Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **November 2019**
Sponsored by **Spamhaus Technology**

The Value of Threat Intelligence

Executive Summary

Cyber security is an ongoing battle between sophisticated and well-funded bad actors and those who must defend corporate networks against their attacks. The bad news is that the latter are typically not winning. A recent Osterman Research survey[i] found that while most organizations self-report that they are doing "well" or "very well" against ransomware, other types of malware infections, and thwarting account takeovers because of the significant emphasis placed on these threats, they are not doing well against just about every other type of threat. These include protecting data sought by attackers, preventing users from reaching malicious sites after they respond to a phishing message, eliminating business email compromise (BEC) attacks, eliminating phishing attempts before they reach end users, and preventing infections on mobile devices.

This missing component for most organizations is the addition of robust and actionable threat intelligence to their existing security defenses, which can be segmented into four subcategories[ii]:

1. Strategic (non-technical information about an organization's threat landscape)
2. Tactical (details of threat actors' tactics, techniques and procedures)
3. Operational (actionable information about specific, incoming attacks)
4. Technical (technical threat indicators, e.g., malware hashes)

The use of good threat intelligence can enable security analysts, threat researchers and others to gain the upper hand in dealing with cyber criminals by giving them the information they need to better understand current and past attacks, and it can give them the tools they need to predict and thwart future attacks. Moreover, good threat intelligence can bolster existing security defenses like SIEMs and firewalls and make them more effective against attacks. Threat intelligence plays a key role in proactive defense to ensure that all security programs are relevant to the fast-evolving threat landscape. This is particularly valuable in security awareness training to ensure users are familiar with known threats.

Good threat intelligence capabilities can provide a great deal of information about the domains and IP addresses that are attempting to gain access to a network.

KEY TAKEAWAYS

Here are the key takeaways discussed in this paper:

- Security incidents are common: a recent Osterman Research survey found that more than four in five organizations reported one or more serious security incidents had occurred during the previous 12 months.
- While the average dwell time – the gap between infiltration and discovery of a threat – is shortening, it is still quite long, enabling bad actors ample time to steal corporate data and financial assets.
- Existing security defenses provide some measure of protection against increasingly sophisticated threats, but the enormous number of data breaches and related problems experienced by many organizations reveals that current security practices are not adequate.
- Good threat intelligence capabilities can provide a great deal of information about the domains and IP addresses that are attempting to gain access to a network. It can enable threat researchers to better understand the source of current and past attacks and better deal with future attacks.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Spamhaus Technology; information about the company is provided at the end of the paper.

Critical Problems in Cyber Security

SECURITY INCIDENTS ARE COMMON

The majority of organizations have endured some type of security incident and/or a successful infiltration of their security defenses during the previous 12 months. As shown in Figure 1, nearly a third of organizations have undergone an accidental leak of sensitive or confidential information, while almost as many have experienced a successful BEC attack or an external phishing attack that deployed malware on the corporate network. We found that only 19 percent of organizations have not reported an occurrence of the problems listed in the table below.

Figure 1
Security Incidents That Have Occurred During the Previous 12 Months

Incident	%
Sensitive / confidential info was accidentally leaked through email	30%
An email as part of a BEC attack successfully tricked one or more lower level employees in our organization	29%
An external phishing attack successfully stole user credentials	28%
A phishing attack was successful in infecting systems on our network with malware	24%
A targeted email attack launched from a compromised account successfully stole a user's account credentials	20%
A fileless/malwareless attack reached an endpoint	20%
A targeted email attack launched from a compromised account successfully infected an endpoint with malware	18%
Sensitive / confidential info was accidentally or intentionally leaked through a channel other than email	14%
An email as part of a CEO Fraud/BEC attack successfully tricked one or more senior executives in our organization	13%
A targeted email attack launched from an internal account successfully infected an endpoint or software system	12%
One or more of our systems were successfully infiltrated through a drive-by malware attack from employee web surfing	12%
Malware has infiltrated our internal systems, but we are uncertain through which channel	10%
One or more of our endpoints had files encrypted because of a successful ransomware attack	10%
A targeted email attack launched from an internal account successfully stole a user's account credentials	9%
A targeted email attack was successful in infecting one or more of our senior executives' systems with malware	9%
An unauthorized user successfully accessed a secure database	7%
An account takeover-based email attack was successful	7%
Sensitive / confidential info was intentionally leaked through email	7%
Sensitive / confidential info was accidentally or intentionally leaked through a social media / cloud application	7%
Sensitive / confidential info was accidentally or intentionally leaked, but how it happened is uncertain	4%
None of these things happened	19%

Source: Osterman Research, Inc.

There are a variety of security issues that concern decision makers.

So, have 19 percent of organizations not experienced any sort of security incident during the previous 12 months? Not everyone in an IT or security department will always be forthcoming about every problem that occurs in their organization. That's

not to say that respondents to our survey aren't telling the truth, but security breaches are typically embarrassing incidents that might reveal mistakes that security staffers have made poor decisions about the security infrastructure they have deployed, and so forth. As a result, we believe that the 19 percent figure shown in the table above might be a bit high, and these problems might be somewhat worse than they seem.

ISSUES THAT CONCERN DECISION MAKERS MOST

There are a variety of security issues that concern decision makers, but the leading concerns are phishing attempts that reach end users and employees who do not recognize phishing and social engineering attacks, as shown in Figure 2. There are several other issues that decision makers are concerned or extremely concerned about – things like zero-day exploits, ransomware attacks, targeted attacks, and compromised login credentials.

Figure 2
Issues About Which Security Teams are Concerned
Percentage Responding "Concerned" or "Extremely Concerned"

Concern	%
Phishing attempts making their way to end users	74%
Employees failing to spot phishing and social engineering attacks	72%
Zero-day exploits	54%
Ransomware attacks successfully infecting endpoints	53%
Targeted attacks	53%
Login credentials being compromised	51%
CEO Fraud/Business Email Compromise attempts making their way to end users	51%
Fileless malware, e.g., rogue browser extensions	49%
Accidental breaches of sensitive or confidential data by employees	49%
Malware getting into your network from employees using the web	49%
Malware other than ransomware successfully infecting endpoints	46%
Malicious breaches of sensitive or confidential data by employees	38%
Command-and-control (C2) callbacks	36%
"Shadow IT" – employees using unauthorized cloud apps and services	32%
Internal threats (threats originating from within your organization)	24%
Spam reaching end users	21%
Cryptocurrency mining malware being installed on your internal PCs or servers	20%
Employees surfing websites that violate corporate policies (e.g., porn sites, gambling sites, etc.)	18%

Source: Osterman Research, Inc.

Losing intellectual property as a result of a competitor's actions would be considered the worst possible scenario.

Note that the figures above include the root causes of exploits *and* the outcomes of those exploits. For example, a phishing attempt that makes its way to an end user might be the delivery mechanism for the attack that will successfully infect an endpoint with ransomware or some other type of malware.

WHAT'S THE WORST SCENARIO?

We asked security decision makers and influencers about the seriousness of various scenarios in which intellectual property would be lost. As shown in Figure 3, losing intellectual property as a result of a competitor's actions would be considered the worst possible scenario, followed closely a loss resulting from the actions of an organized criminal group.

Figure 3
Scenarios for Losing Intellectual Property
Percentage Responding "Serious" or "Extremely Serious"

Source: Osterman Research, Inc.

WILL THE CLOUD INCREASE SECURITY THREATS?

The wholesale migration of key applications and critical data assets to the cloud by many organizations raises a key question for corporate decision makers: will migrating applications and data to the cloud improve security or will it make things worse? There are a couple of views on this:

- Security will worsen as applications and data move to the cloud because each application provider uses a different security model. Also, because credential theft may be more likely in cloud environments, organizations may become more vulnerable to phishing, BEC, social engineering and other threats. For example, the migration to Office 365 has spawned a large number of Office 365-specific phishing attempts that attempt to steal login credentials.
- On the other hand, security could improve as applications, data and security capabilities migrate to the cloud, since specialist security providers are sometimes better at managing sophisticated and emerging threats. This is especially true when comparing cloud security providers to in-house security teams in smaller organizations.

One of the fundamental problems that organizations face in the context of security breaches is that many incursions are difficult to detect and many take a very long time to detect.

The Ability to Respond to Threats is Key

MANY ORGANIZATIONS HAVE BEEN BREACHED, BUT MANY DON'T KNOW IT YET

One of the fundamental problems that organizations face in the context of security breaches is that many incursions are difficult to detect and many take a very long time to detect. The so-called "dwell time" – the length of time between the initial compromise and when it is discovered – is fairly long, although it has been improving over time. For example, FireEye Mandiant has been tracking dwell time since 2011

and has found that global dwell time has decreased significantly, from 416 days in 2011 to 78 days in 2018. However, there are significant variations in dwell time across geographies – in 2018 it was 71 days in the Americas; 177 days in Europe, the Middle East, Africa and north/northwest Asia; and 204 days in southeast Asia, Australia and Oceania[iii].

While the decreases in dwell time are good news, even a "short" gap of 71 days between initial compromise and detection means that an infiltrator has nearly 2.5 months to poke around a corporate network, steal data, learn the typical amounts and timing of wire transfers, and so forth. In short, while shortening dwell time is a good thing, it's still long enough for cyber criminals to wreak havoc on an organization.

CYBER CRIMINALS HAVE A NUMBER OF APPROACHES

Cyber criminals employ a number of basic approaches to infiltrate their potential victims. While we call these out as separate bullet points, they are mostly interrelated – a single threat can include many of these threat vectors:

- **Phishing emails**
  These are widely distributed email messages focused on obtaining information from users. Cyber criminals seek information such as login credentials, credit card information, healthcare login credentials, Social Security numbers and other confidential information. Phishing emails seem to be from trustworthy sources with which potential victims might have established relationships, making it more likely that some recipients will become victims.

- **Spearphishing emails**
  A more focused version of phishing, spearphishing is targeted at a small group of potential victims, such as senior managers in a company or developers. Spearphishing requires criminals to study their targets and craft a message that is intended to have a high degree of believability and a potentially high open rate.

- **Botnets**
  Botnets are groups of computers that have been quietly compromised and that can be used for a wide variety of uses, such as sending spam, malware, etc.

- **Malware**
  "Malware" is an encompassing term that includes many types of malicious code. Cyber criminals will distribute malware through different channels, although email continues to be the primary threat vector.

- **Spam**
  One of the oldest threat vectors is spam. While traditional spam is normally more an annoyance than a threat, it is often used as part of malware-distribution campaigns.

- **Social engineering**
  Threats like phishing emails normally use social engineering techniques. However, phishing can also occur via compromised social media accounts, instant messaging or chat accounts, or via text messages. In some cases, victims can be compromised via voice calls or even in-person.

- **Other threats**
  There are a number of other threats, such as simple employee errors, watering holes, the use of consumer tools in the workplace, copycat mobile applications, malvertising, brute force hacking, compromised search engine queries, and gullible users.

Even a "short" gap of 71 days between initial compromise and detection means that an infiltrator has nearly 2.5 months to poke around a corporate network.

DOMAIN AND IP INFORMATION

A common thread running through these varied threats is that the vast majority of them contain some type of domain and/or IP information that can support domain/DNS-based investigations. For example:

- During attacks, botnets will generally contact command and control IP addresses (and sometimes domains) that can be identified by analyzing firewall logs. DNS lookups of domain names can provide secondary support to an investigation, but because threat actors often won't use registered domains, firewall logs tend to provide better intelligence.

- In some cases, malware can be reverse-engineered to obtain relevant information, such as IP addresses or domain names. Malware hashes also allow organizations to proactively identify known threats

In short, these threats will sometimes include information about their source that can be useful to security analysts, forensics investigators, threat hunters, and others in determining who is responsible for sending them. However, many believe that "soft" indicators, such as IP, domain (not necessarily URL) and geolocation indicators by themselves are not sufficient to thwart threats. Indicators tied to specific payloads, such as malware hashes, allow for proactive malware detection and force threat actors to frequently adapt and manipulate their payloads. While this turns into a cat-and-mouse game, it keeps threat actors on a hind-foot. Correlating individual IOCs from identified threats and understanding threat actor TTP's and how they are evolving are also necessary components to a strong network defense.

THREATS ARE BECOMING MORE SOPHISTICATED

Cyber criminals are developing more sophisticated methods to gain access to intellectual property, financial assets, sensitive data, etc. Here are some of the methods they use:

- Cyber criminals use credential-stuffing, a technique in which usernames and passwords gathered from earlier breaches are used in automated attacks on various sites. It's effective because many users will use the same login credentials on multiple sites. One source has found that credential-stuffing tools are effective in one in 20 attempts[iv], and that there was an average of 115 million credential stuffing attacks every day during 2018[v].

- There has been a big increase in PDF-based attacks during 2019. One source found in excess of 47,000 new attack variants within PDF files in all of 2018, but discovered 73,000 such attacks in March 2019 alone[vi].

- Magecart, which refers to both a data-skimming technique and a consortium of hacker groups, uses a browser to steal sensitive data from online forms, such as those found on e-commerce sites, travel reservations sites, and other consumer-facing web properties. Data-skimming threats, led by Magecart, were a significant threat in 2018 and are continuing as a serious threat in 2019.

- Rogue browser extensions serving as malware have seen a major uptick. Many serve useful purposes, but they can also serve as "man-in-the-browser" attacks as two-factor authentication interceptors, keyloggers, screen scrapers, and data exfiltration tools. They are hard to detect because they're simple JavaScript and HTML rather than executable, part of a trusted browser application, are and execute entirely in memory. This makes them able to avoid detection by antivirus and sandboxing technologies.

- Primarily Russian Asus laptop users were victimized in early 2019 by cyber criminals who hijacked a legitimate software update tool to distribute malware that created a backdoor on infected computers. Approximately one million users were targeted and 57,000 users were infected[vii].

A common thread running through these varied threats is that the vast majority of them contain some type of domain and/or IP information that can form the basis for domain/DNS-based investigations.

- Some hackers will use local Windows tools to infect endpoints, such as PowerShell, Windows Scripting Host and the Windows Management Instrumentation command line if they can gain administrator privileges[viii].

- Cloud-to-cloud brute force attacks are becoming more common as a growing number of organizations move key applications to the cloud. These attacks assume that users commonly employ the same usernames and passwords across multiple accounts, allowing cyber criminals to focus on high-value accounts[ix].

THE CONSEQUENCES CAN BE ENORMOUS

The consequences of any of these attacks can be devastating. They include losing intellectual property, customer data, employee records, and login credentials, and they can grant bad actors access to corporate financial accounts, allowing them to drain these accounts in short order. Longer term consequences can be even more devastating, such as loss of corporate reputation, loss of long-term customers, an inability to gain new customers and, in some cases, companies going out of business. In an era of privacy regulations that fine organizations for significant breaches, such as the European Union's General Data Protection Regulation (GDPR), the consequences can ramp up very quickly.

Good Threat Intelligence is Essential

Generally, the first step in preventing the spread of cyber attacks and preventing future attacks is identifying that an incursion or data exfiltration has taken place. This identification can come from a variety of sources, such as examining log files and other data sources from firewalls, network monitoring tools, SIEMs, EDR tools, intrusion prevention systems, etc. Unfortunately, victims like employees and customers can also be a useful source of identification for threats when they complain that something has gone wrong and after significant damage has been done.

That approach is not adequate to deal with a growing variety of threats. For example, an attack launched from a domain that is only a few hours old will leave a significant proportion of conventional security defenses useless by being unable to detect the attack. Long dwell times mean that bad actors are free to roam around corporate networks for months before they're detected. Combined with security teams that are receiving too many alerts, working with inadequate budgets, and facing a severe cyber security skills shortage, the result is that for many organizations attacks are becoming increasingly effective.

Conventional approaches to security are normally not adequate to protect against more sophisticated threats.

In short, conventional approaches to security are normally not adequate to protect against more sophisticated threats. Security and forensics teams require better and more insight into bad actors so that they can gain a more thorough understanding of their identity, the way that they operate, and what they might do in the future. Security teams that have this information are better able to defend against existing techniques, and can then predict and prevent future attacks from the same bad actors.

THE GOAL IS TO UNDERSTAND BAD ACTORS AND THE SOURCE OF THREATS

Online activity results in a trail of data that includes domains and IP addresses. There are good sources of information that provide useful data on them, but relatively few organizations use this data as part of their security defenses. Many SIEMs, firewalls and other security tools often don't incorporate good threat intelligence on entities that are outside of the corporate network.

Conventional security approaches provide some level of protection, but they don't provide enough of a defense against highly sophisticated threats and bad actors that

create a threat quickly and then discard it. As a result, a key improvement in current security solutions must include:

- Understanding the identities of cyber criminals
- How they operate, and
- The detailed sources of the threats that organizations face

What good threat intelligence enables is a more extensive view into the threat landscape than conventional security defenses can provide so that threats can be predicted and dealt with in a proactive manner. It's a bit like the difference between a good burglar alarm that will detect every entry into a building versus having a detailed history of every person who approaches the building before they have a chance to enter.

But what if we could observe the burglar in action and anticipate his next move? In this analogy, think of threat intelligence as the ability to gather data on developing tactics that the burglar might use to break in or defeat the alarm system. That threat intelligence—understanding how the burglar is most likely going to try to break in—makes a critical difference. In security, we can use threat intelligence to implement mitigating controls and alerts to improve our security posture. This is particularly relevant to phishing. By using threat intelligence in a proactive defense approach, we can better ensure that all security programs, including security awareness, are relevant to the fast-evolving threat landscape.

THREAT INTELLIGENCE CAN PROVIDE A WEALTH OF INFORMATION

Threat intelligence plays a critical role in proactive threat hunting. One of the reasons attacker dwell time has reduced over the years is that organizations are getting better at proactively looking for signs of compromise and identifying it sooner. Actionable threat intelligence is an essential component of proactive threat intelligence, but it's not simply limited to known bad domains, IPs, binaries, etc. By understanding emerging threat actor tactics, this information can be used to look for patterns that could indicate compromise, even in the absence of connections to known bad infrastructure.

Good threat intelligence capabilities can provide a great deal of information about the domains and IP addresses that are attempting to gain access to a network. For example:

- Data about the behavior of domains and IP addresses that are somehow linked to threats can be used to develop a profile about individuals or entities that attempt to control the infrastructure or gain access to data. This information can be gathered from a variety of data sources that cross-index enormous volumes of information about domain registrants and those to whom IP addresses are assigned.

- This data can be augmented with additional information about the entities to which they connect in order to determine if they are somehow connecting with nefarious sources, allowing relationships between domains to be determined.

- DNS data can be monitored in near real-time to discover domains that have been newly registered and to defend against threats that can come in from these new domains. Because new domains are often used to launch attacks within just a few hours after their creation, a security team can create a policy that will, for example, block access from all domains that are less than 24 hours old, using threat intelligence to trigger a firewall, intrusion protection system or SIEM rule. This can serve as an effective means of blocking a significant proportion of threats that might come in through email and other sources.

What good threat intelligence enables is a more extensive view into the threat landscape than conventional security defenses can provide.

THE CHANGING ECONOMICS OF THREAT INTELLIGENCE

Threat intelligence should be used more, but it isn't. This is partly because of the perception that it's too expensive, that security teams just can't get the budget to use it, or because security teams perceive that it will simply add to their already overloaded volume of work.

That said, new threat intelligence tools enable attack attribution to be accomplished more quickly and in a more efficient manner than early-generation, manual capabilities. Using newer generation tools enables threat researchers to quickly and efficiently find data about threat sources, and to populate SIEMs, firewalls and other security solutions with additional threat intelligence capabilities.

THE ULTIMATE GOAL

There are five goals for security teams in using good threat intelligence:

1. To determine the risk of each domain so that a quick and accurate decision can be made about allowing, blocking or throttling traffic from them.

2. To enable a thorough understanding about threat actors' infrastructure that will impact an organization.

3. To gain this understanding quickly so that threats can be dealt with rapidly and as close to real time as possible.

4. To provide threat researchers, threat hunters and security defenses with the information they need to thwart future attacks.

5. To do all of this as inexpensively as possible.

There are a variety of challenges in managing threat intelligence.

The Current State of Threat Intelligence

Gartner defines threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.[x]"

HOW EXTENSIVELY IS THREAT INTELLIGENCE USED TODAY?

The research we conducted for this white paper, which was conducted among enterprise-level organizations, found that only slightly more than one in five use threat intelligence extensively and rely upon it as a critical element of their security operations, as shown in Figure 4; slightly more use threat intelligence and consider it to be important, but not critical. The majority, however, while perhaps considering threat intelligence to be useful, do not rely upon it.

Figure 4
Current and Planned Use of Threat Intelligence

	2019	2020
We use it extensively and rely upon it as a critical element of security operations	22%	28%
We use it and consider it to be important	25%	22%
We consider it as part of our wider security strategy	31%	30%
It is somewhat important, but not as critical as other elements of our security operations	15%	13%
Threat intelligence is a minor element of security operations	6%	6%
We don't use threat intelligence	2%	1%

Source: Osterman Research, Inc.

Our research also found that interest in the use of threat intelligence is growing modestly, although a significantly higher proportion of organizations will use it extensively and consider it a critical element of their security infrastructure over the next 12 months.

WHERE DO ORGANIZATIONS OBTAIN THREAT INTELLIGENCE?

We found that organizations are obtaining their threat intelligence from a variety of sources, including as part of a managed security service provider's service (70 percent of organizations), commercial feeds (62 percent), open-source feeds (59 percent), industry bodies (26 percent) and other sources (18 percent).

THE CHALLENGES IN MANAGING THREAT INTELLIGENCE

There are a variety of challenges in managing threat intelligence, but the leading challenges are digging through the threat intelligence feeds to attribute threats to their sources, the time hit that is required to use this data, budget issues, being able to act on the information in a timely manner, and keeping up with all of the threat intelligence information that comes in, as shown in Figure 5.

There are a variety of challenges in managing threat intelligence.

Figure 5
Challenges in Using Threat Intelligence
Percentage Responding "Very Challenging" or a "Major Challenge"

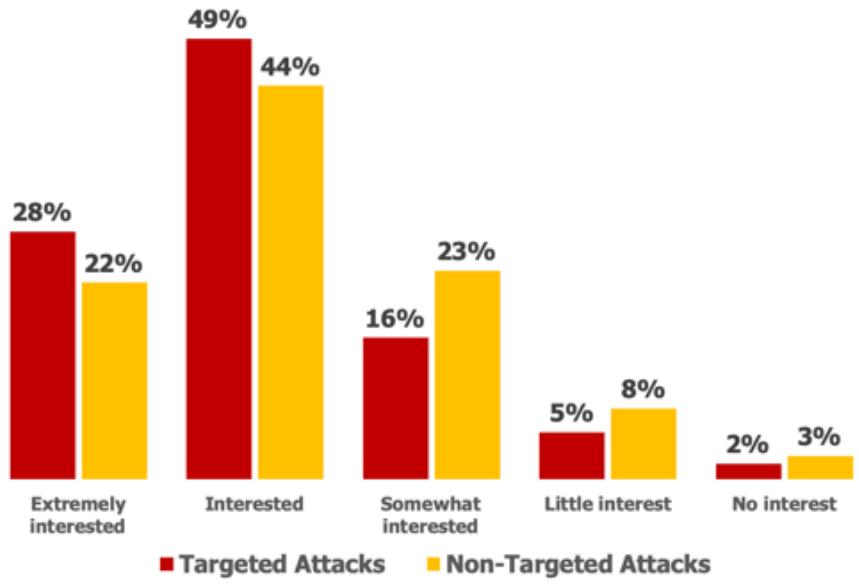
Source: Osterman Research, Inc.

What the data in the figure above tells us is that organizations really don't know how to use threat intelligence effectively, and they are not employing newer generation capabilities that will enable much more efficient use of their data feeds. For example, newer threat intelligence capabilities will enable data to be used efficiently without undue workload imposed on security staffers, yet the two leading challenges shown above are focused on the perceived additional workload imposed on security staffers.

THE IMPORTANCE OF THREAT ATTRIBUTION

One of the primary goals of using threat intelligence is using it to determine who is behind attacks. Our research found that the majority of decision makers are very interested in the practice of threat attribution, particularly for targeted attacks. As shown in Figure 6, we found that 77 percent are interested or extremely interested in threat attribution for targeted attacks, and 66 percent are this interested in threat attribution for non-targeted attacks.

Figure 6
Interest in Threat Attribution for Targeted and Non-Targeted Attacks



Source: Osterman Research, Inc.

Threat attribution is an essential application of threat intelligence.

Threat attribution is an essential application of threat intelligence. As noted by John Scimone, Chief Security Officer for Dell, without threat attribution and accountability, there is simply no disincentive for cyber crime given the very high reward-to-risk ratio for most cyber crime.

Our research found that 77 percent of organizations believe that understanding the source of threats allows them to focus on the threats that matter most to them. The fact that decision makers and influencers are more interested in threat attribution for targeted than non-targeted attacks supports this idea. We also found that 80 percent of decision makers and influencers agree or strongly agree with the idea that threat attribution enables them to prepare for and respond to threats more effectively. Moreover, and not surprisingly, IT security management (e.g., CISOs and heads of security) express the greatest interest in threat attribution, followed by IT management and non-managers in the security department (e.g., security analysts).

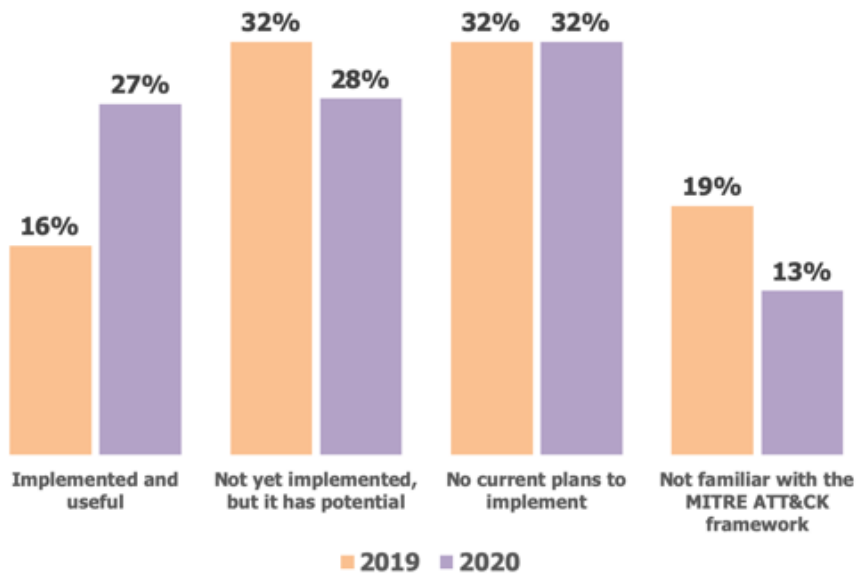
THE IMPORTANCE OF THE MITRE ATT&CK FRAMEWORK

According to MITRE, the MITRE ATT&CK™ framework is "a globally-accessible knowledge base of adversary tactics and techniques based on real-world

observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.[xi]" Threat intelligence is used in the context of the MITRE ATT&CK framework to help threat hunters understand the techniques that have been used by threat actors as part of their tactics in attempting to achieve various objectives, such as initial access to a network or gaining access to user credentials.

Our research found that there is increasing interest in using the MITRE ATT&CK framework to catalogue and track threats. As shown in Figure 7, 48 percent of decision makers and influencers consider that it has potential or it's already implemented and useful for them; over the next 12 months, that figure is set to increase to 55 percent.

Figure 7
Perceived Utility of the MITRE ATT&CK Framework, 2019 and 2020



Source: Osterman Research, Inc.

Threat researchers need to understand current threats so that they can defend against the complex and connected infrastructure employed by bad actors.

Some Best Practices to Consider

Osterman Research recommends a number of best practices to consider in the context of applying threat intelligence:

- **Understand current threats**
  Threat researchers need to understand current threats so that they can defend against the complex and connected infrastructure employed by bad actors. Being able to search across integrated databases of domain information is key in understanding the network of domains in use by threat actors, enabling spam filters, firewalls, intrusion protection systems, SIEMs and other solutions to proactively guard against these threats.

- **Understand past threats**
  Understanding past threats that have already breached network defenses and created a data breach is essential. Threat researchers that are armed with data about the extended threat infrastructure can review log and other data to understand the dwell time of a breach. Threat intelligence data can also assist

threat researchers in conducting thorough forensic analysis of data breaches, infiltrations and various other types of anomalous network behavior.

- **Understand future threats**
  Once a good threat intelligence infrastructure has been created, suspicious or malicious registrations of new domains can alert threat researchers to assist in preventing future attacks. Because the past activities of bad actors can enable researchers to accurately guess their future actions, a thorough understanding of previous actions can help to predict future ones.

- **Understand the importance of good security awareness training**
  Users should be trained properly to act as a key line of defense against various types of threats. For example, even if a phishing email with a link to a malicious domain makes its way through the gauntlet of security defenses an organization may have established, a savvy and well-trained user will be much less likely to click on the link and enable a threat to take hold in the network. Security awareness training should focus not only on threats that can come from communication and collaboration tools, but also good password management, understanding the importance of regular software updates, the dangers associated with oversharing on social media and elsewhere, the need to comply with privacy regulations, etc.

- **Deploy the right security tools**
  A key element of any security infrastructure is deployment of the right security systems and solutions to protect against various types of threats. Depending on the organization, these will include EDR solutions, various other endpoint solutions, unified threat management systems, firewalls, intrusion prevention systems, etc. It's essential that these solutions can integrate nicely with threat intelligence capabilities so that regularly updated information can be fed into these systems in order to make them as effective as possible.

- **Use good sources of threat intelligence**
  Good sources of threat intelligence should be used to provide threat researchers with robust real-time/current and historical data. This information can be used to provide better defensive capabilities against bad actors who are using domains with a poor reputation and that are likelier candidates for malicious behavior. Similarly, good threat intelligence can enable proactive investigation of threat sources and discover previously unknown sources of malicious content or behavior.

  The benefits of using threat intelligence as a component of a security infrastructure are several:

  - It reduces the likelihood of a data breach and so increases the likelihood of compliance with the growing number of privacy obligations like the GDPR and the California Consumer Privacy Act.

  - It enables threat researchers to determine how attacks started and the methods that bad actors used to exploit weaknesses in corporate defenses. This information can be invaluable in preventing future attacks.

  - It reduces the likelihood that Internet properties and brands can be misused through more careful monitoring of how corporate brands are used.

  - It helps to identify how digital corporate assets are used and can help researchers to identify if they are being misused.

Good sources of threat intelligence should be used to provide threat researchers with robust real-time/ current and historical data.

Summary

Because threat actors are employing ever-increasing sophistication in their tools, techniques and procedures, security professionals are finding it difficult to defend against a growing array of threats from organized criminal operations, state-sponsored actors, and others. By gathering threat data from internal and external sources and turning it into actionable threat intelligence, security analysts can more effectively combat cyber threats by developing a better understanding of attackers, creating better risk assessments, and conducting better informed and more effective investigations.

Sponsor of This White Paper

Spamhaus is the trusted authority on threat intelligence, uniquely placed in the industry because of our strong ethics, impartiality and quality of actionable data. This data not only protects, but also provides insight across networks and email worldwide. Our datasets are used by leading global technology companies, enterprise business, internet service providers and hosting companies, among others.

Our IP and domain datasets, which are currently protecting over 3 billion mailboxes globally, are easily integrated into your current infrastructure, at both the email and DNS level. This makes them a cost effective, set and forget solution, allowing you to focus resources elsewhere.

For threat hunting and incident management our passive DNS data and enhanced datasets allow your security teams to speed up and simplify security investigations.

With over 2 decades of experience we are the industry leaders in threat intelligence data to protect and inform.

www.spamhaustech.com

@SpamhausTech

REFERENCES

[i] Source: *New Methods for Solving Phishing, Business Email Compromise, Account Takeovers and Other Security Threats*, Osterman Research, Inc.

[ii] https://www.recordedfuture.com/strategic-threat-intelligence/

[iii] https://content.fireeye.com/m-trends/rpt-m-trends-2019

[iv] https://biztechmagazine.com/article/2019/03/rsa-2019-cybercriminals-overlooked-tactics-and-favorite-industries-target

[v] https://secureteam.co.uk/news/credential-stuffing-on-the-rise/

[vi] https://www.sonicwall.com/news/sonicwall-detects-reports-dramatic-rise-in-fraudulent-pdf-files-in-q1-2019/

[vii] https://www.consumerreports.org/hacking/shadowhammer-hackers-attack-asus-computers-through-routine-software-update/

[viii] https://www.tsg.com/blog/security/3-top-cybercriminal-tactics-you-need-know-2019-and-how-prevent-them

[ix] https://www.navisite.com/blog/beware-five-innovative-cyberattacks-office-365

[x] https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

[xi] https://attack.mitre.org