VECTRA®

Post-Intrusion Report

Spring 2016

VECTRA

TABLE OF CONTENTS

Introduction

In early 2016, cybersecurity continues to be a central concern among virtually all industries, businesses and organizations. Despite record investments in prevention security controls, attackers of every stripe have shown that they remain quite adept at breaking into protected networks to steal and damage critical assets.

Finding and stopping these attacks is now a priority at all levels, from boardrooms to the command line. This third edition of the Vectra® Networks Post-Intrusion Report takes an analytical look into what is going on inside actual customer networks and how attack techniques and strategies are evolving.

Executive summary

All organizations showed signs of an active intrusion – As in previous reports, all organizations detected in-progress targeted attack behaviors, including internal reconnaissance, lateral movement and data exfiltration.

Security teams are catching attackers in the act – While the symptoms of targeted attacks remain common, exfiltration rates remain low. This indicates that most organizations can detect and stop attacks before damage is done.

Attackers are getting quieter inside the network – Since the last report, brute-force attacks dropped from first to the third most-common lateral movement technique, behind more subtle Kerberos and internal replication techniques.

Hidden tunnels are on the rise – While rare, hidden tunnels in HTTP and HTTPS continue to rise as command-and-control and exfiltration channels. Hidden tunnels are the third most-common command-and-control technique and the second most-common exfiltration technique.

Tighter controls led to fewer exfiltrations – Networks with the lowest detection rates early in the attack lifecycle had the lowest exfiltration rates. Organizations with low command-and-control rates had correspondingly low exfiltration rates.

Background and methodology

This report is based on a significant increase in sample sizes compared to the previous report, which analyzed data from 40 customer organizations. In this report, the sample size tripled to 120 organizations comprised of more than 1.3 million hosts.

The report is based on anonymized metadata analyzed from actual production deployments of Vectra customers and prospects that have opted into the metadata-sharing program. The data in this report was collected throughout the first calendar quarter of 2016.

Organizations from a variety of industries contributed to the report, including:

- Education
- Energy
- Financial services
- Gaming and hospitality
- Government
- Healthcare
- Manufacturing
- Media
- Professional services
- Retail
- Technology
- Telecommunications

Where appropriate, this report presents the results by industry and highlights relevant differences between industries.

There was a wide variance in the size of the networks analyzed, with the smallest consisting of a few hundred hosts to the largest network with more than 300,000.

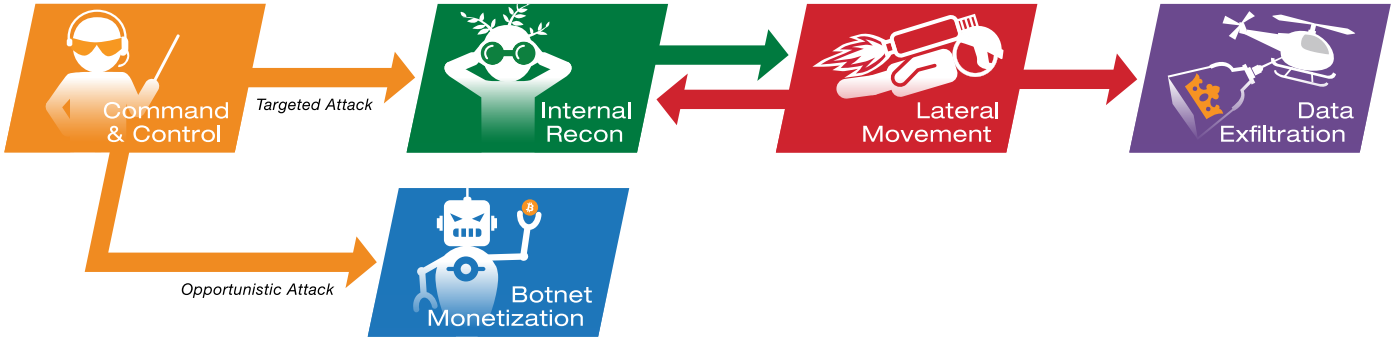
To account for this variance, raw detection counts and threats detected per 1,000 network hosts are reported. This provides a way to compare the prevalence of threats in a network on a per capita basis.

The behaviors and threats detailed in this report are based on the direct analysis of network traffic. Vectra is deployed inside the network to analyze north-south traffic to and from the Internet as well as east-west internal traffic between network hosts.

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.

Data from inside the kill chain

By analyzing all internal and Internet-bound traffic, Vectra detects threats and malicious techniques during all phases of an attack. Detections are grouped into five key phases based on their strategic role in an attack. Each one also represents an opportunity to detect and disrupt an intrusion.



The five phases of an active cyber attack.

Command-and-control

Command-and-control (C&C) includes a wide range of techniques that allow cybercriminals to administer and coordinate an attack over time. C&C communications flow bidirectionally between the inside of the network and the Internet.

C&C communications can be automated between malware and a C&C server to control common crimeware and botnet-based threats or driven by a human using a remote access tool (RAT) to carry out a targeted attack.

Botnet monetization

This category distinguishes large-scale botnet behaviors from targeted attack behaviors. Botnet monetization behaviors are commonly associated with click fraud, sending spam or generating DDoS traffic at a target.

These behaviors can consume valuable resources and damage the external reputation of the network. However, they are typically not focused on targeting an organization's more critical assets.

Internal reconnaissance

Internal reconnaissance is a vital part of a targeted attack and typically begins shortly after an initial infection. Reconnaissance lets cybercriminals orient an attack inside a network and identify targets for lateral movement.

Lateral movement

Lateral movement involves the many ways attackers can spread inside target networks. It's a strategic, fundamental phase of a targeted attack that allows cybercriminals to establish multiple points of persistence in a network while moving deeper toward key assets.

Data exfiltration

Data exfiltration techniques move compromised data from inside a network to a remote external attacker. Representing an in-to-out flow of data, exfiltration can include multiple hops or staging phases inside the network as an attacker attempts to evade security controls.

Overall detection trends

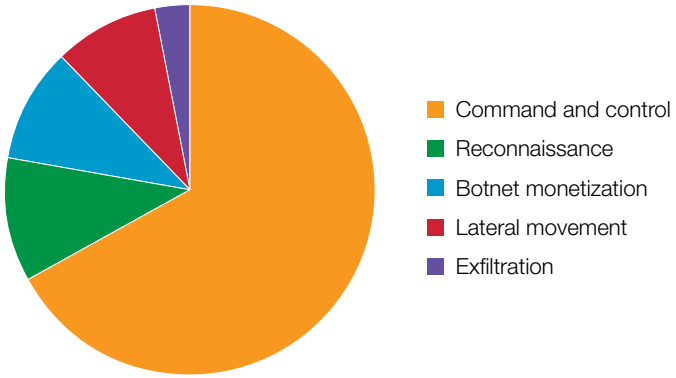
Detection rates hold steady – Detections remained steady when adjusted for time and the total number of network hosts. Organizations generated an average of 30.2 detections per month for every 1,000 hosts. This is down slightly from 31.2 detections per 1,000 hosts per month noted in the previous report.

C&C is the high-volume offender – True to form, C&C claimed the top spot in overall detection counts, with 67% of all detections. These results come as no surprise because C&C traffic is a key requirement for botnet attacks and is an enabler for later phases of an attack.

All organizations detected targeted attacks – All organizations had one or more detections of internal reconnaissance, lateral movement or data exfiltration. Of the 120 participating organizations, 117, or 97.5%, detected at least one of these behaviors during each month of the study.

Security teams are catching attackers in the act – While the symptoms of targeted attacks remain common, there are encouraging signs that security teams are finding and stopping attacks before significant damage is done

Overall, fewer detections were observed deeper in the kill chain. Internal reconnaissance was the most common targeted behavior at 11% of all detections, followed by lateral movement at 9%, and data exfiltration at 3%.



Detection category	Detection count	Percentage
Botnet monetization	13,011	10.5%
Command and control	83,578	67.2%
Exfiltration	3,865	3.1%
Lateral movement	10,691	8.6%
Reconnaissance	14,201	11.4%

Overall detections by category.

Command-and-control detection highlights

The C&C category was busy, accounting for 67% of all detections. These detections tend to be generated at a higher volume because attackers continually move their C&C infrastructure to stay ahead of blacklists and reputation feeds.

As a result, the Vectra detections dedicated to exposing this cat-and-mouse behavior were triggered the most. This includes HTTP C&C, fake browser, and the use of domain generation algorithms (DGA).

Spotlight on HTTP C&C

The HTTP C&C detection was the most common C&C detection and the most common single detection overall. It uses supervised machine learning to recognize the unique pattern and behavior of C&C traffic, even if the URL or domain it communicates with is not on a block list.

This detection model incorporates user agent anomalies, beaconing analysis and geolocation data for vital context. Even with high-volume detections, the HTTP C&C model is 98% accurate and detected C&C infrastructure across Kelihos, Dridex and a variety of other malware families as well as Android-based malware.

Covert communications

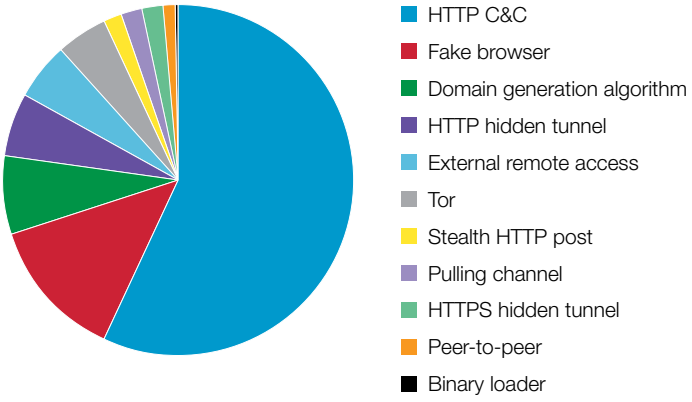
Attackers use a variety of techniques to hide their communications and stay a step ahead of traditional security. Vectra applies data science to the direct analysis of traffic to reveal hidden communications used for C&C.

In this report, there was a big jump in the use of HTTP and HTTPS for hidden tunnels. The HTTP hidden tunnel detection was the fourth most-common detection within C&C, which showed a major increase from the previous report.

HTTPS hidden tunnels are tracked separately and were less common than HTTP-based tunnels. Together, HTTP and HTTPS tunnels accounted for 7.6% of C&C detections, putting them slightly ahead of DGA detections for third place overall.

External remote access was the next most-common detection type, trailing just behind the hidden tunnels. These are particularly important detections because they can indicate that an attacker has real-time control over an internal host.

These are significant events because the presence of a RAT allows a human to directly drive the attack. It often immediately precedes the escalation of an attack to other targeted behaviors, such as lateral movement.



Detection type	Detection count	Percentage
HTTP C&C	47,626	57.0%
Fake browser	11,042	13.2%
Domain generation algorithm	6,045	7.2%
HTTP hidden tunnel	4,852	5.8%
External remote access	4,440	5.3%
Tor	3,760	4.5%
Stealth HTTP post	1,615	1.9%
Pulling channel	1,555	1.9%
HTTPS hidden tunnel	1,520	1.8%
Peer-to-peer	1,006	1.2%
Binary loader	101	0.1%

Command-and-control detections.

Botnet monetization detection highlights

Botnet monetization was the third most-common detection category and provides valuable insight into how botnet operators are shifting their tactics. While botnet infections may pose a lower risk to organizations than a targeted attack, they are by no means risk free.

Each bot infection marks an instance where an internal host was compromised to do an outside attacker's bidding. The data also shows that attackers increasingly use these hosts in a way that can damage the reputation of an organization.

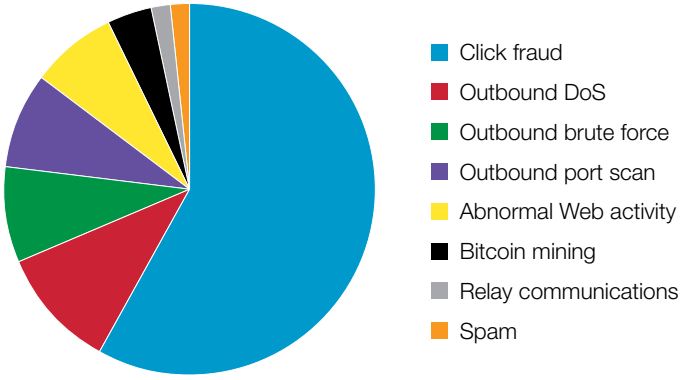
Click fraud leads; spam continues to decline

For the third consecutive report period, click fraud was the most commonly observed botnet behavior, representing more botnet detections than all others combined.

But while still dominant, click fraud detections were actually down a bit proportionally, compared to other detections. In the previous report, this category accounted for 85% of botnet detections. In this report, it declined to 58%.

The large volume of click fraud detections is not particularly surprising because the model is based on attackers who typically make miniscule amounts of money for each automated click.

While click fraud extends its stay at the top of the botnet charts, spam continues to slide. The prevalence of spam has been slowly declining over the past two reports, and was the least common botnet behavior observed in this report.



Detection type	Detection count	Percentage
Click fraud	6,975	58.1%
Outbound DoS	1,272	10.6%
Outbound brute force	996	8.3%
Outbound port scan	993	8.3%
Abnormal Web activity	926	7.7%
Bitcoin mining	443	3.7%
Relay communications	206	1.7%
Spam	195	1.6%

Botnet monetization detections.

Putting your reputation on the line

Although botnet monetization may not present the same level of risk as a targeted attack, it is not without risk to organizations and the data shows why. The proportional decline of click fraud was due largely to an increase in denial-of-service, outbound brute force and port scanning.

Taken together, these three detections represent 27% of botnet events, more than double the 12% observed in the last report. These events are especially significant because they can damage an organization's reputation.

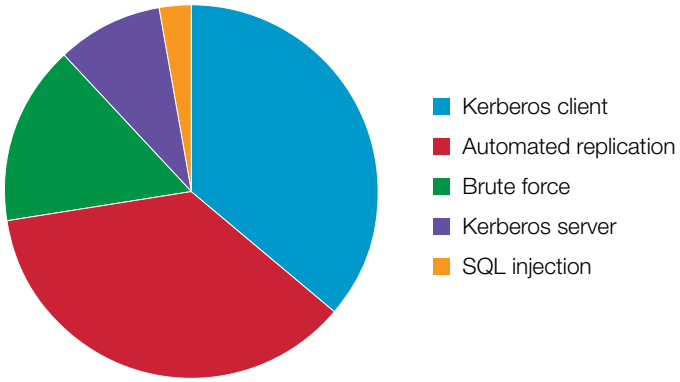
As intelligence feeds keep trying to deliver data faster, the chances of these botnet behaviors landing an organization's IP addresses on a black list increases considerably.

Lateral movement detection highlights

Lateral movement is the most strategic phase of an attack and it sets targeted attacks apart from more traditional threats. The ability to spread deeper into the network, gain privileges and establish persistence within the network are key to the success of a targeted attack.

This report shows a significant drop in brute force techniques in favor of a shift to more subtle strategies. Kerberos client and automated replication detections are tied for the lead in lateral movement, with each representing 36% of lateral movement detections.

Although complimentary, these detections reveal different approaches for cybercriminals as they progress their attack inside a victim network.



Detection type	Detection count	Percentage
Kerberos client	3,885	36.3%
Automated replication	3,884	36.3%
Brute force	1,653	15.5%
Kerberos server	977	9.1%
SQL injection	293	2.7%

Lateral movement detections.

Stealing the keys to the kingdom

Once inside the network, attackers often attempt to steal passwords or Kerberos tickets from valid users. This gives attackers access to privileged resources without additional malware or exploits and avoids attracting the attention of security teams.

The Vectra Kerberos client detection monitors the Kerberos infrastructure in a network to identify a variety of lateral movement techniques. These techniques may include account scans, service scans and potentially compromised user credentials.

Of all lateral movement detections, 36.3% were of this type. This is a significant find because it creates a need for new detection techniques. Instead of looking for overt indicators of compromise like malware artifacts, security teams must recognize behavioral anomalies based on local traffic patterns and local machine learning.

It also points to the critical role that identity plays in the progression of an attack. The combination of brute force, Kerberos client, and Kerberos server detections accounted for 61% of all lateral movement detections.

Automated replication

The automated replication detection is the co-champion of lateral movement, coming in only a single detection behind Kerberos client – 3,884 detections to 3,885. This detection model reveals when attackers deliver the same payload to multiple hosts.

These payloads can include malware, exploits or other tools that allow attackers to pivot through the network. They represent the most common way that attackers move laterally inside a network without using stolen user credentials.

Exfiltration detection highlights

The last phase in the cyber attack kill chain, exfiltration, occurs over an extended period of time until the threat is detected and resolved.

Attackers dedicate considerable effort and ingenuity to exfiltration. The inside-to-outside flow of critical assets must always cross the network perimeter to reach the wilds of the Internet and runs the risk of detection by prevention security defenses.

The good news is exfiltration behaviors are far and away the most rarely detected phase of attack in this report. The evidence means most attacks are detected and stopped before significant damage occurs.

The data smuggler detection was the most commonly observed exfiltration over the course of the study. This behavior-based detection model observes the flow of data into and out of devices.

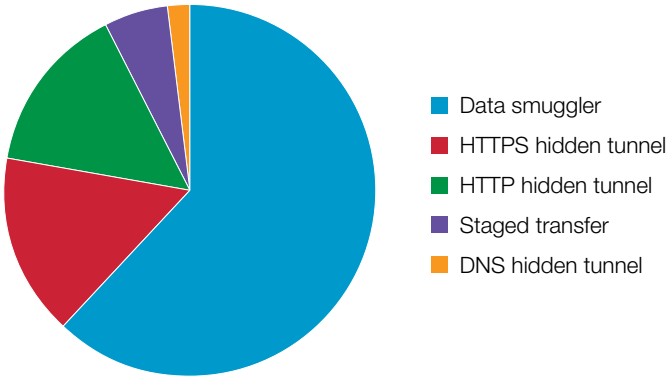
As with all of Vectra exfiltration detection models, this model identifies exfiltration over encrypted channels without the need for decryption.

HTTPS leads the way in hidden tunnels used for exfiltration

As shown earlier, HTTP is the protocol of choice for attackers who use C&C communication through hidden tunnels. However, this trend was reversed when it came time for the attacker to actually steal data, with HTTPS edging out HTTP.

HTTPS accounted for 15.9% of exfiltration detections compared to 14.5% that used unencrypted HTTP. This could be a sign that attackers are taking additional precautions to avoid perimeter security and data-loss prevention (DLP) controls during the exfiltration phase.

However, it should be noted that the number of exfiltration detections were much lower than C&C detections, and Vectra continues to monitor the trend for future editions of the Post-Intrusion Report.



Detection type	Detection count	Percentage
Data smuggler	2,450	62.1%
HTTPS hidden tunnel	627	15.9%
HTTP hidden tunnel	574	14.5%
Staged transfer	225	5.7%
DNS hidden tunnel	70	1.8%

Data exfiltration detections.

Threats by industry

Organizations from different industries can have very different resources, risks and challenges when it comes to cybersecurity.

As a result, Vectra segmented its detection data by industry to provide additional insight into how they compare to one another as well as to reveal any trends or challenges that are unique to a given industry.

As mentioned earlier in this report, participating organizations were segmented into the following industry categories:

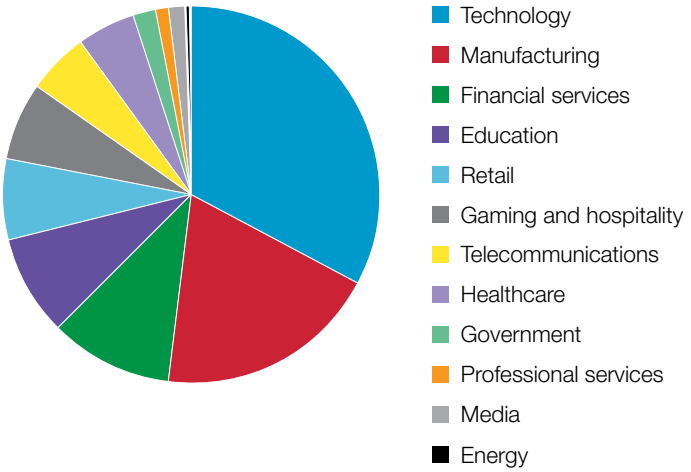
- Education
- Energy
- Financial services
- Gaming and hospitality
- Government
- Healthcare
- Manufacturing
- Media
- Professional services
- Retail
- Technology
- Telecommunications

Industry demographics

Naturally, some networks are larger than others, and some industries tend to have large networks on average. For example, a university network will often have a large number of end users and likewise generate a large number of detections.

The table below shows the proportional breakdown of each industry based on the number of host devices observed in their networks.

Technology led the way, accounting for one-third of all hosts. Manufacturing, financial services and education were also big contributors in terms of the total number of hosts, while the energy sector had the smallest representation.



Industry	Number of Hosts	Percentage
Technology	456,836	33.0%
Manufacturing	265,814	19.2%
Financial services	143,793	10.4%
Education	118,658	8.6%
Retail	98,067	7.1%
Gaming and hospitality	92,656	6.7%
Telecommunications	73,933	5.3%
Healthcare	69,523	5.0%
Government	26,604	1.9%
Professional services	16,820	1.2%
Media	15,946	1.2%
Energy	6,876	0.5%

Distribution of hosts by industry.

Measuring threats per capita

To ensure that data from a specific industry was not over or underrepresented, this report normalized the data in terms of how many threats were detected on a per host basis.

Furthermore, unlike traditional security products that generate thousands of alerts per day, Vectra detections tend to occur at a lower rate. A single Vectra detection pre-correlates hundreds or even thousands of underlying threat events gathered over time.

As a result, the data is ultimately delivered in terms of how many threats were detected per 1,000 network hosts per month (detections/1,000 hosts/month).

The table below shows how many threats were detected in each industry on a per capita basis. Note that the total detections were accrued over a period of three months.

Financial services showed the lowest overall detection rate, with an average of 11 threats detected per 1,000 hosts per month. Gaming and hospitality was the second lowest with a detection rate of 11.6.

On the other end of the spectrum, education had the highest detection rate with more than 64 detections per 1,000 hosts per month. Media and energy also had relatively high detection rates, but this might be attributable to their small sample sizes.

These results align with general expectations. Higher education in particular tends to have more permissive network policies due to the pressures of supporting large, diverse user groups while maintaining academic freedom. Conversely, financial services have strict policies and invest more aggressively in security controls.

Comparing industries across the kill chain

Although certain industries detected more threats than others, every network had some. A majority of networks showed advanced attack phases – reconnaissance, lateral movement and exfiltration – during each month of the analysis.

For deeper insight, Vectra subdivided detection rates by the phase of the attack kill chain. One notable statistic is that the rate of C&C detections seemed to predict exfiltration. In general, industries with lower C&C rates had lower exfiltration rates, and vice versa.

	Total detections	Total hosts	Per 1,000 hosts/month
Education	22,862	118,658	64.2
Energy	1,089	6,876	52.8
Financial services	4,763	143,793	11.0
Government	1,493	26,604	18.7
Healthcare	6,791	69,523	32.6
Gaming and hospitality	3,215	92,656	11.6
Manufacturing	12,610	265,814	15.8
Media	2,544	15,946	53.2
Professional services	1,946	16,820	38.6
Retail	4,440	98,067	15.1
Technology	56,354	456,836	41.1
Telecommunications	7,239	73,933	32.6
All industries	**123,345**	**1,385,526**	**30.2**

Industry threats detected on a per capita basis.

This correlation is interesting and worth monitoring in the future. However, it is important to note that an exfiltration should not be judged based purely on event counts.

The volume and importance of stolen data is of paramount importance. As a result, even a small amount of data exfiltration can have significant impact on the victim organization.

Notes and trends by industry

The following section provides a brief summary of significant findings in each industry.

Financial services

Financial services had the lowest overall detection rate, highlighted by very low botnet and C&C detections. Both categories were significantly lower than other industries, which illustrates that financial services is doing a much better job of managing commodity threats.

While the overall C&C numbers were lower, the techniques that were observed were more exotic. Financial services showed higher than normal rates of hidden tunnels and pulling instructions, both of which are tough to detect using signatures and reputation lists.

Interestingly, financial services had a relatively average rate of internal reconnaissance and lateral movement. However, this could be due to more frequent penetration testing and vulnerability scanning.

Gaming and hospitality

The gaming and hospitality sector had low detection rates across all attack phases of the kill chain. Like financial services, the gaming and hospitality numbers show that the direct protection of financial assets tends to have the most fastidious approach to network security.

Retail

Retailers had a relatively low overall detection rate of 15.1 per month per 1,000 users. This could be a sign that diligent regulatory efforts across the retail industry might be yielding tangible benefits.

But while the overall numbers are good, there is cause for concern and room for improvement. Despite having respectable C&C detection numbers, there was a high rate of external remote access detections in the category.

These detections tend to be the most serious within the C&C threat phase because they reveal real-time control of the attack by a person.

Manufacturing

Manufacturing environments had lower-than-average detection rates across the board. The only significant anomaly was that manufacturing was somewhat of a bastion for Tor traffic, which was down in most other industries.

Government

Government networks were represented by a relatively wide spectrum of organizations, spanning local, state and national government as well as law enforcement agencies. Overall, this group showed lower-than-average detection rates, although lateral movement detections pointed to a need for improvement.

Healthcare

Healthcare came in around the middle of the pack in terms of overall detection rates. As a group, healthcare organizations had a relatively high amount of C&C traffic. On a per capita basis, healthcare showed high rates of click-fraud, HTTP C&C and external remote access.

	Botnet	Command and control	Reconnaissance	Lateral movement	Exfiltration
Education	4.5	49.3	2.7	5.7	2.0
Energy	1.2	23.0	8.9	18.5	1.2
Financial services	0.2	1.2	5.3	4.3	0.1
Government	1.2	6.3	3.7	7.3	0.3
Healthcare	3.7	24.0	1.7	2.3	0.8
Gaming and hospitality	5.8	4.2	0.7	0.8	0.2
Manufacturing	2.6	8.4	2.4	2.1	0.4
Media	15.8	11.5	21.1	3.8	1.0
Professional services	0.8	12.9	4.8	19.1	1.0
Retail	0.6	6.9	4.2	2.2	1.1
Technology	4.0	31.0	3.4	1.1	1.6
Telecommunications	1.0	27.0	4.0	0.5	0.1
All industries	**3.1**	**20.1**	**3.4**	**2.6**	**0.9**

Detections per 1,000 hosts per month by category.

Telecommunications

Telecommunications had good numbers overall with the exception of C&C traffic. C&C detections were high across the board, and the industry was the overall leader in terms of malware pulling instructions.

However, the silver lining in telecommunications is that it was the only industry where high rates of C&C traffic detections did not correspond with high rates of exfiltration behaviors.

Professional services

Professional services represents another diverse group ranging from legal to engineering and construction firms. This sector was noteworthy for having the highest rates of lateral movement detections.

In this regard, the professional services industry was an equal opportunity offender, exhibiting high rates of brute force, Kerberos-based attacks, as well as internal spreading.

Technology

Technology organizations represented the largest overall group. These organizations showed higher-than-average detection rates per capita and was behind education in terms of C&C and exfiltration data rates.

Within these categories, the sector showed high rates of HTTP hidden tunnels, staged exfiltrations and data smuggler detections.

Energy

Energy had relatively high detection rates overall, but had the least number of hosts. Detection rates were considerably above average for the reconnaissance and lateral movement phases of attack.

These appeared to be tied to internal malware outbreaks that led to internal port-scanning and automated replication of malware within the networks.

Media

Like the energy sector, media organizations showed high detection rates per capita, but had a relatively small number of hosts. However, even with its small sample size, the sector showed particularly high rates of botnet traffic as well as reconnaissance.

Most significantly, the botnet traffic in question was performing outbound port scans of other networks, which presents considerable risk to an organization's reputation.

Education

Networks in the education segment showed the highest overall per-host detection rates, including the highest rates of C&C and exfiltration detections. Detections were relatively high across these categories, with high click fraud rates and HTTPS hidden tunnels.

In these networks, infected university-owned assets are usually remediated very quickly but student computers are not.

Conclusion

In this edition of the Post-Intrusion Report, Vectra significantly expanded the scope of analysis by tripling the number of participating organizations. They consisted of more than 1.3 million hosts, a more than five-fold increase over the previous report.

While overall detection rates held steady, Vectra did observe some shifts within attacker tactics. In particular, the use of hidden tunnels for C&C and exfiltration appears to be growing in popularity.

Once attackers get inside a network, analysis shows that they are shifting away from brute force attacks in favor of more subtle attacks against the Kerberos infrastructure and internal replication.

At a high-level, financial services networks provide a security model for other industries to emulate. In general, networks that had lower rates of C&C detections also had the lowest rates of data exfiltration.

Vectra would like to thank the organizations who opted-in to share metadata that was analyzed for this report, and will diligently look toward the future to identify the next wave of attack trends and detections.

VECTRA®

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com