Verifica della riscrittura dell'URL del filtro epidemie

Sommario

Introduzione

In questo documento viene descritto come verificare l'opzione di modifica dei messaggi dei filtri epidemie (OF) per la riscrittura degli URL.

Premesse

Se il livello di rischio del messaggio supera la soglia di modifica del messaggio, la funzione Filtri epidemie riscrive tutti gli URL nel messaggio per reindirizzare l'utente alla pagina iniziale del proxy di Cisco Web Security, se fa clic su uno di essi. AsyncOS riscrive tutti gli URL all'interno di un messaggio ad eccezione di quelli che puntano ai domini ignorati.

Per la riscrittura degli URL sono disponibili le opzioni seguenti:

- Attiva solo per i messaggi non firmati. Questa opzione consente ad AsyncOS di riscrivere gli URL nei messaggi non firmati che soddisfano o superano la soglia di modifica dei messaggi, ma non firmati. Cisco consiglia di utilizzare questa impostazione per la riscrittura dell'URL. **Nota:** È possibile che gli URL di un messaggio firmato da DomainKeys/DKIM vengano riscritti e la firma del messaggio venga invalidata se la verifica della firma di DomainKeys/DKIM è effettuata da un server o da un accessorio della rete diverso da Email Security Appliance. L'accessorio considera un messaggio firmato se è crittografato tramite S/MIME o se contiene una firma S/MIME.
- Èpossibile che gli URL di un messaggio firmato da DomainKeys/DKIM vengano riscritti e la firma del messaggio venga invalidata se la verifica della firma di DomainKeys/DKIM è effettuata da un server o da un accessorio della rete diverso da Email Security Appliance.L'accessorio considera un messaggio firmato se è crittografato tramite S/MIME o se contiene una firma S/MIME.
- Attiva per tutti i messaggi. Questa opzione consente ad AsyncOS di riscrivere gli URL in tutti i messaggi che soddisfano o superano la soglia di modifica dei messaggi, inclusi quelli firmati. Se AsyncOS modifica un messaggio firmato, la firma non sarà più valida.
- Disattiva. Questa opzione disabilita la riscrittura degli URL per i filtri epidemie.

Èpossibile modificare un criterio per escludere dalla modifica gli URL di determinati domini. Per ignorare i domini, immettere l'indirizzo IPv4, l'indirizzo IPv6, l'intervallo CIDR, il nome host, il nome host parziale o il dominio nel campo Ignora analisi dominio. Separare più voci utilizzando le

virgole.

La funzione Ignora analisi dominio è simile all'elenco indirizzi globale utilizzato dal filtro URL, ma indipendente da esso. Per ulteriori informazioni su tale elenco, vedere "Creating Whitelists for URL Filtering" nel manuale ESA User Guide.

Verifica della riscrittura dell'URL del filtro epidemie

Ci sono due opzioni per testare OF sull'ESA.

Prova della prima parte

Includere un URL dannoso nel corpo dell'e-mail. URL di test sicuro utilizzabile:

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

Quando vengono inviati, i log di esempio di posta devono contenere:

```
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
```

I log di posta indicano che l'URL è stato riscritto da OF tramite il proxy Cisco Web Security. Tenere inoltre presente che il messaggio potrebbe essere nella quarantena per l'epidemia, come illustrato nell'esempio.

Il corpo dell'e-mail consegnato al risultato finale mostrerà quanto segue:

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.

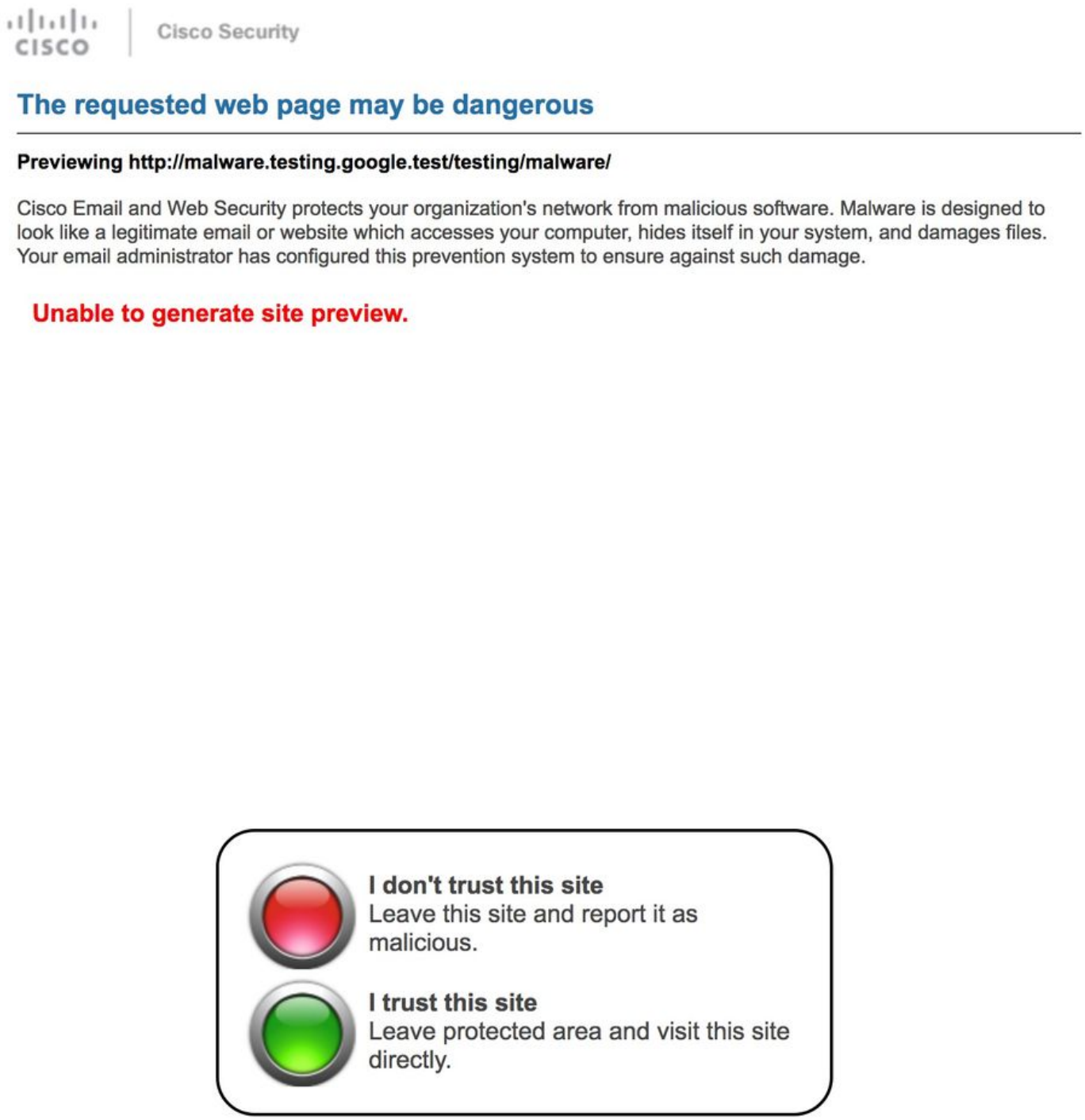
If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

Here.

http://secure-web.cisco.com/1ZzJhYfgzugtou3v__nw-VbytKC7kXMoWpj93VzB1wL2PuGPyCMDQ_DH4k4uYLGEfKi0U-D_lOtZp4TnwCkXE8iZ7MuiouY6PUDX5h_eluxNeebE3dVdoBU6EvlDJSPBvfL21qdeZ52HQ74ahop81kBXttP-ZlcoYNPjkxBq2lUR1AG9u1b2w2mC_bYnT-XoeEWxQs_Mjd7NRBjTFRLNGzH7uii_o-QPPCFMKqGC85swJ8Y5Um7pG_f3qydi2Hk2r9lYV-gixFC9m-a6Q0HBSLYLNp4JIpxJy5Hc_8ieJRvzHAY9UjRy-Az6SEV2hvjsrwy03HbOm-f9sJDRbnrXclhNgk4gbpjtXWdkQGSxSsxaxdxkFy6yUAF605wSlNVA6/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F

Quando l'utente finale riceve l'e-mail, fa clic sull'URL riscritto e viene reindirizzato al proxy Cisco

Web Security che visualizza:



Nota: Viene visualizzato il messaggio "Unable to generate site preview" (Impossibile generare l'anteprima del sito) in base alla codifica/HTML dell'URL o del sito Web originale. Un sito Web con fogli di stile CSS, riquadri HTML o rendering complesso non sarà in grado di generare un'anteprima del sito.

Prova della parte seconda

La seconda opzione consiste nell'includere i dati con-nel corpo o nell'allegato dell'e-mail in modo da avere il trigger OF.

Per avere successo, è necessario procedere in due modi:

1. Creare un file (il file di testo semplice funzionerà) con il nome "hello.voftest" di dimensioni comprese tra 25000 e 30000 byte e allegare il file al messaggio di prova. Verranno attivate le regole di collegamento dei virus.
2. Inserire il seguente testo di stringa di test GTUBE ("Generic Test for Unsolicited Bulk Email") da 72 byte nel corpo di un messaggio di posta elettronica:

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

In questo modo verranno attivate le regole di codifica e di phishing. L'esempio dei log di posta deve contenere:

```
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
```

I log di posta indicano che l'URL è stato riscritto da OF tramite il proxy Cisco Web Security. Tenere inoltre presente che il messaggio potrebbe essere nella quarantena per l'epidemia, come illustrato nell'esempio.

Il corpo dell'e-mail consegnato al risultato finale mostrerà quanto segue:

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

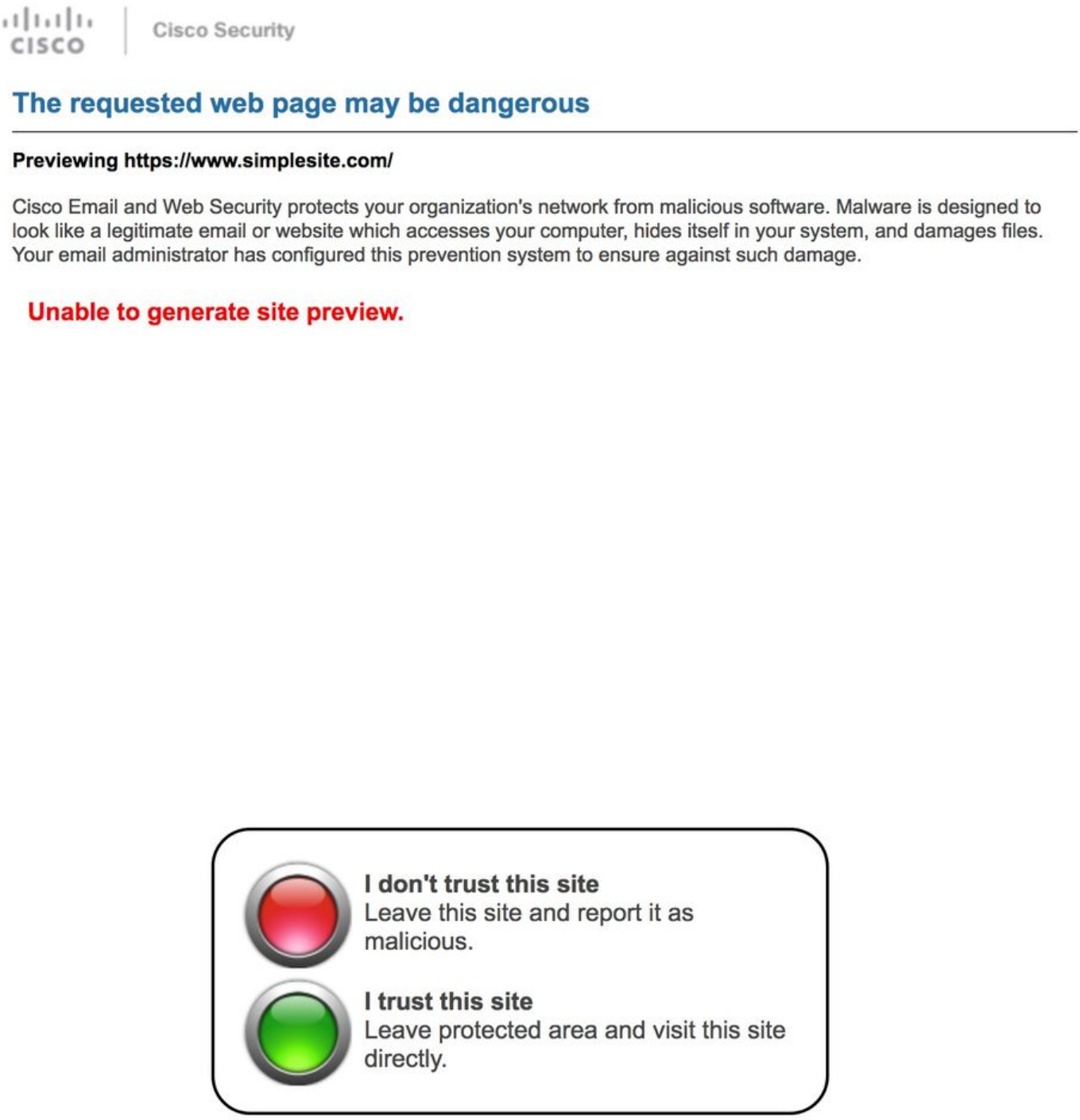
It may pose as a legitimate company, tricking victims into revealing personal information.

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_XwacJhK0Y5fYXfiQJ9sSgledHbUH3ssTG4qJszR9zf1dMRpEPjq0U11EVsDE2NF3nKRlWKrkCtAe1GNtTi5TGeYK9PZ8-3l1zXVm2nrQmGj2PQH4yylSkPJ6-SgJHyrTKiOpa6JgbKMc1pEMumW6Zyoa4DyjrrronTquLumPRnqvmK1oxaW0EoxsJ9eWAuhz4jnvefLw7hl3tqcQWpNu3XqNREskHE4ac949ysMDRPMoK4Z8rfSYv1uKLQIjJst_7OS1zVJLAy9MYpa3iL226q7gIYMBTyDJri8zdz7u6WI4y_ZPlsv2trZ3OQ0-VRc5PHtU_8AlYRqNw4G2990p8ek0OM4G4dYjY-jt9c8aaIo2USnQ7Cg/https%3A%2F%2Fwww.simplesite.com%2F

Quando l'utente finale riceve l'e-mail, fa clic sull'URL riscritto e viene reindirizzato al proxy Cisco Web Security che visualizza:



Nota: Viene visualizzato il messaggio "Unable to generate site preview" (Impossibile generare l'anteprima del sito) in base alla codifica/HTML dell'URL o del sito Web originale. Un sito Web con fogli di stile CSS, riquadri HTML o rendering complesso non sarà in grado di generare un'anteprima del sito.

Informazioni correlate

- Guide per l'utente finale di Cisco Email Security Appliance
- Documentazione e supporto tecnico – Cisco Systems