GFI White Paper

How Web Reputation increases your online protection

GFI®

Contents

Introduction to Web Reputation

Web Reputation is the latest method in use to boost protection against current to future malicious content on the web for those browsing the Internet. Using Web Reputation, websites are assessed for immediate and potential threats, malicious content and risky characteristics and a score (0 – 100) is given.

In a similar way that Content Categorization places websites into different categories and classifies them based on their content, Web Reputation scores are used to determine the risk factor of each website.

Once the score for a website has been determined, this will help an administrator to take action – block/proceed with caution/allow access to those websites.

Although a good antivirus engine offers significant threat coverage, and multiple antivirus engines provide greater protection than you get with a single antivirus engine, it is very difficult to achieve total protection in a very dynamic Web 2.0 world. Web Reputation fills a void left by traditional protection engines by giving a "safety" rating to websites and where necessary, allowing proactive blocking of risky sites.

The GFI WebMonitor™ WebGrade Web Reputation Index is a comprehensive security assessment of a website based not only on its current threat level, but also on its potential to be a threat in the future. It gives each URL a score (0-100) – the lower the score, the greater the risk that website poses to users. Broadly speaking, web reputation scores typically fall into five risk bands:

- High Risk (1 – 20)
- Suspicious (21 – 40)
- Moderate Risk (41 – 60)
- Low Risk (61 – 80)
- Trustworthy (81 – 100)

Why use Web Reputation?

To better understand the benefits of Web Reputation, here is a real world example. Let's say you are going on vacation. While you are planning your holiday, you check the reviews of the hotel where you would like to stay before you actually take a decision to book or not. Unless you confirm that the hotel (which you've never stayed in before) has been given a good rating in various categories (price, cleanliness, location, family-friendly) etc. you wouldn't book your stay there.

The same concept applies to the Web. The Web Reputation Index is calculating a score for a website for you to proactively determine, on the basis of various 'safety variables', whether you should visit that site or not.

The value of using Web Reputation and antivirus software

With the growing number of malware threats and an ever-changing security landscape, it is increasingly difficult for traditional antivirus engines to be constantly up-to-date and protect users from ALL the latest threats. Different antivirus vendors have different response times to different types of emerging threats – some focus on speed and all the latest threats, while others focus on complete coverage with threat signatures going back many years.

Therefore, having additional defence mechanisms in place to protect you against new zero-hour and zero-day threats is a must. Malware authors are constantly changing their techniques and use various tricks to outsmart antivirus engines. The ability to assess websites and domains on the basis of reputation radically boosts the software's capability to protect users and organizations against new and unknown threats.

Web Reputation enhances the security engine coverage through two main features:

- It predicts the security risk a website poses before an actual threat is detected
- It keeps a record of previously infected sites and uses this data as part of the scoring mechanism

The value of using Web Reputation with Content Categorization

In web filtering, categories are used to identify the type of website, e.g. "News and Media", "Shopping" and "Search Engines" among others. Some categories are by their very nature a security risk e.g. "Phishing" or "Malware". However, all categories may feature websites which have reputation scores across the spectrum (see bands above).

What this means is that in any category you can have a mix of sites which are a risk, and others which are safe.

For example, a hypothetical website (www.snipe-a-fish.com) is categorized under "Hobbies and Recreation" – a category which is not typically considered a security threat. Although the website is in a category which is not known for pushing malicious content, the website itself is very poorly maintained, is prone to infection, and is therefore a high security risk. In fact, the website had been compromised already in the past and used to distribute malware.

On the other hand, there are many sites which are very highly rated in the same category. Such a broad range of scores in the same category holds true for all categories – meaning that the risk factor of a website is usually independent of the category in which the website is found.

This is why Web Reputation is so important – it adds a layer of protection irrespective of the category the website is in.

Anatomy of a malware attack

Cyber criminals know that the weakest link in most organizations is not the technology, but (in the majority of cases) the person sitting in front of a computer. These criminals, often out for financial gain, exploit the popularity of high traffic sites such as YouTube, Facebook and Twitter to distribute malicious links and payloads. Very often users are not even aware that by clicking on links they may be exposing their machine and the network to a number of threats. This 'attack surface' grew considerably with the introduction of short URLs (e.g. http://bit.ly/q9GelC) – all URLs look practically the same.

The attackers also know that few users think about risk when they visit a new website and they use this behavior to their advantage, riding piggy-back on the success of high traffic sites which are used to initiate the transmission of malicious content.

This content however requires a host, i.e. a website from where the content can be distributed. There are two ways to create malicious content on the web:

- Create a new website or use an existing website to host the malicious content
- Compromise (hack) a legitimate site and inject malicious content

Cybercriminals and security organizations are playing a constant cat-and-mouse game – one side creating new malicious content, the other designing protective measures to block it. The best weapon for criminals is an ever-changing malware host. Effective attacks require a website or malware strain which is currently not recognized by antivirus engines. So the best means of attack is to actually deploy new websites or website hosts as often as possible. This ensures that these websites have not been recognized by security organizations and consequently blocked. Once a website is 'caught' by antivirus engines or other security measures, it loses its effectiveness and would need to be taken down and replaced by another.

Zero-day/zero-hour

0-day/0-hour: the period of time from when a new malware hosting website is created until it is recognized as malicious. During this period, activity on these sites is considered high risk.

In the zero-hour period, no matter how many antivirus engines you have deployed, anybody visiting a website hosting new malicious content is at risk and their machine will probably be infected.

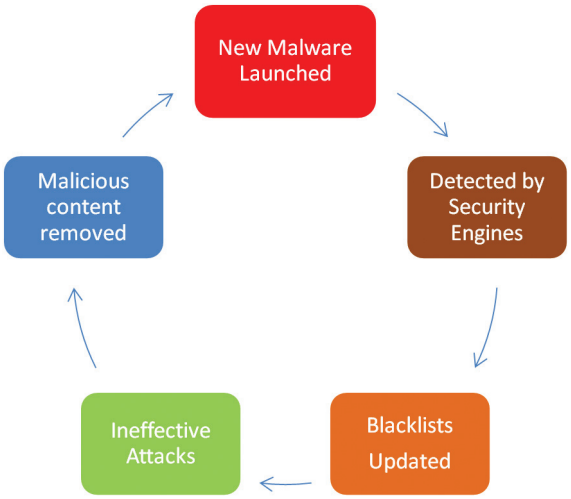

Figure 1 - Stages in malware attack cycle

So how do we mitigate this problem? Reputation is the answer. Certain types of websites, including those which have not been seen before are immediately classified as "Suspicious". Applying a reputation score to websites and classifying them as "Suspicious" is a proactive approach to security – you are addressing a risk before it can become a serious threat.

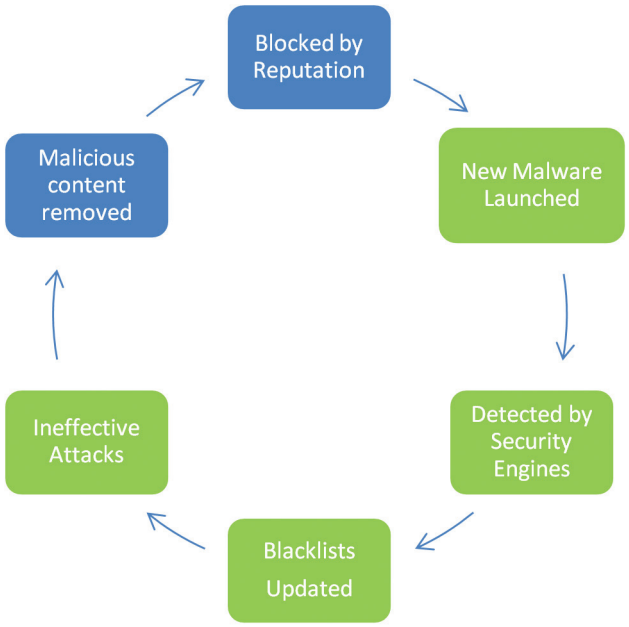

Figure 2 - How Reputation protects against unknown threats

How to use a Web Reputation Index – different scenarios

Known Compromised Sites – high risk (0 – 20)

As soon as a website is detected as being compromised, its score immediately drops into the High Risk zone. Any website classified in the High Risk Zone should be treated as a "No Go Area" – the risk of infection is high for sites in the High Risk zone.

Once the infection is cleaned, the site's reputation is restored; though the reputation score will now take into account the fact that this site has an infection history (thus its score will initially be lower).

Usage: Anything in the High Risk Zone should be blocked.

Unknown and Suspicious Sites (21 – 40) – proactive protection

Unknown sites are typically sites which are relatively new and have never have been reviewed. With the classification engine scanning thousands of URLs per second, any legitimate URL will most likely have already been scanned and given an appropriate rating.

Sites in this zone should be treated as suspicious.

Usage: Anything in the Suspicious Zone should be blocked unless shown to be legitimate.

Other Known Sites (41 – 60) – moderate risk

These are other known sites which have been around for several months and could still present a risk because:

- They have been infected in the past year
- They have exhibited some kind of risky characteristic

Usage: Proceed with caution! These sites should be handled with care and visited only by those who are knowledgeable in the subject area and will not expose others to the risk of infection.

Relatively Safe Sites – (61 – 80) – low risk

These known sites exhibit few risky characteristics and therefore are relatively safe.

Usage: These sites have a low risk of infection and access can be given to everyone.

Trustworthy (81-100) – trustworthy

These are highly trusted sites which exhibit little to no risk and therefore are trustworthy and safe to visit.

Usage: These sites have the lowest risk of infection and access can be given to everyone.

How is the Web Reputation Index calculated

Web Reputation is calculated using a large number of factors and a machine learning process. Rather than controlling the process manually, advanced techniques are used to allow the classifier to determine the correct weights based on millions of examples of "good websites" and "bad websites". The following are some of the features analyzed:

- Location of website
  - Geography (Country/City)
  - ISP/WebHost
  - IP neighborhood

Some areas of the Internet are known to be "bad neighborhoods". A website hosted in these neighborhoods could increase its risk rating.

- Behavior and Content of website
  - JavaScript content and characteristics
  - Popups
  - Redirects
  - Executable file downloads

Websites which typically have or distribute malicious content are similar in terms of the content they provide. For example, creating multiple redirects to different websites is a technique which may be used by hackers to mask the true destination a website is trying to send users to.

- Legitimacy
  - Domain/Category Age
  - Number of IP addresses for a site
  - Top Level Domain

The above characteristics also show how legitimate a website is. For example, a website can be deployed with malicious content within a few hours. New websites are treated suspiciously unless it is otherwise clear that they are legitimate.

- Threat History
  - Past Safety Track Record (history of infections in the last three and 12 month-periods)

A site which has been infected in the past is a greater risk than a website which has a clean track record.

More than 400 weighted variables are used to give a correct score. The weighting is not decided arbitrarily but based on the process's capacity to analyze and determine the ideal weightings for each analyzed feature.

Reputation Index for websites with malicious content

A website which is found to be distributing malicious content is immediately put into the high-risk zone. The website stays in this zone until it has been "cleaned". Once it is clean, rather than giving it the same score as before, the infection history is taken into consideration and its original score is only restored over a period of time. Most reputation services do not maintain a history of behaviour; on the other hand, the WebGrade Reputation index grows and decays over time depending on the behaviour of a website.

Dynamic real-time updates

Changes in the score of a website are immediately available via the hybrid reputation index service which consists of a local database of popular sites – and an online querying mechanism for sites not in the local database. Websites are revisited often to update the classification of the content; the revisit frequency varies depending on parameters such as the change velocity of the site, popularity, ranking, history of previous changes, and other relevant factors.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

GFI 2230 sep11

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus