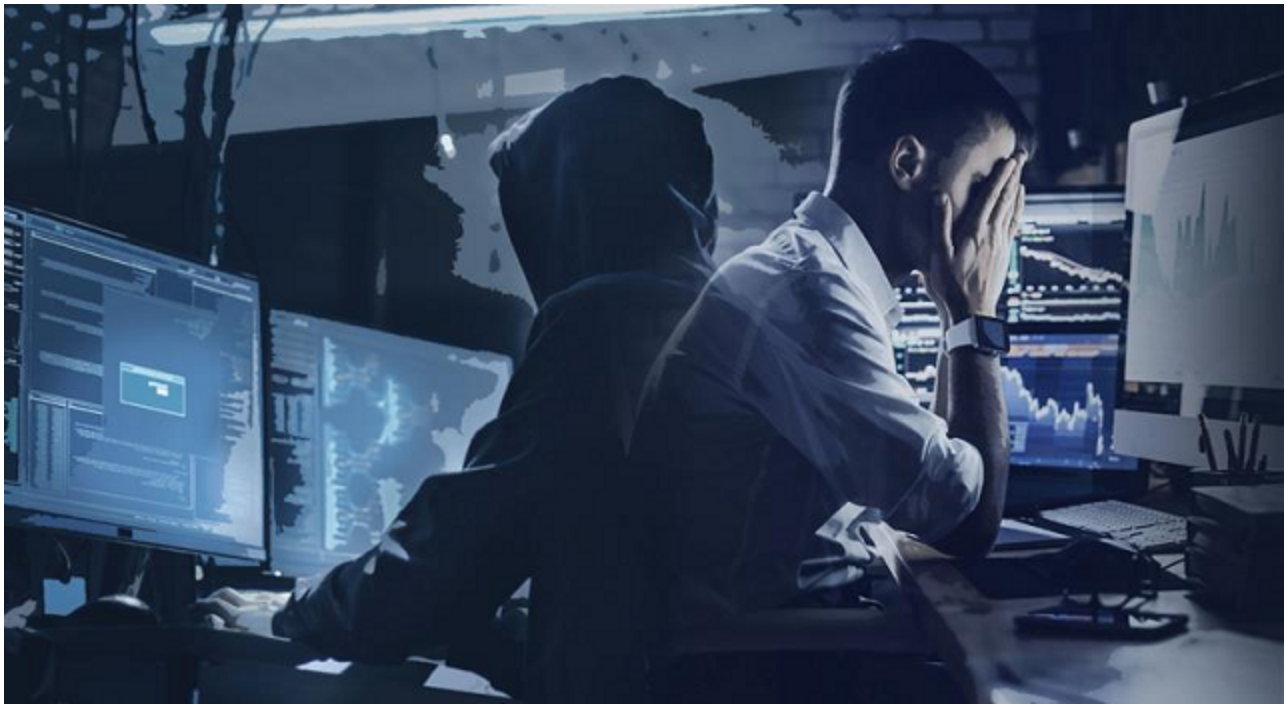
The Impact of Modern Ransomware on Manufacturing Networks

trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html

December 1, 2020



As a graphical interface, HMIs are extremely reliant on image files. Every button, value, logo, pipe, and piece of equipment represented in the HMI has a corresponding image file somewhere in the HMI software's directory. Not only that, configurations that contain values, mappings, logic, thresholds, and lexicons are stored in text files alongside the image files. In one ransomware incident that affected an HMI, we found that 88% of the encrypted files were JPEG, BMP, or GIF files — the images used by the HMI to render the interface. If all of these files were encrypted, recovering the affected systems would not just end with a reinstallation of the ICS software. Additionally, the custom HMI or SCADA interface would need to be restored as well.

Take note that ransomware does not need to directly target the ICS software's processes in order to incapacitate the ICS. By encrypting the files that the HMI, SCADA, or engineering workstation (EWS) depends on, ransomware can render the system useless, resulting in both a Loss of View and Loss of Control scenario for the operator, and ultimately, Loss of Productivity and Revenue for the factory.

Theft of Operational Information

Networked file sharing is practically a necessity in manufacturing environments. On the operational side of things, engineers and designers use it not only as a means to share design and engineering documents that they are working on, but also as a repository for reference files, guidelines, parts lists, tooling, and workflow.

On the business operational side of things, managers and staff use network shares to store information about vendors, suppliers, purchase orders, invoices, and the like. A dedicated supply chain management (SCM), and/or product life cycle management (PLM) system and its associated databases could even be found on Level 4 or 5.

Although a ransomware attack that affects these file repositories and databases would not necessarily disrupt the production line, it would hamper business operations, supply chain management, and product engineering and design. Unfortunately, those are only the short-term consequences. Modern ransomware operations also involve data theft, which leaves a permanent impact.

In a trend started by the Maze ransomware, it is now almost standard practice for ransomware groups to steal data from their victims, utilizing off-the-shelf file backup tools to do the job. Initially, the purpose of this was to increase the likelihood of payment by the victim, as the data leak allows for the additional threat of blackmail. However, data from ransomware victims is also being leaked to or sold in the underground. This is particularly unfortunate for enterprises since design and engineering documents could contain intellectual property. In addition, vendor and supplier information could contain confidential supply chain data such as pricing and order information.

Manufacturing companies should consider these possibilities in case they ever face a ransomware incident. Once the production and business operations are restored, an assessment of stolen data needs to be done. Afterward, organizations should ask themselves a painful question: If the data is leaked or sold, what would the repercussions be for production, business relationships, and customers? The answers to this would guide an organization's post-mortem actions and enable a more effective response strategy.

Post-Intrusion Ransomware

Over the years, there has been a dramatic decrease in incidents of ransomware arriving as email attachments or being installed through malicious websites (see Figure 4). However, judging by news headlines, many might think that the amount of ransomware being distributed at large has not decreased at all.

Ransomware

Ransomware threats have disrupted the manufacturing industry significantly in 2020. In a disturbing trend during the third quarter of the year, attackers appeared to be singling out manufacturing organizations as a victim of choice in their ransomware operations.

By: Ryan Flores December 01, 2020 Read time: (words)

Content added to Folio