VECTRA®

Attacker Behavior Industry Report

January-March 2017

VECTRA®

TABLE OF CONTENTS

Introduction

The Vectra® Networks Attacker Behavior Industry Report provides a first-hand analysis of active and persistent attacker behaviors inside the enterprise networks of Vectra customers. This study takes a multidisciplinary approach that spans all strategic phases of the attack lifecycle. By examining attacker behaviors, Vectra uncovered where potential exposure and risk exists within an organization and identified strong indicators of potentially damaging

Key findings

- The highest volume of attacker behaviors was in healthcare (164 detections per 1,000 hosts) followed by education (145 detections per 1,000 hosts). This points to a level of openness and exposure in these verticals.
- Entertainment and healthcare had the widest range of attacker behaviors with a high level of detections across the entire attack lifecycle. Botnet, command-and-control (C&C), reconnaissance, lateral movement, and exfiltration showed the highest levels of activity. This indicates that targeted attacks might easily progress through the attack lifecycle.
- C&C activity is nearly three-times as likely in education and healthcare. These are early indicators of an attack because they usually precede other stages of the attack lifecycle.
- The financial and technology industries have below-average detection rates, with 37 and 38 detections per 1,000 hosts, respectively. This indicates the presence of stronger policies, mature response capabilities, and better control of the attack surface.
- Botnet activity occurs most often in entertainment and was detected six-times more than the average for all industries, followed by media. These opportunistic attack behaviors leverage hosts for external gain, such as bitcoin mining or outbound spam.
- The food and beverage industry showed the lowest volume of attacker behaviors, with 17 detections per 1,000 hosts. It is the only industry where detection rates in all five categories of the attack lifecycle are below the median count.
- Vectra customers achieved a 29x workload reduction for Tier-1 analysts in detection, triage, correlation and prioritization of security incidents, enabling them to focus on compromised hosts that pose the highest risk.
- When normalizing detections to per 1,000 hosts compared to the previous year, there is a sharp increase in every industry for C&C, reconnaissance, lateral movement, and data exfiltration.

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 active breaches by directly monitoring network traffic on the wire in these environments. North-south traffic to and from the internet and internal east-west traffic between network hosts are also analyzed.

This analysis provides important visibility into advanced phases of attacks. 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 industry and highlights relevant differences between industries.

Over 90 days, Vectra monitored 2,145,708 hosts. On these hosts, Vectra detected 1,805,188 different network behaviors that were condensed to 140,341 detections. These detections were then triaged down to 62,119 hosts. Across all participating organizations, 3,720 hosts were tagged as critical and 6,987 were tagged as high, enabling security analysts to quickly respond to and mitigate the highest-risk 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 as well as their impact on the operational fitness of the organization.

Changes since the previous Attacker Behavior Industry Report

Detections per 1,000 hosts	Botnet	Command and control	Recon	Lateral	Exfiltration
2016	3	20	3	3	1
2017	3	34	13	11	4
% increase	0%	70%	333%	266%	300%

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 to find them.

Vectra performs nonstop automated threat hunting using artificial intelligence to detect attacker behaviors. These behaviors are correlated with 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 hosts 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. Vectra provides security analysts with the most important information, which can be used to make a decision 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 hosts to the largest networks with more than 300,000.

To account for this variance, the data has been normalized to a network with 1,000 hosts, making it easier to compare the prevalence of threats in a network on a per capita basis. A host is any device with an IP address including IoT devices, smartphones, tablets, laptops, servers and workloads.

Overall, Vectra reduced the investigation workload of security analysts by 29x, compared to manually investigating all attacker behaviors and compromised host devices.

Host scoring

Vectra monitors individual host devices on the network for extended periods of time and attributes detections to any host that behaves suspiciously. The detection scores and when they occurred are key inputs for the host scores.

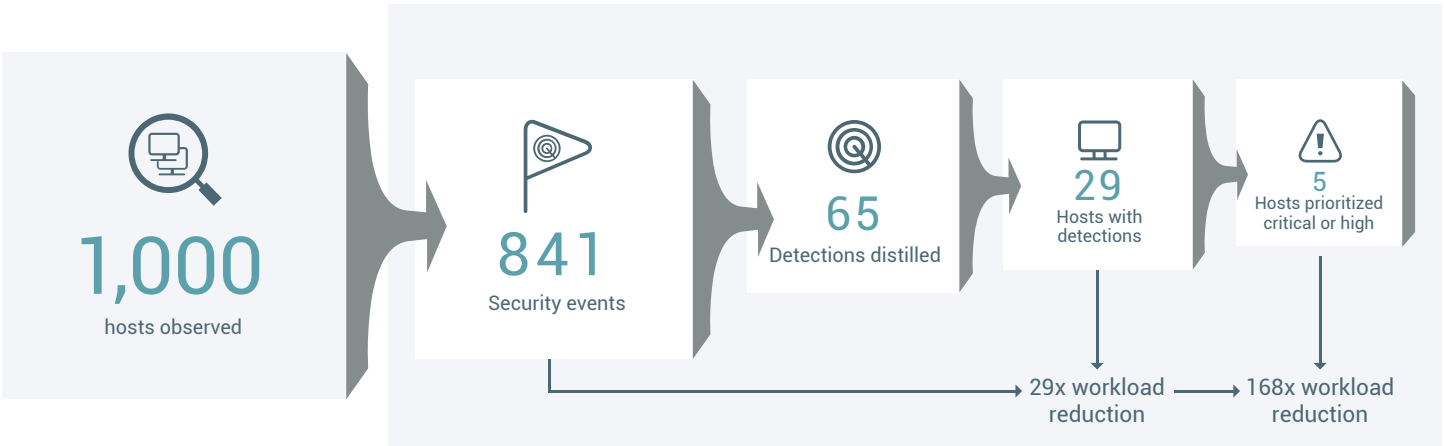
Since detections are dynamic, changes in their scores cause changes to attributed host scores. Critical and high scores help security analysts prioritize their investigation efforts because they represent behaviors with the highest certainty and greatest potential to cause significant damage.

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

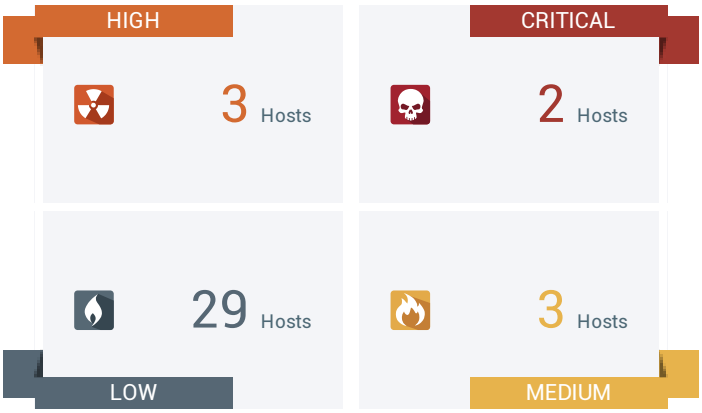
Every detection type has a maximum lifespan, ranging from a few days to a month. When a detection has no recurring activity, its effect on a host score will slowly decline to zero. A detection past its maximum lifespan becomes inactive and has no impact on the host score.

For this report, *Host Severity* statistics are based on the peak number of host scores. Detections before a 90-day period can cause hosts to have a score within the 90-day period. These detections were not included in *Host Detection* statistics.

Reduction in workload for Tier-1 security analysts



An overview of host severity detections per 1,000 host devices



The numbers above reflect detections per 1,000 hosts. This means for every 1,000 hosts, two were critical and three were high. These are the areas that require a security analyst's immediate attention.

In this instance, Vectra reduced the workload from 841 security events to the five hosts that required immediate attention. This time savings increases a security analyst's incident response efficiency and ensures what matters most is not lost in the noise.

Overall detection trends

- **Detection rates:** Organizations had an average of 29 hosts with threat detections for every 1,000 hosts. This represents a 29x reduction in the number of events requiring investigation and triage.
- **Command-and-control represented the bulk of detections:** C&C traffic is a key component of a botnet attack and is an enabler for later phases of a targeted attack.
- **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.
- **Ransomware is a growing problem:** Ransomware detections are categorized as lateral movement. By observing the category trends, there is an alarming indication that ransomware does not always have C&C-associated traffic.

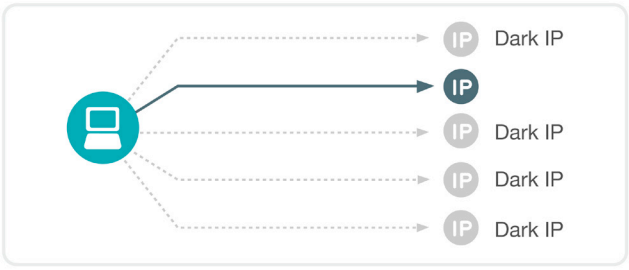
Real-world scenarios

Ransomware: Rapid response saves critical files

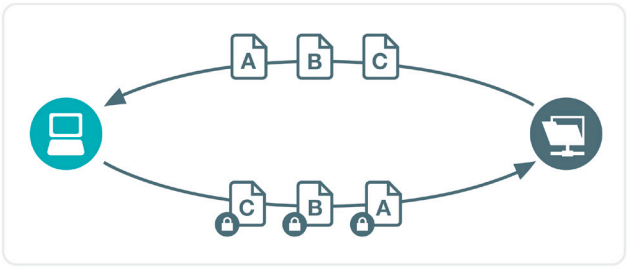
Organizations need to stay ahead of ransomware attacks as they become more prevalent. Ransomware has successfully extorted millions of dollars from people and organizations after infecting and encrypting their systems.

Vectra saw a large increase in ransomware attacks, due in part to the ease of mounting an attack as well as the widespread use of bitcoin as a means of anonymous money transactions. Vectra ransomware detections have been successful and customers stopped multiple attacks before critical assets were encrypted and held hostage.

- Organization: Multiple organizations, including education, government and technology. Ransomware had a large uptick in activity this year in every industry.
  - Detected early phases of reconnaissance and file-share encryption by several ransomware variants.



Darknet scan (looking for shares)



Ransomware file activity (encrypting)

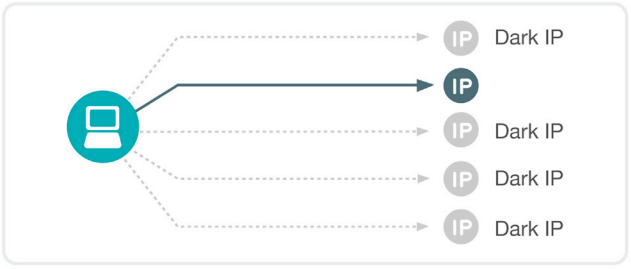
  - Analysis: The most often seen method is through phishing email attacks, followed by internal scanning for file-shares, and then immediate encryption. Many attacks occur within an hour from the time of infection to the time to encryption.
  - Outcome: Early, high-priority alerting allowed affected hosts to be isolated before substantial damage was done (only a single share was impacted in all cases).

Ransomware: WannaCry introduces fast propagation

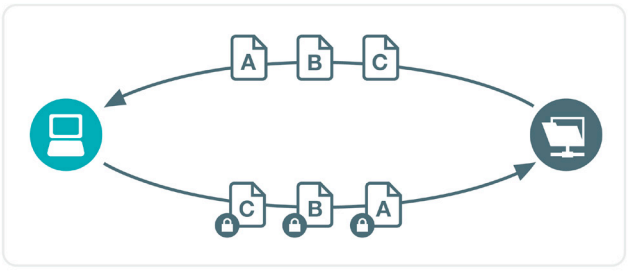
It is important to remember that before ransomware can encrypt files, it needs to locate file-shares on the network. This requires performing internal reconnaissance. Vectra detects reconnaissance behaviors and triages all the behaviors associated with infected hosts.

Hosts infected with ransomware are at high risk and these behaviors receive the highest threat and certainty scores to prioritize those hosts for immediate incident response.

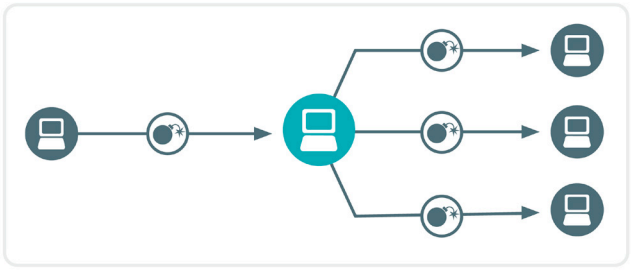
- Organization: Undisclosed
  - Detected C&C communication over the TOR network.
  - Sweeping the internal network and the internet on Port 445 for computers with the vulnerability MS17-010.
  - Automated replication of malware once a machine with vulnerability MS17-010 has been found.
  - Encryption of files on local and mapped network file shares.



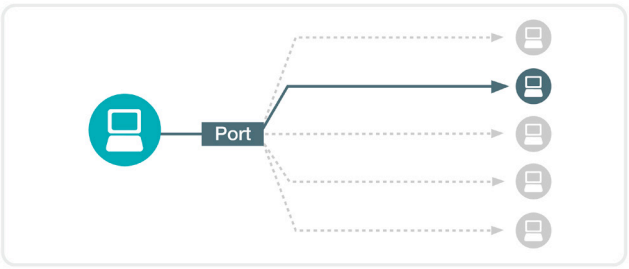
Darknet scan (looking for shares)



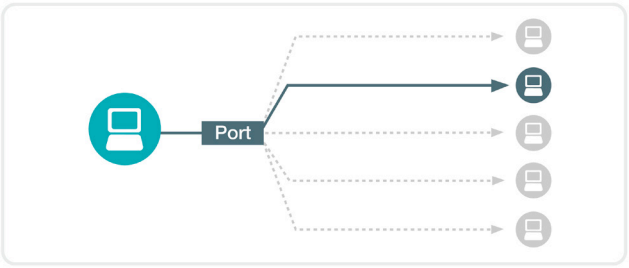
Ransomware file activity (encrypting)



Automated replication (MS17-010)



Outbound port sweep (Port 445)



Port sweep (Port 445)

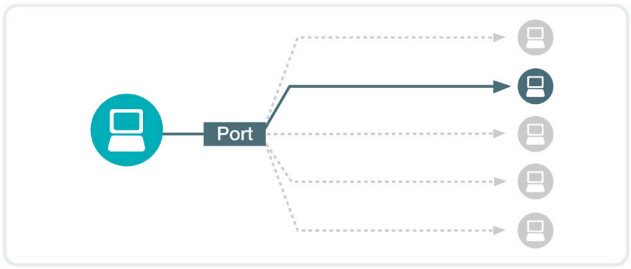
- Analysis: WannaCry introduced a new dynamic in the propagation of ransomware by combining behaviors seen with worms along with behaviors seen with ransomware. Fortunately, Vectra already monitors and detects these behaviors.
- Outcome: Early, high-priority alerting allowed affected hosts to be isolated before damage was done.

When lightweight devices are a threat: IoT botnets

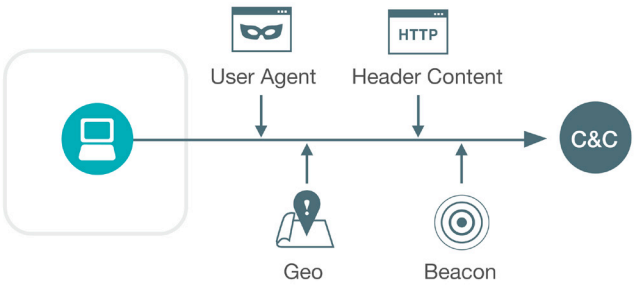
IoT devices are being connected to networks in record numbers and represent a ripe new attack surface. Endpoint security can't run on lightweight IoT operating systems and IoT devices are rarely patched and updated.

This means that vulnerabilities can be left unaddressed for months or years. Likewise, these devices are unlikely to be protected by signatures and will almost assuredly be unable to run client-based security.

• Organization: Financial
  - C&C and reconnaissance were detected on multiple IP video cameras running default administrative access on Linux operating systems. This is how devices are shipped from the manufacturer and is a widespread problem in every organization.



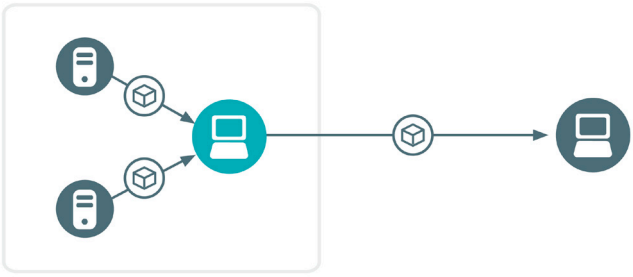
Port sweep (Telnet/23)



HTTP C&C

  - Analysis: Mirai botnet.
  - Outcome: Threats remediated and preventive actions taken across the network environment.

• Organization: Entertainment
  - Exfiltration to China detected on cash-counting machines. Infection occurred at the manufacturer and not in the organization. Vendors often ship unsecure internet-enabled technology.



Data smuggler

  - Analysis: Poorly configured OS resulted in exploit.
  - Outcome: Cash-counting machines remediated and patched.

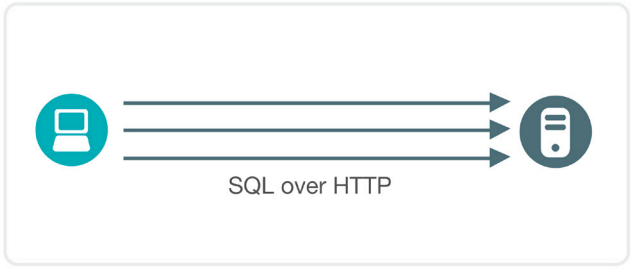
Unsecure web apps: SQLi and data exfiltration

Probing and exploiting internal web application vulnerabilities can be a prelude to a targeted attack that obtains access to data and then exfiltrates it.

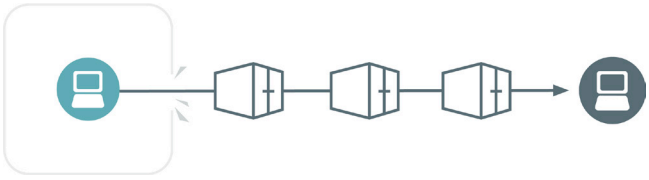
Application software that passes SQL statements in HTTP post data or as part of a URL may be vulnerable to attackers because they can send very different input than the application expects to receive.

If it is an attack, SQL injection is often followed by large volumes of data rapidly being exfiltrated from the network.

• Organization: Financial
  - SQLi followed by a 3.6-GB exfiltration via an internet-facing web application. Database weaknesses are common in organizations and this is one of the most common type of attacks for stealing information.



SQLi observed by monitoring lateral traffic between app and database tiers



3.6 GB smash and grab

  - Analysis: SQL database was unsecured and left the organization exposed. No other tool was detected in the compromise.
  - Outcome: The web application was remediated before additional damage was done.

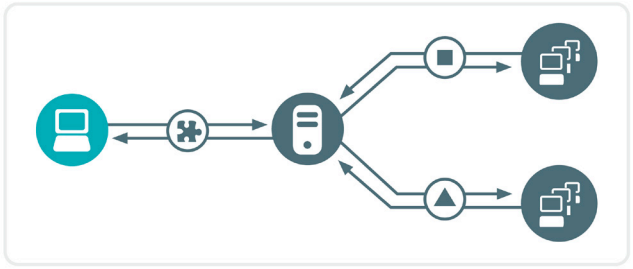
Unapproved ATM maintenance

Port hijacking is a technique attackers use to enable communication to a compromised server without raising alarms that may go off when a new port is used on an existing server.

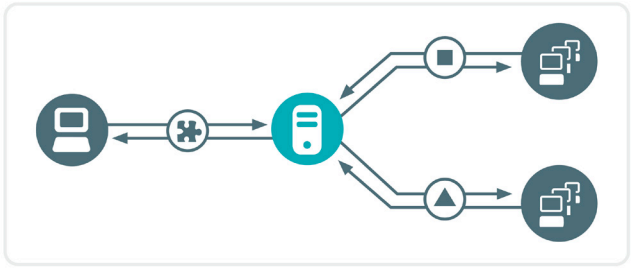
Compromised servers are often more valuable to attackers than compromised laptops because they always remain on the network, are often located in the data center, and have direct access to critical information and resources.

Even unapproved behavior on a critical resource, such as server access outside of controlled time-windows, can be damaging to an organization.

- Organization: Financial
  - Shellknocker triggered on multiple ATMs. These are not public networks but are always a cause for concern.



Shellknocker client



Shellknocker server

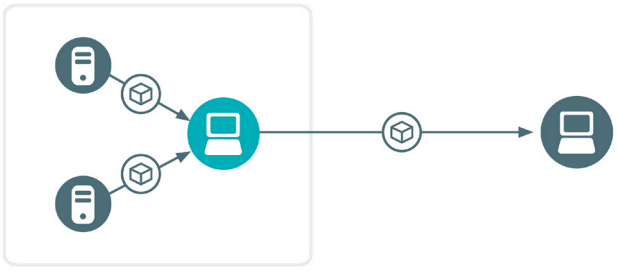
  - Analysis: Unapproved maintenance had been performed on ATMs, which created serious compliance and security risks.
  - Outcome: Better communication and enforcement of security policy.

Unintentional insider threat: Leaking high-value IP

Data exfiltration is often accidental but it carries the same risk as a targeted attack by an external actor. The chances of accidental loss are high in a connected world with internet-based file-sharing and storage services.

It is important to monitor all data transfers from critical hosts, such as PCI in-scope assets and hosts with PII of PHI. The internal servers from which the data was retrieved indicates that the data was acquired. The business risk is high if the servers contain valuable information and the external service to which the data was uploaded is not sanctioned by IT.

- Organization: Education
  - A multi-gigabyte exfiltration was triggered on an end-user client. While data should be stored on servers, it is normal for data transfers to occur at the endpoint. The size of the transfer over a short duration was significant.



Data smuggler

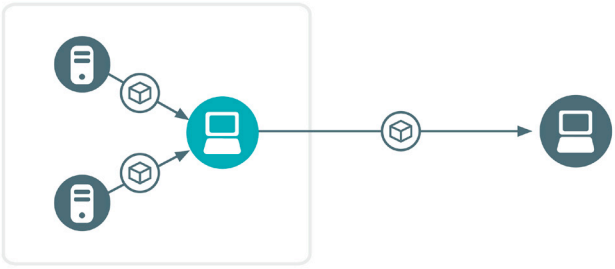
  - Analysis: In violation of policy, a genome database was shared with an external party for testing. This was not detected by other security controls.
  - Outcome: Better communication and enforcement of security policy.

Free anti-virus cloud scan

Sometimes data loss is not obvious. What appears to be legitimate software could be a backdoor to a nefarious company, allowing data to leave in what appears to be appropriate means.

In many cases, legitimate vendor activity is indistinguishable from attacker behaviors. While it is important to understand the actions of attackers as well as suppliers, behaviors are not always what they appear on the surface. Data that leaves the network without approval is bad, regardless of how it happens.

- Organization: Education
  - Multiple exfiltration events were triggered to the same destination from a handful of systems. This was caused by free anti-virus software from China that appeared legitimate but was creating exposure that bypassed security controls.



Data smuggler

  - Analysis: Free anti-virus software from China was uploading all new files to the cloud for analysis.
  - Outcome: Due to the open nature of education environments, security has no ability to ban software. However, this incident led to stricter controls around data access for systems running the tools.

Threats by industry

To dig a bit deeper into threats seen in real networks, Vectra has provided a breakdown of detection statistics by industry.

The table below shows the percentage of threat detections that were triggered in each industry. Each category represents attacker behaviors related to a specific stage of 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.

Behaviors such as lateral movement, which occur later in the cyber-attack lifecycle, warrant high-priority action from incident response teams to prevent irreversible damage from a data exfiltration.

Vectra performed an analysis of the number of detections per 1,000 hosts seen on the network. This view provides an entirely different perspective by showing how each industry fared per capita as well as which industries generated the most detections by volume. Education and healthcare represent the highest percentage of detections across all industries.

The percentage of threat detections per industry

Detections per 1,000 hosts	Total	Botnet	Command and control	Reconnaissance	Lateral movement	Exfiltration
All Industries	100%	6%	44%	19%	24%	6%
Education	14%	5%	77%	7%	4%	8%
Energy	4%	2%	26%	38%	31%	2%
Entertainment	10%	21%	40%	14%	16%	8%
Financial	4%	5%	19%	32%	41%	3%
Government	6%	7%	35%	20%	35%	3%
Healthcare	16%	5%	65%	10%	9%	10%
Media	12%	11%	22%	20%	20%	28%
Services	8%	4%	41%	25%	22%	8%
Technology	4%	3%	42%	21%	24%	11%
Retail	6%	6%	61%	16%	15%	2%
Manufacturing	6%	2%	28%	33%	33%	4%
Legal	8%	7%	48%	12%	23%	10%
Food and beverage	2%	6%	35%	18%	35%	6%

Detections per 1,000 host devices by industry

Detections per 1,000 hosts	Total	Botnet	Command and control	Reconnaissance	Lateral movement	Exfiltration
Median for all industries	62	4	27	12	15	4
Education	145	7	111	10	6	11
Energy	42	1	11	16	13	1
Entertainment	97	20	39	14	16	8
Financial	37	2	7	12	15	1
Government	60	4	21	12	21	2
Healthcare	164	9	107	17	15	16
Media	123	13	27	24	25	34
Services	83	3	34	21	18	7
Technology	38	1	16	8	9	4
Retail	62	4	38	10	9	1
Manufacturing	57	1	16	19	19	2
Legal	83	6	40	10	19	8
Food and beverage	17	1	6	3	6	1

The columns to the right show the percentage of detections for each category and how they compare to the median average for each category. Red highlights indicate a higher-than-median percentage while green indicates a lower-than-median percentage. For example, the median for C&C detections is 44%. Education, healthcare and retail experienced abnormally high counts.

Another interesting trend is the absence of a relation between a high C&C detection with reconnaissance or lateral movement. This implies that these behaviors might not be dependent upon large volumes of outbound communication and have been seen in customer deployments. Targeted attacks often create very little outbound noise to avoid detection by perimeter tools.

The table above shows the results in terms of the number of detections per 1,000 network hosts. The average number across all industries is shown at the top of the table in gray. Red denotes above-average detections per host while green is average or below average.

The data shows that healthcare and education are consistently targeted and attackers can easily evade perimeter defenses. The financial and technology sectors might be equally targeted, but they appear to do a better job of prevention and mitigation. This makes sense considering the enormous spend and focus at financial and technology companies over the years.

Education has significant exposure due to its dynamic student population, which is difficult to control. Students often connect three or more personal devices – including laptops, smartphones and gaming consoles – to campus networks. This is where a lot of the C&C activity occurs.

Healthcare also saw increasing numbers of internet-connected devices, which is likely due to the expanding footprint of IoT devices in hospitals. These unsecured devices are easy targets for cybercriminals.

Education and healthcare both contend with a level of openness in their networks and thus face a greater risk of exposure to cyber attacks.

Entertainment and healthcare experienced the widest range of attacker behaviors across the entire attack lifecycle. The number of botnet, C&C, reconnaissance, lateral movement, and data exfiltration detections were above average in these industries.

This points out the relative ease in which targeted threats can progress through the cyber-attack lifecycle. Most often, this occurs when the attack surface is large and easy for an attacker to navigate and incident response programs are not as mature as they should be.

C&C is the early indicator of an attack and usually happens in the early stages of the attack lifecycle. When a strong incident response program is in place, attacks can be stopped faster and earlier in the lifecycle, as seen in the financial and technology industries.

Botnet activity occurs most often in the entertainment industry, with detections representing more than six-times the average for all industries, followed by media. Botnets are opportunistic and leverage host device processing power for external gain, such as bitcoin mining and outbound spam. It is often unrelated to a targeted attack and therefore does not frequently follow the same progression.

Conclusion

In this edition of the Attacker Behavior Industry Report, Vectra significantly expanded the scope of analysis by tripling the number of participating organizations. They consisted of more than 2 million hosts.

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 cyber attackers automate and increase the efficiencies of their own technology, there is a very real need to automate information security detection and response tools to stop threats faster.

At the same time, there is a global shortage of highly-skilled cybersecurity professionals to handle detection and response at any reasonable speed. Consequently, the use of artificial intelligence is absolutely essential to augment existing cybersecurity teams so they can detect and respond to threats faster and stay well ahead of attackers.

VECTRA®
Security that thinks®

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

© 2017 Vectra Networks, Inc. All rights reserved. Vectra, the Vectra Networks logo and Security that thinks are registered trademarks and the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra Networks. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.