Improved network security with IP and DNS reputation

Business white paper
**Table of contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Understanding today’s network security threats</td>
<td>3</td>
</tr>
<tr>
<td>Categories of cyber threats</td>
<td>3</td>
</tr>
<tr>
<td>“Bad” devices</td>
<td>4</td>
</tr>
<tr>
<td>Device reputation, a critical first step</td>
<td>6</td>
</tr>
<tr>
<td>Why TippingPoint IP and DNS reputation services?</td>
<td>6</td>
</tr>
<tr>
<td>Full, powerful protection</td>
<td>7</td>
</tr>
<tr>
<td>Your next step</td>
<td>7</td>
</tr>
</tbody>
</table>
Introduction

Understanding today’s network security threats
As cyber threats across the globe continue to increase in number and sophistication, security and networking personnel must not only work harder but also smarter to stay ahead of malicious attacks. Sophisticated scanning, penetrating, and obfuscating tools and techniques are more widely available now more than ever before. Worst of all, hackers are now highly motivated to penetrate networks, applications, and databases to steal information that can quickly be sold for profit using botnets and other resources they control.

The problem is compounded by the low risk of being caught; the risk of prosecution is even lower. How would a botnet attack crafted by a Romanian teenager using a machine in Bolivia to attack a bank server in the U.S. be traced? And even if a trace were possible, what law enforcement agency would be likely to understand the nature of the crime, let alone help prosecute it? In the meantime, a company might find itself on the front page of a national newspaper—for less than positive reasons.

Categories of cyber threats
A common first line of defense is identifying the types of traffic on the enterprise network. For the purposes of this white paper, they are broken down into the following three high-level categories:

1. Known “Good Traffic”—trusted traffic that should pass through the network, unimpeded and uninspected

2. Known “Bad Traffic”—traffic that should be blocked proactively before it can attempt to compromise the network

3. Unknown or “Ugly Traffic”—untrusted traffic that requires deep packet inspection to determine if it is “good” (legitimate) or “bad” (malicious)
**“Bad” devices**

To stay ahead of today’s onslaught of threats, enterprises can identify known “bad” devices based on IP or DNS addresses and block the traffic they spew. These devices, existing in large quantities, are:

**Botnet Command and Control (CnC) sites:**
It’s estimated that there are 5,000 to 6,000 botnet command and control sites worldwide on any given day. If communications with their compromised hosts or bot army could be identified and stopped, their effectiveness would be seriously reduced. Unfortunately, this can be extremely challenging—botnet CnC servers are constantly moving to evade detection and blocking efforts from security and network personnel. In fact, botnet masters, those individuals who control and manage a botnet network, use a variety of techniques to avoid being discovered:

- To communicate with their bots, bot masters use standard channels such as IRC, P2P, and HTTP traffic—including Twitter and instant messaging. This allows them to bypass traditional firewalls and some intrusion prevention system (IPS) security measures.
- Bots may use dynamic algorithms to select CnC servers, making it almost impossible to block them using firewall access control lists (ACLs).
- Bots use both DNS and IP addresses for identifying CnC servers.

Consequently, identifying botnet CnC servers requires detailed botnet analysis and frequent updating of CnC lists.

**Malware depots:** It is estimated that 2,500 to 50,000 devices, which act as malware depots or host malicious content are discovered daily worldwide. If these devices could be identified and stopped from spreading malware, then new hosts on enterprise networks could be significantly reduced or even prevented from compromising network security. Unfortunately, the sheer number of current malware depots is staggering.

Depots are generally categorized into two primary types. The first includes Web sites that are designed to lure victims and then infect their devices. The second and possibly even more dangerous type, includes Web sites of legitimate businesses that are compromised because they haven’t been properly secured. These sites are trusted and typically visited by large numbers of users, allowing the malware on them to spread much faster.

These depots can also be used as botnet drop sites, and for hosting malware software updates. However, unlike the botnet CnC sites, the lookup mechanism for these depots is almost always the DNS name and not the IP address. Therefore, identification involves: (1) monitoring for malware downloads and tracking their origin, and (2) evaluating data hosting sites worldwide.

**Phishing sites:** There are approximately 50,000 or more new phishing sites introduced to the Internet monthly. Identifying and blocking access to these devices could protect users from falling prey to often very credible looking scams. As with the malware depot sites, control is a challenge because of the large number of Web sites that host these scams. In fact, the Anti-Phishing Working Group identified 56,000 unique phishing sites in August 2009 alone as shown in the chart below.

![Phishing Activity Trends Chart](chart.png)

Unique phishing sites detected from July through September 2009. Anti-Phishing Working Group, Phishing Activity Trends Report, Q3-2009

---

1. Shadowserver Foundation, online botnet monitoring
4. Anti-Phishing Working Group, Phishing Activity Trends Report, Q3-2009
The two primary types of phishing sites are purpose-built sites that lure victims and gather their private information, and sites that appear to be part of a known credible business. In the latter case, a business Web site is usually compromised and visitors are redirected to the phishing site that is generally identical to the Web site of the compromised business—except that it is solely designed for criminals to gather private information.

This type of phishing site is a threat to both the user and to the company whose Web site is compromised and whose customers are being scammed. Most of these sites are reached through DNS name requests. Accurately identifying them involves finding and evaluating phishing scams that use multiple delivery mechanisms, and evaluating the associated phishing sites throughout the Internet.

**Compromised hosts:** Host systems (typically personal computers, laptops, and so on) estimated to number in the millions\(^5\) are compromised most commonly by bot malware. These compromised hosts may reside in corporate networks for some time without detection. They are typically under the control of a remote botnet master through botnet CnC sites. Compromised hosts are extremely dangerous because they can be used by a botnet master to conduct a variety of malicious attacks, including:

- Spreading malware to other hosts
- Compromising additional hosts to create more botnet devices
- Performing reconnaissance scans
- Providing access to local networks for further compromise
- Conducting Distributed Denial of Service (DDoS) attacks
- Conducting email spam or phishing campaigns
- Conducting online-click fraud scams

Tracking these compromised devices is challenging and requires a worldwide community of participants that contribute event and attack data.

\(^5\) MessageLabs Intelligence: 2009 Annual Security Report
Device reputation, a critical first step

To develop a clear picture of a device’s reputation, it must first be determined if the device is “behaving badly”, or in other words, if it is generating exploit traffic or attacks; has been compromised and is part of a botnet; or is hosting a site that spreads malware. Once a device’s reputation is known, then organizations can use that information to block access to and from devices that have a known bad reputation.

Enterprises need a reputation database with significant metadata on each of these badly behaving devices—identified through IPv4 or IPv6 addresses or DNS names—for effective network policy enforcement. Developing and maintaining comprehensive and current information, a significant challenge given the amount of data and its ever-changing nature, requires a security research team that can:

• Collect large amounts of device data
• Correlate these large data sets
• Validate the results of these data sets so that devices aren’t wrongfully entered into the Reputation Database
• Provide frequent database updates to keep up with changing attacks
• Prioritize the database entries through assigning a Reputation Score

To acquire this information the team must:

• Collect real-time attack events with very detailed attack data from a large worldwide community of sensors
• Analyze Web traffic and crawl Web sites of interest to collect data on sites hosting malicious content or scams
• Conduct careful malware analysis to identify botnet CnC sites, and botnet and malware drop sites
• Analyze attacks and scams to identify the devices that are participating in or conducting the attacks

Probably the most important component in building this strong reputation service is the depth of the database. It requires a worldwide community of participants contributing event data. Database quality depends heavily on the size, scope, and distribution of the attack collection sites, and the quality and depth of the collected attack data.

Why TippingPoint IP and DNS reputation services?

HP offers enterprises security solutions that leverage TippingPoint Lighthouses, a worldwide network of attack monitoring installations, and TippingPoint ThreatLinQ, a customer-facing, real-time threat landscape database. This active research infrastructure greatly increases the quantity and quality of data that HP’s TippingPoint solutions can provide. The strength of these solutions is also augmented with the data and analysis from partner organizations such as the SANS Institute, other Web and email research firms, as well as open source malware, phishing, and botnet research communities.

To deliver the benefits of this extensive data collection, the TippingPoint Reputation Digital Vaccine Service channels all data and ongoing update data feeds to an enforcement point in the network, such as an inline TippingPoint IPS that inspects traffic in real-time and can enforce reputation security policies. Enterprises can set policies based on a reputation score that considers information from the reputation database, including IPv4 and IPv6 addresses and DNS names, as well as metadata tags for each database entry. For example, an organization may decide to prevent visits to a Web site that has a DNS Domain Score of 80 out of 100 or higher, meaning the Web site is known to host malicious content.

Policy can also be based on location or geography: an organization that only conducts business in North America, for instance, might set policy to block or initiate alerts on any in-bound traffic from Europe, Africa, South America, and Asia. In addition, policies can be set based on the type or the reason for the bad reputation score. For example, an organization may block IP addresses that are known to attack or exploit sources, Web sites that are known to host malware, IP addresses that are known botnet CnC locations, or IP addresses that are known spam sources. It may also choose to block all inbound traffic from spam sources using an IPS platform that is positioned in front of its DMZ and email server.
To provide strong first-line perimeter protection against botnets and malware, the TippingPoint Reputation Digital Vaccine Service blocks outbound user requests to bad domains and blocks inbound traffic from bad IP addresses. As a complement to other email security devices, it also protects users from spam and phishing emails, and safeguards the network from devices known to conduct DDoS and Web application attacks. Administrators may also add their own IP and DNS reputation lists into the reputation database.

Full, powerful protection

A robust set of HP TippingPoint solutions helps enterprises increase security with automated services that reduce administrative burdens while increasing protection. Parallel security services—the TippingPoint Reputation Digital Vaccine Service that expands a “known bad” traffic set and the standard TippingPoint Digital Vaccine Service that inspects and applies policy on gray traffic—take advantage of the multi-threaded processing capabilities unique to the TippingPoint N-Platform IPS. IT staff can efficiently administer these security solutions with the TippingPoint Security Management System that not only helps enterprises align policy setting with their own network profile, but also generates the reporting needed to show compliance with internal mandates and regulatory requirements.