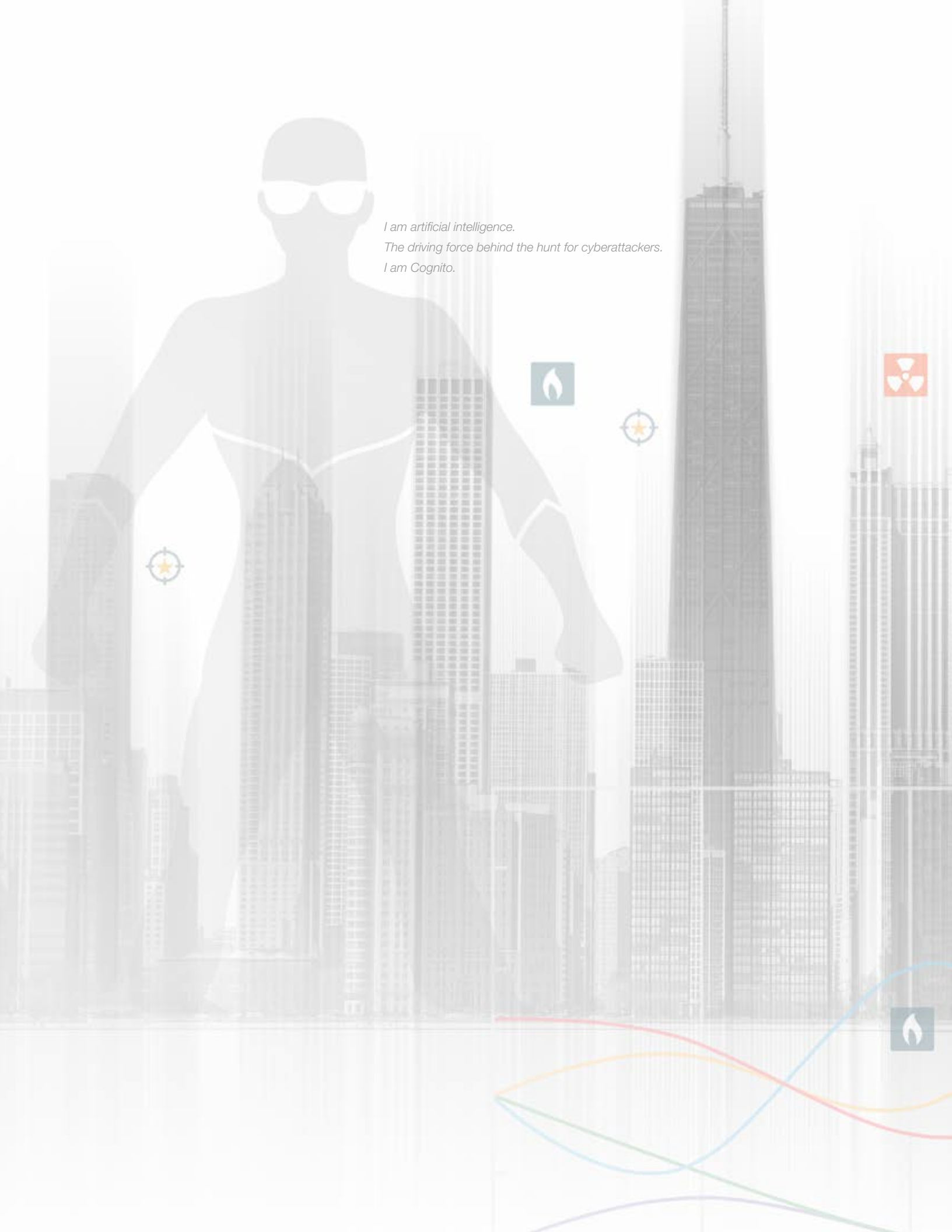
VECTRA

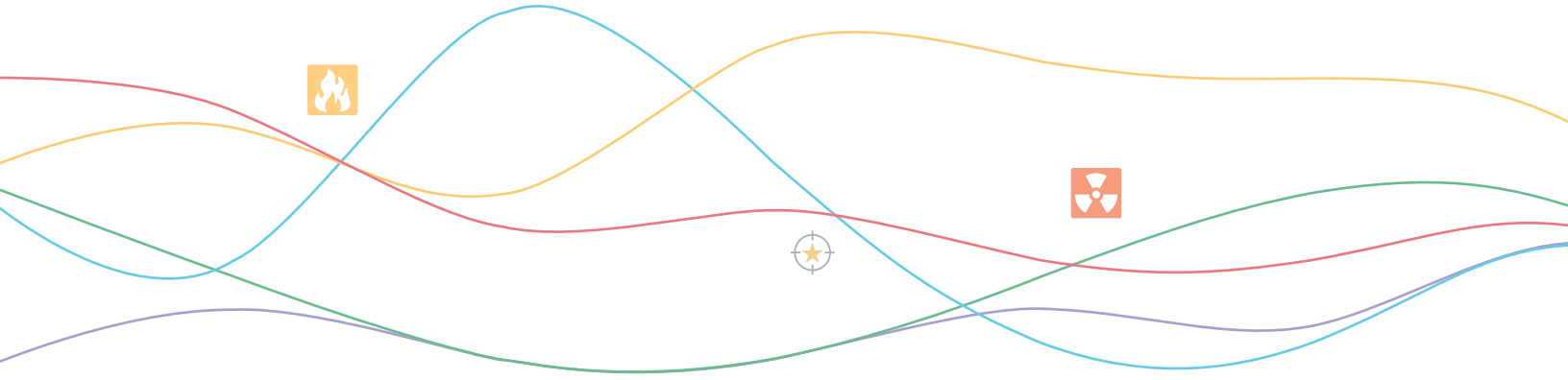
Attacker Behavior Industry Report

2018 RSA Conference Edition


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

VECTRA

TABLE OF CONTENTS



The 2018 RSA Conference 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 August 2017 through January 2018.

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 1,429 attacker behavior detections per 10,000 devices.
- The highest volume of attacker behaviors per industry were in higher education (3,715 detections per 10,000 devices) followed by engineering (2,918 detections per 10,000 devices). This is primarily due to command-and-control (C&C) activity in higher education and reconnaissance activity in engineering.
- C&C activity in higher education is four-times above the industry average of 460 detections per 10,000 devices with 2,205 detections per 10,000 devices. These early attack indicators usually precede other stages and are often associated with opportunistic botnet behaviors in higher education.
- The government and technology industries have the lowest detection rates, with 496 and 349 detections per 10,000 devices, respectively. This could indicate the presence of stronger policies, mature response capabilities, and better control of the attack surface.
- Botnet activity occurs most often in higher education, with 151 detections per 10,000 devices, which is five-times the industry average of 33 detections per 10,000 devices. These opportunistic attack behaviors leverage devices for external gain, such as bitcoin mining or outbound spam.
- Vectra customers achieved a 32X workload reduction for Tier-1 analysts in detection, triage, correlation and prioritization of security incidents, enabling them to focus on compromised devices that pose the highest risk.
- When normalizing detections per 10,000 devices compared to the previous year, there is a sharp increase in every industry for C&C, reconnaissance, lateral movement, and data exfiltration detections.

Background and methodology

The data 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 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 bypass perimeter security controls and observes the progression of the attack after an initial compromise.

The Attacker Behavior Industry Report also presents data by specific industries and highlights relevant differences between industries.

From **August 2017 through January 2018**, Vectra monitored about **4.6 million devices and workloads**. On these devices and workloads, Vectra detected over **12 million different attacker behaviors** that were condensed to **652,000 detections**.

These detections were then triaged down to **373,000 devices and workloads**. Across all participating organizations, in a one-month period, over **6,000** devices and workloads were tagged as **critical** and over **9,000** were tagged as **high-risk**, enabling security analysts to respond fast to mitigate these threats.

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 efficiency and their impact on the operational fitness of the organization.

Time is the most important factor in detecting network breaches. 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.

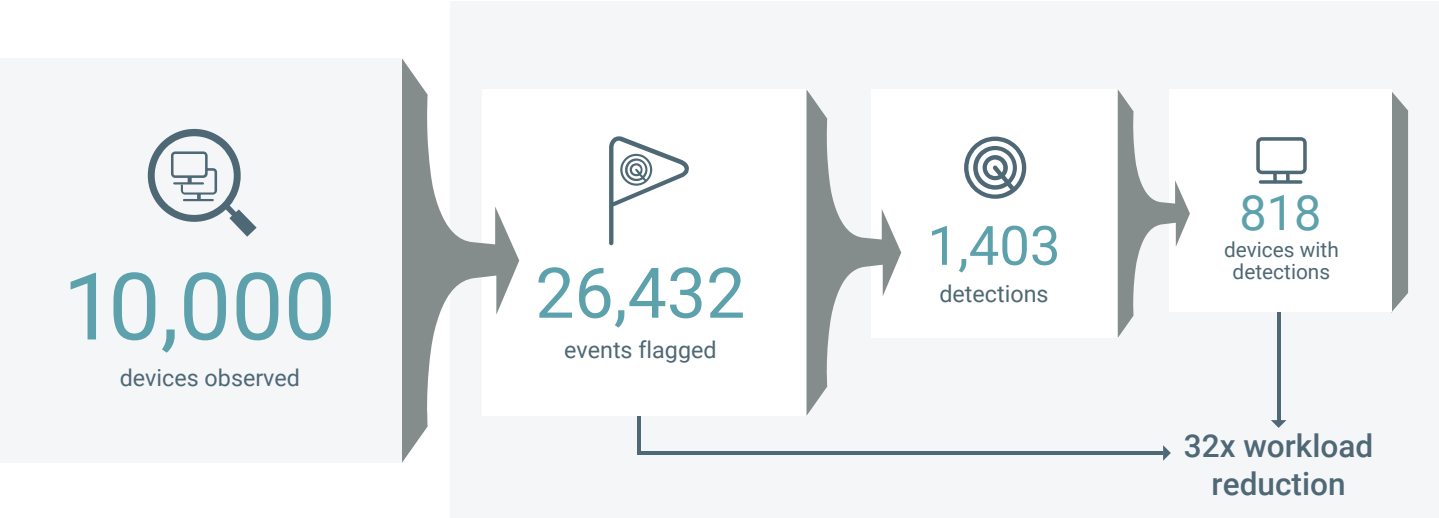
Using AI, Cognito from Vectra performs nonstop automated threat hunting to detect attacker behaviors in real time. These behaviors are correlated with compromised devices, which are in turn correlated with common attack vectors and larger attack campaigns. Thousands of threat indicators are reduced to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

It is important to note that attacker behaviors are 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 on how to respond before an attack causes damage.

There was a wide variance in the size of the networks analyzed, with the smallest consisting of a few hundred devices and workloads to the largest networks with more than 400,000.

To account for this variance, the data has been normalized to a network with 10,000 devices and workloads, making it easier to compare the prevalence of threats in a network on a per capita basis. Any 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 32X, compared to manually investigating all attacker behaviors and compromised host devices.

Scoring

Cognito 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 when they occurred are key inputs for the host device 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.

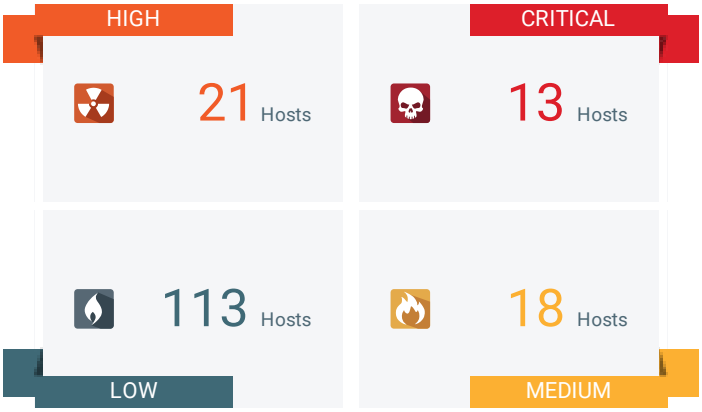
Certainty is based on the degree of difference between the threat behavior that caused the detection and normal behavior. As such, the certainty score of an individual detection changes over time.

Since detections are dynamic, changes in their scores cause changes to attributed host device 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 will slowly decline to zero. A detection past its maximum lifespan becomes inactive and has no impact on the host device score.

For every 10,000 devices and workloads monitored in a one-month period, an average of 13 were marked *critical* and 21 were marked *high*. These devices and workloads present the greatest threat to the organization and require a security analyst's immediate attention.

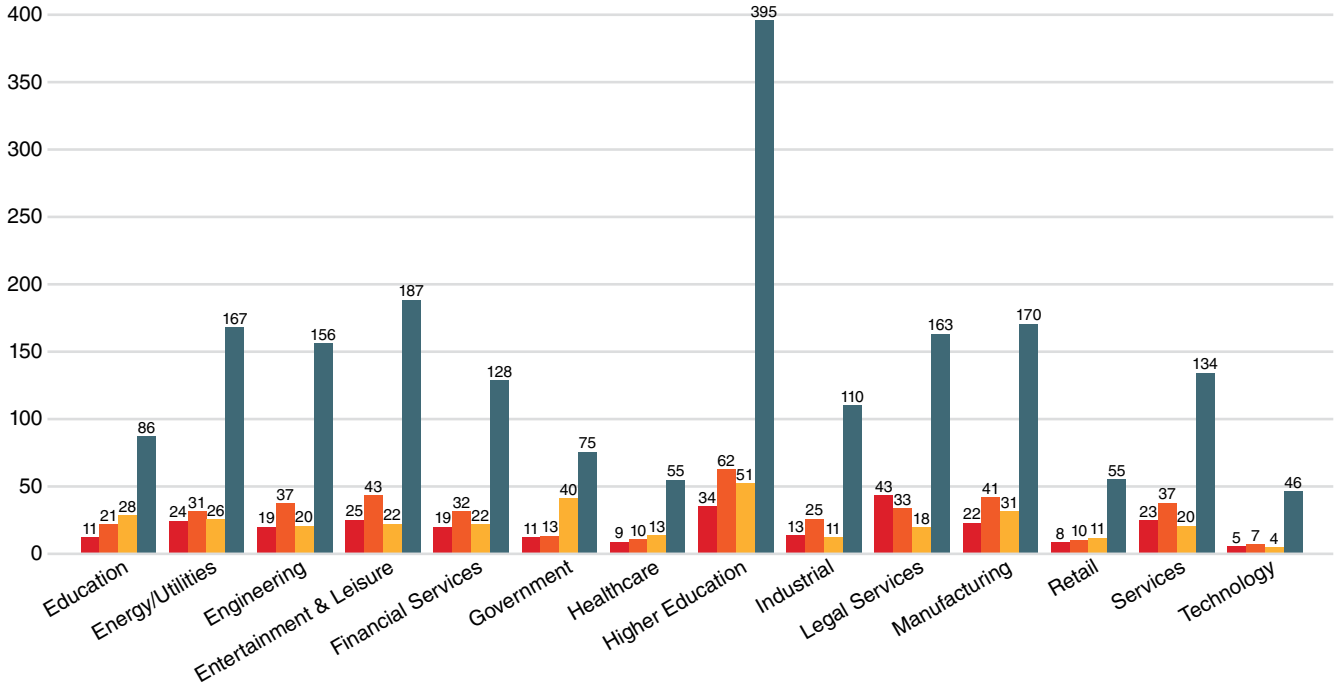


Vectra benchmarked the volume of host devices and workloads prioritized for each severity in relation to each vertical industry and with the overall average, as shown in the bar graph below.

For example, the number of low alerts in higher education is over three-times the normal rate, which is indicative of attacker behaviors that are opportunistic.

Inversely, the technology industry has a low volume of devices prioritized as high or critical, which indicates cyberattackers do not often progress deep into the attack lifecycle.

An overview of detections per 10,000 devices and workloads



Overall detection trends

- **Detection rates:** Organizations had an average of 818 devices with threat detections for every 10,000 devices in a one-month period. This represents a 32X 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 faster, before damage is done.
- **Bitcoin is a growing problem:** While considered opportunistic, bitcoin mining is experiencing a surge in activity that is likely related to the spike in price of bitcoin. These behaviors are seen predominantly in higher education, where student systems are open to exposure or students are performing the mining.

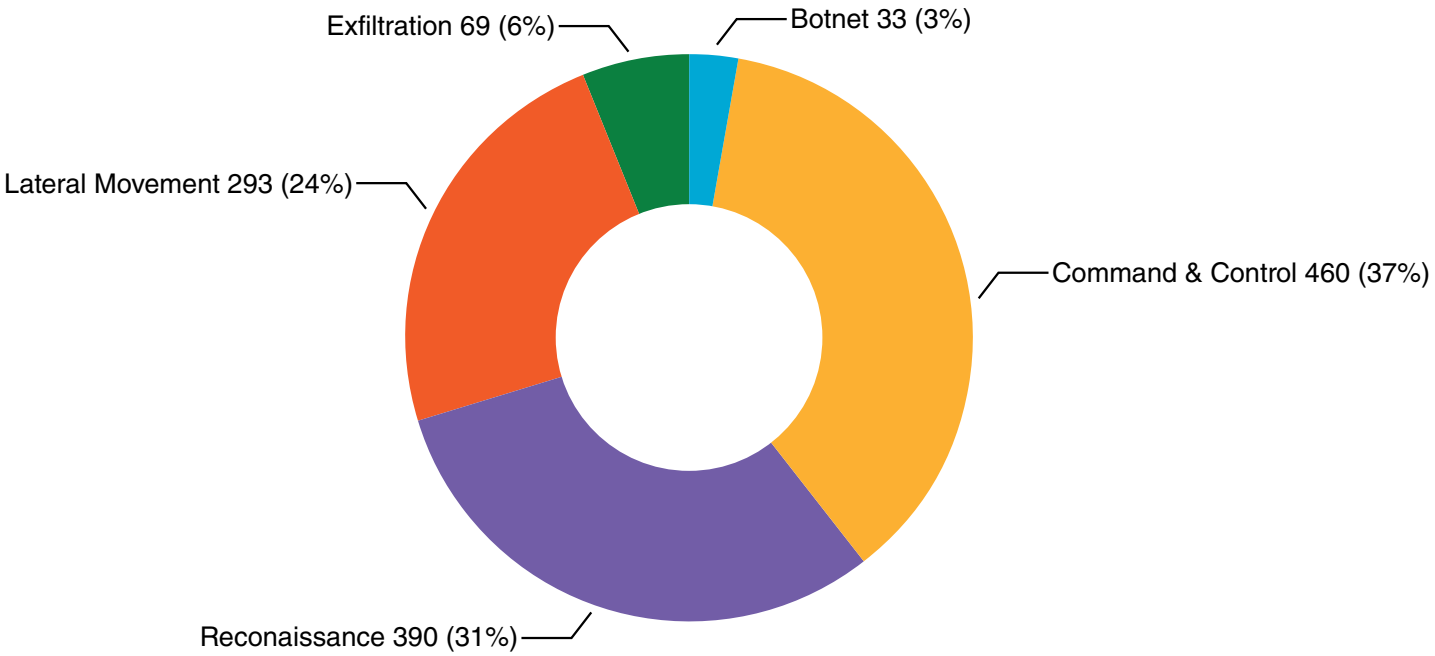
Threats by type per 10,000 devices

To dig deeper, Vectra provides a breakdown of detection statistics by industry. The pie-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, they are interrelated and we often see an attack progress through the stages with the ultimate outcome of financial gain, data exfiltration or data destruction.

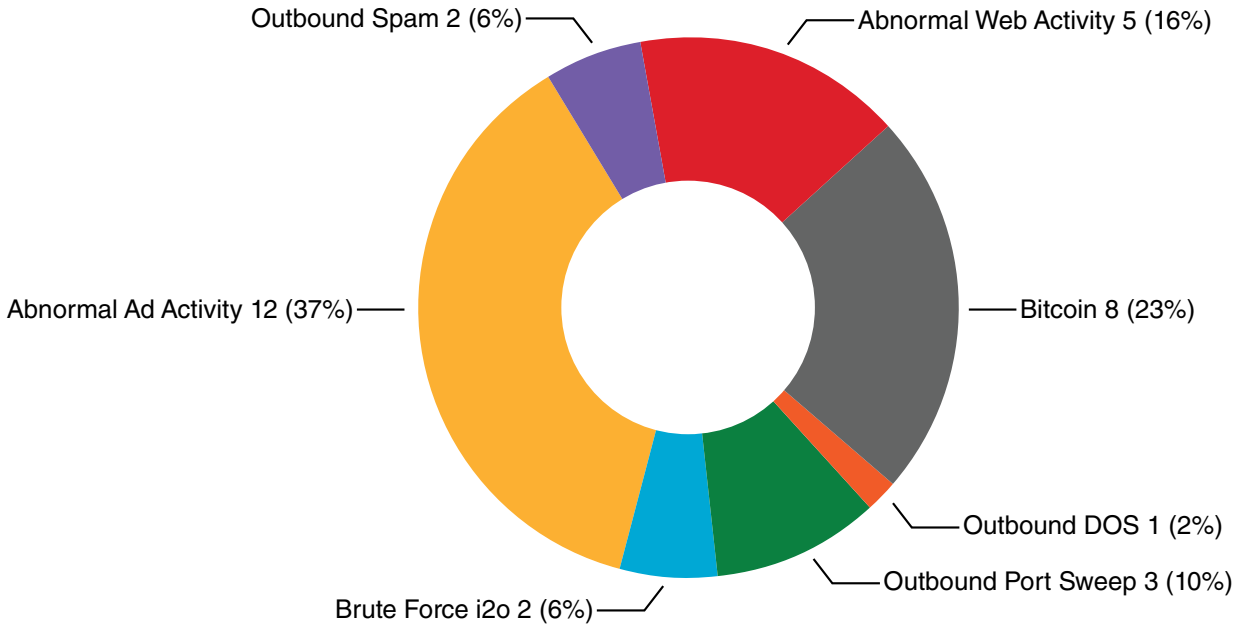
This data represents in-progress attacker behaviors. Activity like C&C and reconnaissance occur in the earlier stages of an attack, enabling organizations to quickly mitigate the threat before it can spread. These are the most common detected behaviors.

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

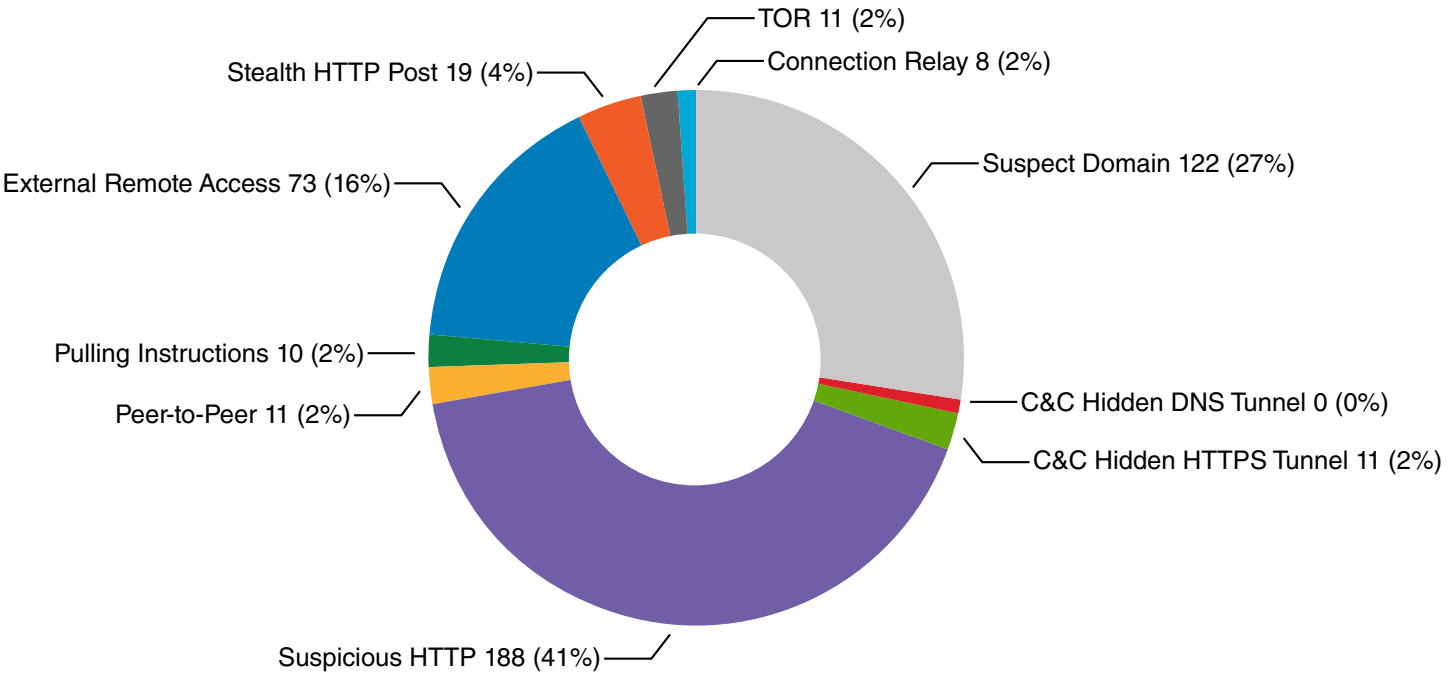
Botnets are opportunistic attack behaviors where a device makes money for its bot herder. The ways in which an infected device can be used to produce value can range from mining bitcoins to sending spam emails to producing fake ad clicks. To turn a profit, the bot herder utilizes devices, their network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



Command and control

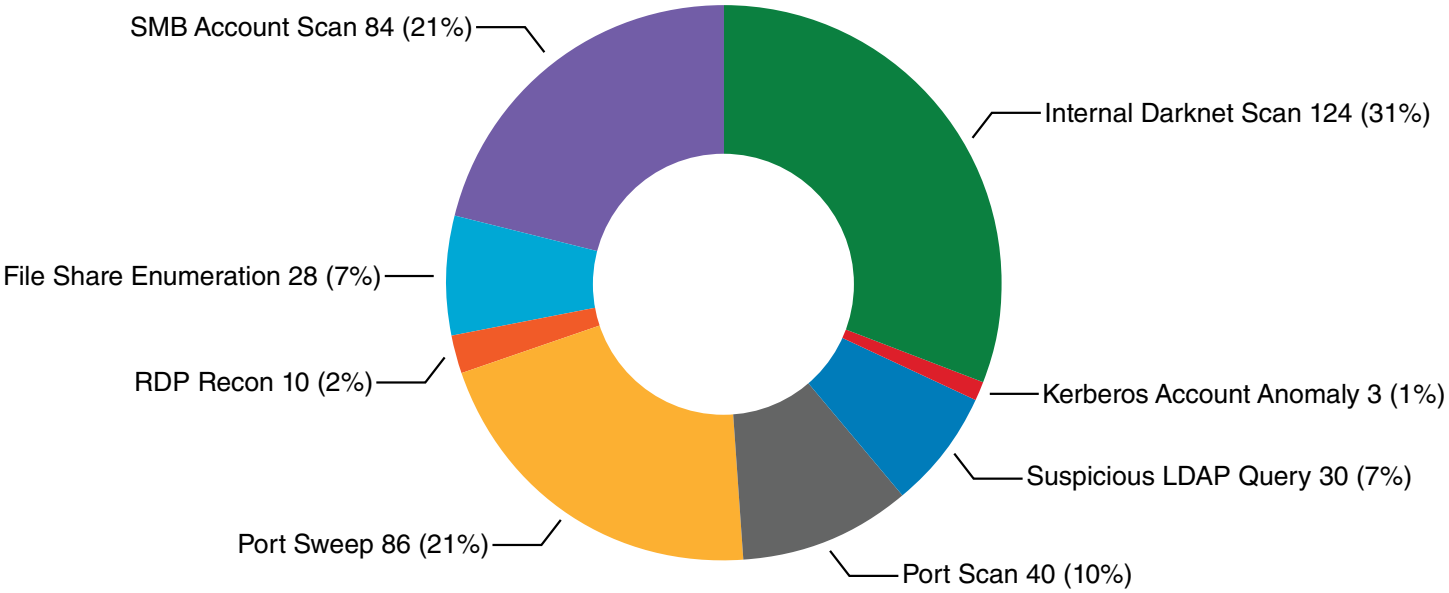
C&C traffic occurs when a device appears to be under control of an external malicious entity. Most often, the control is automated because the device is part of a botnet or has adware or spyware installed.

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

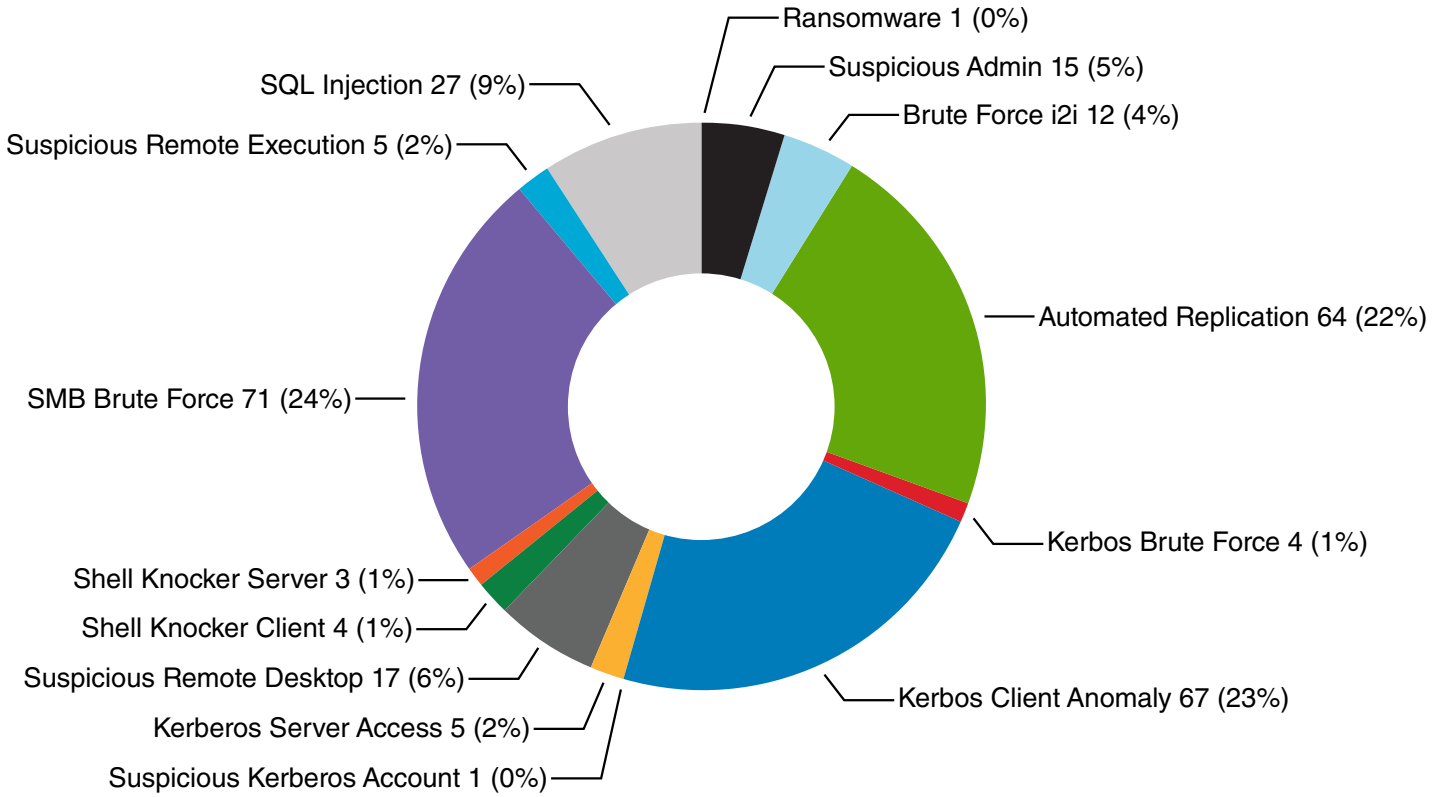
Reconnaissance attacker behaviors occur when a device is used to map-out the enterprise infrastructure. This activity is often part of a targeted attack, although it might indicate that botnets are attempting to spread internally to other devices. Detection types cover fast scans and slow scans of systems,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



Lateral movement

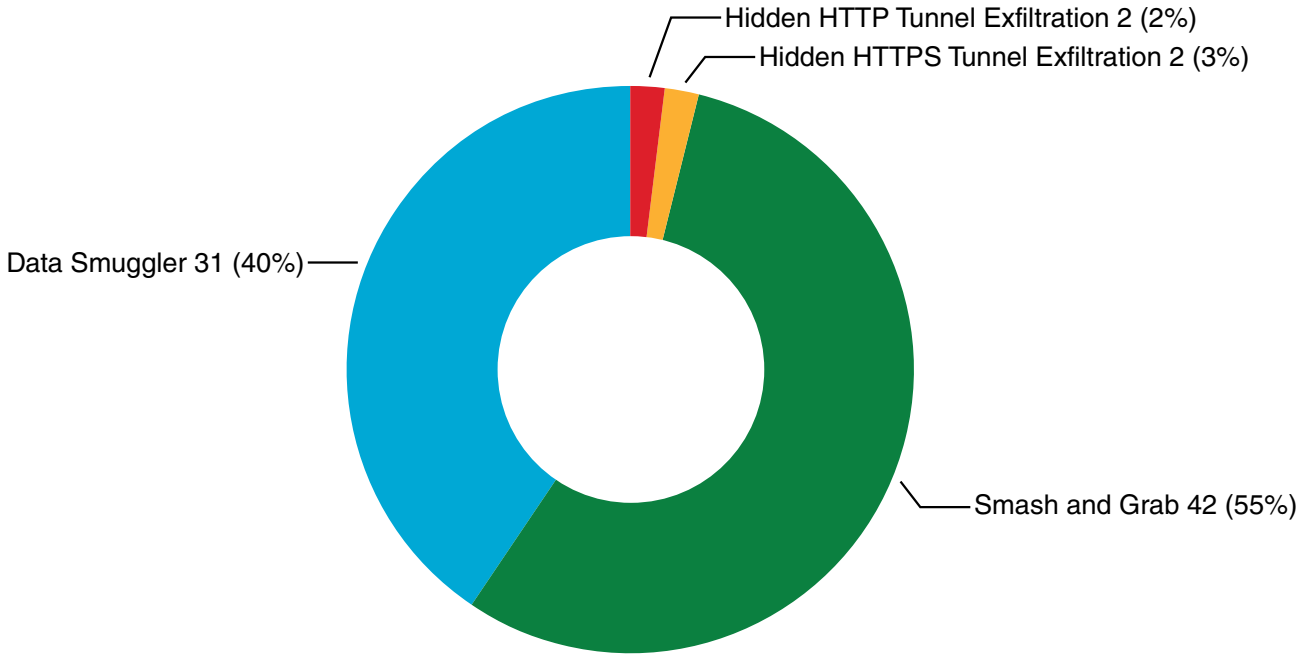
Lateral movement covers scenarios of lateral action meant to further a targeted attack. This can involve attempts to steal account credentials or to steal data from another device.

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

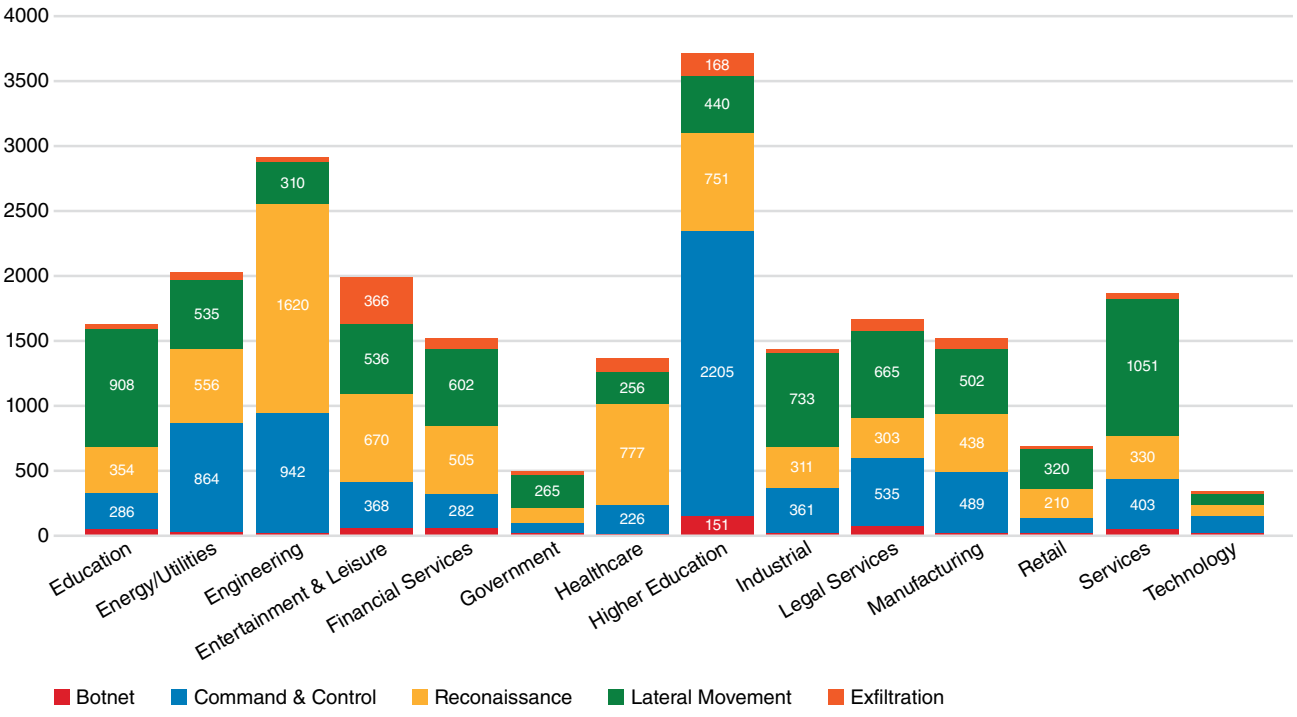
Data exfiltration behaviors occur when data is sent to the outside in a way that is meant to hide the transfer. Normally, legitimate data transfers do not involve the use of techniques meant to hide the transfer. The device transmitting the data, where it is transmitting the data, the amount of data, and the technique used to send it are indicators of exfiltration.



Threats by industry per 10,000 devices

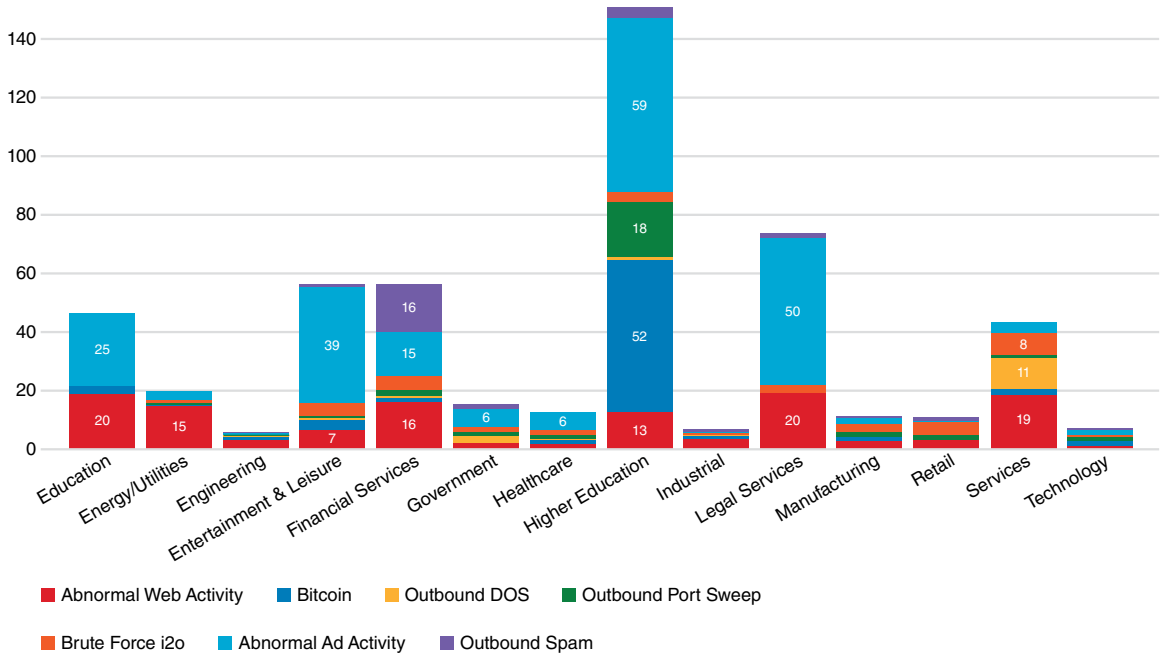
The bar-chart below shows the volume of threat detections that were triggered in each industry. This view shows how each industry fared per capita as well as which industries generated the most detections by volume.

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



Botnets by industry

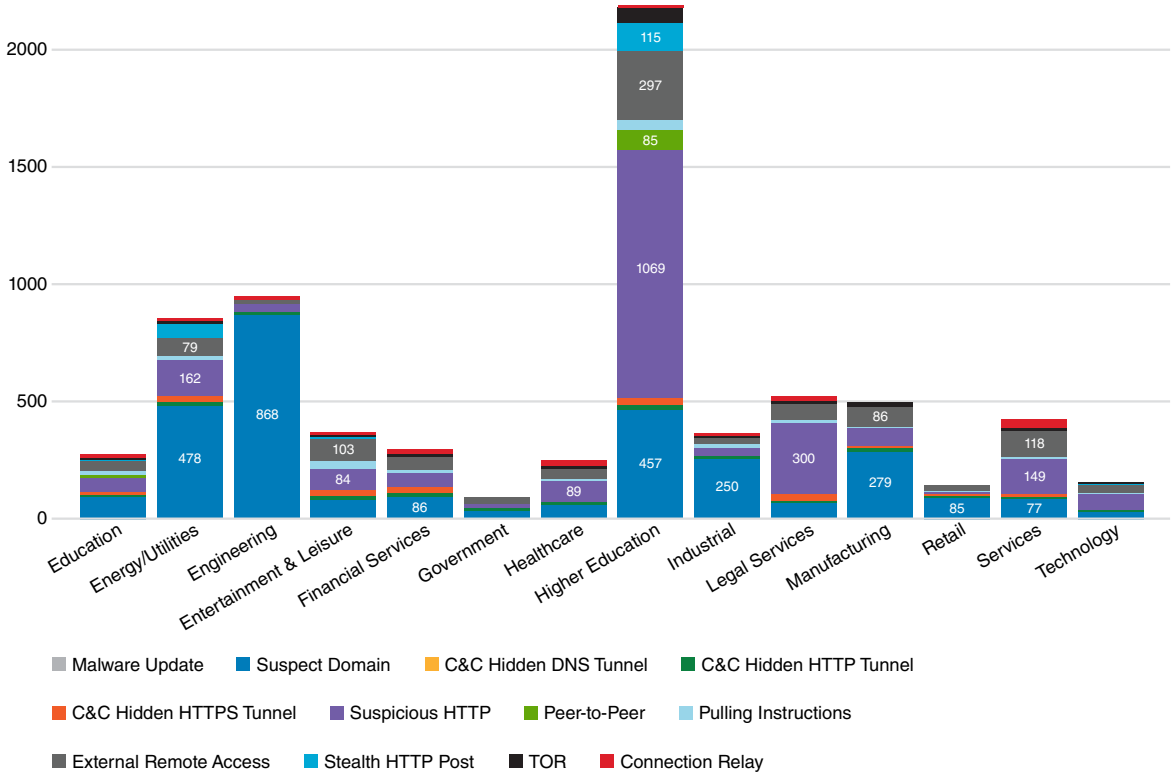
Cognito from Vectra observed a startling trend in bitcoin mining and abnormal web activity in higher education. Bitcoin mining has experienced a surge in popularity with cybercriminals, particularly among large student populations. This is likely due to a lack of security controls, which makes them lucrative targets for botnet herders.



C&C by industry

Due to the association between botnet and C&C traffic, Cognito from Vectra found that higher education has the largest volume of C&C behaviors, primarily related to suspicious HTTP.

Student systems often lack security controls that would normally detect and stop C&C behavior. Consequently, C&C attacks are much easier to execute in student environments.

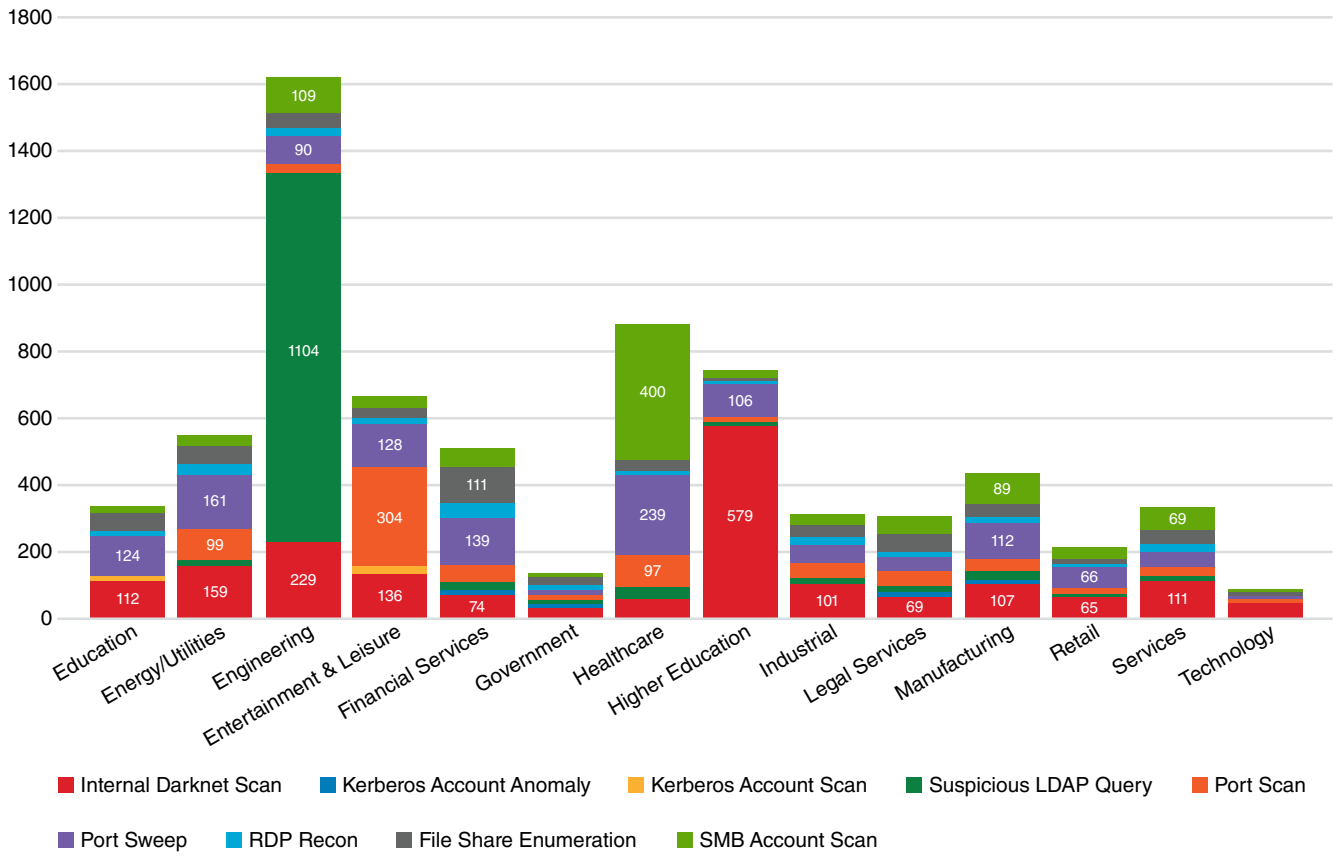


Reconnaissance by industry

Across the board, Cognito 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.

Cognito also detected large volumes of suspicious LDAP queries across the engineering 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.

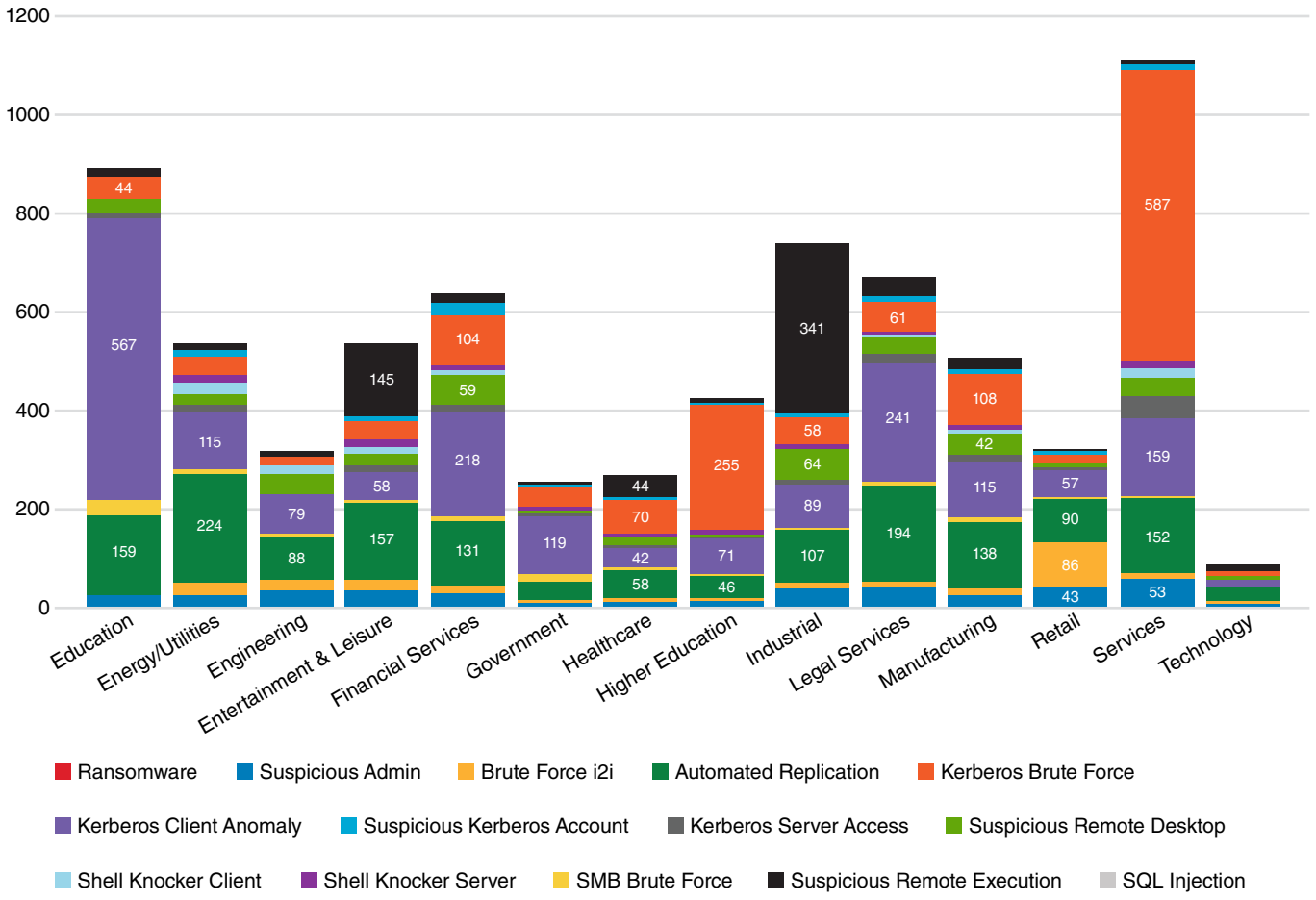
Attackers prefer to use this form of reconnaissance because the risk of detection is relatively low and less noticeable than a port sweep or a port scan.



Lateral movement by industry

In education, Cognito observed a large spike in Kerberos client anomalous behaviors. This indicates a Kerberos account is being used differently than its learned baseline in one or more ways – connecting to unusual domain controllers, using unusual devices or accessing unusual services or generating unusual volumes of Kerberos requests using normal domain controllers, usual devices and usual services.

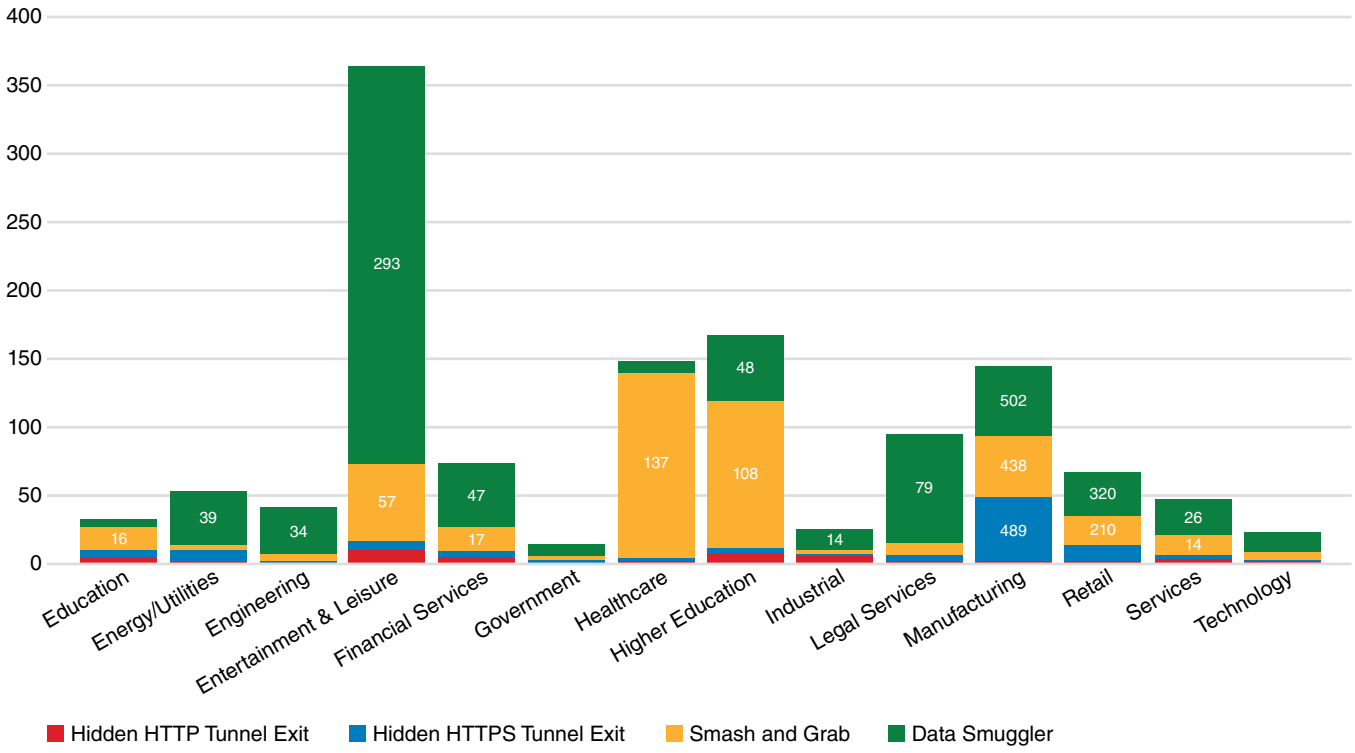
In the services industry, Cognito detected a large volume of SMB brute-force behaviors, which indicates that a device is making multiple login attempts, using the same accounts, to access a file server.



Exfiltration by industry

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

The second most-common exfiltration behavior is data smuggling, which was observed primarily in the entertainment and leisure industry. It is detected when an internal host acquires a large amount of data from one or more servers and sends significant volumes of data to an external system.



Conclusion

This edition of the Attacker Behavior Industry Report expands the scope of analysis by increasing the number and average size of participating organizations. They consisted of more than 4.6 million devices, more than twice the number of devices in the previous report.

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 are cause for concern.

As sophisticated cyberattackers automate and increase the efficiencies of their own technology, there is an urgent need to automate information security 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 detect and respond to threats faster and stay well ahead of attackers.


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

VECTRA®
Security that thinks®

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