The Impact of Modern Ransomware on Manufacturing Networks

By Trend Micro (words)

Published: 2020-12-01 · Archived: 2026-04-05 23:43:49 UTC

Ransomware threats have disrupted the manufacturing industry significantly in 2020. These attacks have resulted in substantial losses in production and disjointed operations. 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. Data from Trend Micro™ Smart Protection Network™ shows how ransomware threat actors have affected different industries.

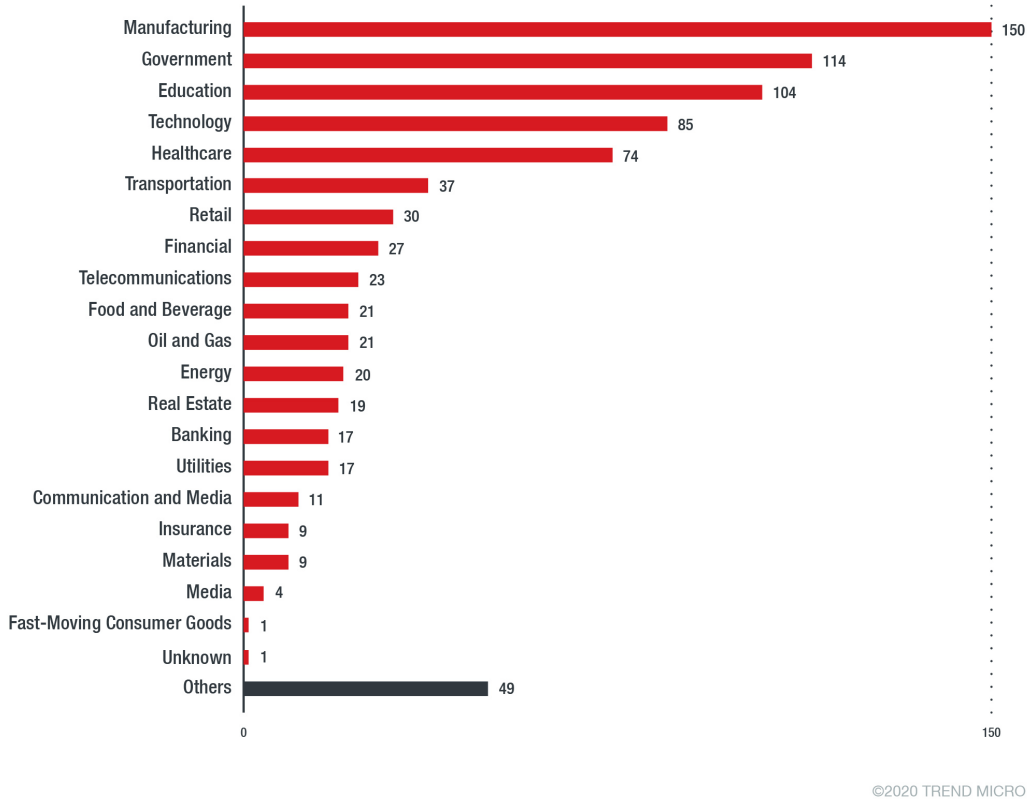
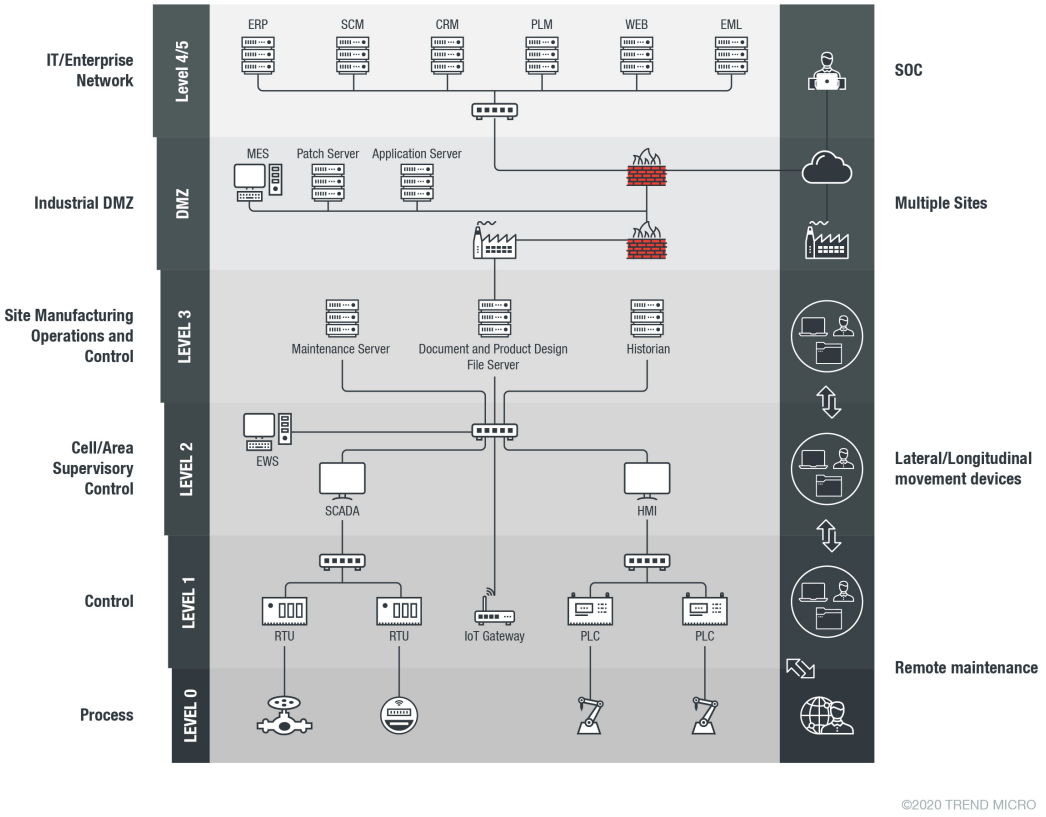


Figure 1. Industries affected by ransomware in Q3 of 2020 (data from Smart Protection Network)

Manufacturing facilities use big physical machines — assembly lines, furnaces, motors, and the like — but both the advancement of technology and the trend of Industry 4.0open on a new tab have also meant that computers have been introduced into production and operation systems. These big industrial machines are controlled or monitored by computers; these computers, in turn, are connected to other computers and networks in order to pass around data.

Figure 1 illustrates the architecture of an Industrial Control System (ICS).



Level 0 is where the big pieces of hardware are. These are the machines that normally come to mind when one thinks a factory or a power plant.

However, to control and monitor these machines, the computers on Level 2 are necessary. The human-machine interface (HMI) and supervisory control and data acquisition (SCADA) computers give the operators visibility and control of the industrial machines, while the engineering workstation contains the blueprints, design documents, robot codes, programs, and configurations that are needed to create the final product.

In many cases, a centralized file server containing the design files and product documents for shared access between engineering workstations can be found on Level 3, as well as the historian, a historical database that contains equipment, performance metrics, and product quality.

What happens if a ransomware attack is able to penetrate the computers on Levels 2 and 3?

Loss of View and Loss of Control

Modern ransomware is not designed to shut down or cripple infected machines. The last ransomware that effectively decommissioned infected computers was Petyaopen on a new tab, which was active in 2017 and 2018. The ransomware families that came after were more careful in their file encryption, purposefully excluding system files and executable files, as these are needed by the computer to boot and operate. Everything else is encrypted. This means that there would be no abrupt shutdown in the factory floor if ransomware were to hit any of the control and monitoring computers in the operational technology (OT) network.

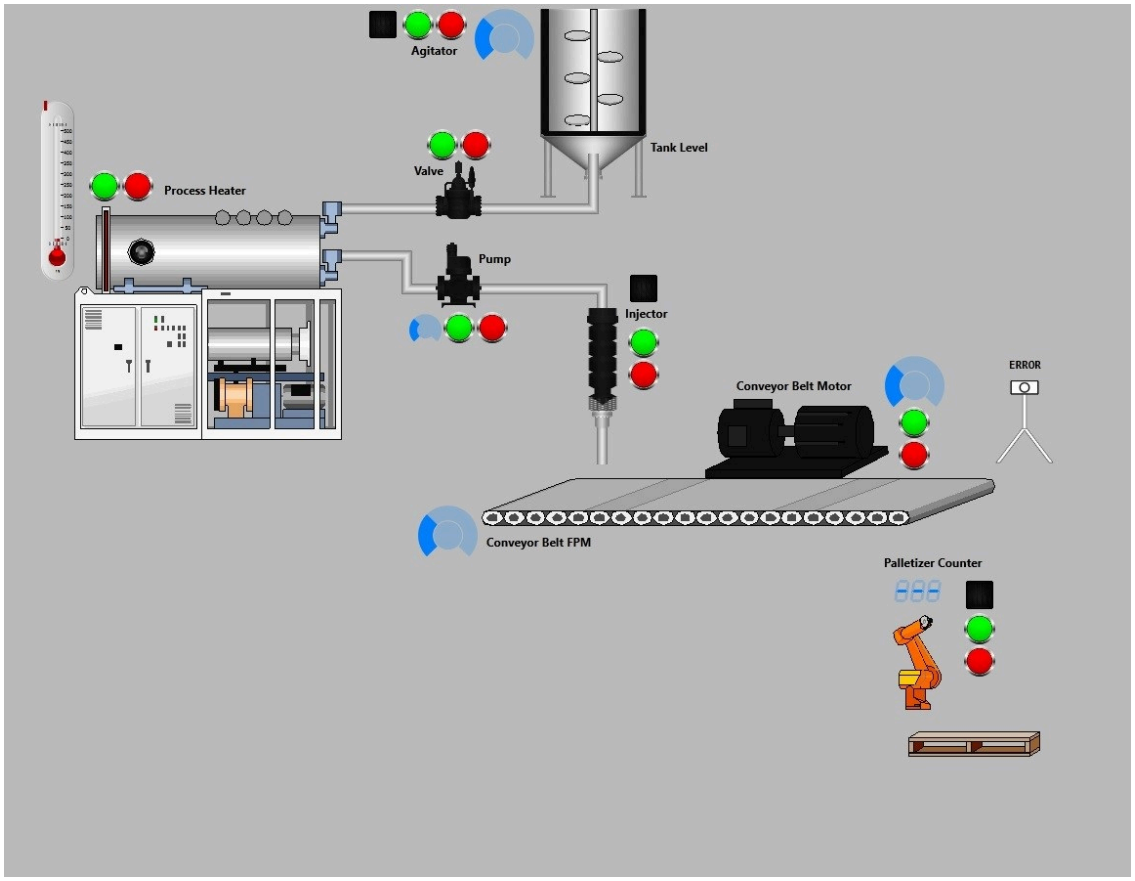


Figure 2. An example of an HMI

However, an HMI that might look like the image above wouldn't be able to load, and would have errors after the ransomware hits.

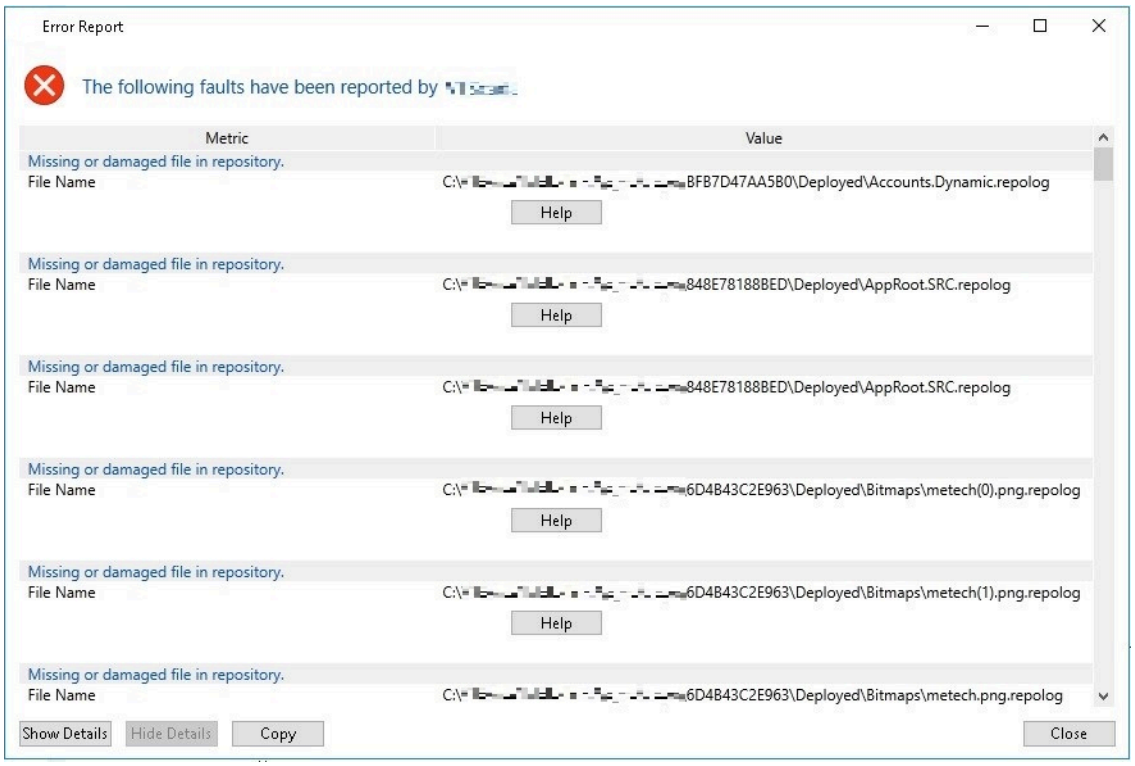


Figure 3. Errors that an HMI could experience due to ransomware

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 Viewopen on a new tab and Loss of Controlopen on a new tab scenario for the operator, and ultimately, Loss of Productivity and Revenueopen on a new tab 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 Mazeopen on a new tab 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.

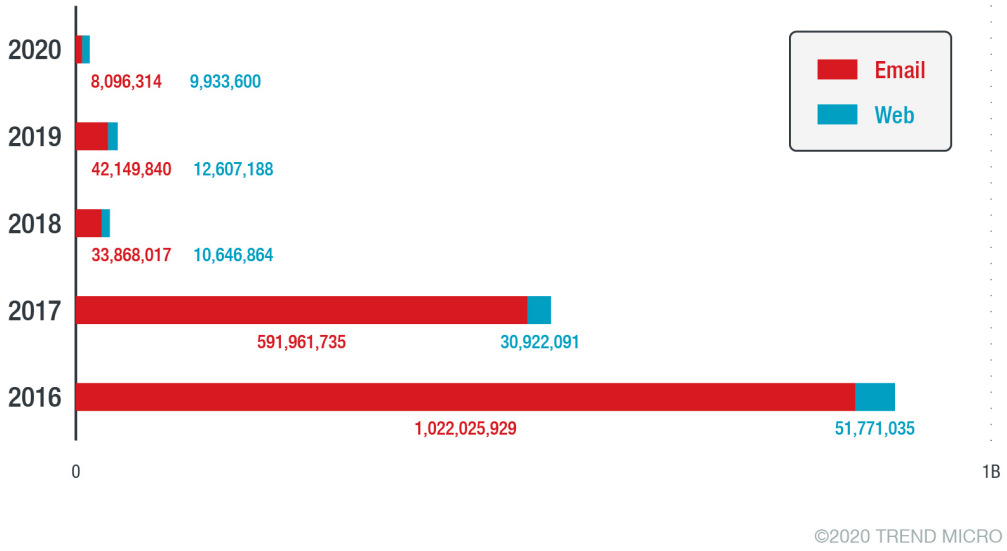


Figure 4. Ransomware detected by Trend Micro as email attachments (email) or in malicious websites (web) over the years

The reason behind this is that in the past few years, ransomware actors have become more selective in their targets. They have started moving away from mass-distributed ransomware spam campaigns and adopting a narrowed-down approach called “big-game hunting.” This means that ransomware actors are not concerned with infecting household desktops (aka small game) and are instead more interested in medium-to-large enterprises (aka big game). The reason behind this shift is that ransomware actors are now under the impression that participating in big-game hunting has larger payouts per infection.

Big-game hunting is more complicated and requires more time to observe, track, and stalk the prey. This is the reason that most ransomware families affecting big industries (such as manufacturing) are called “post-intrusion ransomware.” Simply put, the attackers would have already gained access to the network through other means before installing the ransomware.

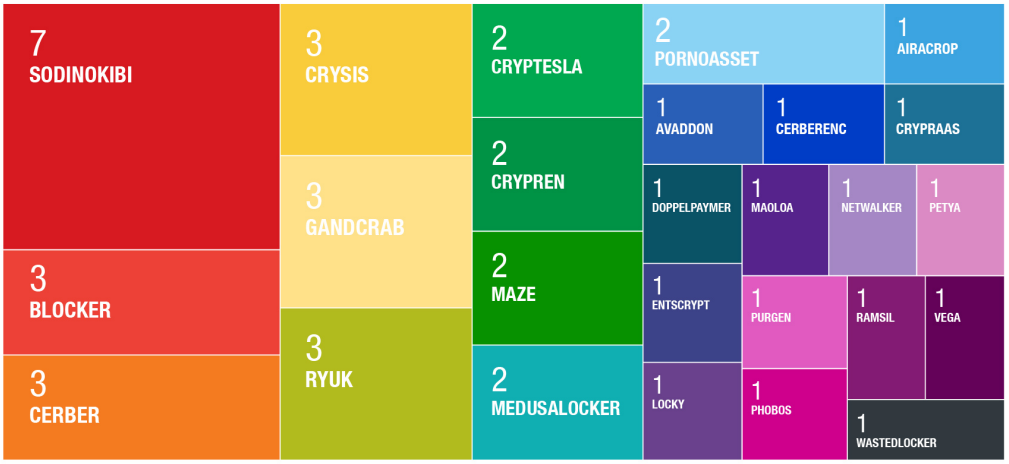


Figure 5. The distribution of different ransomware families affecting manufacturing networks in Q3 of 2020

Most of the different ransomware affecting manufacturing during Q3 of 2020 are known to be post-intrusion ransomware. Sodinokibiopen on a new tab, the ransomware that affected the most manufacturing networks during Q3, is installed after attackers gain access to vulnerable Oracle WebLogic servers. Gandcrab is usually installed after attackers exploit vulnerable public-facing MySQL servers. The ransomware Ryuk is installed by attackers who have already gained a foothold in networks through the Emotet malware. Attackers installing Sodinokibi, Medusalocker, Crysis, and a host of other ransomware are known to abuse weak RDP credentials.

More importantly, this shows that a ransomware incident is not a single incident. Rather, it is a manifestation of several security problems that enable attackers to gain access into a network, move laterally, and identify key assets to ransom.

Both the recent data on the manufacturing industry and the pattern of ransomware in ICS systems suggest that there might be holes in the demilitarized zone (DMZ) and network segmentation. These factors enable a compromise from the IT network to traverse into the OT network. Another possible issue is that there are remote access connections directly to the OT network that are weak or unaccounted for. Nevertheless, true recovery does not end when the ransomware incident is mitigated and production and operations are able to resume. It ends when the security weaknesses that enabled the ransomware infection in the first place are finally addressed.

Securing Manufacturing Networks

As we have seen in the past few years, manufacturing networks are as easy to compromiseopen on a new tab as any other network in other industries. Even with the specialized equipment, software, and protocol and network segmentation, attackers are routinely able to ransom ICS systems.

Standard security best practices and solutions should work, but these should be deployed in a manner that is sensitive to the production environment. Aside from the standard capabilities of security solutions, the additional

requirements that security officers in the manufacturing industry should look at when evaluating security solutions are:

- **Low latency**. Solutions should avoid interfering with time-sensitive production processes.
- **Protocols that are aware of OT protocols in the field**. Security products should properly identify and monitor traffic coming to and from ICS systems.
- **Integrated monitoring and detection on IT and OT networks**. Security strategies need products that can work together and send data between network segments, thereby increasing ease of use and simplifying monitoring and response.

In a short period, ransomware actors have learned how to target and navigate manufacturing networks. It is therefore necessary to integrate secure solutions and implement security best practices in critical industries.

Read more about Trend Micro's security solutions for manufacturing and smart factoriesopen on a new tab.

Tags

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