

# Crimes of Opportunity: Increasing Frequency of Low Sophistication Operational Technology Compromises

---

[fireeye.com/blog/threat-research/2021/05/increasing-low-sophistication-operational-technology-compromises.html](https://fireeye.com/blog/threat-research/2021/05/increasing-low-sophistication-operational-technology-compromises.html)



## Breadcrumb

---

Threat Research

Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker

May 25, 2021

7 mins read

Threat Actors

Attacks on control processes supported by operational technology (OT) are often perceived as necessarily complex. This is because disrupting or modifying a control process to cause a predictable effect is often quite difficult and can require a lot of time and resources. However, Mandiant Threat Intelligence has observed simpler attacks, where actors with varying levels of skill and resources use common IT tools and techniques to gain access to and interact with exposed OT systems.

The activity is typically not sophisticated and is normally not targeted against specific organizations. Rather, the compromises appear to be driven by threat actors who are motivated to achieve ideological, egotistical, or financial objectives by taking advantage of an ample supply of internet-connected OT systems. As the actors are not interested in causing specific physical outcomes, they target whatever is available on the internet.

Mandiant has observed an increase in compromises of internet-accessible OT assets over the past several years. In this blog post we discuss previously undisclosed compromises and place them in context alongside publicly known incidents. Although none of these incidents have appeared to significantly impact the physical world, their increasing frequency and relative severity calls for analysis on their possible risks and implications.

Visit our website to learn more about Mandiant's OT security practice or contact us directly to request [Mandiant services](#) or [threat intelligence](#).

## **Compromises of Internet-Exposed OT Are Increasing in Frequency**

---

While Mandiant has monitored threat actors claiming to share or sell access to internet-exposed OT systems since at least 2012, we have seen a significant increase in the frequency and relative severity of incidents in the past few years. The most common activity we observe involves actors trying to make money off exposed OT systems, but we also see actors simply sharing knowledge and expertise. More recently, we have observed more low sophistication threat activity leveraging broadly known tactics, techniques, and procedures (TTPs), and commodity tools to access, interact with, or gather information from internet exposed assets—something we had seen very little of in the past.

This low sophistication threat activity has impacted a variety of targets across different industries, ranging from solar energy panels and water control systems, to building automation systems (BAS) and home security systems in academic and private residences. While some critical infrastructure targets are very sensitive in nature, other targets present very little risk.

The following timeline presents a selection of some public and previously undisclosed OT compromises Mandiant observed between 2020 and early 2021. We note that, although it is possible many of these incidents involved process interaction, high confidence validation is not feasible as most often the evidence is provided by the actor itself.

Selection of notable low sophistication OT compromises: January 2020 to April 2021

Figure 1: Selection of notable low sophistication OT compromises: January 2020 to April 2021

## **Low Sophistication OT Threat Activity Can Take Many Forms**

---

A consistent characteristic we observe among low sophisticated compromises is that actors most often exploit unsecure remote access services, such as virtual network computing (VNC) connections, to remotely access the compromised control systems. Graphical user interfaces (GUI), such as human machine interfaces (HMI), become the low-hanging fruit of process-oriented OT attacks as they provide a user-friendly representation of complex industrial processes, which enables actors to modify control variables without prior knowledge of a process. In many cases, the actors showed evidence of compromised control processes via images of GUIs, IP addresses, system timestamps, and videos.

*Low Sophistication Threat Actors Access HMIs and Manipulate Control Processes*

In March 2020, we analyzed a series of screenshots shared by a threat actor who claimed to compromise dozens of control systems across North America, Western and Central Europe, and East Asia. Based on the timestamps from the images, the actor appeared to gain unauthorized access to these assets over a five-day period. The actor also shared a low-quality cell phone video showing their explicit interaction with a Dutch-language temperature control system.

While much of this type of activity appears opportunistic in nature, some may also be driven by political motivations. For example, we have seen hacktivist groups that frequently use anti-Israel/pro-Palestine rhetoric in social media posts share images indicating that they had compromised OT assets in Israel, including a solar energy asset and the webserver of a datalogger used for different applications such as mining exploration and dam surveillance (Figure 2).



Figure 2: Screenshots of compromised web-interfaces supporting OT

Some threat actors appear particularly eager to demonstrate their interaction with compromised control systems. One threat actor shared multiple screen recordings making arbitrary set point changes to compromised HMIs via remote connections from their own desktop. While we suspect many of the victims compromised by this threat actor were small- and medium-sized businesses, on one occasion the group appeared to have successfully accessed the BAS of a hotel in Australia belonging to a major international hotel chain (Figure 3).



Figure 3: Screenshots showing a possible compromise of a hotel BAS  
*Some Amateur Actors Show Limited OT Expertise*

Some of the actors we track made comments that indicated they had either a limited understanding of the OT assets they compromised or that they were simply attempting to gain notoriety. For example, one threat actor shared a screenshot of a purportedly

compromised German-language rail control system. We conducted a reverse image search of the screenshot and identified the asset as the web interface for an ECoS 50210 command station designed for model train sets (Figure 4).

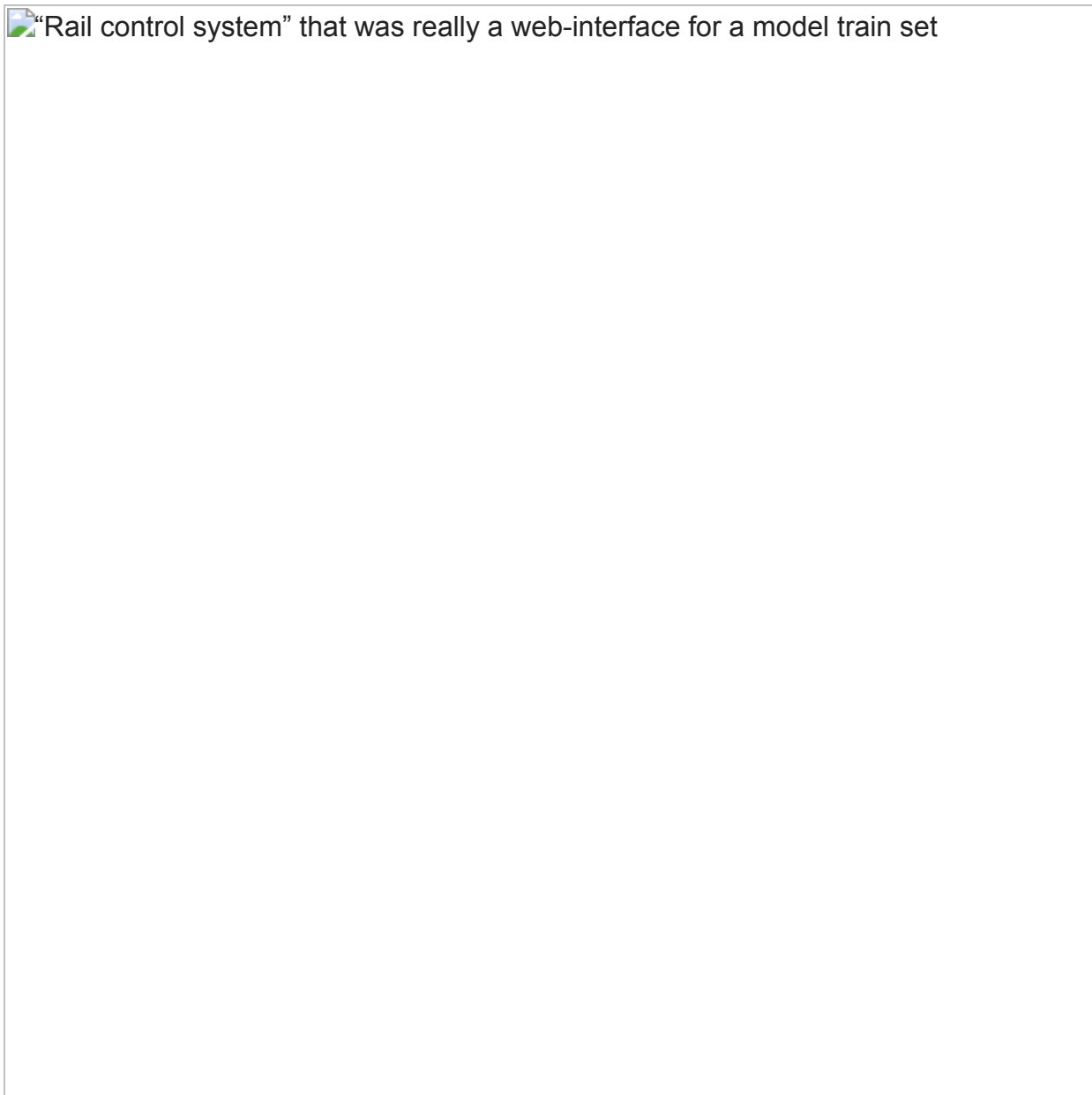


Figure 4: “Rail control system” that was really a web-interface for a model train set  
Another group made a similar gaffe when they claimed to retaliate for an explosion at a missile facility in Iran by compromising an Israeli “gas system.” A video of their operation showed that they had actually compromised a kitchen ventilation system installed at a restaurant in Ramat Hasharon, Israel (Figure 5).

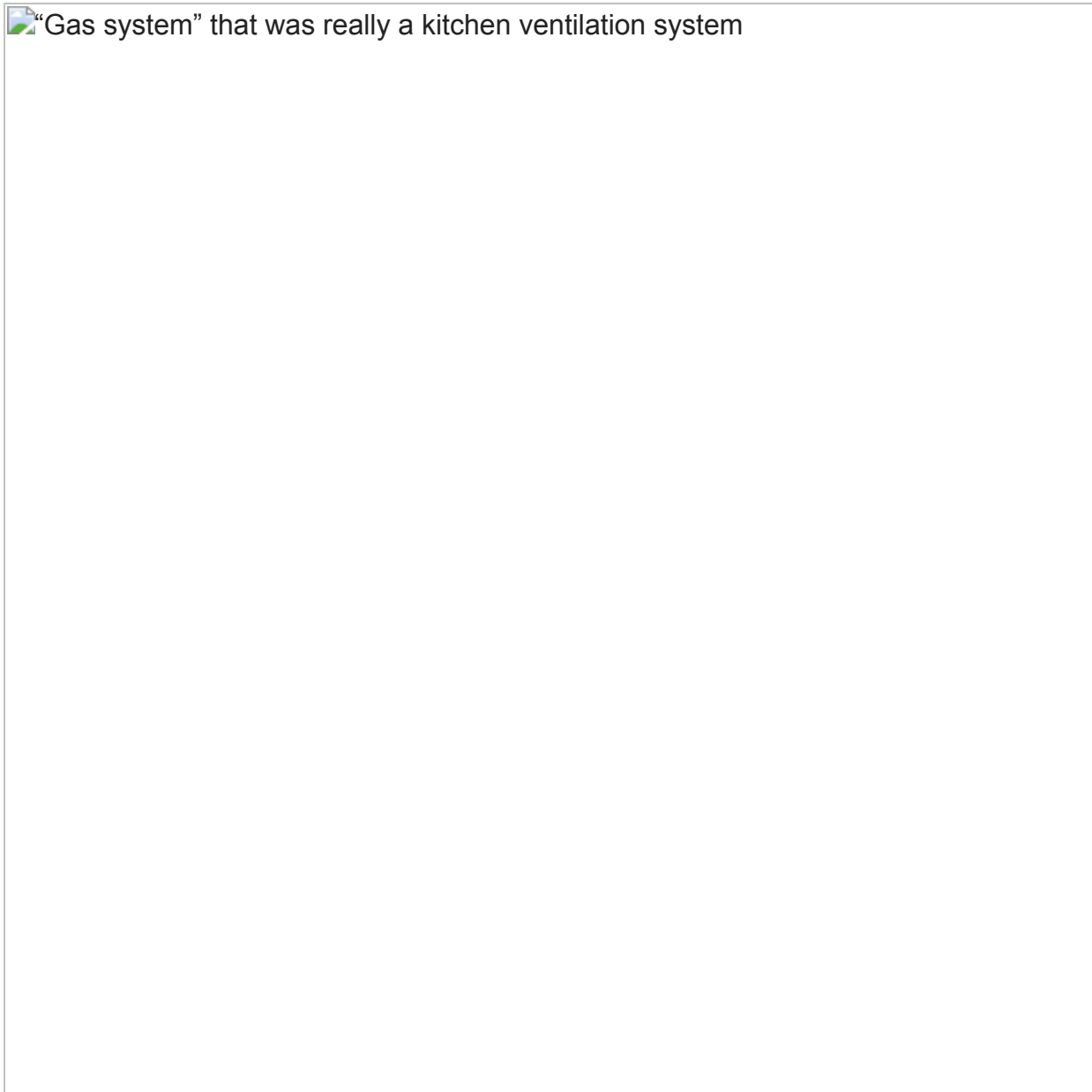


Figure 5: “Gas system” that was really a kitchen ventilation system  
*Low Sophistication OT Threat Activity is Supported by Hactivist Tutorials*

In a few instances, actors operating as part of hacktivist collectives created and shared tutorials that instructed their affiliates and sympathetic parties on how to identify and compromise internet-accessible OT assets. The tutorials typically described simple methodologies, such as using VNC utilities to connect to IP addresses identified in Shodan or Censys searches for port 5900. These methods appear to have been used in some of the incidents we described, as some of the shared screenshots of compromised OT systems also showed the actor’s web browser tabs displaying similar Shodan queries and remote access tools.


 Hactivist tutorial describing how to access the HMI of an industrial gas and liquid burner

Figure 6: Hactivist tutorial describing how to access the HMI of an industrial gas and liquid burner

### **Low Sophistication OT Compromises Pose A Growing Risk**

---

Each of the low sophistication incidents we observe is unique and poses a different level of risk, which we normally determine by examining the actor's previous work and reputation, the target's industry, and the nature of the compromised process, among other things. While low sophistication incidents do not appear to commonly impact physical environments, they remain concerning for the following reasons.

- Each incident provides threat actors with opportunities to learn more about OT, such as the underlying technology, physical processes, and operations. These opportunities can increase an adversary's ability and enhance their tradecraft.



- Even low-sophistication intrusions into OT environments carry the risk of disruption to physical processes, mainly in the case of industries or organizations with less mature security practices. As the number of intrusions increase, so does the risk of process disruption.
- The publicity of these incidents normalizes cyber operations against OT and may encourage other threat actors to increasingly target or impact these systems. This is consistent with the increase in OT activity by more resourced financially-motivated groups and ransomware operators.

## **Security Best Practices and Situational Awareness Help Prevent Low Sophistication Compromises**

---

Defense against low sophistication compromises is best addressed by implementing security best practices and gaining situational awareness about the threat exposure of assets and data. Implementing security controls to defend against this activity is also the foundation for mature security programs that seek to prevent and identify complex OT threats before they introduce a risk to the safety of people and infrastructure.

- Whenever feasible, remove OT assets from public-facing networks. If remote access is required, deploy access controls and monitor traffic for unusual activity to minimize unintended interaction and safeguard asset information.
- Apply common network-hardening techniques to remotely accessible and edge devices, such as disabling unused services, changing default credentials, reviewing asset configurations, and creating whitelists for access.
- Determine if relevant assets are discoverable using online scanners such as Shodan and Censys. Leverage support from knowledgeable security researchers to identify exposed assets and leaked information. Mandiant Threat Intelligence offers subscription content, custom analysis, and black box assessments that help organizations identify internet-exposed assets and information.
- Maintain situational awareness on threat actors' interest in cyber physical systems and the development of OT exploits, with particular interest in attention driven to your organization, third party providers, or original equipment manufacturers (OEM).
- Configure HMIs and other control system assets to enforce acceptable input ranges and prohibit hazardous variable states. Similar to web application security, automation programmers should treat all operator input as potentially malicious and gain security assurances by validating that the operator input is within acceptable thresholds.

Visit our website to learn more about Mandiant's OT security practice or contact us directly to request Mandiant services or threat intelligence.