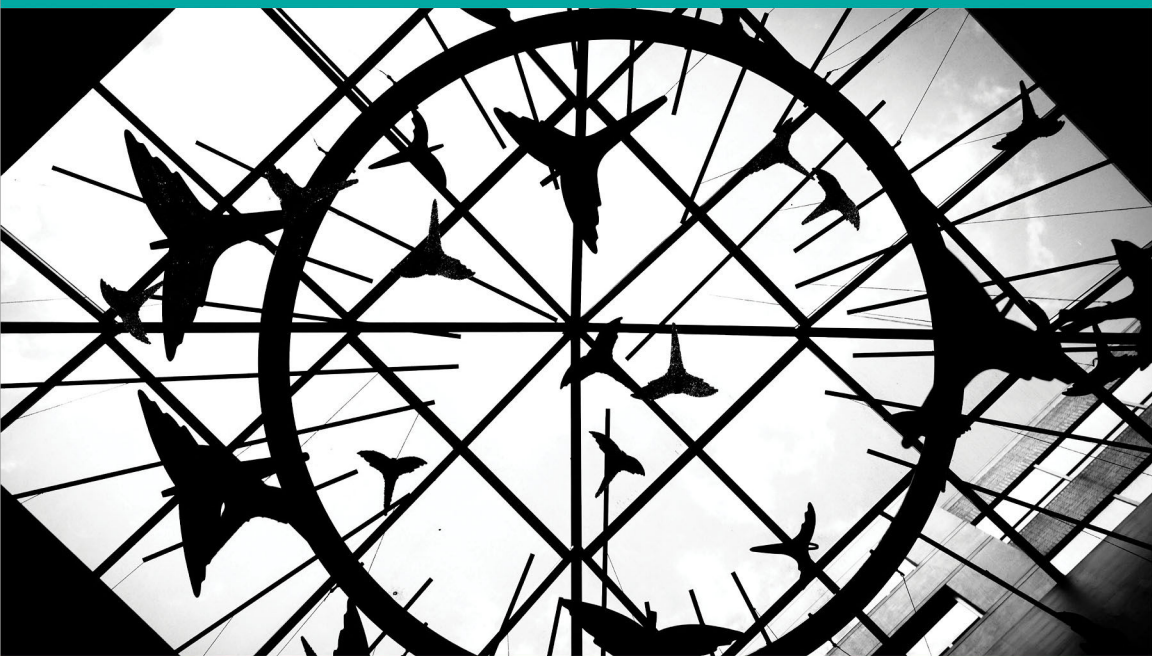


O'REILLY®

Security with AI and Machine Learning

Using Advanced Tools to Improve
Security at the Edge



Laurent Gil & Allan Liska

Security with AI and Machine Learning

*Using Advanced Tools to Improve
Application Security at the Edge*

Laurent Gil and Allan Liska

Beijing • Boston • Farnham • Sebastopol • Tokyo

O'REILLY®

Security with AI and Machine Learning

by Laurent Gil and Allan Liska

Copyright © 2019 O'Reilly Media. All rights reserved.

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (<http://oreilly.com>). For more information, contact our corporate/institutional sales department: 800-998-9938 or corporate@oreilly.com.

Editor: Virginia Wilson

Production Editors: Nan Barber and
Christopher Faucher

Copyeditor: Octal Publishing, LLC

Proofreader: Nan Barber

Interior Designer: David Futato

Cover Designer: Karen Montgomery

Illustrator: Rebecca Demarest

October 2018: First Edition

Revision History for the First Edition

2018-10-08: First Release

2019-02-04: Second Release

The O'Reilly logo is a registered trademark of O'Reilly Media, Inc. *Security with AI and Machine Learning*, the cover image, and related trade dress are trademarks of O'Reilly Media, Inc.

The views expressed in this work are those of the authors, and do not represent the publisher's views. While the publisher and the authors have used good faith efforts to ensure that the information and instructions contained in this work are accurate, the publisher and the authors disclaim all responsibility for errors or omissions, including without limitation responsibility for damages resulting from the use of or reliance on this work. Use of the information and instructions contained in this work is at your own risk. If any code samples or other technology this work contains or describes is subject to open source licenses or the intellectual property rights of others, it is your responsibility to ensure that your use thereof complies with such licenses and/or rights.

This work is part of a collaboration between O'Reilly and Oracle Dyn. See our [statement of editorial independence](#).

978-1-492-04312-6

[LSI]

Table of Contents

Preface.....	v
1. The Role of ML and AI in Security.....	1
Where Rules-Based, Signature-Based, and Firewall Solutions Fall Short	2
Preparing for Unexpected Attacks	4
2. Understanding AI, ML, and Automation.....	7
AI and ML	7
Automation	9
Challenges in Adopting AI and ML	10
The Way Forward	11
3. Focusing on the Threat of Malicious Bots.....	15
Bots and Botnets	15
Bots and Remote Code Execution	18
4. The Evolution of the Botnet.....	23
A Thriving Underground Market	23
The Bot Marketplace	24
AI and ML Adoption in Botnets	29
Staying Ahead of the Next Attack with Threat Intelligence	30
5. AI and ML on the Security Front: A Focus on Web Applications.....	33
Finding Anomalies	33
Bringing ML to Bot Attack Remediation	35

Using Supervised ML-Based Defenses for Security Events and Log Analysis	35
Deploying Increasingly Sophisticated Malware Detection	36
Using AI to Identify Bots	37
6. AI and ML on the Security Front: Beyond Bots.	39
Identifying the Insider Threat	39
Tracking Attacker Dwell Time	40
Orchestrating Protection	41
ML and AI in Security Solutions Today	42
7. ML and AI Case Studies.	43
Case Study: Global Media Company Fights Scraping Bots	43
When Nothing Else Works: Using Very Sophisticated ML Engines with a Data Science Team	51
The Results	54
8. Looking Ahead: AI, ML, and Managed Security Service Providers. .	57
The MSSP as an AI and ML Source	57
Cloud-Based WAFs Using AI and ML	59
9. Conclusion: Why AI and ML Are Pivotal to the Future of Enterprise Security.	61

Preface

It seems that every presentation from every security vendor begins with an introductory slide explaining how the number and complexity of attacks an organization faces have continued to grow exponentially. Of course, everyone from security operations center (SOC) analysts, who are drowning in alerts, to chief information security officers (CISOs), who are desperately trying to make sense of the trends in security, is acutely aware of the situation. The question is how do we, collectively, solve the problem of overwhelmed security teams? The answer in many cases now involves machine learning (ML) and artificial intelligence (AI).

The goal of this report is to present a high-level overview aimed at a security leadership audience of ML and AI and demonstrate the ways security tools are using both of these technologies to identify threats earlier, connect attack patterns, and allow operators and analysts to focus on their core mission rather than chasing around false positives. This report also looks at the ways in which managed security service providers (MSSPs) are using AI and ML to identify patterns from across their customer base to improve security for everyone.

A secondary goal of the report is also to help tamp down the hype associated with ML and AI. It seems that ML and AI have become the new buzzwords at security conferences, replacing “big data” and “threat intelligence” as the go-to marketing terms. This report provides a reasoned overview of the strengths and limitations of ML and AI in security today as well as going forward.

The Role of ML and AI in Security

Why has there been such a sudden explosion of ML and AI in security? The truth is that these technologies have been underpinning many security tools for years. Frankly, both tools are necessary precisely because there has been such a rapid increase in the number and complexity of attacks. These attacks carry a high cost for business. Recent studies predict that global annual cybercrime costs will grow from \$3 trillion in 2015 to \$6 trillion annually by 2021. This includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.¹ Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed \$1 trillion cumulatively from 2017 to 2021.²

The reality is that organizations have not been able to rely for a while on a “set it and forget it” approach to security using antiquated, inflexible, and static defenses. Instead, adaptive and automated security tools that rely on ML and AI under the hood are becoming the norm in security, and your security team must adapt to these technologies in order to be able to succeed.

¹ *Cybersecurity Ventures Annual Crime Report*

² *Cybersecurity Market Report*; published quarterly by Cybersecurity Ventures; 2018

Security teams are tasked with protecting an organization's data, operations, and people. To protect against the current attack posture of their adversaries, these teams will need increasingly advanced tools.

As the sophistication level of malicious bots and other attacks increases, traditional approaches to security, like antivirus software or basic malware detection, become less effective. In this chapter, we examine what is not working now and what will still be insufficient in the future, while laying the groundwork for the increased use of ML- and AI-based security tools and solutions.

Where Rules-Based, Signature-Based, and Firewall Solutions Fall Short

To illustrate why *rules-based* and *signature-based* security solutions are not strong enough to manage today's attackers, consider antivirus software, which has become a staple of organizations over the past 30 years. Traditional antivirus software is rules-based, triggered to block access when recognized signature patterns are encountered. For example, if a known remote access Trojan (RAT) infects a system, the antivirus installed on the system recognizes the RAT based on a signature (generally a file hash) and stops the file from executing.

What the antivirus solution does not do is close off the infection point, whether that is a vulnerability in the browser, a phishing email, or some other attack vector. Unfortunately, this leaves the attacker free to strike again with a new variation of the RAT for which the victim's antivirus solution does not currently have a signature. Antivirus software also does not account for legitimate programs being used in malicious ways. To avoid being detected by traditional antivirus software, many malware authors have switched to so-called *file-less malware*. This malware relies on tools already installed on the victims' systems such as a web browser, PowerShell, or another scripting engine to carry out their malicious commands. Because these are well-known "good" programs, the antivirus solutions allow them to operate, even though they are engaging in malicious activity.

This is why many antivirus developers have switched detection to more heuristic methods. Rather than search just for matching file

hashes, they instead monitor for behaviors that are indicative of malicious code. The antivirus programs look for code that writes to certain registry keys on Microsoft Windows systems or requests certain permissions on macOS devices and stops that activity, irrespective of whether the antivirus has a signature for the malicious files.

Firewalls work in a similar way. For example, if an attacker tries to telnet to almost any host on the internet, the request will most likely be blocked. This is because most security admins disable inbound telnet at the firewall. Even when the telnet daemon is running on internal systems, it is generally blocked at the firewall, meaning external attackers cannot access an internal system using telnet. Of course, attackers can use telnet to access systems that are outside of the firewall, such as routers, assuming the telnet daemon is running on those systems. This is why it is important to disable the telnet daemon directly on the devices, in addition to blocking the protocol at the firewall.

Generally, firewalls are inadequate to defeat today's attacks. Firewalls either block or allow traffic with no regard for the content of the traffic. This is why attackers have moved to exfiltrate stolen data using ports 80 and 443 (HTTP and HTTPS, respectively). Almost every organization has to allow traffic outbound on these ports, otherwise people in that organization cannot do their jobs. The attackers know this, and they'll normally open their backdoors and establish command and control communications with their victims using ports 80 and 443. As a result, data can be stolen out of the network through the firewall.

This is also the reason why phishing attacks are so rampant today. Attackers in most cases can't get in through the firewalls from the outside-in to attack an internal computer; therefore, they phish people and get them to do the work for them. The victims click, they are directed to a malicious site, and the return "malicious" traffic is allowed through the firewall. It's just the way firewalls work. Most often the return traffic is an exploit for a known vulnerability and some additional code that will be executed by the victim, opening up a backdoor on the system.

In comparison, when firewalls are deployed in front of websites and applications, organizations must leave ports 80 and 443 wide open to the internet. These ports must be opened "inbound" so that users on the internet can access the services running on the downstream

servers and applications. Because these ports must be left open to support web services, inbound attacks and malware exploits, among other threats, pass through the firewall undetected. In this case, firewalls provide little, if any protection inbound.

When it comes to malicious bots and other more sophisticated threats targeting web applications, traditional approaches such as using firewalls do not work, because the attackers know how to get around them. Today's advanced malicious actors can find an access path that can easily defeat rule- and signature-based security platforms. Attackers understand how traditional security technologies work and use this knowledge to their advantage.

Preparing for Unexpected Attacks

Every website, router, or server is, in one way or another, potentially vulnerable to attacks. Although there is a lot of hype around *zero-day attacks* (those attacks that were previously unknown or unpublished) most attackers take advantage of published vulnerabilities. Attackers can react quickly to newly reported vulnerabilities, often writing exploit code within hours of a new vulnerability being announced. Most often, attackers learn of vulnerabilities from the *NVD website* (NVD), vendor notifications and a patch availability announcement, or they discover vulnerabilities on their own.

It then becomes a race between the attackers launching active exploits against a known vulnerability and an organization being able to patch that vulnerability. Unfortunately, it is usually easier to write an exploit than it is to quickly patch newly discovered vulnerabilities. Organizations must go through myriad tests and patch deployment approvals prior to installing the patch. This is what led to the well-known *Equifax breach*. The vulnerability that affected Equifax was already known; a patch was available, but the patch was not deployed.

With attacks like this, signature-based security solutions work only when they have a signature for a certain exploit looking to take advantage of a known vulnerability. If a signature is not specifically created for an exploit, a signature-based security solution cannot “develop one on its own.” Human intervention is needed. In addition, every security technology vendor will race against time to develop a signature and apply it as a rule to its technology to catch and stop a known exploit. As a result, attackers tweak their exploits

and create slightly different variants designed to defeat signature-based approaches. This is one of the reasons why there are massive numbers of malware variants today.

Software vendors often win the race against attackers by announcing to their customers that a vulnerability has been found and then quickly making a patch available. In some cases, it can take longer than others depending on the critical nature of the vulnerability or the amount of time it takes to develop a patch. And, in the case of the Equifax breach, human error intervened when someone simply forgot to apply the needed patch that would have likely stopped the breach.

In contrast to the more traditional “after-the-fact” approaches to security that we just discussed, ML and AI provide a nonlinear way to identify attacks, looking beyond simple signatures, identifying similarities to what has happened before, and flagging things that appear to be anomalies. The following chapter discusses ML and AI defenses in more detail.

In subsequent chapters, this report introduces the sometimes-confusing concepts of ML and AI, provides an overview of the threat that is posed by automated bots, and discusses ways that security teams can use ML and AI to better protect their organization from malicious bots and other threats.

Understanding AI, ML, and Automation

Prior to discussing the ways in which you can use ML and AI to help your defenders better protect your organization, let's step back and define the terms. There is a lot of confusion around the definition of ML and AI and how the technologies interact with each other. In addition to defining these terms, no discussion of ML and AI is complete if it doesn't touch on automation. One of the overarching goals of both ML and AI is to reliably automate the process of identifying patterns and connections. In addition, and specifically to security, ML and AI allow security teams to reliably automate mundane tasks, freeing analysts to focus on their core mission, as opposed to spending their days chasing false positives.

AI and ML

Although many people in the industry have a tendency to use the terms AI and ML interchangeably, they are not the same thing. AI is defined as the theory and development of computer systems that are able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. With AI, machines demonstrate “intelligence” (some call this the “simulation of an intelligent behavior”), in contrast to the natural intelligence displayed by humans. The term is applied when a machine mimics cognitive functions that

humans associate with other human minds, such as learning and problem solving.

Machine learning is an application of AI that provides systems with the ability to automatically learn and improve from experience without being explicitly programmed. ML focuses on the development of computer programs that can access data and use it to learn for themselves. The more machines are trained, the “smarter” they become, as long as the training material is valuable for the tasks that the machines are supposed to focus on. In the current defense landscape, ML is more established and, therefore, more likely to be used defensively as compared to AI. With ML, humans—generally analysts in the case of security—are responsible for training the machine, and the machine is capable of learning with the help of humans as feedback systems.

Curt Aubley of CrowdStrike proposed that one way to distinguish between the two types of technologies is that AI is like the Terminators from the movie series of the same name, whereas Iron Man’s suit is an example of ML. The terminators are completely autonomous and can adapt to the situation around them as it changes. The Iron Man suit is constantly giving Tony Stark feedback as well as accepting new inputs from him.

A more realistic example that provides a better understanding of the differences between AI and ML is one of the most common uses of the two combined capabilities: monitoring for credit card fraud. Credit card companies monitor billions of transactions each day, looking for potential fraudulent transactions. The algorithms need to account for millions of factors. Some algorithms are obvious, such as a credit card that is physically swiped in New York City cannot be physically swiped in Singapore five minutes later. But other factors are not as obvious. For example, when a card that is regularly used to buy clothes at a retailer such as Target or Kohl’s is suddenly used to buy clothes at Gucci, it might raise a red flag. But it is not immediately clear whether that is fraudulent activity or just someone buying clothes for a special occasion. No human can possibly account for all the different ways that fraudulent transactions can manifest themselves, so the algorithms must consider any anomalous transactions. This is where AI is part of the process. The ML part of the process involves combing through those billions of transactions each day, discovering new patterns that indicate fraud and adjusting the AI algorithms to account for the new information.

ML and AI do not always need to work together; some systems take advantage of one technology or the other, but not both. In addition, most of the time both AI and ML are invisible to the end user. Modern security information and event managers (SIEMs) use ML to search through hundreds of millions of log events to build alerts, but the security operations center (SOC) analyst sees only the alerts. Similarly, Facebook and Google use AI to help automatically identify and tag users in pictures millions of times each day. The technology is invisible to the user; they just know that when they upload a picture, all of their friends are automatically tagged in it.

Automation

Automation is simply defined as the technique, method, or system of operating or controlling a process by highly automatic means, reducing human intervention to a minimum. Automation is really just manual rules and processes repeated automatically, but nothing is learned, as in the case with ML and AI. Automation is often the end result of AI and ML systems within an organization. For instance, an organization might use AI and ML to identify suspicious activity and then use automation to automatically provide alerts on that activity, or even take action to stop it. In other words, automation might be the visible result of AI and ML systems.

Automation driven by AI and ML backend systems is one of the biggest growth areas in cybersecurity. Although it has become somewhat cliché to say that security teams are overwhelmed by alerts, it is true. Automation, especially through orchestration platforms, allows security teams to have the orchestration system automatically perform mundane or repetitive tasks that have a low false-positive rate. This, in turn, frees security teams to work on the more complex alerts, which is a priority as cyberthreats escalate in speed and intensity.

Challenges in Adopting AI and ML

It should be noted, that as powerful as AI and ML are, they are not without their downsides. Any organization that's serious about incorporating AI and ML into its security program should consider some of the potential pitfalls and be prepared to address them.

One of the biggest challenges that your organization might face when embarking on the AI and ML journey is the challenge of collecting data to feed into AI and ML systems. Security vendors have become a lot better over the past few years about creating open systems that communicate well with one another, but not all vendors play nice with all of the other vendors in the sandbox.

From a practical perspective, this means that your team will often struggle to get data from one system into another system, or even to extract the necessary data at all. Building out new AI and ML systems requires a lot of planning and might require some arm-twisting of vendors to ensure that they will play nice.

Even when different security vendors are willing to talk to one another, they sometimes don't speak the same language. Some tools might output data only in Syslog format, whereas others output in XML or JSON. Whatever AI and ML system your organization adopts must be able to ingest the data in whatever format it is presented and understand its structure so that it can be parsed and correlated against other data types being ingested by the AI and ML system.

Even when the systems talk to one another, there are often organizational politics that come into play. This happens at organizations of any size, but it can be especially common in large organizations. Simply put, you, as the security leader, need input from specific systems, but the owners of those systems don't want to share it. Irrespective of whether their reasons are valid, getting the necessary data can be as much of a political challenge as it is a technical one. That is why any AI and machine learning initiatives within your organizations need to have senior executive or board sponsorship. This helps to ensure that any reluctance to share will be addressed at a high level and encourages more cooperation between departments.

Finally, let's address something that was touched on briefly earlier in this chapter: AI and ML systems require a lot of maintenance, at

least initially. Not only do you need to feed the right data into these systems, but there needs to be a continuous curation of the data in the system to help it learn what your organization considers good output and bad output. In other words, your analyst team must help train the AI and ML systems to better understand the kind of results the analysts are looking for.

These caveats aren't meant to scare anyone away from adopting AI and ML solutions; in fact, for most organizations the adoption is inevitable. However, it is important to note some of the potential challenges and be prepared to deal with them.

The Way Forward

Most security professionals agree that first-generation and even next-generation security technologies cannot keep pace with the scale of attacks targeting their organizations. What's more, cyberattackers are proving these traditional defenses and legacy approaches are not solving the problem. Today, attackers seem to have the upper hand as demonstrated by the sheer number of successful breaches. Traditional endpoint security can't keep up with sophisticated attack techniques, while outdated edge defenses are being rendered ineffective by the sheer volume of alerts. This leaves many security teams forced to play "whack-a-mole" security, jumping from one threat to the next without ever truly solving the problem.

This analogy presents a way to move forward with a clear understanding between AI, ML, and human activity: Many who've had a chance to visit a military airshow are often amazed at the technologies on display. Attendees can usually observe firsthand an array of fighter jets with tons of airpower, attack helicopters with astonishing features, and bombers with stealth capabilities. But is the technology sitting on that airfield (or flying over your head) all that is needed to win a battle? The answer is no. These magnificent technologies on their own are nothing more than metal, plastic, and glass. What makes these technologies effective is the highly skilled humans that operate these fighting machines, and the intelligent computer systems that reside within them.

Most people don't realize that when a pilot is flying an aircraft cruising at nearly Mach 2, that pilot really does not have direct control of the "stick"; a computer does. The reason is that humans often react too quickly or radically when in danger. If the pilot pulls too hard on

the control stick in a plane, it could be disastrous. So, the computer running the aircraft actually compensates for this and ensures that the pilot's moves on the stick do not put the plane in danger.

As you might observe, there is a synergy occurring in many of these aircraft. The human-computer synergy is quite apparent. It not only keeps the aircraft safe, it also keeps the human in check. In this case, the computer compensates for the potential human error caused by the pilot.

Turning back to this security discussion, it is clear that as a new generation of security technologies comes to market, a slightly different human-computer collaboration will become even more apparent.

Security technologies using AI and ML are a reality today. However, these advances are not designed to eliminate humans from the equation. It's actually the opposite. They're designed to *equip* the human with the tools that they need to better defend their organizations against cybercrime. However, misunderstandings are prevalent surrounding AI and what it actually is.

Some people believe AI will lead to an end-of-the-world scenario as in the previously referenced movie *The Terminator*. Great for headlines—however that's not what AI is all about. Others believe AI-enabled security technology is designed to be “set it and forget it,” replacing the skilled human operator with some sort of robot, which is not the case, either.

When implemented correctly, AI and ML can be a force multiplier. The goal is to teach a cybersecurity technology to automate and reduce false positives, and do it all much faster than humans could ever hope to. ML in cybersecurity uses the concept of creating models that often contain a large number of good and malicious pieces of data. These could be real-time pieces of data or data that was captured and stored from known samples. As an ML engine runs a model, it makes assumptions about what is good data, what is malicious data, and what is still clearly unknown.

After the ML engine has finished running a model, the results are captured. When a human interprets the results, the human then begins to “train the ML engine,” telling it what assumptions were correct, what mistakes were made, and what still needs to be rerun.

With the distinction between the roles and interplay of AI, ML, and essential human involvement clearly defined, we can move on to the next chapter to discuss some of the practical applications of these technologies in security.

Focusing on the Threat of Malicious Bots

Your security team is not the only one that is increasingly relying on ML, AI, and automation. Cybercriminals and nation-state actors all use automation and rudimentary machine learning to build out large-scale attack infrastructures. These infrastructures are often referred to colloquially as bots or botnets reflecting the automated nature of the attacks. This chapter covers some of the different types of bots, how they work, and the dangers they pose to organizations.

Bots and Botnets

By some measures bots make up more than half of all internet traffic and are the number one catalyst for attacks, ranging from botnets launching *distributed denial of service* (DDoS) attacks to malicious bot traffic that simulates human behavior to perpetrate online fraud, all at an exponentially expanding scale. Reports on a recent industry study analyzing more than 7.3 trillion bot requests per month reveal that in the last three months of 2017, the attacks made up more than 40% of malicious login attempts. The study also reports that attackers are looking to add enterprise systems as a part of their botnet by exploiting remote code execution vulnerabilities in enterprise-level software.¹

¹ 2017 sees huge increase in bot traffic and crime; IT Pro Portal.

The terms bot and botnet get thrown around a lot, but what do they really mean? There are a lot of different types of bots that perform different functions, but a malware *bot* is a piece of code that automates and amplifies the ability of an attacker to exploit as many targets as possible as quickly as possible. Bots generally consist of three parts:

- Scanning
- Exploitation/tasking
- Command-and-control communication

The first task involves a bot wading through millions or tens of millions of public-facing IP addresses probing for specific technologies and applications that the bot is designed to exploit. Sometimes, that scanning is made easier by the use of third-party sources such as the *Shodan databases*, but often these bots are operating completely autonomously.

When the bot finds a system that it can exploit, it attempts to do so. That exploitation might consist of an actual exploit (discussed in more detail in a few moments), but the exploitation might also be a brute-force login attack using a list of common username–password combinations. It could also be a website where the bot is trying to gather information by sidestepping CAPTCHA protections.

After a bot has successfully exploited a system, it either installs a payload or communicates directly back to a command-and-control (C&C) host that it has successfully exploited a system. The attacker might act if it is a high-value target, but often the attacker is just collecting systems that will be used to redirect other attacks or activated all at once to launch a DDoS attack.

Those collective systems, controlled by an attacker from one or more (C&C) servers, are known as a *botnet*. **Figure 3-1** shows the topology of a C&C botnet. The botmaster is the attacker that manages the C&C servers, which are responsible for tasking the infected systems in order to continue growing the botnet or attacking targeted systems.

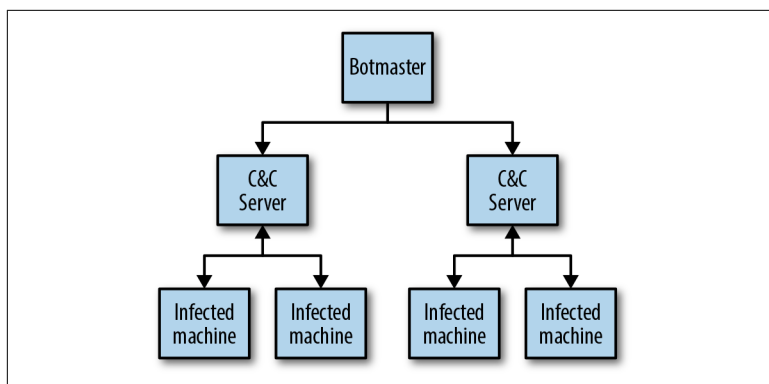


Figure 3-1. Botnet hierarchy

Botnets tend to be single purpose, depending on the tools installed by the attacker. The most common type of botnet is one that is used for DDoS attacks. DDoS attacks are a very profitable industry on underground forums, and attackers that control large botnets sell their services for anywhere from \$50 for a one-hour attack to thousands of dollars for a large-scale sustained attack. DDoS botnets are generally looking to exploit home routers used for residential high-speed internet access. These systems are rarely monitored, often left unpatched, and therefore make easy and persistent targets for attackers.

Some botnets are used to spread malware by compromising websites and embedding code that redirects victims to an exploit server owned by the attacker. These botnets often exploit flaws in web applications such as WordPress or Joomla. The attacker is generally not using this malware to gain access to an organization (and most of the time these sites are hosted on separate infrastructure outside of the organization, so there is not direct access); instead, the attacker is looking to infect visitors to those sites with ransomware, cryptocurrency mining malware, or banking trojans.

Some botnets are designed to help an attacker gain access to enterprise-level organizations. These botnets tend to target vulnerabilities in internet-facing applications that usually allow direct access to the network. Often these bots will target tools like JBOSS or attempt to brute-force Microsoft's Remote Desktop Protocol (RDP). These botnets use exploits that target well-known vulnerabilities and are usually looking for systems that vulnerability management teams don't know about or left unpatched. The attacker that controls

access to these systems can use that access to further exploit networks that are of interest, or they might sell access to those networks in the underground market.

Finally, there are botnets that are designed to steal information from websites. These bots, often operated by unscrupulous competitors or price aggregate sites, are built to *scrape* target websites for information or pricing and use the collected data to give the attacker a competitive advantage. These bots are particularly difficult to block because they are designed to mimic web user behavior pretty assiduously, and organizations that attempt to block these bots run the risk of keeping legitimate users from accessing their website and losing customers.

Bots and Remote Code Execution

Using bots and botnets for remote code execution is one of their earliest and most common uses. These bots tend to operate in two stages. The first stage scans hundreds of millions of IP addresses looking for internet-facing systems that appear to have a predefined list of vulnerabilities. When the scanning bot finds a potentially vulnerable system, it reaches back to an exploit kit, such as Metasploit, which launches the attack and installs a loader that calls back to one of the C&C servers owned by the attacker.

This is one of the reasons why bots can be so difficult to track and stop: in the anatomy of an attack, the bot will originate from one IP address, the actual exploitation will come from another IP address, and the C&C server will be a different IP address. None of these IP addresses will be connected, because they are from systems compromised by the attacker. This means there is no rhyme or reason to where the attacks originate, which makes it very difficult to put rules in place to block them.

Not all exploit bots operate using the two-stage process. Purpose-built bots that are targeting only a single application or technology will often embed whatever necessary exploit code or login credentials in the scanning bot. This allows the bot to infect a system and then turn the newly infected system into a bot that continues the scanning and infecting process. As a result, there are hundreds of thousands of bots looking for new systems to infect at any one time.

Most exploits targeting an OS or application are specially designed and include some sort of buffer, stack, or heap overflow combined with a piece of remote code that is then executed by the targeted system. When doing a search on <http://cve.mitre.org/> for the terms “remote code execution,” the search returns with 16,035 known vulnerabilities dating all the way back to 1999, and the list is growing daily. These are pinpointed weak spots that would allow code to be remotely executed by the vulnerable operating system (OS) or application. When attackers are crafting their exploits, they add additional code that they hope is executed by the target system. When the “remote” code is executed, most of it allows a back door to be opened on the target system, thus allowing the attacker control over your systems, right through any edge defenses.

Often, the remote code that is executed by the targeted OS or application not only allows attackers to gain access to a system, but also potentially downloads additional code to enable attackers to remain resident in that system for long periods of time. The vulnerabilities in these cases are not created by the “usage” of the OS or application directly. Instead, they are mistakenly created by the manufacturers or developers of the OS or application.

One of the most effective deterrents against exploitation-based botnets is good vulnerability management. Vulnerability management and prioritization of patching is not the most exciting aspect of information security, but it is critical to stopping systems from becoming part of a botnet, and there is a role for AI and machine learning in vulnerability management.

It is important to keep in mind that these botnets are not using so-called *zero day* exploits, which are exploits that have not yet been publicly released. Instead, they are relying on shared proof-of-concept code for well-known vulnerabilities. Using AI and ML, companies that specialize in vulnerability management tools can determine which exploits are active in the wild and being used by the various exploit kits. That information is then shared with vulnerability management teams (VMTs) so that they can prioritize patching of publicly exposed systems that might be susceptible to currently widely exploitable vulnerabilities. Of course, in order for this to be an effective strategy, an organization must perform regular scans of its systems, both internal and external, and it must have a regular patching cycle.

More Flexible Malicious Bots, More Risks to Your Business

As long as there remain easily accessible and exploitable systems connected to the internet, the threat of bots and botnets will continue to grow. Bot traffic continues to grow because bots are cheap to maintain, successful in exploiting targets, and help cybercriminals make money. That is why they are used to infiltrate enterprise web and mobile applications at the cloud or network edge, exploiting vulnerabilities and performing account takeovers, account creations, credit card fraud, DDoS attacks, and more. Bot traffic continues to scale, sometimes faster than the protections in place to defend against it can adapt, which is why in March of 2018, GitHub was unreachable for 10 minutes as it was the victim of the **largest DDoS attack on record**.

The bot threat is more than just a threat of exploitation or DDoS attacks. Threat actors can also use bots to attack API endpoints, where traditional bot challenges such as JavaScript, device fingerprinting, and CAPTCHA programs intended to distinguish human from machine input are not effective at thwarting bot attacks. An attacker can use successful exploitation of an API endpoint to expose sensitive data such as customer information or intellectual property.

In short, the modern botnet poses multiple threats to an organization. Even an unsuccessful attack can affect performance, availability, customer experience, and, ultimately, the bottom line.

In addition, botnets are constantly adapting to new techniques and new types of malware. For example, there's *cryptocurrency mining*, which is when attackers use JavaScript or malware to mine for Bitcoins or another cryptocurrency. In fact, according to industry reports, cryptocurrency mining malware is quickly becoming an attacker favorite, with nearly 90% of all remote code execution attacks in late 2017 sending a request to an external source to try to install cryptocurrency mining malware. These attacks primarily exploit vulnerabilities in the web application source code to download and run different cryptocurrency mining malware on the infected server or exploit web servers and implant code that downloads a cryptocurrency miner to visitors to the site. One of the reasons that cryptocurrency mining has been so successful is that they don't steal information or disrupt other services on the machine, so they tend

to be low priority for removal. Thus, while a single cryptocurrency miner doesn't generate much revenue for an attacker, thousands of them running for extended periods of time can.²

Bots and botnets pose a multifaceted threat to organizations that is difficult to defend against using existing security tools. For organizations to mount an effective defense, security teams must increasingly rely on automation as part of their defense strategies. The subsequent chapters discuss how to effectively and efficiently use AI and ML to prevent and mitigate these attacks.

² New Research: [Crypto-mining Drives Almost 90% of All Remote Code Execution Attacks](#); Imperva blog.

The Evolution of the Botnet

This chapter focuses on the ways in which the threat from bots and botnets has continued to evolve. Just as your security team cannot rely on technology from 5 or 10 years ago, threat actors are constantly changing their attack strategies and finding new ways to wreak havoc on unsuspecting networks. This includes changing up tactics, including incorporating ML into their own capabilities. Of course, attackers aren't afraid to dip back into classics tricks that still work. Defenders need to be able to protect against these new attack methodologies while still ensuring that defenses against older attacks remain in place.

A Thriving Underground Market

Before getting to the actions of sophisticated threat actors, it is important to understand the evolving underground market. This begins with the increase in commoditization and specialization by threat actors, which makes it easier for less-sophisticated threat actors to “get a foot in the door” by purchasing tools or access from other actors that specialize in various areas of cybercrime. Some of these specialties include the following:

- Launching distributed denial of service (DDoS) attacks
- Phishing campaigns
- Managing ransomware campaigns

- Selling access to organizations
- Developing malware for rent or sale

This specialization allows attackers that have a specific skill to continue to improve the capabilities of their tool or service. The revenue stream that comes from selling their capability means that they now have the time to work on adding features or improving antidetection mechanisms, making them more effective. For example, an attacker who specializes in selling access can spend time gaining and maintaining access to hundreds of organizations without detection. Another actor who needs a foothold into a specific organization can buy that access for \$10 to \$50. This is a benefit to both parties: the first actor makes money selling access, whereas the second actor saves time by not having to spend days or weeks finding an initial entry point.

Attackers who provide quality products or services gain a strong reputation on the various underground forums and can charge a premium for their services. Newer attackers often seek them out, especially if they get in over their head during an attack. An example of this came when two novice attackers used acquired point-of-sale (POS) malware and actually deployed it into the POS network of a major retailer. As a result, they **accessed and sold 100 million credit cards** at the peak of the holiday shopping season.

All of this equated to an underground market that conducts about \$6.7 million in business, just from sales of malware and other malicious activity, every year **according to Carbon Black**.

The Bot Marketplace

A lot of the rise in the underground market can be attributed to the rise in the adoption of Internet of Things (IoT) devices. The internet-connected world has witnessed large numbers of poorly protected technologies being taken over and conscripted into botnets with amazing firepower. Just a few weeks after the 1.3 Terabyte DDoS attack that was reported against GitHub, a **1.7 Terabyte DDoS attack** was reported against another, unnamed ISP, according to Arbor networks. This is something that had never been seen before.

So, are DDoS attacks the only attack vector these infected devices are capable of? Unfortunately, they are not.

The Problem with “Set It and Forget It”

These IoT devices present a security challenge around the world. Similar to the idea of “set it and forget it,” discussed in the Preface, these IoT devices, often internet-facing home and small office routers, are deployed and then never touched again. Because these devices are provided to a consumer or small office by the ISP or by the larger IT organization, there is an assumption that whoever provided the router will also manage it. That is usually not the case. So, these routers sit untouched for years, generally until they are replaced, without being patched and often without their default usernames and passwords being changed.

This means there are potentially hundreds of millions of vulnerable systems for attackers to compromise. And, because the botnet owners use the devices to attack outward, as opposed to attacking the network to which the routers are attached, the victims of these attacks rarely know that their routers (or other IoT devices have been compromised).

One of the easiest protections for consumers and small businesses is to update their home routers frequently and change their default passwords. These simple steps make it significantly more difficult for botnet owners to build and maintain their botnets and make the internet safer for everyone.

The recent exponential growth in botnet attacks can be traced back to the release of the *Mirai botnet*. The **Mirai malware** was first unleashed on the web in mid-2016. The initial variant of Mirai was rather simple in its infection and take-over technique. The writers of Mirai must have done some research by looking at user manuals for common IoT devices, ultimately selecting IP video cameras. They included a list of factory default usernames and passwords in the malware and used this list in the attack.

The Mirai botnet used Telnet and/or Secure Shell (SSH) plus the long list of usernames and passwords, and, more often than not, successfully logged into a significant number of IP cameras located all over the world. After the malware determined that access was gained, it instructed the camera to download additional code. This

code included instructions to maintain command and control in order for the cameras to communicate back to the attackers running the botnet. It also included a large list of DDoS attack tools and code to self-propagate like a worm and infect other similar cameras. Although it was rather simple, it was also ingenious.

In October of 2016 the **source code for the Mirai botnet was made publicly available on GitHub**. Since then, a number of Mirai copycats, including Reaper, Satori, and Okiru, have been released. **Figure 4-1** illustrates some of the highlights of the Mirai timeline. These variants keep the underlying source code but have added new capabilities that make them more dangerous. These variants no longer rely solely on well-known usernames and passwords, instead they are now exploiting vulnerabilities in the software that many of the IoT devices are running. The current and future variants of Mirai and their attack methodology are poised to become an important challenge the entire industry will face before the end of this decade.

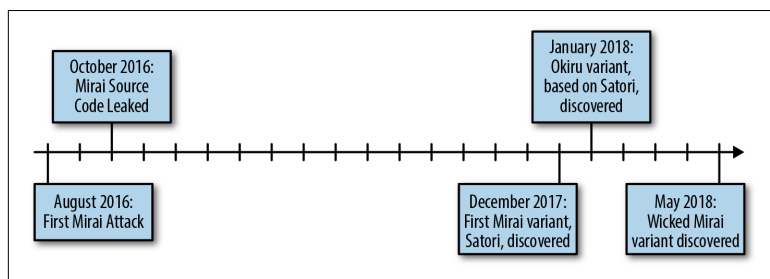


Figure 4-1. Timeline of Mirai activity

As a result of Mirai and its variants targeting consumer IoT devices, on May 25, 2018 the US Federal Bureau of Investigation (FBI) released a Public Service Announcement titled *Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide*. The announcement says:

The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices. Foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office and home office routers. The malware is able to perform multiple functions, including possible information collection, device exploitation, and blocking network traffic.

The size and scope of the infrastructure impacted by this VPNFilter malware is significant. The malware targets routers produced by several manufacturers and network-attached storage devices by at least one manufacturer. The initial infection vector for this malware is currently unknown.¹

To further highlight the challenges surrounding consumer-based IoT and often the lack of security when they're developed and deployed, governments all over the world are at a loss as to what to do about the threat they represent. Not only are governments, critical infrastructure, organizations, and consumers being attacked by an onslaught of malicious bots, no world-wide governing body has any real control over the manufacturers of IoT technologies. Unlike electricity, water, and air quality standards that are pretty much applied in most modern countries, there are no cybersecurity standards for consumer-based IoT devices.

As a result of not having any international standards in place for manufacturers of IoT devices and realizing adoption rates and the cyberthreat is real and growing, some governments have taken up initiatives with other governments to at least begin a dialog for cooperation. For example, in early 2016 the [EU-China Joint White Paper on the Internet of Things](#) was released. The whitepaper highlights the following:

Formulation of ten action plans for IoT development: the plans cover various perspectives, including top-level design, standard development, technology development, application and promotion, industry support, business models, **safety and security**, supportive measures, laws and regulations, personal trainings, etc.

This is a move in the right direction.

Beyond this effort mentioned, the US government has started IoT and botnet-related initiatives, as well. For example, in early 2018, [A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats](#) was released for public comment. In the draft, the following is discussed:

¹ Federal Bureau of Investigation, [Public Service Announcement](#); Internet Crime Complaint Center (IC3); 2018.

The opportunities and challenges we face in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes.

Automated, distributed attacks are a global problem

The majority of the compromised devices in recent botnets have been geographically located outside the United States. Increasing the resilience of the internet and communications ecosystem against these threats will require coordinated action with international partners.

Effective tools exist but are not widely used

The tools, processes, and practices required to significantly enhance the resilience of the internet and communications ecosystem are widely available, if imperfect, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.

Products should be secured during all stages of the life cycle

Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.

Education and awareness are needed

Knowledge gaps in home and enterprise customers, product developers, manufacturers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient. In particular, customer-friendly mechanisms to identify more secure choices analogous to the Energy Star program or National Highway Traffic Safety Administration (NHTSA) 5-Star Safety Ratings are needed to inform buying decisions.

Market incentives are misaligned

Perceived market incentives do not align with the goal of “dramatically reducing threats perpetrated by automated and distributed attacks.” Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.

Automated, distributed attacks are an ecosystem-wide challenge

No single stakeholder community can address the problem in isolation.

In the light of the two aforementioned efforts, governments are making strides in the right direction to address the malicious bot issue that the internet ecosystem faces today. However, organizations are still being forced to address the problem on their own by implementing a host of protection mechanisms, as governments try to get their arms around policy that would address the issues without hampering the growth and adoption of consumer IoT.

One word of caution: it is easy to get sucked into all of the hype around the latest threats, and there are a lot of security threats that organizations face. But, there is no need to be in a constant panic mode. It is important for security teams to understand what the latest threats are, how to defend against them, and what the potential exposure of the organization to those threats is. One of the best ways to do that is through threat intelligence.

AI and ML Adoption in Botnets

Some of the most sophisticated threat actors are now incorporating ML into their attacks. This is a dramatic change in the behavior for cybercriminals as they take advantage of ML to launch attacks that imitate nonmalicious behaviors and eliminate the patterns used to traditionally identify malicious behaviors. This section highlights some examples that are affecting organizations today.

One of the earliest adoptions of ML in botnets was in the realm of brute-force password attacks. A brute-force password attack is one in which the attacker tries hundreds, thousands, or even tens of thousands of passwords against a system in an attempt to gain access.

The problem with brute-force password attempts is that they are noisy, with each failed password attempt generating a new log entry, and many systems have timeout security features that will block access to a system if an incorrect password is entered too many times.

To increase their chances of success in brute-force attacks, botnet operators will feed multiple password databases that have been exposed on underground forums into the botnet. The botnet will process the hundreds of millions or billions of entries and identify the most common passwords used. The botnet will then start with those passwords first in an effort to reduce the number of attempts.

As more password datasets are added, the botnet continuously adjusts the common passwords that it tries.

Not as common (but a growing trend) is for botnets to look at regional datasets based on the target location. For example, if the IP address of the target host indicates it is in Pennsylvania, the botnet might change the order in which it tries passwords to include variants of the Pittsburgh Steelers or the Philadelphia Eagles.

A second area of marked growth in AI and ML for malicious purposes is defeating CAPTCHA challenges. This will be discussed further in the next chapter, but attackers have become very good at bypassing CAPTCHA challenges, even those involving object recognition (e.g., identify all pictures containing storefronts).

This is an example of hundreds or thousands of humans providing information into an AI and ML system to make it more effective. Attackers that sell these CAPTCHA bypass systems on the underground market claim up to **98% efficiency at detecting objects in the CAPTCHA photos**.

Although AI and ML has not seen widespread adoption by most attackers, there are definitely some more advanced attackers who are building these technologies into their tools.

Staying Ahead of the Next Attack with Threat Intelligence

Most businesses are, at best, only aware of today's current threats. Even when organizations implement what is believed to be the best security defenses, inadequate security training, staff turnover, and the high volume of threat activity on a daily basis leave most businesses vulnerable to malicious attacks in one respect or another.

Much as today's more aggressive attackers understand this, security analysts, specialists, and executives need to think about what's next. Imagination is needed to envision the threats that are just around the corner. This is where threat intelligence becomes so important to your organization. Many in security view threat intelligence as simply indicators, such as bad IP addresses, domains, or file hashes. But three different types of threat intelligence should be considered: *operational*, *tactical*, and *strategic*.

Operational threat intelligence is intelligence that you can use immediately to stop an attack such as the aforementioned indicators. Tactical threat intelligence provides information about the person or group behind the indicator, with a focus on the tactics, techniques, and procedures (TTPs) of the adversary.

Strategic intelligence, which is our primary focus here, is really about seeing the big picture. It is an understanding not only of what attacks are happening now, but also what attacks might come in the future.

Moreover, strategic intelligence is about understanding the strengths and weaknesses within your organization and what is needed to better protect it against current and future attacks. When talking about strategic intelligence, many organizations panic because they don't think they have the proper resources or vision to "predict the future." But it is not really all that difficult, and many organizations do it without really knowing they are doing it.

Strategic intelligence involves planning for the future based on available information. Very few organizations predicted the **Meltdown and Spectre vulnerabilities** when they were announced. After they were announced, it was logical to assume more vulnerabilities of this nature would be found and take proactive steps to protect the organization from this new category of attack. Similarly, if every month an Adobe Flash vulnerability is announced, it is safe to assume that more will be announced in the future and to take steps to minimize the installation of Adobe Flash within your organization.

Strategic intelligence is not magic. It means that your organization needs to understand the preferred attack methods of today's attackers as well as understand where in the organization you are most susceptible to these attacks. After that information is gathered, your organization can then take smart steps to protect itself from current and future attacks.

To be effective, strategic intelligence must involve every part of your organization and must be driven by senior leadership within the organization to get different departments engaged. If there is any secret to success here, this is it. After buy-in from the top down is in place, you can move forward with your strategic intelligence plans. As we discuss in **Chapter 5**, much of your strategy will center

around the increasing need to move beyond familiar security tools and solutions, as you implement newer approaches to cybersecurity.

AI and ML on the Security Front: A Focus on Web Applications

AI and ML techniques and solutions, combined with automation, are now being used in security for threat detection and remediation. In the case of inbound web application requests, AI and ML techniques are exceptionally useful when it comes to observing, quantifying, and classifying inbound requests based on the degree of maliciousness.

Finding Anomalies

In most cases, ML solutions can develop an understanding of existing vulnerabilities because they are capable of being taught how to recognize potential attacks that could exploit these vulnerabilities. Increasingly advanced applications of AI and ML are not interested in identifying and defending against familiar threats; this is something traditional security systems can often achieve. Instead, AI and ML systems are being deployed to find and classify anomalies. In the case of protecting web applications, AI and ML systems are being used to determine whether an inbound request “appears” to be legitimate traffic or whether it is malicious in nature.

ML techniques eliminate the need to have human analysts spend time on what is already understood, or what are often repeatable and mundane tasks. The machine can handle known and well-documented threats while also homing in on the anomalies and threat indicators that have not been seen before. As a point of refer-

ence, suppose that a website receives 1,000,000 requests per day, and only 100 of those requests are considered unusual, by whatever definition of unusual an organization uses. ML analysis can label those 100 requests as anomalies and highlight them for the security analyst. After they're highlighted, the analyst can now spend more time investigating whether they are truly malicious in nature instead of trying to "find the anomalies" on their own.

In fact, web application monitoring is the perfect use case for ML and AI. It is physically impossible for a single human to review millions of lines of web logs each day looking for anomalies. ML is required to identify unusual behavioral patterns and bring them to the attention of analysts. More important, for common and repeated suspicious behaviors, organizations can use ML to automatically block the traffic and alert an analyst that the problem has been resolved. Not only does this help an organization become more efficient, it can help save money.

In the first scenario, in which ML identifies a potential attack and alerts an analyst, the analyst must investigate to determine whether the attack was real. While that investigation is ongoing, an attacker might have already gained access to an organization's database and might even be downloading sensitive customer or organizational data. In the second scenario, the potential is blocked, and then an alert is generated. The analyst still must investigate, but if the attack turns out to have been a serious one, it has already been stopped. There is no costly data breach, and the attacker has moved on to another target.

AI techniques can also respond faster to vulnerabilities. Techniques that are used with web application firewalls (WAFs) for inbound web requests, for example, would compare all inbound requests against a list of known good and bad requests, regardless of whether they are "known" to be good or bad. This activity can add up to millions of comparisons, and it takes a significant amount of time to examine databases of everything seen in the past and run comparisons with each and every one of them. Instead of comparing one thing with millions of possibilities, AI techniques can rapidly identify a pattern in the requests that can then be analyzed for its threat potential.

The great thing about this process is that it works even for unknown vulnerabilities. For example, in March 2018, many distributed denial

of service (DDoS) protection companies noticed an **uptick in probing of the memcached port (UDP port 11211)**. Memcached is a protocol design to cache data in RAM, which can reduce latency on Linux and Windows servers by reducing the number of remote calls a system is making. Attackers figured out that they could use memcached to launch DDoS attacks, and very few organizations were protected against memcached traffic. DDoS protection providers were able to see those early probes because their AI/ML systems identified those probes as unusual. Thus, they were able to determine that a new type of botnet was being built and put protections in place to stop those attacks when they were first launched.

The following sections offer more specific examples of ML and AI techniques in action.

Bringing ML to Bot Attack Remediation

Much of the bot remediation activity today is still a very manual process. Bots using certain IP addresses or domains are identified, then steps can be taken to bar access by blocking them at the proxy or firewall.

However, the introduction of ML can greatly improve defense capabilities by using external threat intelligence about bot behaviors and combining it with data collected about real traffic samples to learn about new bot patterns. This information is then fed into a ML solution. After a ML solution consumes the various data points, it can be told to run multiple models whereby the human provides training input in an active feedback loop approach. ML solutions in turn can launch automated processes for blocking bot traffic based on the machine's new understanding of what type of bot traffic to now look for. This process is called *active learning with labeled data*, and machine learning solutions can perform this process continuously without growing tired or becoming overwhelmed.

Using Supervised ML-Based Defenses for Security Events and Log Analysis

The use of supervised ML can greatly speed, augment, and assist the work of security analysts and engineers to identify and mitigate exact threat sources. These analysts and engineers are tasked with viewing security events and logs, and then analyzing a multitude of

data points generated from the deployed security controls such as firewalls, IPSs, IDSs, sandboxes, WAFs, endpoint protection platform (EPP) solutions, and privileged access management (PAM) solutions. Combing through collected data to pinpoint specific security threats can take weeks, even months, to accomplish. Taking steps to mitigate the threats takes even longer. Most analysts and engineers already carry a full workload, making it more difficult for them to expand responsibilities. Hiring more resources to ferret out attacks is often not possible. All the while, malicious activities are wreaking havoc on a company's online presence and performance, while damaging business revenue and reputation along the way.

Products are already on the market that employ human-based, supervised ML. For most of these products, an IT security analyst initially provides feedback to the AI engines that are at work scanning massive numbers of log entries to identify anomalous behaviors. The supervised ML system augments the analyst as it's trained to improve detection of "significant events" in the logs and to immediately bring those events to the analyst's attention, which means that your business is more quickly on the path to threat resolution.

Deploying Increasingly Sophisticated Malware Detection

In the case of websites that allow file uploads like pictures, forms, or documents, the traditional website malware detection runs on the servers themselves, and it identifies malicious files that might have already been uploaded to the server. This after-the-fact malware detection might have allowed the malware to cause damage to the application and data files already. Even worse, the malware might not have been detected at all until some user executes it, doing nothing more than spreading more malware internally and to website visitors as well.

We can implement more sophisticated and thoughtful ML techniques in the cloud or at the network edge, and we can apply these techniques to malware detection, as well. This can help identify and stop human and nonhuman malicious activities before they go beyond the edge to the servers and applications sitting behind.

Using AI to Identify Bots

Analyzing the user's behavior as they visit a website or application is one way to protect against the invasion of nonhuman visitors; in other words, bots. In the past, nonhuman activity was rarely identified, and there were only rudimentary bot challenges like CAPTCHA, which are still so often used today. However, all of that has changed. Today there are better bot challenges used for detection, such as JavaScript challenges, human interaction challenges, and device fingerprint challenges. And these challenges are getting better at detecting bot activity.

ML-based bot management solutions can be capable of automatically tweaking the existing bot challenges to improve detection rates. They can also identify what existing or new bot challenge is needed to defeat a particular bot that uses a repeating tactic or displays a certain pattern of activity. ML-based bot management solutions are definitely needed to defend against that massive rise in malicious bot traffic due to the steady stream of compromised consumer Internet of Things (IoT) devices—turned into malicious bots.

Today, security analysts can implement various bot challenges on a moment's notice, identifying normal usage patterns for each web application based on legitimate user and visitor behavior analysis, and provide customizable security postures for bots that deviate from the standard usage behavior, activity, or frequency. These technologies are available today, and ML is only making them better.

Of course, AI and ML have uses beyond the realm of bot and botnet protection. [Chapter 6](#) focuses on some other areas of security where AI and ML can drive success.

AI and ML on the Security Front: Beyond Bots

AI and ML aren't just useful for bot detection and remediation; they are also used to improve a wide variety of security challenges. This chapter discusses some of the areas where AI and ML are making a big impact in security.

Identifying the Insider Threat

Users have established patterns of behavior within a network. They log in at a certain time, log out at a certain time, visit the same systems within the network, and generally communicate to the same places. But sometimes those patterns change. The pattern might be a one-time thing, such as someone who jumps in to help accounting toward the end of the quarter, or it might be a permanent change because of new job responsibilities. Of course, sometimes that change in behavior is because the user is accessing systems they shouldn't for malicious purposes. This is what is known as an *insider threat*, and it is a real challenge for security teams to deal with.

How can your security team examine millions of lines of logs and network traffic flow data to look for patterns that indicate whether a change in behavior is malicious or part of the regular workflow? There is a framework created around this type of analysis called user and entity behavior analytics (UEBA) that tracks the behavior of users and systems within an organization. UEBA looks at traffic

flows, as well as roles and responsibilities, and alerts on any behavior outside the norm.

For example, a human resources professional should never have a reason to log in as an administrator to a mail server. When UEBA tools detect that type of access, an alert is sent. Similarly, a server that is designated as an internal monitoring server should not be sending thousands of emails to external addresses. When that behavior is detected, an alert is sent.

UEBA tools rely heavily on AI and ML—along with constant feedback and updates from the team that maintains the UEBA system—to comb through millions of events to find anomalous activity that could indicate an insider threat or an attacker impersonating an internal user.

Tracking Attacker Dwell Time

Another significant problem to examine is the issue of *attacker dwell time*, which indicates how long an attacker has remained resident in a network without being detected. Attacker dwell time is most often associated with advanced persistent threat (APT) actors. APTs are attackers, often, but not always a nation state, that use advanced tactics and techniques to avoid detection while within a target network. Rather than a typical “smash and grab” operation, APTs will spend months or years within a target organization until they get the specific information they want.

APTs take their time going from internal system to internal system in order to steal data, commit fraud, and cause disruptions. After an attacker has gained access, it is very difficult to detect their activity. Their back-door traffic often looks like every other piece of traffic from an internal perspective. This is due to the fact that the attack has already happened, the back door has been opened, it has remained open, and no one has detected it yet.

Most attacker-related data breaches today come in two fashions. The attacker either comes in the front door and attacks the applications that are exposed to the internet, or the attacker compromises and takes over an internal computer through a phishing attack. In the latter case, the attacker has complete control over an internal system and can remain in constant communication with that system from

anywhere in the world, with its own communications with that system going right through any edge defenses in place.

Detecting APTs and their back-door communications are also a perfect task for AI- and ML-enabled traffic monitoring tools. To the normal human analyst who looks at traffic statistics all day, trying to find the one system that is being controlled remotely by an attacker is nearly impossible using the simplistic traffic monitoring tools on the market today. However, AI and ML can enable monitoring tools of the future that could potentially detect an APT within minutes.

Orchestrating Protection

Another area that has been greatly aided by the addition of AI and ML is the security orchestration, automation, and response (SOAR) market. The SOAR market, which includes vendors such as Phantom (now part of Splunk), Swimlane, and Komand (now part of Rapid7) could not exist without ML capabilities. SOAR technologies use ML to automate the security response to common incidents.

For example, well-known commodity Trojans are often more of a nuisance than a real threat to an organization, but they must be dealt with when one manages to elude the security protections in place. Rather than waste the time of a security operations center (SOC) analyst removing the Trojan, the SOAR tools can automatically block the Trojan and then initiate whatever cleanup steps that need to be taken (wipe and restore the infected machine, disconnect it from the network for further analysis, etc.). SOAR tools work in conjunction with the security, IT, and helpdesk teams to learn the processes and procedures in place to deal with different types of security incidents and then take over those responses that can be automated.

As procedures are put in place to deal with new threats, the SOAR tools ingest that information and adapt to the new procedures and act accordingly. The most effective orchestration tools are those that are able to connect with all security and networking systems within an organization. This allows the SOAR platform to have the maximum visibility of the organization and allows it to automate as many low-level security tasks as possible.

ML and AI in Security Solutions Today

Many of the security products in your organization today, including security information and event managers (SIEMs) such as Splunk, ArcSight, and AlienVault; managed security service providers (MSSP); and advanced next-generation antivirus solutions from providers such as Carbon Black and Cylance offer some sort of AI and ML capabilities. You might not even know that they are using AI and ML because these abilities are hidden below the surface, operating in the background to continuously improve the performance of these products, based on feedback from your team.

Many providers will tout that their products and solutions are “intelligent” and include ML and AI components. Not all of these products allow security teams to directly interact with the ML and AI capabilities. The AI and ML can be fed into the system by the security company’s own analysts, thus presenting the equivalent of an AI and ML black box to their customers. This is not necessarily a bad thing, given that many security teams are not ready for a full AI and ML integration, but this is a good conversation to have with all your vendors, whether that is with new vendors or when it is time to renew existing vendors. The goal is that your organization wants to have vendors that can grow with your team as you move to incorporate more AI and ML into your daily workflow.

ML and AI Case Studies

The discussion in this book has been relatively abstract to this point. With new technologies, such as AI and ML, it can be difficult to picture how these tools will improve the efficiency and workflow of your security team. More important, it can be difficult to understand how using these tools can help you save money or at least get a better return on your investment. This chapter presents one case study that focuses on the use of AI and ML to detect and mitigate a sophisticated bot attack. This type of attack is a common problem and is an especially good fit for AI and ML technologies, as well as being easy to implement.

Case Study: Global Media Company Fights Scraping Bots

To better understand how AI and ML can thwart malicious bots, this case study discusses how a global media company with a large marketing presence that includes more than 50,000 websites and which runs more than 20,000 pay-per-click campaigns (Figures 7-1 and 7-2) at any given time took preventive action when experiencing a high volume of sophisticated scraping bots.

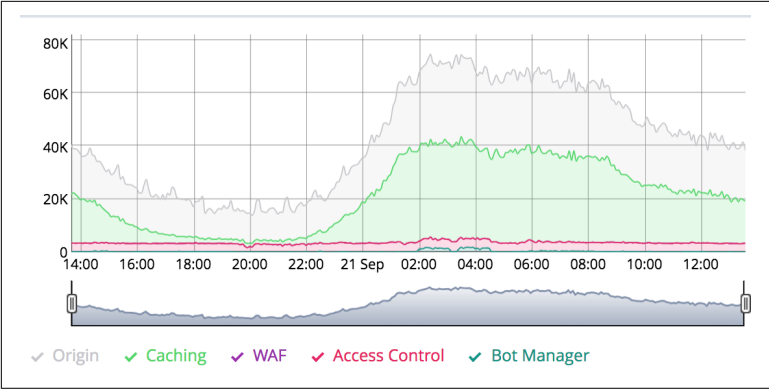


Figure 7-1. Typical traffic from the customer (number of HTTPS Requests per 5 minutes, over 24 hours). Note that the figure also shows blocked attack traffic (traffic identified by the WAF, Access Control, and Bot Manager are blocked) and caching performance (in green)

Country	Requests	Traffic
United Kingdom of Great Britain and Northern Ireland	7M (58%)	91.01 GB (36%)
United States of America	4M (31%)	147.36 GB (59%)
France	803k (6%)	1.52 GB
Ireland	148k	2.25 GB
India	114k	1.63 GB
Poland	48k	0.65 GB
Germany	41k	0.34 GB
Australia	41k	1.40 GB
China	28k	0.79 GB

Figure 7-2. Typical traffic from the customer (number of HTTPS Requests over 24 hours)

A scraping bot is one that visits a website and grabs content to repurpose it on another site. This is a common tactic used by disreputable “news” websites. Rather than create original content, they steal content from other sites and post it as their own. These deceitful news sites then use “shady” search engine optimization (SEO) techniques to elevate their sites in search engines. So, not only are they stealing content, they are also stealing clicks away from legitimate sites that produce original content. This type of activity is sur-

prisingly common. Take a paragraph from almost any story on a news site and run it through a search engine, and there will often be dozens of clones of that story on sites with domains that are just slightly off.

The Problem

The onslaught of malicious bots was stealing data from the media company's sites and providing that data to third-party competitors, negatively affecting revenue streams and diluting brand recognition. However, this wasn't just a matter of copyright theft, there was also resource theft. The high volume of nonhuman traffic impeded the user experience and increased the number of servers needed to handle the onslaught of requests. This increased hardware spending on web services 100% year over year, but the increase in expenditures was necessary to ensure that sufficient resources were available to handle the significant load.

A traditional web application firewall was unable to solve the problem, because these web scraping bots, at least at first glance, look like legitimate traffic. When a normal user visits a website, the web browser makes what is called a "GET" request. The GET request does just what it suggests: it "gets" the requested content. For example, a visitor to the CNN home page will, temporarily, download all the content on the front page, and any article the visitor clicks will also be downloaded as part of the HTTP/HTTPS transaction. That is how the web browser can render the HTML content for the visitor.

Human versus Bot Behavior

Sometimes, there are significant differences. A legitimate user stays on a rendered page for several seconds or longer as that user is reading the content. Then, they might click one or two links from the main page (more if the site is particularly good at keeping visitors) and stay on each of those pages for several seconds or longer to read the content.

Typically, bots do not do that. When a bot visits a targeted web page, it often immediately begins visiting links that are on that page to grab as much content as possible, as quickly as possible. A bot might spend a fraction of a second on a page and will visit hundreds or thousands of pages while on a site. Such a bot can be easily identi-

fied and blocked using real-time, behavior-based analytics, as illustrated in **Figure 7-3**. The behavior of the end user is determined by looking at time spent on page, links clicked by the user, scrolling actions, historical pages visited, to name just a few examples.

Human Interaction Challenge
Human Interaction Challenge is an advanced countermeasure that looks for natural human interactions such as as [redacted]

Actions to be taken for detected bots
Choose appropriate actions to take for any bots detected utilizing Human Interaction Challenge.

Action threshold
Specify the number of failed requests before taking action.

Threshold expiry period
Number of seconds before threshold expires.

Action expiry period
Number of seconds between challenges to the same IP address.

NAT Support
When enabled, a unique hash is added to the IP Address expiration time, which prevents the blocking of visitors with shared IPs.

Interactions threshold
The number of interactions required for passing the challenge.

Interactions threshold
The number of interactions required for passing the challenge.

Recording period
The number of seconds to record the interactions from the users.

☒ Enable Human Interaction Challenge

Actions to be taken for detected bots
☐ Alert only [?](#)
☐ Block with error page [?](#)
☐ Block with response code [?](#)
☒ Show captcha page [?](#)

Action threshold
 requests [?](#)

Threshold expiry period
 seconds

Action expiry period
 seconds

☒ NAT Support

Interactions threshold
 interactions

Recording period
 seconds

Figure 7-3. Behavioral analysis setup

Some more advanced bots have become better at hiding their tracks. They will spend longer periods of time on each page in order to better mimic real visitor behavior, and they will also divide the scraping of subpages among hundreds of bots so that it doesn't look like one IP address is doing all of the scraping. Even then, with a close examination of traffic, and knowing what to look for, it is possible to distinguish bot visitors from human visitors, as shown in **7-4**. But doing so “on the fly” requires AI and ML.



















IP	Country	Requests	Ratio
[REDACTED]	 United Kingdom of Great Britain and Northern Ireland	1,320	[REDACTED]
[REDACTED]	 United States of America	540	[REDACTED]
[REDACTED]	 United States of America	357	[REDACTED]
[REDACTED]	 Bangladesh	350	[REDACTED]
[REDACTED]	 United States of America	298	[REDACTED]
[REDACTED]	 United States of America	292	[REDACTED]
[REDACTED]	 United Kingdom of Great Britain and Northern Ireland	195	[REDACTED]
[REDACTED]	 Netherlands	194	[REDACTED]
[REDACTED]	 China	135	[REDACTED]
[REDACTED]	 Pakistan	130	[REDACTED]
[REDACTED]	 United States of America	66	[REDACTED]
[REDACTED]	 United States of America	55	[REDACTED]
[REDACTED]	 United States of America	51	[REDACTED]
[REDACTED]	 United States of America	51	[REDACTED]
[REDACTED]	 United States of America	47	[REDACTED]
[REDACTED]	 United States of America	44	[REDACTED]
[REDACTED]	 United States of America	43	[REDACTED]
[REDACTED]	 United States of America	38	[REDACTED]

Figure 7-4. A sample of IPs from identified malicious bots over a period of a few hours.

Remember, no matter how much time and effort an attacker invests in building a botnet to mimic legitimate traffic to a website, the one thing that attacker doesn't have is the metrics on how visitors to the site engage with the web applications. As long as you have that information available, it is possible to detect bot traffic—even advanced bot traffic, using AI and ML.

Bot Management

In this case, the media company implemented a layered bot manager solution that incorporated analytics and controls, combined with an extra layer of ML, based on input from a data science team.

Human Interaction Analysis: 90% Were Bots

A human interaction bot mitigation (based on behavior analysis) was able to block about 90% of the suspicious activities, as depicted in **Figure 7-5**. The remaining 10% required a much more sophisticated ML approach.

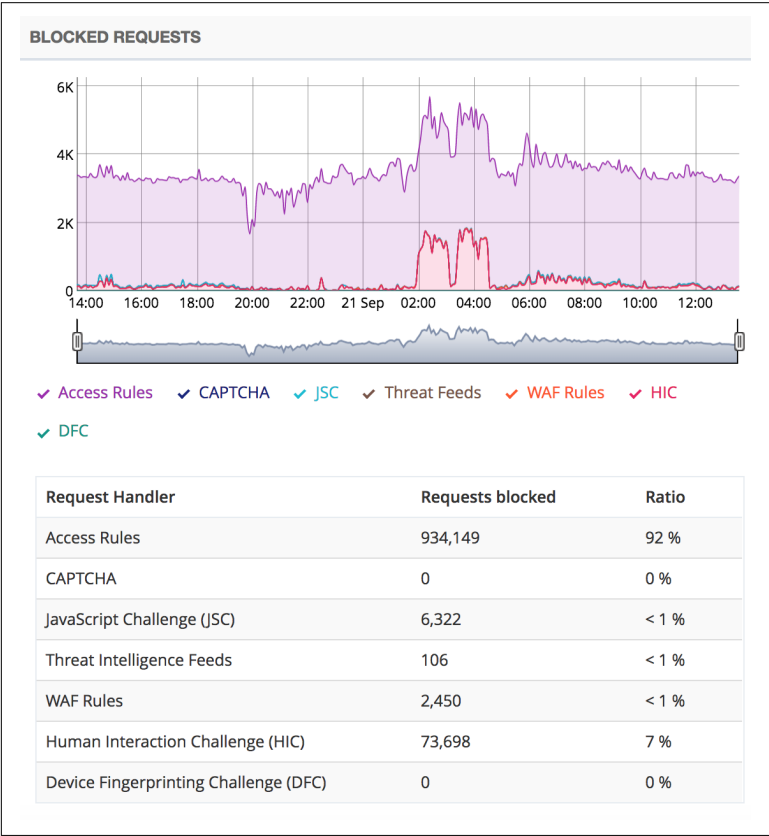


Figure 7-5. Requests blocked by Human Interaction Analysis. Note that about 7% of the traffic is blocked by a Human Interaction Challenge.

The global media company’s client traffic pattern displayed a spike in malicious bot activity blocked by Human Interaction Challenge (HIC). Note also that a very large number of blocked requests were coming from compromised hosts. Access rules block users based on threat intelligence database that contains a very large number of known compromised users (based on IP addresses).

JavaScript challenge

About 8% of identified malicious bots were blocked by simple *JavaScript Challenge*. JavaScript Challenge identifies visitors that do not have a browser with a full JavaScript engine (typical of crude bots). This bot challenge does not use behavior analysis and is typically useful to prevent large-scale DDoS attacks and small “background noise” attacks.

The complex bots were identified (see Figures 7-6 and 7-7) when they failed the bot management solution’s HIC. This challenge identified normal usage patterns for each web application, based on expected visitor behavior that was provided by analysts. Customized security postures were deployed to stop bots that deviate from the standard usage behavior using a combination of anomalous and behavioral analysis, as shown in Figure 7-6.

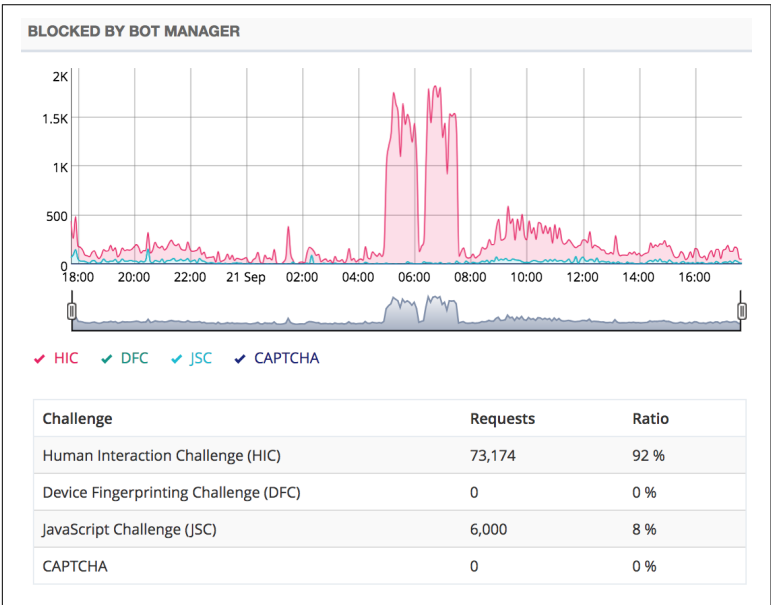


Figure 7-6. The Human Interaction Challenge (labeled HIC in the graph) blocked 92% of identified malicious bots. JavaScript Challenge blocked the remaining 8%.

As a result, the company was able to identify and isolate the highly advanced bots that were able to bypass traditional bot management and mitigation techniques.

It would not stop...

Advanced bot protection has now been in place for more than months, but the attackers are still sending daily bot traffic, even though the site is now being well protected.

Limiting resource utilizations

There is also an unexpected benefit to the enhanced bot protection. The company’s image store infrastructure had been strained due to the massive amount of static content that the sites were expected to serve to its global user base.

Also, as expected, most of the bot traffic represents uncacheable search from the site; hence, it shows a disproportionate workload for the web servers.

The caching functionality (included with the botnet protections implemented) dramatically reduced the load on infrastructure (see [Figure 7-7](#)), providing much-needed headroom while the organization continued to upgrade its infrastructure.

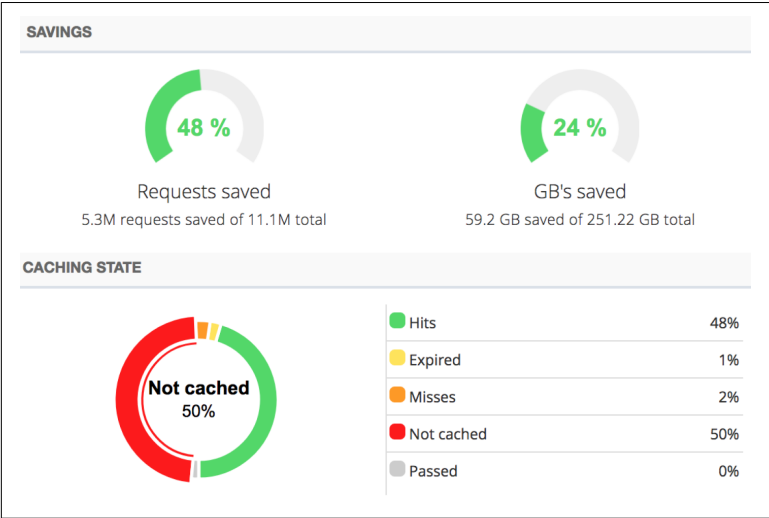


Figure 7-7. Caching improvements created by the bot management solution.

When Nothing Else Works: Using Very Sophisticated ML Engines with a Data Science Team

For this organization, there were about 20,000 suspect requests over a few days (from a total of 56,000,000 legitimate requests over the same period). Those suspect requests came from many IP address, with a clear pattern: the same IP/user would systematically go through the entire subcontent of the site and never come back and then be replaced by another IP looking for different subcontent.

The traffic would come from apparently legitimate user agents, as shown here:

```
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/62.0.3202.75 Safari/537.36"
```

A data science team applied an unsupervised ML algorithm to see whether the pattern of these 60,000 requests could be identified. This is what was found:

- The attack traffic was interspersed within the legitimate traffic, spread over several hundred IPs. Graphical analysis of the attack was inconclusive (that is, human analysts were not able to see visual patterns), as demonstrated in [Figure 7-8](#).

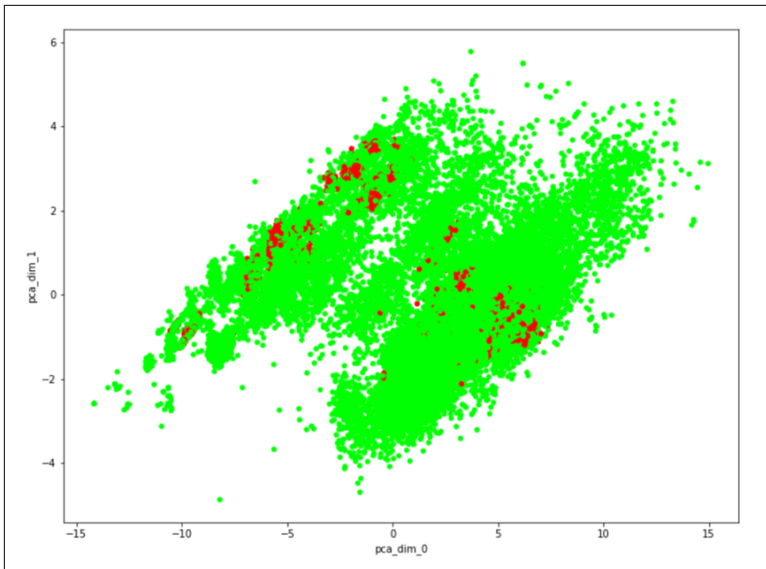


Figure 7-8. Example of attack traffic (in red) and legitimate traffic (in green), using a data visualization tool (x and y are irrelevant for this exercise, the goal is to identify patterns).

- The ML platform finally identified a very strong pattern (with a correlation of almost 100%, the pattern represents almost all the attack traffic), using vectors of more than 120 elements (that is, more than 120 different pieces of information define an attack request). The pattern could only be identified over a space of 120 dimensions, as shown in [Figure 7-9](#).

name	gabor_id	malicious	accept	accept-charset	accept-encoding	accept-language	accepts	alexatoolbar-abx_ns_ph	authority	authorization	...
0	0	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
1	1	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
2	2	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
3	3	0	1.0	0.0	1.0	1.0	0.0	0.0	0.0	0.0	...
4	4	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
5	5	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
6	6	0	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
7	7	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
8	8	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
9	9	0	1.0	0.0	1.0	1.0	0.0	0.0	0.0	0.0	...
10	10	0	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
11	11	0	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
12	12	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	...
13	13	0	1.0	0.0	1.0	1.0	0.0	0.0	0.0	0.0	...
14	14	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
15	15	1	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...
16	16	0	1.0	0.0	1.0	1.0	0.0	0.0	0.0	0.0	...
17	17	0	1.0	0.0	1.0	0.0	0.0	0.0	0.0	0.0	...

Figure 7-9. Example of a vector that defines the pattern of the attack traffic.

Correlated elements

The highest correlated elements of the vector represent a random sort group of headers and header content (certain sorts of HTTPS headers and values can represent the main part of the attack traffic), as shown in [Figure 7-10](#).

	sorted_header_names	unsorted_header_names	mean_malicious	count
0	accept,accept-encoding,cookie,host,upgrade- code,x-f		1.000000	1544
1	accept,accept-encoding,host,upgrade- requests,		1.000000	423
2	accept,accept-encoding,cache- control,cookie,host,pragma,referrer,service- worker,forwarded-for		1.000000	364
3	accept,accept- encoding,cookie,host,referrer,upgrade- requests,user-agent,x-client-ip,x-country-code,x- forwarded-for		1.000000	259
4	accept,		0.937536	3506
5			0.923567	9106
6	accept,accept-encoding, user-agent,x- client-ip,		0.744928	345

Figure 7-10. Main elements of the traffic vector, with correlation to the attack traffic.

After the ML engine was deployed in production, the platform was able to identify almost all malicious traffic with only a few false positives, as illustrated here:

	predicted_malicious_0	predicted_malicious_1
malicious_0	81947	1016
malicious_1	0	14544

The Results

The bot management solution allowed the media company to mitigate attack traffic using several strategies: ML-based, automated HIC (a behavior-based analysis of the traffic) and sophisticated, supervised ML that prevent traffic that corresponds to a pattern that is hard for humans to visualize. This was represented by vectors of

more than 120 elements. Such ML was applied by a specialized team of data scientists.

At the same time, the company was able to apply controls to restrict resources (bandwidth and CPU) allocated to illicit traffic. The company continues to work closely with the managed services provider that provided the cloud-based bot management solution in order to research and identify increasingly advanced—and, in many cases, custom—malicious bots and other targeted attacks.

Looking Ahead: AI, ML, and Managed Security Service Providers

Chapter 5 discussed how AI and ML are improving bot detection, whereas **Chapter 6** discussed other areas in security for which the introduction of AI and ML has had a real impact. This chapter examines how managed security service providers (MSSPs) are incorporating these technologies, developing AI and ML techniques of their own and how that can benefit your organization. Your organization might not be ready to adopt AI and ML solutions in-house—given the many challenges associated with AI and ML and the fact that most security teams are already overworked, the idea of adding new capability seems daunting. However, by using an MSSP, your organization can potentially reap the benefits of the investment that the MSSP has made in AI and ML technologies. Just as with anything else in security, a successful partnership with an MSSP does require work on your end, but it can help improve your organization's security posture.

The MSSP as an AI and ML Source

MSSPs have always had an inherent advantage when it comes to security: rather than protecting a single organization from attacks, the MSSP is protecting hundreds or thousands of clients from all types of attacks. The security operations center (SOC) analysts who work for MSSPs are presented with thousands of different attacks at any time, and they work with organizations ranging from sprawling

government agencies to small businesses. This means that the SOC analysts not only need to be able to quickly pivot from one attack type to another, they also need to be able to pivot from one environment, including the level of experience of the security person or team in that environment, to another.

That is why, over the years, MSSPs have developed the use of independent layers of threat detection techniques. Many of these MSSPs have had to build AI and ML solutions in-house to process billions of security events across thousands of different security solutions every hour. The results of that AI and ML becomes operational, tactical, and strategic threat intelligence that gets fed back into monitoring systems for all customers and allows MSSPs to quickly respond to a customer threat and alert that customer in a manner in which the customer can process and act on the event.

Technologies such as anti-DDoS systems, web application firewalls (WAFs), and bot management solutions are fully capable of consuming operational and even tactical threat intelligence and can be used not only to detect threat actors, but also to stop their activity. This allows MSSPs to share information garnered from monitoring one customer's systems with all other customers, irrespective of whether the other customers have the same system. Almost all of this is invisible to the customer, unless an alert is triggered.

More importantly, MSSPs are often incentivized to share what they have learned (without attribution, of course) not just with their customers, but with the broader internet. Through blogs, conference presentations, and white papers, MSSPs are helping customers and noncustomers alike better protect themselves against the most advanced bots.

MSSPs have been taking advantage of AI-enabled log management systems and tools to find the critical events that are of the highest importance. Some of the events could indicate that attackers are probing targeted victims in search of ways to get in. Other events could suggest that an attack is currently underway or indicate that an attack has already occurred, and the attacker has achieved a foothold.

Time is of the essence when it comes to identifying and halting malicious activity. Believe it or not, according to a report by Trustwave, “the median number of days from the first intrusion to detection of the compromise decreased to 49 days in 2016 from 80.5 days

in 2015, with values ranging from zero days to almost 2,000 days (more than five years).”¹

What this means is that the time from a system being taken over to the time it's detected is currently being measured in months, not minutes. Most organizations that have been breached allow an attacker to remain resident in their networks for days, weeks, months, or even longer. Again, the promise of AI and ML enable advanced persistent threat (APT) detection technologies that are likely to help reduce the attacker dwell time to days, hours, or even seconds. That is another advantage that an MSSP brings. The MSSP SOC monitors its customers' security stack 24/7/365 and is constantly on the lookout for new types of intrusions. The MSSP SOC staff knows about new tactics long before most in-house SOCs do, and they apply that knowledge, using AI and ML, to all of their customers.

Cloud-Based WAFs Using AI and ML

WAF appliances installed within the data center were, for the longest time, a standard requirement for many enterprises to combat malicious traffic at the network layers. In recent years the static, appliance-based WAF has been replaced by cloud-based WAF offerings. Cloud-based WAFs provide additional scalability, cost-effectiveness due to a lack of hardware spend, and the flexibility of real-time updates from the threat intelligence team that operates the cloud-based WAF. Because of the proliferation of malicious application layer attacks, such as volumetric DDoS and content scraping, cloud-based WAFs have almost become a requirement. Their ease of deployment, flexibility, expandability, and ability to rapidly deploy protections against newly discovered threats has made them an indispensable tool for any organization looking to protect their web applications.

As the frequency and breadth of application layer data breaches continue to increase throughout 2018, the use of cloud-based WAFs is likely to surge in lockstep. Investments from cloud providers to expand the functionality of their respective WAF offerings should drive a shift away from deploying third-party virtual machines

¹ 2017 Trustwave Global Security Report

(VMs) toward adopting proprietary alternatives. That will still be able to take advantage of well-recognized rule sets from pure-play security vendors such as Alert Logic, Fortinet, and F5. The use of ML and AI to bolster WAF rule sets and reputation feeds will increase, ensuring that applications are up to date with the most recent patches to better defend against previously unknown threats.

Addressing the Application Security Challenge

One of the greatest challenges of web application security is securing applications appropriately, without blocking good traffic. It is actually quite the balancing act for those configuring and tuning edge defenses. For example, WAFs often take months to tune effectively, while at the same time DevOps groups are turning out application updates at intervals that are outpacing their SecOps counterparts. This is where AI and ML comes in.

With AI and ML, operators can teach the WAF to get better at its job by reducing false positives and negatives; in an extremely short period of time. The time to tune a ML-enabled WAF is often in measured in hours not months, and those that embrace the technology are beginning to stay ahead of DevOps—and attackers, as well.

In truth, exploited application vulnerabilities are the primary cause of web application data breaches, and WAFs are one of the most difficult technologies to use effectively. As today's security vendors begin to embed AI and ML functionality into their cloud-based WAF technology, they are enabling the human-computer synergy so badly needed in web application security. WAF vendors who are not embracing AI and ML for a host of different reasons will eventually go by the wayside, like their first-generation firewall counterparts.

Conclusion: Why AI and ML Are Pivotal to the Future of Enterprise Security

There is no doubt that AI- and ML-enabled technologies are already a critical part of many security team's arsenal. Despite the hesitation many in security have around AI and ML, especially as buzzwords, the fact is that many security tools are already using AI and ML behind the scenes. There are just too many new and evolving threats for even the largest security team to effectively track them. AI and ML allow security vendors and security teams to focus on their core mission while letting the AI and ML do the bulk of the grunt work to build better security solutions.

Here are some steps that organizations can follow when adopting AI and ML:

- Embrace AI and ML approaches
- Agree that this is where security is going
- Develop a team to investigate the feasibility of using what is available now
- Stay abreast of what is coming
- Document and track all your research and findings.

AI and ML might become very important because of regulations like General Data Protection Regulation (GDPR) in the European

Union, The Personal Information Protection and Electronics Documents Act in Canada, the California Consumer Privacy Act of 2018, and other regulations that are likely coming soon. An organization must do everything possible to protect the consumer-based data it maintains. Organizations that fail to do so will face huge fines.

However, what most organizations don't realize is that these regulations do not advise on what types of technology are needed to protect the data of their customers and employees. The regulations broadly state that it is the responsibility of the organization to do everything possible to keep applications and data secure. Reading through the specific language used in these regulations, you will often find terms such as "reasonable security procedures," "appropriate practices," or "nature of the information to protect." What this means is that an organization that has been breached will need to demonstrate, most likely in a court of law, that everything possible was done to protect the personally identifiable information and other data it stores. This completely hints at the concept of *due care*, which is defined as the effort made by an ordinarily prudent or reasonable party to avoid harm to another.

One can easily envision the courtrooms of the future in which the defendants will be CISOs, CIOs, and CEOs of major corporations standing in front of a jury of their peers—or even worse, standing in front of a group of their government legislators—trying to explain why they did not exercise due care similar to their peers. It doesn't take a lot of imagination to envision this, just look at Mark Zuckerberg's (CEO of Facebook) or Richard Smith's (former CEO of Equifax) testimony in front of Congress.

Moving forward, as AI and ML become embedded in the existing tools in use today, or the new tools making their way to the market with AI and ML already baked in, highly skilled human operators will still be needed to understand how to use the tools to their fullest ability. Just as pilots understand their aircraft to an extreme degree, security professionals will need to understand the AI- and ML-enabled tools at their disposal. Or to put it another way, no one shows up to a modern-day battlefield carrying a spear.

The future of AI-enabled security is quite promising. Organizations are already beginning to understand how to operate their human-computer, AI- and ML-enabled defenses more like pilots operate their fighter jets.

In that spirit, attackers beware. Modern-day cyberpilots are getting better equipped and becoming much smarter at defeating your attacks.

About the Authors

Laurent Gil runs product strategy for internet security at Oracle Cloud. A cofounder of Zenedge Inc., Laurent joined Oracle Dyn Global Business Unit in early 2018 with Oracle's acquisition of Zenedge. Prior to that, Laurent was CEO and cofounder of facial recognition software and machine learning company, Viewdle, which was acquired by Google in 2012.

Laurent holds degrees from the Cybernetic Institute of Ukraine (Doctorate Honoris Causa), the Wharton School of Business (MBA), Supélec (M.Sc., Computer Science and Signal processing), the Collège des Ingénieurs in Paris (post-graduate degree, Management), and is Summa Cum Laude of The University of Bordeaux (B.S. Mathematics).

Allan Liska is a solutions architect at Recorded Future. Allan has more than 15 years experience in information security and has worked as both a blue teamer and a red teamer for the intelligence community and the private sector. Allan has helped countless organizations improve their security posture using more effective and integrated intelligence. He is the author of *The Practice of Network Security, Building an Intelligence-Led Security Program* (Syngress) and *NTP Security: A Quick-Start Guide* (Apress), and the coauthor of *DNS Security: Defending the Domain Name System* (Syngress) and *Ransomware: Defending Against Digital Extortion* (O'Reilly).