Malware Prevention with Blue Coat Proxies

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "software". The expression is a general term used to mean a variety of forms of hostile, intrusive, or annoying software or program code including computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software.

Malware prevention cannot be achieved by one method on its own, it is best achieved by putting up many layers – this includes the firewall and desktop-based solutions. This document explains how the Blue Coat family of products can deliver best-in-class defense against a multitude of security issues that threaten organizations.

The content policy language (CPL) included with Blue Coat's ProxySG provides a powerful toolkit for blocking mobile malicious code (MMC) and preventing Malware infection encountered on the Internet. With the addition of Blue Coat Web Filter's on-box and dynamic real-time rating (DRTR) service, these rules can be selectively applied so that the "bad neighborhoods" of the Internet receive additional protective measures. Finally the Blue Coat ProxyAV (anti-malware) can be added to provide heuristic analysis and signature scanning, to augment your desktop-level AV product choice. This system follows the doctrine of "defense in depth" rather than assuming any one defensive tactic is sufficient.

NOTE: Where Visual Policy Manager (VPM) methods can replace CPL, they have been described; where they cannot replace CPL, you can write the given CPL to a text file and then install it as a policy using the Management Console ***Policy > Policy Files*** *page.*

Implementation of five methods of defense against malware is described:

- Blocking Access to Malware Sites
- Detecting Hidden File Types
- Removing Active Content from HTML Pages
- Blocking Mobile Malicious Code
- Implementing Anti-malware Protection

Blocking Access to Malware Sites

Firstly, not accessing a malicious website guarantees avoiding infection by it. To that end Blue Coat Web Filter (BCWF) provides the "Spyware/Malware Sources," "Spyware Effects/Privacy Concerns," and "Phishing" URL categories. Blocking access to these categories of websites removes known bad sites from the risk of infection. Additionally, the dynamic real-time rating service of BCWF includes automatic detection of phishing kits, phishing look-alike web pages, and untrustworthy temporary DNS registered hostnames, to protect against new and emerging threats. However the concept that bad things only exist in bad sites has its limitations. Often attacks come from MMC injected into popular websites where reputation and host ratings, or known bad URL categories, do not block access for the user. Therefore another method of the defense provides content analysis for these cases. The point with this method is to remove the known bad sites up front.

You can see Blue Coat URL categories by going to Blue Coat Category Descriptions; you can discover the category of a URL using the Blue Coat Web Page Review Process. Unlike other systems, Blue Coat can cross categorize a single site into multiple categories (up to four) and you can create custom URL categories of your own.

Table 1 offers recommendations of actions that can be set on a per-URL category basis.

Table 1: Blue Coat URL Category Recommendations Example

Category	Recommendation
Spyware effects	Block and Report
Spyware sources	Block all executables and report
Pornography	Block and Report
Social Networking	Block all executables

Using CPL to Block Access to Known Malware Phone-Home Sites

The "Spyware Effects/Privacy Concerns" URL category can be used to identify already infected computers in an organization by logging/alerting when known, phone-home type traffic is detected.

This rule blocks known malware phone actions with the policy action "force_deny" that can not be overridden by later actions:

```
<proxy>
url.category=("Phishing","Spyware Effects/Privacy Concerns") force_deny
```

Using the Management Console to Block Access to Malware Sites

1. Go to **Content Filtering > General** and enable **Blue Coat Web Filter**; leave the **Lookup Mode** set to **Always**. Click **Apply** to finish.
2. Go to **Configuration > Content Filtering > Blue Coat**; enter a User Name and Password (click **Change Password**) and download the database at the default URL by clicking **Download now**. Click **Apply** to finish.
3. Use VPM to write a policy rule to deny these categories: In a Web Access layer, click **Add Rule**. Right-click the **Destination** setting and choose **Set**. The Set Destination Object dialog opens
4. Click **New** and choose **Request URL Category**. The Add Request URL Category dialog opens.
5. Expand the **Blue Coat** option and select the categories for that rule that you want. You can name the object at the top of the dialog to reflect the URL categories. When you are finished, click **OK**. Click **OK** again to set the object. Click **Install Policy** to finish.

For details, see the SG Appliance Configuration and Management Guide, "Configuring Blue Coat Web Filter" section.

Detecting Hidden File Types

The defense in depth strategy continues with detailed CPL tests to prevent misrepresentation of true file types, or container mismatch. Too often today, malicious executable content is misrepresented as safe file types such as "JPG" or "GIF". Blocking this makes use of policy tests comparing the claimed file type to the actual initial data in the files. ProxySG also provides an Apparent Data Type check within the Management Console that can be applied to policy rules in the Visual Policy Manager (VPM).

Using CPL to Detect Hidden File Types

The following is an example of a CPL policy designed to compare the claimed file type to its header and block when a mismatch is found.

```
define condition Object_RepresentedAs_Executable
    ; Test URL extension
    url.extension=(exe,com,cab,ocx,dll,msi)
    ; Test for content-type headers
    response.header.Content-Type="application/cab"
    response.header.Content-Type="application/octet-stream"
    response.header.Content-Type="application/x-msdownload"
    response.header.Content-Type="application/x-msdos-program"
    ; Test for content-disposition (how to save) headers
    response.x_header.Content-Disposition = "\.(exe|com|cab|ocx|dll|msi)($|[^a-z0-9])"
end
;
define condition Object_Data_Executable
    ;exe, com, ocx
    http.response.data.2.case_sensitive="MZ"
    ;msi
    http.response.data.8.regex="^\xD0\xCF\x11\xE0\xA1\xB1\x1A\xE1"
    ;cab
    http.response.data.4.case_sensitive="MSCF"
end
;
<proxy>
condition=!Object_RepresentedAs_Executable \
condition=Object_Data_Executable force_deny
```

NOTE: The bang (!) means “not,” so this test translates to: “not represented as an executable and data is executable.”

This example tests only for misrepresentation of a few data types (exe, com, cab, ocx, dll, and msi). A more protective policy would leverage these types of tests to deny other file types entirely; for example, ".scr" or ".ani;" MS Windows screensavers and animated cursor files are almost always disguised malware.

Using VPM to Detect Hidden Data Types

This policy defines data types to be examined for authenticity and exempts those data types from action that are authenticate while blocking those data types that are masquerading as something else.

1. In a Web Access Layer, right-click the **Destination** setting and choose **Set**. The Set Destination Object dialog opens.
2. Click **New** and choose **Combined Destination Object**. The Add Combined Destination Object dialog opens.
3. Add a Response Data object:
    a. Click **New** and choose **Response Data**. The Add Response Data Object dialog opens.

    b. Enter the regex value for each data type you want detected and removed; add each data type to the combined destination object **At least one of these objects** group by selecting it at left and clicking **Add >>** at top.
4. Continue by adding a file extensions object to the combined destination object:
    a. Click **New** and choose **File Extensions**. The Add File Extensions Object dialog opens.

   b. Select all executable files extensions. Once finished, click **OK**, then add the file extensions object to the combined destination object **None of these objects** group by selecting it at left and clicking **Add >>** at bottom.

5. Continue by adding an HTTP mime types object to the combined destination object:

   a. Click **New** and choose **HTTP Mime Types**. The Add HTTP Mime Types object dialog opens.

   b. Select all executable mime types. Once finished, click **OK**; then add the HTTP mime types object to the combined destination object **None of these objects** group by selecting it at left and clicking **Add >>** at bottom.

   c. Optional: If there are additional mime types that you want to block not available in the HTTP Mime Types object dialog, you can add a **Response Header** object and enter those there and then add that object to the **None of these objects** group.

6. Select the **Negate** checkbox below the **None of these objects** group. Click **OK** to complete creation of the combined destination object. Click **OK** to set the combined destination object

7. Right-click the **Action** setting and choose **Set**. The Set Action dialog opens. Scroll down to **Force Deny**, select and click **OK**. Click **Install Policy** to finish.

For details, see the SG Appliance Configuration and Management Guide, "Destination Column Object Reference, Response Data" section.

Removing Active Content from HTML Pages

Mobile Malicious Code (MMC) is not an "executable" in the traditional "exe" file sense, it exploits vulnerabilities in the browser (or other client application) software through malicious JavaScript, VBScript, Flash or ActiveX modules. Protection against these can take several forms from stripping all "active-content" from pages, to selectively "de-fanging" malicious code methods, and/or signature/heuristic scanning.

The safest option that still allows access to Web pages is sanitizing the HTML to remove all active-content; however, this has significant impact on today's interactive Web 2.0 sites. Due to the risk of over-blocking, this option should be applied in conjunction with the BCWF to only occur on the riskiest, least business-oriented sites. Any exceptions can then be handled by whitelisting.

Using CPL to Remove Active Content from HTML Pages

The following CPL policy defines white-listed domains and URLs first, then high-risk domains and URLs, and then the action to remove from the high-risk sites certain active content code "tags." While the white list of trusted web pages is created in CPL it may be edited later through the VPM for convenient maintenance.

```
; Define a whitelist category with a list of domains/URLs
define category WhiteList-ActiveContentHTML
   playboyenterprises.com
end category WhiteList-ActiveContentHTML
;
define condition HighRisk_Categories
   url.category=("Adult/Mature Content","Pornography","Gambling")
   url.category=("Non-viewable","Placeholders","Suspicious")
   url.category=("Proxy Avoidance")
end
;
; define the transformation action to remove certain tags
```

```
define active_content transform_Strip_ActiveContent
    tag_replace object <<EOT
        Risky content removed from this page (object).
    EOT
    tag_replace script <<EOT
        Risky content removed from this page (script).
    EOT
    tag_replace embed <<EOT
        Risky content removed from this page (embed)).
    EOT
    tag_replace applet <<EOT
        Risky content removed from this page (applet).
    EOT
end active_content transform_Strip_Risky_Tags
define action Strip_ActiveContent
    transform transform_Strip_ActiveContent
end
;
; Apply conditional test and action (note the use of line-wrapping \)
<proxy>
    category=!WhiteList-ActiveContentHTML \
    condition=HighRisk_Categories \
    action.Strip_ActiveContent(yes)
```

Using VPM to Remove Active Content

You can create a "strip active content" Action object in the VPM and apply it to a Web Access Layer:

1. In the VPM for a Web Access Layer, right-click the **Action** setting and choose **Set**. The Set Action Object dialog opens.
2. Click **New** and choose **Strip Active Content**. The Add Strip Active Content Object dialog opens.
3. Select the active content types that you want removed; your choices include <applet>, <embed>, <object>, and <script> objects. Click **OK** to close the dialog. Click **Install Policy** to finish.

Exempting the SG Appliance and Whitelisting Domains and URLs

Stripping active content might interfere with Web applications deployed on your intranet. For example, if you create a policy rule that removes Java applets, and the destination defined in the rule contains an IP address of a SG appliance functioning as a proxy, the policy rule actually disables the Management Console because the Console itself is comprised of Java applets. To prevent this, for each SG appliance functioning as a proxy, create a rule using the VPM that exempts the IP address of the appliance from the stripping action:

1. Click **Add Rule**. A new rule line displays for the Strip Active Content policy.
2. Click **Move Up**; the rule to exempt the SG appliance must precede the rule that strips active content.
3. Right-click the **Destination** setting and choose **Set**. The Set Destination Object dialog opens.
4. Click **New** and choose **Destination IP/Subnet Object**. The Add Destination IP/Subnet Object dialog opens.
5. Enter the SG appliance IP address and subnet and click **OK**. The value entered displays as an object choice in the Set Destination Object dialog. You can enter multiple IP addresses here for exemption from the policy, if needed. When finished, click **Close** to dismiss the dialog; click **OK** to set the IP address as the Destination

*NOTE: Create a combined destination object by clicking **New > Combined Destination Object** and adding the URLs to the **At least one of these objects** group. Click **OK** to finish creating the object; click **OK** to set it.*

6. Exempt the SG appliance or the Combined Destination object: Right-click the IP address or combined destination object in the **Destination** setting and select **Negate** from the drop-down list.
7. Right-click the **Action** setting and choose **Set**. The Set Action Object dialog opens.
8. Click **New** and choose **Strip Active Contents**. The Add Strip Active Contents dialog opens. Select the same active contents types that you chose previously. Click **OK** to create the object; click **OK** to set it. Click Install Policy to finish.

For details, see the SG Appliance Configuration and Management Guide.

Blocking Mobile Malicious Code

The next level of protection is an attempt to "de-fang" malicious active code inserted into Web pages. Certain aspects of the typical malware infector are uncommon in normal web pages. This can be used against them to prevent their code from executing if it reaches the browser. Two techniques for this in CPL are "script string rewriting" and "script injection."

Before You Begin

String rewriting is a CPU intensive action and should be deployed with care. Commonly this level of protection is only needed for external resources and can be disabled for websites within the trusted network. Without an understanding of where your data is coming from (a trusted or untrusted site) these mechanisms introduce delay for the user and can over-block legitimate code from trusted sources. By blending the source of the data, the user downloading the data, and acquiring an understanding of the data itself, more accurate decisions can be made that don't over-block. Blue Coat recommends that an analysis of activity be made before-hand so that proper exceptions can be developed. The following table is an example of the kinds of decisions that need to be considered before deploying the MMC policy.

Table 2: Example Data Classifications

User	Source	Data	Decision
Anyone	Unknown	Request for input	Warn or block user; potential phishing site
Anyone	Adobe	Executable	Allow as site is trusted
Non-IT department	IT Category	Executable	Warn user, provide IT number
IT department	IT Category	Executable	Allow
Anyone	Sports	Executable	Block

Using CPL for String Rewriting and Script Injection

String rewriting in scripts allows certain keywords in the HTML malware to be replaced with innocuous substitutions; while script injection can override those functions typically used by malware to unpack itself and thus silently prevent the browser from executing them. Because a full implementation of these techniques is too large for this document, the following is a sample script to replace one string pattern ("string_pattern") and override the "eval" JavaScript function.

```
define javascript transform_override_JS_functions
prolog <<EOF
//Deny all "eval" calls
function bluecoat_eval()
{
   //do nothing, we intend to disable the eval function
}
eval = bluecoat_eval;
//
EOF
end
;
define action override_JS_functions
   transform transform_override_JS_functions
end
;
define url_rewrite transform_ScriptStringReplace
   rewrite_script_substring "REMOVED" "string_pattern"
end
define action ScriptStringReplace
   transform transform_ScriptStringReplace
end
;
<proxy>
   action.override_JS_functions(yes) action.ScriptStringReplace(yes)
```

Implementing Anti-Malware Protection

Assuming all the above levels of defense are applied, a significant reduction in malware can be achieved with ProxySG and BCWF alone; however, no solution is complete without leveraging the billions of dollars spent each year by the antivirus industry on signature and heuristic based detections. This is available via the Blue Coat ProxyAV.

Blue Coat recommends that all objects be subjected to such scanning regardless of their website of origin, or file type. The ProxySG + ProxyAV solution makes this workable via the "scan once, serve many" technology. Each time a browser request is received, the ProxySG checks its object store for a cached copy, if one is found that was analyzed with the most recent AV-heuristics engine version, it can be delivered immediately. If the object in cache was analyzed before an update to the AV-heuristics engine, then the object is re-analyzed before delivery to the user. For non-cacheable objects, a finger print cache is kept to avoid analyzing the same file on frequent requests. Once an AV-heuristics engine update occurs, the finger print cache for non-cacheable objects restarts. Note that ProxyAV has four options for analysis, it can scan, trickle first, trickle last or defer scan (for long load objects).

Using CPL to Implement Antivirus Protection

```
; This policy assumes you have configured an ICAP response-modification
; external service/service-group named "proxyav".
; Additionally this policy will deny all access if that service is
; unavailable (fail_closed), if the preferred action is "fail_open"
; modify as appropriate.
<cache>
    response.icap_service(proxyav,fail_closed)
```

Using VPM to Implement Antivirus Protection

To create the ICAP service using the VPM:

1. Go to **External Services > ICAP** in the Management Console. Click **New** and create an ICAP service; name the service **proxyav**. Click **Apply** to finish creating the service; click **Edit** to specify service parameters, including the URL and port of the service.
2. Using VPM, in a Web Content Layer, right-click the **Action** setting and choose **Set**. The Set Service Object dialog opens.
3. Click **New** and choose **Set ICAP Response Service**. Add the **proxyav** service and click **OK**. Click **Install Policy** to finish.

Selection of which AV engine to run on ProxyAV should be made to compliment the desktop antivirus solution in place throughout the enterprise. Blue Coat supports four different AV vendors and recommends using a different vendor at the gateway vs. the desktop so that two separate anti-malware labs are working to protect your network.

Note: ICAP can be used for both inbound and outbound traffic analysis. Typically ProxyAV is deployed for inbound traffic analysis while a data loss prevention solution is deployed for outbound traffic analysis. Multiple ProxyAVs can be load balanced from a ProxySG device.

Testing the Policies

Alongside the "Malware Prevention with Blue Coat ProxySG" document is a zip file, "MMC-testpage.zip," which you can use to test the Detect Hidden File Types, Remove Active Content, and Block MMC policies. Download and unpack the zip file, place the files on a web-server, and modify the policies you want to test to trigger specific actions on the test file's URL.

Including a Redirect and Alert Message for Users

Blue Coat recommends including a redirect for affected messages to a website with a message for users alerting them to the fact that their web page, or email was altered. For example, "We have blocked a piece of active code from website (insert hostname) as it was trying to execute a command that breaks our security policy. Contact IT Support for more information."

There are several ways to alert users of proxy actions; for instructions on using the VPM to create Notify User objects for a policy, see the SG Appliance Configuration and Management Guide, "Action Column Object Reference, Notify User" section. To implement a disclaimer page, see the ProxySG Technical Brief – Creating a Disclaimer Page.

Using Reporter

A vital part of any comprehensive anti-malware solution also utilizes Blue Coat's Reporter function to see which users have been "saved" from malware, viruses and spyware the most – giving management information on the employees that need the most training. Reports on spyware effects (also known as "phone-home" traffic) show which PCs have been infected and need to be cleaned.

Blue Coat Reporter analyzes comprehensive log files from Blue Coat ProxySG in over 150 pre-defined reports, including malware, spyware, IM, P2P, and popular sites. Beyond URL filtering, Reporter provides visibility to Web content, performance, threats, and trending over defined time periods. With comprehensive, policy-enabled logging, Blue Coat Reporter with ProxySG provides the advantage of capturing data regarding all user Web activities. Reporter quickly processes robust log data, providing easy-to-view reports for department managers, HR managers, security specialists, and network administrators. Blue Coat provides the ultimate architecture for complete Web visibility and control.

Conclusion

The Internet today consists of much more than the traditional web page; instant messaging, streaming content, and file-sharing traffic, malware, viruses and spyware now enter and leave the network through many methods. ProxySG provides full visibility and protection within all common Internet protocols, including SSL encrypted traffic (HTTPS).

Some threats arrive outside the content itself, such as buffer-overflow exploits against player applications. The ProxySG with CPL can have rules such as those described in this document, to block many such attacks. Additionally, the nature of a proxy itself assists: client and server communications are separate network connections, so only data the proxy software chooses to transfer gets through. Internal consistency and buffer checking in the ProxySG prevent some exploits even without special configuration.

ProxySG appliances are a powerful solution for protecting against Web threats, including malware, spyware, viruses, and malicious code, because proxies have visibility and understanding of users, content, and applications, and can use this information to apply appropriate controls. They can accelerate legitimate business-critical applications, manage or mitigate the effect of non-business applications, and stop malicious traffic before it reaches the user.