Web Domain Name System Reputation

Danger could be lurking behind any website. Cyber adversaries routinely hack into legitimate websites or create their own malicious sites to upload malware to the computers of unsuspecting web visitors. Botnets, which use collections of usually unsuspecting Internet-connected computers to execute malicious tasks, often use exploited web servers to launch attacks and issue instructions.

Early attempts to counter these threats included IP address blocking and DNS blacklisting. However, administrators who maintained the databases for these blacklisting systems could not keep up with the sheer volume of IP address and DNS registration updates. Additionally, attackers might upload malware to well-known websites that cannot be blocked due to their importance. Hence, there is a need to quickly and reliably block particular pages or sections of a website rather than the entire site.

Web Domain Name System (DNS) reputation services address these needs. Although a web DNS reputation service is not a cure-all for preventing malicious attacks, it is a reliable and useful part of a multi-layered defense.

What is a Web Domain Name System Reputation Service?

Most web DNS reputation services use computer algorithms to detect and block access to malicious web pages. Today's reputation services are typically quite accurate, with only a small risk of generating false positives (mistakenly labeling safe content as malicious).

Rather than classifying a web page with a simplistic good/bad response, these services operate in shades of gray, allowing for a range of responses. Organizations and individuals then have greater flexibility in tailoring their own web access policies. For example, consider this sample web DNS reputation policy:

Response: Bad
Action: Block all access

Response: Very Suspicious
Action: Block all executable content (e.g. Java, Javascript, ActiveX, Flash, macros, embedded or script content) but allow filtered text content

Response: Suspicious
Action: Block all executable content

Response: Somewhat Suspicious
Action: Do not download executable files

Response: Good
Action: No restrictions on content

Web DNS Reputation Service Providers

There are multiple options for implementing web DNS reputation services in your network, from the host-based solutions to Internet Service Provider level capabilities.

Web Reputation Websites

There are several websites that provide up-to-date information on malicious web traffic and spam (e.g. www.senderbase.org, trustedsource.org, spamcop.net). Before deciding which Web DNS Reputation Service to use, visit several sites to get a good feel for the information they provide and determine which best meets your needs.

Vendor Products

For individual devices, multiple vendors incorporate access to web reputation services in their security products (e.g. host security suites) and typically include the cost of using reputation services in the price of the product. Some of these products may already be in use at your facility or on your mobile device, e.g. Symantec™ (Norton™ Safe Web), McAfee® (Web Gateway), and Trend Micro™ (Web Reputation Services and Smart Surfing)[1]. Other providers offer dedicated hardware for a cost to access their web reputation services (e.g. Cisco IronPort® Web Security Appliance)[2].

Browser Options

Additionally, some browsers make use of reputation services. Consider using the Phishing Filter in Internet Explorer® or choose the "Block reported attack sites" and "Block reported web forgeries" options in Firefox®. For Chrome™, install the WebFilter Pro add-on.[3]

Internet Service Providers

Some Internet service providers also provide Web DNS Reputation Services. Contact the service provider for more information on using their reputation service. Corporate and government Chief Information Officers can consult with their respective IT offices regarding use of web reputation services.

Third-Party Product Integration

Some vendors provide a software development kit (an embeddable application programming interface) that enables third-party products to query their web reputation service. Contact the vendor for licensing terms and restrictions.

Other Reputation Services

There are numerous reputation services for files and e-mail, but those are not covered in this publication.

What about Mislabeling?

In the event safe content is mislabeled malicious, the web DNS reputation service has a procedure in place whereby a website administrator can contact the reputation service to have the website verified and its reputation restored. In some cases, a reputation service may require additional patching and hardening of the server before restoring its reputation. Some services will automatically improve reputations when bad behavior stops; however, that process can take up to 30 days or longer to take effect.

There are tools available on the Internet that will search various reputation services to determine whether a particular IP address is on one or more blacklists. Most of these tools are free to use.

In the event malicious content is mislabeled safe (a rare event) or has not yet been detected on a website, local host-based security suites will minimize the threat as long as they are kept up-to-date. If available, automatic updating of host-based security suites on servers, desktop computers, and mobile devices should be enabled unless there are valid reasons not to.

If automatic updates cannot be enabled, the security suites should at least be configured to alert when updates are available for download and installation. Also, these security suites should be configured so that regular users cannot disable or bypass them.

Why Not Just Filter All Content Locally?

Scanning and filtering the content of a webpage is a rather intensive task even for a computer. Consider a company with a large number of employees simultaneously accessing various web pages on the Internet. The filtering systems would require significant resources.

By employing a reputation service, scanning and filtering are only performed on sites that really require it and the amount of scanning and filtering can be tuned based upon the reputation. This lessens the load on the filtering systems, reducing the resources they require, and making them more cost effective and able to deliver content in a timely manner.

Additional Information

- Antivirus File Reputation Services
  http://www.nsa.gov/ia/mitigation_guidance/
- Host Protection Technology Study
  http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml

[1] Norton™ and Symantec™ are registered trademarks of Symantec Corporation. McAfee® is a registered trademark of McAfee, Inc.. Trend Micro® is a registered trademark of Trend Micro Incorporated.

[2] IronPort® is a registered trademark of Cisco.

[3] Interent Explorer® is a registered trademark of Microsoft Corporation. Firefox® is a registered trademark of Mozilla Foundation. Chrome® is a registered trademark of Google.