KnowBe4
Human error. Conquered.

WHITEPAPER

Using Threat Intelligence to Build Data-Driven Defense

by Javvad Malik

Table of Contents

Intelligence. That's what we need. The unfortunate reality of most enterprises is that those tasked with their defense fail to fully comprehend threats and risks as well as they ought to.

INTRODUCTION

In 2018, Gartner estimated the global market for information security products and services would reach an incredible US$114 billion. Enterprise customers account for much of that spending. Businesses of all shapes and sizes spend millions each year on trying to keep their networks, their intellectual property, and their customers safe.

There's nothing inherently wrong with that. Every day, security engineers face challenges that force them to rely on third-party tools and appliances, or even consult with external teams. That said, it's always healthy to examine if businesses are spending their security budgets wisely, or instead blowing millions on white-elephant technologies that offer scant protection.

The overwhelming majority of security decision makers act with the best of intentions. However, it's entirely plausible that they may be disproportionately pending their limited budget on countering one type of external threat, while remaining oblivious to the fact that they're vulnerable to several other avenues of ingress that they hadn't previously thought of.

So, how does one counter that decision blindness? I'll tell you this; salvation won't be found wandering the halls of your local infosec trade show. It's a sad indictment of our industry that style often trumps substance, and marketing hype is often treated as a substitute for sober contemplation of security threats based on real-world conditions and intelligence.

Intelligence. That's what we need. The unfortunate reality of most enterprises is that those tasked with their defense fail to fully comprehend threats and risks as well as they ought to. And the few resources they have are often employed against the wrong threats and aren't sufficiently monitored to ensure they're producing the right results.

I don't write that as a pejorative. Like I said, most security decision makers act with the best of intentions, and care deeply about their responsibilities. Rather, I want to underline the complex nature of contemporary enterprise IT infrastructures, paired with the confusing and often sensationalist nature of how information security products and services are marketed.

Compounding the situation further is the unfortunate reality that they often fail to ask the right questions. To their employees. To their vendors. To their third-party consultants.

As enterprises grow, clear and frank communication becomes harder, and it becomes more cumbersome to leverage internal data to drive prudent decision making.

I've mentioned the symptoms of the disease, but what about the causes? It's tricky to generalize here, as all enterprises are inherently different. However, in my decades-long experience within the security sector, I've noticed the following trends:

- Security teams are dealing with an ever-increasing number of threats. Each year, the information security community identifies roughly 12,000 new threats, each impacting different applications, and with their own unique characteristics when it comes to exploitation and remediation. How do teams, often chronically understaffed and underequipped, manage to cope with that?

- I fear some readers may find this point controversial, but I believe that we've lost perspective of what constitutes a top-priority risk. Far too many organizations outsource their thinking on risk to the CVSS system and choose to prioritize remediation on those vulnerabilities with the most critical of scores. This often ignores real-world conditions and asset infrastructures, resulting in less severe, but arguably more exploitable vulnerabilities being ignored.
- There's far too much competition for resources. I touched on this with my first point, when I mentioned the proliferation of identified threats; but that's just a small part of the picture. One issue is that teams focus too much on compliance, which sets a bare-minimum security standard. Compliance is often time-consuming and bureaucratic, and results in overwhelmed teams failing to address more pressing issues.
- And then there's the fact that many enterprises work at a glacial rate. You can attribute this to slow budget cycles, which force decision makers to wait in order to acquire vital new equipment and manpower. You can also blame it on the fact that trench-level teams are often overwhelmed, working on multiple projects simultaneously. On top of that, there's internal politics, which is often the death knell for any prudent security policy.

Let's put data in the driving seat

One of the most enduring security buzz phrases of the past decade has been "data driven." Tools like SIEMs and data analytics platforms allow teams to gather vast oceans of data about how their systems work, and crucially, how external actors interact with them.

As with any buzzword, there's some hype; but there's also some substance. My friend and colleague Roger Grimes introduced me to the concept of "data-driven defense." This concept is a paradigm-shift compared to how many organizations currently use data in their information security decision making.

Here's how most enterprises use data: they see threats appear in their preferred alerting tool of choice, and almost unconsciously, they apply the first band-aid they see. This works, but it also doesn't; as it means that all threats are treated equally, and are remediated regardless of the level of risk they present to the business.

This can be visually depicted in figure 1 below.

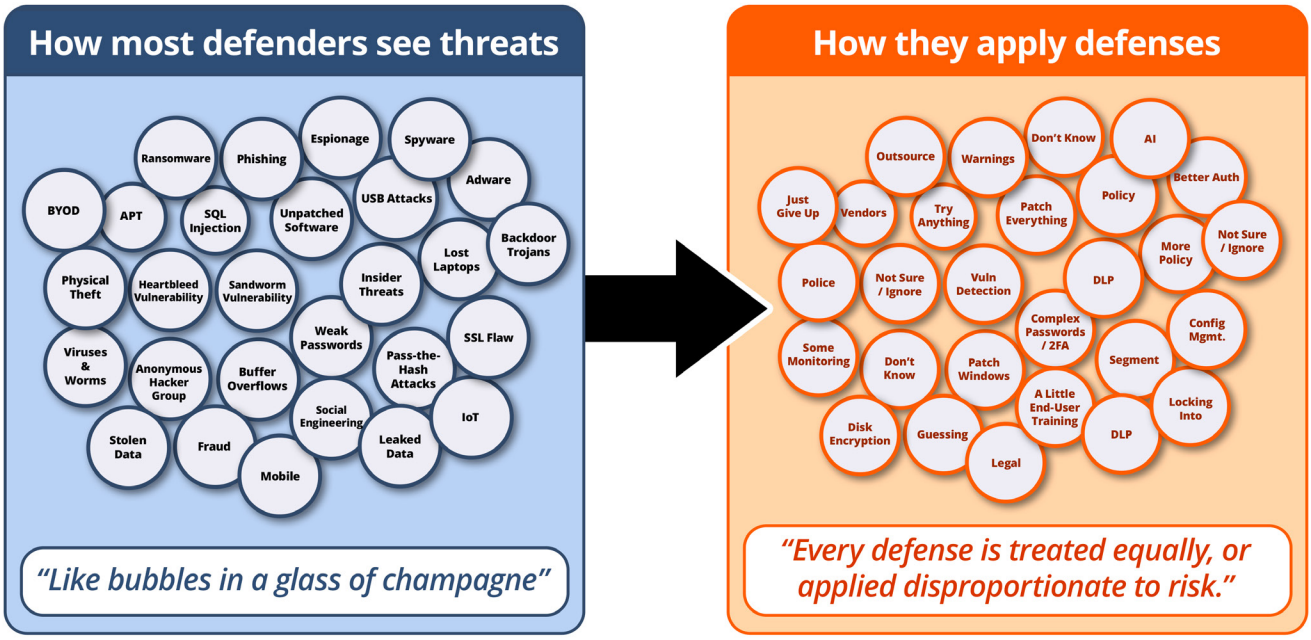


Figure 1 Source: R. Grimes, Data-Driven Defense

That allows some level of security, but it's also an extremely inefficient way of doing security. Paraphrasing George Orwell's Animal Farm: "All threats are equal, but some threats are more equal than others."

Yes, it's prudent to want to reduce one's exposure to external security threats. But it's arguably more sensible to focus one's efforts in discerning what the biggest issues are to your business; and invest the largest proportion of security controls and spending into that area.

If you're a military leader, why would you invest your resources into anti-aircraft cannons when your adversaries are coming from the sea? It's the same principle.

Data-driven defense forces you to completely adjust your thinking. Firstly, it requires you re-examine your entire model of threat perception, focusing on root causes, rather than individual security episodes. Root causes are determined by three main factors: data, relevance, and the individual experience of those working within the organization, who possess the relevant security knowledge required to make critical judgements.

This is depicted in figure 2 below.

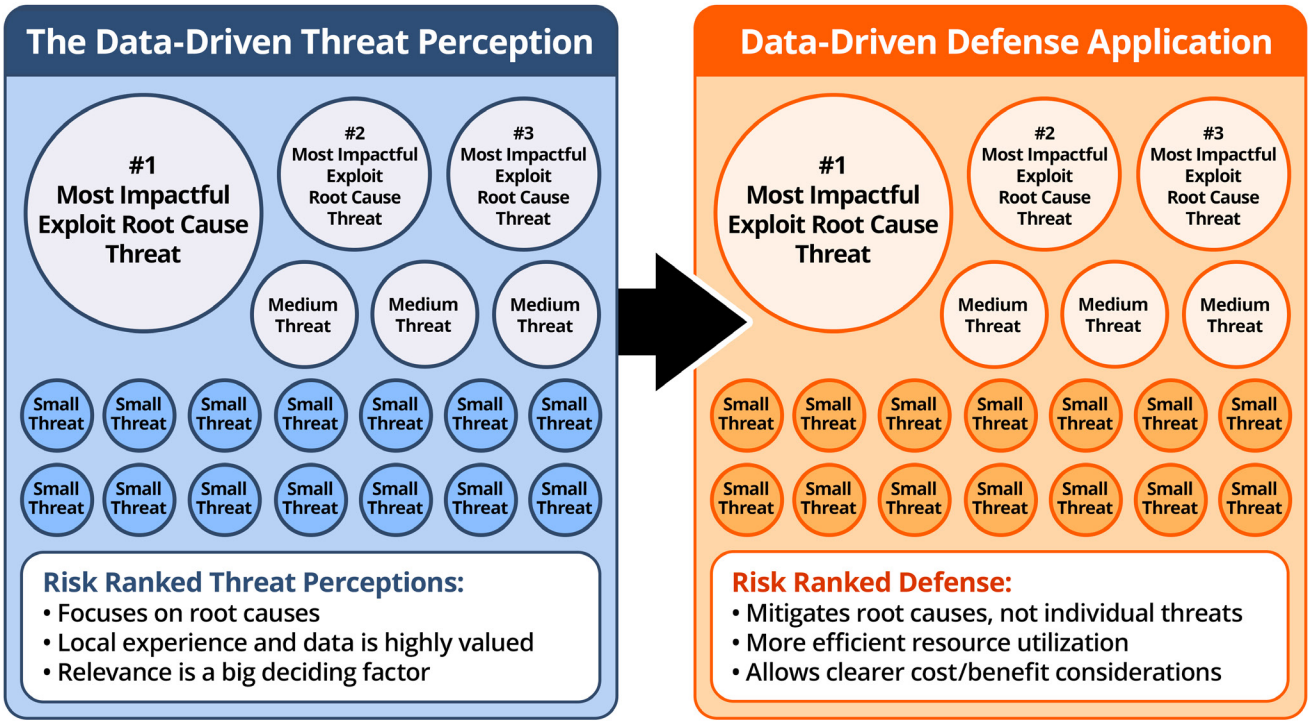


Figure 2 Source: R. Grimes Data-driven Defense

Once an organization has determined the pressing root causes requiring remediation, teams will then prioritize resources to counter them. This is inherently more efficient than patching every CVSS that crosses one's desk. It also makes it easier to weigh the costs and benefits of each security-related decision, making scarce resources go further.

UNDERSTANDING THREAT INTELLIGENCE REPORTS

Threat intelligence reports are an excellent (and often woefully undervalued) way for businesses to understand risks, newly discovered vulnerabilities, and bad actors. They're based on empirical research by dedicated security teams who spend their days poring through the seedy underbelly of the internet, trawling through hacker Twitter feeds and dark web forums.

And, for any security decision maker wishing to pivot towards a data-driven approach, they're an essential tool in one's utility belt.

There is no standard way to write or publish a threat intelligence report. Many vendors will share threat intelligence in their own manner. Usually there is a description of what the objective of the attacker is, the typical target, and in some cases, attempt to attribute who the attacker is. Other than that, there is usually a list of things companies should look out for such as hashes, domains, suspicious IPs and so forth, collectively referred to as indicators of compromise or IoCs.

IoCs are usually ingested by enterprise platforms like SIEMs and used by security teams to search for threats within their network. However, for the purposes of this study, I didn't delve into the IoCs; rather, I spent my time trying to understand how attackers find their way into organizations.

To compile a list of recent threat intelligence reports in an unbiased manner, I visited Open Threat Exchange (otx.alienvault.com), and looked at the 100 most recent reports from AlienVault. These are recent reports curated and shared by the Alien Labs team. I believed this was a good approach to remove any author bias.

For the sake of clarity, I'd like to add a quick caveat: in gathering these reports, I performed some editorial curation where I discarded those which I deemed lacked enough information or depth. These were relatively few and far between, however.

The 100 reports gathered contained threat intelligence information from 43 different vendors and sources. Many of these came from what would reasonably be considered household names in the security industry, including Kaspersky, Securelist, ESET, McAfee, and Trend Micro.

Figure 3 to the right has a complete list of all the vendors and the number of reports. For a complete list of every report, please refer to Appendix A.

Source	#
AhnLab	2
AliBaba	1
AlienVault	1
Alyac	7
Anomali	2
Binary Defense	1
Bromium	1
Checkpoint	5
Cisco Talos	4
Crowdstrike	1
Cybereason	3
Cylance Threat Vector	2
Dragos	1
Esentire	1
ESET WeLiveSecurity	7
FireEye	2
Fortinet	2
G Data Software	1
Intezer	1
Kaspersky Securelist	4
Lookout	1
Malwarebytes	1
McAfee	2
Netlab	1
NTT Security	1
Objective-See	1
Palo Alto Unit 42	2
Proofpoint	3
PT Security	1
Recorded Future	1
RiskIQ	2
Secureworks	1
Snyk	1
Sophos	2
Sucuri	1
Symantec	4
Tencent	1
Threatrecon	2
Trend Micro	7
Twitter	11
Wexin	1
Yoroi	2
ZDNet	2
Grand Total	**100**

Figure 3: Source of threat intelligence reports analyzed

Interestingly, the source with the largest representation is Twitter. That's hardly surprising, given the anonymity it offers, and the fact that it's the unofficial "water cooler" for the security community, both legit and otherwise. It's also an easy place to put initial findings and thoughts prior to a full report being written up.

Initial Access

Could these 100 reports offer an insight into the most common avenue of ingress used by threat actors? That was my main area of interest. After all, if we can identify this, we can focus our resources on closing that particular door – or even just guard it more intently.

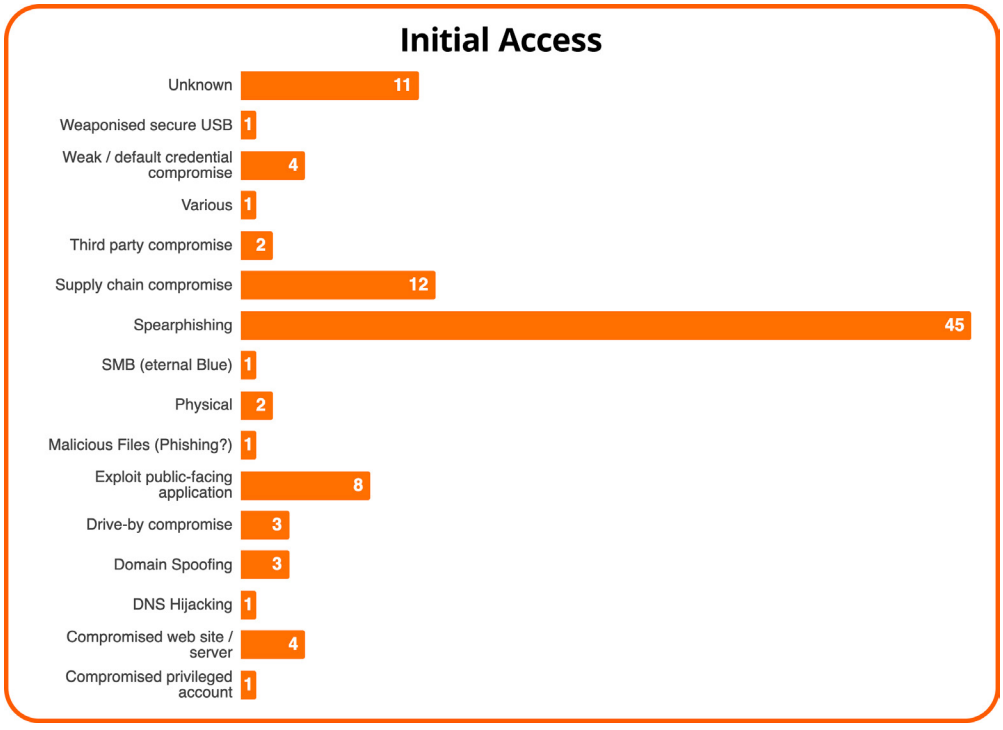
Again, here I had to do some manual editorial curation of my own. I attempted to categorize attempts as closely as I could to the MITRE ATT&CK terminology, which is a standard that's gaining widespread adoption by security researchers. For now, it's as close as security researchers will get to a style guide. However, there were times when I had to use my own professional judgement.

For instance, the ATT&CK terminology has three different spearphishing categories, all depending on the actual methodology of exploitation. Link-based, attachment-based, and spearphishing as a service are all treated as distinct entities.

However, for the sake of clarity and simplicity, I decided to aggregate them all into one monolithic category—phishing.

I also went the other way, grouping disparate attacks into a single bucket. For example, the ATT&CK terminology uses "supply chain compromises", which I used for several different methodologies, such as when a malicious actor inserts a compromised link into the description of a video, or when they manage to upload a compromised video onto a third-party app store. For a more detailed breakdown with some notes, please refer to the table in Appendix A. If you visit the reports, maybe you can come up with a different classification for the initial access.

As you'll see in the below table, an overwhelming plurality of threats, 45 out of 100, focus on exploiting "wetware." These threats include phishing, spearphishing, and social engineering.



It's worth bearing in mind that this isn't the only category which has social engineering techniques at its core. For example, domain spoofing attacks also rely on tricking a user into visiting a site which appears to be a legitimate domain.

That's not to say that all the attacks rely on user error. Exploiting public-facing applications, DNS hijacking, and compromising websites / apps collectively amounted to 13 reports. Not an insignificant number from this sample size, but still far behind phishing. One could include drive-by downloads into this category, as those attacks usually take advantage of unpatched software.

Supply chain compromise is the third biggest category, with 12 of the reports falling into that category. Any attack which used a trusted source as a mechanism to distribute malware can fall into this category. For example, in the Checkpoint report Operation Tripoli, which targets individuals in Libya by creating a fake Facebook page and luring victims into clicking links and downloading files that are supposed to inform about the latest airstrike in the country, or the capturing of terrorists, but instead contain malware.

Similarly, there are a couple of instances of malicious mobile apps that infect phones, which is an example of supply chain compromise. ESET and Lookout covered these in reports on android malware and Monokle, respectively, that rely on users downloading the malicious apps.

One could also argue that using weak or default credentials (as well as reusing credentials) is a user's responsibility. Although, when these attacks are against IoT devices, there is sometimes no easy option for users to change the default credentials.

It's also interesting to look at third-party compromise. The use of a third party isn't necessarily the primary avenue – the primary attack vector was what compromised the third party. Although for the victim, it would appear to be the primary attack. Which is where we can go around in circles for a while trying to establish what exactly constitutes the primary infection source.

What does that mean? Well, if you can divert your security efforts into policing your external sources of communication, like email, SMS, instant messenger, social media, and train your users to be wary of social-based attacks, you are more likely to prevent almost half of all attacks from organized criminal groups and nation states.

I'll end this section with a question: Based on these 100 threat intelligence reports, are you focusing half of your security resources on protecting against social-based attacks? If not, why?

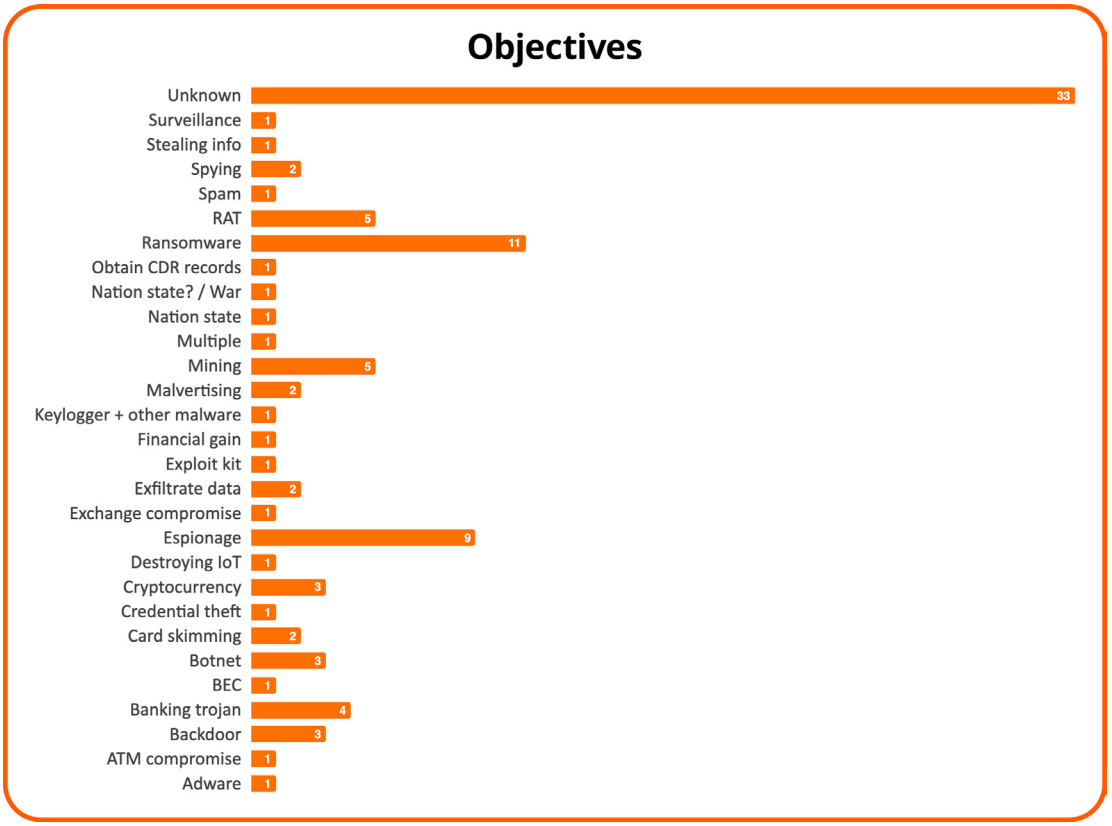
Why Hackers Hack

Of course, if we focus solely on methodology, we end up ignoring one major component of threat-intelligence: the objective of an adversary.

This is typically hard for security teams to discern. And, for what it's worth, it's often not a pressing concern. If you've been hacked, you're probably more concerned with the technological and regulatory aftermath, rather than discerning the motivation behind the hack.

Fortunately, some threat intelligence reports can shine a valuable light on this. While it was unclear as to what the true objective of the attacker was for 33 reports, I did learn from the remaining reports that money is a major motivator for cyber criminals. Having said that, much like the initial access vectors, there is no standard terminology in place, so I took what I could from the individual reports and listed them out and combined them where possible. However, there are still some areas of ambiguity and overlap, which is worth bearing in mind when looking at this table.

For 11 percent of the attacks examined, the distribution of ransomware is the main priority.



Ransomware is an enduring threat for businesses, governments, and individual users. The total global cost of ransomware (which include remediation, lost productivity, and in some cases, paying the ransom) is difficult to measure. However, Lloyds of London estimates that a potential worst-case scenario ransomware epidemic could cost as much as $200 billion, with retail and healthcare among the two most affected sectors, followed by manufacturing.

The third most common objective for attackers is the distribution of cryptocurrency mining software using a tactic known as “cryptojacking.” This represented five percent of all threats. Cryptojacking can take many forms, from relatively benign in-browser elements, to more sophisticated mining programs that exploit weaknesses in serverless application hosting platforms.

In any form, cryptojacking is something to be wary of. Even the most benign strains found on a user’s laptop can result in slower performance (and therefore lower productivity), as well as increased power consumption. In some cases, cryptojacking malware can exploit weaknesses in a company’s cloud computing infrastructure to activate new VM or serverless instances. This could potentially result in huge bills for the victims, as most cloud computing providers charge based on usage.

Espionage, at nine percent, was the second highest objective. As anyone in our industry knows, digital attacks can allow a state or organized crime actor to obtain confidential trade secrets, R&D information, or financial documents.

This information isn’t necessarily as useful as knowing the most common avenues of ingress. However, understanding the motivations behind cyber criminals can go a long way towards building an informed, evidence-driven protective strategy.

Reading between the lines, there is a clear distinction between the objectives of cyber criminals and nation-state actors. With criminals going after money, while nation states more interested in espionage, spying, or disrupting operations.

It's not entirely surprising to see more activity from cyber criminals. This is probably due to an increase in active criminals compared to state actors, and the fact that state actors are better at covering their activity.

While it's easy to group the attackers into two broad classes of nation states and cyber criminals, there are others such as competitors, insiders, hacktivists, curious skiddies (script kiddies), and so forth. Understanding adversaries can be useful for some organizations, but as Adam Shostack warns in his book *Thread Modeling: Designing for Security*, focusing on attackers may not be as useful as one may anticipate. Attacker lists don't often contain enough information to allow people to figure out what an attacker will actually do. Which is why it's probably better to focus on what actual techniques are used and defend against those.

For most organizations, with money clearly so high on the agenda, denying an adversary the opportunity to profit from your misfortune can go some way towards making your business a less attractive target.

The Root Cause

As we've mentioned, far too many defensive security strategies focus on two main areas: remediation and damage control. While these elements are important, it's clear that far too many people are ignoring the elephant in the room: the root causes of their vulnerabilities.

It's somewhat a defeatist mentality to believe that attacks will eventually get through, so there's little value in trying to prevent them. Rather, one should take steps to prevent the attacks as much as possible, and then have capabilities to detect where an attack is successful as quickly as possible and remediate. Resources such as threat intelligence, which is quite widely available, freely, as part of products, or as separate feeds, can help reduce the gap from an external knowledge perspective —but it still requires organizations to internally examine where their threats are coming from.

Of course, each organization has its own security Achilles heel. In my view, the best way to identify this is with frank conversation and thoughtful analysis. A good exercise is to ask the following questions:

- Can your team identify any specific weaknesses in your organization? These can be technological, procedural, or cultural. If they could allow an attacker ingress into your infrastructure, they matter.
- Is this answer consistent across all stakeholders? If so, it's worth prioritizing.

For most organizations, with money clearly so high on the agenda, denying an adversary the opportunity to profit from your misfortune can go some way towards making your business a less attractive target.

- Does the data you've gathered internally, as well as sourced externally (i.e., a threat intelligence report), back this up?

If we look at the data gathered from the aforementioned 100 threat intelligence reports, it's clear that social-based threats pose the greatest risk. Therefore, it'd be prudent to focus on organization-wide training to mitigate against them, complimented with a range of technical controls that would limit the scope for a social engineering-based attack.

However, it's worth noting that the sands of security are frequently shifting. Nothing is set in stone, and it's worth constantly checking and re-checking to identify new potential areas for improvement. You should always complement external data with your own internal findings, in order to identify the main threats that pose the greatest level of risk.

CONCLUSION

Data is the lifeblood of most security teams, although it's often critically undervalued. Data—broad, empirical data—is the only real way to identify the root cause of insecurity within an organization. Ignore it at your own peril.

And don't be afraid to broaden the sources of data that you use. As we discussed, external threat intelligence reports can identify contemporary trends, such as that social engineering remains a common avenue of attack for adversaries.

Technical elements, like ransomware and cryptojacking, aren't the problem. They're a symptom of a broader concern – namely, how they got into your organization in the first place. This should always be your primary concern.

Furthermore, you should always aim to create your own threat-intelligence reports. While external sources are often invaluable, don't discount the data gathered by your own intrusion detection and prevention systems. You could argue that this is more useful, as it's relevant to your own organization.

Context, as always, is king.

APPENDIX A - THE 100 REPORTS

Title	Source	Primary target	Objectives	Initial Access	Notes
GermanWiper ransomware hits Germany hard, destroys files, asks for ransom	ZDNet	Germany	Ransomware	Spearphishing	
Baldr vs The World	Sophos	Gamers	Credential theft	Supply Chain Compromise	Links in youtube videos
Double Dragon: A dual espionage and cyber crime operation	FireEye	Video Game Industry	Ransomware	third party compromise	
Sodinokibi: The Crown Prince of Ransomware	Cybereason	Asia	Ransomware	Spearphishing	
Sharpening the Machete	ESET We live security	Venezuela Govt	Espionage	Spearphishing	
Rocke in the Netflow	Palo Alto Unit 42	Cryptocurrency	Mining	Spearphishing	
Zegost from Within – New Campaign Targeting Internal Interests	Fortinet		Exfiltrate data	Spearphishing	
Clop Ransomware	McAfee		Ransomware	Spearphishing	
YTY Framework in New Targeted Campaign Against Pakistan Government	Threatrecon	Pakistan Govt		Spearphishing	
LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards	Proofpoint	utilities	Nation state	Spearphishing	
Hexane Targeting Oil and Gas	Dragos	Oil and gas	Espionage	third party compromise	
Suspected muddywaters phishing	Twitter	Uzbekistan		Spearphishing	
FormJacking	Symantec	Websites	Stealing info	Compromised web site / server	
Malvertising: Online advertising's darker side	Cisco Talos		Malvertising	Drive-by compromise	
Java ATM Malware: The Insider Threat Phantom	Yoroi	Finance	ATM Compromise	Physical	
Android ransomware is back	ESET We live security	Mobile	Ransomware	Supply Chain Compromise	Malicious app
Fake Google Domains Used in Evasive Magento Skimmer	Sucuri	Finance	Card Skimming	Domain Spoofing	
Dridex's Bag of Tricks: An Analysis of its Masquerading and Code Injection Techniques	Bromium	Finance	Banking trojan	Spearphishing	
EXPLOIT KITS "SHADE" INTO NEW TERRITORY	Cybereason	Japan	Ransomware	Drive-by compromise	
Gamaredon uses Strait of Hormuz Themed Phishing Document	Twitter	Ukraine		Spearphishing	
AmmyRat campaign targeting Korea	AhnLab	Korea, Republic of		Spearphishing	
TA505 impersonates Airlines	Alyac		RAT	Spearphishing	
Phishing Targeting Protonmail users	RiskIQ	Bellingcat researchers		Spearphishing	

Title	Source	Primary target	Objectives	Initial Access	Notes
The Growth of SectorF01 Group's Cyber Espionage Activities	ThreatRecon	Southeast Asia (Govt, edu, research, various)	Espionage	Spearphishing	
Dragonfly Targets ICS Systems Using Man on the Side Attacks	Secureworks	Energy	Nation state? / War	Spearphishing	
Chinese APT "Operation LagTime IT" Targets Government Information Technology Agencies in Eastern Asia	Proofpoint	Government		Spearphishing	
Monokle	Lookout	Targeted	Surveillance	Supply Chain Compromise	Malicious app
P2P Worm Spreads Crypto-Miners in the Wild	Yoroi	Cryptocurrency	mining	Supply Chain Compromise	Torrents
Multistage Attack Delivers BillGates/ Setag Backdoor	Trend micro		Botnet	Exploit public-facing application	
WatchBog Mining Malware Exploiting Jira Servers	AliBaba	Cryptocurrency	mining	Exploit public-facing application	
URL Spreading Shellbot and XMRig Using 17-year old XHide	Trend micro	Cryptocurrency	Mining	Weak / default credential compromise	
Targeted ransomware: GoGaLocker and MegaCortex	Symantec		Ransomware	Spearphishing	
TrickBot campaign using .docm files via malspam	Checkpoint		Banking trojan	Spearphishing	
Rubella and Dryad Office Macro Builder	McAfee			Spearphishing	
Unofficial Telegram App Secretly Loads Infinite Malicious Sites	Symantec	Mobile		Supply Chain Compromise	Unofficial app
Hard Pass: Declining APT34's Invite to Join Their Professional Network	FireEye	Government, energy utilities, oil and gas		Spearphishing	
Spam Campaign Targets Colombian Entities	Trend micro	Colombia	BEC	Spearphishing	
Okrum: Ke3chang group targets diplomatic missions	ESET We live security	Government	Exfiltrate data	Domain Spoofing	
EvilGnome Rare Malware Spying on Linux Desktop Users	Intezer		Spying	Supply Chain Compromise	
Targeted trickbot activity drops 'powerbrace' backdoor	NTT Security	Finance	Backdoor	Spearphishing	
SLUB Gets Rid of GitHub, Intensifies Slack use	Trend micro		Backdoor	Drive-by compromise	
Continuing Lazarus Attacks	Twitter				
Fancy Bear Phishing	Twitter	NGO		Spearphishing	
Server-side polymorphism and PowerShell backdoors	Gdata software		Backdoor	Spearphishing	
Konni Campaign Targetting Mobiles	Twitter	Korea, Republic of			
Continued targetting of the Financial Sector by Lazarus	Alyac	Finance		Spearphishing	
Turla renews its arsenal with Topinambour	Kaspersky Securelist	Government	RAT	Supply Chain Compromise	
Lazarus Mobile Malware	Twitter	Finance			
Meet DoppelPaymer Ransomware and Dridex 2.0	Crowdstrike		Ransomware	Compromised privileged account	
Oto Gonderici Excel formula injections target Turkish victims	sophos			Spearphishing	
Buhtrap group uses zero-day in latest espionage campaigns	ESET We live security	Government	Espionage		
Newly Identified StrongPity Operations	AlienVault	Turkey			
New Miori Variant Uses Unique Protocol to Communicate with C2	Trend micro		Botnet	Weak / default credential compromise	Scan and execute script on hosts

Title	Source	Primary target	Objectives	Initial Access	Notes
Android Adware	Checkpoint		adware	Supply Chain Compromise	
The eCh0raix Ransomware	Anomali		Ransomware	Weak / default credential compromise	
New FinSpy iOS and Android implants revealed ITW	Kaspersky Securelist		Spying		
Windows zero-day CVE-2019-1132 exploited in targeted attacks	ESET We live security			Physical	Need to log onto system
The 2019 Resurgence of Smokeloader	Checkpoint				
Sea Turtle keeps on swimming, finds new victims, DNS hijacking techniques	Cisco Talos	Government		DNS Hijacking	
Continued DPRK targeting of Cryptocurrency Traders	Twitter	Korea, Republic of			
Anubis Android Malware Returns with Over 17,000 Samples	Trend Micro	Finance	Banking trojan		
Ruby gem strong_password Backdoored	Snyk			Supply Chain Compromise	
Malicious campaign targets South Korean users with backdoor-laced torrents	ESET We live security	Korea, Republic of	Botnet	Supply Chain Compromise	Torrents
How we uncovered an attack on government entities in Europe	PT Security	Government	Espionage	Spearphishing	
TA505 using new malware Gelup and Flowerpipi	Trend Micro	Japan, Philippines, Argentina	Spam	Spearphishing	
Multiple Chinese Threat Groups Exploiting CVE-2018-0798 Equation Editor Vulnerability Since Late 2018	Anomali			Exploit public-facing application	
TA505 begins summer campaigns with a new pet malware downloader, AndroMut	Proofpoint		RAT	Spearphishing	
Sodin ransomware exploits Windows vulnerability and processor architecture	Kaspersky Securelist	MSP	Ransomware	Exploit public-facing application	
Hangul Vulnerability Exploited by Attackers	Twitter	Government		Malicious files (phishing?)	
MuddyWater attacks organization in Tajikistan	Wexin	Government		Spearphishing	
USCYBERCOM Malware Alert July 2019	Kaspersky Securelist	Saudi Arabia		Spearphishing	
Malspam campaign E-Invoice dropping Danabot	Twitter	Poland	Banking trojan	Spearphishing	
Continued Lazarus APT attack on cryptographic traders	Alyac	Korea, Republic of	cryptocurrency	Spearphishing	
Venus 121 APT Sends Spearphishing Documents	Alyac	Government		Spearphishing	
Gorgon Group Malware	Twitter			Spearphishing	
Spoofed Microsoft domains - June 2019	Twitter			Domain spoofing	
The Gopher in the Room: Analysis of GoLang Malware in the Wild	Palo Alto Unit 42	Various	Multiple	Various	
Ratsnif - New Network Vermin from OceanLotus	Cylance Threat Vector		Espionage		
RATs and stealers rush through Heaven's Gate with new loader	Cisco Talos		Keylogger + other malware	Spearphishing	
Skimmer For All	Fortinet	Finance	Card skimming	Compromised web site / server	Web app
Operation Tripoli	Checkpoint	Government, telecoms		Supply chain compromise	Facebook pages

Title	Source	Primary target	Objectives	Initial Access	Notes
New Dridex Variant Evading Traditional Antivirus	Esentire			Spearphishing	
An Analysis of Godlua Backdoor	Netlab			Exploit public-facing application	Widget connector macro
Welcome Spelevo: New exploit kit full of old tricks	Cisco Talos		exploit kit	Compromised web site / server	
Continued attacks by Kimsuky	Alyac			Spearphishing	
Iranian Threat Actor Amasses Large Cyber Operations Infrastructure Network to Target Saudi Organizations	Recorded Future	Saudi Arabia		Spearphishing	
GreenFlash Sundown exploit kit expands via large malvertising campaign	Malwarebytes		Malvertising	Compromised web site / server	
Silex IoT BrickerBot Malware	ZDNet		Destroying IoT	Weak / default credential compromise	
Gift Cardsharks	RiskIQ	Gift card retailers	Financial gain	Spearphishing	
Lazarus continuing to target crypto-currencies	Alyac		Cryptocurrency	Spearphishing	
Kimsuky targtets Korean Crypto-currency Exchanges	Alyac	Cryptocurrency	Exchange compromise	Spearphishing	
A worldwide campaign against telecom providers	Cybereason	Telecoms	obtain CDR records	Exploit public-facing application	
Tick group targets South Korea with USB Air Gap Jumper	Ahnlab	Japan, Korea	Espionage	Weaponised secure USB	
DarkHotel disclosed the latest attack on Chinese foreign trade	Tencent	Government	Espionage		
HydSeven Attack Against Coinbase	Objective-See	Cryptocurrency	Cryptocurrency	Exploit public-facing application	Zero day
Gh0stCringe	Binary Defense		RAT	SMB (eternal Blue)	
DanaBot Demands a Ransom Payment	Checkpoint		Ransomware	Spearphishing	
Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments	Symantec	Government, IT and comms, Education	Espionage	Exploit public-facing application	
LoudMiner Cross-platform mining in cracked VST software	ESET We live security	Cryptocurrency	Mining	Supply Chain Compromise	Pirate software
MenuPass QuasarRAT Backdoor	Cylance Threat Vector	EMEA various	RAT	Spearphishing	

Additional Resources

Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make better security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. - USA Office | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234)
KnowBe4 UK, Ltd. | The Hawkhills Estate, Easingwold, York Y061 3FE | Tel: +44 1347 487512
www.KnowBe4.com | Email: Sales@KnowBe4.com