Technical Brief: SEP Network Intrusion Prevention System

Network Intrusion Prevention System for Symantec Endpoint Protection 11.X

User Guide

Contents

1.0 Overview ................................................................................................................................. 1
2.0 Introduction .............................................................................................................................. 1
3.0 Enabling IPS in SEP 11 ......................................................................................................... 3
4.0 Threat Prevention Types ......................................................................................................... 3
5.0 Incident Priorities of Threat Categories of IPS Signatures for Investigation ...................... 13
6.0 Intrusion Prevention System Engine Overview .................................................................... 14
7.0 Endpoint Protection Manager Reports .................................................................................. 19
1.0 Overview
This guide is a tool to help IT managers understand the benefits of using Symantec’s Network Intrusion Prevention System (IPS) technology in Symantec™ Endpoint Protection (SEP), version 11.x, against today’s threats. It should also help you understand the different types of threats IPS can protect you against, the differences in the alerts, and how to be more efficient in investigating incidents using the technology. This guide also includes some of the common questions asked and recommended steps to take when investigating an incident.

2.0 Introduction
The threat landscape for enterprises has changed significantly over the last few years. As a result, your solution for preventing today’s threats should change with it. It used to be that virus threats were spread mainly via email. In today’s threat landscape, enterprise desktops are infected most often via Web-based attacks resulting from everyday user activities. Merely by visiting a website, a user’s system can be silently infected via a drive-by download attack. Moreover, if your users are allowed to download applications to their desktops, they may be duped into downloading malicious code posing as supplemental software, such as in the ploy that prompts a visitor to a site to install a “video codec/player” required to supposedly view content, but which actually instead infects the computer. In addition, Web-attack toolkits have made it much simpler for attackers to create broadcast drive-by attacks that can attempt to exploit as many as 25 vulnerabilities at a time. These attacks come from websites your users may visit at any time. The result is a silently delivered payload of malware that is dynamically generated using server-side polymorphism. In other words, every malware attack delivered is distinct. This means that antivirus alone from any security vendor is unable to protect against these new Web-based attacks. To protect against the multiple infection vectors of today’s threat landscape, multiple layers of protection technology are required on the endpoint.
One major protection solution for today's threats is the client-based network IPS capability that exists within the standard client installation of Symantec Endpoint Protection. Historically, intrusion prevention system (IPS) and intrusion detection system (IDS) technology has been considered complicated. Now, Symantec has leveraged the intelligence available on the endpoint and integrated the IPS technology to the point that it has become a powerful, easily implemented tool in enterprise malware prevention. Symantec's IPS is a layer of defense that keeps known and unknown threats from ever reaching your users' systems. The IPS solution protects against the primary infection vectors for enterprise and consumer endpoints, including:

- Protection against Web-attack toolkits and drive-by downloads
- Protection from malware and bot-infected systems that spread on a LAN
- Protection from social-engineering attacks

Symantec IPS technology is turned-on by default on tens of millions of systems and provides high reliability, and low system-impact protection.

In 2010, Symantec protection technologies blocked more than 3 billion attacks; approximately 48 percent of these were caught using IPS. Web-based attacks—that IPS is essential at protecting against—nearly doubled in 2010, and Symantec continues to see more than 10-15 million Web-based attacks per day. Thus, if you are not running IPS with Symantec Endpoint Protection, you are missing a considerable portion of available protection. Symantec highly recommends the use of IPS on every corporate desktop as part of our recommended best practices for stopping malware.

In addition to IPS, SEP includes multiple protection technologies. For example, the SEP IPS component is part of the Network Threat Protection module of SEP, which also includes the Firewall and Network Intrusion Prevention components.

To protect yourself completely against current threats, four pillars of protection are essential: network threats, reputation, file-based antivirus, and behavioral. The next release of SEP (version 12.1) will include our reputation technology as well as our real-time active-behavioral protection, Sonar 3. Symantec anticipates that this approach will result in a much more distributed protection.

3.0 Enabling IPS in SEP 11

In SEP 11.x, the IPS capability is located within the Network Threat Protection module. To enable IPS, ensure that the Network Threat Protection module is set to ON. If you have not enabled Network Threat Protection, it can easily be done within the management console. An automatic update can then be pushed out to all clients. A Symantec support article showing how to enable and disable features in Endpoint Protection is available here.²

4.0 Threat Prevention Types

Network IPS is actually a misnomer since the solution does much more than protect against just intrusions. It also provides protection for multiple types of threat categories (which will be explained in the upcoming sections). To make it easier to determine which category of threat you are seeing, we have added a category prefix to the IPS signature name, which can be reviewed here. Analyzing the alerts and logs from the IPS technology can give you a powerful tool in

identifying infected systems and can determine the threat and risk posture of your enterprise endpoints based on your users’ normal activities.

The Network IPS within SEP provides protection for the following types of threats (with the attack category prefix in parentheses, if one exists):

- Protection against unpatched vulnerabilities
- Base operating system threat prevention (OS Attack)
- Drive-by download and Web-attack threat prevention (Web Attack)
- Social engineering and misleading application threat prevention (Fake App Attack)
- Malware post-infection system detection (System Infected)
- Malicious domain, website and IP-blocking prevention (Malicious Site)
- Spyware/adware prevention
- Policy-based detection: peer-to-peer and instant messenger detection/prevention

4.1 Protection from Unpatched Vulnerabilities: – Generic Exploit Blocking (GEB)

Web-attack toolkits and malware silently exploit underlying software vulnerabilities to get onto your users’ systems. One way that SEP IPS provides powerful protection is to focus on protecting against the underlying vulnerabilities in application and browser plug-ins, instead of specifically against just the exploits that target them, as is the case with purely signature-based antivirus solutions. Compromises from successfully exploited vulnerabilities could include:

- Running arbitrary instructions of the attacker’s choosing
- Downloading files from the Internet
- Running a local file
- Crashing the application

Symantec provides protection against vulnerabilities being exploited by determining any way a given vulnerability can be exploited. Protecting the vulnerability provides a type of “network patching” Symantec refers to as “generic exploit blocking” (GEB). A single GEB IPS signature can provide blocking for hundreds of thousands of malware variants to protect your users. More importantly, GEB signatures provide zero-day malware protection against known vulnerabilities. As an example, for the MS-RPC, MS08-067 vulnerability, Symantec provided GEB protection against the underlying vulnerability the same day as Microsoft announced the vulnerability. This protected against any malware from exploiting the underlying vulnerability before the malware was ever created. W32.Downadup (also known as Conficker) was created months later. Customers that had deployed SEP IPS were protected against the malware outbreaks, thereby neutering the malware. Symantec continually assesses and analyzes critical vulnerabilities, and if they are remotely exploitable via the Internet or network, they will be considered for future IPS signature updates.

4.2 Base Operating System Threat Prevention (OS Attack)

Vulnerabilities such as MS-RPC, LSASS, SQL Server, or the more recent MS-RPC vulnerabilities in the MS08-067 Microsoft Security Bulletin are considered base operating system (BOS) vulnerabilities. Symantec Endpoint Protection IPS protects against BOS vulnerabilities. Signatures in this category include the “OS Attack” prefix.
Remotely exploitable vulnerabilities in the BOS used to be one of the primary ways enterprises and consumer customers were exploited; however, improvements in patches and updated best practices have reduced such threats. Symantec provides GEB protection against critically rated, remotely exploitable operating system (OS) vulnerabilities used to exploit the base operating systems in Microsoft Windows.

4.2.1 Recommended next steps for BOS protection alerts

IPS signatures that trigger “OS Attack” BOS prevention indicate that the end-system has been protected against an attack and that the connection has been dropped. If the source address of the attack is coming from an internal IP address, this may indicate that a system on the network is infected and is trying to propagate by exploiting BOS vulnerabilities (such as MS RPC and LSASS.) You should check the source IP to find the potentially infected system or from where the attack is originating. Many threats such as W32.Downadup/Conficker and various bots spread in this manner.

Example IPS Signatures: “Sig ID 23179 OS Attack: MSRPC Server Service BO” means that SEP IPS has protected you against an attempt to exploit a buffer overflow vulnerability in the MS-RPC Server Service, which is covered in MS08-067. This vulnerability is exploited by thousands of malware variants, of which two are especially notorious—W32.Downadup/Conficker and Stuxnet. Your system is safe, but the source IP that indicates the source of the attack should be investigated if this is within your network boundary. The server-side or upstream computer is most likely infected.

<table>
<thead>
<tr>
<th>IPS Signature ID</th>
<th>IPS Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>23179</td>
<td>OS Attack: MSRPC Server Service BO</td>
</tr>
<tr>
<td>20409</td>
<td>OS Attack: MS ASN1 Integer Overflow TCP</td>
</tr>
<tr>
<td>20648</td>
<td>OS Attack: MS RPC Network DDE BO</td>
</tr>
<tr>
<td>21702</td>
<td>OS Attack: MSRPC SrvSvc NetApi Buffer Overflow (2)</td>
</tr>
<tr>
<td>20386</td>
<td>OS Attack: MS RPCSS Attack (2)</td>
</tr>
<tr>
<td>20443</td>
<td>OS Attack: MS RPC LSASS DS Oversized Request (TCP)</td>
</tr>
<tr>
<td>20615</td>
<td>OS Attack: MSRPC Malicious LSASS DS Request BO (1)</td>
</tr>
<tr>
<td>21260</td>
<td>OS Attack: NetBIOS MS PnP QueryResConfList BO</td>
</tr>
<tr>
<td>20624</td>
<td>OS Attack: MS RPCSS Attack (3)</td>
</tr>
<tr>
<td>20081</td>
<td>OS Attack: MS SQL Stack BO</td>
</tr>
<tr>
<td>20631</td>
<td>OS Attack: MSRPC Malicious LSASS DS Request BO (2)</td>
</tr>
<tr>
<td>20385</td>
<td>OS Attack: MSRPC DCOM BO (2)</td>
</tr>
</tbody>
</table>

Examples of OS Attack and BOS IPS event protection

4.3 Drive-by Download and Web-Attack Threat Prevention (Web Attack)

Symantec often identifies legitimate mainstream websites that have been compromised and then inconspicuously repurposed to mount Web attacks. Commonly referred to as drive-by download attacks, these attacks are some of the most insidious forms of malware infection currently out there because they occur without visitors to the compromised sites being aware of the attacks. Just browsing to an infected website may allow executable content to be automatically downloaded onto the user’s computer without his or her knowledge or permission. No user interaction is required and the system is silently infected. The majority of users (or an enterprise’s IT administrators) would have NO idea that the system has been compromised. Mainstream websites unknowingly hosting drive-by-downloads or malicious advertisements (malvertisements) are primary ways that enterprise users are currently infected.
Symantec Endpoint Protection IPS provides protection against drive-by downloads. IPS signatures in this category have the “Web Attack” prefix. When an IPS “Web Attack” signature is triggered, this signifies that the Web attack that targeted your system was prevented and that the connection was terminated. Your system is safe. Caution should be taken not to revisit the website that was hosting the malicious content.

Anatomy of a drive-by download

Each year, Symantec IPS technology prevents millions of drive-by download attacks. Drive-by downloads work by exploiting the underlying vulnerabilities in browsers, multimedia plug-ins, document readers and ActiveX plug-ins. Drive-by downloads are launched from compromised or intentionally malicious sites that are coded to identify if the visitor’s browser is vulnerable to attack and, if so, which vulnerabilities in the attack arsenal to use. Symantec has observed attacks exploiting as many as 25 different vulnerabilities at once. It takes only one vulnerability for your system to be compromised.

Symantec uses GEB protection against vulnerabilities exploited by drive-by downloads. This results in automatic and silent protection of these Web-based attacks before the malicious payload ever reaches your users’ disks—a significant advantage in preventing an attack. You can further enhance your protection by patching vulnerable applications that are commonly exploited, such as Java, Adobe Flash, Adobe Reader, Apple QuickTime, and others. For more background on top vulnerabilities being exploited, please consult the Symantec Internet Security Threat Report.

Symantec also provides generic Web-attack protection by fingerprinting the network characteristics of Web-attack toolkits. This provides protection against vulnerabilities being exploited by versions of Web-attack toolkits that Symantec has identified. This provides protection against newly-released vulnerabilities for which Symantec may not yet have a specific GEB signature. To identify if this protection is triggering within your environment, look for signatures with names such as “Malicious Toolkit,” or the names of specific Web-attack toolkit families such as Neosploit or Phoenix. (For more information, please see the Symantec Report on Web-Attack Toolkits.) This also provides a level of protection against zero-day vulnerabilities when those vulnerabilities have been added to the toolkits.

The SEP IPS solution is a substantial and significant protection improvement over using an antivirus-only solution. Attacks using obfuscation techniques with malicious JavaScript and that exploit ActiveX controls can be difficult if not impossible
to detect with IPS solutions. Symantec has created additional threat prevention technologies to thwart Web-based attacks that will be included SEP 12.

4.3.1 Recommended next steps for “Web Attack” drive-by download protection IPS alerts

IPS signatures that trigger with a “Web Attack” prefix indicate that a system on your network has been protected from a drive-by download and that the connection has been dropped. No further analysis on the end-system should be required. If there is a particular website that is triggering an IPS signature, that site should not be revisited until it has been cleared as safe. To find out more information about the attack, you should review the detailed IPS signature threat write-up at the Symantec Security Response site (see section “IPS Signature Threat Write-ups, Signature Updates, and LiveUpdate).

**Example IPS Signature:** “Sig ID 23153 Web Attack: Acrobat PDF Suspicious File Download” means that SEP IPS has protected you against a drive-by download attempting to exploit a vulnerability in the Adobe Acrobat browser plug-in. Your system is safe and no further investigation should be required.

**Example IPS Signature**

```
<table>
<thead>
<tr>
<th>IPS Signature ID</th>
<th>IPS Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>23218</td>
<td>Web Attack: Acrobat Suspicious Executable File Download</td>
</tr>
<tr>
<td>23970</td>
<td>Web Attack: Malicious Toolkit Variant Activity 17</td>
</tr>
<tr>
<td>23952</td>
<td>Web Attack: Neoploit Toolkit Request</td>
</tr>
<tr>
<td>23153</td>
<td>Web Attack: Acrobat PDF Suspicious File Download</td>
</tr>
<tr>
<td>23086</td>
<td>Web Attack: Malicious Toolkit Variant Activity</td>
</tr>
<tr>
<td>23766</td>
<td>Web Attack: Facebook LikeJacking</td>
</tr>
<tr>
<td>23784</td>
<td>Web Attack: Phoenix Toolkit Download Request</td>
</tr>
<tr>
<td>23254</td>
<td>Web Attack: Malicious Toolkit Variant Activity 3</td>
</tr>
<tr>
<td>23352</td>
<td>Web Attack: Malicious JavaScript Encoder 5</td>
</tr>
<tr>
<td>23329</td>
<td>Web Attack: Adobe SWF Malicious File Download</td>
</tr>
</tbody>
</table>
```

**Examples of “Web Attack” IPS signatures**

4.4 Social Engineering and Misleading Application Prevention (Fake App Attack)

Malware authors have other tools at their disposal to attack even cautious users and their computers. Many of these attacks employ social-engineering techniques. The term social engineering is really a modern day equivalent of what is more traditionally called a confidence trick or a con. It is used to describe situations where people are tricked into doing things they would not otherwise voluntarily do. Online social-engineering attacks often focus on what are categorized as misleading applications or rogueware—applications that mislead their real intent. These attacks can come from a range of Internet activities, including using a search engine, clicking links from within social media applications or email messages, trying to view a video, or being lured into clicking a malicious advertisement presented on a website. The ploy then presents a pop-up window with warnings of a malware infection, that the user’s hard drive needs to be defragmented, or that the user needs to install a video player. Agreeing to any of these prompts may result in the user loading a malicious application onto his or her own system (often resulting in the user ending up in the very same compromised condition that the original social-engineering prompt purported to resolve). These misleading applications are continually changing with millions of variants, making detection with antivirus alone unfeasible.
Symantec IPS signatures provide prevention capabilities against these misleading applications by preventing fake application attacks from popping up. IPS signatures for this category of threat have been categorized with a “Fake App Attack” prefix.

4.4.1 Types of social-engineering attacks: fake codec and fake antivirus

There are two main types of social engineering used by malware creators: fake codecs and fake antivirus scanner pages.

4.4.2 Fake codec

There are dozens of different multimedia file formats on the Web, and many require special software for the user to access the content. As such, experienced Web users know that they sometimes need to download and install an additional media player or browser plug-in module in order to view content on the site they are visiting. It is not unusual to be prompted to download the latest version of a new player or plug-in when visiting a new site. Commonly called a codec (coder-decoder), the term is used to describe a piece of software that can decode a binary file and reconstitute a version of the original audio or video. Malware authors play into this acceptance by establishing websites that host tempting content such as adult content or promised repositories of audio and video files. Upon attempting to access the content, the user is first prompted to install a new codec in order to be able to access it. Instead of a codec, however, the executable content is really malware that the user is authorizing to be downloaded and installed on his or her computer.

![Example fake codec dialog](image)

4.4.3 Fake scanner Web page

A variant of the malicious advertisement technique is to create a website to promote a service or product that blatantly misrepresents the truth. Such sites are easily able to leverage the JavaScript capabilities of a browser to get it to open a window with content that looks like a legitimate operating system alert notification. Figure 8 shows a false alert notification that purports that the user’s computer is infected. In reality, this is simply a scare tactic. Symantec has observed thousands of such fake scanner pages using innovative and persuasive social-engineering strategies. Malware authors create millions of variants of these false alerts, meaning that antivirus alone is not enough to detect them. The SEP IPS solution prevents users from being redirected to the sites serving up misleading applications and blocks the connections.
4.4.4 Recommended next steps for “Fake App Attack” misleading application protection IPS alerts

If you see an IPS “Fake App Attack” alert, it means that IPS has proactively prevented a social engineering/fake application attack from occurring. No further investigation should be required. These attacks are quite common and may spring from simple actions such as search engine queries or clicking on social media links. The key difference is that user interaction is required to install the malicious payload on users’ systems. Therefore, as long as users do not download and install such applications, they should be safe.

Here are a few ways to help your users against these threats:

- Limit the ability of users to download and install software
- If they are given such permissions, educate them to install software from the software vendor’s website or from approved IT software distribution servers
- Educate them about new attacks (such as fake AV pop-ups or plug-in messages that could occur from normal everyday activity)

If you want to find out more information about the attack, you can read the detailed IPS signature threat write-up on the Symantec Security Response site (see section “IPS Signature Threat Write-ups, Signature Updates, and LiveUpdate). These IPS events are slightly lower in priority for analysis than events tagged as “Web Attacks.” Analysis and correlation with any further antivirus, behavioral-based, or reputation-based events would raise the priority level for investigations.
Tip: Often users will call the help desk stating that alerts are popping up or that their systems are infected. Try to determine if the alerts are coming from the real Symantec security software present on the endpoint, from a dialog or window originating from a Web page, or if the user actually downloaded and installed an application that included a fake antivirus solution. Often, the purported threat will be from the sort of animated graphic or GIF (shown above in figure 8) that attempts to trick users into thinking that they are infected and for them to install the fake application in order to further trick them into paying for something that, in reality, does not detect anything.

Example IPS Signature: “Sig ID 23973 FakeApp Attack: FakeAV WebPage Request 1” means that SEP IPS has prevented a social engineering attack. This attack would have popped up a fake antivirus Web page and then tried to trick the user into thinking that his or her system was infected. The system should be safe and no further investigation should be required.

<table>
<thead>
<tr>
<th>IPS Signature ID</th>
<th>IPS Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>23683</td>
<td>FakeApp Attack: FakeAV Redirect Request 3</td>
</tr>
<tr>
<td>23973</td>
<td>FakeApp Attack: FakeAV WebPage Request 1</td>
</tr>
<tr>
<td>23005</td>
<td>FakeApp Attack: Fake Scan Webpage</td>
</tr>
<tr>
<td>23033</td>
<td>FakeApp Attack: Misleading Application Detection</td>
</tr>
<tr>
<td>23186</td>
<td>FakeApp Attack: Fake Codec Request (2)</td>
</tr>
<tr>
<td>23375</td>
<td>FakeApp Attack: Misleading Application File Download</td>
</tr>
<tr>
<td>24020</td>
<td>FakeApp Attack: FakeAV Redirect Request 9</td>
</tr>
<tr>
<td>23461</td>
<td>FakeApp Attack: Fake Codec Download Website</td>
</tr>
<tr>
<td>23489</td>
<td>FakeApp Attack: Fake AV Install Request 3</td>
</tr>
</tbody>
</table>

Examples of misleading application signatures

4.5 Malware Post Infection System Detection (System Infected)

The rapid growth of server-side polymorphic attacks has made it a challenge for traditional antivirus-only solutions to keep pace with malware threats. Symantec Endpoint Protection IPS can aid in the identification and neutralization of infected systems. Malware that has bypassed antivirus and other detection methods often updates itself over the Web or tries to propagate further over a compromised network. The SEP IPS solution includes signatures that tell you if systems are infected and if there is abnormal activity occurring on the network. These signatures indicate activity of a potentially infected system and that the IPS is detecting a compromised system trying to get updates or that is attempting to propagate further and infect additional systems.

4.5.1 Recommended next steps for System Infected alerts (System Infected)

Note: These signatures alerts should be investigated first when trying to remove malware and infections in an enterprise, as this indicates the presence of an infection that antivirus has NOT detected or removed. If you see alerts similar to these activity signatures below, the end systems should be investigated for infections, scanned with an updated antivirus solution, and cleaned up.

For malware infections that have been detected by the IPS System Infected alerts, but are not detected with antivirus, you should do further analysis of these systems, including:

1. Run the Symantec Power Eraser solution included in the SEP Support tool. Symantec Power Eraser includes a powerful reputation-based detection mechanism not included in the main SEP 11 product.
2. Submit suspected malware-infected files to Symantec Security Response for analysis.

3. Open a support case and work with the Symantec Enterprise customer support team to assist in malware removal, or work with a security partner that specializes in malware removal.

To find out more information about the attack, you should read the detailed IPS signature threat write-up on the Symantec Security Response site (see section “IPS Signature Threat Write-ups, Signature Updates, and LiveUpdate).

Example IPS Signature: “Sig ID 23621 System Infected: Tidserv Request” means that your system is infected and that SEP IPS has detected the presence of the Tidserv rootkit that was missed by the antivirus program and that SEP IPS has stopped the attempt of the Tidserv malware to send outbound connections. You should immediately investigate and remove the infection with the recommended removal tools. Symantec has removal tools specifically for Tidserv that should be used in addition to the Symantec Power Eraser included in the SEP support tool. Symantec customers with valid support contracts can work with our enterprise customer support agents to assist them.

<table>
<thead>
<tr>
<th>IPS Signature ID</th>
<th>IPS Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>23621</td>
<td>System Infected: Tidserv Request</td>
</tr>
<tr>
<td>23615</td>
<td>System Infected: HTTPS Tidserv Request 2</td>
</tr>
<tr>
<td>23576</td>
<td>System Infected: HTTPS Tidserv C and C Domain Request</td>
</tr>
<tr>
<td>23320</td>
<td>System Infected: P2P Download</td>
</tr>
<tr>
<td>23048</td>
<td>System Infected: Trojan Brisv A</td>
</tr>
<tr>
<td>23271</td>
<td>System Infected: ZBOT Activity</td>
</tr>
<tr>
<td>23943</td>
<td>System Infected: Trojan Vundo 2</td>
</tr>
<tr>
<td>23304</td>
<td>System Infected: W32 Waledac Malicious Domain</td>
</tr>
<tr>
<td>23367</td>
<td>System Infected: Koobface Executable Hosting Domains</td>
</tr>
<tr>
<td>23456</td>
<td>System Infected: SDBot</td>
</tr>
<tr>
<td>23545</td>
<td>System Infected: Koobface C&amp;C Update Communication</td>
</tr>
<tr>
<td>23547</td>
<td>System Infected: Koobface C&amp;C Malicious File Download</td>
</tr>
<tr>
<td>23548</td>
<td>System Infected: Koobface C&amp;C Server Domains Request</td>
</tr>
<tr>
<td>23549</td>
<td>System Infected: Yabucks Trojan</td>
</tr>
</tbody>
</table>

Examples of post-compromised system detection activity signatures

4.6 Malicious Domains, Websites and IP address protection (Malicious Site)

Symantec Endpoint Protection IPS has the ability to block known malicious domains, websites, and IP addresses. These sites may include combinations of threats—including drive-by downloads and social-engineering attacks—and have been flagged with Symantec’s domain reputation solution as hosting malicious content. An IPS signature alert detecting an attempt to visit the malicious website will have the “Malicious Site” prefix in the description.

If an IPS alert occurs with the “Malicious Site” prefix, your system was protected from any traffic from the malicious site and the connection was dropped. No further attempts should be made to visit the site hosting the malicious content.

4.7 Spyware/Adware Detection

Spyware and adware continue to be a security risk to enterprise users. To help mitigate the risk and identify potential policy violations, SEP IPS can be used to detect a range of spyware and adware on endpoint systems. The detection of
Spyware and adware might NOT indicate an infection, but may just indicate the presence of a risk that you need to assess. These detections can be used to manage your enterprise security policies, or used to identify and determine whether these risks are allowed to run within your enterprise.

### 4.7.1 Recommended next steps for Spyware/Adware events

An IPS alert identified as Spyware/Adware should be investigated according to the policy of your organization. These IPS events are often enabled or disabled based on usage policies within an enterprise. To find out more information about the IPS event, you should read the detailed IPS signature threat write-up on the Symantec Security Response site (see section “IPS Signature Threat Write-ups, Signature Updates, and LiveUpdate”).

<table>
<thead>
<tr>
<th>IPS Signature ID</th>
<th>IPS Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>20781</td>
<td>TopMoxie Requesting Build Files</td>
</tr>
<tr>
<td>20782</td>
<td>Topmoxie Recoding Downloads and Offers</td>
</tr>
<tr>
<td>20784</td>
<td>HTTP 180Solutions Config Event</td>
</tr>
<tr>
<td>20800</td>
<td>HTTP MyWay Configuration Request</td>
</tr>
<tr>
<td>21329</td>
<td>CometCursor Cursor Download</td>
</tr>
<tr>
<td>21475</td>
<td>Webrebate Activity</td>
</tr>
</tbody>
</table>

**Examples of some of the Adware/Spyware detection signatures (note these do not have a prefix):**

### 4.8 Peer-to-Peer and Instant Messaging Identification/Detection

The SEP IPS solution includes capabilities to detect a variety of non-encrypted peer-to-peer (P2P) and instant messaging (IM) traffic. This type of detection MUST be added via a custom policy because these types of events are considered audit or policy-based detections. Nothing is inherently malicious about this type of traffic, but it may violate your corporate or enterprise usage policy. Some companies can use these signatures to identify potential data leaks because traffic such as P2P is notoriously used by malware to send information out of a company. This detection can assist you in monitoring traffic patterns within your network. Alerts of these types of triggers only indicate the potential presence of P2P or IM traffic. These detections can be used to manage a policy within your enterprise, or used to identify and determine whether these risks are allowed to run within your enterprise or not.

Note: P2P and IM traffic is often able to blend into normal HTTP traffic or use encryption techniques, making detection of this traffic difficult. SEP IPS detection should NOT be considered a comprehensive solution for detecting such traffic.

<table>
<thead>
<tr>
<th>IPS Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM ICQ Request (OSCAR)</td>
</tr>
<tr>
<td>Yahoo! Conference Login</td>
</tr>
<tr>
<td>Yahoo! IM Activity</td>
</tr>
<tr>
<td>Yahoo! IM Conference Invite</td>
</tr>
<tr>
<td>Yahoo! IM File Transfer</td>
</tr>
<tr>
<td>Yahoo! IM Login</td>
</tr>
<tr>
<td>P2P Ares Client Connection</td>
</tr>
<tr>
<td>P2P BitTorrent Activity</td>
</tr>
<tr>
<td>P2P BitTorrent Request</td>
</tr>
</tbody>
</table>

**Examples of some of the P2P and IM signatures (note the absence of a prefix):**
5.0 Incident Priorities of Threat Categories of IPS Signatures for Investigation

Symantec created IPS signature threat categories to clarify which types of threats and outbreaks you are battling. We have also ranked these threat categories according to their danger to the enterprise. Every organization is different, so these suggestions should be used as a starting place from which to decide if the danger level they pose needs to be raised or lowered based on the needs of your organization.

As noted above, P2P, IM, and Spyware/Adware signatures are considered audit detections and are not enabled by default. The presence of this traffic is not considered malicious, but needs to be determined by your policies. These audit signatures do not currently include a prefix.

Our recommendation is to prioritize attack event categories according to these priority levels (P1, P2, etc.):

- **System Infected (P1):** Threat events with the “System Infected” prefix should be the highest priority events being investigated for breach and malware removal. These events clearly indicate that an active infection of malware, Trojan, or a bot is trying to communicate outbound and that the signature is detecting this.

- **OS Attack (P2):** Threat events with the “OS Attack” prefix should be investigated with the second highest priority. These events occurring within an enterprise indicate that, while the individual system has been protected from the attack, you have an active infection coming from the server-bound direction. Correlation of these events can also easily help you pinpoint where the attack is originating.

- **Web Attack (P3):** Threat events with the “Web Attack” prefix should be investigated with the third highest priority. These systems were protected from a Web-based attack. Web attacks are higher priority over “Fake App” attacks due to their ability to infect a computer without a user’s knowledge. Analysis and correlation with any further antivirus, behavioral-based, or reputation-based events would raise the priority level for investigations.
• **Fake App Attack (P4):** Threat events with the “Fake App Attack” prefix should be investigated with the fourth highest priority. These end systems were protected from a social-engineering ploy using a fake antivirus or fake codec attack. No further investigation should be required. Since user interaction is required and the occurrence of these events is quite common from simple actions—such as Web searches or clicking on links within social media pages or email messages—these are considered slightly lower in priority for analysis than Web attacks. Analysis and correlation with any further antivirus, behavioral-based, or reputation-based events would raise the priority level for investigations.

• **Malicious Site (P5):** Threat events with the “Malicious Site” prefix should be investigated with the lowest priority. These end systems were protected from visiting a domain, website, or IP address of a known malicious site. No malicious activity should be able to come from this site as the malicious site event blocked all further communication.

• **Attack (P6):** Threat events with the “Attack” prefix are general attacks that may not have a specific category or that use other vectors such as different file formats or additional application vulnerabilities. Examples of such signatures may include MS Word, PowerPoint, Excel, or instant messaging applications. Investigation should be determined on a case-by-case basis.

### 6.0 Intrusion Prevention System Engine Overview

The Symantec IPS engine is a high-speed, multifaceted network-scanning and prevention solution focused at detecting and preventing today’s threats and security risks. The IPS engine uses deep-inspection protocol parsing and threat prevention capabilities to quickly and accurately detect threats and stop them on the network BEFORE they reach your users’ systems. For example, if a drive-by download tries to exploit a vulnerability in a PDF reader on a user’s system, the IPS engine inspects the network traffic going to that system and identifies the HTTP traffic. It then parses the HTTP header and finds the PDF content. The IPS engine breaks apart the PDF content and looks for compressed JavaScript. Only a subset of the IPS signatures then attempts to match, looking for an exploitation of the vulnerability. If there is a condition for exploitation of the vulnerability, then the connection is dropped, thus completely protecting the user. No malware is ever delivered to the user’s system. This is part of the high-speed, yet intelligent, protection technology.

The IPS solution is backed up by threat content and signatures created by Symantec’s Security Technology and Response (STAR) organization. STAR comprises over 500 threat researchers, analysts, and engineers who conduct vulnerability analysis and outbreak monitoring through the Symantec DeepSight™ Threat Management System and the Global Intelligence Network. Intelligence is gathered from more than 24,000 sensors worldwide to ensure that Symantec’s security solutions provide up-to-the-minute threat details. The IPS solution uses the LiveUpdate infrastructure to provide critical threat prevention content and updates.

### 6.1 Customers who want to run Network IPS, but not the SEP Firewall

For customers that want to use only the IPS capability and not the firewall in SEP 11, there is a [Symantec Knowledgebase article](https://www.symantec.com) for how to configure the firewall in a “pass-through mode.” This mode is compatible with the Microsoft Windows firewall, but not additional third-party client firewalls. IT managers can also withdraw the SEP Firewall policy from the group or location and only apply the SEP IPS policy. This will essentially have the SEP IPS enabled, but not have the SEP Firewall running.

In SEP 12, you will be able to enable the Firewall and IPS modules separately.
6.2 IPS Signature Threat Write-ups, Signature Updates, and LiveUpdate

Threat prevention signatures are created by engineers with Symantec STAR. Signature updates are provided via Symantec’s LiveUpdate servers and other automatic mechanisms.


The latest security updates for your SEP product can be found on the “Virus Definitions & Security Updates” page. From there, mouseover “All Security Updates by Product” and choose the product about which you want more information. Note that Symantec Antivirus 9 and 10 do NOT have IPS capabilities.

You can view the signature updates by release date. This includes the LiveUpdate Def ID that includes the full date code of the security update.
When you click through to the Security Update listings, you will get a list of the vulnerability coverage and threat coverage that was added, changed, or deleted. The severity is included to help guide you in determining the potential impact of issues and the impact on an enterprise. The Security Focus Bugtraq ID (BID) vulnerability information is included if it is applicable. Issues such as misleading applications and fake antivirus applications will not have an associated BID associated.

From this page, you can get even more information about the particular vulnerability or threat. For each issue, there is information that includes the threat description, severity, systems that could potentially be affected, and additional resource information. Often, if there is a CVE or MS-ID reference, it will be included here. Note that Microsoft IDs are often linked to multiple BIDs, so these IDs are not used as the primary vulnerability tracking mechanism. If the BID is included, you can look at the Security Focus BID listing to get more information.
Specific threat details

A full catalog of all Symantec signatures can be viewed at the Attack Signatures overview page. This may include signatures that are not included in your actual product or version that you have deployed, or is configured in your local policy.

6.3 Am I Protected from a New Vulnerability Being Exploited?

Symantec analysts have an incredible insight into the threat landscape that enables Symantec to quickly and accurately identify which vulnerabilities are being exploited around the globe. Nonetheless, many IPS vulnerability signatures cannot technically be written, as they would likely negatively affect the performance and availability of the enterprise endpoints. False positives and accuracy are other factors as well.

Symantec looks at a number of factors in determining protection for a vulnerability. This includes the threat information available, how critical and/or exploitable it is, its false-positive impact, and how possible it is even to create a signature reliably. Our priority is protecting against critical, remotely exploitable vulnerabilities in widely used applications and services that can allow code execution. Many vulnerabilities are local or privilege escalations that cannot be remotely exploited and therefore are not candidates for IPS signatures.

Factors that determine whether Symantec will provide a vulnerability IPS signature include:

- How widespread is the impact the vulnerability for enterprise and consumer users?
- What are the DeepSight and Security Response classifications of the vulnerability?
- Is the vulnerability remotely exploitable?
- Does the vulnerability allow for remote code execution?
- Do we have enough information about how this would be exploited?
- How likely and quickly will the vulnerability be exploited?
- How prone would an IPS signature be to false positives or false negatives?
- Which engine technology should we use in providing protection for the vulnerability? (E.g., AV-Bloodhound/IPS/Behavior/Reputation)
- What is the potential performance impact on an endpoint?
- Can our IPS engine technology implemented in the product provide protection?
6.4 Reporting False Positives

With tens of millions of customers having SEP IPS technology enabled by default, Symantec is very aware of potential false positives and takes numerous steps to prevent them. If you identify a possible false positive where our IPS technology is triggering on valid traffic, please visit the Symantec Security Response website to submit it.

IPS alerts include a signature ID and IPS event name

**Steps for submitting a false positive:**

1) Gather everything possible about the false positive including:
   a. The IPS SID (Signature ID) and the exact spelling of the IPS event alert name from the IPS log. Example: “[SID: 23831] Web Attack: Malicious Toolkit Variant 16 detected"
   b. The application that was blocked from the IPS log, including the full path. Example: “Traffic has been blocked from this application: C:\Program Files\Internet Explorer\EXPLOR\EXPLOR\EXPLOR.EXE”
   c. Source and destination IP addresses
   d. Security Update definition revision/date
   e. Version of SEP and MR level
   f. Any additional steps or software installed that could be helpful in resolving the situation. Example: “When browsing the website, www.example.com, and clicking on this first link, the IPS signature triggers”

2) Having a packet capture (PCAP) of occurrence would be preferred

3) To submit the IPS false positive, include all the information gathered to the Symantec Security Response website (http://www.symantec.com/business/security_response/index.jsp) and click on the link “Report a Suspected Erroneous Detection (False Positive)”

6.5 Mitigating False Positives:

If you do have a false positive that is preventing you from accessing a system or website, you can disable a single IPS/Network Threat Protection rule by removing it from your currently applied policy. Contact Symantec customer support if you have a question on how to do this.
6.6 Potential Performance Issues

With tens of millions of customers having our IPS technology enabled by default, Symantec is aware of potential performance degradations. On an enterprise endpoint or desktop, the impact on performance for everyday operations should be minimal, especially when compared to the overall protection benefit that is being provided against the threat landscape. If you have critical servers that are NOT able to tolerate even slight performance degradation, you should consider using our separate server protection solution, Symantec Critical System Protection.

7.0 Endpoint Protection Manager Reports

7.1 IPS Alerts

To find out which threats are affecting your enterprise and to use the IPS information to assist in identifying sources of infected machines or machines that are under attack, you need to check the Intrusion Prevention or Network Threat Protection logs within the Endpoint Protection Manager (SEPM). These are separate from the antivirus logs and events. To view all of the Intrusion Prevention or Network Threat Protection events:

1. Log onto SEPM
2. Click on the “Monitors” button
3. Click on the “Logs” tab
4. Select the "Network Threat Protection" log type
5. Select the "Attacks" log content
6. Click the "View Log" button
SEP manager console

SEP manager console showing event log
SEP manager console showing event description

Event Description: [SD: 21470] Adlogix SetupFile Request detected. Traffic has been blocked from this application. C:\Program Files\Mozilla Firefox\firefox.exe
Attack Type: Intrusion Prevention
Event Time: 12/14/2009 18:39:47
Remote Host IP: 66.152.93.119
Occurrence: 10
Alert: 1
Begin Time: 12/14/2009 18:39:33
End Time: 12/14/2009 18:39:47
Domain Name: Default
Site Name: Site Elisha
Server Name: Elisha
Group Name: My Company/Marketing
Computer Name:
  Current: Elisha
  When event occurred: Elisha
IP Address:
  Current: 192.168.99.1
  When event occurred: 10.180.148.153
Operating system name: Windows XP Professional
Location Name: Default
User Name: SymUser
Severity: Critical
Local MAC: 001AA9E0C91
Remote MAC: 000000000000
Hardware Key: 202E2D2B2F4A8E71E3A1658787BE0E4A7
Network Protocol: TCP
Traffic Direction: Outbound
Send SNMP trap: 1
Remote Host Name:
Hack Type: 0
Application Name: C:\Program Files\Mozilla Firefox\firefox.exe
About Symantec
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com