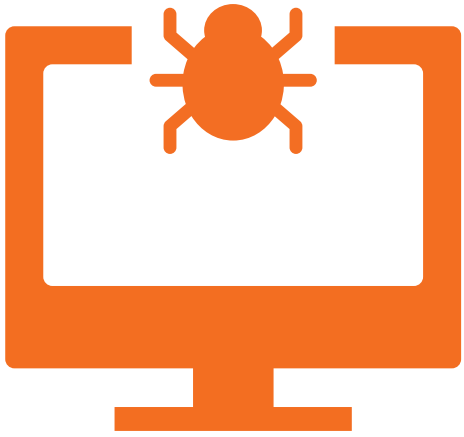
SOPHOS



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 60% 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 3.4 billion users on the web each day (1), conducting 3.5 billion search queries, with Google alone(2), on over 1 billion websites.

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,[1] the number of sites deemed dangerous by Safe Browsing is consistently in the hundreds of thousands per week.

Number of sites deemed dangerous by Safe Browsing

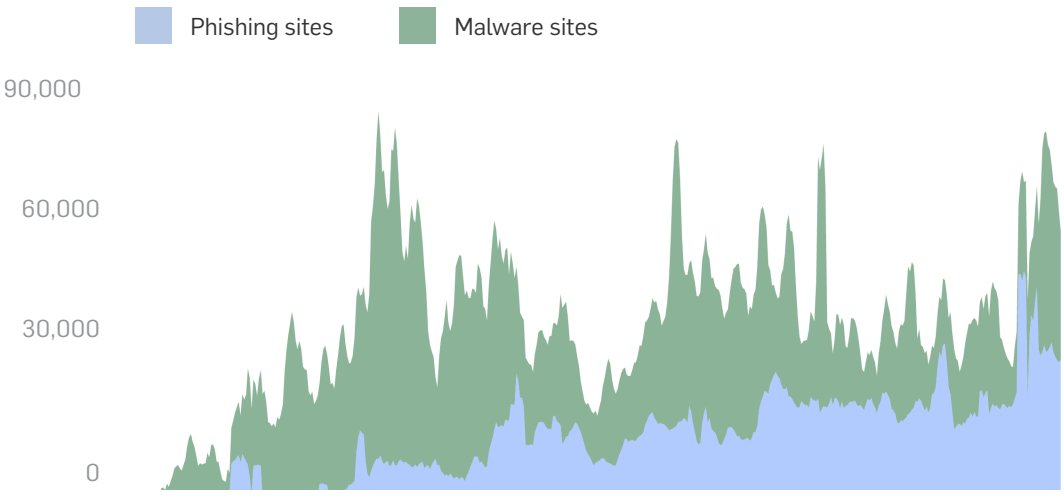


Figure 1: Number of users seeing warnings each week from Google Safe Browsing.
Source: Google Transparency Report.

1, 2 and 3. Internet Live Stats

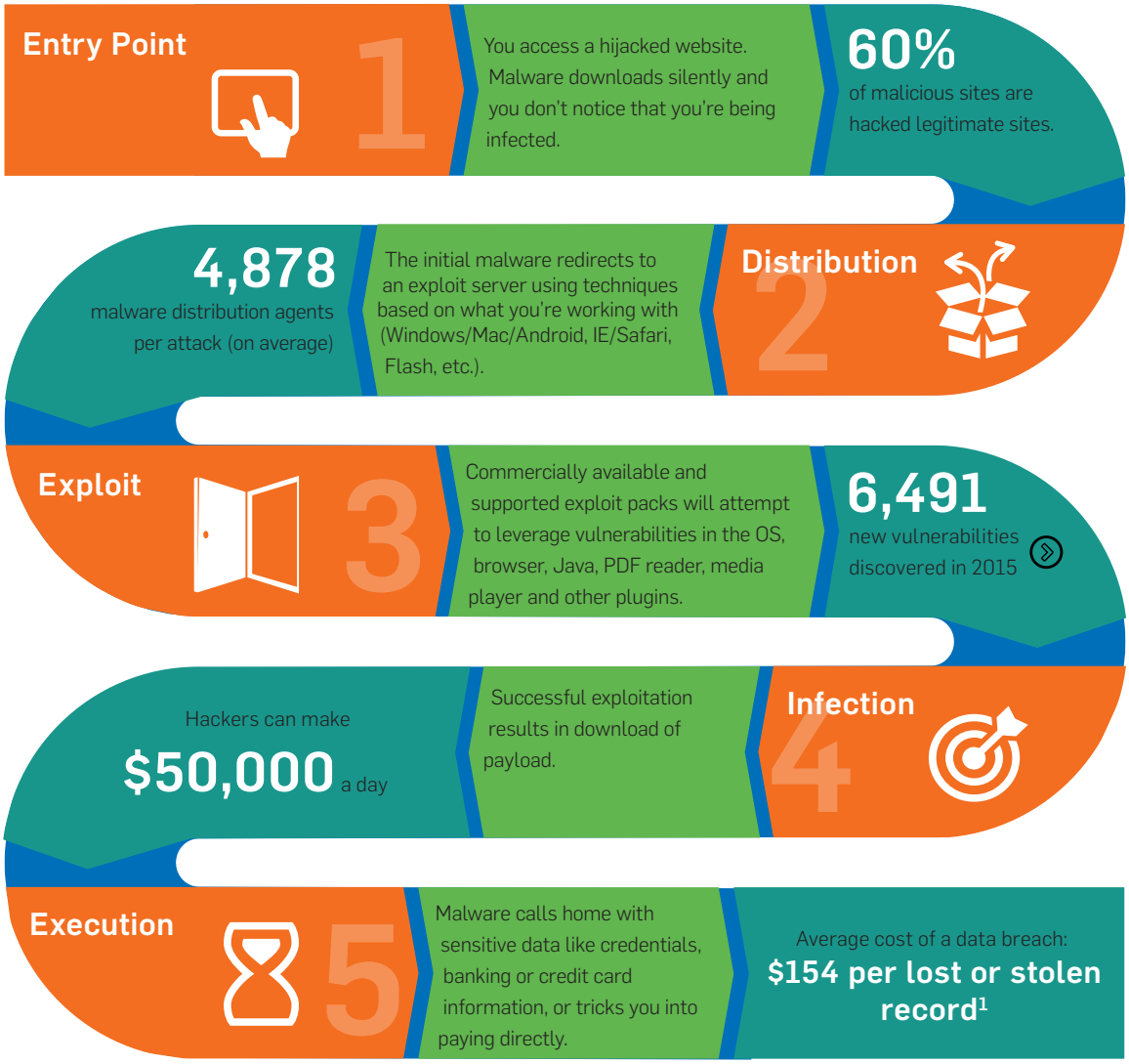
1 http://www.internetlivestats.com/internet-users/

2 http://www.internetlivestats.com/google-search-statistics/#share

3 http://www.internetlivestats.com/total-number-of-websites/

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.



Ponemon Institute May 2015 https://securityintelligence.com/cost-of-a-data-breach-2015/

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 a malicious JavaScript injected into legitimate web content that redirects the browser to further malicious 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.

Some campaigns, such as Darkleech for example, have been active for several years. As the exploit kit landscape changes, the underlying traffic redirection tools simply change as necessary.

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.

Categories like blogs, hosting and businesses are far more susceptible to hosting malware than adult or gambling sites.

Top 10 infected website categories

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 network sandboxing and JavaScript emulation, which can detect suspicious or malicious code before it reaches the browser. And you need technologies like this this not just at your network gateway, but also on your endpoints or in your desktop antivirus to protect offsite users.

Be sure to use an up-to-date browser and 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 and unique passwords and two-factor authentication wherever possible. Audit your site's code to find out of date software and 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 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.

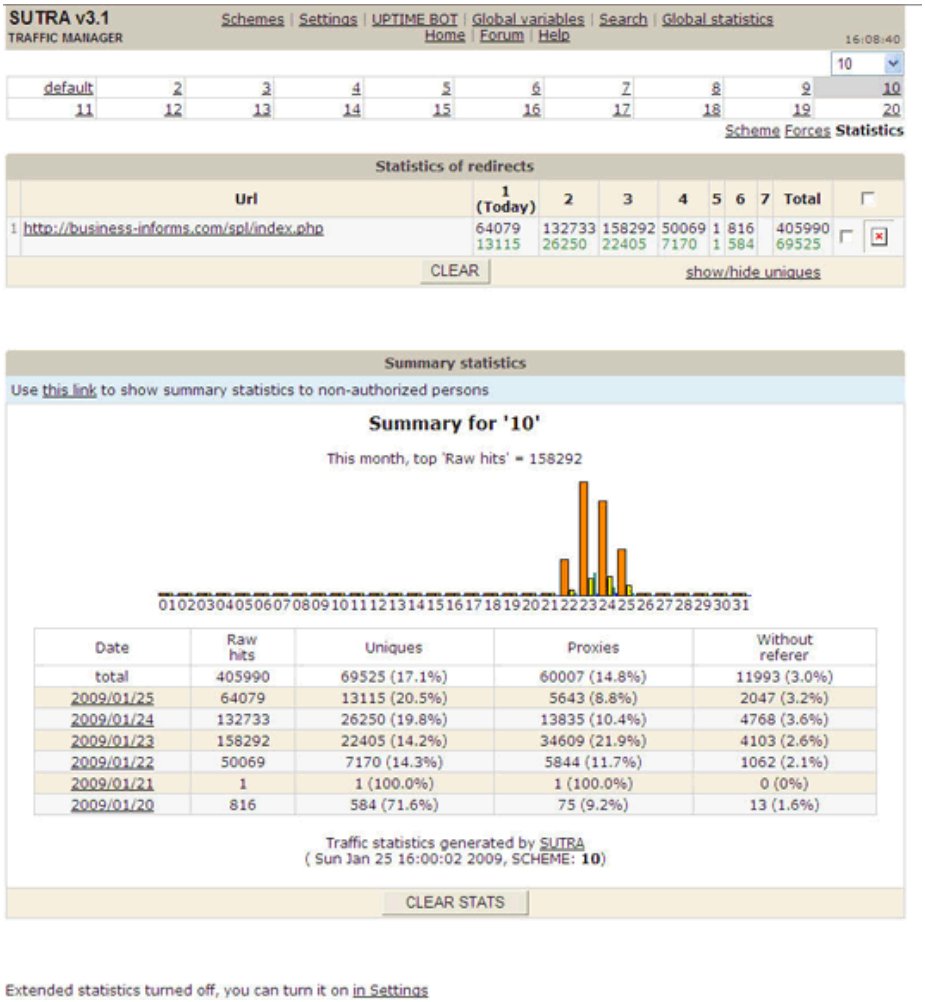


Figure 4: Commercial TDS solutions like Sutra are often employed by hackers to keep their malware hosting sites hidden behind a complex traffic distribution infrastructure.

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 inweb browsers and associated plugins such as Flash, Silverlight, and Java.

Exploit packs

Cybercriminals typically purchase exploit packs on the black market, making money for their creators. Angler first appeared in late 2013, and since then has significantly grown in popularity in the cyber underworld. Its aggressive tactics for evading detection by security products have resulted in numerous variations of the various components it uses (HTML, JavaScript, Flash, Silverlight, Java, and more). Until recently Angler has been extremely prevalent. For example, in May 2015, Sophos uncovered thousands of new web pages compromised with Angler every day.

Once a user's browser has landed on a site hosting the Angler exploit kit, it will load files that target vulnerabilities relevant to the victim's computer based on information readily available from the browser.

The good news is that SophosLabs recently noticed all Angler activity ceasing. Sophos suspects that Angler's disappearance is related to a recent, large-scale cybercrime crackdown in Russia, when Russia's Federal Security Service (FSB) arrested 50 suspects suspected of being part of a criminal group that had stolen nearly $50 million by means of banking malware known as Lurk.

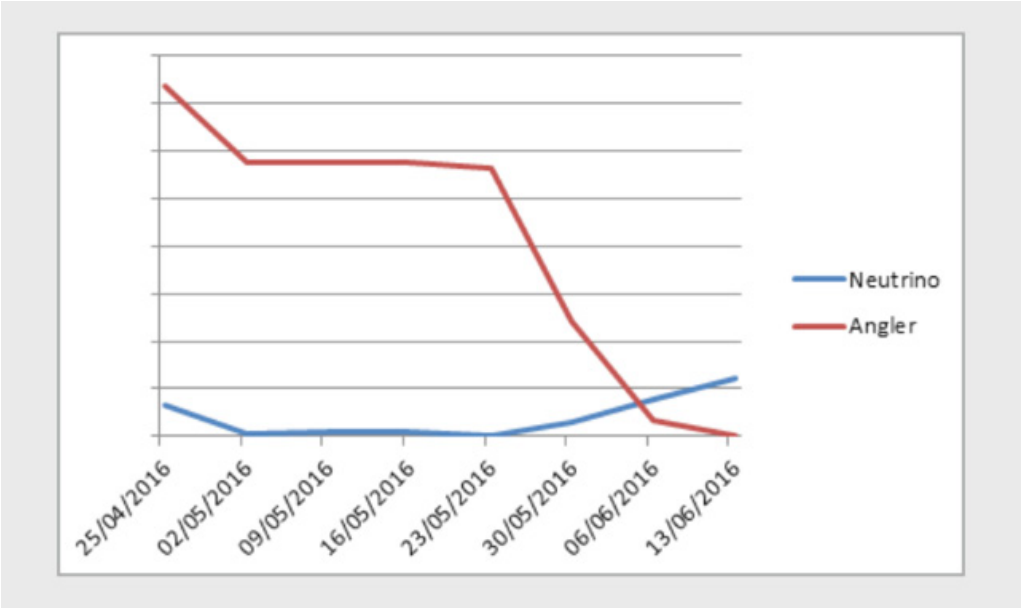


Figure 5: Instances of Angler as recorded by Sophos Labs

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.[2]

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.[3] 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.

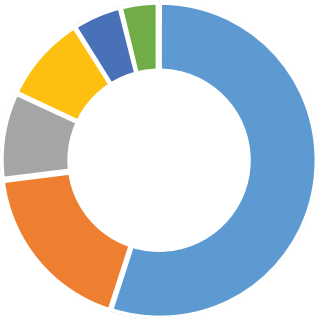
In devising a **web client software policy**, here are a few key security considerations to keep in mind:

- **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.
- **Flash:** Unless you require Flash for business related web applications, disable or remove it from your users' computers, or use web controls to block inbound Flash content.
- **Silverlight:** Unless you require Silverlight for business related applications, disable or remove it from your users' computers.
- **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.



CryptXXX*	**55%**	Cryptowall*	**9%**
Teslacrypt*	**18%**	Gozi	**5%**
Vawtrak	**9%**	Other	**4%**

Note the ransomware here (*), with majority of payloads being some flavor of ransomware.

Figure 6: A breakdown of payloads from Angler during May 2016 Source: SophosLabs

- **Ransomware:** Ransomware is a class of malware that restricts access to a user's computer or files, demanding payment to regain access. CryptXXX, Teslacrypt, and Cryptowall are all forms of ransomware. In total Ransomware was 82% of Angler payloads demonstrating ransomware's increasing dominance of the threat landscape as cyber criminals have seen just how profitable this type of attack can be.
- **Vawtrak:** Vawtrak is an information stealing malware family that is primarily used to gain unauthorized access to bank accounts through online banking websites. Machines infected by Vawtrak form part of a botnet that collectively harvests login credentials for the online accounts to a wide variety of financial and other industry organizations. These stolen credentials are used to initiate fraudulent transfers to bank accounts controlled by the Vawtrak botnet administrators.
- **Gozi:** Gozi is a widespread and successful family of zombie malware, dating back to 2007, that aims to steal online banking credentials using HTML injection.

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 Encrypting ransomware uses increasingly sophisticated encryption to make files inaccessible until the ransom is paid. Cryptolocker, one of the most prevalent ransomware, encrypts all personal and work related files and will only decrypt them in exchange for a $500 fee. The encryption is sophisticated enough that the only option, in lieu of restoring from a backup, is to pay the ransom.

For more detailed information click here: The Current State of Ransomware and here: How to stay protected against ransomware.

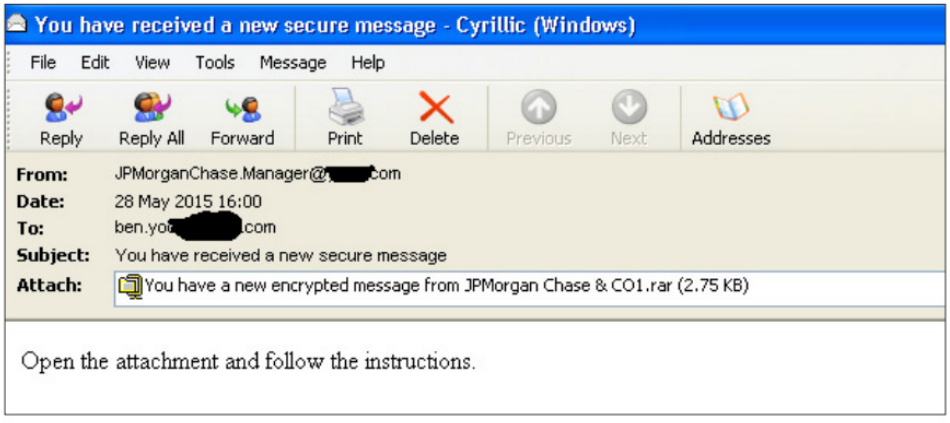


Figure 7: Email with spam attachment that contains a CHM file which links to the CryptoWall payload

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 6i3cb6owitcouepv.payoptvars.com/[redacted]
2. 6i3cb6owitcouepv.payforusa.com/[redacted]
3. 6i3cb6owitcouepv.paywelcomefor.com/[redacted]
4. 6i3cb6owitcouepv.payemarateslines.com/[redacted]

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. 6i3cb6owitcouepv.onion/[redacted] ◄Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
6i3cb6owitcouepv.payoptvars.com/[redacted] ◄Your Personal PAGE
6i3cb6owitcouepv.onion/[redacted] ◄Your Personal PAGE(using TOR)
[redacted] ◄Your personal code (if you open the site (or TOR 's) directly)

Figure 8: Cryptowall ransom demand

Figure 9: Payment page with offer to decrypt one file for free

Ransomware for Mac: With the growing market share of Apple Macs among consumers and corporate users, it's perhaps not surprising that there are now variants of ransomware forthe Mac OSX/KeRanger-A. The criminals have largely copied the ransomware formula that works on Windows. The malware encrypts everything it can find in your home directory and a long list of file types on all mounted volumes such as USB keys, removable disks, and network shares.

If you don't have a backup from which you can restore your scrambled files, the only practical way to get them back is to follow the instructions in the README_FOR_DECRYPT.txt file which is created in every directory where a file was encrypted. As you can see, in figure 9 below, it involves paying a ransom of over $400 to restore your files.

README_FOR_DECRYPT.txt

```
Your computer has been locked and all your files has been encrypted with
2048-bit RSA encryption.

Instruction for decrypt:

1. Go to [redacted]( IF NOT WORKING JUST
DOWNLOAD TOR BROWSER AND OPEN THIS LINK: [redacted])
2. Use [redacted]as your ID for authentication
3. Pay 1 BTC (~410.63$) for decryption pack using bitcoins (wallet is
your ID for authentication - [redacted])
4. Download decrypt pack and run

---> Also at [redacted] you can decrypt 1 file
for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you
are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!!) BITCOINS
HOW TO BUY BITCOINS:
https://localbitcoins.com/guides/how-to-buy-bitcoins
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
```

Figure 9: OSX/KeRanger-A file decryption instructions. https://nakedsecurity.sophos.com/2016/03/08/ransomware-arrives-on-the-mac-osxkeranger-a-what-you-need-to-know/

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. This can help prevent ransomware from encrypting your files. Ransomware typically relies on the call-home connection to get the key(s) used for encrypting user documents. In this case, call-home detection can prevent file encryption, since the traffic is blocked.

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 web gateway solutions let you take control of your web traffic and block the latest threats everywhere users go - even when they're not on your network. Sophos solutions include advanced web malware protection with technologies like network sandboxing for complete peace of mind. You can choose either a cloud-delivered secure web gateway or a dedicated purpose-built web appliance. Plus, at the endpoint, our affordable bundles deliver comprehensive security for users and data - all with a single license. We also 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 Protection Bundles

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

11.16.wpna.simple