Exploits and TrickBot disrupt manufacturing operations

By Mark Stockley

Published: 2022-08-24 · Archived: 2026-04-05 22:06:44 UTC

September 2021 saw a huge spike of exploit detections against the manufacturing industry, with a distributed spread between California, Florida, Ohio, and Missouri. This is combined with heavy detections of unseen malware, identified through our AI engine, spiking in May as well as September 2021.

May brought with it a flood of attacks that exploited the Dell system driver exploit (CVE-2021-21551), where we observed the greatest number of detections in Michigan. During this month, JBS, one of the largest meat suppliers, was targeted by the REvil group who likely exploited this vulnerability to infiltrate the network. By June, overall detection of this threat against manufacturing firms began to fall significantly, with only about two dozen detections averaged between November 2021 and June 2022.

In the first half of the year, we observed spiking detections of threats associated with tech support scams. These threats install applications on the system that create fake error messages, urging the user to call a “help center” that is, in reality, a scam operation. These spikes were in March and May 2021 and focused primarily on firms in New York and Texas. However, detections of this threat declined steadily through the rest of the analyzed timeframe.

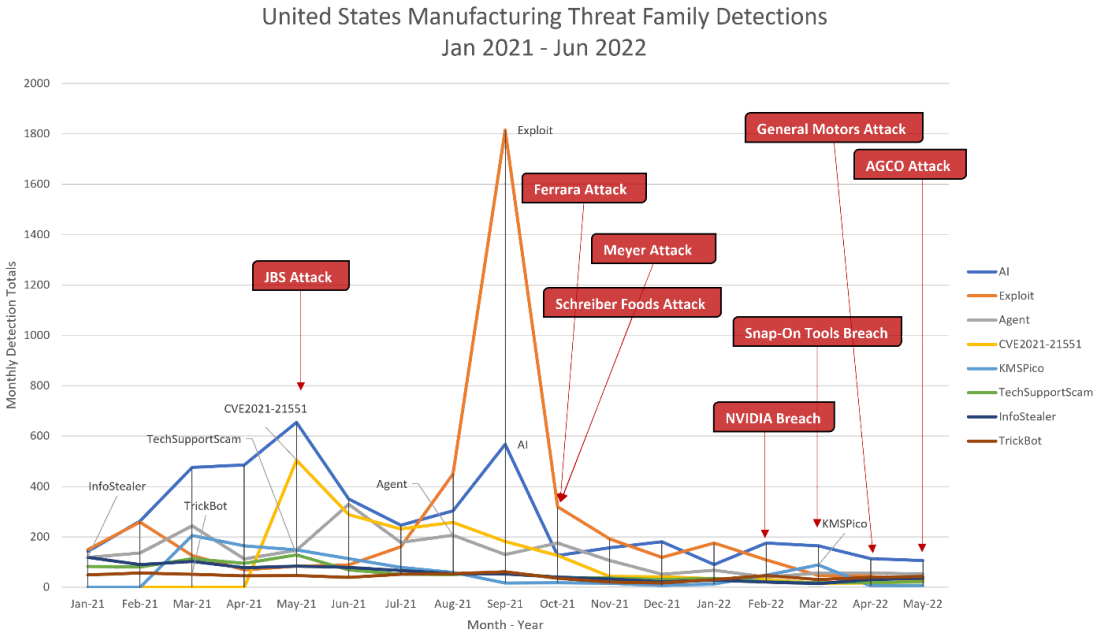

Figure 1. United States manufacturing threat family detections by month

The notorious TrickBot Trojan was detected constantly throughout 2021, with small spikes in February and September 2021 and February 2022. This threat is very capable of infecting a single endpoint, and by using

additional tools and features, can compromise the entire network, often for the benefit of launching additional malware.

While our detections of TrickBot focused on attacks in New York, the fallout from the September spike saw three more manufacturer breaches, all in October. Victims of these attacks included the candy maker Ferrara, who was targeted right before Halloween, and the cookware company Meyer, whose employee data was leaked.

Schreiber Foods, a cheese manufacturer, dealt with attacks attempting to disrupt plant and distribution center operations. That attack actually caused a nationwide shortage for cream cheese!

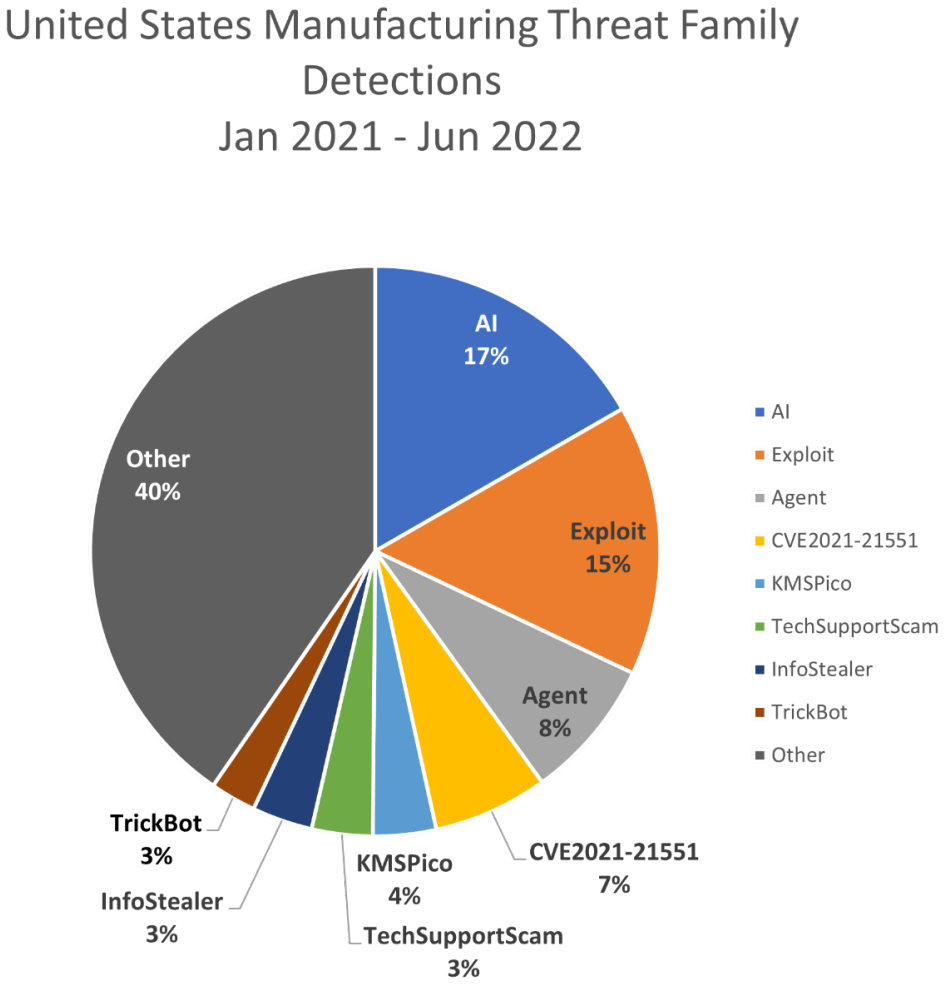

Figure 2. United States manufacturing family threat detections pie chart

Finally, manufacturing companies in North Carolina dealt with heavy information stealing spyware during the first few months of 2021, with a gradual decline to December 2021. However, that trend reversed in January 2022 with new spikes in February and April 2022.

Between February and May 2022, the industry dealt with significant manufacturer breaches. For example, the video card maker NVIDIA dealt with a significant attack in February 2022; March saw the infection of the tool manufacturer Snap-On Tools by Conti ransomware; in April there was an operation against General Motors; and in May, infiltration of the agricultural company, AGCO.

Exploits were a serious issue for the manufacturing industry in 2021. In fact, the JBS attack coincides with spikes of certain exploits, and after a huge spike in exploit detections during September, we observed three attacks in a single month. One of those attacks disrupted operations and caused a nationwide supply chain issue.

However, things aren't the same in 2022, and detections for exploits have dropped significantly. Despite that, we've seen at least four major manufacturing attacks occur between February and May 2022, with threats like trojans, information stealers and backdoors possibly to blame for the breaches.

Recommendations for the manufacturing industry

With all that in mind, we recommend that businesses who operate in the manufacturing industry consider the most important part of their security plan, which is to keep things moving. Therefore, we highly recommend that there be some division between networks for offices, plants, and distribution centers to reduce the chance that an infection of an endpoint will lead to a factory needing to shut down.

Combine this with a security playbook which will inform all staff on what procedures need to be followed if a cyberattack is discovered. For example, who to call, what systems to secure, etc. In the case of manufacturing firms, it's important to describe how to keep operations continuing, even during an active breach.

Historically, exploit protection has been very important for this industry, so utilizing anti-exploit technology to block these types of attacks on all endpoints and servers will greatly reduce the chance attackers can use this method for infiltration.

Next, the discovery of a lot of tech support scam malware could be the result of users who have too many rights on their endpoint, installing third-party, unverified software onto their corporate systems. So doing a thorough audit of user accesses and rights on their endpoint will reduce the junk they are able to install and greatly reduce the chance that junk will be bundled with something nasty.

Finally, the discovery of so many TrickBot attacks against this industry means that manufacturing is clearly a top target for this group. TrickBot frequently compromises every endpoint in a network before preparing it for a ransomware attack. Ransomware attacks that disrupt operations and start bleeding the company money are more likely to be quickly resolved, so going after manufacturing firms is a great way to get paid quick. To protect against this threat, you need to use anti-malware software that uses behavior as well as signatures to identify TrickBot and quickly remove it from the system.

In addition, TrickBot has multiple methods of initial infection, including phishing attacks against employees, so educating staff on how to recognize phishing is a great idea. But going one step further would be to deploy a phishing button in your organization's email client. This make it easy for employees to submit a suspect email to be analyzed by the security team for any malicious intent.
