OT Ransomware Extortion Attacks Leak Critical OT Information

By Mandiant

Published: 2022-01-31 · Archived: 2026-04-06 01:26:52 UTC

Written by: Daniel Kapellmann Zafra, Corey Hidelbrandt, Nathan Brubaker, Keith Lunden

---

Data leaks have always been a concern for organizations. The exposure of sensitive information can result in damage to reputation, legal penalties, loss of intellectual property, and even impact the privacy of employees and customers. However, there is little research about the challenges posed to industrial organizations when threat actors disclose sensitive details about their OT security, production, operations, or technology.

In 2021, Mandiant Threat Intelligence continued observing ransomware operators attempting to extort thousands of victims by disclosing terabytes of stolen information on shaming sites. This trend, which we refer to as "Multifaceted Extortion," impacted over 1,300 organizations from critical infrastructure and industrial production sectors in just one year.

To validate the extent to which multifaceted extortion leaks represent a risk to OT, Mandiant analyzed a semi-random selection of samples from industries that typically leverage OT systems for production. Using various technical and human resources, we downloaded and parsed through many terabytes of dump data and found a substantial amount of sensitive OT documentation. This included network and engineering diagrams, images of operator panels, information on third-party services, and more. We note that our analysis of each dump was limited due to the scale of our dataset and that a more targeted examination of a handful of dumps would probably uncover more documentation per organization.

Based on our analysis, one out of every seven leaks from industrial organizations posted in ransomware extortion sites is likely to expose sensitive OT documentation. Access to this type of data can enable threat actors to learn about an industrial environment, identify paths of least resistance, and engineer cyber physical attacks. On top of this, other data also included in the leaks about employees, processes, projects, etc. can provide an actor with a very accurate picture of the target's culture, plans, and operations.

Mandiant Found a Range of Sensitive OT Documents on Extortion Sites

In early 2020, Mandiant observed media claims indicating ransomware leaks exposed aerospace manufacturing designs and third party technical documentation from an electric utility. A year later, an actor reshared a 2.3 GB Doppelpaymer extortion leak from a major Latin American oil and gas organization in an underground forum, claiming it contained OT information.

We analyzed that leak and found a variety of sensitive data including usernames and passwords, IP addresses, remote services, asset tags, original equipment manufacturer (OEM) information, operator panels, network diagrams, etc. All information which a sophisticated threat actor would be hunting for during reconnaissance or what Mandiant's red teamers would employ to identify attack paths in a target OT network.

Figure 1: Extortion leak for a major Latin American oil and gas organization

To better understand the risk these data leaks pose to OT asset owners, we built a large dataset. Over a couple of months, a small team of analysts and data researchers filtered through hundreds of leaks, collected, and analyzed samples to find OT documentation. We identified at least 10 dumps that contained sensitive OT technical data. Due to the volume of data in many leaks, we performed only superficial analysis of the dumps, however had we invested additional resources to process our samples further, we would have likely found a significant amount of additional information.

We note that most threat actors would likely focus their efforts on a smaller number of organizations due to resource limitations or a preexisting interest in a specific target or targets. This would allow the actor to focus their resources on finding more information on each target, which would be essential for any sophisticated attack.

Initial Triage

In 2021, we identified over 3,000 extortion leaks released by ransomware operators. Around 1,300 of these leaks were from organizations in industrial sectors that are likely to use OT systems, such as energy and water utilities, or manufacturing. We selected and retrieved a couple hundred of these samples by skimming through readily available file listings or other indicators of interest such as comments from the actor, or the targets' subindustry. In many cases, we were not able to acquire or access data from a leak because of timing or errors in the shared files; in these cases, we discarded the leak.

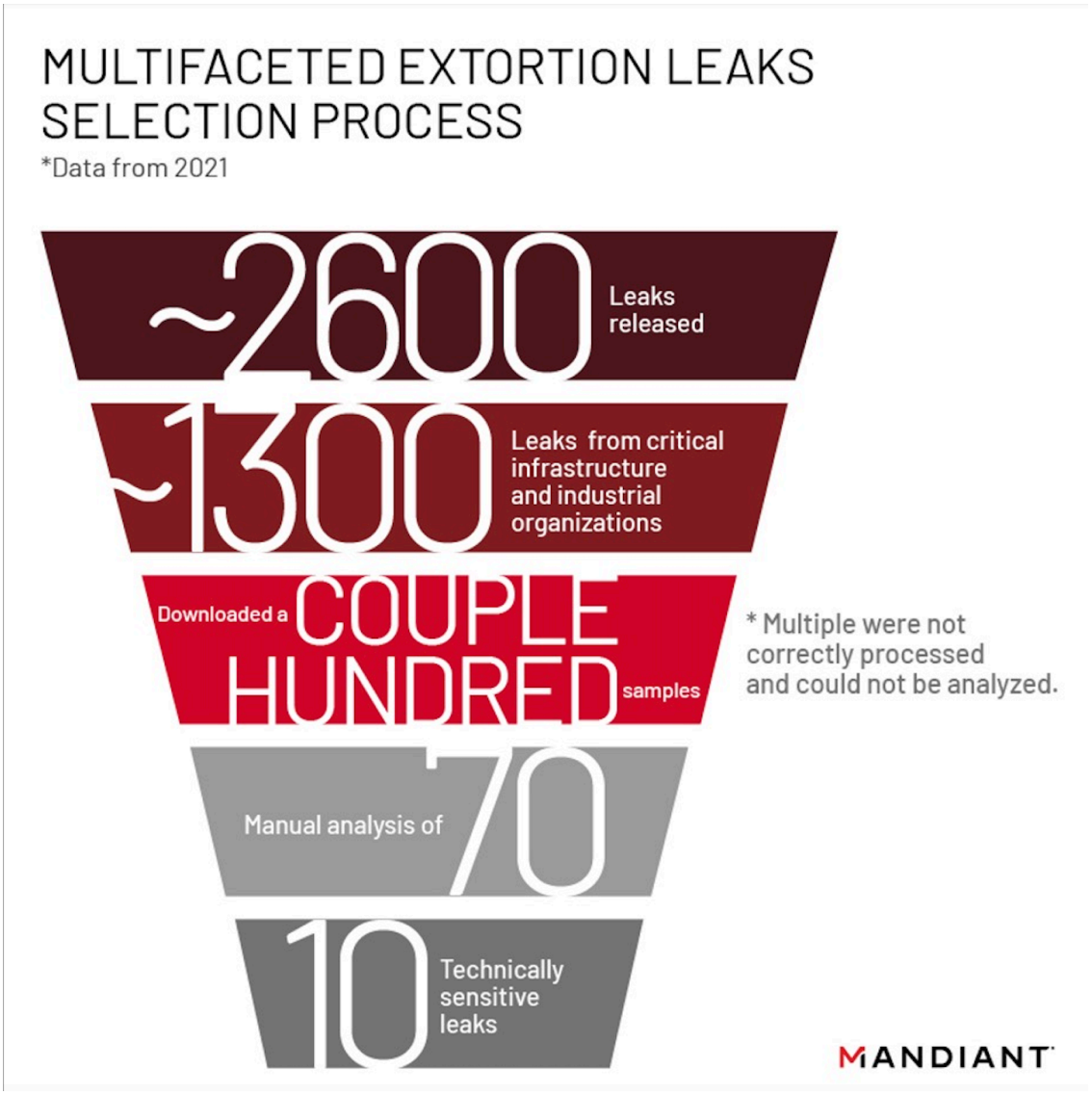

Figure 2: Filtered volume of extortion leaks

After initial triage, we collected and manually analyzed approximately 70 leaks using custom and publicly available tools. We found that one out of every seven leaks contained at least some useful OT information, while the rest contained data related to employees, finances, customers, legal documentation, among other things. Mandiant did not further analyze those files, though we note they remain available to threat actors for other purposes.

Collecting Several Terabytes of Already Filtered Data

Ransomware extortion leaks are mostly shared on a variety of threat actor-operated sites on the dark web. Although each actor operates differently, advertisements for incoming leaks are typically posted in hacker forums or on social media. Anyone with access to a Tor browser can visit the sites and download available dumps.

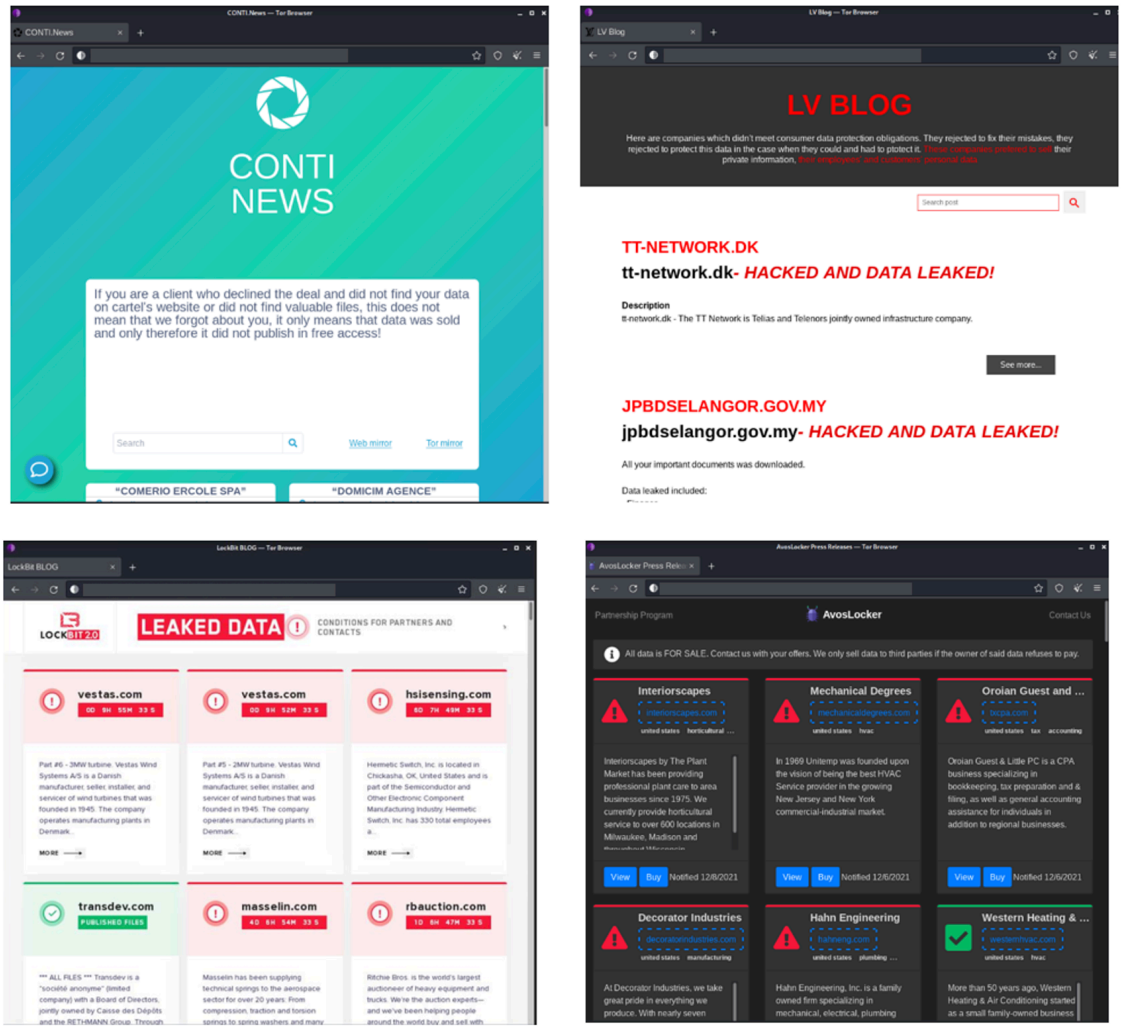

Figure 3: Example images from ransomware extortion sites

Downloading a single extortion leak is very simple but collecting multiple samples from different leaks is quite complex given the enormous volume of available data. The ability to download each of these leaks depends on multiple factors such as the infrastructure from the attacker and the downloader, the time during which the data is exposed, the number of users acquiring the file, and the quality of the file itself.

Acquiring each dump may require multiple hours and sometimes days. The dumps can often fill entire hard drives or virtual machines. To be able to collect, store, and further analyze multiple dumps, Mandiant leveraged a custom-built internal collections pipeline. It is likely that only well-resourced actors would have enough resources to reproduce this approach.

Analyzing the Samples to Find Sensitive Technical Documentation

We leveraged manual and automated file analysis to hunt through the data from interesting samples. We looked for documents such as network and process diagrams, machine interfaces, asset inventories, usernames and passwords, and project files. In a few cases we also examined third-party vendor agreements.

Method #1: File Listing of Manual Analysis

We browsed through file listings to identify keywords that hinted at the existence of OT-related data. We obtained the file listings in a few ways:

- Sometimes actors released a directory or text file listing to advertise the extortion leak.
- If there was no file listing available, we attempted to create it ourselves.
    - For small and medium-sized dumps we used Autopsy, a free publicly available forensics tool. The tool is also included in Mandiant's FLARE VM image which is distributed as open source.
    - For larger dumps, we used custom-built tools or downloaded the files locally to build a listing via default tools like rar or 7z.
- If we were not able to acquire a listing, we browsed manually through file names.

In some cases, a quick look at the listing and keyword searching was enough to determine if the dump was suitable for analysis, but in other cases the file naming conventions did not reveal much information. Another aspect that added a layer of complexity was that the extortion leaks contained data in various languages.

Method #2: Forensic Analysis with Public and Custom Tools

For small and medium-sized dumps we used Autopsy, which enabled us to analyze relatively large-sized folders. The tool can parse a file and provide summaries of timestamps, file types, keywords, and other useful data. We were also able to search for keywords using regular expressions to find data such as IP addresses or usernames, and to quickly visualize .jpeg images of existent files.

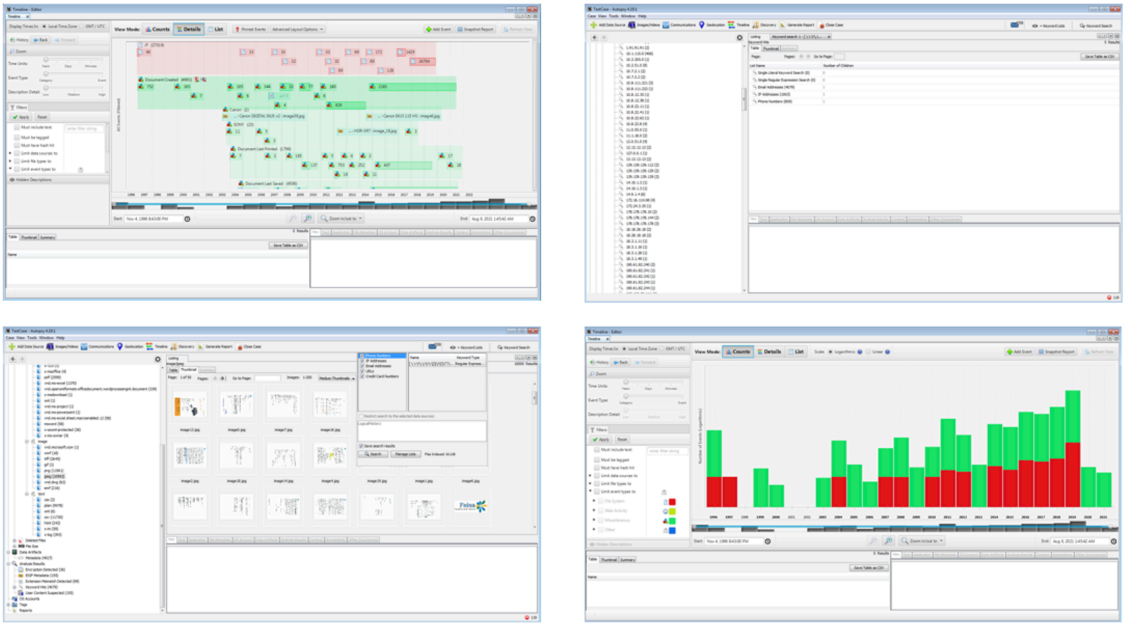

Figure 4: Analysis of extortion leak files using Autopsy

However, Autopsy struggled to analyze larger dumps. It would require multiple hours to parse a dump of just a couple gigabytes, yet we had identified leaks that contained terabytes of data. As a result, we had to build custom tools to visualize and analyze larger amounts of data. We note that even using custom tooling, we still required significant storage capabilities and human investment to handle the data.

We Found a Substantial Amount of OT Documentation

Finding sensitive OT documentation across such a large volume of files is not simple, but it is possible. Our findings included data from organizations across different sectors and regions. Although each of the leaks contained full information about the victim, we redacted their names and other proprietary information.

Victim **(Names Redacted)**	**Leak Contents**
Manufacturer of industrial and passenger trains	Password administration credentials for an OEM, requirements for control architecture and communication channels for European tram vehicle, backups of Siemens TIA Portal PLC project files, etc.
Two oil and gas organizations	In-depth network and process documentation, including diagrams, HMIs, spreadsheets, etc.
Control systems integrator	Engineering documentation from customer projects (Some files were password protected, which we did not attempt to bypass).
Hydroelectric energy producer	Most data was financial and accounting related, however we identified a list of names, emails, user privileges, and some passwords from IT, plant maintenance, and operations employees.
Satellite vehicle tracking service provider	Product diagrams, visualizations, and source code from a proprietary platform used to track automobile fleets via Global Positioning System (GPS).
Renewable energy producer	Legal agreements between the victim and customers stating the conditions for maintenance and supply of renewable energy infrastructure. The contracts stated that the service provider had full access to the third party's SCADA system via public internet IP addresses.

Table 1: Selection of findings

Sophisticated Threat Actors Can Leverage Data Leaks to Support Reconnaissance Efforts

Sensitive OT and network documentation exposed in ransomware extortion leaks is readily available for anyone to download, including security researchers, industry competitors, or threat actors. As we have highlighted, the most concerning scenario involves well-resourced actors that have the capability to systematically hunt for data to learn about specific targets.

- Historically, espionage campaigns have helped state-sponsored groups to acquire details about the operations of industrial organizations. This reconnaissance data has supported different stages of real cyber

physical attacks such as the Ukraine power outages in 2015 and 2016 and the TRITON incident.
    - Data from extortion leaks may provide sophisticated actors with information on targets, while limiting their exposure to defenders and cost of operations.
    - Actors may also select targets based on readily available sensitive data about the victim's infrastructure, assets, security flaws, and processes.
    - Attacks that leverage higher levels of cyber physical reconnaissance data are likely to result in more significant and precise impacts.
    - Mandiant has released blogs describing how we use network details and process documentation to model attack scenarios during OT red teaming engagements.
- Actors that have limited resources and capabilities will likely have more limited visibility into data from large extortion leaks. However, they can still explore dumps learn about an organization, satisfy their curiosity, or reshare the contents.

Protecting OT Data from Multifaceted Extortion Leaks

Based on our analysis, one out of every seven leaks from industrial organizations posted in ransomware extortion sites is likely to expose sensitive OT documentation. Access to this type of data can enable threat actors to learn about an industrial environment, identify paths of least resistance, and engineer cyber physical attacks. On top of this, other data also included in the leaks about employees, processes, projects, etc. can provide an actor with a very accurate picture of the target's culture, plans, and operations.

Even if the exposed OT data is relatively old, the typical life span of cyber physical systems ranges from twenty to thirty years, resulting in leaks being relevant for reconnaissance efforts for decades—much longer than exposed information on IT infrastructure. To prevent and mitigate the risks presented by exposed OT data, we suggest the following:

- Create and enforce robust data handling policies for employees and subcontractors to ensure that internal documentation is protected. Avoid storing highly sensitive operational data in less-secure networks.
- Place special attention on selecting subcontractors that implement comprehensive security programs to safeguard operational data.
- Victims of ransomware intrusions should assess the value of any leaked data to determine what compensatory controls can help decrease the risk of further intrusions.
- Change any leaked credentials and API keys. Consider changing exposed IP addresses for critical systems and OT jump servers.
- Periodically conduct red team exercises to identify externally exposed and insecure internal information.
    - Mandiant offers a suite of service options, including OT red teaming, to help OT asset owners mitigate risk or respond to incidents after they occur.

Acknowledgements

This research was made possible thanks to the hard work of many people not listed on the by line. A huge thanks to the Mandiant Research Team and everyone else who supported this effort.

Posted in

- Threat Intelligence
- Security & Identity
