HOW MALWARE CAN STEAL YOUR DATA
AND WHAT YOU CAN DO TO STOP IT
As applications drive business, more and more valuable data is accessed and exchanged through them.

Cybercriminals attempt to compromise your apps with schemes like social engineering, malware writing, botnet herding, credit card fraud, credential laundering, trading in stolen digital goods, and selling corporate intellectual property—all intended to generate increasing returns.

In a world of different types of criminals with varying skill levels, time commitments, resources, and specializations, there’s only one constant: attackers have their eyes set firmly on your apps and the data behind them—and they’re using malware to steal it.

51% of data breaches include malware

1 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
THE ATTACKS:
HOW MALWARE STEALS 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. While the tactics, techniques, and procedures vary, each criminal scheme has two fundamental parts: the technical attack (the hacking) and the monetization scheme (the exploitation of the data).

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

BOT SITE SCRAPING

In 2016, more than half of the traffic on the Internet was initiated by software and not humans.² While not all bots are bad³, cybercriminals use autonomous programs 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 helps 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.

Attacker 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 could detect multiple failed attempts, the attackers could harness a large botnet with different IP addresses.

³ http://botnerds.com/types-of-bots/
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.¹ What do criminals do with all those exposed records? Credential stuffing is an automated attack powered by malware tools such as Sentry MBA where a cybercriminal acquires login credentials and makes repeated attempts to take over corporate or personal accounts.²

Now, 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.³ 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 a minimal amount of effort. And there are billions of leaked credentials available on the dark web for fractions of a penny a piece.⁴

To learn more about why credential stuffing is such a big threat—and what you can do about it—see Credential Stuffing: A Security Epidemic.

---

³ https://www.entrepreneur.com/article/246902
⁷ https://www.entrepreneur.com/article/246902
HOW MALWARE CAN STEAL YOUR DATA—AND WHAT YOU CAN DO TO STOP IT

MALWARE MITM 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 that collects the user’s username and password.

CONTENT INJECTION

Increasing concerns about privacy and bolstered support for encryption led to the majority of the Internet being encrypted for the first time in 2016.⁸ While that’s good news for people concerned about data protection, it means that nearly half of online traffic remains insecure and vulnerable to man-in-the-middle (MiTM) attacks.

MiTM attacks happen when a cybercriminal eavesdrops, intercepts, or alters communication between two parties—without either of them knowing. Unencrypted websites can be easily intercepted and altered while being sent from the server to the browser by anyone who can see the transmission, such as an ISP, a user on the same wireless network, or any hacked router. Without the guarantee of encryption provided by HTTPS, users can’t ever be sure that the page they’re looking at (and entering data into) is the page they think it is.

Attackers can also inject malware, malicious scripts, and fake messages into the browser. Look out for cross-site scripting (XSS), which involves an attacker injecting scripts into a trusted website with the intent of stealing personal information, gaining control of mobile devices, transferring money, and more.⁹ Some ISPs have begun monitoring users’ traffic and injecting their own ads into your browser.¹⁰ Cybercriminals also employ clickjacking (hiding malicious links under legitimate content) to perpetrate banner-ad fraud or trick users into installing malware.

Malware MITM

INTERCEPTED AND ALTERED CONTENT

USER NAME AND PASSWORD ARE STOLEN

INJECTED SCRIPT REDIRECTS TO A FAKE PAGE

USER

WEBSITE

CONTENT INJECTION

INTERCEPTED CONTENT

DESIRED SITE

INFECTED USER

ORIGINAL CONNECTION

https://f5.com/labs/articles/threat-intelligence/malware/webinject-analysis-newsidroncom-22441
THE MONETIZATION:
HOW CRIMINALS CASH IN

After they steal data from your applications, criminals turn their sights to figuring out how 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 the intellectual property, user IDs, and email addresses to other criminals or to unknown users on darknet forums.11

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 becomes what’s the most profitable way for criminals 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 out of it and send it 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) gleans any stored value, credit card 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 financial accounts. However, attackers can still get value from this data.

A stolen Twitter account may only sell for 10 cents on the dark web, but if an attacker uses a bot running on hijacked computers to steal thousands of accounts every day, it can be a very lucrative proposition.13

$80

A SINGLE STOLEN PAYPAL ACCOUNT CAN SELL FOR AS MUCH AS $80 ON THE DARK WEB.12

HOW MALWARE CAN STEAL YOUR DATA—AND WHAT YOU CAN DO TO STOP IT

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 funneling ultimately 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, and sell the personal information (like zip codes, family member names, and emails) for identity theft or use it to help crack related accounts.

Attacker 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. Uber accounts have become more popular to steal and sell, going for around two dollars each on dark web forums.

WHAT CAN YOU DO WITH A STOLEN ACCOUNT?

There are numerous pieces of malware that can help attackers compromise Facebook accounts, which are especially valuable, because of the social nature of the platform. Facebook users post all sorts of 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 from that person’s friends or family.16

---

THE STRATEGY:
PROTECT YOUR ORGANIZATION WITH 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 help 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.

AS TECHNOLOGY CONTINUES TO EVOLVE, SO WILL THE SCAMS THAT CYBERCRIMINALS USE TO MAKE MONEY.

FRAUD MONITORING

Businesses in all industries are at risk of 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 employs a combination of machine-based analysis and human experts who evaluate the behavior of accounts that can’t be classified as either definitively bad or good through machine learning.17 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.

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.

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 protecting your organization against the threats of today—and tomorrow—at F5 Labs.  

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

Learn more about application security at the AppProtectLibrary.