测试爆发过滤器URL重写

目录

简介

本文描述如何为URL重写测试爆发过滤器()消息修改选项。

背景信息

如果消息威胁级别超出消息修改阈值，爆发过滤器功能重写在消息的所有URL重定向用户到Cisco Web安全代理飞溅页，如果他们点击任何一个。 AsyncOS重写URL在消息里面除了那个指向被绕过的域的所有。

URL重写的可以使用以下选项：：

- 仅Enable (event)未签名的消息的。此选项允许AsyncOS重写在满足或超出消息修改阈值的未签名的消息，但是没签字的消息的URL。Cisco推荐使用此设置URL重写。 **Note**:如果一种服务器或工具在您的网络除电子邮件安全工具之外对验证DomainKeys/DKIM签名，负责电子邮件安全工具可能重写在一个DomainKeys/DKIM签字的消息的URL和无效消息签名。工具考虑一个消息签字，如果被加密使用S/MIME或包含一个S/MIME签名。 如果一种服务器或工具在您的网络除电子邮件安全工具之外对验证DomainKeys/DKIM签名，负责电子邮件安全工具可能重写在一个DomainKeys/DKIM签字的消息的URL和无效消息签名。工具考虑一个消息签字，如果被加密使用S/MIME或包含一个S/MIME签名。
- 所有消息的Enable (event)。此选项允许AsyncOS重写在满足或超出消息修改阈值的所有消息的URL，包括签字的那些。如果AsyncOS修改一个签字的消息，签名变得无效。
- 功能失效。此选项禁用重写为爆发过滤器的URL。

您能修改策略排除URL到某些域从修改。要绕过域，请输入IPv4地址、IPv6地址、CIDR范围、主机名-，部分主机名-或域在旁路域扫描字段。使用逗号，分离多个条目。

旁路域扫描功能是类似于，但是独立， URL过滤使用的全局whitelist。关于该whitelist的更多信息，请参阅“创建URL过滤的Whitelists”在ESA用户指南。

测试爆发过滤器URL重写

有两个选项对测试在ESA。

测试第一部分

包括有恶意的URL在电子邮件正文。 能使用的安全的测试URL ：

http://malware.testing.google.test/testing/malware/

当发送，邮件日志示例应该包含类似于以下：

```
Tue Jul  3 09:31:38 2018 Info: MID 185843 Outbreak Filters: verdict positive
Tue Jul  3 09:31:38 2018 Info: MID 185843 Threat Level=5 Category=Malware Type=Malware
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten to MID 185844 by url-threat-protection
filter 'Threat Protection'
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185843 done
Tue Jul  3 09:31:38 2018 Info: MID 185844 Virus Threat Level=5
Tue Jul  3 09:31:38 2018 Warning: MID 185844 Failed to add disclaimer as header. Disclaimer has
been added as attachment.
Tue Jul  3 09:31:38 2018 Info: MID 185844 rewritten to MID 185845 by add-heading filter 'Heading
Stamping'
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185844 done
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185846 done
Tue Jul  3 09:31:38 2018 Info: MID 185845 enqueued for transfer to centralized quarantine
"Outbreak" (Outbreak rule Malware: Malware)
Tue Jul  3 09:31:38 2018 Info: MID 185845 queued for delivery
```

注意邮件日志显示我们“重写的URL”的，指示通过Cisco Web安全代理重写此URL。 并且，请注意消息在我们的示例可能在爆发检疫，如显示这里。

最终结果将有显示以下的被传送的电子邮件正文：

WARNING: Your email security system has determined the message below may be a potential threat.

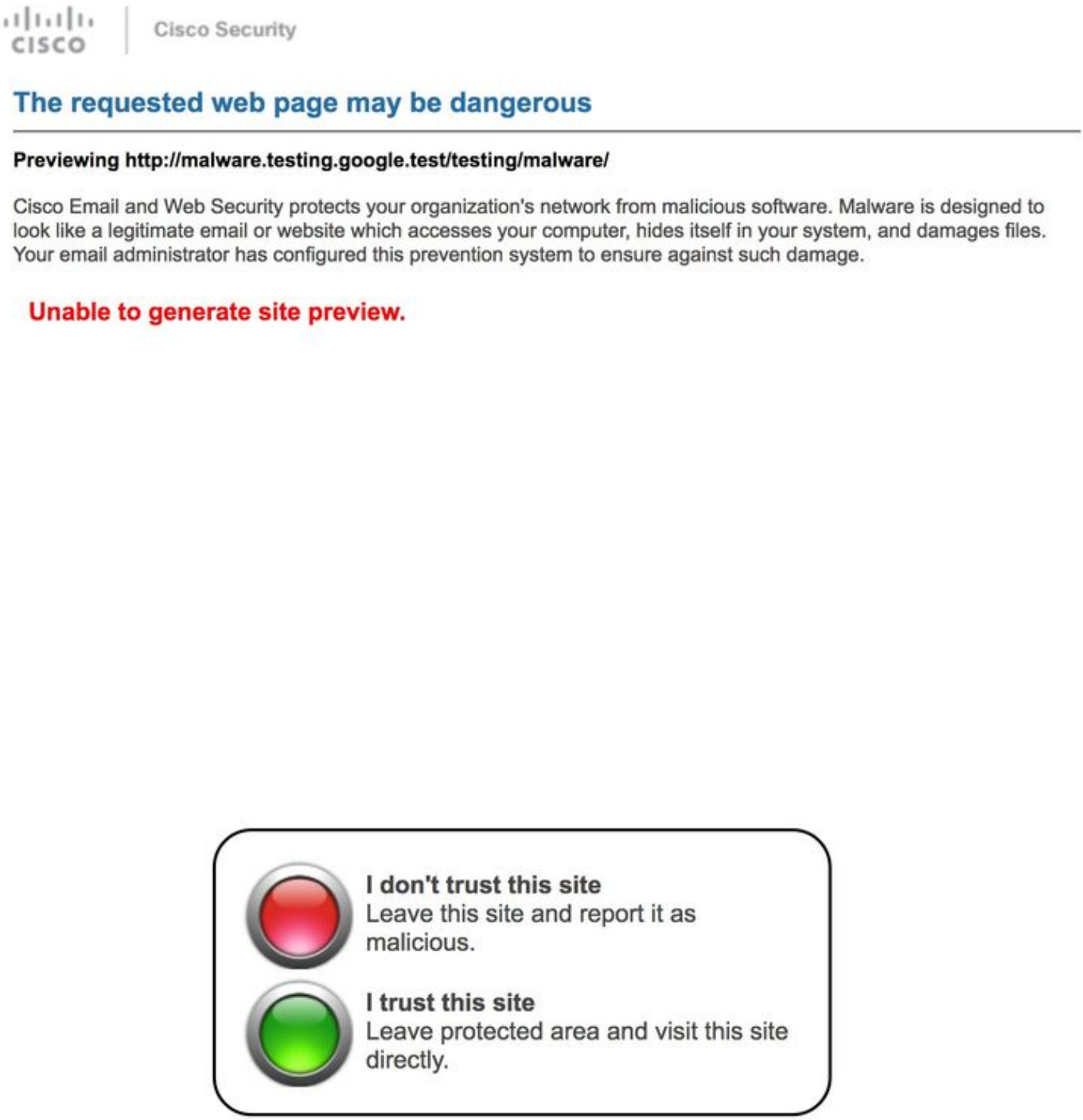
It may trick victims into clicking a link and downloading malware. Do not open suspicious links.

If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

Here.

http://secure-web.cisco.com/1ZzJhYfgzugtou3v__nw-VbytKC7kXMoWpj93VzB1wL2PuGPyCMDQ_DH4k4uYLGEfKi0U-D_lOtZp4TnwCkXE8iZ7MuiouY6PUDX5h_eluxNeebE3dVdoBU6EvlDJSPBvfL21qdeZ52HQ74ahop81kBXttP-ZIcoYNPjkxBq2lUR1AG9u1b2w2mC_bYnT-XoeEWxQs_Mjd7NRBjTFRLNGzH7uii_o-QPPCFMKqGC85swJ8Y5Um7pG_f3qydi2Hk2r9IYV-gixFC9m-a6Q0HBSLYLNp4JIpxJy5Hc_8ieJRvzHAY9UjRy-Az6SEV2hvjsrwy03HbOm-f9sJDRbnrXcIhNgk4gbpjtXWdkQGSxSsxaxdxkFy6yUAF605wSINVA6/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F

当终端用户当前收到电子邮件时，点击重写的URL，他们重定向对Cisco Web安全代理并且看到：



Note:“无法生成站点预览”将显示根据原始URL或网站的HTML/encoding。 有CSS ， HTML面或者复杂转换的一个网站不能生成站点预览。

测试部分两

第二个选项是包括在电子邮件正文或附件内的数据为了有触发器。

有两个选项为了成功：

1. 用名字“hello.voftest”创建一个文件(简单的文字文件将做)在25000个和30000个字节之间的大小，并且附加该文件您的测试电子邮件。这将触发病毒附件规则。

2. 安置以下GTUBE (“未经请求的大批电子邮件的通用的测试”) 72字节测试stringtext在电子邮件的正文：

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTPHISH-STANDARD-ANTI-PHISH-TEST-EMAIL*C.34X
```

这触发和phish规则。 邮件日志示例应该包含类似于以下：

```
Tue Jul  3 09:44:12 2018 Info: MID 185880 Outbreak Filters: verdict positive
Tue Jul  3 09:44:12 2018 Info: MID 185880 Threat Level=5 Category=Phish Type=Phish
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten to MID 185881 by url-threat-protection
filter 'Threat Protection'
Tue Jul  3 09:44:12 2018 Info: Message finished MID 185880 done
Tue Jul  3 09:44:12 2018 Info: MID 185881 Virus Threat Level=5
Tue Jul  3 09:44:12 2018 Warning: MID 185881 Failed to add disclaimer as header. Disclaimer has
been added as attachment.
Tue Jul  3 09:44:12 2018 Info: MID 185881 rewritten to MID 185882 by add-heading filter 'Heading
Stamping'
Tue Jul  3 09:44:12 2018 Info: Message finished MID 185881 done
Tue Jul  3 09:44:13 2018 Info: MID 185882 enqueued for transfer to centralized quarantine
"Outbreak" (Outbreak rule Phish: Phish)
Tue Jul  3 09:44:13 2018 Info: MID 185882 queued for delivery
```

注意邮件日志显示我们“重写的URL”的，指示通过Cisco Web安全代理重写此URL。 并且，请注意消息在我们的示例可能在爆发检疫，如显示这里。

最终结果将有显示以下的被传送的电子邮件正文：

WARNING: Your email security system has determined the message below may be a potential threat.

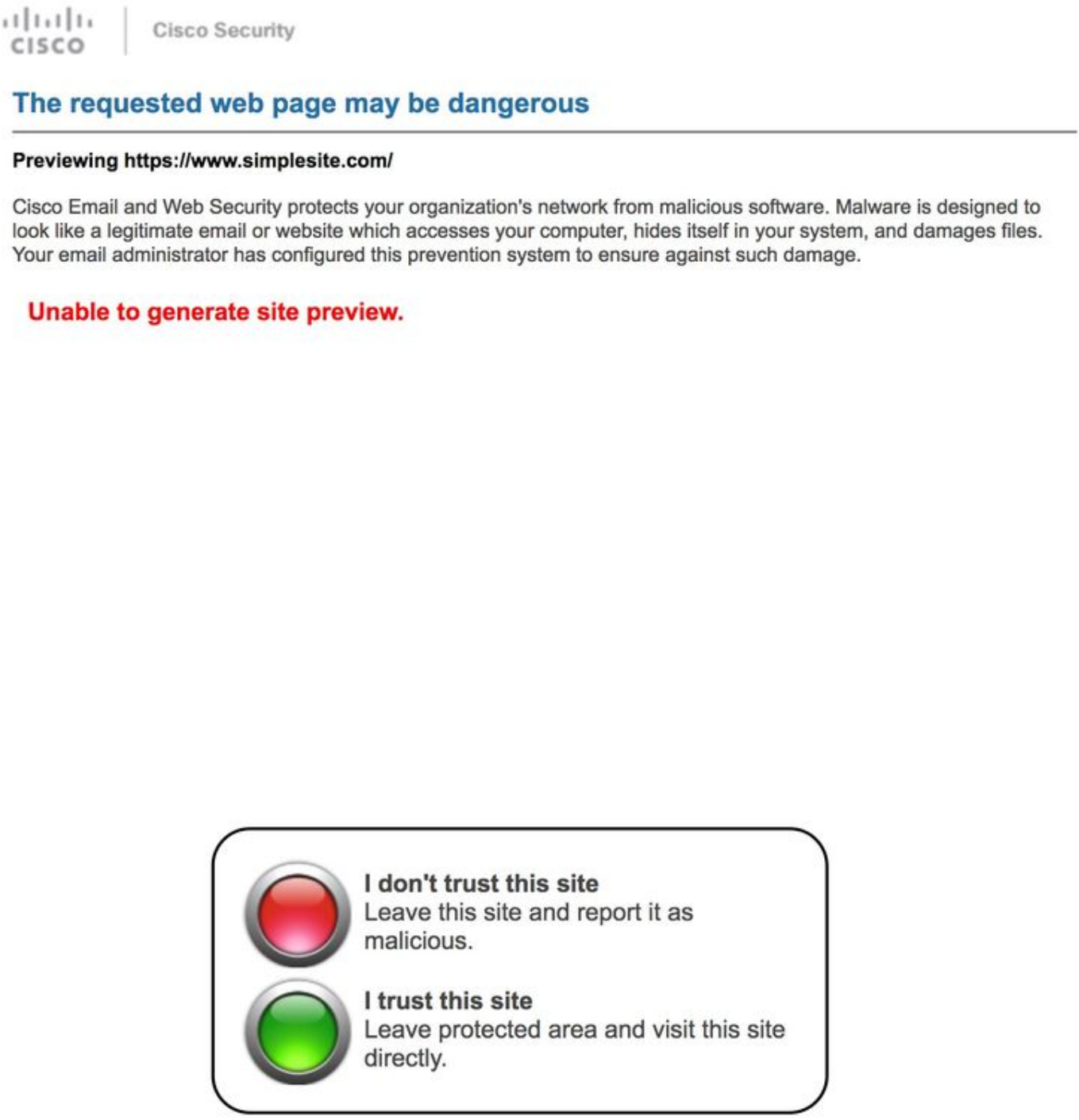
It may pose as a legitimate company, tricking victims into revealing personal information.

If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTPHISH-STANDARD-ANTI-PHISH-TEST-EMAIL*C.34X

https://secure-web.cisco.com/1Rs3ykyK_-fhhFahFEVsZdaxsTZUT7Qgp5h_XwacJhK0Y5fYXfiQJ9sSgledHbUH3ssTG4qJszR9zf1dMRpEPjq0U11EVsDE2NF3nKRlWKrkCtAe1GNtTi5TGeYK9PZ8-3l1zXVm2nrQmGj2PQH4yyISkPJ6-SgJHyrTKlOpa6JgbKMc1pEMumW6Zyoa4DyjrrronTquLumPRnqvmK1oxaW0EoxsI9eWAuhz4jnvefLw7hl3tqcQWpNu3XqNREskHE4ac949ysMDRPMoK4Z8rfSYv1uKLQIjJst_7OS1zVJLAy9MYpa3iL226q7gIYMBTyDJri8zdz7u6WI4y_ZPlsv2trZ3OQ0-VRc5PHtU_8AlYRqNw4G2990p8ek0OM4G4dYjY-jt9c8aalo2U5nQ7Cg/https%3A%2F%2Fwww.simplesite.com%2F

当终端用户当前收到电子邮件时，点击重写的URL，他们重定向对Cisco Web安全代理并且看到：



Note:“无法生成站点预览”将显示根据原始URL或网站的HTML/encoding。 有CSS ， HTML面或者复杂转换的一个网站不能生成站点预览。

相关信息

- Cisco电子邮件安全工具终端用户指南
- 技术支持和文档 - Cisco Systems