HOW MALWARE AND BOTS STEAL YOUR DATA

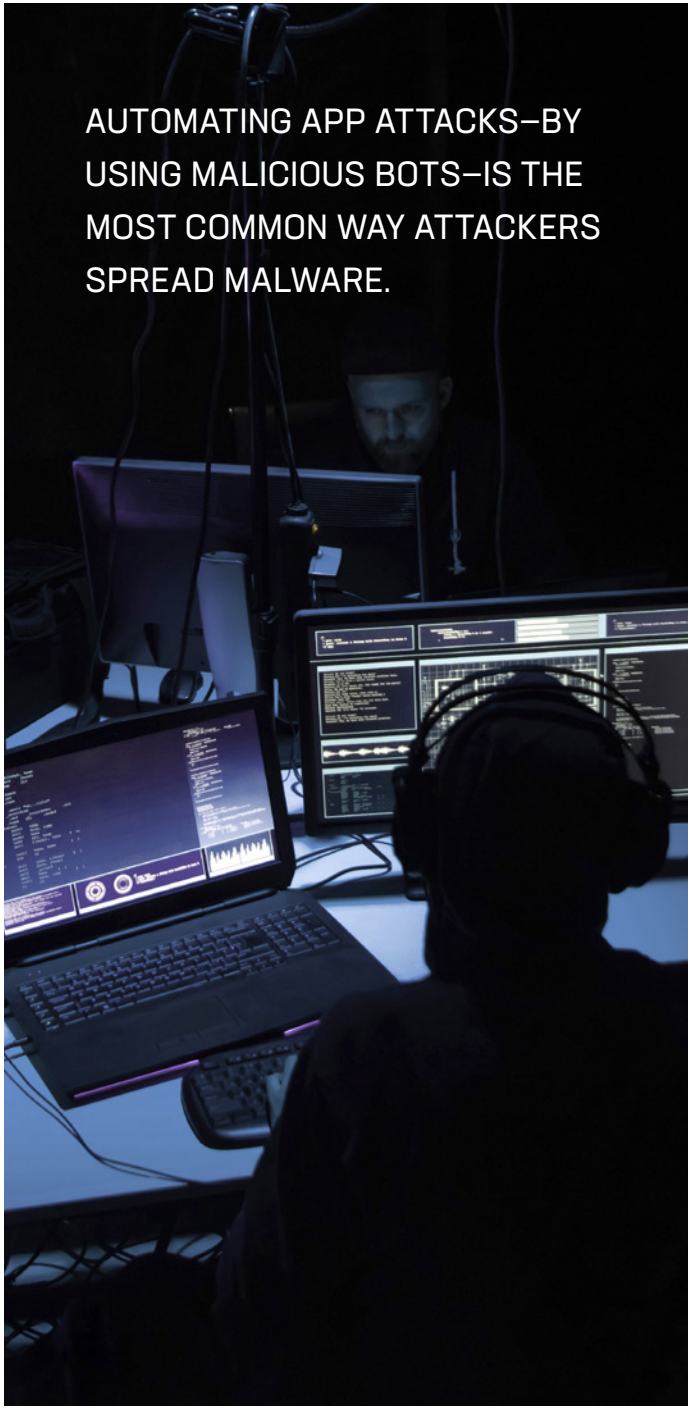
THINK APP SECURITY FIRST

INTRODUCTION

Tech advances like the cloud, mobile technology, and the app-based software model have changed the way today's modern business operates.

They've also changed the way criminals attack and steal from businesses. Criminals strive to be agile in much the same way that companies do. Spreading malware is a favorite technique among attackers. According to the *2019 Data Breach Investigations Report*, 28% of data breaches included malware.[1]

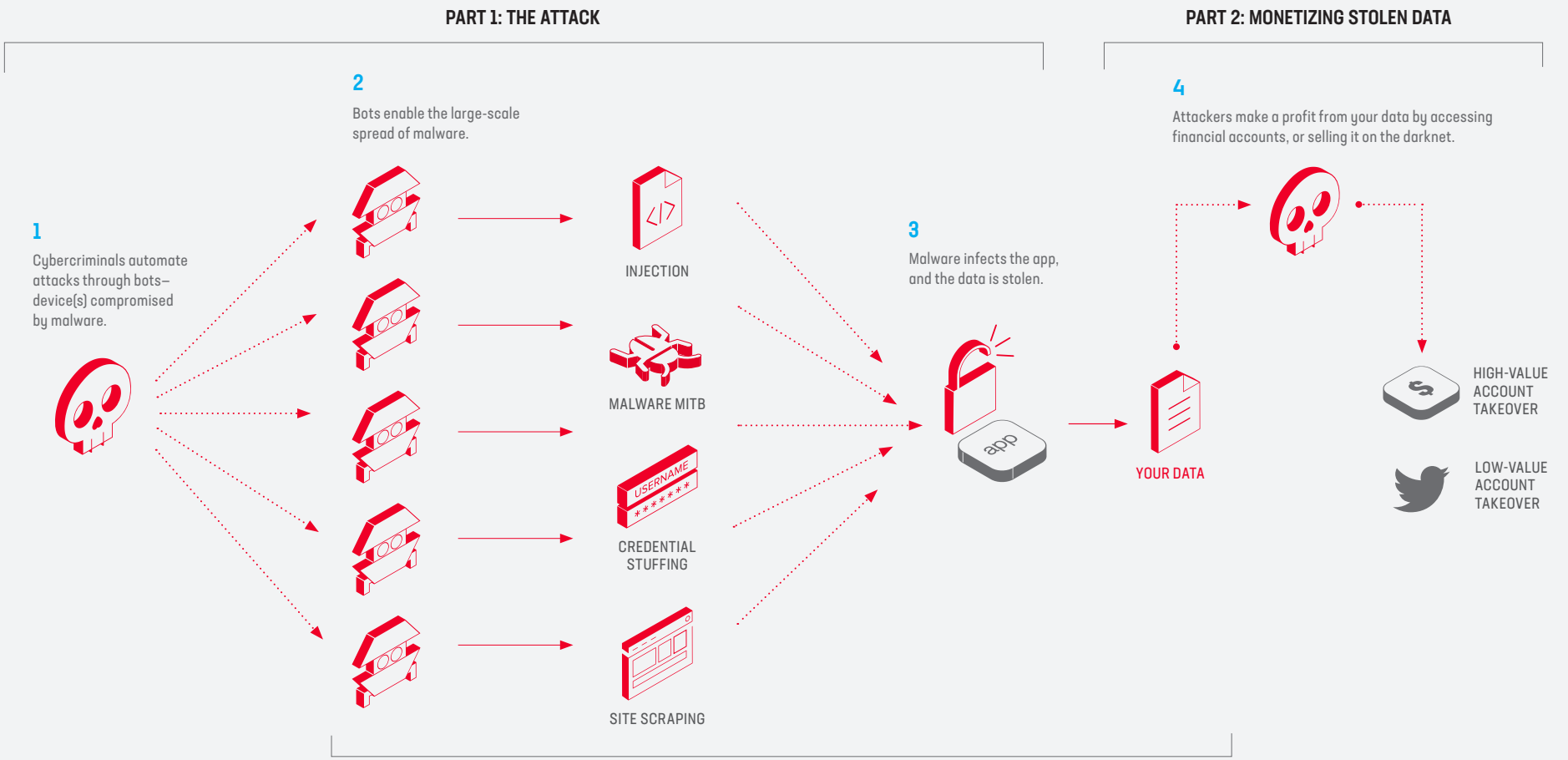
While malware's pervasiveness may not come as a surprise to many people, what's not always so well understood is that automating app attacks—by means of malicious bots—is the most common way cybercriminals commit their crimes and spread malware. It helps them achieve scale.



[1] https://enterprise.verizon.com/resources/reports/dbir/

AUTOMATION OF APP ATTACKS WITH MALICIOUS BOTS

Criminal schemes have two fundamental parts: the technical attack (hacking) and the monetization scheme.



50K 50K CUSTOMERS WERE VICTIMS OF BOT-DRIVEN MALWARE [2]

[2] https://enterprise.verizon.com/resources/reports/dbir/

1. THE ATTACKS: HOW MALWARE-INFECTED BOTS STEAL YOUR DATA

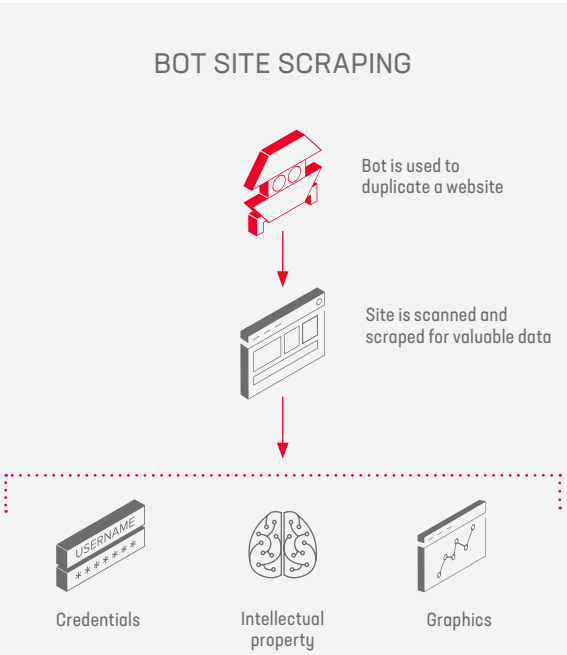
Malware is a general term that includes any piece of malicious software (virus, worm, spyware, ransomware, trojan, rootkit, etc.) designed to pose a threat to users. Bots, those autonomous programs that automatically carry out simple, repeatable tasks, are the medium for attackers to spread the malware. While the tactics, techniques, and procedures vary, each criminal scheme has two fundamental parts: the technical attack (hacking the system and stealing the data) and the monetization scheme (the exploitation of the data).

Let's take a look at some of the ways cybercriminals use malware and bots to compromise the integrity of your applications and steal private data.

BOT SITE SCRAPING

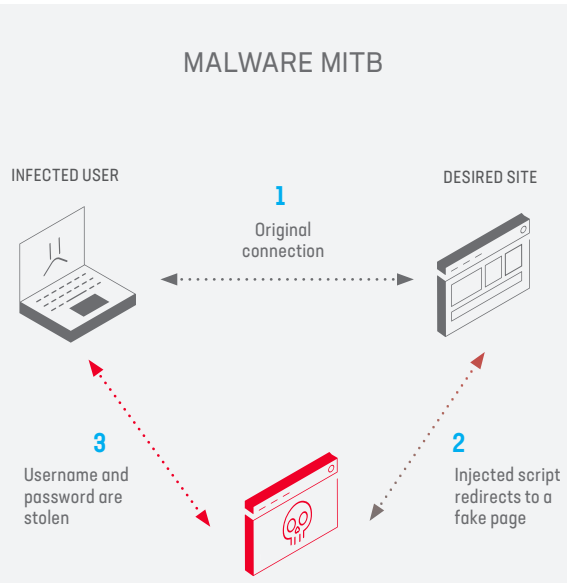
Starting in 2016, automated traffic surpassed human generated traffic on the internet. Not all bots are bad, but in the hands of cybercriminals, these autonomous programs can be used for any number of malicious purposes. For example, it's easy to use a bot to duplicate a website, which can then be scanned for pricing information (which can be sold to competitors), intellectual property such as videos or PDFs, email addresses or usernames that are sometimes hidden in web code, and logos or graphics, (which could help an attacker design a realistic phishing site).

Attackers can also use bots to scrape usernames from websites with poorly designed logins. For example, on some sites, the login screen returns a "Bad username" message when the username and password are both incorrect, but returns a "Bad password" message when the username is correct and the password is incorrect. This makes it easy to build a bot to test and discover usernames. To circumvent web application firewall defenses that detect multiple failed attempts, the attackers harness a large botnet with different IP addresses.



MALWARE MITB ATTACKS

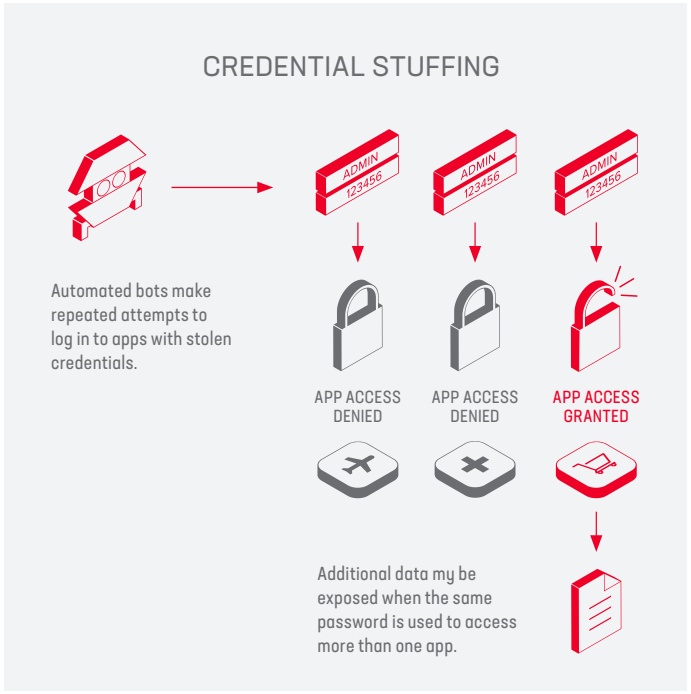
In this specialized attack, a user infected with malware browses a site. The malware recognizes the URL as one it wants to steal credentials from and injects malicious JavaScript, which functions much like content injection, but at the software level. The injected script then redirects the session to a fake page (which may have been built using assets that the cybercriminals acquired using bot site scraping) that collects the user's username and password.



CREDENTIAL STUFFING

Think your users are who their credentials say they are? Think again. Malware-based credential theft has quickly become one of the biggest security problems that organizations face today. Consider this: in the first six months of 2017, there were 2,227 breaches reported, exposing over 6 billion records and putting countless accounts at risk.[3] What do criminals do with all those exposed records? Oftentimes, they are used for credential stuffing. Credential stuffing is an automated attack powered by malware tools such as Sentry MBA. In this type of attack, cybercriminals acquire login credentials and make repeated attempts to take over corporate or personal accounts.[4]

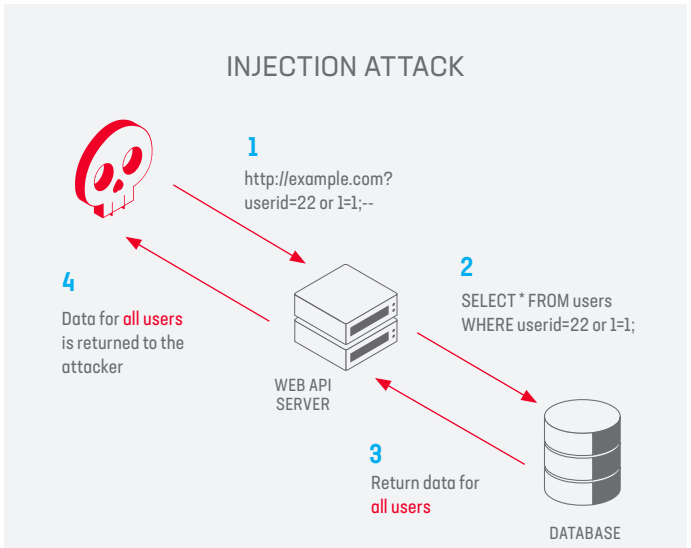
If everyone changed their passwords when their credentials were exposed, these attacks wouldn't be successful. However, with so many online accounts to manage, 75 percent of users recycle credentials across accounts.[5] These insecure password practices lead to a 1 to 2 percent success rate for credential stuffing attacks, which means that if a cybercriminal scoops up 1 million stolen credential records, they can take over 10,000 to 20,000 accounts with minimal effort—and there are billions of leaked credentials available on the dark web for fractions of a penny apiece.[6]



INJECTION ATTACKS

Injection attacks are listed as the number one web app security risk in the OWASP Top 10. These attacks are not only very dangerous but also widespread, especially in legacy applications. Virtually every web app is potentially vulnerable to some type of injection attack, so attackers can use bots to perform automated vulnerability scans to identify potential targets. Once identified, there is typically further manual probing to exploit the vulnerability.

Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. SQL Injections are the most common injection attack type, and can result in authentication bypass, information disclosure, denial-of-service (DoS), or even full system compromise.



[3] https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20MidYear%20Data%20Breach%20QuickView%20Report.pdf
[4] https://www.infosecurity-magazine.com/news/sentry-mba-tool-used-in-attacks-on/
[5] https://www.entrepreneur.com/article/246902
[6] https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0

2. THE MONETIZATION: HOW CRIMINALS CASH IN

After they steal data from your applications, criminals turn their sights to finding ways to profit from that data. Sometimes the scheme is as straightforward as stealing bank account credentials and draining the account, or using ransomware to extort a payment from a business or individual.

However, cybercriminals also sell intellectual property, user IDs, and email addresses to other criminals or to unknown users on darknet forums.

Let's take a look at some of the most popular schemes that hackers use to monetize the data that they've stolen.

HIGH-VALUE ACCOUNT TAKEOVER

With so many stolen login credentials out there, the question is not how to get credentials, but what is the most profitable way to use them? In the case of financial accounts, it's simple. Once you have control of the account, drain the money, stock, or frequent flier miles and send them to a remote server where the malware processes fraudulent transactions on the accounts the criminal has stolen.

At the same time, the attacker (or their helpful bot) captures any stored value, credit card, and bank account numbers, and other personally identifiable information from the stolen accounts.

LOW-VALUE ACCOUNT TAKEOVER

Not all stolen credentials can be used to access high-value accounts, but attackers still find ways to monetize low-value account information. A stolen Twitter account may only sell for 10 cents on the dark web, but attackers work at scale. Using a bot running on hijacked computers, they steal thousands of these accounts every day, making this type of account theft a very lucrative endeavor.[7]

WHAT CAN YOU DO WITH A STOLEN ACCOUNT?

The simplest way to monetize a stolen account is to rack up fraudulent charges. Attackers can launder stolen credit cards using a series of eBay accounts to create a network of fake buyers and sellers—with all the purchases ultimately funneling to the attacker's pocket. Alternatively, hijacked accounts can be used to launch spam at other users, drive up banner ad clicks with click fraud, or the personal information (like zip codes, family member names, and emails) associated with the account can be sold, used for identity theft, or used to help crack related accounts.

Attackers can sell stolen Netflix accounts for a few dollars to other users who will then get to watch free movies without the knowledge of the original owner.[7] Uber accounts have become more popular to steal and sell, going for around two dollars each each on dark web forums.[9]

There are numerous pieces of malware that can help attackers compromise Facebook accounts. Facebook users post personally identifiable information such as their mother's maiden name, their home town, their high school, the names of their children, etc., which makes these accounts a gold mine for attackers engaged in identity theft. In addition, information gleaned from Facebook accounts has been used in schemes such as virtual kidnapping, where an attacker pretends to have kidnapped a victim and demands a ransom.[10]

$80

A SINGLE STOLEN PAYPAL ACCOUNT CAN SELL FOR AS MUCH AS $80 ON THE DARK WEB.[11]

[7] https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/
[8] https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/
[9] https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/
[10] https://f5.com/labs/articles/threat-intelligence/cyber-security/virtual-kidnapping-the-latest-in-an-endless-stream-of-scams-25840
[11] https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/

3. THE STRATEGY: PROTECT YOUR ORGANIZATION WITH A LAYERED DEFENSE

With so many cybercriminals stealing so much data—and having so many ways to turn that data into cold, hard cash—you may be left wondering whether there's any solution to the problem of malware.

While there's no single thing you can do to prevent these kinds of attacks, a layered defense strategy can dramatically reduce your vulnerability to malware.

STRONG AUTHENTICATION

The first piece of the defense puzzle is a strong system of authentication. Since credentials are almost always the target of malware attacks, strong authentication can help keep the identities of your users secure and your organizational data safe.

Unfortunately, strong authentication can become quite expensive at scale, so some organizations choose to implement multifactor authentication solely for high-risk users, including C-level team members or employees who have access to valuable corporate information.

FRAUD MONITORING

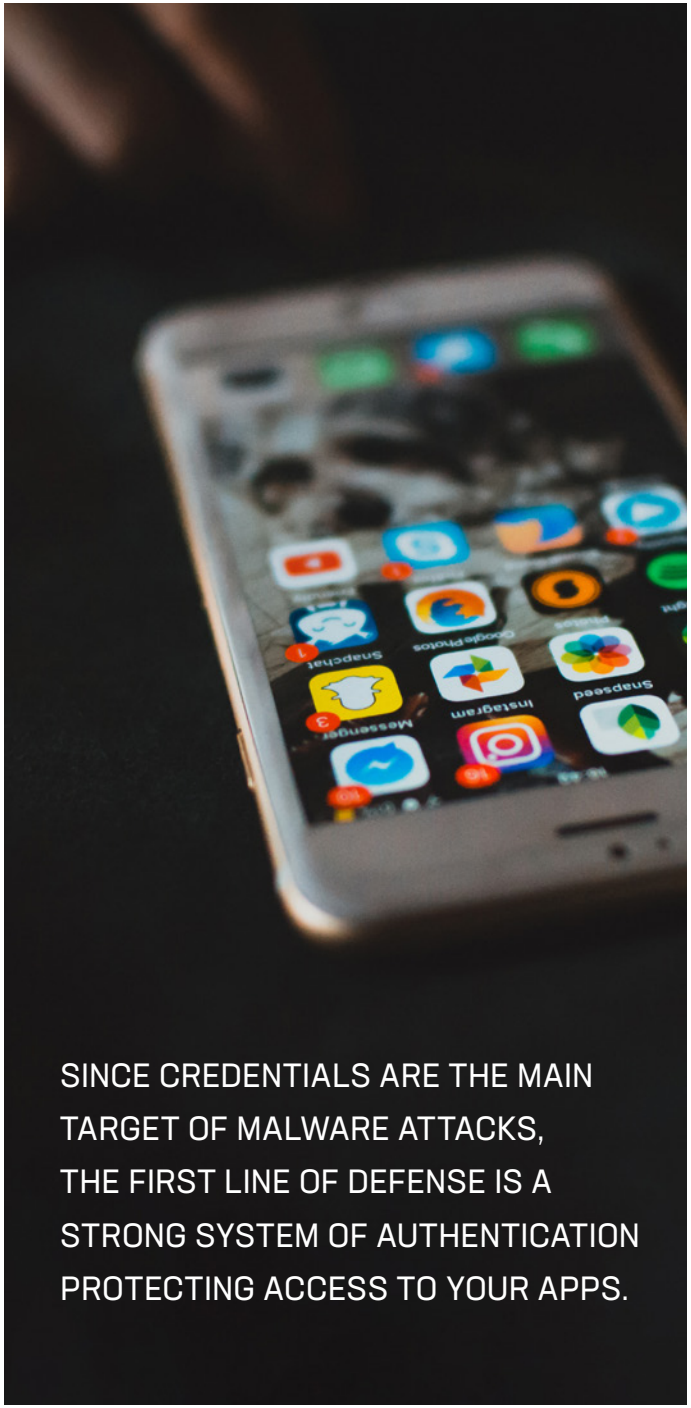
Businesses in all industries are vulnerable to web fraud, which is a multifaceted threat that costs organizations billions of dollars a year. While you can't ever fully prevent fraud, you can utilize several methods to reduce its effects.

Fraud monitoring pairs machine-based analysis with human experts; machine learning-based analysis identifies clear cases of fraud, and the human experts review more nebulous account activity.[12] Again, this can be expensive to acquire and support, but a strong fraud monitoring service can help mitigate catastrophic losses due to malware-based theft.

BOT MANAGEMENT

It's important to defend against bad bots without disrupting the good ones. You can minimize your bot risk with multi-layered, proactive defenses that identify and block bad bot traffic before it impacts your web and mobile-based apps. Filtering out unwanted bot traffic will not only help you maximize your app performance, it also eliminates bad data from your business analytics and helps you focus on the most critical security alerts.

[12] http://www.bankinfosecurity.eu/interviews/tips-for-fighting-fraud-big-data-i-2269



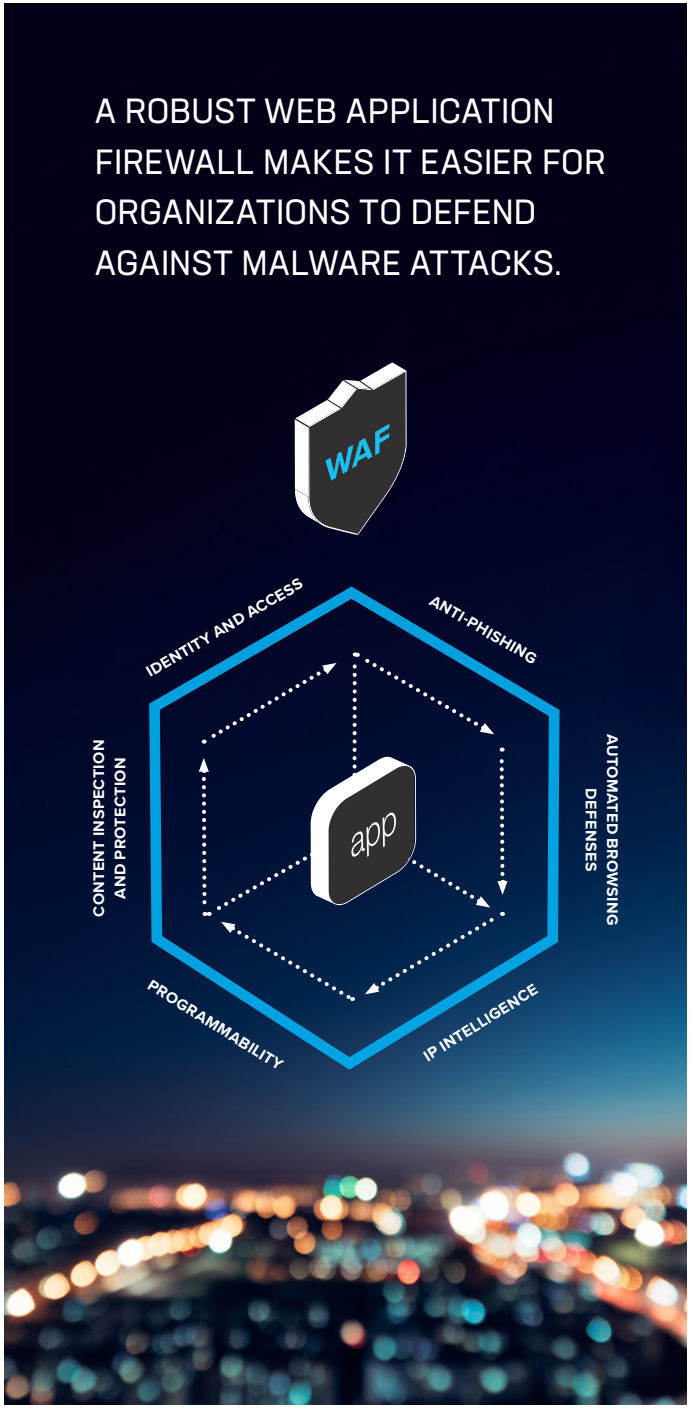
WEB APPLICATION FIREWALL

A robust web application firewall makes it easier for organizations to defend themselves against malware attacks. It can stop bots from scraping your sites—protecting your intellectual property and decreasing the chances of a successful phishing campaign. You can detect and stop brute force and credential stuffing attacks, identify and block browser session hijacking attacks, and prevent the execution of fraudulent transactions.

THE TAKEAWAY

While none of these solutions completely protects you from the ubiquitous problem of malware, a defense-in-depth strategy can help you mitigate the effects it has on your organization.

Learn more about how you can reduce your risk of fraud and better manage bot traffic by visiting F5.com/bots.



THINK APP SECURITY FIRST

Always-on, always-connected apps can help power and transform your business–but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.

Find more security resources at **f5.com/solutions**.

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com