Testen der URL-Umschreibung für Outbreak-Filter

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Nachrichtenänderungsoption für Outbreak-Filter (OF) für die URL-Umschreibung getestet wird.

Hintergrundinformationen

Wenn der Bedrohungsgrad der Nachricht den Grenzwert für Nachrichtenmodifizierung überschreitet, schreibt die Outbreak-Filterfunktion alle URLs in der Nachricht um, um den Benutzer an die Splash-Seite des Cisco Web Security-Proxys umzuleiten, wenn er auf eine dieser Links klickt. AsyncOS schreibt alle URLs in einer Nachricht zurück, mit Ausnahme derjenigen, die auf umgeleitete Domänen verweisen.

Die folgenden Optionen sind für das Umschreiben von URLs verfügbar:

- Nur für nicht signierte Nachrichten aktivieren. Diese Option ermöglicht AsyncOS das Umschreiben von URLs in nicht signierten Nachrichten, die den Grenzwert für die Nachrichtenänderung, jedoch keine signierten Nachrichten erfüllen oder überschreiten. Cisco empfiehlt, diese Einstellung für das Umschreiben von URLs zu verwenden. **Hinweis**: Die E-Mail-Security-Appliance kann URLs in einer von DomainKeys/DKIM signierten Nachricht umschreiben und die Signatur der Nachricht ungültig machen, wenn ein Server oder eine Appliance in Ihrem Netzwerk, mit Ausnahme der E-Mail-Security-Appliance, für die Überprüfung der DomainKeys/DKIM-Signatur zuständig ist. Die Appliance betrachtet eine signierte Nachricht, wenn sie mit S/MIME verschlüsselt ist oder eine S/MIME-Signatur enthält.
- Die E-Mail-Security-Appliance kann URLs in einer von DomainKeys/DKIM signierten Nachricht umschreiben und die Signatur der Nachricht ungültig machen, wenn ein Server oder eine Appliance in Ihrem Netzwerk, mit Ausnahme der E-Mail-Security-Appliance, für die Überprüfung der DomainKeys/DKIM-Signatur zuständig ist.Die Appliance betrachtet eine signierte Nachricht, wenn sie mit S/MIME verschlüsselt ist oder eine S/MIME-Signatur enthält.
- Aktivieren Sie diese Option für alle Nachrichten. Diese Option ermöglicht AsyncOS das Umschreiben von URLs in allen Nachrichten, die den Grenzwert für die Nachrichtenänderung erfüllen oder überschreiten, einschließlich signierter Nachrichten. Wenn AsyncOS eine signierte Nachricht ändert, wird die Signatur ungültig.

- Deaktivieren. Mit dieser Option wird die URL-Umschreibung für Outbreak-Filter deaktiviert.

Sie können eine Richtlinie ändern, um URLs zu bestimmten Domänen von der Änderung auszuschließen. Um Domänen zu umgehen, geben Sie die IPv4-Adresse, die IPv6-Adresse, den CIDR-Bereich, den Hostnamen, den partiellen Hostnamen oder die Domäne im Feld "Domain Scanning" umgehen ein. Trennen Sie mehrere Einträge durch Kommas.

Die Funktion zum Scannen von Domänen umgehen ähnelt der globalen Liste, die von der URL-Filterung verwendet wird, ist jedoch unabhängig davon. Weitere Informationen zu dieser Liste finden Sie unter "Creating Whitelists for URL Filtering" (Erstellen von Whitelists für URL-Filterung) im ESA-Benutzerhandbuch.

Testen der URL-Umschreibung für Outbreak-Filter

Es gibt zwei Möglichkeiten zum Testen von OF auf ESA.

Prüfung von Teil 1

Bringen Sie eine schädliche URL in den E-Mail-Text ein. Sichere Test-URL, die verwendet werden kann:

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

Beim Versenden sollten die Beispiele für E-Mail-Protokolle ähnlich wie die folgenden enthalten:

```
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
```

Beachten Sie, dass die E-Mail-Protokolle uns eine "umgeschriebene URL" anzeigen, die besagt, dass OF diese URL über den Cisco Web Security-Proxy neu geschrieben hat. Beachten Sie außerdem, dass die Nachricht möglicherweise in der Outbreak-Quarantäne gespeichert ist, wie in unserem Beispiel gezeigt.

Im Endergebnis wird der E-Mail-Text angezeigt, der folgende Informationen enthält:

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

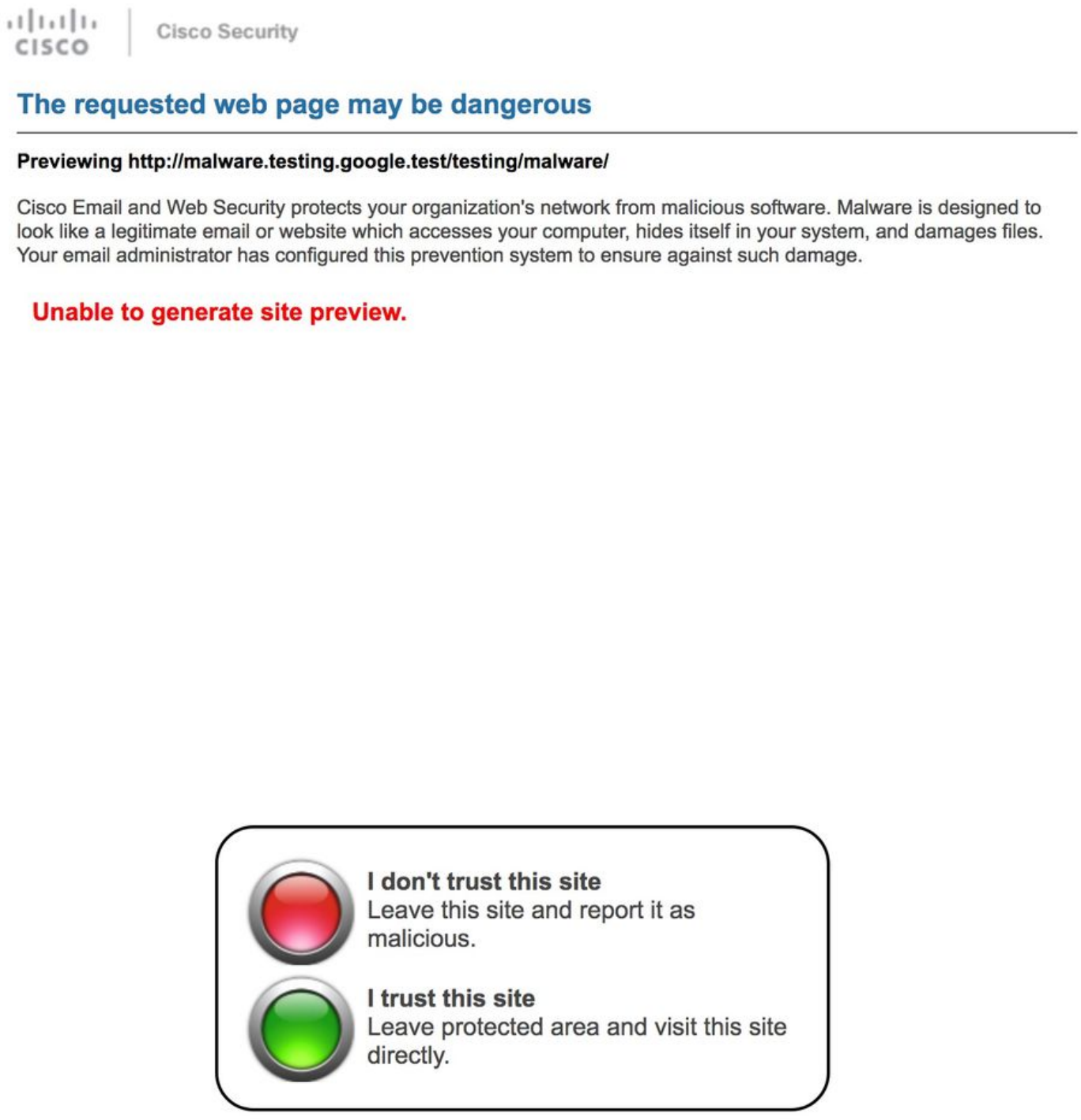
It may trick victims into clicking a link and downloading malware. Do not open suspicious links.

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-ZlcoYNPjkxBq2IUR1AG9u1b2w2mC_bYnT-XoeEWxQs_Mjd7NRBjTFRLNGzH7uii_o-QPPCFMKqGC85swJ8Y5Um7pG_f3qydi2Hk2r9lYV-gixFC9m-a6Q0HBSLYLNp4JIpxJy5Hc_8ieJRvzHAY9UjRy-Az6SEV2hvjsrwy03HbOm-f9sJDRbnrXclhNgk4gbpjtXWdkQGSxSsxaxdxkFy6yUAF605wSINVA6/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F

Wenn der Endbenutzer die E-Mail jetzt empfängt, klickt er auf die umgeschriebene URL, wird er an den Cisco Web Security-Proxy umgeleitet und wird angezeigt unter:



Hinweis: "Site Preview konnte nicht erstellt werden" wird basierend auf der HTML/Codierung

der ursprünglichen URL oder Website angezeigt. Eine Website mit CSS, HTML-Bereichen oder komplexem Rendering kann keine Seitenvorschau erstellen.

Prüfung von Teil 2

Die zweite Option besteht darin, Daten mit in den E-Mail-Text oder -Anhang einzufügen, um OF-Trigger zu erhalten.

Um Erfolg zu haben, gibt es zwei Optionen:

1. Erstellen Sie eine Datei (eine einfache Textdatei wird ausgeführt) mit dem Namen "hello.voftest" im Bereich von 25.000 bis 3.000 Byte, und fügen Sie diese Datei an Ihre Test-E-Mail an. Dies löst die Virus-Attachment-Regeln aus.
2. Platzieren Sie den folgenden 72-Byte-Testzeichentext (GTUBE, Generic Test for Unsolicited Bulk Email) in den Text einer E-Mail:

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

Dadurch werden OF und die Phishing-Regeln ausgelöst. Das Beispiel für Mail-Protokolle sollte ähnlich wie folgt sein:

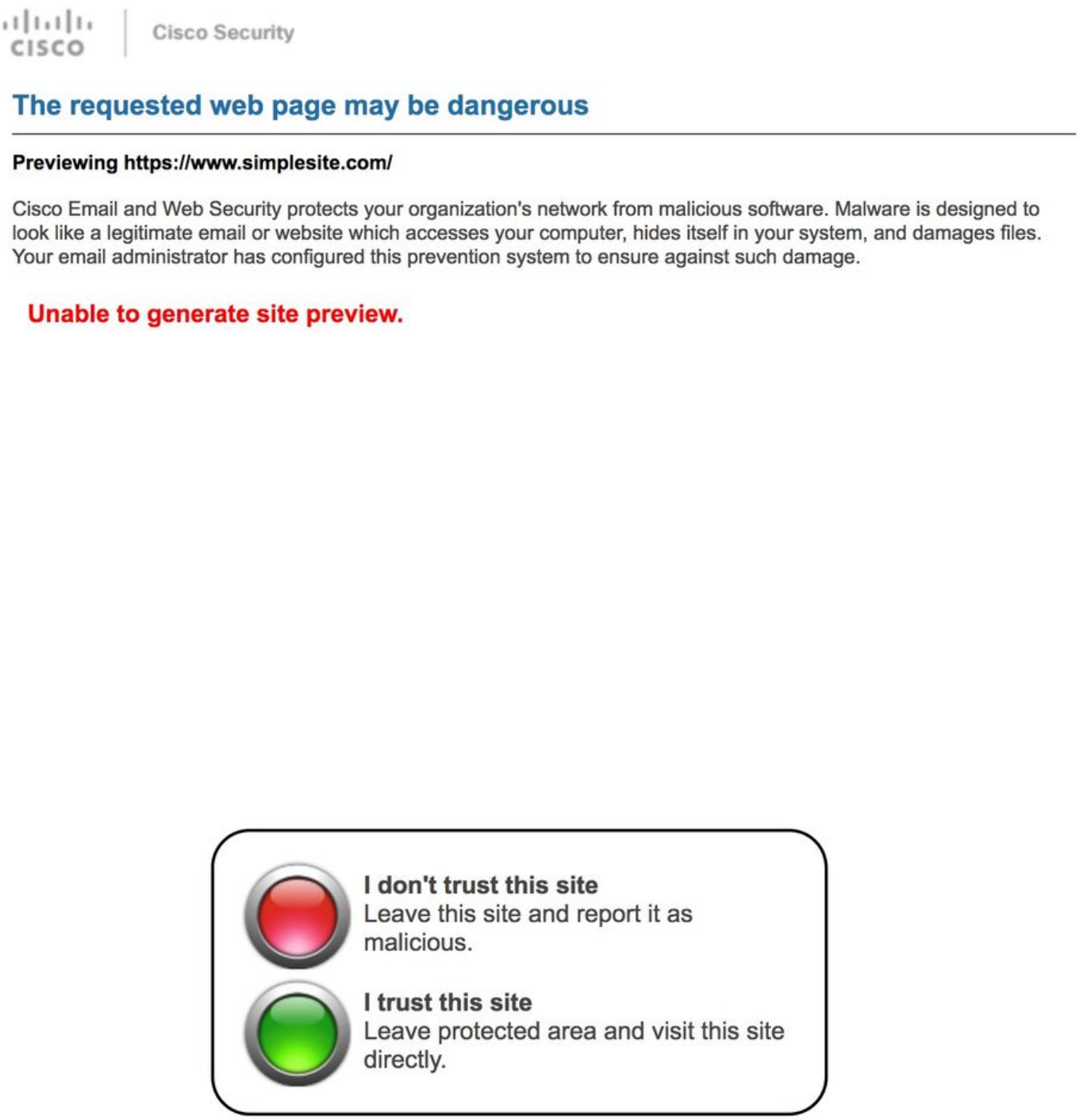
```
Tue Jul  3 09:44:12 2018 Info: MID 185880 Outbreak Filters: verdict positive
Tue Jul  3 09:44:12 2018 Info: MID 185880 Threat Level=5 Category=Phish Type=Phish
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten 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
```

Beachten Sie, dass die E-Mail-Protokolle uns eine "umgeschriebene URL" anzeigen, die besagt, dass OF diese URL über den Cisco Web Security-Proxy neu geschrieben hat. Beachten Sie außerdem, dass die Nachricht möglicherweise in der Outbreak-Quarantäne gespeichert ist, wie in unserem Beispiel gezeigt.

Im Endergebnis wird der E-Mail-Text angezeigt, der folgende Informationen enthält:

Wenn der Endbenutzer die E-Mail jetzt empfängt, klickt er auf die umgeschriebene URL, wird er

an den Cisco Web Security-Proxy umgeleitet und wird angezeigt unter:



Hinweis: "Site Preview konnte nicht erstellt werden" wird basierend auf der HTML/Codierung der ursprünglichen URL oder Website angezeigt. Eine Website mit CSS, HTML-Bereichen oder komplexem Rendering kann keine Seitenvorschau erstellen.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems