Malware Types and Risks in IT, ACS, and OT Environments

By Daniel Ehrenreich

The following describes cybersecurity attacks that it may be experienced in IT, or Automation and Control Systems (ACS) environments. It also discusses what may be required to recover after such an attack, and what measures may be taken to mitigate the effect of these attacks.

RANSOMWARE

Malicious software that gains access to sensitive information within a system, and encrypts that information so the user cannot access it.

Introduction

Industrial Automation and Control Systems/Operation Technology (ACS-OT) cyber security practitioners were traditionally educated to worry about cyber-attack vectors, such as those directed against the organization's IT Zone. None can be blamed for that misunderstanding because Ransomware, Distributed Denial of Service (DDoS), and exposure of confidential information are all IT-directed attacks. When I asked, "Is ACS-OT Directed Ransomware at Purdue Levels 1&2 likely to happen?" most instantly thought about incidents like the Colonial pipeline, Norway Aluminum, JBS meat, etc. After a few moments of thinking about the technological aspects of the ransomware processes, most replied, "Yes, it Can." From a technology point of view, they were right. When I asked if they would pay $10 to receive the decrypting key to restore the encrypted HMI or PLC, knowing that professional attackers are expecting payment of millions for the decrypting key, all replied, "Yes, for such an amount, I will not hesitate". However, when I explained that most of the published incidents related to industrial operations were IT-directed ransomware attacks, they agreed to spend 10 minutes listening.

This paper does not deal with cyber-attacks such as manipulating the PLC or the HMI programs or placing a logic time bomb in the system, but it aims to explain why ACS-OT-directed Ransomware (delivery of the decrypting key for money) is unlikely to happen.

IT Ransomware Attacks	**ACS-OT Ransomware Attacks**
Ransomware directed attacks involve encrypting databases and programs, but not everyone knows that a ransomware attacker may demand a ransom payment in three phases. 1) When such an attack occurs, IT users receive a red-screen message indicating that the database was encrypted and that they	Technically, the encrypting process may also work in that zone. This assumption is correct, but we must elaborate deeply on it. Data stored in the ACS-OT zone is usually not confidential (!), except in systems that run a secret technological process (food, pharma,

cannot operate the business processes. Organizations that hold up-to-date backup files for the data and a Golden Image for the processes may refuse to pay the ransom and restore the business operation. Upon receiving that disappointing message, the attacker might reply, “I leaked all your data, including privacy information, and if you disagree to pay, I will publish or sell the information.” Now, the backup files are useless, and the organization must negotiate. When the attacker feels the payment will arrive soon, his appetite might grow and send you a new message: ”I also have information on all your customers, suppliers, and their details. If you do not pay extra, I might attack them as well, and they will blame you”. Ransomware attacks are a highly profitable “business operation,” and professional attackers expect to receive high ransom payments for the two or all three demands explained above.	etc.). Therefore, a “smart attacker” will not invest in exfiltrating operation-related data from the ACS-OT zone. Once an attacker decides to penetrate the ACS-OT zone, he might do that to manipulate the process, cause an operation outage, or damage or risk lives. This can be done through an internally or externally generated cyber-attack or through the supply chain. Furthermore, we often say that once an attacker penetrates the ACS-OT zone, “Game-is-Over” because he can harm the system within minutes, manipulate the database and/or the process, causing an outage, damage, or risk lives.
Restoration of the ACS-OT zone IT zones are almost always where hackers will have developed and tested their malware. Provided that encryption and decryption were correctly conducted and the attacker delivered a reliable decrypting key, there is a good probability that having paid the ransom, the target files and databases may be recovered. Some companies do have a policy of not paying ransomware blackmailers, but it is technically feasible.	**Restoration of the ACS-OT zone** Technically, decrypting the ACS-OT database and the process files is possible, assuming the encryption was correctly conducted and the attacker delivered a reliable decrypting key. However, remember, you cannot trust that assumption for ACS-OT! Consequently, any part of the decrypted ACS-OT system that an attacker earlier encrypted for receiving the ransom might not operate safely. You may obtain the decrypting key if you wish, but you cannot use it for a system that controls a critical safety-oriented process. Obviously, these recommendations apply to safety-oriented systems. If you deal with simple processes such as counting produced packages in a warehouse or collecting data

	from mechanical utility meters, you may try to restore the operation with the decrypting key if you are confident that it will comply with the SRP (Safety-Reliability-Performance) Triad. ACS-OT operations must be periodically evaluated according to the SRP Triad. If you cannot be assured that the restored ACS-OT will safely operate, you must clear the affected zone (PLCs, HMIs, Control Servers, etc.), reinstall all appliances from a stored Golden Image, and copy the required operational data from the Historian Server. After that, you must perform in-depth testing of the repaired system. Complete system reinstallation is your only choice!
Mitigation of IT Risks Cybersecurity monitoring systems….	**Mitigation of ACS-OT Risks** Secure Interfaces between IT and ACS-OT networks. Perform in-depth testing of the repaired system. Complete system reinstallation is the preferred choice!
Conclusions **Non-industrial Operations…..**	**Conclusions** Industrial operations must be prepared to ensure business operation continuity with increasingly interconnected (negligently converged) architectures between the IT and ACS-OT zones and a growing amount of communicated data across the organization. To achieve the desired cyber security goals, the IT and OT experts must collaborate to correctly select and deploy the cyber defense measures. The role of management at industrial and utility-related facilities is to allocate the needed resources and hire manpower to be at least one step ahead of attackers.

Daniel Ehrenreich, BSc.

is a consultant and lecturer acting at Secure Communications and Control Experts (SCCE) and periodically teaches and presents at industry conferences on the integration of cyber defense with industrial control systems; Daniel has over 33 years of engineering experience with ACS and OT systems for electricity, water, gas, and power plants as part of his activities at Tadiran, Motorola, Siemens, and Waterfall Security and is an active member of several ISA-IEC 62443 Workgroups. Daniel was re-selected as Chairperson for the **9th ACS CyberSec 2025** conference in Israel on 8-1-2025.

Source LinkedIn.