VECTRA

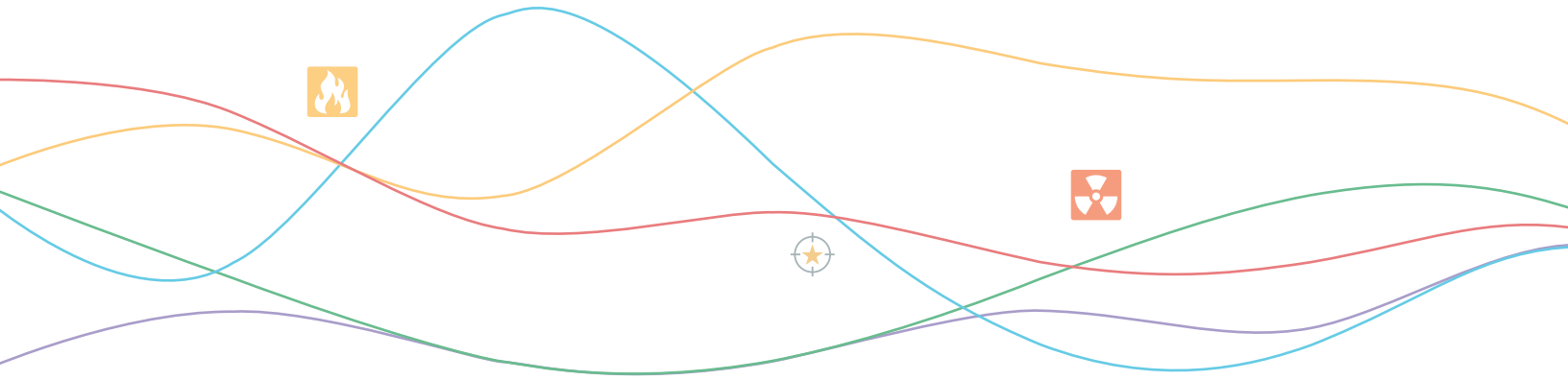
I am artificial intelligence.
The driving force behind the hunt for cyberattackers.
I am Cognito.

The increased risk of cyberattacks against manufacturing organizations

2018 Spotlight Report

VECTRA®

TABLE OF CONTENTS



Manufacturing organizations today rely on countless devices that are wirelessly connected, including numerous industrial internet-of-things (IIoT) devices and others that integrate information technology (IT) with operational technology (OT).

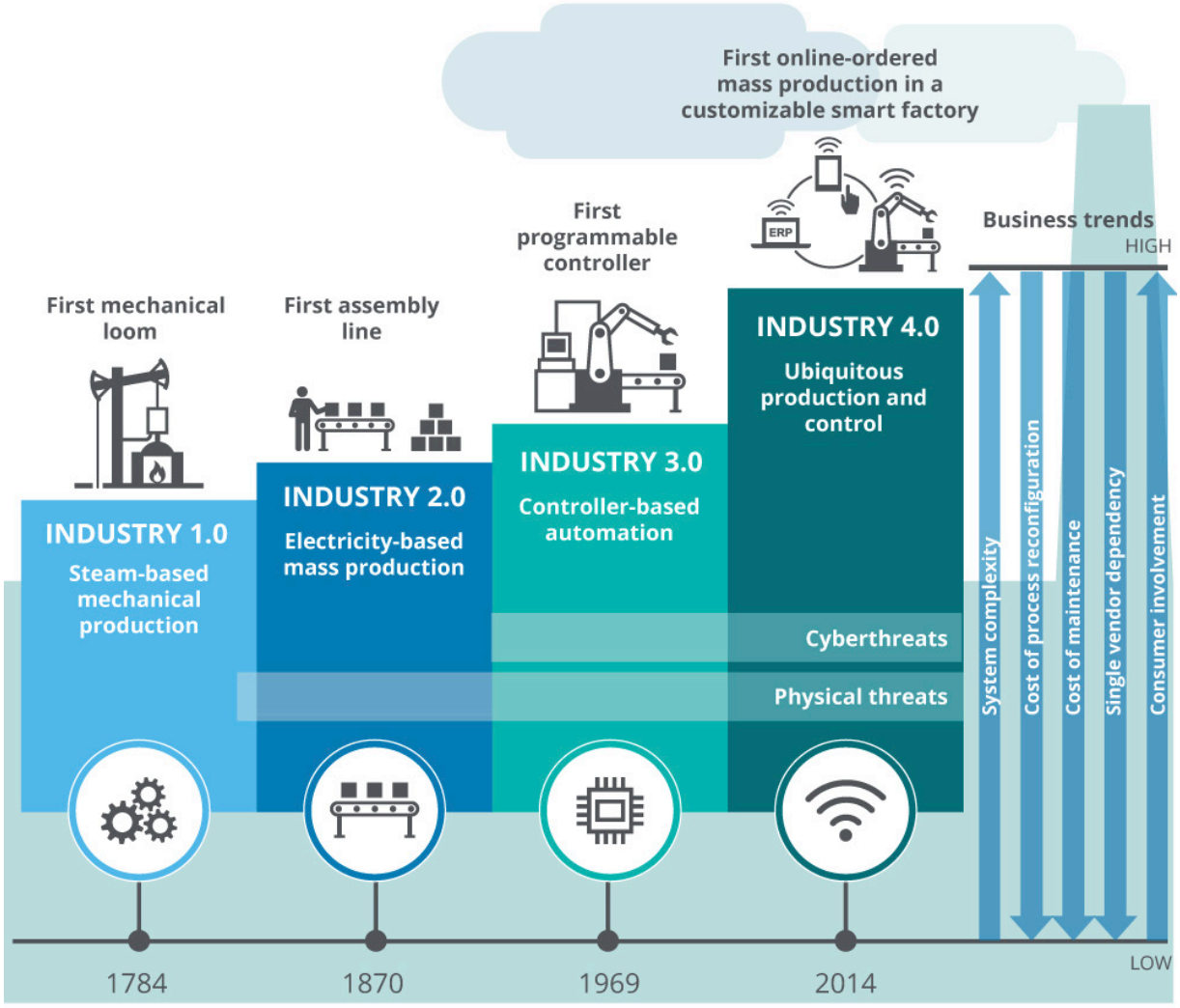
Without air-gapped industrial control systems, which are being replaced by cloud-based digital systems, these connections create a massive attack surface that is easy for cybercriminals to infiltrate with the intent to spy, spread and steal.

Visibility into these internal connected systems is necessary to curtail the extent of damage from a cyberattack. Manufacturing security operations now require automated, real-time analysis of entire networks to proactively detect and respond to in-progress threats before they do damage.

Manufacturing enterprises and Industry 4.0

The massive effort to automate real-time data collection across the manufacturing supply chain is known as Industry 4.0. It involves the integration of digital systems, IIoT devices and cloud computing resources in the manufacturing supply chain.

This new digital supply chain is driven by the integration of IT with OT – known as IT/OT convergence – and is increasing exponentially.



Source: Deloitte

Deloitte University Press | dupress.deloitte.com

Industry 4.0 brings with it a new operational risk for connected, smart manufacturers and digital supply networks. The interconnected nature of Industry 4.0-driven operations and the pace of digital transformation mean that cyberattacks can have far more damaging effects than ever before, and manufacturers and their supply networks may not be prepared for the risks.

For cyber-risk to be adequately addressed in the age of Industry 4.0, manufacturing organizations need to ensure that proper visibility and response capabilities are in place to detect and respond to events as they occur.

The information in this spotlight report is based on observations and data from the 2018 Black Hat Edition of the Attacker Behavior Industry Report from Vectra®. The report reveals attacker behaviors and trends in networks from over 250 opt-in customers in manufacturing and eight other industries.

From January-June 2018, the Cognito™ cyberattack-detection and threat-hunting platform from Vectra monitored network traffic and collected rich metadata from more than 4 million devices and workloads from customer cloud, data center and enterprise environments.

The analysis of this metadata provides a better understanding about attacker behaviors and trends as well as business risks, enabling Vectra customers to avoid catastrophic data breaches.

Analysis of cyberattacker behaviors in the manufacturing industry

Rich metadata from the Vectra Cognito platform revealed a high volume of malicious internal reconnaissance and lateral movement behaviors among manufacturing organizations. These behaviors are critical phases in the cyberattack lifecycle during which cybercriminals spy, spread and steal inside the network.

When attackers succeed: Data breaches in manufacturing

The 2018 Verizon Data Breach Industry Report provides insight into the potential intent and motives behind cyberattacks in the manufacturing industry.

State-affiliated attackers: 53% of breaches in manufacturing

Manufacturing capabilities are closely related to the health of a nation's economy. Many nation-states want to give their companies an edge. State-sponsored attackers caused more than half of the data breaches in manufacturing.

The most common types of data stolen were personal (32%), secrets (30%) and credentials (24%), according to the Verizon report.

Cyberespionage: 31% of breaches in manufacturing

Along with state-sponsored attacks, there was growth in cyberespionage. Espionage was the leading motive behind breaches in manufacturing.

This trend is reaffirmed when looking at the actor motive. While 53% of attempted attacks against the manufacturing industry had a financial motive, 47% of attempts were motivated by espionage, according to the Verizon report.

Servers: 58% of breaches in manufacturing

At least one server was compromised in more than half of the data breaches in manufacturing, according to the Verizon report. Opportunistic attacks usually stick to endpoints and IoT devices, while attackers who are intent on stealing intellectual property and mapping-out critical assets target servers.

This Spotlight Report raises three important issues:

1. The most common types of cyberattacks found in manufacturing organizations.
2. The malicious behaviors and actions behind these cyberattacks.
3. The business risks associated with these attacker behaviors.

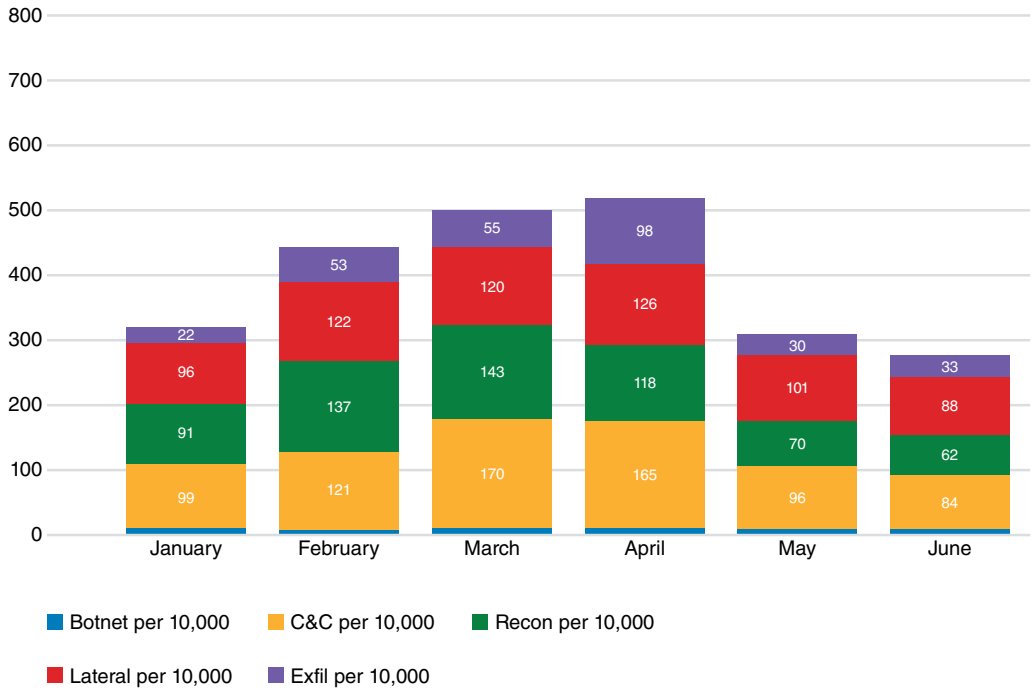


Figure 1: Attacker detections across all industries per 10,000 host devices

The volume of attacker detections per 10,000 host devices across all industries indicates that the numbers of malicious command-and-control, reconnaissance and lateral movement behaviors are relatively equal to each other within each industry.

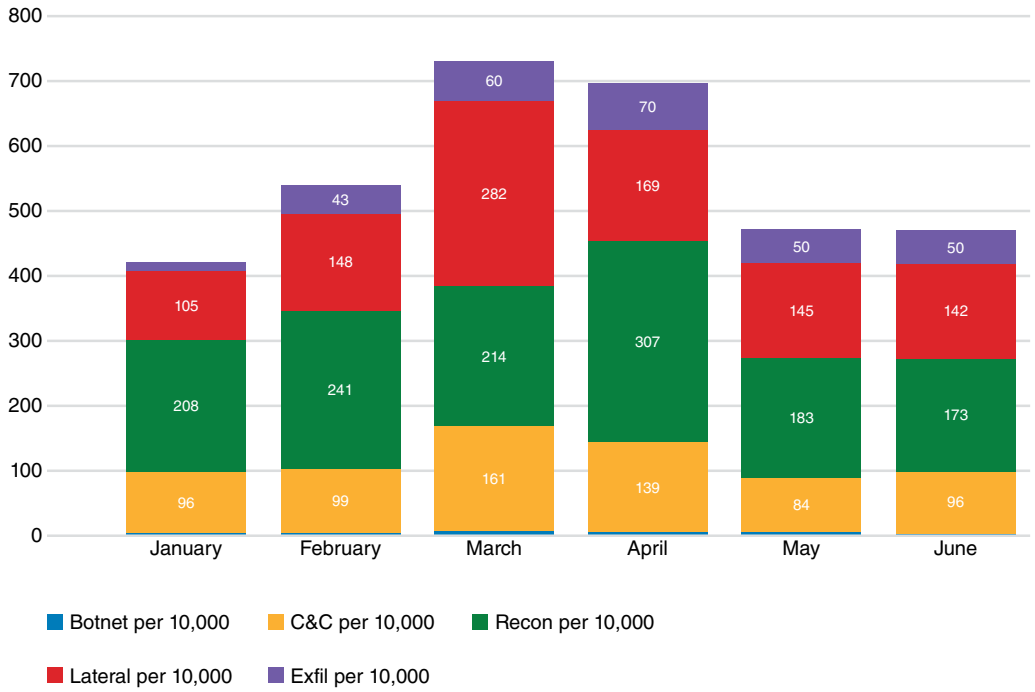


Figure 2: Attacker detections in manufacturing per 10,000 host devices

The monthly volume of attacker detections per 10,000 host devices in the manufacturing industry shows a much higher volume of malicious internal behaviors. In many instances, there is a 2:1 ratio of malicious behaviors for lateral movement over command-and-control.

These behaviors reflect the ease and speed with which attacks can proliferate inside manufacturing networks due to the large volume of unsecured IIoT devices and insufficient internal access controls.

Most manufacturers do not invest heavily in security access controls for business reasons. These controls can interrupt and isolate manufacturing systems that are critical for lean production lines and digital supply chain processes.

Many factories connect IIoT devices to flat, unpartitioned networks that rely on communication with general computing devices and enterprise applications. These digital factories have internet-enabled production lines to produce data telemetry and remote management.

In the past, manufacturers relied on more customized, proprietary protocols, which made mounting an attack more difficult for cybercriminals. The conversion from proprietary protocols to standard protocols makes it easier to infiltrate networks to spy, spread and steal.

Cyberattack severity

The combination of malicious behaviors across the attack lifecycle and the context of specific behaviors is a strong threat indicator. The Cognito platform from Vectra correlates attacker behaviors to compromised host devices, assigns a threat-severity score and prioritizes the highest-risk threats.

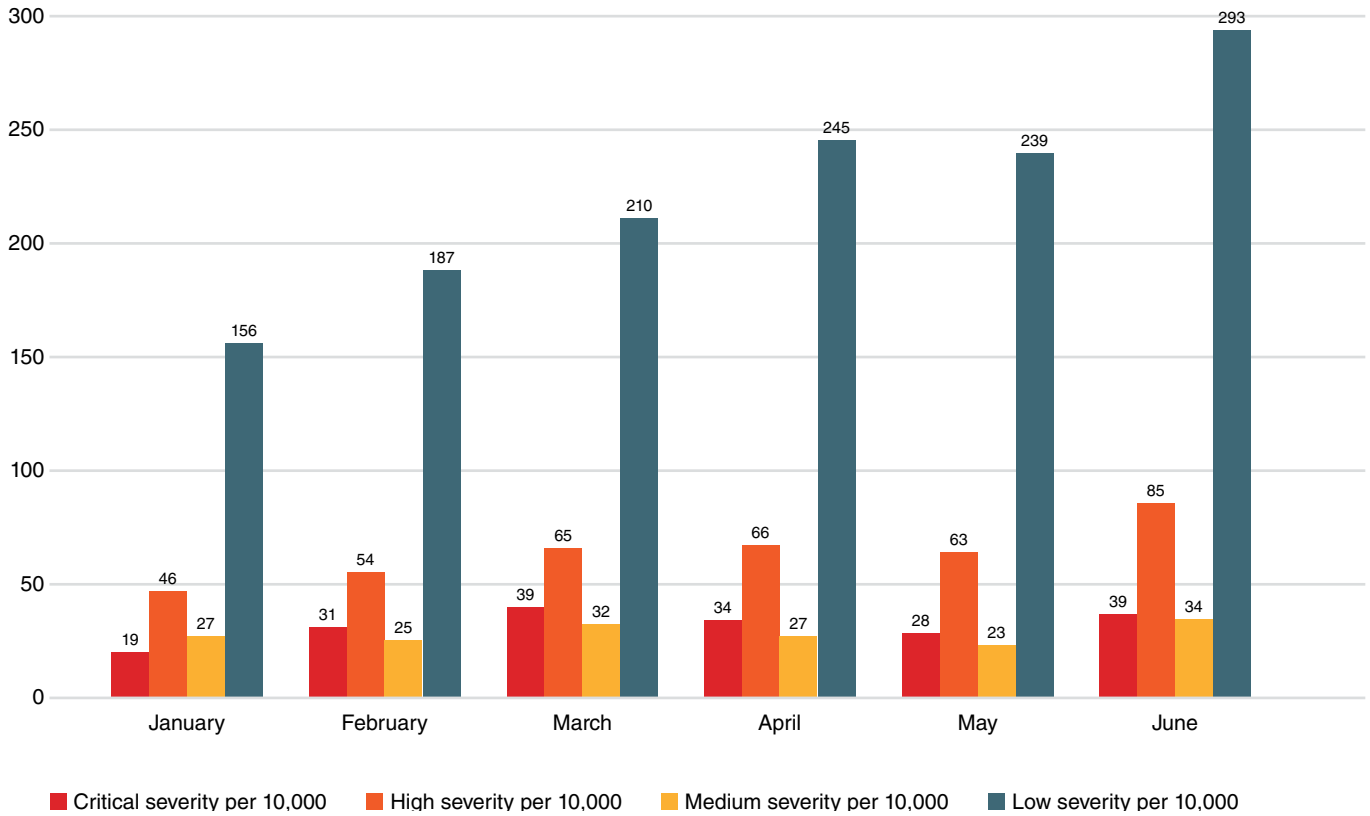


Figure 3: Threat-severity scores in manufacturing per 10,000 host devices

Botnet attack behaviors

Botnets represent opportunistic attacks that are not targeted at specific organizations. While botnet attacks persist everywhere, their occurrence is not significant in manufacturing and is more often associated with user desktops that browse the web.

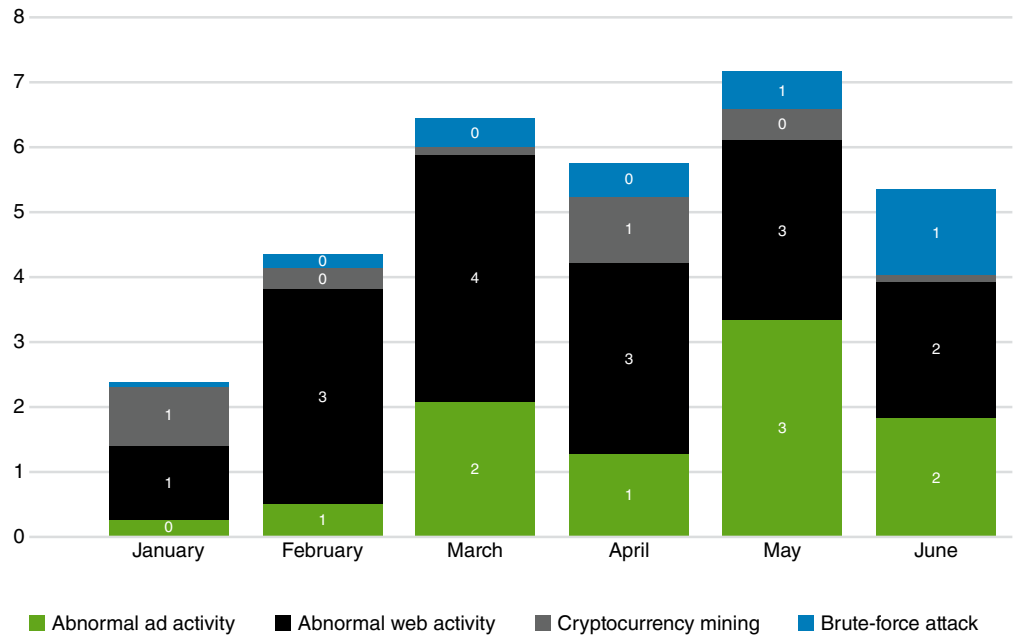


Figure 4: Botnet attack behaviors in manufacturing per 10,000 host devices

Command-and-control behaviors

The use of external remote access tools is the most common command-and-control behavior in manufacturing, which is shown in green in Figure 5. External remote access occurs when an internal host device connects to an external server.

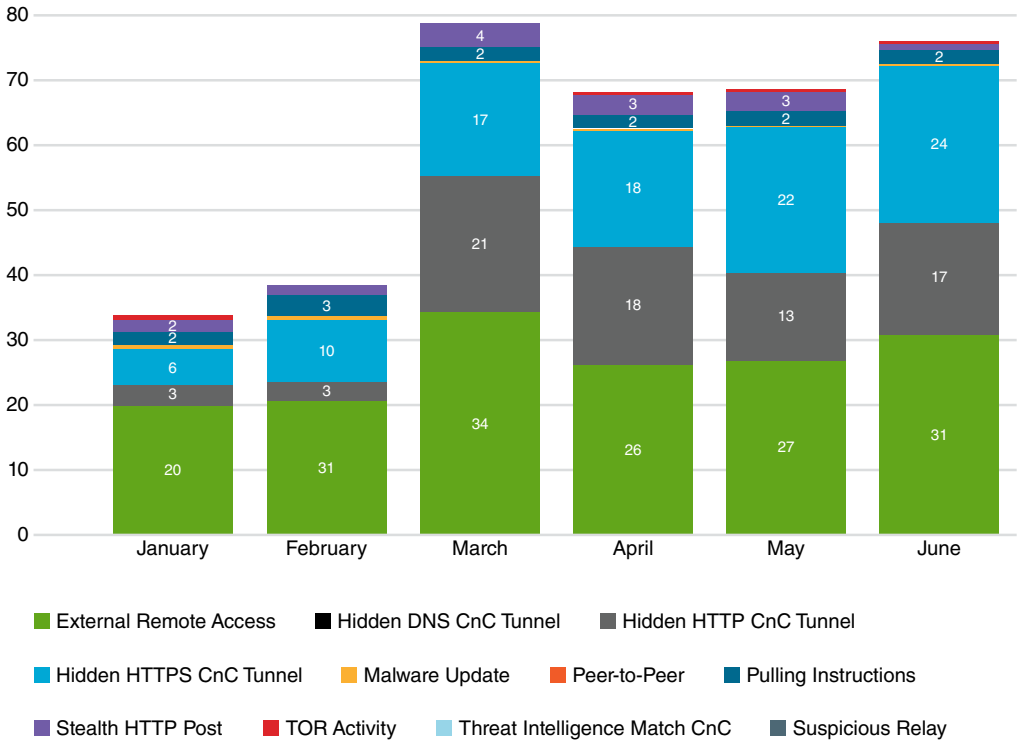


Figure 5: Command-and-control behaviors in manufacturing per 10,000 host devices

In this instance, the behavior is inverse from normal outbound client-to-server traffic. The client receives instructions from the external server, and a human on the outside controls the exchange.

While external remote access is common in manufacturing operations, it introduces risk. Cyberattackers also perform external remote access, but with the intent to disrupt industrial control systems.

Additionally, IIoT devices can be used as a beachhead to launch an attack. Once an attacker establishes a foothold in IIoT devices, it is difficult for network security systems to identify the backdoor compromise.

Consequently, IIoT devices collectively represent a vast, easy-to-penetrate attack surface that enables cybercriminals to perform internal reconnaissance, with the goal of stealing critical assets and destroying infrastructure.

Internal reconnaissance behaviors

Vectra observed a spike in internal reconnaissance behaviors in manufacturing due to internal darknet scans and SMB account scans, as shown in Figure 6. Internal darknet scans occur when internal host devices search for internal IP addresses that do not exist on the network.

An SMB account scan occurs when a host rapidly makes use of multiple accounts via the SMB protocol, which can be used for file sharing, RPC and other lateral movement.

Manufacturing networks consist of many gateways that communicate with smart devices and machines. These gateways are connected to each other in a mesh topology to simplify peer-to-peer communication. Cyberattackers leverage the same self-discovery used by peer-to-peer devices to map a manufacturing network in search of critical assets to steal or damage.

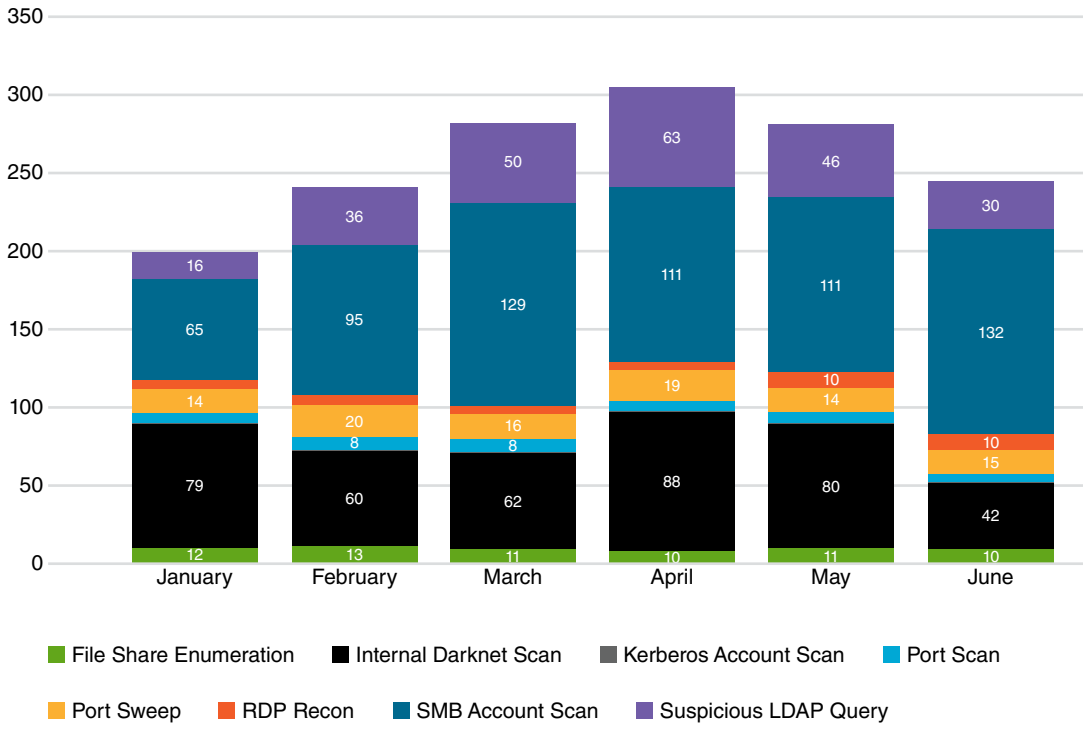


Figure 6: Internal reconnaissance behaviors in manufacturing per 10,000 host devices

Lateral movement behaviors

Lateral movement occurs when connected systems and devices communicate with each other across the network. Figure 7 shows a high level of activity associated with authentication, with SMB brute-force behaviors being the most common.

SMB brute-force behaviors occur when an internal host utilizes the SMB protocol to make multiple login attempts for the same user account, which most often fail. Vectra observed a high volume of automated replication, which indicates an internal host device is sending similar payloads to several internal targets.

IIoT systems make it easy for attackers to move laterally across a manufacturing network, jumping across non-critical and critical subsystems, until they find a way to complete their exploitative missions.

It is critical to maintain visibility into all internal connected systems to understand which are legitimate and which are attackers propagating on the network.

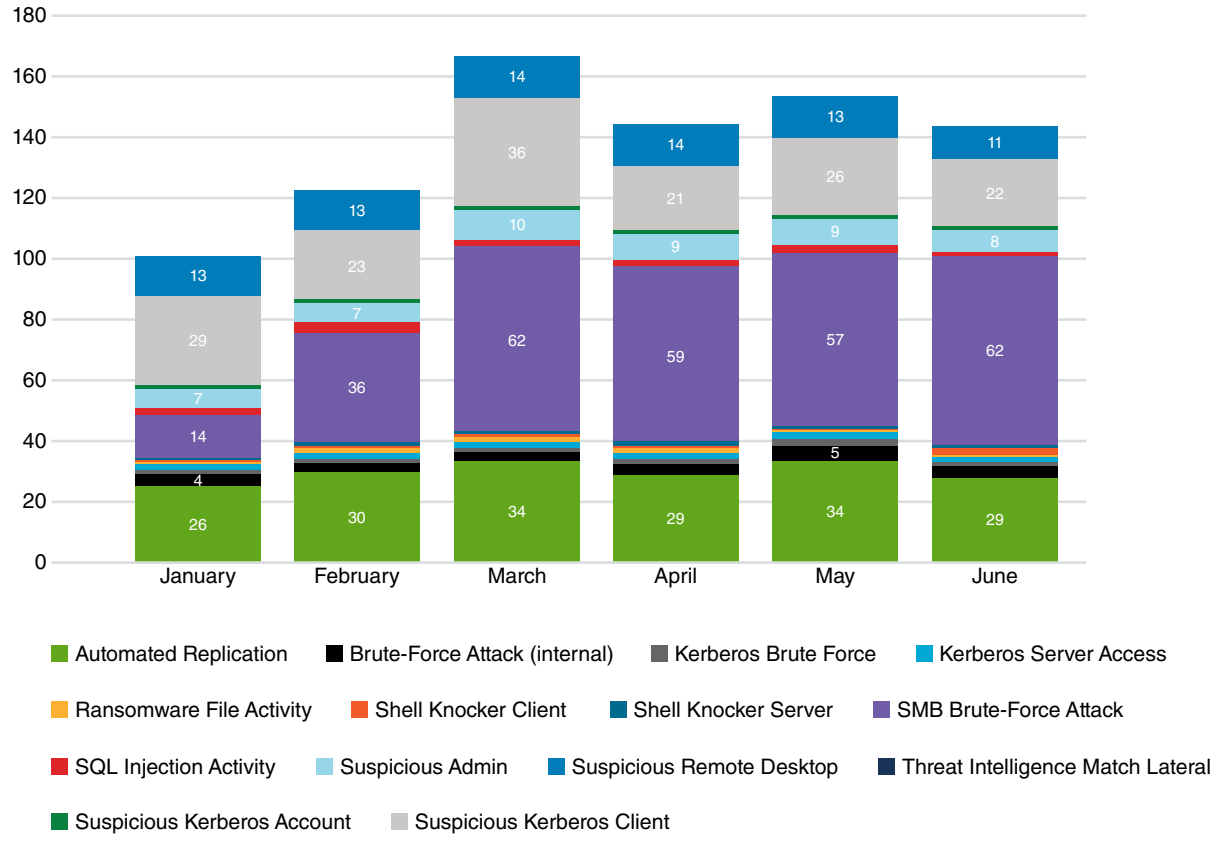


Figure 7: Lateral movement behaviors in manufacturing per 10,000 host devices

Exfiltration behaviors

Among exfiltration behaviors, data smuggling was the most prevalent in the manufacturing industry. With data smuggling, an internal host device controlled by an outside attacker acquires a large amount of data from one or more internal servers and then sends a large data payload to an external system.

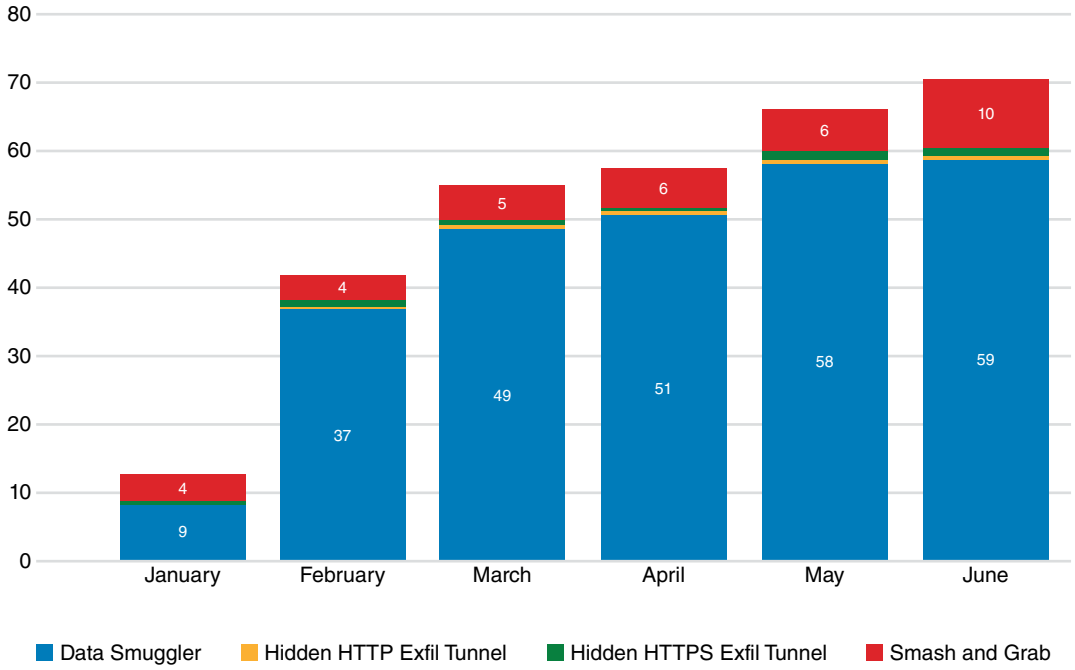


Figure 8: Exfiltration behaviors in manufacturing per 10,000 host devices

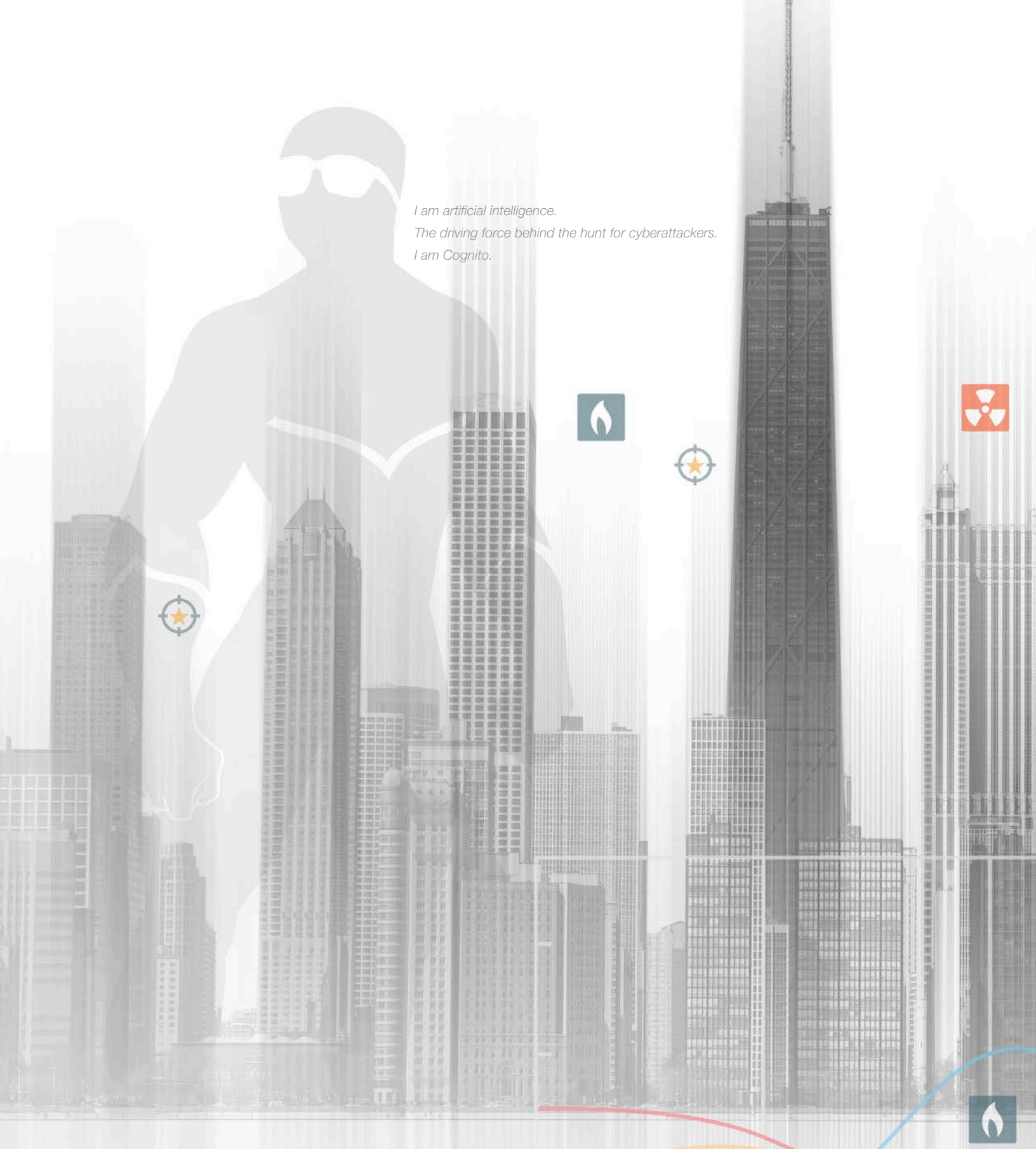
Conclusion

Driven by Industry 4.0 initiatives, more manufacturing processes are becoming automated and connected to the cloud, resulting in big improvements for speed and efficiency of industrial production.

But the IT/OT convergence in manufacturing – along with unpartitioned networks, insufficient access controls and the proliferation of IIoT devices – has created a massive and vulnerable attack surface that cybercriminals can exploit to steal intellectual property and disrupt business operations.

Consequently, a higher-than-normal rate of malicious internal reconnaissance behaviors indicates that attackers are mapping-out manufacturing networks in search of critical assets to steal or damage. And the abnormally high level of lateral movement behaviors is a strong indicator that attacks are proliferating inside the network.

To learn more about cyberattacker behaviors seen in other real-world cloud, data center and enterprise environments, get the 2018 Black Hat Edition of the Attacker Behavior Industry Report from Vectra.



VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai