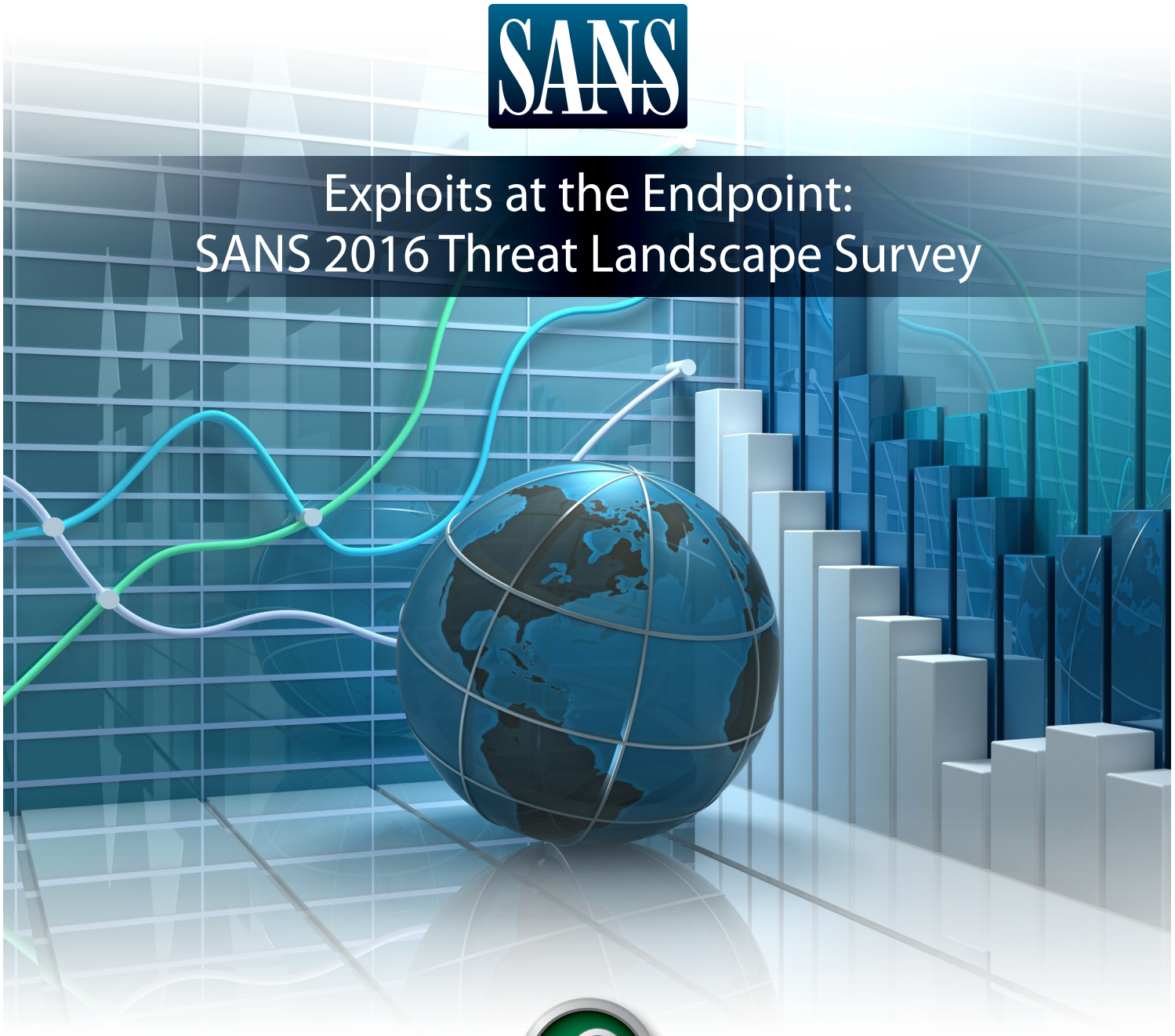


Exploits at the Endpoint: SANS 2016 Threat Landscape Survey

A SANS Survey

Written by Lee Neely

September 2016

Sponsored by
Check Point Software Technologies, Ltd.

Executive Summary

The perfect storm is upon us: Users with their many devices are falling victim to phishing and ransomware at alarming rates, based on the results of a new SANS survey taken by 301 IT professionals. In it, user actions at the endpoint represent the most common entry points allowing threats into organizations.

Results reveal that ransomware, which spreads by phishing and web downloads, is the No. 1 type of malware making its way into organizations. In the survey, this scenario repeats itself industrywide, indicating a dangerous trend. For example, a Los Angeles hospital hit by ransomware in February 2016 had all its medical records locked up for hours, and law firms, schools and even city governments fall victim to these attacks.[1] In April, the FBI estimated a $1billion ransomware market for 2016, with $209 million collected by cybercriminals in the first three months of 2016.[2]

TAKEAWAY:

Given the reliance on user interaction for propagation and the prevalence of ransomware, users—through no fault of their own—have become the biggest threat.

Of threats discovered by survey takers, 39% bypassed the network gateway firewalls, and 37% went undetected by IDSes, while endpoint security tools detected half, and routine operations uncovered 85% of threats inside the enterprise. This reinforces the risks of overreliance on signatures or known patterns to detect and stop threats.

In our connected and cloud-based world, solutions that adapt to the changing work environment are necessary to keep users, their devices and the networks they use out of trouble.

Key Findings

How Attackers Get into User Endpoints

of identified, impactful threats initially entered via email attachment

of attacks were executed by users clicking web links in email

also experienced attacks involving web drive-by or downloads

How Attackers Bypass Endpoint Defenses

through user error

through social engineering

through zero-day/unknown

[1] www.pbs.org/newshour/bb/ransomware-attack-takes-down-la-hospital-for-hours

[2] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology

About Our Respondents

The purpose of this survey was to uncover the threats organizations encounter in the real world, when and how they become incidents, how organizations rank threats and what defenses continue to work. Essentially, we wanted to learn what threat scenarios keep IT managers and security professionals awake at night and the best means of combating them.

IT Ops and Security Professionals

The survey was completed by 301 IT and security professionals, balanced between respondents with security roles and those with IT roles: 33% were security administrators or analysts, 11% system administrators or analysts, 11% IT managers or directors, and 9% were in security management. These represent key personnel who are hip-deep in threats and threat responses. They also represent the general SANS membership base.

Although some threats are industry specific, the overall results indicate that we all face the same primary threats such as phishing, ransomware and Trojan horses.

Size and Type of Industry

The top seven industries represented by our respondents are government, banking/finance, technology, healthcare, education, cyber security and manufacturing. No industry is exempt from threats. Although some threats are industry specific, the overall results indicate that we all face the same primary threats such as phishing, ransomware and Trojan horses. See Figure 1.

What is your organization's primary industry?

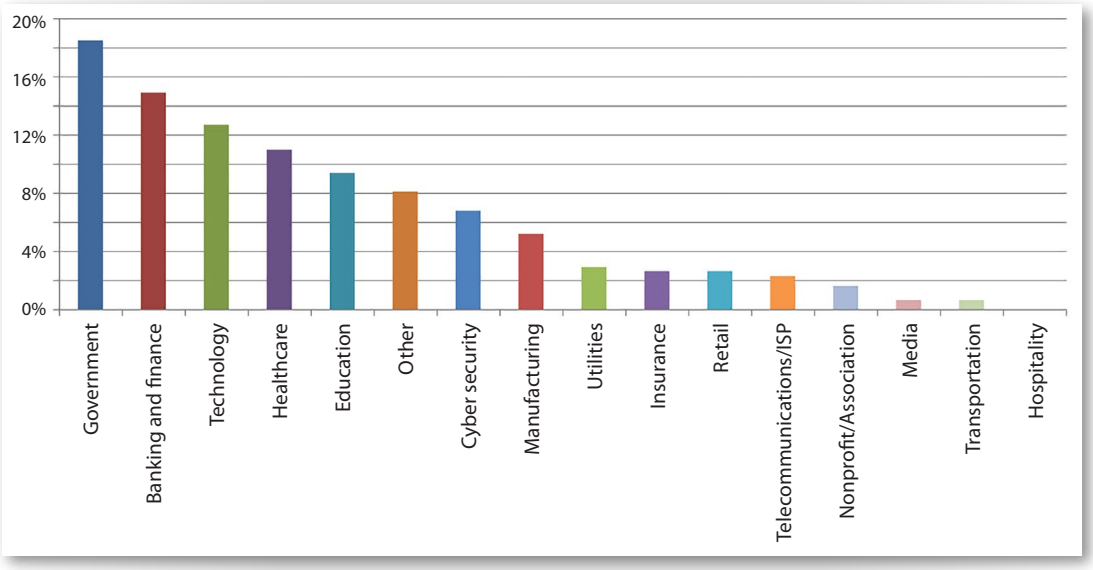


Figure 1. Type of Industry

The responses reflect input from IT professionals from companies of different sizes, with 28% coming from small to midsize companies (101–1,000 employees); 14% representing very small companies (fewer than 100 employees); then a relatively even split between medium companies (1,001–2,000 employees), large (2,001–5,000 employees) and very large (15,001–50,000 employees). See Figure 2.

TAKEAWAY:

All types of organizations are experiencing similar threats, regardless of their size or geographic location.

What is the size of the workforce at your organization, including employees, contractors and consultants?

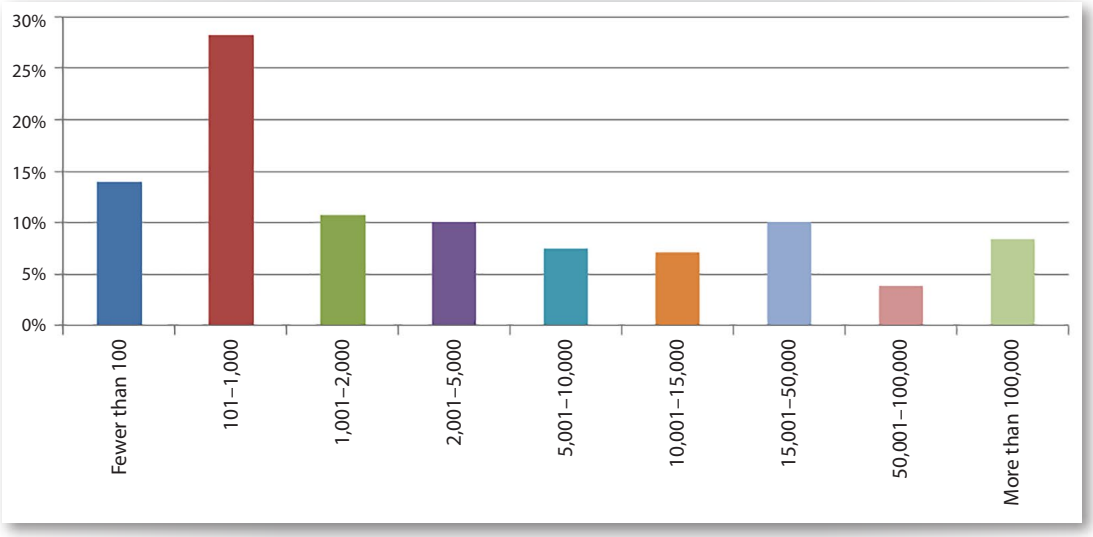


Figure 2. Workforce Size

Across the Globe

Threats also do not confine themselves to geographic regions. In this survey, respondents were from around the world, and all indicated experiencing similar phishing and ransomware threats. Most companies were United States-based and headquartered, with a concentration of operations in Europe and Asia. See Figure 3.

In what countries or regions does your organization have operations? Where is your corporate headquarters? *Select all that apply.*

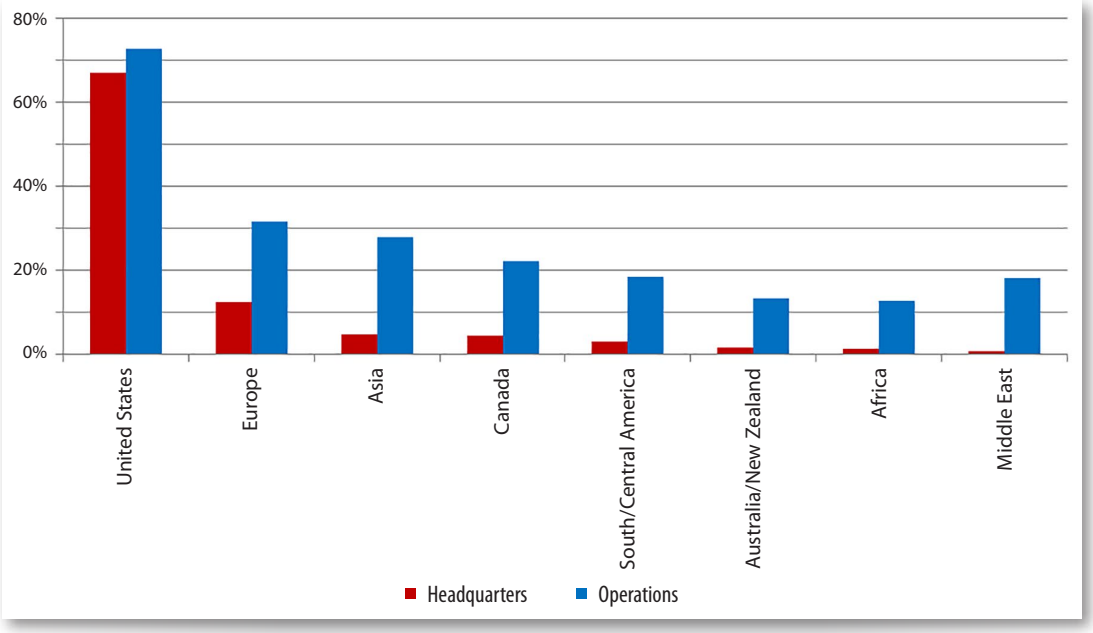


Figure 3. Operations and Headquarters

U.S. responses were about 2.3 times the volume of European responses; however, results were similar between regions. Phishing, including spearphishing and whaling, combined with ransomware make up the top significant impact threats for both regions, but respondents in the U.S. and Europe rank them slightly differently. See Table 1 for the specific U.S.-Europe regional breakdowns.

Table 1. Threats Manifested and Discovered, United States and Europe

Threats that Caused Significant Impact	U.S.	Europe
Experienced significant impact from all forms of phishing	43%	39%
Experienced significant impact from ransomware	19%	12%
Experienced significant impact from APTs	11%	11%
Experienced significant impact from SQL	5%	7%
Experienced significant impact from Trojans	5%	6%
Threats on the Rise		
Phishing	71%	63%
Spearphishing/Whaling	54%	51%
Ransomware	50%	55%
Spyware	26%	25%
DDoS	19%	27%
How Impactful Threats Get In		
As email attachments	76%	76%
As web link in email	45%	44%
Browser drive-by or download	44%	33%
How Threats Are Discovered		
Endpoint security tools	54%	42%
Calls to help desk	49%	39%
Alerts from IPS/UTM at gateway	38%	43%
Log or event review	37%	39%
Monitoring for unusual activity	36%	46%

In Europe, calls to the help desk are tied with "log or event review" for fourth place, whereas in the U.S. they were the second top means by which significant threats are discovered. In the U.S., monitoring for unusual activities is last on respondents' list of how they discover such threats, as opposed to being the top means of discovery, as it was in Europe. These results show that how organizations find threats is the only variable in which European and U.S. differences manifest themselves.

However, for the most part, location was not significant, except that the European respondents may be ahead of their U.S. counterparts in deploying automated monitoring and alerting solutions.

Just over 80% of respondents' organizations reported having a phishing incident in the past 12 months, and 27% said those threats resulted in a significant impact. Spearphishing or whaling occurred in 58% of organizations, with 13% reporting a significant impact. While Trojan horses were the next most common threat seen by 53% of participants, the impact was generally low at 7%, when compared to ransomware, reported by 49% of respondents, with 19% seeing a significant impact from the incident. See Figure 4.

Over the past 12 months, which of the following types of threats have you seen in your organization? Of those, please indicate which types of threats had the most significant impact on your organization? *Select all that apply.*

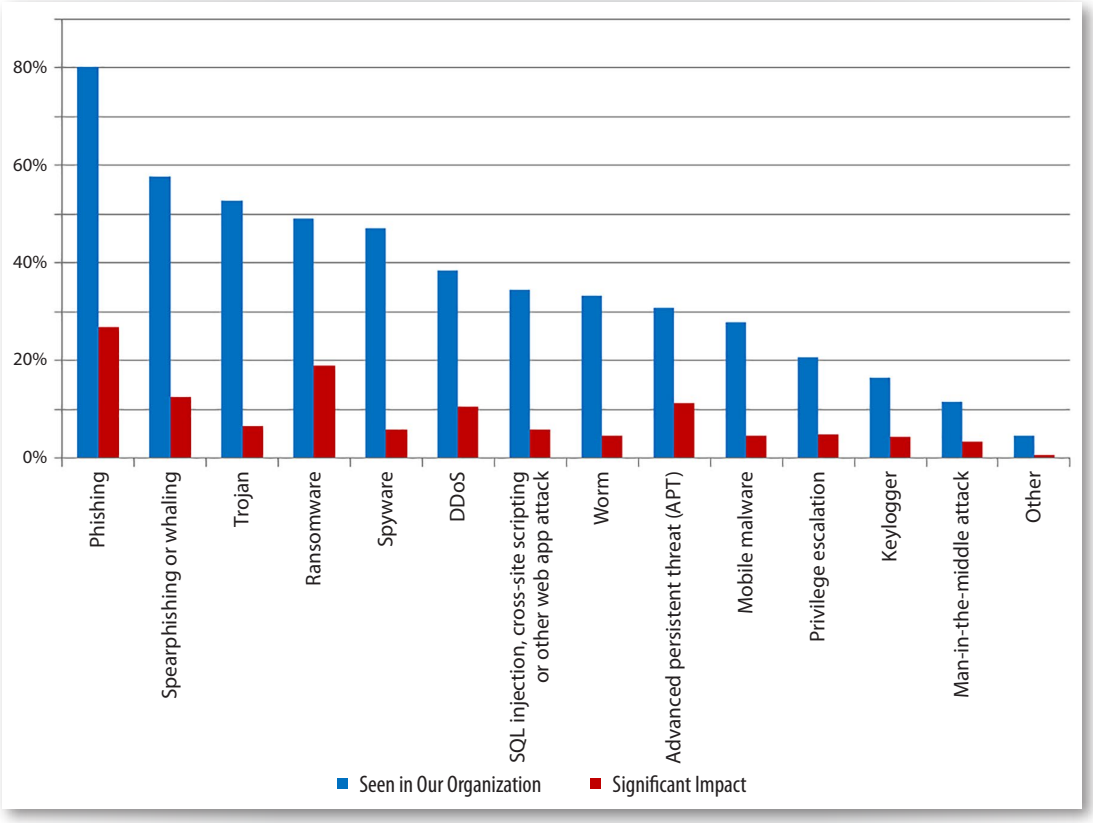


Figure 4. Phishing, Ransomware and APT Cause Greatest Impact

This scenario is ripe for enabling the propagation of ransomware. In 2015, the FBI received 2,453 reports of ransomware holdups, costing victims more than $24 million.[3] Recent estimates indicate that 390 thousand new malicious programs (malware) emerge every day,[4] while others suggest that 93% of all phishing attacks now include ransomware.[5]

The top reported threats (phishing, spearphishing or whaling, and ransomware) will consume a lot of our attention, and the next-level threats are still out there and can't be disregarded: Trojans, DDoS and APT are next in line when factoring significant impact into the weighting.

On the Rise

Here again, phishing, followed by ransomware and spearphishing or whaling, are the fastest-rising types of threats entering into organizations. The lower occurrence of worms and keyloggers is also noteworthy. See Figure 5, which reflects responses of only those respondents who knew whether they were seeing changes in frequency of these threats.

Please indicate if you've seen an increase or decrease in these types of threats over the past 12 months.

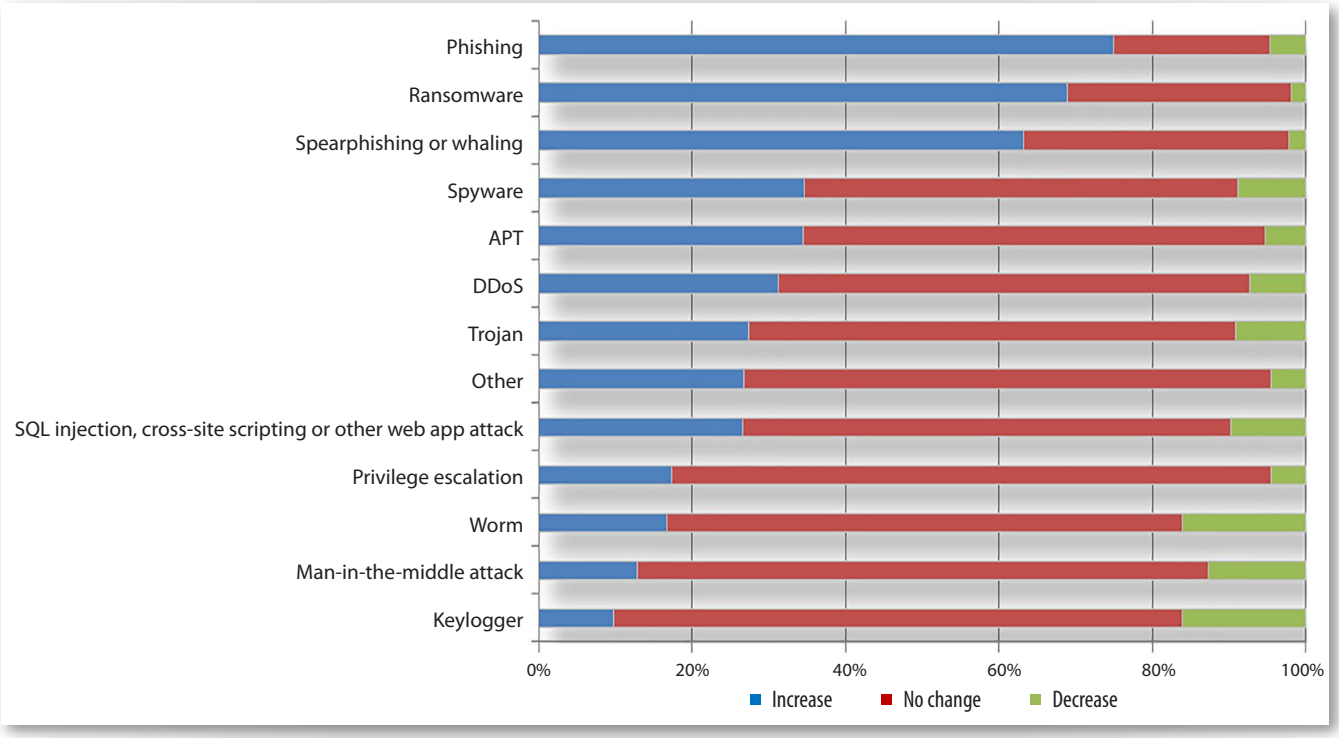


Figure 5. Phishing, Ransomware, Spearphishing Most on the Rise

[3] http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/index.html?iid=EL

[4] www.av-test.org/en/statistics/malware

[5] www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html

As these phishing and ransomware trends intersect, they create the perfect storm for legitimate user actions to result in significant, costly consequences to the organization, such as having to pay tens of thousands of dollars in ransom to retrieve critical access to maliciously encrypted data or to regain control of keys, or experiencing service denials that cause loss of business.

To respondents, the significance of the impact is tied to key corporate concerns: the cost to recover and the loss of sensitive information. Clearly, IT professionals know what's at stake. See Figure 6.

TAKEAWAY:

Spending money on new tools to address the latest threat specifically is often problematic and expensive. Organizations should look at their environments holistically, even in the midst of a breach, as they make decisions on applying tools or updating policies and processes.

What were the top three reasons you consider this incident to be the most significant?

Please rank your top three reasons in order of impact, with "First" being the most significant.

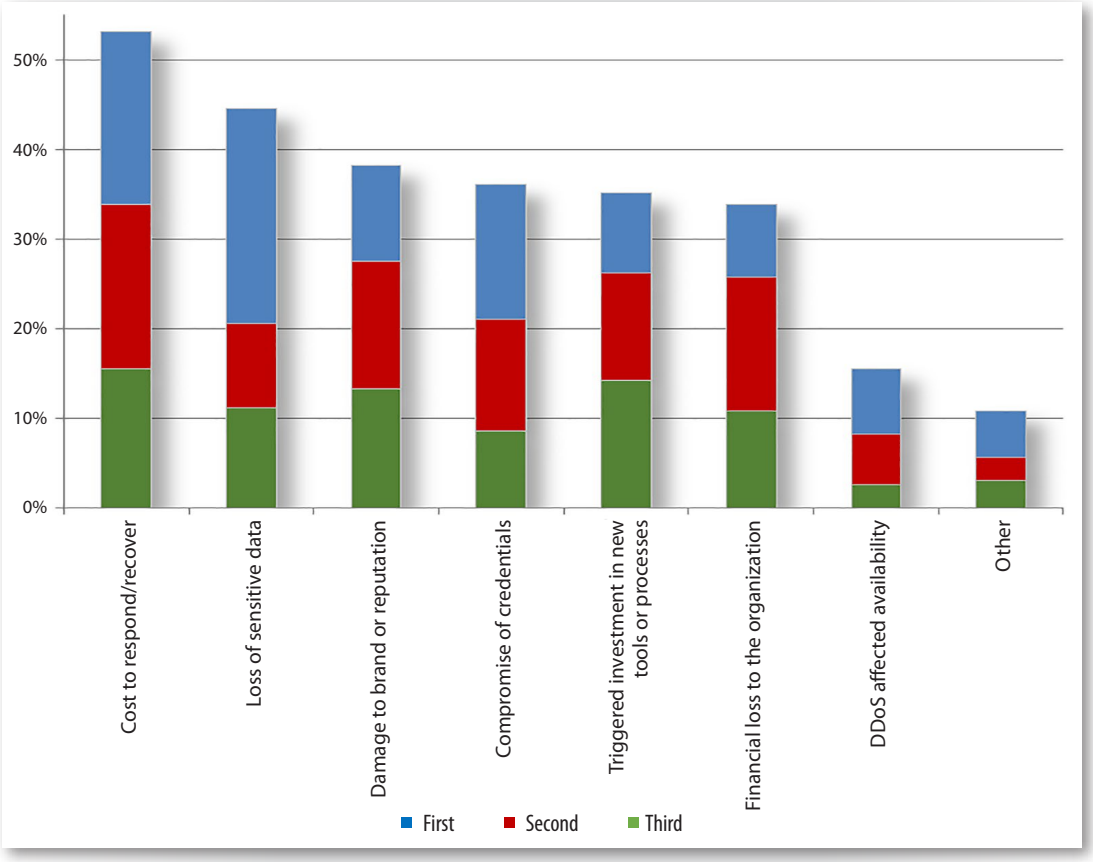


Figure 6. Cost, Loss and Damage to Reputation Top Measures of Impact

Respondents also listed damage to brand or reputation and compromise of credentials as indications of a significant incident. Interestingly, an incident that results in investments in new tools or processes ranked as a stronger indicator than financial loss to the organization.

How Threats Get In

The top ways threats are entering respondents' organizations are via email attachments, clicking a link in an email, and via a web drive-by or download. See Figure 7.

How did the threats with the most impact to your organization enter your infrastructure?
Select all that apply.

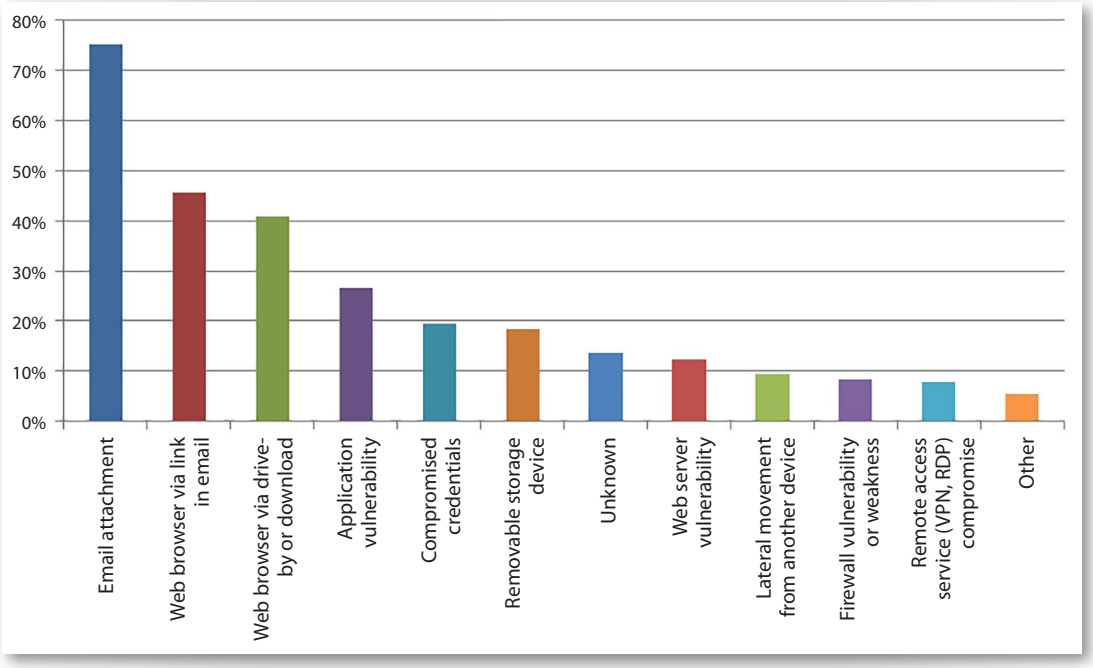


Figure 7. Threats Entering from User Endpoints

This hints at gaps in our protections, either technical or administrative, which include training users not to click on links or attachments, because these are the principal ways ransomware infections start. Counting on the user alone to "do the right thing" is not a viable security strategy. Endpoint security tools, help desk operations and security teams should work in unity to automate education and prevention.

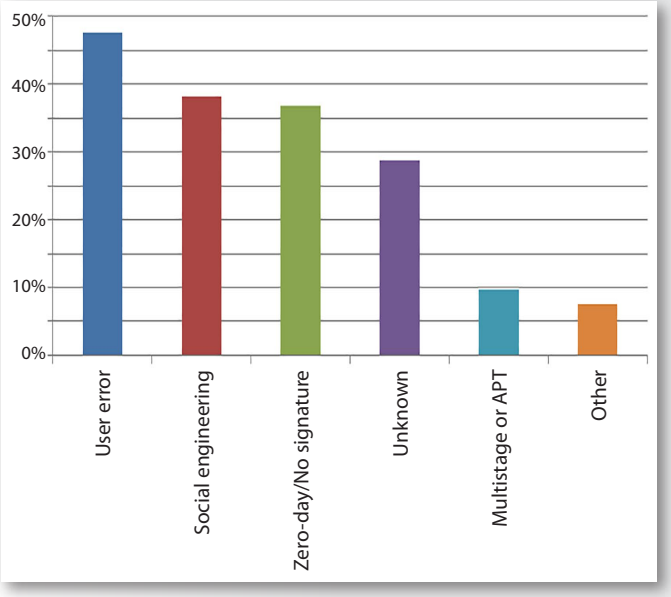
Gaps in Protections

Based on survey results, we know that user, operational and technical gaps leave vulnerabilities that allowed threats to bypass existing endpoint security:

- **User gaps.** The top successful bypasses were user-based, such as opening an attachment, clicking a link, or installing software, either by a user acting alone (deliberately or in error) or through deception (social engineering).
- **Operational gaps.** Despite advances in network and endpoint security, email monitoring, threat intelligence and event management, attackers take advantage of deployments in detection-only mode, conducting attacks or establishing footholds for APT activity before defenders are able to remediate events.
- **Technical gaps.** Too much of detection still depends on knowing what to look for, and while signatures are helpful, they are no match for the beasts of zero-day exploits, polymorphic malware, and modern exploit kits, for which there simply are no signatures.

Also, as malware evolves, the signature changes, so until the new signature propagates from the vendor all the way to the detection infrastructure, that new malware will not be detected. The same is true for network devices monitoring for threats active in their networks, as shown in Figure 8.

How did the threat (malware) get past your existing endpoint antivirus or security? ***Select all that apply.***



How did the threat (malware) get past your existing network security? ***Select all that apply.***

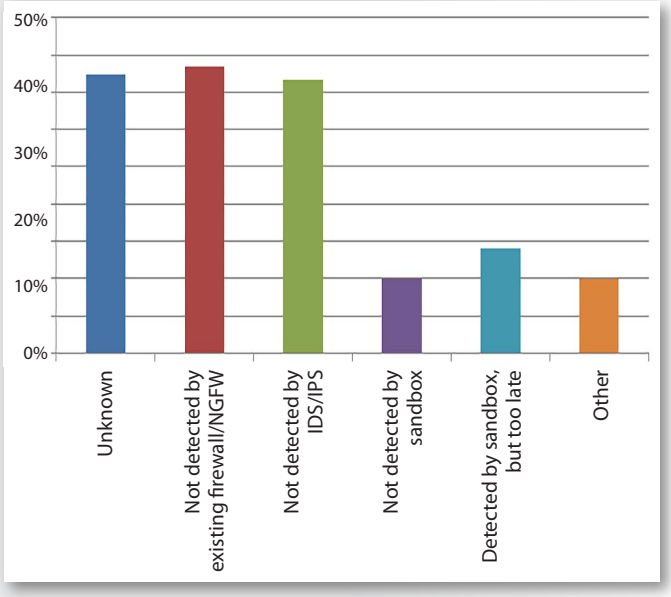


Figure 8. Bypassing Endpoint and Network Security

Firewall/next-generation firewall (NGFW), IDS/IPS and sandboxes are all catching some of the threats, but clearly not enough of them. The success of detection is dependent on the placement of network protections. A threat could evade network security via a hotspot or thumb drive; or worse, if an organization filters or blocks only inbound connections, malware could then communicate externally, download additional material, be commanded to move laterally within the organization or otherwise evolve unchecked.

TAKEAWAY:

Users should only be able to reach vetted web services from the corporate network. Take precautions, such as always requiring a VPN through the corporate network when connecting corporate assets to other networks, so your corporate protections remain in effect.

Where Are Tools Challenged (Shortfalls)

For decades, the detection of threats was principally a matter of catching the right information because it matched a database of known threat signatures. Results of this survey show that threats without signatures will not be detected reliably. Some 83% find endpoint scanning helpful, while 70% find IDS/IPS/unified threat management (UTM) systems helpful, even though today's threats are mostly slipping past them. Network monitoring/deep packet inspection (DPI) and threat intelligence are also helpful, according to respondents, as illustrated in Figure 9.

What tools or services do you find most helpful in accurately detecting impactful threats before they take a foothold in your enterprise? ***Please respond to all that apply.***

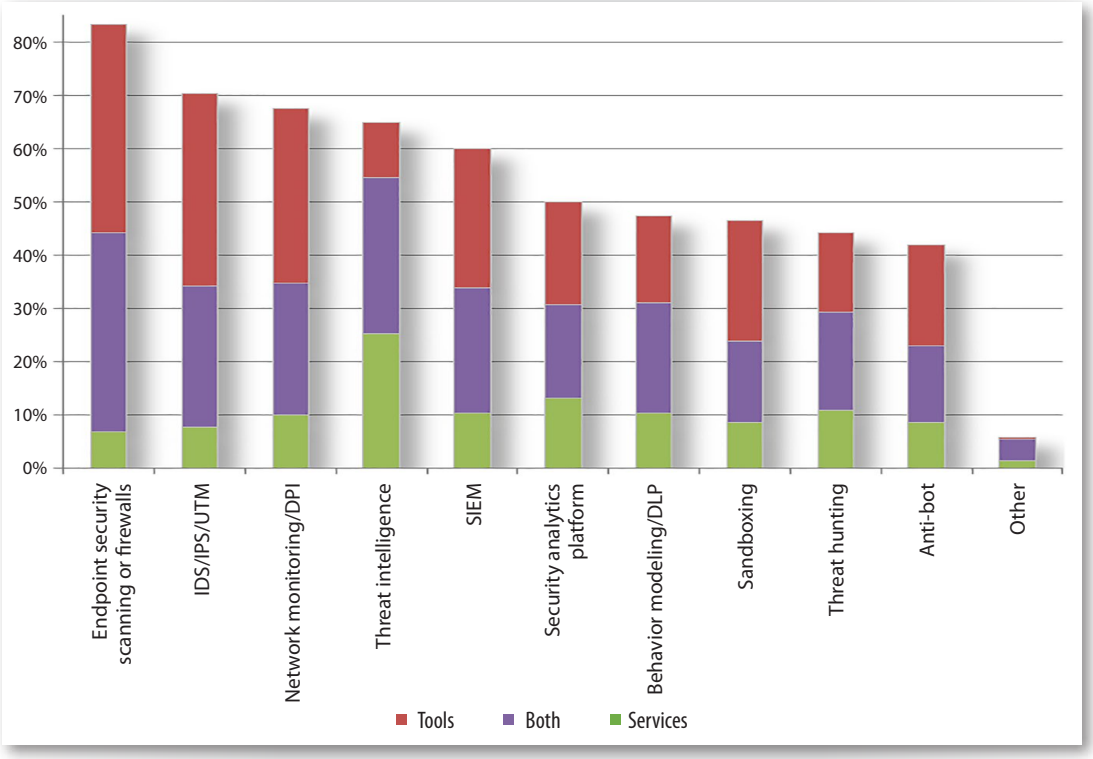


Figure 9. Endpoint and Network Tools Still Helpful in Detection

Additional opportunities exist for extension of the network perimeter to include services to protect mobile or remote users wherever they are. For example, a VPN that simply relays traffic from a mobile endpoint to the Internet, not providing corporate services, with strong but automatic authentication, could help protect the user regardless of location or network connection security.

Behavior modeling/data loss prevention (DLP), while reported by only 47% of respondents, is an area that Gartner predicts will grow as the use of analytics to detect threat increases.[6] While subscribing to threat intelligence sources helps increase awareness for the blue team, automated mechanisms to implement protections (block, observe, notify, etc.) from these newly identified threats are critical. In most cases when threats are occurring, analysts don't have time to implement new controls manually before the threat manifests itself.

Threats, Vectors and Incidents

When describing the ecosystem of an attack, we need to start with definitions. The SANS Internet Storm Center has a nice glossary of industry standard definitions of the following terms:[7]

- A *threat* is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.
- A *threat vector* is the method a threat uses to get to the target.
- An *incident* is an adverse network event in an information system or network or the threat of the occurrence of such an event.

According to OWASP, an *attack surface* describes all of the different points where attackers could get into a system and where they could get data out.[8]

How do these all come together to create a ripe ecosystem for the attacker? The attacker looks for weaknesses in the system to define the attack surface. Once he or she identifies an attack surface that includes a threat vector the attacker can leverage, the attacker can use that vulnerability to compromise the system. For example, an attacker may send a phishing email that includes a link to zero-day malware, which establishes a toehold for a remote command and control server. The attacker may then have someone call the user to entice him or her to click the link and run the malware, or even direct the user to a "safe" alternative, which is also malware. There is usually more than one viable attack vector or vulnerability, which is why defensive measures are so important to get right.

Is the User a Threat, a Vulnerability—or Both?

"By commonly used definitions, the user is a threat, not a vulnerability. What the user **does** may be a vulnerability. The user's behavior, the user's lack of knowledge, the process the user relies on . . . those may **have** vulnerabilities. But the user is not a vulnerability, just as a criminal is not a vulnerability."

—Ed Skoudis, Pen Test Curriculum Lead and Faculty Fellow, SANS Institute

[6] www.gartner.com/doc/3294335/market-trends-user-entity-behavior [Subscription required for access.]

[7] https://isc.sans.edu/glossary.html

[8] www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet

Getting Beyond Signatures

Modern adaptive threats, like zero-day vulnerabilities, don't have a ready supply of signatures to scan for. This means we need new mechanisms to stop them. The most common call to action is to whitelist everything that's allowed to operate on an endpoint. Another means is to install behavior-based detections, where threat detection tools flag and stop anomalous or nefarious actions (such as unapproved system calls, suspicious user activities, unusual traffic, etc.), rather than looking solely at specific binaries for known signatures.

Organizations should take actions to ensure that corporate network protections, such as strongly authenticated VPN, travel with mobile workers. Keep corporate assets in protective envelopes with session sandboxing and other techniques. This includes requiring access to those services through corporate network controls, even for outsourcers, to keep the corporate protections embedded in the communication path.

It is advisable to have multiple solutions working together to protect the network and the endpoint. Reliance on a single solution or single point of protection may leave gaps in your coverage. Employ a defense-in-depth strategy, with varying tools on the endpoint, desktop, server, network and in-line with web browsing to increase the coverage and prepare for threats at multiple layers.

Most important, use automation to protect users from making mistakes that will be costly. For example, include appropriate restrictions and protections relating to the introduction of removable media and software installation and vetting. These restrictions, communicated through appropriate training, must work together to allow users to get their work done securely.

Holding Them Back

Lack of signatures for unknown threats, followed by lack of skills and budgets, are the primary reasons organizations lack confidence in their ability to detect and respond to threats. In the survey, 60% of respondents say that new, unknown threats without a signature are challenging their ability to protect against threats, while 56% are limited by lack of skills and budget to implement protections. See Figure 10.

What challenges do you face in protecting against threats in your enterprise?
Select all that apply.

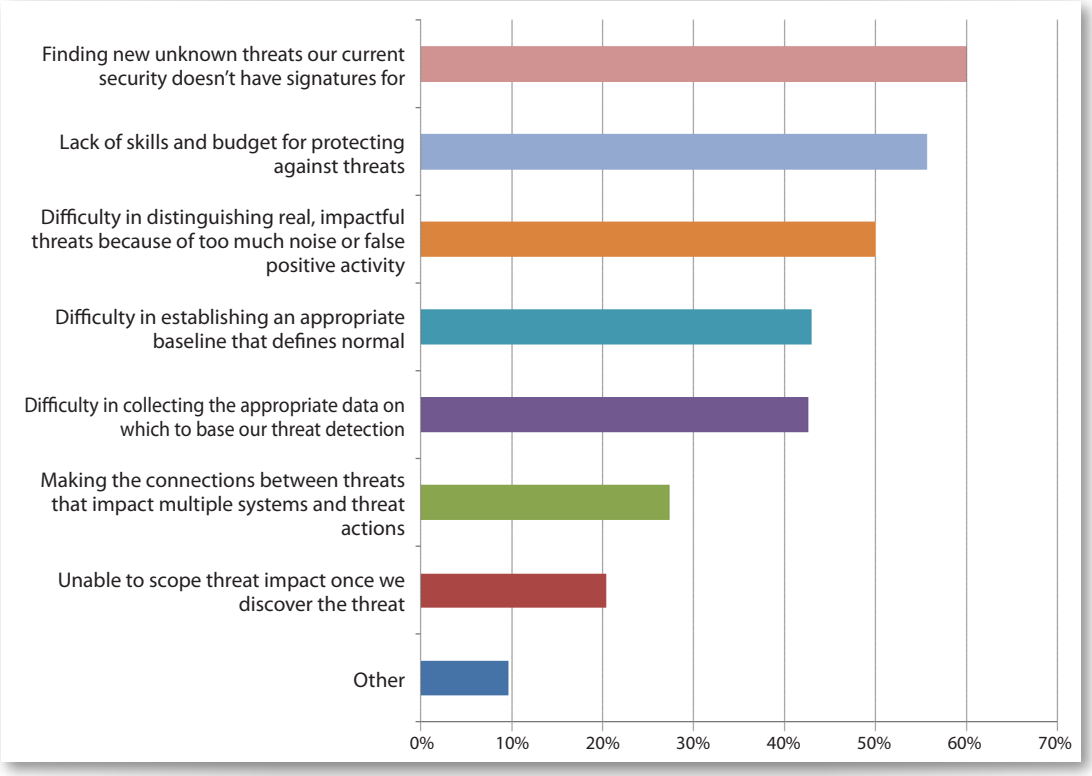


Figure 10. Challenges to Threat Protection

TAKEAWAY:

Challenges with data collection from network and endpoint sources, correlation with observed and reported results, and impact analysis all stem from lack of the right skills with the right tools in place to target, defend and otherwise keep threats in check.

If you don't have the skills and the corresponding budget to implement controls, gaps in defense will allow threats to slip past the protections in place. Furthermore, it will be almost impossible to implement new solutions to bridge any identified gaps in coverage.

Impact and Discovery

As further evidence about the need to improve network and endpoint protections from user-enabled threats, only 16% are very confident that they can detect significant threats on their networks and endpoints, and just 12% of respondents indicated they are very confident in their ability to prevent impactful threats before they cause damage. Another 26% feel very confident they could respond to threats. In addition, the majority (52%) report they are confident or very confident that they have removed all artifacts of the threat during the remediation phase. See Table 2.

TAKEAWAY:

If you cannot be sure that you've eliminated the threat, returning to normal operations is hard to defend to those who must accept the risk and attempt to return to business as usual.

Table 2. Ability to Respond to Threats

	Very Confident	Confident	Somewhat Confident	Not Confident
Prevent impactful threats before they cause damage on your network and endpoints	11.7%	46.1%	30.0%	11.3%
Detect impactful threats occurring on your network and endpoints	15.7%	44.8%	27.4%	10.4%
Remove all artifacts of impactful threats on network and endpoints	16.1%	36.1%	34.3%	11.3%
Respond to impactful threats on the network and endpoints	26.1%	37.0%	27.0%	6.5%

Taken as a whole, the good news is that the majority feel confident or very confident in their ability to perform these tasks. However, while more than 60% feel confident or very confident in their ability to detect, prevent and respond to impactful threats, almost 40% are only somewhat confident in their capabilities or are not confident at all. Clearly there is room to improve on all fronts. It's important to realize that efforts to prevent impactful threats will also yield benefits by reducing the number of events requiring a response.

Impact of Threats

While 43% of threats did not result in sensitive data loss, DDoS or other significant impact, 34% said 1–5% of their threats resulted in sensitive data loss, another 11% said their threats resulted in data loss 6–10% of the time, and 12% of threats resulted in data loss more than 10% of the time. See Figure 11.

What percentage of discovered threats led to an actual compromise of sensitive data, business outage (DDoS) or other significant impact?

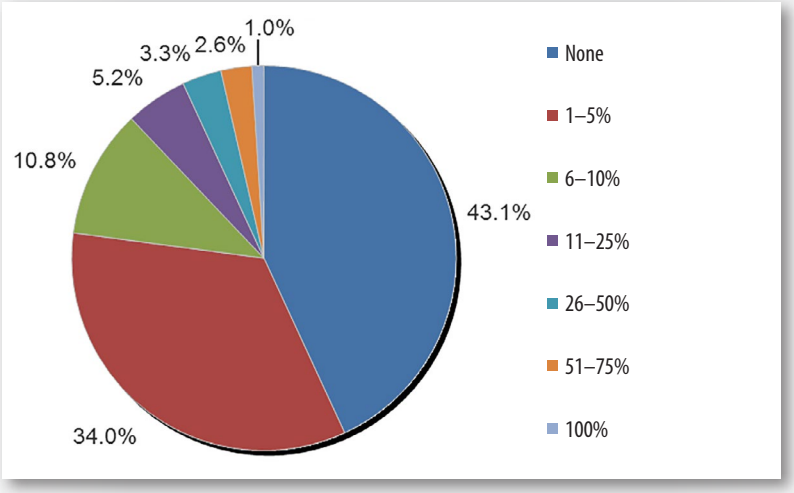


Figure 11. Threats Turned to Compromises[9]

This means that we're finding threats quickly. The majority of respondents (70%) report that the time to discover a threat that actually became an incident takes less than 24 hours, and 64% remediate in under 24 hours, as shown in Figure 12.

Time to Discovery Versus Time to Remediate

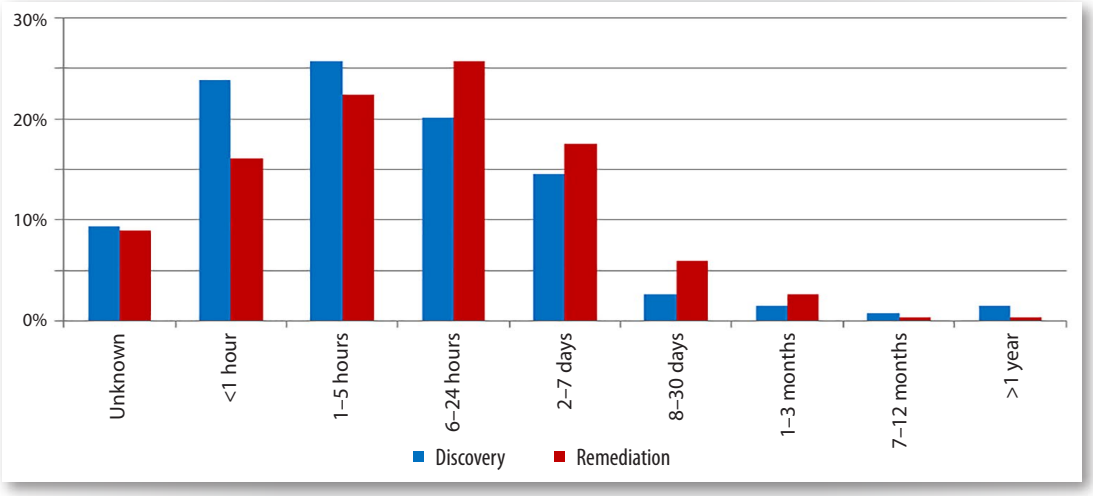


Figure 12. Time to Detect, Remediate[10]

[9] No respondents selected 76–99%.

[10] No respondents reported needing 4 to 6 months for discovery or remediation.

These results seem to fly in the face of the lack of confidence respondents have in their ability to detect, respond to and remediate attacks. It is possible that respondents have underestimated the speed with which they are able to address threats.

Discovering Threats

Security personnel find most threats (85%) during routine operations, with 24% discovering them through routine vulnerability assessments, according to the survey. This is a good indication that most organizations have enough tools and processes to make detection part of their operational fabric.

For half of the respondents, endpoint security tools are successfully discovering threats, and 47% reported discovering threats through user calls to the help desk. (Of course, at the point where the user is contacting the help desk to request support, the malware has already had an opportunity to cause damage and potentially spread beyond that user's system.) Figure 13 also reveals the limited effect of gateway security, discussed earlier in this paper.

TAKEAWAY:

Participants are telling us that endpoint security is their most strategic defense at this time, with their users (by way of calls to the help desk) being the second greatest discovery tool for finding the most significant threats. Having tools beyond the endpoint is also critical for defense in-depth protection.

How were the most impactful threats discovered? ***Select all that apply.***

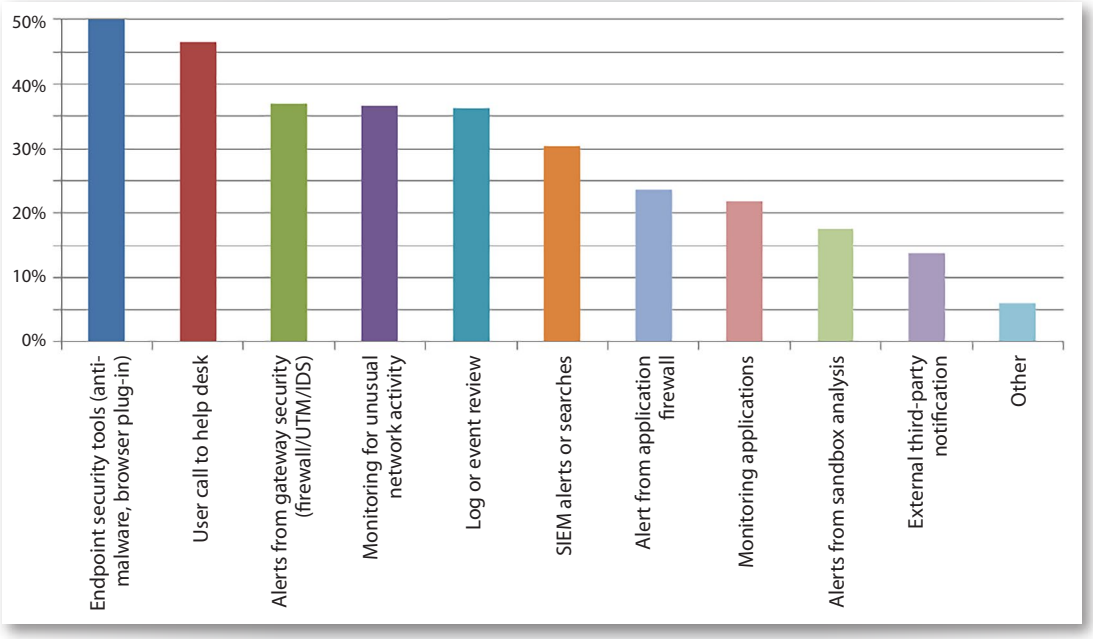


Figure 13. Endpoint Tools for Discovering Threats

Just as endpoints and their users are part of the problem, this figure illustrates that they are also the most effective tools for detecting threats. As endpoint security tools have evolved from simple antivirus detection engines to systems that check file, email and web traffic interaction with the endpoint, visibility into the potential attack surface has also improved.

Determining Impact

Organizations are using good, old-fashioned forensics to determine the impact of a given manifested threat. They are also leveraging threat intelligence, most likely processed through their SIEM, which tied with threat intelligence in usefulness, as shown in Figure 14.

What tools or services do you find most helpful in accurately determining the scope of events involving the discovered threats? ***Please respond to all that apply.***

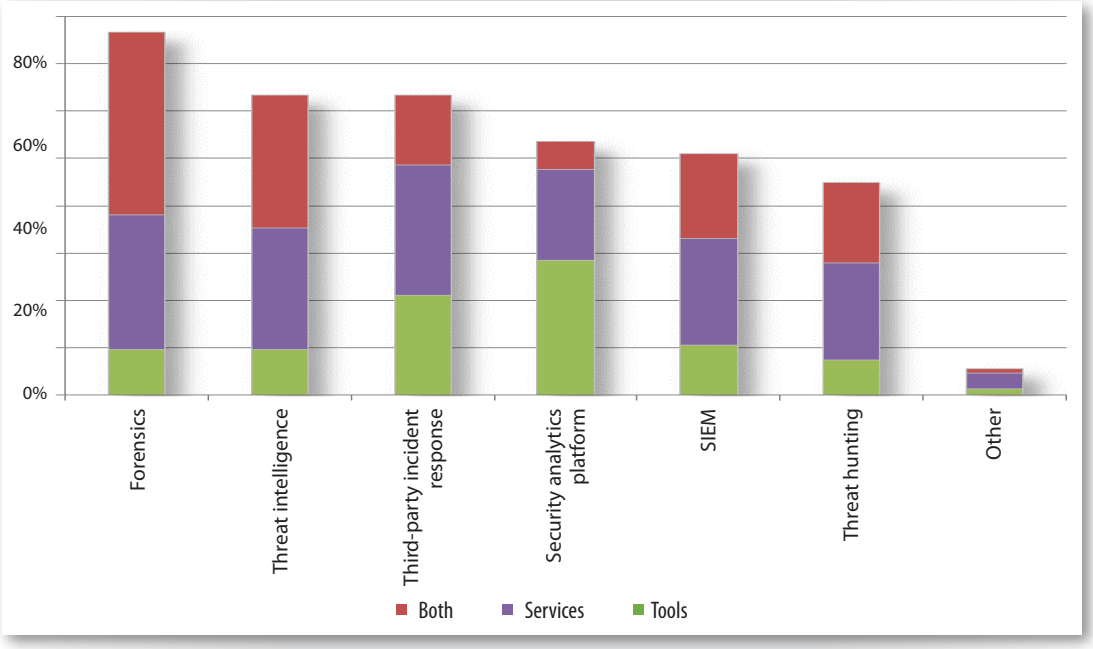


Figure 14. Forensics, Intelligence and SIEM Most Useful in Scoping Threat Events

Organizations are also able to determine the root cause of significant threats at least 70% of the time, while 14% say they are not able to determine root cause and 16% don't know.

Root cause determination processes are still dependent on associated manual processes. Respondents ranked their top choices for determining root cause as: 1) automated search, 2) interviews of affected parties and 3) automated hunting for unknown threats. Their second choices, in order, were manual log analysis, manual analysis of endpoint data and automated searches using disparate tool and information sources. Considering that most incidents involve multiple methods of investigation, the heavy reliance on manual methods (including interviews) is of concern as the volume of threats increases. While organizations collect much of the right data, the tools they are using are unable to find it without manual intervention, as shown in Figure 15.

What methods do you use to determine root cause of an incident?

Please rank your top three methods. Rank the method used most often "First."

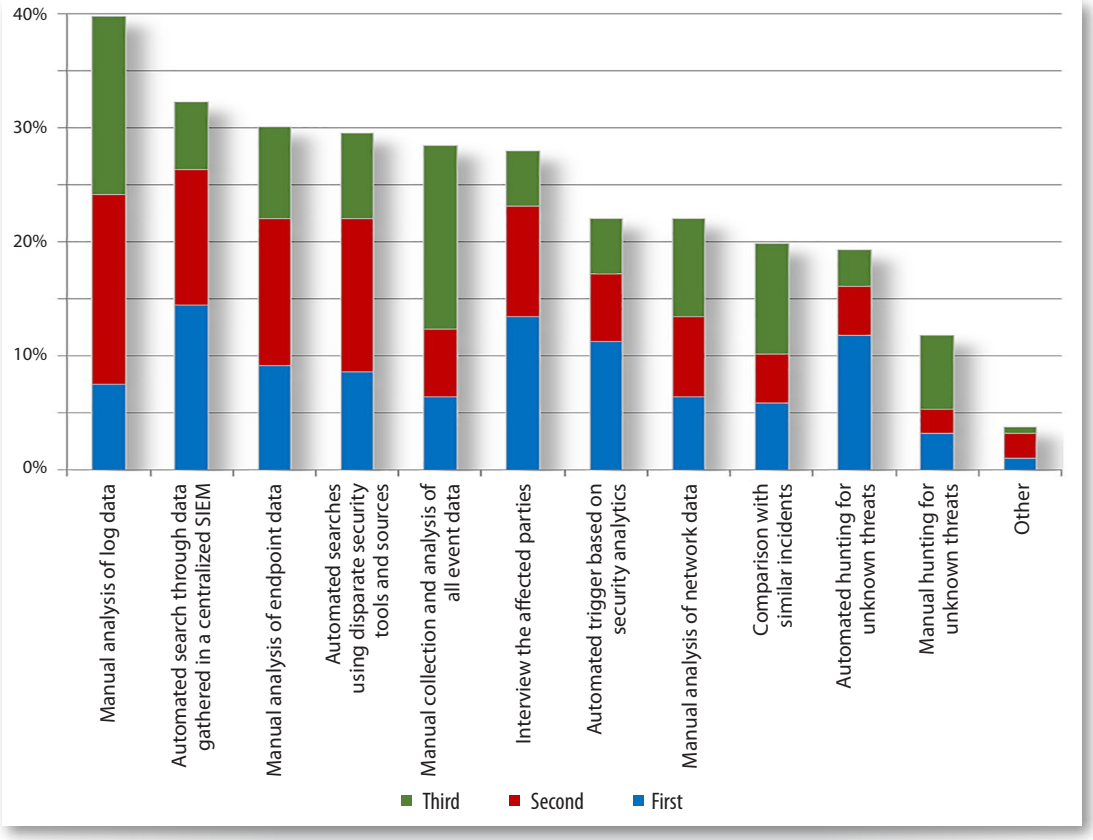


Figure 15. How Root Cause Is Determined

It's important to get to the root cause of incidents, because such knowledge is the first step toward preventing recurrence. Root cause provides new intelligence to protect the endpoint and/or network from future instances of the same threat and threat actor. It is also important for knowing where and how to apply the best controls.

Conclusion

The results of this survey remind us that although we are collectively working to install the greatest detection and defense mechanisms, users and their endpoints are the most common cause of breaches *and* the most critical component in our cyber defenses.

Despite the ever-growing landscape of detection-avoiding malware classes, endpoint security tools are still the primary detection method, followed closely by calls to the help desk. By that same token, our threat intelligence, monitoring, event review and SIEM tools also provide much discovery information, indicating that we are not reliant on the endpoint for all the heavy lifting here.

The call to action stems from the reliance on current endpoint detection in an area where the No. 1 source of malware (ransomware) is evolving and changing faster than signature-based detection services can stay abreast of the threat. Next-generation protections both at the perimeter and within the network have to augment the endpoint security to detect malicious activity that may have started with the endpoint, such as unusual system calls, sensitive data transfers, and more. In addition, endpoint security must augment network security, and the tools should share their data for more real-time detection and prevention at the endpoint, where most threats originate.

It's also important to enable mobile worker devices to continue to be protected by corporate services regardless of location so they never operate without a safety net. Organizations also need behavior-based comprehensive threat analysis systems and extensive whitelisting to stay ahead of the current threat landscape.

Threats are always changing. For now, users and their devices are ground zero. Phishing has turned to spearphishing and whaling exploits that are well-researched and convincing enough to get corporate officers to click links and download attachments that open their enterprises to risk. Ransomware is taking hold in organizations through the user endpoint and via phishing and drive-by downloads into browsers from the web. Under the current landscape, shoring up the end user/endpoint protections should be top priority for organizations that want to make the biggest impact on reducing their overall risk.

About the Author

Lee Neely, a SANS mentor instructor, teaches cyber security courses for SANS. He worked with the SANS SCORE (Security Consensus Operational Readiness Evaluation) project to develop the iOS Step-by-Step Configuration Guide, as well as the Mobile Device Configuration Checklist included in the SEC575 course. Lee holds the GMOB, GPEN, GWAPT, CISSP, CISA, CISM and CRISC certifications. At the Lawrence Livermore National Laboratory (LLNL), Lee leads LLNL's cyber security new technology group, working to develop secure implementations of new technology, including developing the secure configurations, risk assessments and policy updates required for its corporate and bring-your-own-device mobile devices.

Sponsor

SANS would like to thank this survey's sponsor:

Check Point®
SOFTWARE TECHNOLOGIES LTD