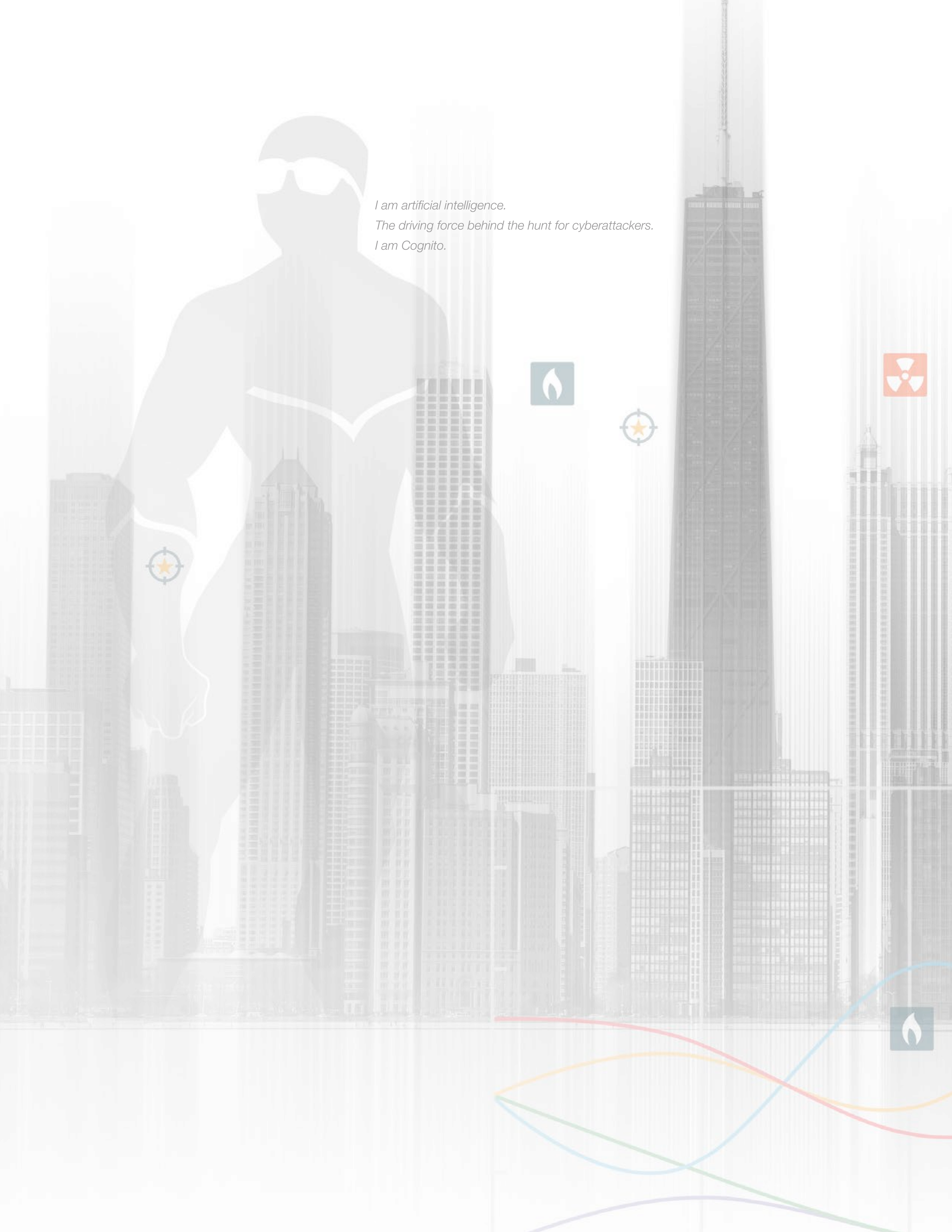
VECTRA®

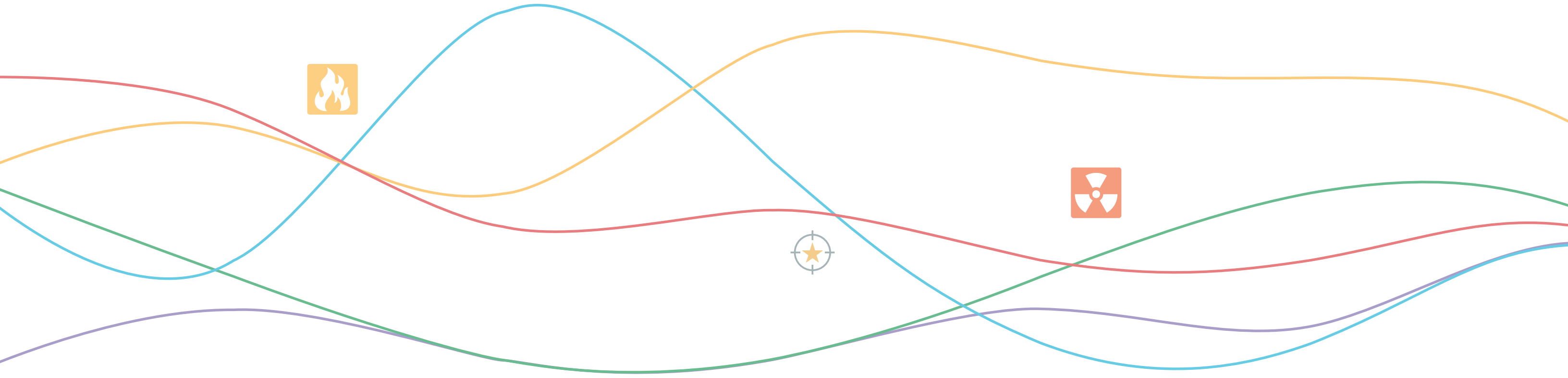
Attacker Behavior Industry Report

2018 Black Hat Edition



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

TABLE OF CONTENTS



The Black Hat Edition of the Vectra® Attacker Behavior Industry Report provides a first-hand analysis of active and persistent attacker behaviors inside cloud, data center and enterprise environments of Vectra customers from January through June 2018.

The report examines a wide range of cyberattack detections and trends from a sample of more than 250 Vectra customers with over 4 million devices per month and workloads from nine different industries.

The research in this report takes a multidisciplinary approach that spans all strategic phases of the attack lifecycle. By using the AI-based Cognito™ platform to detect attacker behaviors, Vectra can identify exposure and risk within organizations as well as indicators of damaging breaches.

Key findings

- Across all industries, there was an average of 2,354 attacker behavior detections per 10,000 host devices. Attacker behaviors from January-June 2018 showed a sharp increase over the same period in 2017.
- Overall, education had the most attacker behaviors at 3,958 detections per 10,000 host devices.
- Energy (3,740 detections per 10,000 host devices) and manufacturing (3,306 detections per 10,000 host devices) showed a large amount of detections due to high levels of lateral movement. Energy and manufacturing are also large adopters of industrial IoT (IIoT) devices and have IT/OT system integration.
- Command-and-control (C&C) activity in higher education continues to persist three-times above the industry average of 725 per 10,000 host devices and exceeds every industry with 2,143 detections per 10,000 host devices. These early attack indicators usually precede other phases of attacks and are often associated with opportunistic botnet behaviors in higher education.
- The retail and healthcare industries have the lowest cyberattack-detection rates, with 1,190 and 1,361 detections per 10,000 host devices, respectively.
- Botnet activity occurs most often in higher education, with 183 detections per 10,000 host devices, which is three-times the industry average of 53 detections per 10,000 host devices. These opportunistic attack behaviors leverage host devices for external gain, such as bitcoin mining or outbound spam.
- Vectra customers achieved a 36X workload reduction for Tier-1 analysts in detection, triage, correlation and prioritization of security incidents, enabling them to focus on mitigating the highest-risk threats.
- When normalizing attacker detections per 10,000 host devices compared to the previous year, there is a sharp increase in every industry for C&C, internal reconnaissance, lateral movement and data exfiltration detections.

Background and methodology

The information in this report is based on anonymized metadata from Vectra customers who have opted to share detection metrics. Vectra identifies behaviors that indicate attacks in progress by directly monitoring all traffic and relevant logs, including traffic to and from the internet, internal traffic between network host devices, and virtualized workloads in private data centers and public clouds.

This analysis provides important visibility into advanced phases of attacks. The Cognito platform from Vectra detects threats that evade perimeter security controls and observes the progression of attacks after the initial compromise.

The 2018 Black Hat Edition of the Vectra Attacker Behavior Industry Report also presents data by specific industries and highlights relevant differences between industries.

From **January through June 2018**, Vectra collected data on more than **4 million devices and workloads per month**. On these devices and workloads, Vectra detected over **10 million different attacker behaviors** that were condensed to **668,000 detections**.

These detections were then triaged down to **420,000 host devices and workloads**. Across all participating organizations, for the six-month period, over **32,000** devices and workloads were tagged as **critical** in risk and over **63,000** were tagged as **high** in risk, enabling security analysts to respond quickly to mitigate these threats. On average, in a single month, **5,343** devices and workloads were tagged as **critical** and **10,438** devices and workloads were tagged as **high**.

Operational efficiency and ROI

Cybersecurity is an ongoing exercise in operational efficiency. Organizations have limited resources to address unlimited risks, threats and attackers. This means that security products must always be evaluated in terms of their efficiency and impact on the operational fitness of the organization.

Time is the most important factor in detecting hidden cyberattacks. To mitigate damage, attacks must be detected in real time before key assets are stolen or damaged. However, detecting and responding to targeted attacks is a very time-consuming process and requires security teams to manually sort through mountains of alerts.

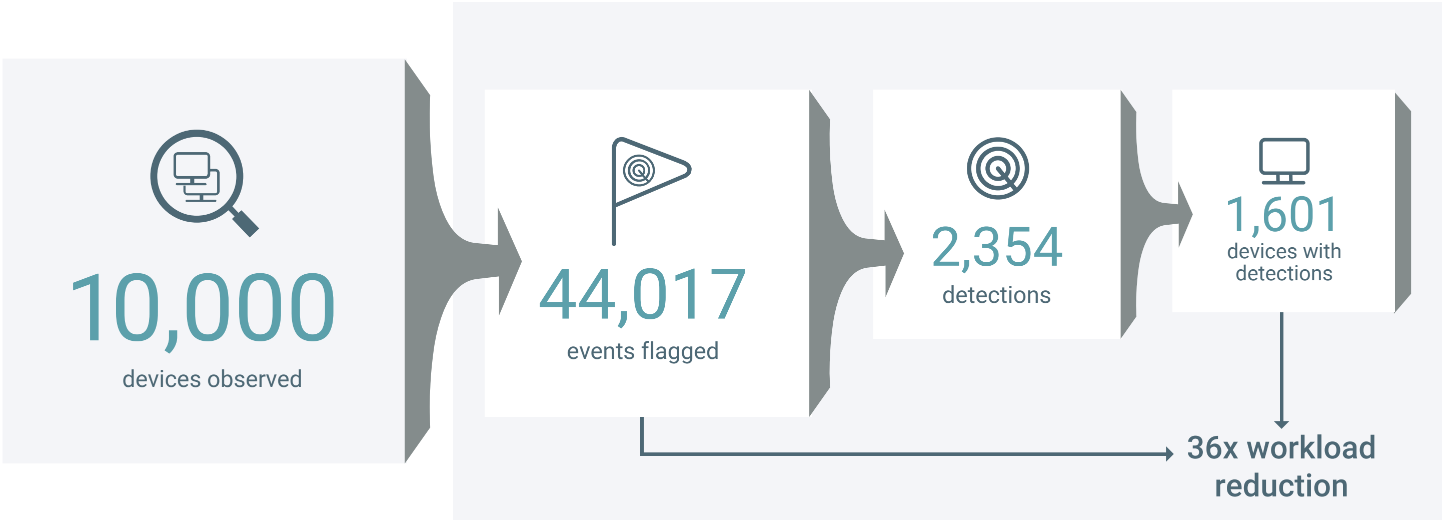
Using artificial intelligence (AI), the Cognito platform from Vectra performs nonstop automated detection of threat behaviors in real time. These behaviors are correlated with compromised host devices, which are in turn correlated with common attack vectors and larger attack campaigns. Thousands of threat indicators are reduced to hundreds of attacker behaviors on dozens of host devices that can be part of broader attack campaigns.

It is important to note that attacker behaviors are still only indicators of compromise. Security analysts must take final action to validate whether an attack is real. Cognito provides security analysts with the most important information in context, which can be used to decide how to respond before an attack causes damage.

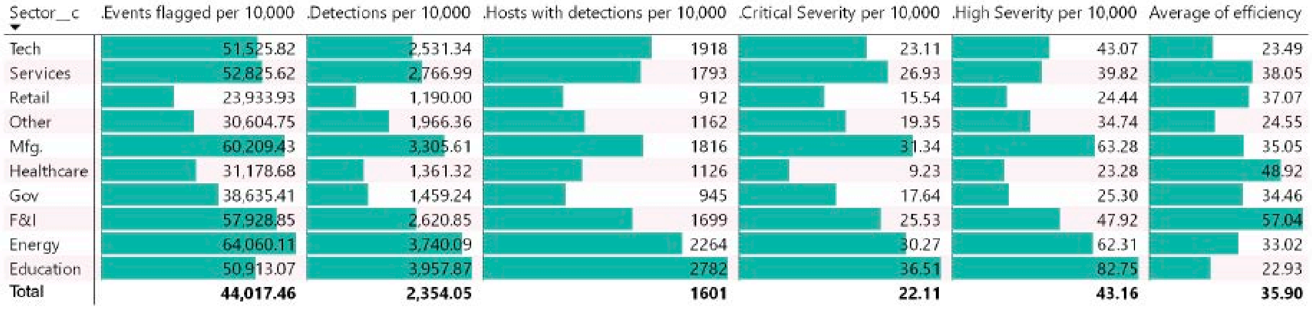
There was a wide variance in the sizes of the networks analyzed, with the smallest consisting of a few hundred host devices and workloads to the largest networks with more than 500,000.

To account for this variance, the data has been normalized to a network with 10,000 host devices and workloads, making it easier to compare the prevalence of threats in a network on a per capita basis. Any host device with an IP address – including IoT devices, smartphones, tablets and laptops – are monitored in addition to servers and virtualized workloads.

Reduction in workload for Tier-1 security analysts



Overall, Vectra reduced the investigation workload of security analysts by 36X compared to manually investigating all attacker behaviors and compromised host devices. There is a significant uptick in the total number of events flagged and nearly twice the number of detections per 10,000 host devices observed.



Sector_c	.Events flagged per 10,000	.Detections per 10,000	.Hosts with detections per 10,000	.Critical Severity per 10,000	.High Severity per 10,000	Average of efficiency
Tech	51,525.82	2,531.34	1918	23.11	43.07	23.49
Services	52,825.62	2,766.99	1793	26.93	39.82	38.05
Retail	23,933.93	1,190.00	912	15.54	24.44	37.07
Other	30,604.75	1,966.36	1162	19.35	34.74	24.55
Mfg.	60,209.43	3,305.61	1816	31.34	63.28	35.05
Healthcare	31,178.68	1,361.32	1126	9.23	23.28	48.92
Gov	38,635.41	1,459.24	945	17.64	25.30	34.46
F&I	57,928.85	2,620.85	1699	25.53	47.92	57.04
Energy	64,060.11	3,740.09	2264	30.27	62.31	33.02
Education	50,913.07	3,957.87	2782	36.51	82.75	22.93
Total	**44,017.46**	**2,354.05**	**1601**	**22.11**	**43.16**	**35.90**

Threat and certainty scores

The Cognito platform from Vectra monitors individual devices and workloads for extended periods of time and attributes detections to any device or workload that behaves suspiciously. The detection scores and times they occurred are key inputs for the host device threat-severity and certainty scores.

Cognito scoring is comprised of two dynamic metrics – threat and certainty scores – applied to individual detections and the host devices against which they are reported.

The threat score of a detection expresses the potential for harm if the security event is true (e.g. if spamming behavior or data exfiltration was occurring). Because a threat is a measure of the potential for harm, it reflects worst-case scenarios.

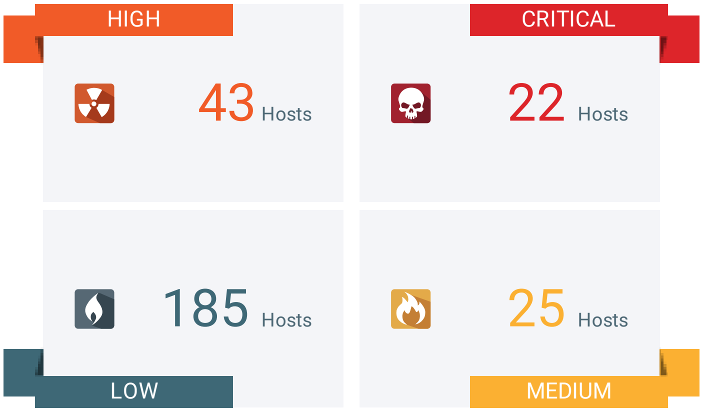
The certainty score of a detection reflects the probability that a given security event occurred (e.g. the probability of spamming behavior occurring, or the probability of data exfiltration occurring), given all the evidence observed so far.

Certainty is based on the degree of difference between the threat behavior that caused the detection and normal behavior. As such, the certainty score of an individual detection changes over time.

Since detections are dynamic, changes in their scores cause changes to attributed host device threat-severity and certainty scores. Critical and high scores help security analysts prioritize their investigation efforts because they represent behaviors with the highest certainty and greatest potential to cause significant damage.

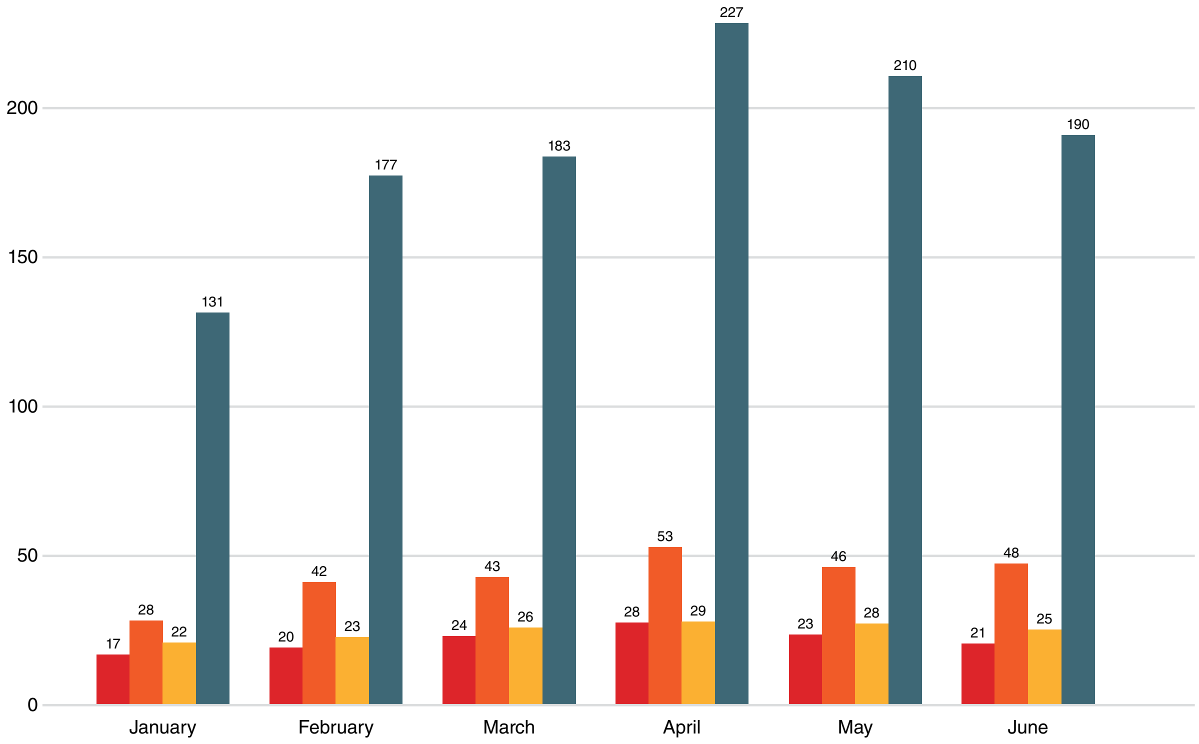
Other factors that influence host device scores include repetition of an observed detection or a combination of detections that indicate a cyberattack is progressing toward its objective.

Every detection type has a maximum lifespan, ranging from a few days to a month. When a detection has no recurring activity, its effect on a host device score slowly declines to zero. A detection past its maximum lifespan becomes inactive and has no impact on the host device score.

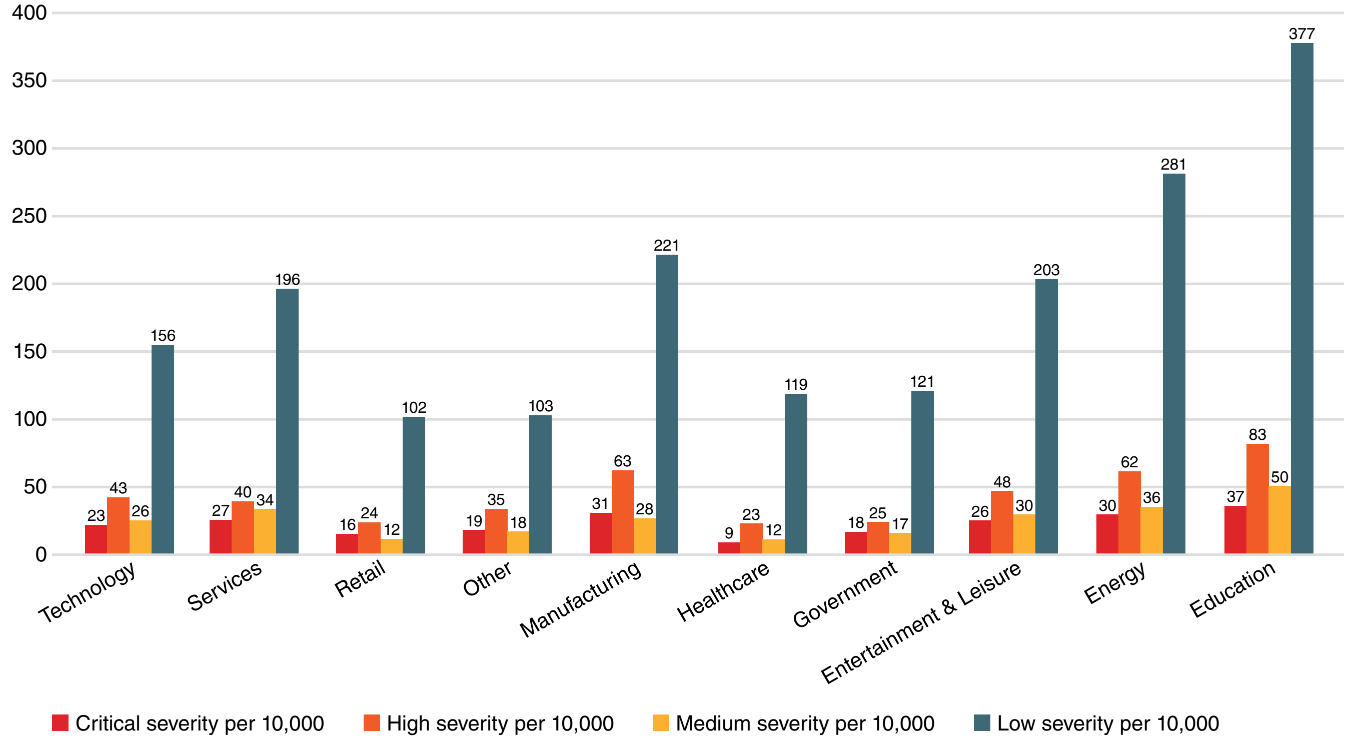


On average, for every 10,000 host devices and workloads monitored in a one-month period, 22 were marked critical and 43 were marked high. These devices and workloads present the greatest threat to the organization and require a security analyst's immediate attention.

Threat-severity and certainty scores per 10,000 host devices and workloads



When breaking down host device statistics across vertical industries, Vectra benchmarked the volume of host devices and workloads prioritized for each threat-severity and certainty level, both in relation to each vertical and as compared to the combined industry threat-severity and certainty scores.



For example, the number of low alerts in higher education is almost twice the normal rate, which indicates attacker behaviors that are opportunistic.

Inversely, the healthcare industry has a low volume of host devices prioritized as high or critical, which indicates that cyberattacks in healthcare do not often progress deep into the attack lifecycle.

Overall detection trends

- **Detection rates:** Organizations had an average of 1,707 host devices with threat detections for every 10,000 host devices in a one-month period. This represents a 36X reduction in the number of events requiring investigation and triage.
- **C&C represented the highest percentage of detections:** C&C traffic is a key component of a botnet attack and is an enabler for later phases of a targeted attack. It is often the first sign of an attack in targeted and opportunistic activity.
- **Cognito from Vectra provides security teams with new efficiencies:** While the symptoms of targeted attacks remain common, there are encouraging signs that security teams are finding and stopping attacks before damage is done.
- **Cryptocurrency mining continues to be the most popular form of opportunistic attacks:** While considered opportunistic, cryptocurrency mining continues to experience a surge in activity. These behaviors are seen predominantly in higher education, where student systems are cryptojacked or students perform the mining.

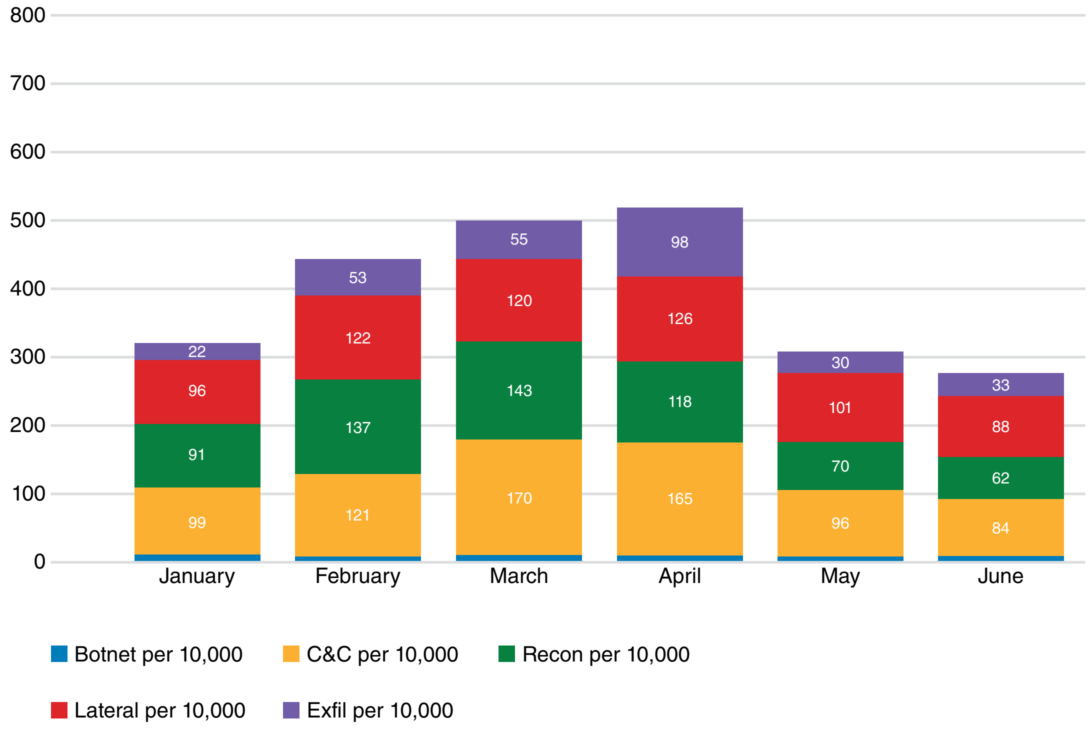
Threats by type per 10,000 host devices

To dig deeper, Vectra provides a breakdown of detection statistics by industry. The charts below show threat behaviors across the attack lifecycle. These behaviors are strong indicators of exposure and risk in an organization and enable security analysts to focus their time and effort on what matters most.

While not every stage is necessary in an attack, each is interrelated, and we often see an attack progress through the lifecycle with the ultimate outcome of financial gain, data exfiltration or data destruction.

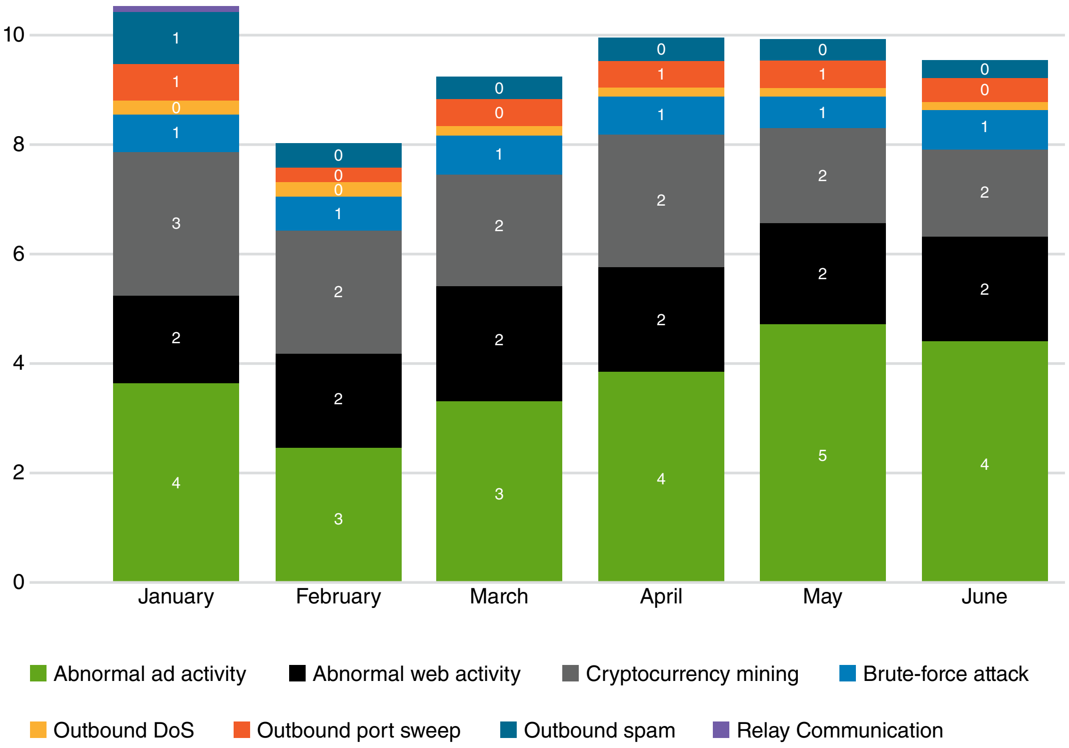
The data in this report represents in-progress attacker behaviors. Activity like C&C and reconnaissance occur in the earlier stages of an attack, enabling organizations to quickly mitigate the threat before it can spread. These are the most common detected behaviors.

Behaviors like lateral movement occur later in the attack lifecycle as cybercriminals strengthen their foothold in an organization by stealing administrative credentials to access servers. These types of detections warrant high-priority action from incident response teams to prevent irreversible damage from a data exfiltration.



Botnets

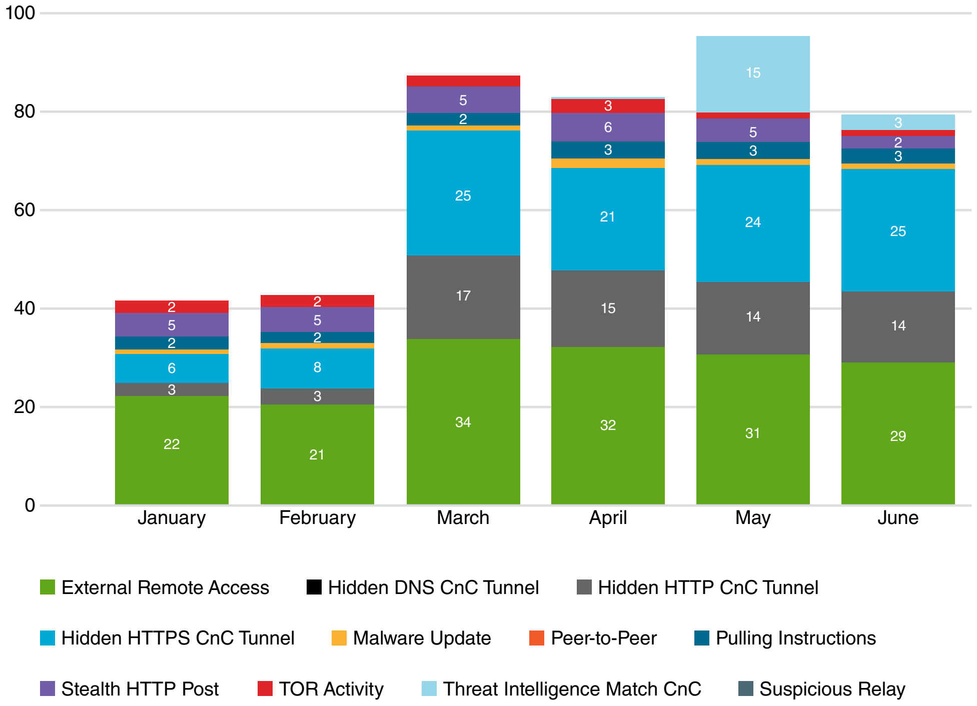
Botnets are opportunistic attack behaviors in which a device makes money for its bot herder. The ways in which an infected host device can be used to produce value can range from cryptomining to sending spam emails to producing fake ad clicks. To turn a profit, bot herders utilize devices, their network connections and, most of all, the unsullied reputation of their assigned IP addresses.



Command and control

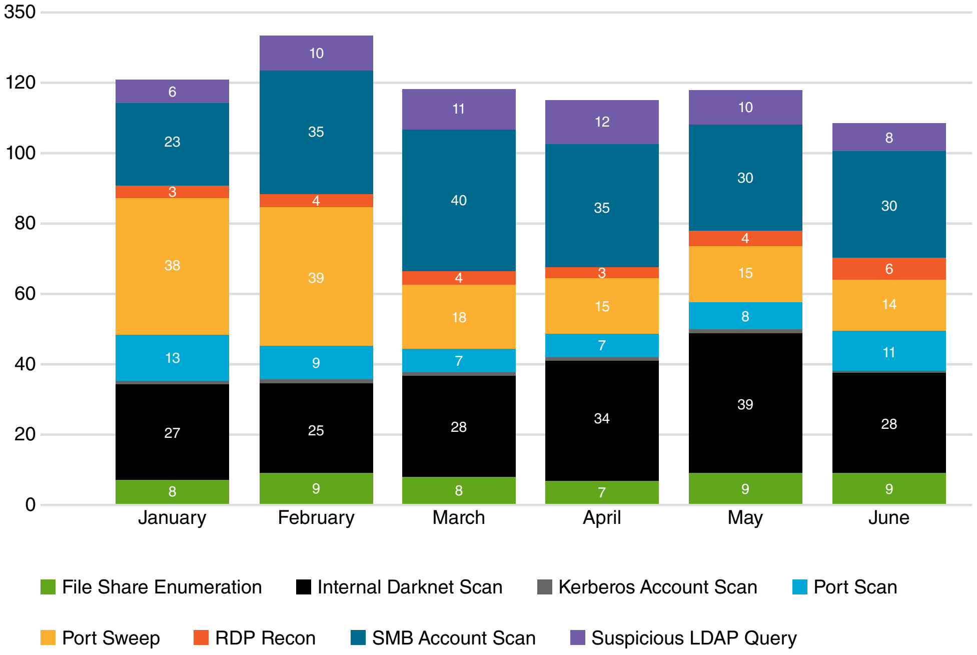
C&C traffic occurs when a device appears to be under the control of an external malicious entity. Most often, the control is automated because the device is part of a botnet or has adware or spyware installed.

Rarely, but most importantly, a device can be manually controlled by a nefarious outsider. This is the most threatening case, and it often means the attack is targeted at a specific organization.



Reconnaissance

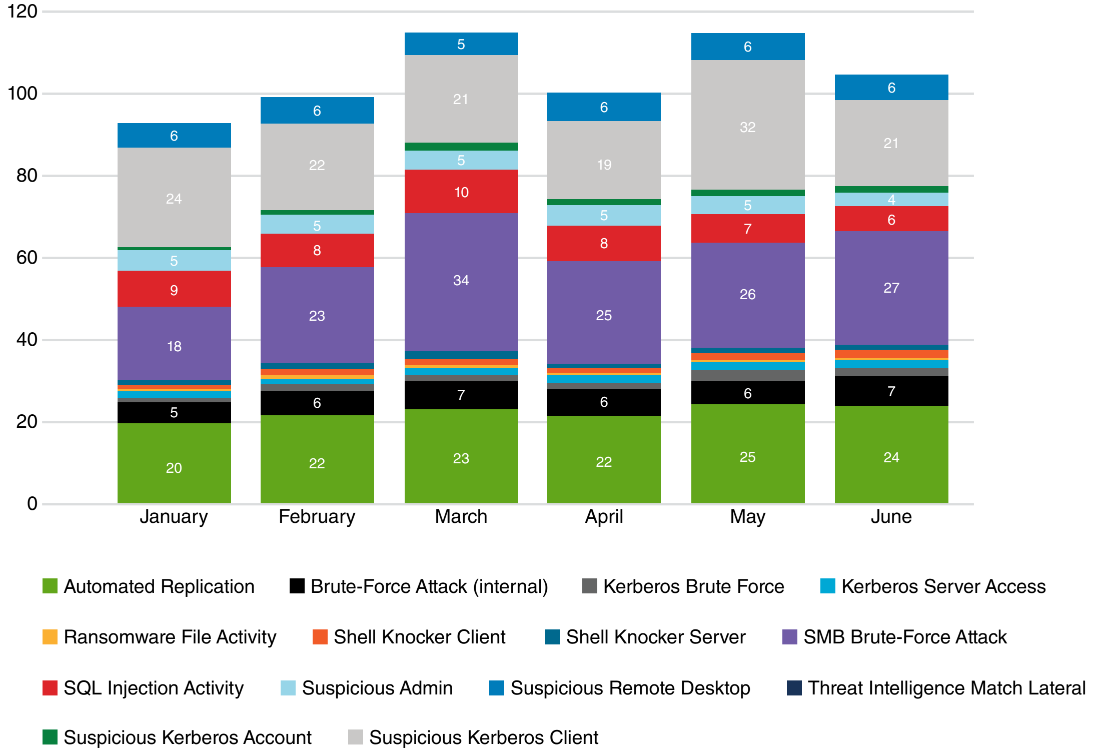
Reconnaissance attacker behaviors occur when a device is used to map-out the enterprise infrastructure. This activity is often part of a targeted attack, although it might indicate that botnets are attempting to spread internally to other devices. Detection types cover fast scans and slow scans of systems, network ports and user accounts.



Lateral movement

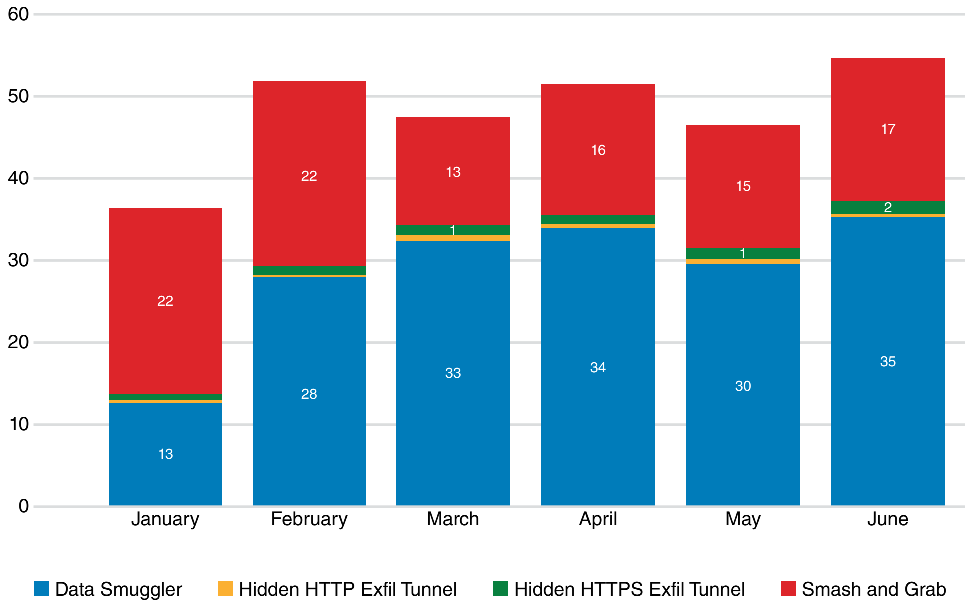
Lateral movement covers scenarios of lateral action meant to further a targeted attack. These can involve attempts to steal account credentials or to steal data from another device.

It can also involve compromising another device to make the attacker's foothold more durable or to get closer to target data. This stage of the attack lifecycle is the precursor to moving into private data centers and public clouds.



Data exfiltration

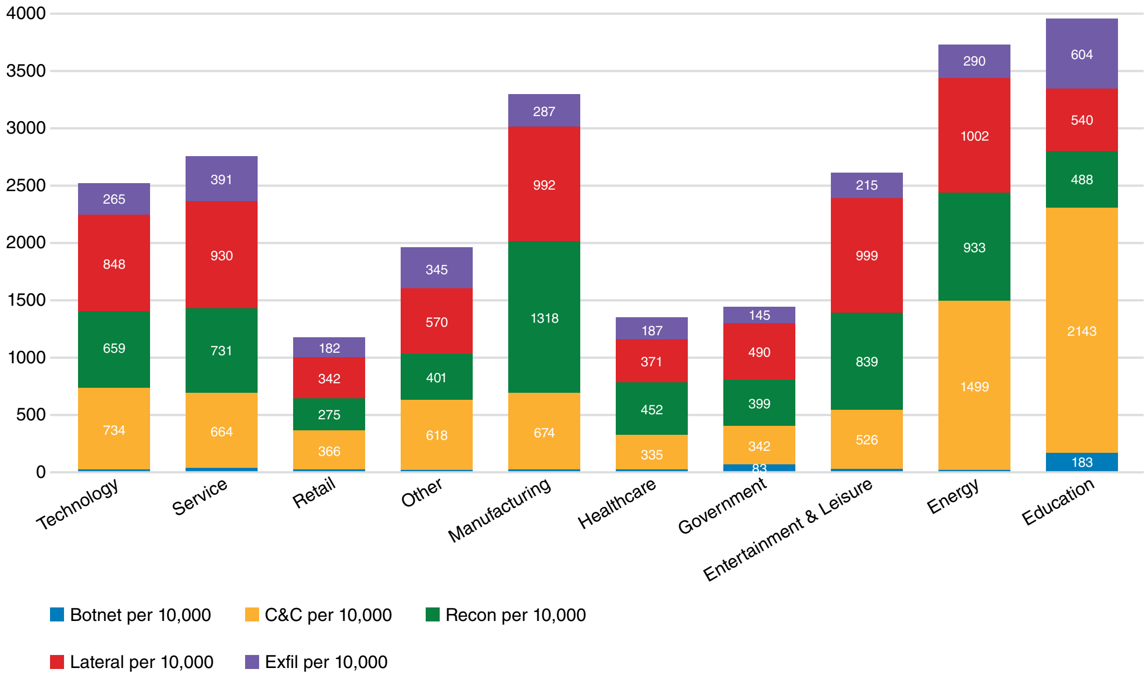
Data exfiltration behaviors occur when data is sent to the outside in a way that is meant to hide the transfer. Normally, legitimate data transfers do not involve the use of techniques meant to hide the transfer. Indicators of exfiltration include the device transmitting the data, the location data is being sent to, the amount of data being sent, and the method used to send it, such as a cloud file share.



Threats by industry per 10,000 host devices

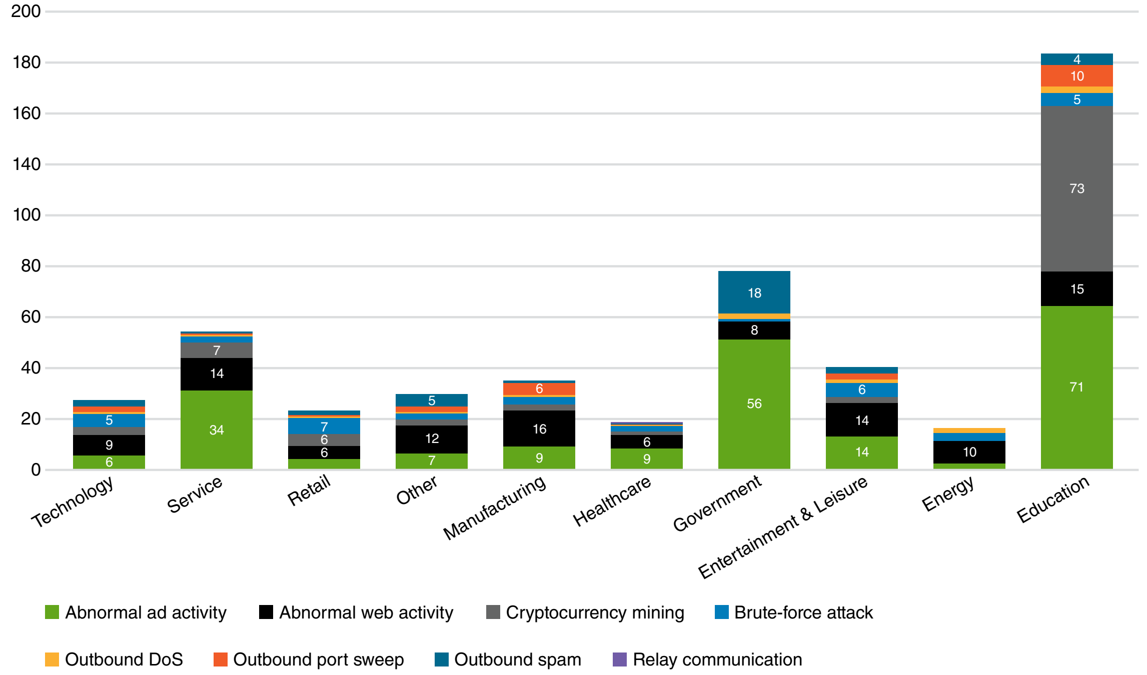
The bar chart below shows the volume of threat detections that were triggered in each industry. This view shows how each industry fared per capita as well as which industries generated the most detections by volume.

Higher education and engineering represent the highest percentages of detections across all industries, primarily due to a high volume of C&C (higher education) and reconnaissance (engineering).



Botnets by industry

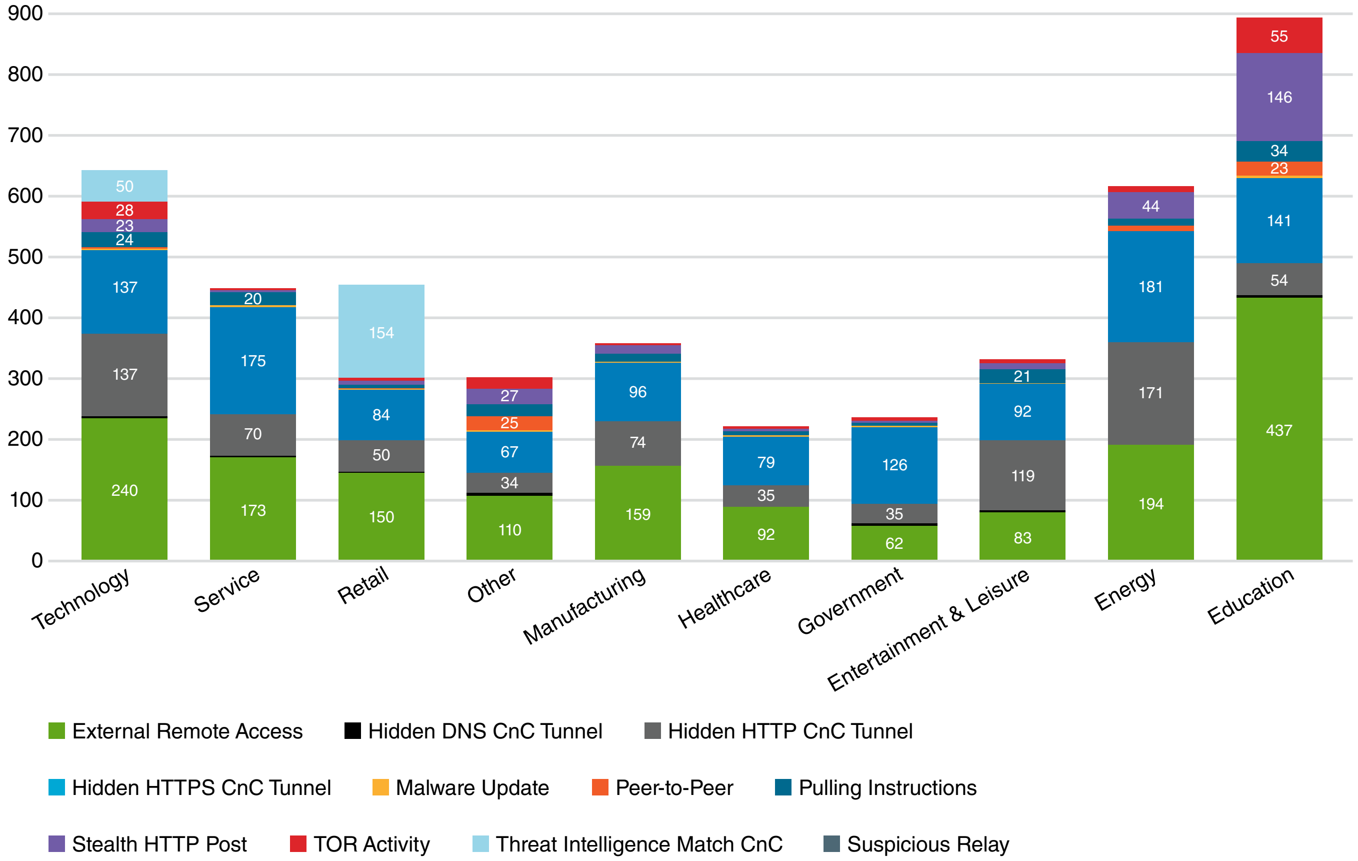
The Cognito platform from Vectra observed an ongoing trend in cryptocurrency mining in higher education. Cryptocurrency mining has experienced a surge in popularity among students who leverage free electricity in their dorms and cyberattackers who target student systems with cryptojacking. Students do not have the same level of security controls as those found in enterprise organizations, making them lucrative targets for botnet herders.



C&C by industry

Due to the association between botnet and C&C traffic, the Cognito platform from Vectra found that higher education has the largest volume of C&C behaviors, primarily related to external remote access and stealth HTTP posts.

Student systems often lack security controls that would normally detect and stop C&C behavior. Students are also more likely to visit suspicious websites that harbor malware. Consequently, C&C attacks are much easier to execute in student environments.

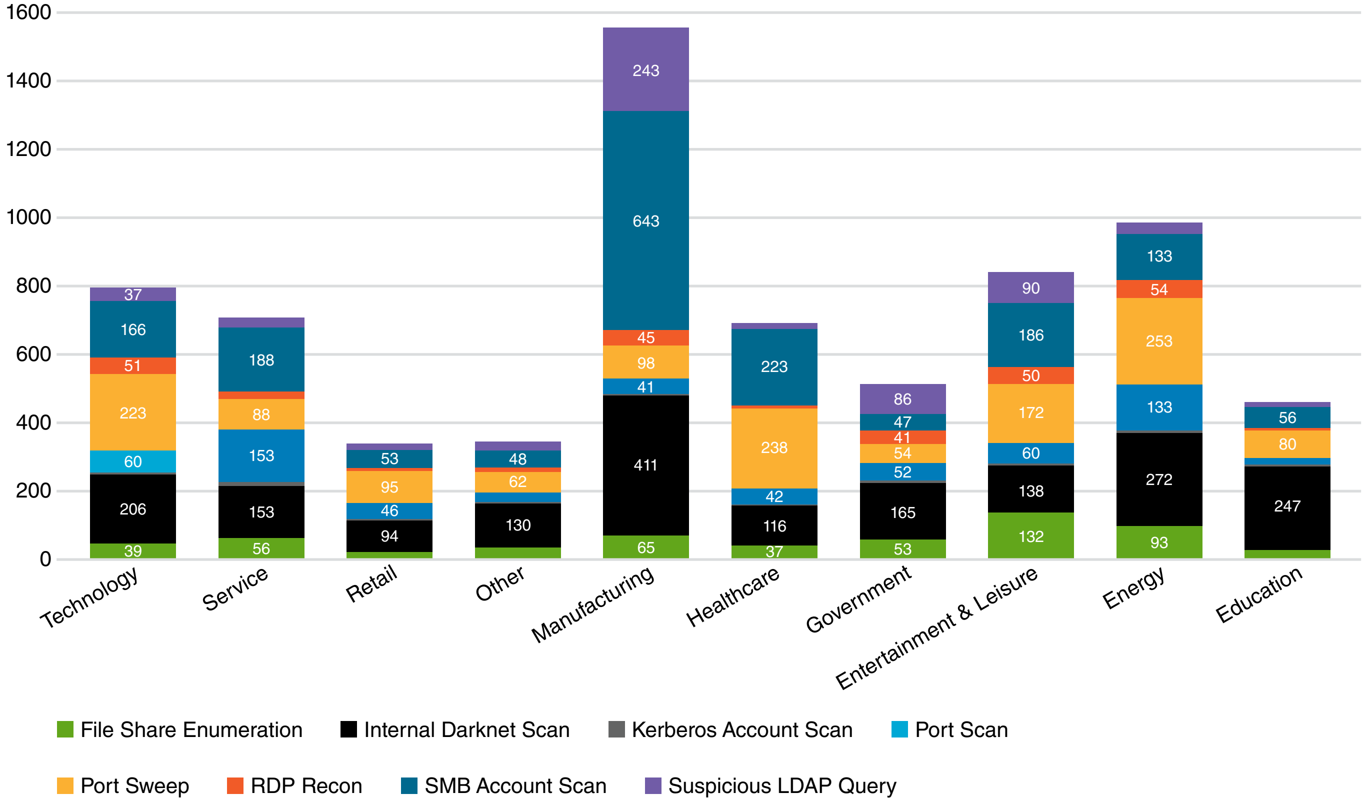


Reconnaissance by industry

Across the board, the Cognito platform from Vectra detected a large volume of darknet scans, which are scans of nonexistent IP addresses on the network. This is quite common for attackers as the first form of reconnaissance behavior. It occurs after C&C communications are established as the attacker looks for targets deeper in the network.

The Cognito platform also detected large volumes of suspicious LDAP in the manufacturing industry. A scan of information in an Active Directory server is an effective way for an attacker to determine what accounts are privileged inside an organization's network and the names of servers and infrastructure components.

Cyberattackers prefer to use this form of reconnaissance because the risk of detection is relatively low, especially compared to a port sweep or a port scan.

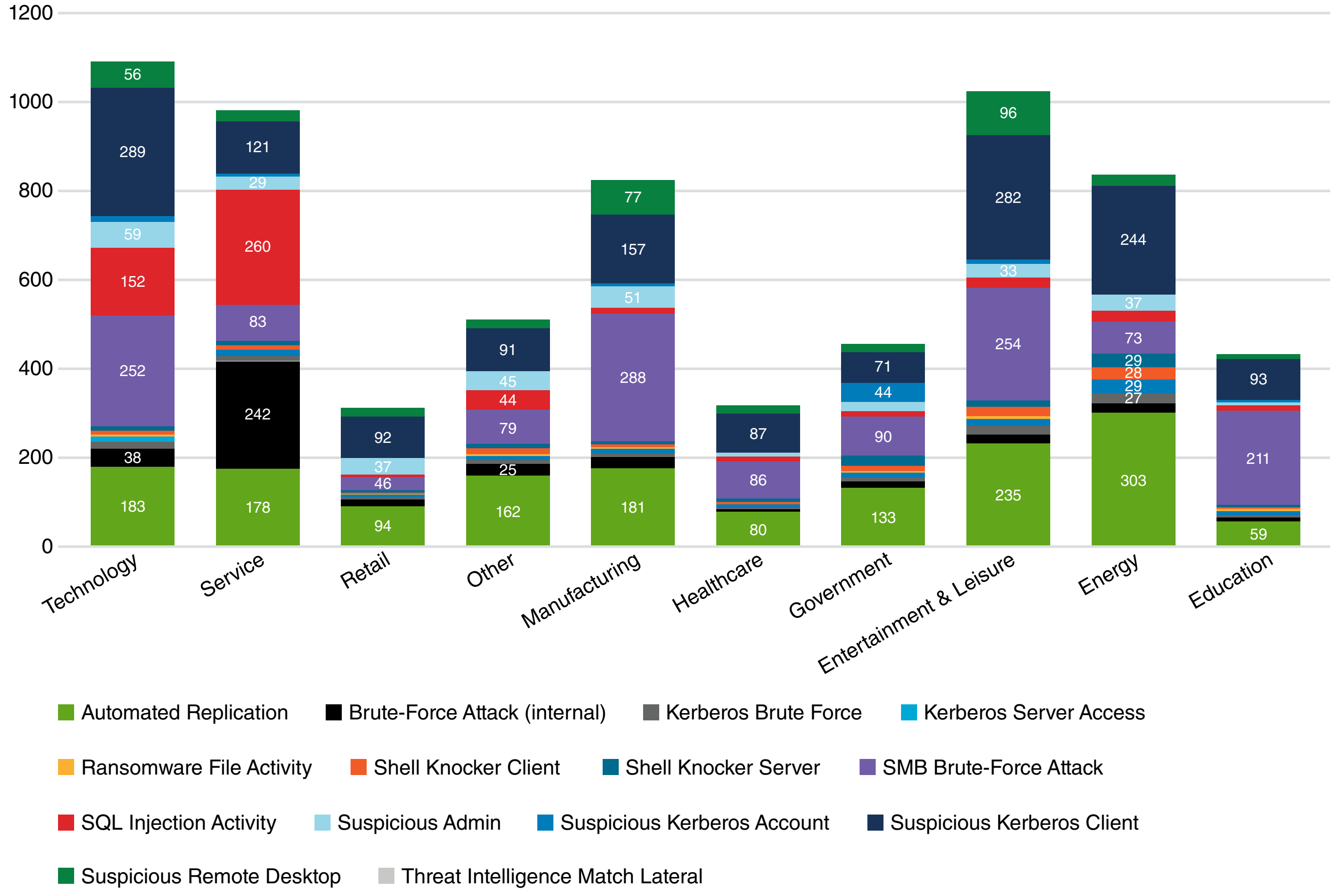


Lateral movement by industry

In technology, services, manufacturing, financial and energy industries, the Cognito platform observed a large spike in Kerberos client anomalous behaviors.

This indicates that a Kerberos account is being used differently than its learned baseline in several ways: Connecting to unusual domain controllers using unusual devices; accessing unusual services; or generating unusual volumes of Kerberos requests using normal domain controllers, usual devices and usual services.

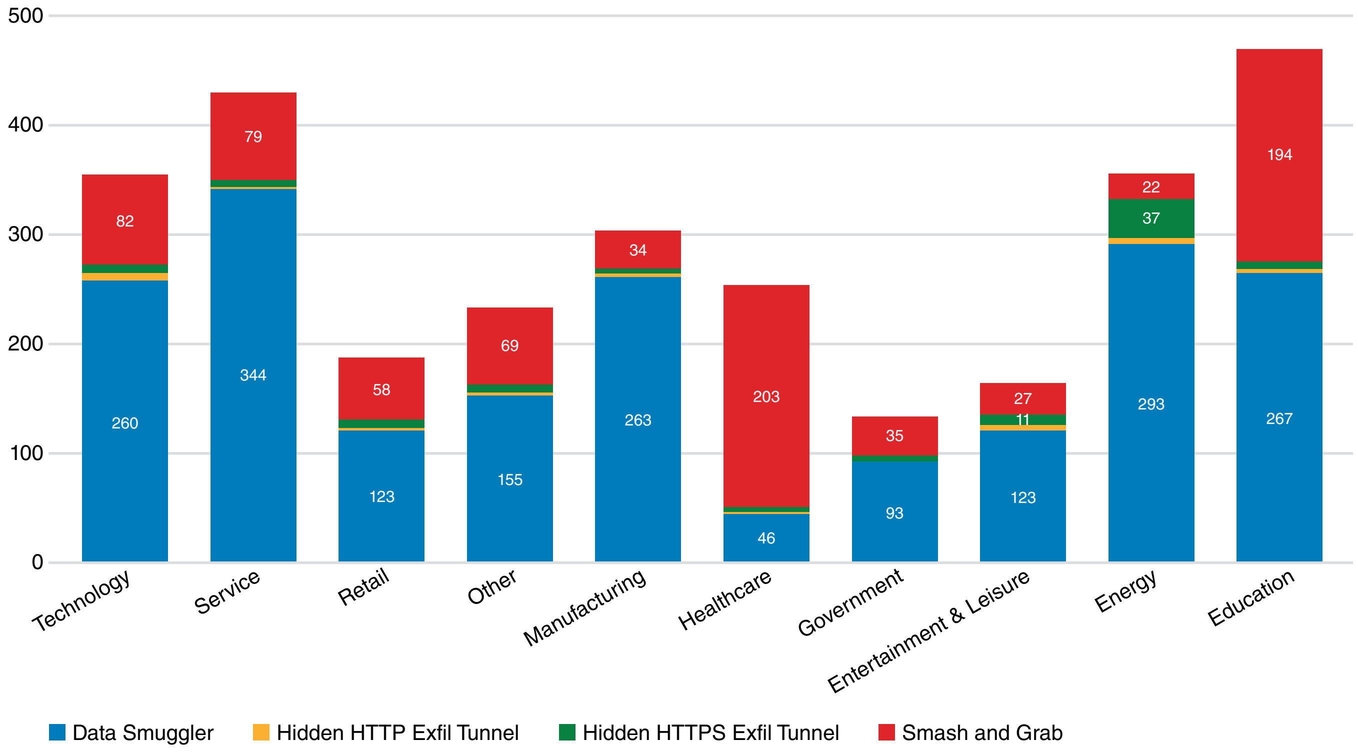
In the technology, manufacturing and education industries, the Cognito platform detected a large volume of SMB brute-force behaviors, which indicates that a device is making multiple login attempts with the same accounts to access a file server.



Exfiltration by industry

The most common exfiltration behavior is data smuggling, which was commonly observed across all industry verticals. It is detected when an internal host device acquires a large amount of data from one or more servers and sends significant volumes of data to an external system.

Smash-and-grab is the second most common exfiltration behavior across all industries. It is triggered when a host device transmits unusually large volumes of data to destinations that are not considered normal for the environment within a short amount of time.



Conclusion

This edition of the Vectra Attacker Behavior Industry Report consisted of more than 4 million devices and workloads per month monitored over a six-month period. Vectra would like to thank the organizations who opted-in to share metadata that was analyzed for this report. Overall, the trends represent an increase in detections and attacker behaviors, which is cause for concern.

As sophisticated cybercriminals automate and increase the efficiencies of their own technology, there is an urgent need to automate attacker-detection and response tools to stop threats faster.

At the same time, there remains a global shortage of highly skilled cybersecurity professionals to handle detection and response at a reasonable speed. As a result, the use of AI is essential to augment existing cybersecurity teams so they can stay well ahead of attackers.

Security that thinks.®

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