External Enumeration and Exploitation of Email and Web Security Solutions

Ben Williams
About this talk

• Background
• Enumerating web filtering solutions
• Enumerating email filtering solutions
• Bypassing filters
Previous presentations (Hacking appliances)

• Blackhat EU 2013 – Hacking Security Appliances
  • http://www.youtube.com/watch?v=rrjSEkSwwOQ

• Blackhat Webcast July 2013 – Hacking Security Appliances

• BlackHat EU 2012 - Exploiting Security Gateways via their Web UIs
  • http://www.youtube.com/watch?v=XfZS1iZ2PpY
Previously (Hacking appliances/gateways)

• Email/Web filtering
  • Baracuda, Symantec, McAfee, Trend Micro, Sophos, Proofpoint
• Firewall, Gateway, Web-filters
  • Pfsense, Untangle, ClearOS, Websense, Citrix
Research this time - Enumeration

• Enumerating and bypassing products and solutions

• Low severity issues which are systemic and persistent

• Using functionality which is there by design
For an attacker: Wouldn’t it be good if ?...

• Vulnerability scanning
  • Hidden vulnerable products could be detected externally

• Phishing and client-side attacks
  • Clear picture of defences before targeting real users

• Email or Web filter policy, or product capability review
  • Automated and remote testing
MailFEET and WebFEET usage to date

• Detailed analysis during NCC Group customer engagements

• Targeting specific products in a test environment
  • To identify product capability and weaknesses

• Limited payloads and tests of a wide variety of domains
  • To improve the tool and produce some stats
WebFEET

- Web Filter External Enumeration Tool (WebFEET)
- Drive-by web-proxy and policy enumeration with JavaScript

- Main components (HTML, JavaScript, PHP)
  - Enumerates proxies
  - Simulates download of files
  - Uploads a report

- For audits and reconnaissance
Header Modification Enumeration

Attacker’s application server
Web security proxy
Web browser
Web filter IP address/hostname/version

HTTP/1.1 200 OK
Date: Thu, 12 Jun 2014 13:26:33 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 13 Mar 2014 20:08:22 GMT
ETag: "1c0a6f-4ab-4f48283e160cb"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 1195

Content-Type: text/html
X-Cache: MISS from ipfire.localdomain
X-Cache-Lookup: MISS from ipfire.localdomain:800
Connection: keep-alive
Header Modification Enumeration

Attacker’s application server

Web security proxy

Web browser
Web filter IP address/hostname/version

- Interesting headers
  - Via
  - X-Cache
  - X-Cache-Lookup
  - Other customer X-headers
  - Subtle modifications
Collected Headers Examples

X-Cache-Lookup: MISS from wp-xxxxxxx.xxx.xx.xx:3128
X-Cache: MISS from 10.xx.xx.xx

Via: 1.0 10.xx.xx.xx (McAfee Web Gateway 7.2.0.1.0.13253)
Via: 1.0 barracuda.xxxxxxxxxxxxx.xxx.xx.xx:8080 (http_scan/4.0.2.6.19)
Via: 1.1 xxxxproxy02.xx.xxxxxx.com:3128 (Cisco-IronPort-WSA/7.5.2-118)
Via: 1.1 backup.xxxx.xxx.xx:3128 (squid/2.7.STABLE9)

X-Cache-Lookup: MISS from xxxxxx:53128, MISS from pfsense:3128

X-WebMarshal-RequestID: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXX
File Download Policy Enumeration

Attacker’s application server

Web security proxy

Web browser
Blocking Request

Attacker's application server

Web security proxy

Web browser
Blocking Response

Attacker’s application server

Web security proxy

Web browser
A Redirect Response

Attacker's application server

Web security proxy

Web browser
This Page Cannot Be Displayed

Based on your organization's access policies, this web site (http://[redacted]/WebFEETstats/payloads/eicar.com) has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware threat EICAR-AV-Test in the category Trojan Horse has been found on this site.

If you have questions, please contact your corporate network administrator and provide the codes shown below.

Date: Mon, 21 Jul 2014 14:59:37 EDT
Username: [redacted]
Source IP: [redacted]
URL: GET http://[redacted]/WebFEETstats/payloads/eicar.com
Category: Uncategorized URLs
Reason: BLOCK-MALWARE
Notification: MALWARE_SPECIFIC
Fundamental Issue With Block-pages

- Attacker’s application server
- Web security proxy
- Web browser
Trend Micro OfficeScan Event

URL Blocked

The URL that you are attempting to access is a potential security risk. Trend Micro OfficeScan has blocked this URL in keeping with the network security policy.

URL: http://[redacted]WebFEETstats/payloads/eicar.com
Risk Level: Risk level cannot be displayed because active scripting is disabled.
Details:

Blocked by Web Reputation, Trend Micro OfficeScan 10.6 SP3, Copyright © 1998-2013, Trend Micro Incorporated. All rights reserved.
Malicious Content Blocked

*Location:*  
WebFEETstats/payloads/eicar.com

The requested location contains malicious content, identified as **EICAR-AV-Test** and was blocked from downloading.

*Message generated:* 3:38:23 PM
Example WebFEET Report

• Demo: Show a WebFEET reports
HTTP vs. HTTPS

• An effective HTTP policy can be irrelevant – because HTTPS interception and filtering are rare

• Even where HTTPS interception is present, there are usually plenty of policy bypasses
HTTPS Inspection

Internet

Normal encryption

CA

Onsite web security solution

Spoofed encryption

Web browser

Twitter: @insidetrust
@nccgroupinfosec
# WebFEET HTTP vs. HTTPS

**Basic Download Block Tests**
Simple threats are tested here, to see if they are allowed, dropped, redirected, or result in a block-page.

<table>
<thead>
<tr>
<th>Test File</th>
<th>Size</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>EICAR basic test</td>
<td>68 bytes</td>
<td>Downloaded: Size = 68</td>
</tr>
<tr>
<td>A standard Windows exe</td>
<td>0.2 MB</td>
<td>Downloaded: Size = 187513</td>
</tr>
<tr>
<td>A file with profanity</td>
<td>39 bytes</td>
<td>Downloaded: Size = 39</td>
</tr>
<tr>
<td>An unlocked breakout shell</td>
<td>0.3 MB</td>
<td>Downloaded: Size = 342854</td>
</tr>
<tr>
<td>A Password dumping tool</td>
<td>0.5 MB</td>
<td>Downloaded: Size = 548715</td>
</tr>
<tr>
<td>EICAR in a zip</td>
<td>184 bytes</td>
<td>Downloaded: Size = 184</td>
</tr>
<tr>
<td>Some VBS script</td>
<td>22 bytes</td>
<td>Downloaded: Size = 22</td>
</tr>
<tr>
<td>A batch file</td>
<td>11 bytes</td>
<td>Downloaded: Size = 11</td>
</tr>
</tbody>
</table>
# HTTPS Certificate Validation Issues

**HTTPS Certificate Handling Enumeration (Correct Certificates)**
Some of these are on non-standard ports, so some proxies may block these because of that (failure to load suggests filtering of non-standard ports, and may make some of the tests below invalid).

<table>
<thead>
<tr>
<th>Category</th>
<th>Test Website</th>
<th>Image</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Certificate</td>
<td><a href="http://www.google.com">www.google.com</a> (HTTPS)</td>
<td><img src="image" alt="8" /></td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Valid Certificate</td>
<td>testssl-valid-r2i1.disig.sk:2444</td>
<td><img src="image" alt="✔" /></td>
<td>Not Blocked</td>
</tr>
</tbody>
</table>

**HTTPS Certificate Handling Enumeration (Incorrect Certificates, these should not load)**
If these resources load, this may be a result of an SSL break at the proxy (SSL MitM) in order to do HTTPS data inspection. This may also be causing external locations with invalid certificates to appear valid to the internal user. Some of these are on non-standard ports, so some proxies may block these anyway (false negative for invalid certs).

<table>
<thead>
<tr>
<th>Category</th>
<th>Test Website</th>
<th>Image</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expired Certificate</td>
<td>testssl-expire-r2i1.disig.sk:2445</td>
<td><img src="image" alt="✗" /></td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Revoked Certificate</td>
<td>testssl-revoked-r2i1.disig.sk:2446</td>
<td><img src="image" alt="✗" /></td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Category</td>
<td>Test Website</td>
<td>Image</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td>-------</td>
<td>-----------</td>
</tr>
<tr>
<td>Adult Material</td>
<td><a href="http://www.porn.com">www.porn.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Adult Material</td>
<td><a href="http://www.redtube.com">www.redtube.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Drugs</td>
<td>ilovesmokingweed.com</td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Drugs</td>
<td>marijuana.com</td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Gambling</td>
<td><a href="http://www.betfred.com">www.betfred.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Gambling</td>
<td><a href="http://www.ladbrokes.com">www.ladbrokes.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Hacking</td>
<td><a href="http://www.exploit-db.com">www.exploit-db.com</a></td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Hacking</td>
<td>hackers.org</td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Job Sites</td>
<td><a href="http://www.totaljobs.com">www.totaljobs.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Job Sites</td>
<td><a href="http://www.newjobs.com">www.newjobs.com</a></td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Online Email</td>
<td>mail.google.com</td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Online Email</td>
<td><a href="http://www.hotmail.com">www.hotmail.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Online Pharmacy</td>
<td><a href="http://www.chemist-4-u.com">www.chemist-4-u.com</a></td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Online Pharmacy</td>
<td><a href="http://www.pharmacy2u.co.uk">www.pharmacy2u.co.uk</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Personal Network Storage and Backup</td>
<td><a href="http://www.dropbox.com">www.dropbox.com</a></td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Personal Network Storage and Backup</td>
<td>pastebin.com</td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
<tr>
<td>Racism and Hate</td>
<td><a href="http://www.chimpout.com">www.chimpout.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Racism and Hate</td>
<td><a href="http://www.stormfront.org">www.stormfront.org</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Tasteless</td>
<td><a href="http://www.4chan.org">www.4chan.org</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Tasteless</td>
<td><a href="http://www.stupidness.com">www.stupidness.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Violence</td>
<td>rotten.com</td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Violence</td>
<td><a href="http://www.livemake.com">www.livemake.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Weapons</td>
<td><a href="http://www.guns.com">www.guns.com</a></td>
<td>🚫</td>
<td>Blocked</td>
</tr>
<tr>
<td>Weapons</td>
<td><a href="http://www.bulkammo.com">www.bulkammo.com</a></td>
<td>🏝️</td>
<td>Not Blocked</td>
</tr>
</tbody>
</table>
So For Web Filtering, I Know:

- What products you are using
  - Sometimes exact versions
- What your policy is for a wide variety of file downloads
- Whether you can detect threats in HTTPS
- How effective your URL filtering is and what categories you block

- All in under 10 seconds – no exploits required
  - Relatively transparent to the end user, but may be logs or alerts on the proxy
MailFEET

• Mail Filter External Enumeration Tool (MailFEET)
• Sends, receives test emails and parses responses

• Main components (python/sqlite)
  • Email sender/logger
  • Email bounce message collector/logger
  • Reporting tool

• For audits and reconnaissance
The following message to < undisclosed > was undeliverable. The reason for the problem:
5.0.0 - Message bounced by administrator

Final-Recipient: rfc822: undisclosed
Action: failed
Status: 5.0.0 (permanent failure)
Diagnostic-Code: smtp; 5.x.0 - Message bounced by administrator (delivery attempts: 0)
Subject: Test message - please ignore (script) 7d34aa0d
Product disclosure examples

• X-IronPort-AV: E=Sophos;i="4.93,874,1378875600";
• MailMarshal (v7,1,0,4874)
• X-Proofpoint-Spam-Details: rule=notspam policy=default score=41 spamscore=0 ndrscore=41 suspectscore=3 adjustscore=0 phishscore=0 adultscore=0 bulkscore=0 classifier=spam adjust=0 reason=mlx scanccount=1 engine=7.0.1-13052400000 definitions=main-1308150307
Fortune 500 non-existent recipient acceptance

- Didn’t accept: 58%
- Accepted: 31%
- Accepted and replied: 11%
Enumerating products in use

• Create signatures for:
  • X-Headers
  • Received headers
  • Message body/attachments
  • Hostnames
Figure 1. Magic Quadrant for Secure Email Gateway

challengers

leaders

Barracuda Networks
Sophos

Trend Micro

Cisco
Proofpoint
Symantec

Microsoft

McAfee

Mimecast
Websense

Clearswift
SilverSky

Fortinet

Dell

Visionaries

Niche players

Completeness of Vision

As of July 2013

Source: Gartner (July 2013)
Email filter appliance product type by vendor (enumeration via bounce message analysis)
Email filtering managed service vs. product for 152 leading organisations

- Manage service: 47%
- Just product (mainly appliances): 33%
- Both service and product: 20%
Policy enumeration

• Send 4 different test messages, to each MX record, of 152 domains – you get 2,500 responses – what happened?
  • Simple text message (no threat)
  • Exe embedded in a Word (2010) document
  • Password protected Excel spreadsheet
  • VBS in Word (2003) document
Types of message you can get back

• Delivery Service Notifications (DSN)
  • Non-delivery report (NDR) “550: Recipient does not exist”
  • Policy block informational messages
  • Message quarantined
  • Message corrupt (could not be processed)
  • Message delayed

• Out of office messages
  • Contain useful user information
Classic disclosure ("block" message)

“A message or attachment you have sent to <Company name> has been filtered. Please use a different file format or place your attachment in a password protected ZIP file and resend the message.”
Message modification examples

Symantec Mail Security replaced exe-in-word-2010.docx with this text message. The original file contained a filtering violation and was quarantined.

Rule: 'Blocked Files'
Context: '[untitled]' 
Disallow due to format

See your system administrator for further information.

Copyright © 1993-2013 McAfee, Inc. All Rights Reserved.
http://www.mcafee.com
Need to quickly classify bounces

• Which are bounces from the mail-server?
  • Which have the original message?
  • Which have the original attachment?
• Which are “block notification” messages?
• Which are “other” types?

• Criteria
  • Checksum original attachment, message size, number of received headers, X-headers, structure, attachments, specific text strings
Basic stats of what gets through

- Some good delivery results with my limited payload sets
- Plain message (no threat): 94.1%
- Exe embedded in Word 2007: 62.1%
- Password protected XLS: 96.1%
- VBS embedded in Word 2003: 73.9%

Small four message test set:

- Message with no threat: 90.0%
- Exe in Word 2010: 60.0%
- Passworded Excel: 100.0%
- VBS in Word 2003: 70.0%
Policy enumeration for NCC clients

• Demo: Show example report

• Demo: Show example document with payload
So For Email Filtering, I Know:

• What products and services you are using
  • Often with exact versions

• What your policy is for a wide variety of file attachments

• Typically between 5 minutes to 1 hour for 50 attachments
  • Multiple MX records and multiple message paths
  • Often transparent to the end user, but may messages quarantined on email filter
Attacks which work

• HTTPS for the Win!

• Hidden payloads requiring “Deep content analysis”
  • Exes and scripts in Word Doc, PowerPoint, Excel etc.
  • Exe and scripts in Zips
  • PowerShell in HTA files or Document macros
  • Multiple layers: Exe in Zip in Documents.
  • Payloads in password protected documents and archives
  • 1000s of potential tests
Summary

• External attackers can enumerate products and policy

• Policies are generally weak
  • No 0-Day required
  • Encryption is the attacker’s friend
  • Embedded threats were rarely detected
Resources

• Updated presentation slides

• Whitepaper on web enumeration
  • Whitepaper on email enumeration

• WebFEET tool
• MailFEET tool
UK Offices
Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

North American Offices
San Francisco
Atlanta
New York
Seattle

Australian Offices
Sydney

European Offices
Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland