Formjacking

Formjacking is a detection for the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of e-commerce sites.

According to the Symantec Internet Security Threat Report 2019, formjackers compromised 4,818 unique websites every month in 2018. Over the course of the year, Symantec blocked over 3.7 million formjacking attempts. Furthermore, over 1 million of those formjacking attempts came during the final two months of 2018—ramping up towards the November Black Friday weekend, and onward throughout the December Christmas shopping period.

So, how does a formjacking attack work?

Formjacking involves inserting malicious code into the website of an e-commerce provider. The malicious code steals payment information such as card details, names, and other personal information commonly used while shopping online. The stolen data is sent to a server for reuse or sale, the victim unaware that their payment information is compromised.

All in all, it seems basic. It is far from it. One hacker used 22 lines of code to modify scripts running on the British Airways site. The attacker stole 380,000 credit card details, netting over £13 million in the process.

How Do Formjacking Groups Make Money?

Most of the time, the stolen credentials are sold online. There are numerous international and Russian-language carding forums with long listings of stolen credit card and other banking information. They're not the illicit, seedy type of site you might imagine.

Some of the most popular carding sites present themselves as a professional outfit—perfect English, perfect grammar, customer services; everything you expect from a legitimate e-commerce site.

How Can You Stop a Formjacking Attack?

Magecart formjacking skimmers use JavaScript to exploit customer payment forms. Using a browser-based script blocker is usually enough to stop a formjacking attack stealing your data.

- Chrome users should check out ScriptSafe
- Firefox users can use NoScript
- Opera users can use ScriptSafe
- Safari users should check out JSBlocker

Once you add one of the script blocking extensions to your browser, you will have significantly more protection against formjacking attacks. It isn't perfect though.

Cryptojacking

Cryptojacking is an emerging online threat that hides on a computer or mobile device and uses the machine's resources to "mine" forms of online money known as cryptocurrencies. It's a burgeoning menace that can take over web browsers, as well as compromise all kinds of devices, from desktops and laptops, to smart phones and even network servers.

Like most other malicious attacks on the computing public, the motive is profit, but unlike many threats, it's designed to stay completely hidden from the user.

Most cryptojacking software is designed to stay hidden from the user, but that doesn't mean it's not taking its toll. This theft of your computing resources slows down other processes, increases your electricity bills, and shortens the life of your device. Depending on how subtle the attack is, you may notice certain red flags. If your PC or Mac slows down or uses its cooling fan more than normal, you may have reason to suspect cryptojacking.

The motivation behind cryptojacking is simple: money. Mining cryptocurrencies can be very lucrative, but turning a profit is now next to impossible without the means to cover large costs. To someone with limited resources and questionable morals, cryptojacking is an effective, inexpensive way to mine valuable coins.

How does cryptojacking works?

Cryptojackers have more than one way to enslave your computer. One method works like classic malware. You click on a malicious link in an email and it loads cryptomining code directly onto your computer. Once your computer is infected, the cryptojacker starts working around the clock to mine cryptocurrency while staying hidden in the background. Because it resides on your PC, it's local—a persistent threat that has infected the computer itself.

An alternative cryptojacking approach is sometimes called drive-by cryptomining. Similar to malicious advertising exploits, the scheme involves embedding a piece of JavaScript code into a Web page. After that, it performs cryptocurrency mining on user machines that visit the page.

How to protect ourselves from cryptojacking?

Whether you've been cryptojacked locally on your system, or through the browser, it can be difficult to manually detect the intrusion after the fact. Likewise, finding the origin of the high CPU usage can be difficult. Processes might be hiding themselves or masking as something legitimate in order to hinder you from stopping the abuse. As a bonus to the cryptojackers, when your computer is running at maximum capacity, it will run ultra slow, and therefore be harder to troubleshoot. As with all other malware precautions, it's much better to install security before you become a victim.

One obvious option is to block JavaScript in the browser that you use to surf the web. Although that interrupts the drive-by cryptojacking, this could likewise block you from using functions that you like and need. There are also specialized programs, such as "No Coin" and "MinerBlock," which block mining activities in popular browsers. Both have extensions for Chrome, Firefox, and Opera. Opera's latest versions even have NoCoin built in.

Ransomeware

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

Ransomware can be devastating to an individual or an organization. Anyone with important data stored on their computer or network is at risk, including government or law enforcement agencies and healthcare systems or other critical infrastructure entities. Recovery can be a difficult process that may require the services of a reputable data recovery specialist, and some victims pay to recover their files. However, there is no guarantee that individuals will recover their files if they pay the ransom.

Following precautions can be taken to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Backup data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when browsing the Internet

Who is a target for ransomware?

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it's a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet — and these organizations may be uniquely sensitive to leakware attacks.

But don't feel like you're safe if you don't fit these categories: as noted, some ransomware spreads automatically and indiscriminately across the internet.

Living off the Land, and Supply Chain attacks

The use of **Living off the Land** (LotL) tactics and tools by cyber criminals has been a growing trend on the cyber security landscape in recent times. The concept of LotL is not new, and has been around for as long as 25 years. Using system tools as backdoors was common back in the day. However, in recent years, it has returned and grown in importance. Fileless attacks, which are often spoken of, are a subset of LotL attacks. The exploitation of dual-use tools and memory only tools is also often referred to under the umbrella of LotL.

Attackers who use LotL tactics use trusted off-the-shelf and preinstalled system tools to carry out their work. It might not be obvious, but there are more than 100 Windows system tools that can be used by cyber attackers for nefarious purposes.

Cyber attackers use these tools for a few reasons, often in an effort to hide their activity: they hope their malicious activity will be hidden in a sea of legitimate processes.

Other reasons for a growth in LotL activity by cyber criminals is a reduced availability of zero-day vulnerabilities and the effort required to find them. Improvements in browser security have made such vulnerabilities more difficult to find. Bug bounty programs have eliminated the easy-to-find vulnerabilities so that only the most dedicated researchers and attackers are able to root out critical vulnerabilities. In some scenarios, system tools are whitelisted and might be the only process allowed to run on a secured system, making them the only tools available for the attacker.

A **supply chain attack**, also called a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data. This has dramatically changes the attack surface of the typical enterprise in the past few years, with more suppliers and service providers touching sensitive data than ever before.

The risks associated with a supply chain attack have never been higher, due to new types of attacks, growing public awareness of the threats, and increased oversight from regulators. Meanwhile, attackers have more resources and tools at their disposal than ever before, creating a perfect storm.

The rise of Targeted Attacks

A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period. They can adapt, adjust, or improve their attacks to counter their victim's defenses.

The US Senate and the International Monetary Fund (IMF) are just the latest in a growing line of high profile companies that have been subjected to a targeted cyberattack. Sony made unwelcome headline news when it had to shut down its PlayStation network after hackers were able to steal customer information, including addresses, dates of birth, etc. In that case over 70 million people's details were exposed. Other examples include Citibank, where personal information was stolen also; and Google, who disclosed that some Gmail accounts had been compromised.

Going back 10 years and more we saw malware like the, "I love you," Netsky and Bagel grabbing the headlines. The motives behind those threats though were very different. It was more akin to graffiti, wanting to infect as many people as they could and become infamous too.

The recent attacks demonstrate that the bad guys are not interested in an "infect all" strategy any more, but rather using more targeted methods. They do not just go after financial information like bank logins or credit card details; they're in fact collecting everything they can get hold of. As we predicted at the beginning of the year, we are now in an age of "steal everything".

It's obvious what the criminals will do with stolen credit card details, but what about my date of birth, my address or even my hobbies? Well one thing they can do is what we call spear phishing; and this seems to be how the IMF was compromised in the first place.

This form of attack is where an individual or organisation is singled out, usually via email. Now most of us receive lots of spam emails and we simply delete them. But what if you get an email that purports to be from your bank/credit card company and to prove it they put the last 4 digits of your credit card number and your date of birth? This looks much more credible and we are more likely to click on any links in the email. Such a link may contain malware. This in turn would also be finely tuned to the target's operating system and applications that run on it. They could get information of this kind by trawling social networks for titbits of information and/or even calling staff at the organisation. By creating a specific piece of malware just to target one organisation, it stays under the radar of security companies and law enforcement agencies. In the case of the IMF it looks like it may have been there unnoticed for several months!

Security Challenges of Cloud

Today's businesses want it all: secure data and applications accessible anywhere from any device. It's possible with cloud technology, but there are inherent challenges to making it a reality.

What can enterprise businesses do to reap the benefits of cloud technology while ensuring a secure environment for sensitive information? Recognizing those challenges is the first step to finding solutions that work. The next step is choosing the right tools and vendors to mitigate those challenges.In our technology driven world, security in the cloud is an issue that should be discussed from the board level all the way down to new employees. The CDNetworks blog recently discussed "what is cloud security" and explained some of its benefits. Now that we understand what cloud security is, let's take a look at some of the key challenges that may be faced.

Here are the major security challenges that companies using cloud infrastructure have to prepare for.

Data breaches

A data breach might be the primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices. It might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual property. An organization's cloud-based data may have value to different parties for different reasons.

Access Management

Since cloud enables acess to company's data from anywhere, companies need to make sure that not everyone has access to that data. This is done through various policies and guardrails that ensure only legitimate users have access to vital information, and bad actors are left out.

Data encryption

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys.

Denial of service (DoS/DDoS attacks)

Distributed denial-of-service attack (DDoS), like any denial-of-service attack (DoS), has as its final goal to stop the functioning of the targeted site so that no one can access it. The services of the targeted host connected to the internet are then stopped temporarily, or even indefinitely.

Advanced persistent threats (APTs)

APTs are a parasitical form of cyber attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them.

IoT Attacks

Internet of Things (IoT) delivers substantial benefits to end users. However, it also brings unprecedented security challenges. A part of the central security issue is that connected devices share implicit trust. This shared trust between connected devices means that the devices automatically transmit their data to each other immediately upon recognition without first running any malware detection tests. The worst-case scenarios of these IoT security dangers result in physical harm or even the loss of life.

The first IoT security attacks began in 2016, and more are anticipated. Here's a rundown of the attacks, expectations for future attacks, and what safety measures IT professionals can use to increase IoT's protection.

The 2016 IoT Botnet Attacks

In 2016, the first wave of IoT security attacks brought down the Internet. The Mirai Botnet hacked into some Internet of Things devices — in this case mainly routers and Internet Protocol (IP) cameras — and transformed the devices into botnets. The centrally-controlled IoT botnets flooded Dyn's, a Domain Name Services (DNS) provider, traffic causing a disruptive bottleneck that blocked Internet access for millions of users worldwide.

The Mirai malware code is easily accessible and adaptable, which makes it harder to prevent its effects. Hackers modify the code to create unique strains of the malware with its own novel Internet interruption tactics while dodging security solutions used in previous iterations of the malware.

Most of the attacks in 2016 took place in China and in the United States, according to Symantec's research.

Current and Future IoT Security Threats

IoT security threats and attacks will rise as the IoT devices become more commonplace. The security threat is high enough for Gartner to estimate "spending on IoT security is expected to reach $547 million in 2018." In the same report, Gartner predicts that 25 percent of attacks in enterprises will involve IoT.

Ericsson's white paper on IoT security warns of potential industrial espionage and surveillance by noting that "the magnitude of data could make it possible to determine company processes through the use of analytics. Even if traffic is encrypted, meaningful patterns may be revealed through the analysis of that traffic." Some countries already worry about the espionage threat. Germany recently banned an IoT doll that was caught listening and recording conversations.

Other scenarios include accessing or controlling a person's home or office. For instance, in Finland, a DDoS attack on a building's heating system left residents without heat.

Election Interference 2018

Cyberspace, and particularly election technology, has become a new domain for those who wish to suppress or interfere with the key processes of democratic societies in order to further their own ends, writes Liisa Past, Next Generation Leader at the McCain Institute for International Leadership and former Chief Research Officer at the Cyber Security Branch of the Estonian Information System Authority.

Influence, social media and information campaigns against elections and election campaigns are no longer an unexpected occurrence. Rather, they have become a planning assumption. Cyber attacks against the essential functions of democratic systems, as well as those who are involved in election campaigns, are often integrated with such operations.

In the case of elections, the networks, data and machines used, as well as the IT systems of those involved in politics, have been targeted. These cyber attacks seek to compromise the confidentiality, availability or integrity of the very systems that underpin the key processes of democracy.

Hence, it is imperative to build tactics, techniques and procedures to deter, detect, combat and mitigate the effects of attacks that can effectively delegitimize electoral outcomes. In addition to the US November 2018 midterms, which are likely to be closely observed by adversarial actors and cyber defenders alike, direct elections across Europe will lead to the election of a new European Parliament in May 2019.

WASHINGTON (Reuters) - Senior Trump administration officials warned Congress on Tuesday of ongoing efforts by Russia to interfere in the 2018 midterm congressional elections as the federal government prepares to hand out $380 million in election security funding to states.

At a briefing attended by about 40 or 50 members of the 435-member U.S. House of Representatives, the heads of FBI, Homeland Security Department and the director of National Intelligence said states and cities overseeing elections need to be prepared for threats.

DHS Secretary Kirstjen Nielsen told reporters she agreed Russia was trying to influence the 2018 elections.