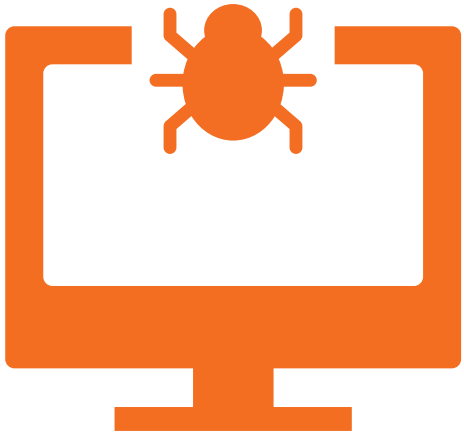
SOPHOS



Five Stages of a Web Malware Attack

A guide to web attacks—plus technology, tools and tactics for effective protection

By **Chris McCormack,** Senior Product Marketing Manager

Today's web attacks are extremely sophisticated and multi-faceted, motivated by a massive underground economy that trades in compromised computers and user information. This paper shows you how modern web attacks work, broken down into five stages, from entry through execution.

We'll explain the advanced techniques hackers use to infect web users and steal data or money, and how most web security products are failing. Most importantly, we'll give you insight into the layers of protection you need, and a checklist for evaluating your policies and the security capabilities of your web protection solution.

Contents

Web Malware by the Numbers

The web is a dangerous place. SophosLabs sees an average of 30,000 new malicious URLs every day, and 80% of them are compromised, legitimate websites. Eighty-five percent of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web.

Further, the opportunities for criminal hackers are growing at an astounding rate. Consider how big the web is and how many people use it daily. There are more than 2.7 billion users on the web each day, conducting 3 billion search queries.[1] There are roughly 700 million websites, a number that grows about 10% per year.[2]

Even if you haven't encountered a web threat or malicious site lately, it's happening to millions of web users every day, spreading the infection. In fact, according to Google's Transparency Report,[3] the number of users who see browser warnings is consistently tens of millions per week.

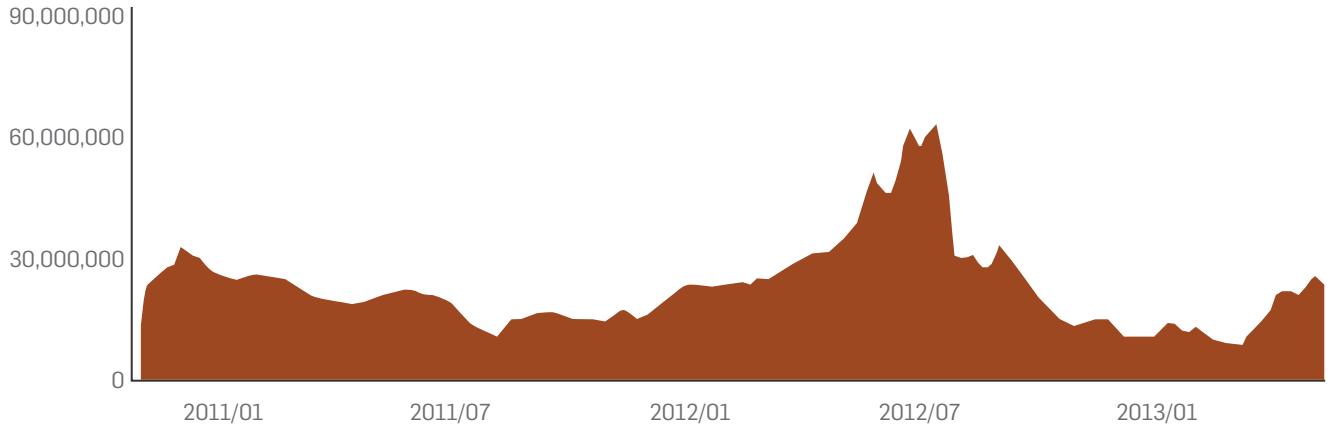


Figure 1: Number of users seeing warnings each week from Google Safe Browsing.
Source: Google Transparency Report.

1 Infographic: The Incredible Growth of Web Usage [1984-2013], WhoIsHostingThis, August 21, 2013, http://www.whoishostingthis.com/blog/2013/08/21/incredible-growth-web-usage-infographic/
2 Internet 2012 in numbers, Royal Pingdom, January 16, 2013, http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/
3 Safe Browsing Transparency Report, Google, http://www.google.com/transparencyreport/safebrowsing/

How a Web Attack Works—The Five Stages

This section shows you how modern web attacks work, broken down into five stages: entry, traffic distribution, exploit, infection and execution.

Figure 2: Infographic of the five stages of a web attack.

Stage 1: Entry

The first part of an attack involves a drive-by download from an entry point, either a hijacked website or an email that contains a malicious link.

Drive-by downloads

A drive-by download is the process of inadvertently downloading malicious web code simply by visiting a web page. A drive-by download happens automatically and without the user knowing.

The most common type of drive-by download is an invisible 0x0 pixel iFrame that contains malicious JavaScript code. And this sophisticated JavaScript can be masked by obfuscation (in other words, making them unreadable), as well as polymorphic (meaning, the code changes with each view). Traditional signature-based antivirus solutions can't detect this kind of tricky code.

How trusted websites get hijacked

Web servers like Apache and IIS, as well as their content management systems, have vulnerabilities. Savvy hackers using website exploit tools can attack these vulnerabilities to inject malicious code into web pages.

One popular exploit tool is called Darkleech, a rogue Apache module that allows attackers to dynamically inject malicious iFrames into websites hosted on the servers. From October 2012 to July 2013, more than 40,000 websites were infected by Darkleech.[4]

Other websites can be taken over through stolen login credentials. Many sites hosted by Wordpress can be compromised using login credentials that are easily guessed or obtained through brute force attacks. Once hackers have the login credentials for your site, they can inject an endless stream of malware.

Technology, tools and tactics for effective protection

For years people have assumed that most threats lurk in the darker parts of the Internet, such as adult, gambling or hacking sites. If that were true, all we would need to stay protected is a URL filter to block those sites. Unfortunately, the truth is more complicated.

When we look at the 10 most-infected website categories, adult sites rank last at just 2%. Categories like blogs, hosting and businesses are far more susceptible to hosting malware.[5]

4 Rampant Apache website attack hits visitors with highly malicious software, Ars Technica, July 3, 2013, http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/

5 Surprise! The Most Dangerous Web Sites Aren't Porn Sites, TechNewsDaily, June 4, 2012, http://www.technewsdaily.com/4365-porn-dangerous-web-site.html

Top 10 infected website categories

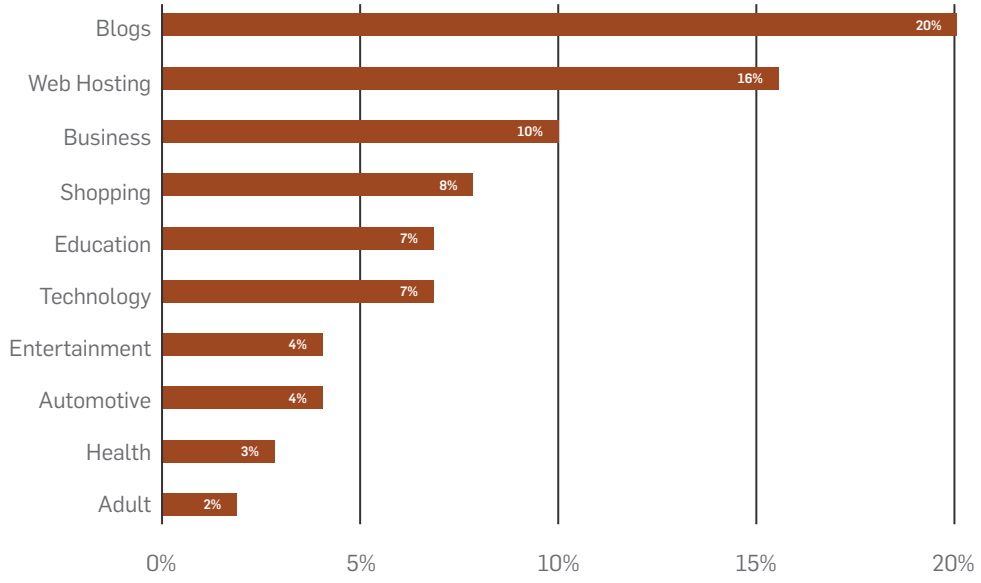


Figure 3: Top 10 categories of malicious sites. Source: TechNewsDaily

And what's worse, malicious ad campaigns (also known as Malvertising) can have wide reach across a broad range of legitimate sites, further compounding the problem of solving this with URL filtering.

So what do you need for effective protection? URL filtering is still important. But a better solution includes **live reputation filtering** that's updated continuously to catch newly infected sites. In addition, a **safe surfing policy** is only effective if users aren't able to easily bypass it, so make sure you can block anonymizing proxy abuse.

Perhaps the most important technology you need to combat web threats at this layer, and beyond, is **advanced web threat protection**. You need the latest threat protection that scans all downloaded web page content for malware using advanced technologies like JavaScript emulation, which can detect suspicious or malicious code before it reaches the browser. And you need this not just at your network gateway, but also on your endpoints or in your desktop antivirus to protect offsite users.

Also be sure to use a browser that supports Google's Safe Browsing API (https://developers.google.com/safe-browsing/) like Chrome, Firefox, or Safari that can identify some malicious sites in search results, giving users a heads-up before they attempt to visit an infected site.

Also invest in some **safe surfing training** with your less computer savvy users to educate them on what to watch for and how to avoid common social engineering tricks and obvious scams in email.

Last but not least, make sure your site is not contributing to the problem. Use strong passwords for your website CMS or Wordpress blogs. And audit your site's code to find potential vulnerabilities. Protect your site with a **web application firewall** that can harden forms and stop unwanted attacks.

Stage 2: Traffic Distribution

Once a drive-by download has reached the browser, the unsuspecting user is redirected to download an exploit kit. However, rather than sending users to known exploit kit hosting sites, elaborate traffic distribution systems (TDS) create multiple redirections that are nearly impossible to track and therefore black-list.

Some TDS systems are legitimate, for instance those used for advertising and referral networks. But like any software, legitimate TDS solutions are prone to being hacked and exploited to drive traffic to malware hosting sites instead of a benign destination.

Cybercriminals are using one TDS called Sutra to manage traffic from drive-by downloads based on a user's IP geolocation, operating system, browser or other metadata that can boost infection rates. Hackers can buy the latest version of Sutra TDS 3.4 for just $100, with a pay-off of more than a million clicks per hour on a low-end server.

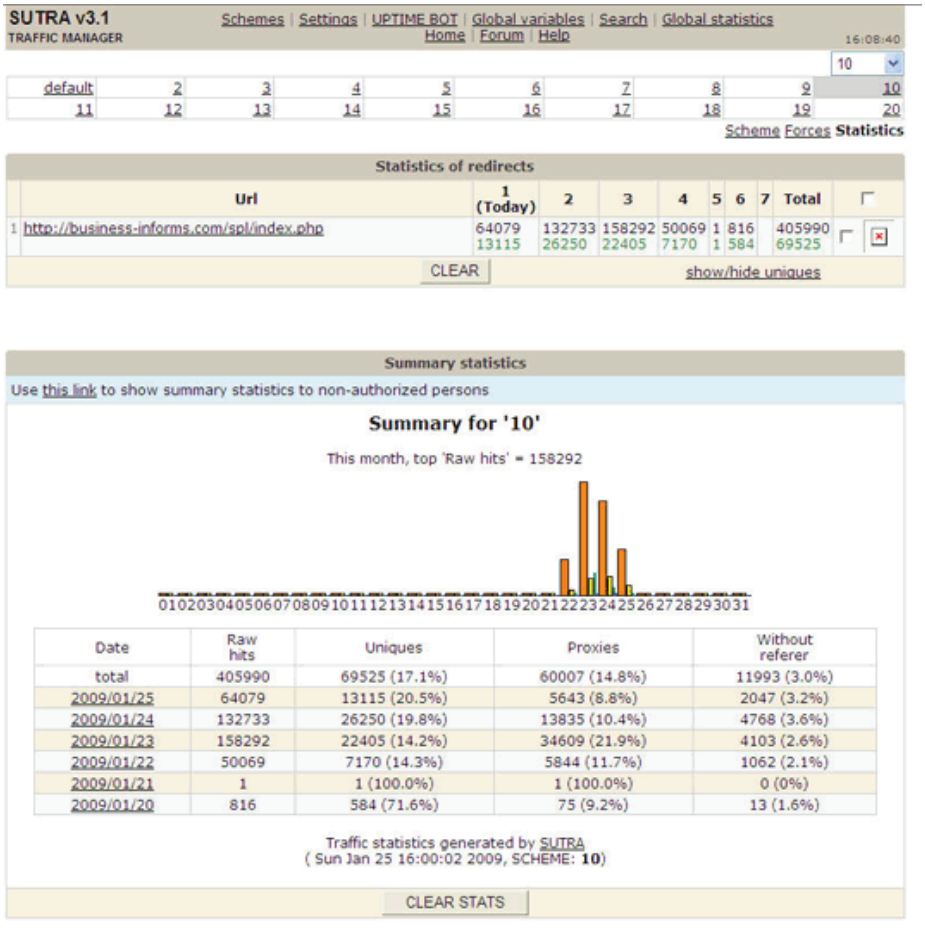


Figure 4: Commercial TDS solutions like Sutra are often employed by hackers to keep their malware hosting sites hidden behind a complex traffic distribution infrastructure.

What's more, these TDS networks often filter traffic to keep their sites hidden from search engine and security companies. They also use fast-flux networks to cycle thousands of IP addresses through DNS records, preventing their malware hosting sites from being blacklisted.

Technology, tools and tactics for effective protection

The stealthy nature of TDS makes security at this layer very challenging. It's impossible for the user to prevent a redirection chain since it happens instantly and silently in the background. It's also extremely challenging for most security companies to keep up.

It's super important that your selected network security and web filtering solution come from a vendor that understands TDS and is investing in tracking TDS system abuse. For example, given the right resources, it's possible to monitor and track the reputation of DNS registrars to keep one step ahead of hackers, blocking proxies and redirects before they even come online.

Stage 3: Exploit

The next phase of a modern web attack is the downloading of an exploit pack from the malware hosting site. These kits execute a large number of exploits against vulnerabilities in web browsers and associated plugins such as Java, PDF readers, and media players.

Exploit packs

Cybercriminals typically purchase exploit packs on the black market, making money for their creators. Since it emerged in late 2010, the Blackhole exploit kit has become one of the most notorious. The Blackhole creators have built a sophisticated business around it—selling it as a service for $500 a month. The Blackhole operators even offer a web-based management console and online technical support.

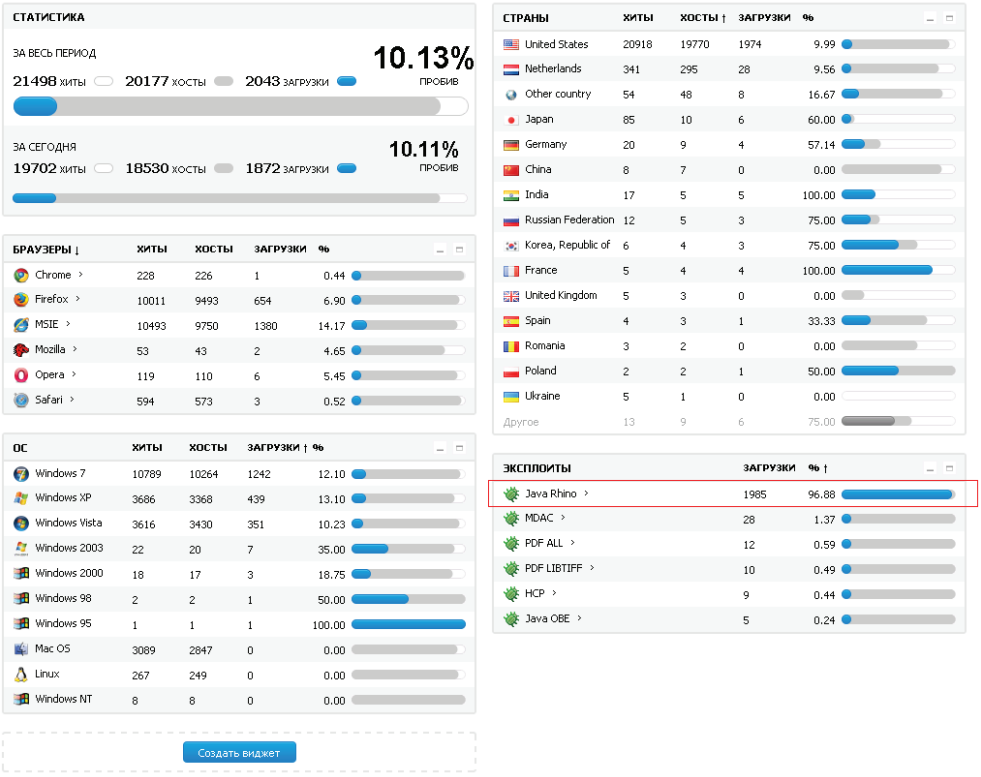


Figure 5: A screenshot of the Blackhole dashboard.

In this snapshot of the Blackhole dashboard, we can see how the cybercriminals are able to track their infection success rate, the number of sites hosting the malware, the systems affected, and the country location of the infected sites.

Once a user's browser has landed on a site hosting the Blackhole exploit kit, it will load files that target vulnerabilities relevant to the victim's computer based on information readily available from the browser. Four types of files are often used to exploit vulnerabilities in the users system:

- **PDF:** PDF files with embedded JavaScript attempt to exploit known vulnerabilities in Adobe Reader.
- **Flash:** Two types of flash files with specially designed code are often loaded to exploit Adobe Flash Player.
- **Java:** JAR files with either JavaScript or applet code are usually the most successful at finding an exploit.
- **HTML/JS/VBS:** Runtime code can be downloaded to target a vulnerability in Microsoft Help and Support Center.

Of course, as with all other parts of a web attack, the scripts, code and content loaded during the exploit kit phase is heavily obfuscated and polymorphic to evade detection.

Java Rhino

Unfortunately, Java is a hacker's dream. Billions of devices and browsers come equipped with Java, and it's on every platform. One of the more popular and successful exploits, Java Rhino, is a script engine included with Java that could be exploited to run arbitrary code outside of the Java sandbox. The exploit works on a vast number of clients running Java version 7 and earlier. Despite a patch being available, this is still a very effective exploit. According to Qualys, 80% of enterprise systems are running an outdated, unpatched version of Java.[6]

Technology, tools and tactics for effective protection

Advanced web malware detection is critical to blocking the exploit code as it's downloaded and before it can attack vulnerabilities. However, the authors of these kits use obfuscation and polymorphism to evade detection from antivirus engines.

Effective web malware protection goes beyond signature-based detection, using a combination of URL filtering to block known hosting sites, and **threat intelligence** that continuously monitors and samples exploit kits to determine detection algorithms.

Another essential strategy for reducing the surface area of attack is tightly controlling your users' choice of web browsers and applications like PDF readers. By limiting the number and variety of these applications, and keeping those carefully selected applications patched, you can dramatically reduce the number of vulnerabilities exploit kits will take advantage of.

It's sad but true—90% of attacks against application vulnerabilities could have been prevented with an existing patch.[7] However, users often forgo **patching** because it can be a tedious job. Fortunately, there are solutions that can integrate with your desktop security solution to control end-user applications and identify and prioritize security patches.

In devising a **web client software policy**, here are a few key security considerations to keep in mind:

- **Browser:** Where possible, stick with a single mainstream browser that supports Google's Safer Browsing API such as Google Chrome, Mozilla Firefox or Apple Safari. Popular browsers invite more exploits but their vendors also have more resources to address vulnerabilities and provide patches more often.
- **Java:** Unless you require Java for business related web applications, disable or remove it from your users' computers, or limit it to only those users that absolutely require it.

6 The Dark Side Of Java, Dark Reading, December 1, 2011, http://www.darkreading.com/attacks-breaches/the-dark-side-of-java/232200604

7 Improving Your 2011 Security Bang for the Buck: Patching Depth and Breadth, Gartner blog, January 4, 2011, http://blogs.gartner.com/neil_macdonald/2011/01/04/improving-your-2011-security-bang-for-the-buck-patching-depth-and-breadth/

- **PDF reader:** Use a single mainstream PDF reader. Keep it patched with the auto-update feature enabled, and advise users to install patches as soon as they become available.
- **Plugins, add-ons and toolbars:** Avoid any browser plugins and toolbars. They only increase the attack surface area.

Stage 4: Infection

Once the attacker exploits an application vulnerability to gain some control over the computer, the next step in the attack is to download a malicious payload to infect the system. The payload is the actual malware or virus that will ultimately steal data or extort money from the user.

The hacker can choose from a wide range of different infectious payloads. Here are some of the most common payloads used today.

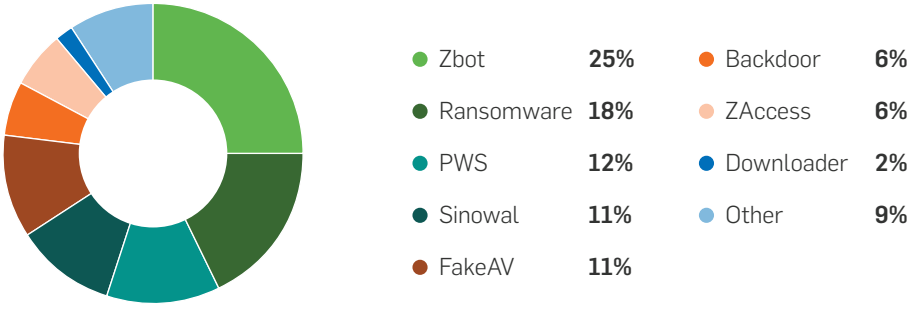


Figure 6: A breakdown of payloads from Blackhole over a two-month period (August and September of 2012). Source: SophosLabs

- **Zbot (Zeus):** Zeus is a Trojan horse that steals personal information by logging keystrokes and grabbing frames in the browser. It initially targeted Windows machines but variants have been found that infect Android mobile devices as well.
- **Ransomware:** Ransomware is a class of malware that restricts access to a user's computer or files, demanding payment to regain access. It primarily targets Windows, but there's also a less harmful but equally annoying Mac variant that recently started appearing.
- **PWS:** PWS is a password stealing and remote access Trojan that infects Windows computers.
- **Sinowal (Torpig):** Torpig is a botnet infection which targets Microsoft Windows computers. It uses a rootkit to steal credentials and allow remote access.
- **FakeAV:** FakeAV (fake antivirus) installs a rouge security software client that appears to be a desktop antivirus application. It scans and finds numerous fake viruses and extorts the user into paying to "clean up" the viruses. It primarily plagued Windows systems, but is now being found on Macs as well.

Technology, tools and tactics for effective protection

At this stage, malware is being downloaded to the victim's computer. At this point in the attack, you're relying on **web malware scanning** and **content filtering** that has so far failed to detect an attack.

The only hope is that the payload is less sophisticated than the malicious code that escaped detection at the earlier stages. Obviously, this is not a dependable defense. The best strategy is to get better **web malware protection** to catch it at an earlier stage in the attack.

Stage 5: Execution

In this final stage of the attack, the malicious payload has been downloaded and installed on the victim's system and now its job is to make the criminal behind it some money. It can do that in a number of ways: by providing credentials, banking or credit card information that can be sold on the black market, or by extorting the user into paying directly. Ransomware and FakeAV are both examples of malware that extort victims into paying. Let's examine some of the latest variants of ransomware to see what goes on.

Encrypting ransomware uses increasingly sophisticated encryption to make files inaccessible until the ransom is paid (usually around $100). In 2013, a new variant called Cryptolocker appeared that encrypts all personal and work related files and will only decrypt them in exchange for a $300 fee. The encryption is sophisticated enough that the only option, in lieu of restoring from a backup, is to pay the ransom.

Non-encrypting ransomware is available in different variants that can lock a user out of their computer in exchange for ransom. One type displays a fake Windows activation message and payment option; another devious variant not only locks a user out, but displays a fake law enforcement message demanding payment of a fine for illegal software or child pornography possession. These latter types of ransomware go to great lengths to look legitimate including localization to fit the victim's language and country of residence.

Figure 7: A typical ransomware demand.

Figure 8: Localized versions of the ransom demand for various countries.

Ransomware for Mac. With the growing market share of Apple Macs among consumers and corporate users, it's perhaps not surprising that there's now a variant of ransomware for the Mac. It works slightly differently, using a simple JavaScript that takes over the browser and constantly reloads the same ransom demand page, regardless of what the user does. In the case of this Mac variation (figure 7), the fix is rather simple. The problem is that the fix is not obvious to the average user and the impact is so annoying that this malware is likely very effective, and lucrative (at $300 per instance).

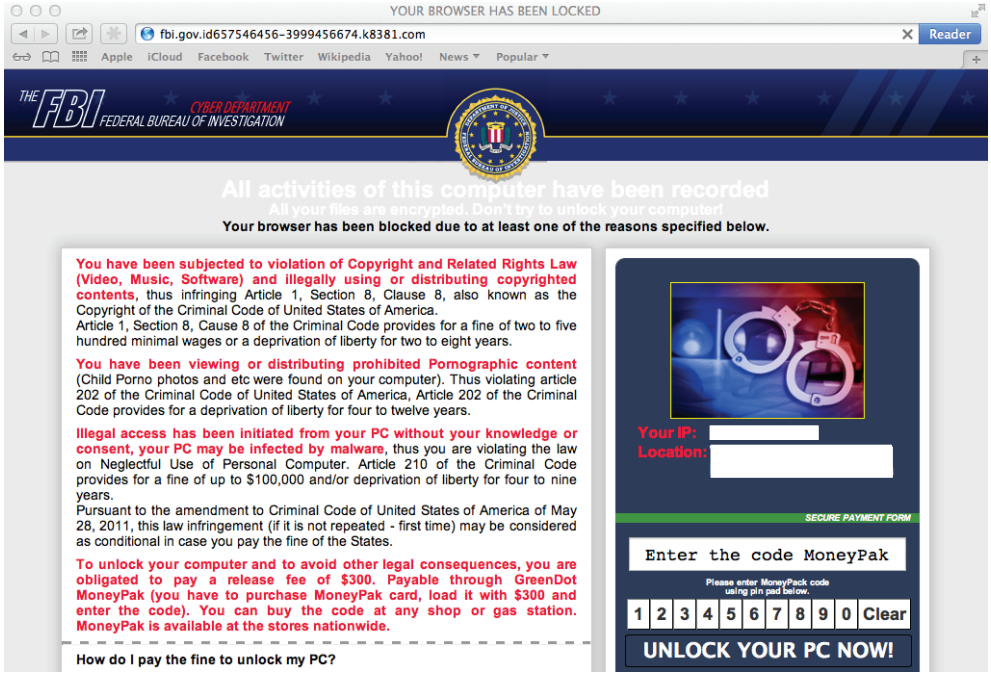


Figure 9: A Mac ransomware message purports to come from the FBI. Source: Malwarebytes, http://blog.malwarebytes.org/intelligence/2013/07/fbi-ransomware-now-targeting-apples-mac-os-x-users/

Technology, tools and tactics for effective protection

An attack at the execution stage moves past your web protection to your last line of defense—your **desktop antivirus**. At this layer, the attack consists of an executable, rootkit, or other malware resident on the machine that's trying to steal sensitive data, encrypt files, or lock a person out of their machine. Once the attack reaches this point, only endpoint protection with real-time updates and advanced **host intrusion prevention system (HIPS)** technology can help prevent the infection.

In the past, antivirus detection relied on signatures. When new threats were discovered, a new detection signature was issued as an update. Today, as we've seen, the threats are too sophisticated and change with each instance to the point where signatures and old-fashioned antivirus updates are no longer effective.

The detection of today's advanced malware requires HIPS. It can catch threats normal antivirus engines cannot by detecting malicious behavior. HIPS engines consist of a set of advanced rules to detect suspicious system behavior and notify you or block it before it can do any substantial damage. The best HIPS implementations build in best practices so you don't have to set up your rules to prevent false positives while still catching new malware.

Another technology that can combat infections at this stage is **call-home detection**. Call-home detection is a feature of some secure web gateway solutions that can detect infected computers by their requests for known malware command-and-control URLs. While this feature can't prevent infection, it can help you identify infected systems on your network.

Checklist of Technology, Tools and Tactics for Effective Web Protection

An effective web protection strategy requires policies to reduce the surface area of attack, appropriate tools and technology to enforce those policies, and protection to block attacks at every layer.

Download our checklist of technology, tools and tactics for effective web protection to evaluate your policies and web protection.

Download now

Sophos Web Protection

At Sophos, we make web protection simple to deploy, manage and maintain. Our affordable suites include everything you need for an effective defense against the latest web threats. We offer the best protection supported by SophosLabs—our global 24/7 threat analysis operation. And we provide the best support in the industry.

Sign up for a free trial at Sophos.com
Sophos Secure Web Gateway
Sophos EndUser Web Protection Suite

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

job number-month.year.designer initials.literture suffix and na.simple

SOPHOS