Malware: The Ubiquitous Menace

Why Web-based Malware is a Pervasive Threat to Customers and Employees
Malware: The Ubiquitous Menace

Why Web-based Malware is a Pervasive Threat to Customers and Employees

Every day seems to bring news of web-based malware attacking another popular, highly trafficked website, causing harm to visitors and tarnishing the site owner’s reputation and bottom line. And for every high-profile attack, there are countless others that never become headline news, yet still cause considerable damage to countless website visitors, not to mention the site owners’ productivity, revenue and focus.

IT departments and Security Operations Centers (SOC) dedicate an enormous amount of time and money on information security—Gartner estimates worldwide spending will reach $76.9 billion in 2015, an 8.2% increase over 2014’s spend. Yet these investments appear highly ineffective at protecting a company’s most important assets—their customers and employees who use the Internet on a daily basis.

The increasing frequency and sophistication of these attacks raise some obvious questions:

• Why are web-based malware attacks on the rise?
• What makes these attacks so costly?
• What role does third-party code play in enabling these attacks?
• Why are IT departments and SOCs—even those with significant budgets and staff—unable to address the dangers associated with third-party code executing on their websites, apps and other public-facing assets?

Too often, IT and SOC managers and executives fail to ask these obvious questions, let alone know the answers. Focused only on securing their networks, mobile devices, end points, internal web applications and email gateways, they neglect the security gaps on the front-end of their website’s user experience. Without answering these questions and addressing the resultant security gaps, IT and SOC leaders can never develop, execute and maintain an effective, 24/7 defense against the ubiquitous threat of web-based malware.
The goals and objectives of web-based malware

Malware is typically a silent, invisible, constantly morphing enemy that attacks in plain sight: on a company’s purportedly secure, public-facing website. In the past, only shady, small-time or ad-supported websites with questionable content were at risk for malware. Now, in order to increase the efficacy and scope of their attacks, malware authors purposely target popular, heavily trafficked websites and mobile apps in all sectors, including ecommerce, travel, banking, insurance, government, entertainment, social media and news and sports. In fact, recent studies report that up to 90% of all malware attacks occur on legitimate sites. In addition to these broad-based attacks, malware campaigns also target employees accessing the corporate site in the hope of gaining access to the corporate network.

With public-facing websites and mobile apps serving as their primary vector, bad actors use web-based malware for financial gain, to steal data, to publicize a specific cause, to criticize the site’s corporate owner or to cause harm to the site visitor’s computer or mobile device. Once injected into a site or executed via a visitor’s browser, malicious code can perform a wide variety of tasks, including:

- Gain remote access and complete control over the site visitor’s computer or mobile device
- Capture and send data from the infected computer or mobile device without the end user’s knowledge or consent
- Disable or modify the computer or mobile device’s security measures
- Encrypt all data on the computer or mobile device and hold it hostage
- Damage or erase other software on the infected computer or mobile device, including the operating system itself

How web-based malware works

Purveyors of web-based malware also have the ability to deliver their malicious code in a wide variety of ways. Regardless of the delivery mechanism, all bad actors must first identify and then exploit any number of vulnerabilities or weaknesses used to serve a website. A vulnerability is typically found in one of the following:

- The owned and operated source code of the targeted website or mobile app
- Third-party code used to populate the site
- Any point in the process of serving an online or mobile ad or content to a targeted site or mobile app

Once the vulnerability is found, malware uses browser or extension limitations to access the user’s device via proprietary code or an exploit kit, which is designed to exploit the targeted vulnerability. The exploit kit typically leverages the browser to download its payload to the site visitor’s computer or mobile device, where the payload can execute immediately or remain dormant, avoiding detection for days, weeks or even months, as it waits for the right conditions to be met before launching an attack. This process replicates itself each time a new visitor loads the compromised website or mobile app, with an entire segment of the website’s audience potentially exposed to this web-based malware.

For payload retrieval, the malicious code may require some type of user interaction: clicking on a compromised link or opening an infected file. A drive-by download, however, requires
Malware: The Ubiquitous Menace

no user interaction, with the payload downloading automatically when the site visitor’s browser loads the desired web page. Unfortunately, the computer or mobile device end user remains completely oblivious both during and after this process, not realizing malware is even present. Of course, that is until the payload’s effects become apparent.

Web-based malware’s exponential, unchecked growth
The growth of web-based malware remains unchecked and serves as a constant, 24/7 threat to every organization with digital properties—online and mobile websites and apps. Consider the following facts:

• 400,000 new malicious programs are detected every day\(^2\)

• 85% of all malware is distributed via the web, with drive-by downloads being the most prominent\(^3\)

• 67% of websites distributing malware are legitimate sites that were compromised\(^4\)

• Traditional security tools miss up to 100% of malware\(^5\)

• The average cost to respond to and remediate just one malware-driven security breach is approximately $62,000, averaging $3.2M a year per company\(^6\)

• 40% of the top breaches recorded to-date occurred in 2013\(^7\)

The fact that 30% of the top breaches occurred in the last 12 months is strong evidence that malware’s impressive, seemingly unstoppable growth rate will only continue, despite massive investments in both traditional and cutting-edge security solutions.

Why web-based malware is here to stay
Unfortunately, web-based malware is now a fact of life for both businesses and consumers because its ubiquitous nature is enabled by a variety of factors, including the steady adoption of mobile and the emergence of the Internet of Things (IoT). Approximately 20% of the world’s population now owns a smartphone, triggering an explosion in mobile apps and advertising. This rapid proliferation of apps and devices generates billions of dollars in annual revenue for the mobile commerce, gaming, advertising and content ecosystems, while also creating a massive opportunity for malware purveyors. The inherent complexity and large number of entities required to serve and execute the mobile consumer experience provides many unprotected entry points for web-based malware to attack.

As the IoT brings interconnectivity—at both work and home—to a whole new level, it also unleashes new distribution channels for malware to exploit. Another factor is the growing popularity of streaming video services like Netflix. Accessed via smart TVs, tablets, smartphones and laptops, these services provide malware creators with a new potential distribution channel.

Malware is incredibly smart and can focus on a select audience using site visitor behavioral and geographic characteristics in concert with data collection and marketing services—the same process used to deliver advertising or a personalized user experience. Unwittingly, these services provide the information needed for malware to target a specific consumer segment with a specific vulnerability, while
simultaneously evading detection due to the sheer volume of attacks targeting a plethora of different consumer groups. On the flip side, this same geographic and behavioral identification is used to aid in obfuscation by purposefully targeting a select group that malware authors believe won’t have active or updated security controls. Their strategic advantage is furthered by the fact that traditional signature-based malware detection tools simply cannot keep pace with malware’s ability to morph and mutate.

Collectively, these various factors enable malware purveyors to:

- Reach broad, even global audiences in very short time frames
- Target specific consumer segments
- Avoid detection by mimicking the same methods legitimate companies use to monetize the web

Direct and indirect costs of web-based malware

No IT or SOC team can afford to ignore the threat web-based malware presents. Nor can they ignore the direct and indirect costs that result from an attack. When malware infects a site visitor, it not only erodes the consumer’s trust in the online and mobile ecosystem, but it also harms the firm’s brand reputation, resulting in significant declines in site traffic, online transactions and revenue. In fact, Economist Intelligence Unit’s 2013 study of consumers in 24 countries reported that 18% of respondents were victims of a data breach; of this number, 38% said they no longer did business with the organization and 46% said they “advised friends and family to be careful of sharing data with the organization.”

Numerous studies have quantified the direct costs of malware. The Ponemon Institute reports that U.S. malware-driven data breaches cost a company $277 per exposed record, with the annualized cost of a cybercrime to be $5.4 million per year. Furthermore, malware-induced data breaches are 4.5 times more costly than breaches caused by “unintended disclosures,” which are the most common type of data breach.

There are also the increasing costs of everyday security tools used to protect an organization’s data, networks, mobile devices, endpoints and internal web-based apps. And don’t forget the opportunity costs associated with IT responding to and remediating an attack, derailing ongoing projects that actually add value and improve IT’s service levels.

Finally, if left unchecked, malware attacks will lead customers to clamor for government oversight and legislation, with the bottom line absorbing the cost of achieving and then maintaining regulatory and liability compliance.

Third-party code plays a prominent role in rendering public-facing websites

What makes a website so vulnerable? The answer is simple and hiding in plain sight: the abundance of third-party code constantly executing on websites, mobile apps and site visitors’ browsers. Almost every public-facing website and app uses several types of third-party code to deliver a dynamic and interactive user experience that helps drive customer engagement and encourage transactions.

In fact, recent analysis indicates that approximately 78% of source code found on Fortune 1,000 websites is from third-party providers. That figure may sound unrealistic,
until you consider all the third-party services required to render a single URL. In addition to backend data analytics and marketing automation platforms, most websites utilize a host of services to enable video, blogs, social feeds and talent acquisition.

To perform their specific function or service, each of these third-party providers places a small amount of their own code on the client’s website, with calls being issued to and from the code to the third party’s own servers. Often times, these third-party vendors may call a fourth or fifth party to aid in providing their service. These fourth parties piggyback on the third-party’s domain, often without the website operator’s knowledge or consent. Subsequently, a large portion of website operations is outsourced to the point that the average website has dozens of different external domains and cookies accessing it at any one time.

The dangers of not managing a website’s third-party code

To be clear, the mere presence of these third-party domains and cookies is NOT the reason web-based malware infects websites and visitors’ browsers with such ease and frequency. Rather, it’s a company’s lack of knowledge about and control over this third-party code that allows these attacks to occur.

While IT and SOC teams diligently anticipate and manage the vulnerabilities and security risks inherent in their networks, end points, internal web apps, email systems and mobile devices, they fail to address and manage the risks associated with third-party code executing on their external website and their site visitors’ browser or device, not realizing each additional piece of code represents another point of vulnerability for malware to exploit. Lacking visibility into the path these domains and cookies take to their site, these teams are unable to know if malware was injected as the code traveled from its point of origin to the consumer’s browser—a significant issue if the site visitor happens to be your employee.

In addition, without the business processes and monitoring tools needed to implement and enforce security and data governance policies for the vendors used to render the site, IT cannot identify web-based malware attacks in real time, which is critical for minimizing the damage. IT also fails to understand the importance of capturing and archiving the activity of this third-party code, making any future remediation extremely difficult, costly and time consuming.

As a result, a company’s website, along with its visitors and employees, are nearly defenseless against web-based malware, because the site’s “external layer,” also known as the “user experience,” remains completely outside the organization’s control and protection. It’s here, where the third-party code needed to render the site executes and where the user’s browser interacts with the site, that malware can inflict its damage with little to no fear of detection for days, weeks and even months. This lack of real-time visibility and control is the main reason web-based malware is so prolific and effective.

Subsequently, it’s critical CIOs, CISOs and their teams recognize that all websites and apps are at risk for such attacks—it’s not just ad-supported websites. Malware purveyors can and do exploit all types of third-party content and services, successfully infecting any targeted site visitors, including the site operator’s own employees.
Given malware’s highly dynamic nature and the fact that most websites have a revolving door of third-party code, is it even possible to protect a site from web-based malware? The answer is an emphatic yes. Protecting a website’s exterior, consumer-facing layer from these attacks is possible, but only by achieving real-time, granular control over the third-party code accessing the site, the app or the visitor’s browser. It’s equally important for IT to understand that gaining this control and visibility is not a one-time event; instead it must be a continuous, 24/7 process of detecting, inspecting and then removing and blocking all unknown, suspicious or malicious code hitting the site or app.

Protecting against web-based malware is possible, but only by achieving real-time, granular control over the third-party code accessing the site or visitor’s browser.

Minimizing and mitigating an organization’s risk for web-based malware

By gaining real-time control and transparency over this third-party code, the teams responsible for managing a website can develop the necessary whitelists and blacklists of allowed and prohibited vendors, domains and cookies. Using these lists, site operators can continuously monitor and inspect the third-party code accessing their digital properties. To ensure no unauthorized domains or cookies are dropped, the appropriate teams should review and update these lists on regular basis.

A vetting process for the vendors involved in serving the site should also be developed, ensuring selected business partners not only adhere to the site’s privacy and data guidelines, but also have their own policies, business processes and technology in place to achieve

The SEA’s Thanksgiving Attack demonstrates the dangers of third-party code

Early Thanksgiving morning 2014 the Syrian Electronic Army (SEA) attacked a wide variety of media websites, including large-volume digital publishers like The New York Times, The Boston Globe and retailers like Office Depot. Benign in nature, this attack consisted of compromising the user experience by directing all visitors to a pop-up screen containing an SEA propaganda message and logo.

The attack was possible because of a vulnerability traced to Gigya, which provides a customer management platform to more than 700 leading brands. This particular attack was not caused by “malvertising,” which is when an infected ad downloads its malicious content to a website visitor’s browsers.

This particular attack occurred because the SEA identified a vulnerability at GoDaddy, which hosts gigya.com’s DNS server. It was through this vulnerability that the SEA gained access to GoDaddy’s servers and redirected Gigya’s Internet traffic to servers at imgur.com, which downloaded an SEA-written JavaScript file called “socialize.js” to any site visitor attempting to load the page. It was this file that displayed the SEA’s message and logo.

This attack is an excellent example of how the presence of third-party code—the gigya.com domain executing on any of the impacted media sites—inaudiently enabled a wide-spread malware attack, impacting hundreds of thousands of people within hours.
ongoing compliance. IT should also institute an ongoing quality assurance process to gauge, score and communicate each vendor’s activity—including any violations—to the functional teams responsible for serving the sites as well as to the vendors themselves. In addition, legal teams should be involved to review vendor agreements and ensure liability resides with the third-party provider.

It is also recommended that IT conduct a comprehensive review of industry best practices, which ensure consumer privacy, and the growing body of government privacy regulations and then compare these to their existing policies, making adjustments as needed. Such reviews should occur on a regular basis and in conjunction with risk and/or legal teams.

Securing the online and mobile user experience

Clearly, web-based malware attacks are a significant problem and they are growing at an alarming rate. Silent, invisible and always changing, this type of malware can easily leverage any third-party code used to serve the website, which means nearly every public-facing website is at risk. It’s also important to realize malware is not a problem specific to ad-supported websites and apps. Rather, it’s a problem for any website utilizing third-party content or services—including data management platforms, advertising re-targeters, analytic firms, sales platforms, video sharing, third-party content and others—all of which must run their own code on a client’s website or visitor’s browser to perform the requested function or service.

Web-based malware’s attack methodology is no secret, so why do traditional security platforms and antivirus scanners fail to detect this malware before it inflicts damage? Several of the large antivirus and filtering companies try to stay ahead of the malicious content, but the content and payloads constantly change, causing delays in flagging and reporting these incidents. Subsequently, it can be several days to several weeks before a firm properly identifies a malware attack, giving the malicious code ample time to cause wide-spread damage. As a result, the public notifications these firms release on an attack are purely informational and not tactically effective for pro-actively protecting and securing companies in the online and mobile ecosystem.

The only way to prevent web-based malware is by monitoring and scanning all digital properties—websites and mobile apps—on a continuous, 24/7 basis. This type of monitoring guarantees the immediate detection of any malicious or unauthorized third-party code present on the site or app, allowing IT and SOC teams to take protective and preventive actions, including blocking the unauthorized domain or cookie and, if needed, all other trackers from this vendor.

Today, most businesses lack the infrastructure, processes and resources to continuously monitor their public-facing websites for suspicious, malicious or faulty code, which is the only proven way to detect and remediate problems as they arise in real-time—not days or weeks later. Compounding this challenge is the fact that multiple functional teams—marketing, ecommerce and IT—share responsibility for the website’s management. However, given the breadth and depth of the dangers web-based malware presents, IT and/or SOC teams must secure these valuable digital properties on a 24/7 basis. Only through continuous monitoring of third-party code and vendors involved in the content and ad execution value chain can businesses protect the user experience for their customers and employees.
Malware: The Ubiquitous Menace

5. "Security tools missing up to 100% of malware, eThreatz testing shows.” CSO Online, January 15, 2015
8. “Privacy Uncovered: Can private life exist in the digital age?” Economist Intelligence Unit, April 18, 2013
9, 10. “2013 Cost of Data Breach Study: Global Analysis.” Ponemon Institute, May 2013

The Media Trust
With a physical presence in 65 countries and 500 cities located around the globe, The Media Trust’s proprietary website and ad tag scanning technology provides continuous, non-stop protection against malware, site performance issues and data leakage, which can lead to lost revenue and privacy violations.

The Company also enables comprehensive quality assurance of an ad campaign’s technical and creative components, supporting display, rich-media, video, search and mobile advertising. In addition, The Media Trust's technology provides publishers with visual ad verification for geographically-targeted campaigns, ensuring thousands of media buys are executed correctly, reducing discrepancies, errors and make-good scenarios in-flight.

More than 500 publishers, ad networks, exchanges, agencies and enterprises—including 40 of comScore’s AdFocus Top 50 websites—rely on The Media Trust’s suite of continuous, non-stop monitoring, detecting and alerting services to protect their websites, their revenue and, most importantly, their brands.