IEC 62443 with potential for orchestration described by DoE Cyber-Intrusion Auto-Response Policy and Management System project. Furthermore, most historians support degraded modes, including the capacity to buffer data when disconnected. We highlight this barrier even though effectiveness tends to be short-lived. To extend the medieval analogy, raising the drawbridge eventually fails in the face of a siege.

Recovery

On the Bow Tie recovery side, a well-executed incident response playbook (IRP) seems like the most obvious way to reduce the overall impact should the top event occur. For this case study, it is essential to avoid common mistakes in handling incidents that could leave a gap, such as a potential pivot to operations. The Bow Tie model strives to align with guidance described in CISA Alert “Technical Approaches to Uncovering and Remediating Malicious Activity” (AA20-245A) and “NCSC Mitigating malware and ransomware attacks - How to defend organizations against malware or ransomware attacks.” Furthermore, while having the IRP well developed is the first step, actually walking through some tabletop exercises (TTXs) that leverage the IRP helps to build a foundation for cyber heroes within the organization. The more this skills development process happens, the more likely these individuals can consider things that otherwise might go undiscovered until a real event occurs.

To pay or not to pay?

Given the specific focus event of a destructive piece of malware (i.e., ransomware) compromising a historian system, our analysis eventually led us down the path of considering whether paying the ransom would be an acceptable outcome to reduce the consequences of our event. Ultimately, the asset owner has a choice to make, and the decision should be rooted in safety and company mission with consideration of legal and ethical obligations. For example, a pharmaceutical company that manufactures high demand, life-saving medication facing this same scenario and cannot recover the system could consider paying the ransom. On the other hand, if the asset owner has to rebuild the system, and there are no life-threatening or safety considerations, it may make more sense not to pay the ransom.



Summary

Overall, the Bow Tie is a structured brainstorming activity that allows teams to systematically analyze existing or desired barriers between threats and consequences to prevent or mitigate a significant event. By visualizing the various threats, prevention and recovery barriers, and consequences, the results are a map that is easy to read, showing the controls an organization can leverage to manage risk levels for the historian. Multiple management level communication is possible with this map as decisions about whether the current level of control is sufficient or if additional resource investments are necessary to reduce the impact potential to an acceptable level.

The identified hazard of destructive malware affecting a historian system within an ICS environment is a genuine risk for many organizations today, so it was chosen for this case study. Often, controls can be seen as a “set and forget” type of thing. By leveraging this Bow Tie analysis, organizations can now raise awareness and improve staff understanding of the barriers in place, including the importance of operating and maintaining those barriers over time. It is essential to reiterate that while Bow Tie and associated TTXs are a great tool to leverage, no matter how much planning, training, or contingency plans exist, there will be some surprises when the event happens, which need to be recorded in the Bow Tie for future reference.

The collaborative engagement between OSIsoft and Dragos in developing this Bow Tie for destructive malware in ICS environments focused on historian systems provided valuable insights. A webinar outlining the process and a walkthrough of some highlights will be occurring on November 19th. We encourage asset owners, operators, and frontline defenders who support critical enterprise to attend, provide additional inputs, and operational use cases into the collaboration to help validate this analysis further.

Acknowledgments

SANS - Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology by Rebekah Mohr
https://www.sans.org/reading-room/whitepapers/ICS/evaluating-cyber-risk-engineering-environments-proposed-framework-methodology-37017

SANS - The Industrial Control System Cyber Kill Chain
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

FAIR loss model
https://cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model_FINAL_Web%20Only.pdf

Global Cybersecurity Alliance - ISA/IEC 62443 Zones and Conduits
https://gca.isa.org/blog/how-to-define-zones-and-conduits

Cyber-Intrusion Auto-Response Policy and Management System
https://www.sce.com/sites/default/files/inline-files/CyberIntrusionAutoResponse_PolicyManagement.pdf

CISA Alert (AA20-245A) Technical Approaches to Uncovering and Remediating Malicious Activity
https://us-cert.cisa.gov/ncas/alerts/aa20-245a

NCSC: Mitigating malware and ransomware attacks - How to defend organizations against malware or ransomware attacks
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#limittheimpact

Microsoft Transform - Hackers hit Norsk Hydro with ransomware. The company responded with transparency
https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

OSIsoft PI Square - Bow Tie for Cyber Security (0x01): How to Tie a Cyber Bow Tie
https://pisquare.osisoft.com/groups/security/blog/2016/08/02/bow-tie-for-cyber-security-0x01-how-to-tie-a-cyber-bow-tie

EPRI Technical Report 3002012752 - Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1