

Web Security



Do you know how systems are usually compromised?

By what's known as a "drive-by download".

Simply viewing an infected web page, your system can render control to someone with malicious intent.

How can you tell which web pages are infected and which ones are safe?

You can't.

It's not just adult web sites, or gambling sites that infect systems it can be any web page on any web site. Our research has shown web pages on a news site that were infected with a drive-by download. The webmaster was not aware of it, nor did they place it there.

Someone "hacked" into their web site, uploaded some malicious code and went on to other malicious activity just waiting for some poor unsuspecting soul to visit the page, get infected and send an alert to the hacker.

Do you know what web sites your employees are visiting?

Do you know which sites are infected and which ones are safe?

The BOX provides security through a number of methods:

- Blacklists of sites
- Blocking methods of download
- Restricting downloadable file types
- Anti-virus
- Managing the security

Let's look at each one of these closer.

Blacklists of sites

At e-Based Security we use three primary methods for building our blacklists. First we collaborate with other groups online and find web sites that have malicious code on them or sites that sponsor malicious activity.

These lists are downloaded daily to each BOX.

Secondly, we have automated systems that continually scan web sites looking for anything malicious. Any sites found here **are not** automatically added to our blacklists because we feel this method isn't foolproof. Our system could detect some code that appears malicious but is actually safe so we also have people literally view these sites.

Last, we have people that scan certain search terms online and find new sites that we haven't added to our lists. This is your assurance that we don't accidentally blacklist a site that you need for your business.

The Internet is a dynamically growing environment – and your defense must be dynamic as well.

As people in your office view web sites, before their browser opens the web page, it's checked against the blacklist. If the web site is blacklisted, the user would see a big red web page that informs them their activity has been blocked and recorded. We can modify the message to suit your environment.

We also know that as a small business owner you may not want to restrict access to web sites. By blocking the method of downloading, we can provide safe viewing of any web site.

Blocking methods of download

If the web page the user wants to see is not on any of our blacklists, next it's passed to our web content filters.

These filters scan the code of the web page looking for anything we've identified as potentially malicious. Generally this is code that allows files to be downloaded to your system – without any interaction from the user.

We have carefully investigated the various methods available for web pages to download files onto your system.

By default these are all blocked.

This does “break” some legitimate web sites. When you or your employees view them, they might look strange. However as your dedicated security team, if there is a web site you need, you can contact us and we will review it – immediately, and providing it passes our tests, we will “whitelist” it, first on your BOX then we'll add it to our master whitelist which gets “pushed” out every day to all clients.

We could do like many other companies and play the “cat and mouse” game with hackers. This is where hackers come out with something malicious, we come out with a signature file for it, they change it slightly so it no longer matches our signature, then we come out with a new signature, then they come out with a slight variation, etc...

However we decided to research the methods used to download code from a web page – there are many, and just block them by default. As stated earlier, we block everything other than that which is absolutely necessary.

For instance, by default, our system would block updates from Microsoft's web site. Obviously this site is already on our whitelist otherwise our clients would not be able to update their systems and that would be bad.

Restricting downloadable file types

We restrict the types of files that can be downloaded. This applies not only to email attachments but also files buried in web sites. Sometimes hackers will have an .exe file on a web site. As you view that page, it tries to download the .exe file onto your system.

That's right, *if* something were downloaded, meaning it made it past our filtering of downloads, the file type is checked. If it's in our list of file types to be blocked, it still doesn't make it onto the user's system.

That's your multiple layers of defense. We've strategically built these layers to provide the most protection possible.

The BOX automatically blocks executable files so you don't have to worry if the file has been modified to “fly under the radar” of your anti-virus software. Renaming the file to something that doesn't “appear” to be an executable doesn't work with The BOX.

We look deep inside the file to determine the file type.

Anti-Virus

If a specific file type is allowed, before it's allowed through The BOX to your system, it's scanned for viruses.

The BOX uses an open source anti-virus program that is constantly updated with new signatures.

Being open source means that you're protected by the collaborative efforts of millions of people around the world. People who take pride in their determination to make the Internet a safer place to work.

You don't have to worry about updating the signatures, it's handled automatically. You don't have to worry about upgrading the anti-virus software we do that for you whenever a new version is released.

Managing the security

Your BOX is fully managed by our team of security professionals. We monitor the logs and the activity for your BOX. We make adjustments to the configuration to "harden" your defense.

If something isn't working the way you require, we'll work with you to modify the configuration so you're still hardened, yet free to safely work online. We have clients who would rather have us filter everything rather than block so they can safely surf whatever web sites they like – without restriction.

Our commitment to your safety and satisfaction is what drives us to constantly strive to find new hacker methods – and then to verify you're still safe.

The BOX – designed specifically for small business owners.

Visit: <http://www.ebasedsecurity.com> to learn more.

Or call, 1-866-838-6108