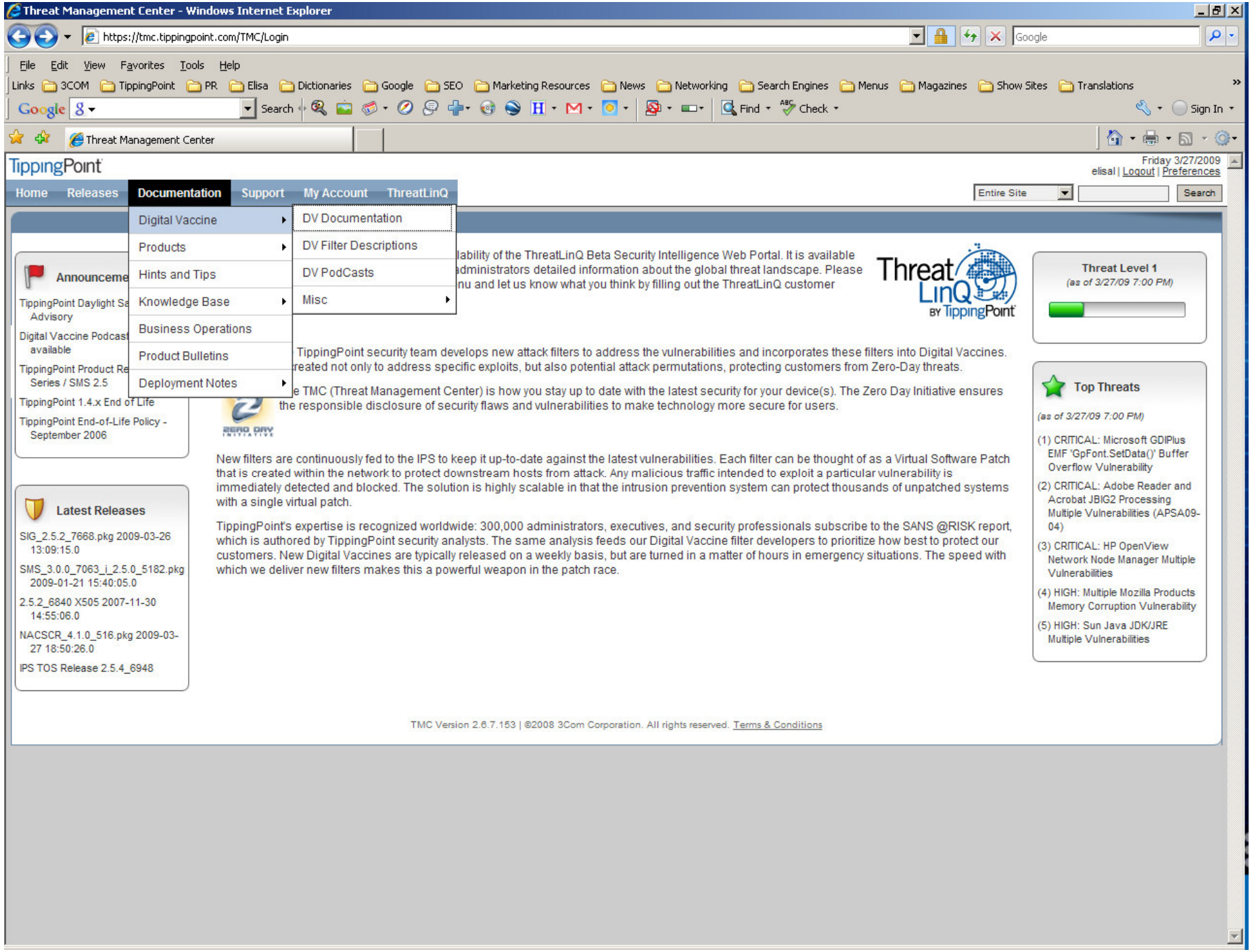
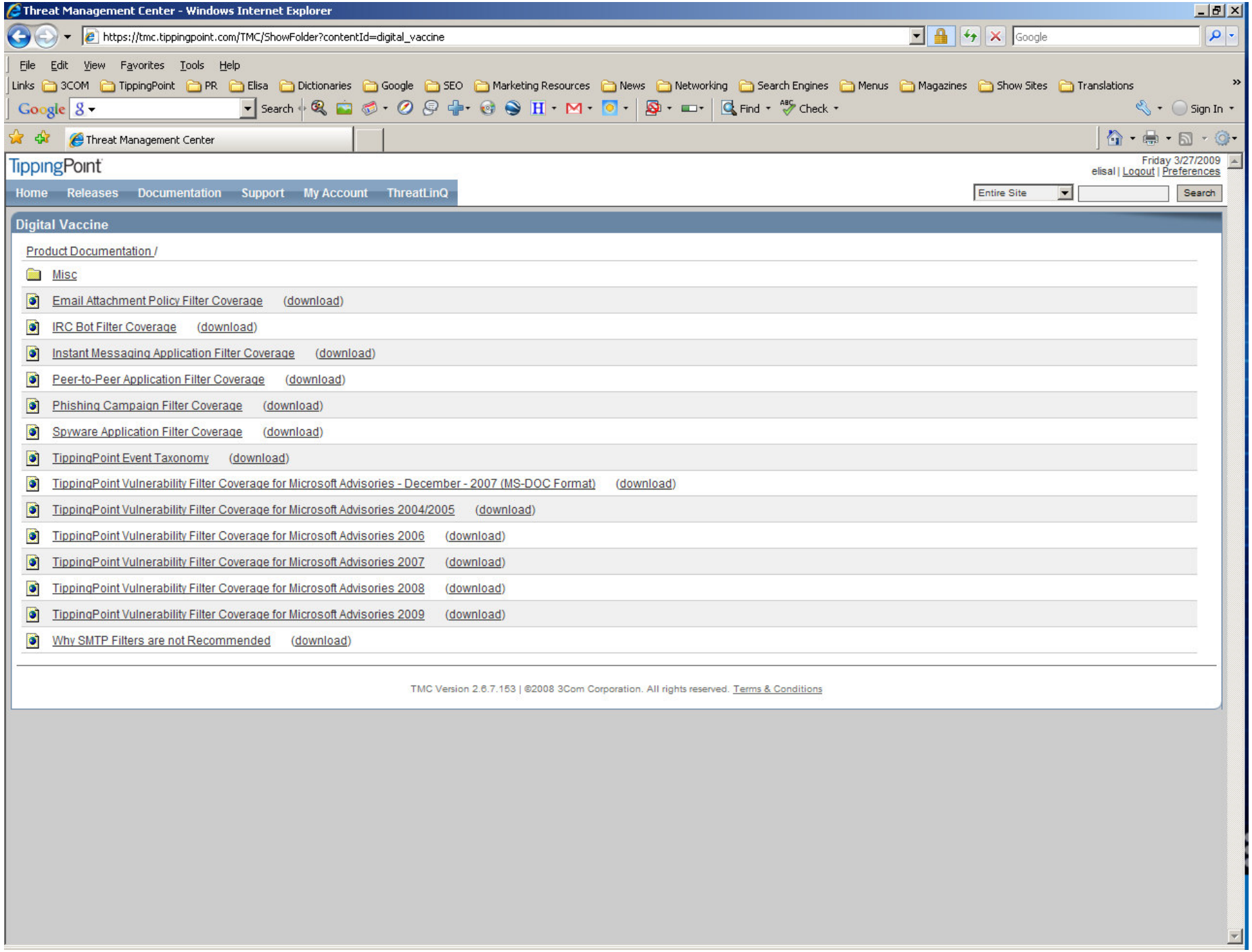
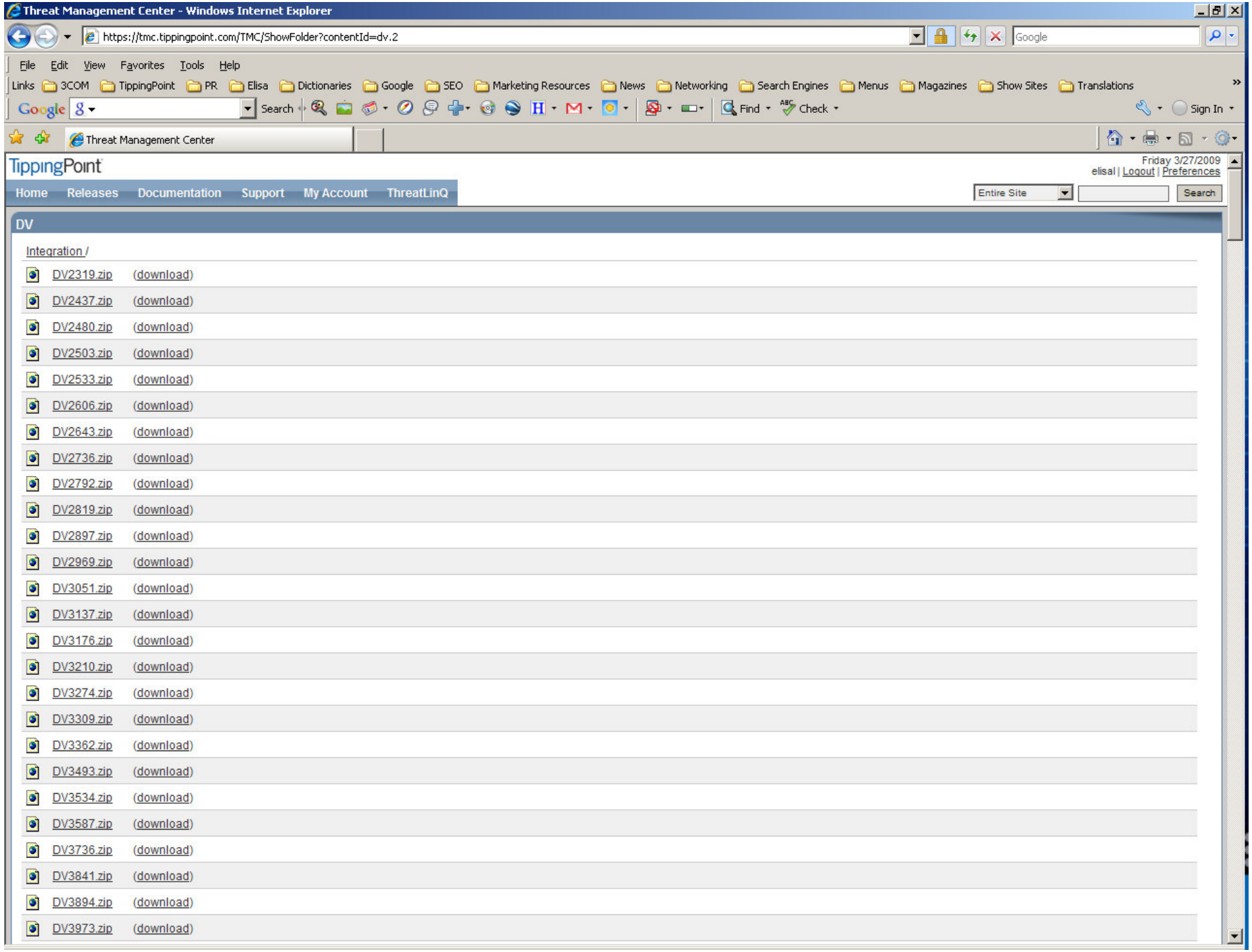
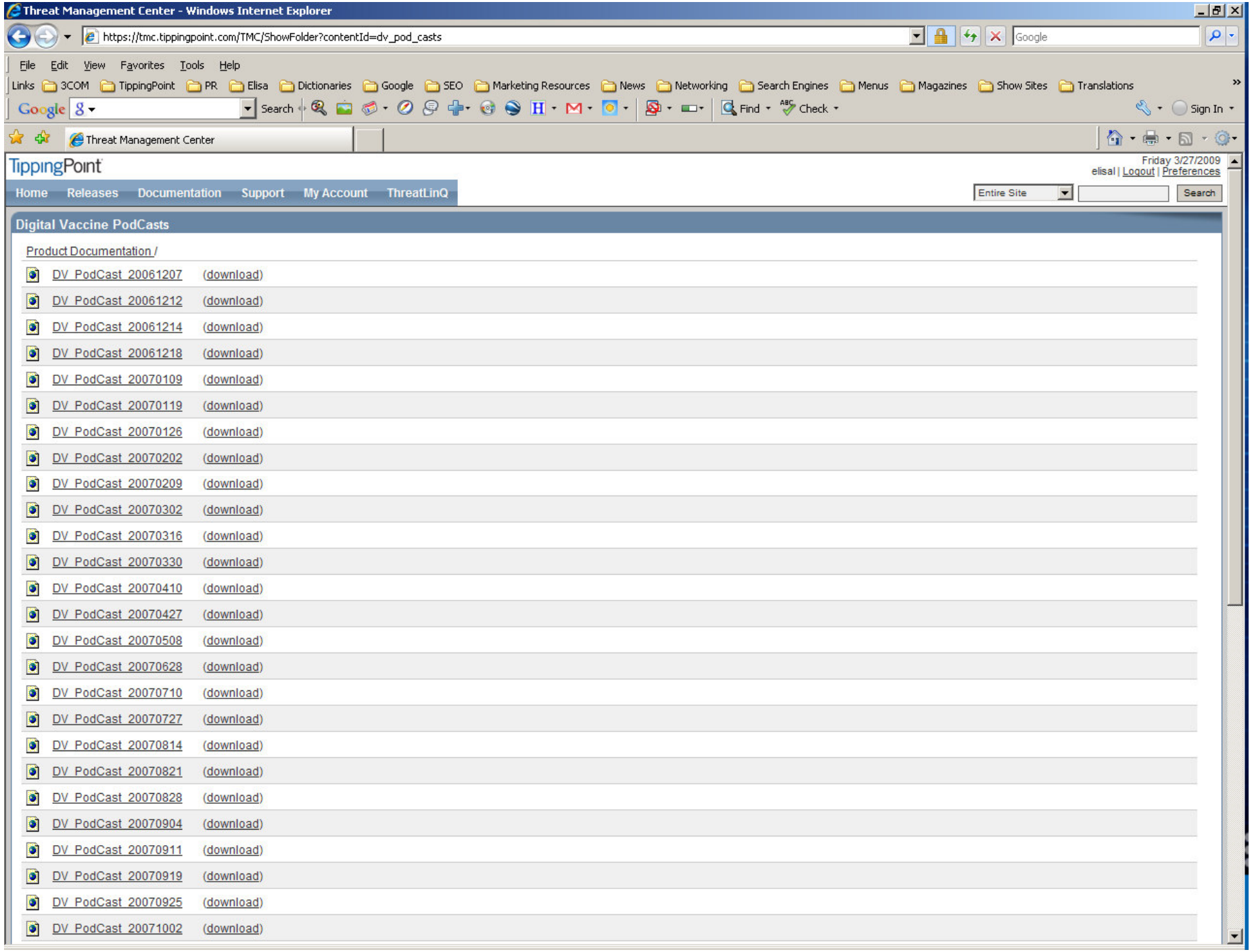
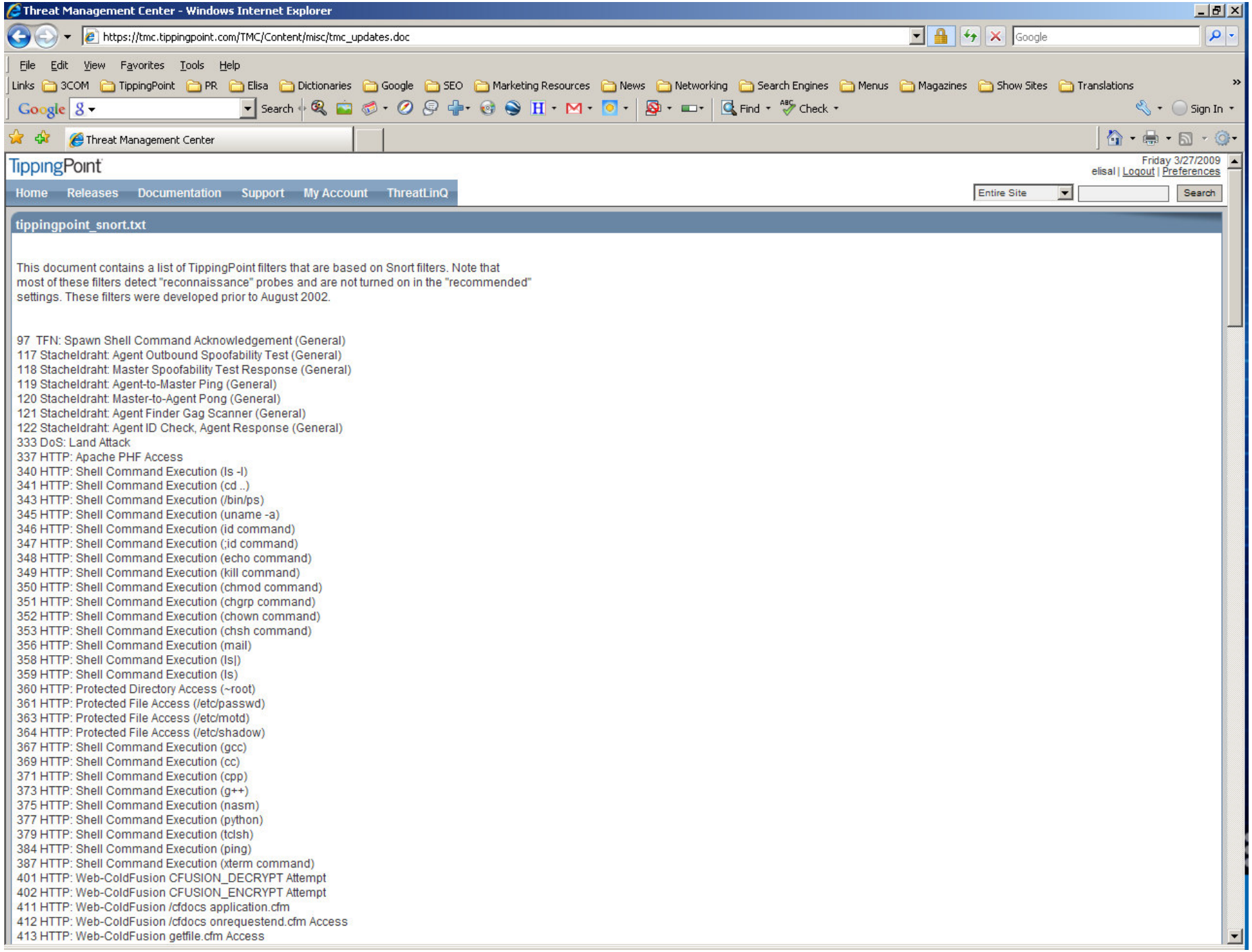

Threat Management Center - Windows Internet Explorer
https://tmc.tippingpoint.com/TMC/Login
Google
File Edit View Favorites Tools Help
Links 3COM TippingPoint PR Elisa Dictionaries Google SEO Marketing Resources News Networking Search Engines Menus Magazines Show Sites Translations
Google Search Find Check Sign In
Threat Management Center
TippingPoint
Friday 3/27/2009
elisal | Logout | Preferences
Home Releases Documentation Support My Account ThreatLinQ
Entire Site Search
Digital Vaccine
Products
Hints and Tips
Knowledge Base
Business Operations
Product Bulletins
Deployment Notes
DV Documentation
DV Filter Descriptions
DV PodCasts
Misc
Announceme
TippingPoint Daylight Sa Advisory
Digital Vaccine Podcast available
TippingPoint Product Re Series / SMS 2.5
TippingPoint 1.4.x End of Life
TippingPoint End-of-Life Policy - September 2006
Latest Releases
SIG_2.5.2_7668.pkg 2009-03-26 13:09:15.0
SMS_3.0.0_7063_i_2.5.0_5182.pkg 2009-01-21 15:40:05.0
2.5.2_6840 X505 2007-11-30 14:55:06.0
NACSCR_4.1.0_516.pkg 2009-03-27 18:50:26.0
IPS TOS Release 2.5.4_6948
lability of the ThreatLinQ Beta Security Intelligence Web Portal. It is available
administrators detailed information about the global threat landscape. Please
nu and let us know what you think by filling out the ThreatLinQ customer
ThreatLinQ BY TippingPoint
TippingPoint security team develops new attack filters to address the vulnerabilities and incorporates these filters into Digital Vaccines.
reated not only to address specific exploits, but also potential attack permutations, protecting customers from Zero-Day threats.
e TMC (Threat Management Center) is how you stay up to date with the latest security for your device(s). The Zero Day Initiative ensures the responsible disclosure of security flaws and vulnerabilities to make technology more secure for users.
New filters are continuously fed to the IPS to keep it up-to-date against the latest vulnerabilities. Each filter can be thought of as a Virtual Software Patch that is created within the network to protect downstream hosts from attack. Any malicious traffic intended to exploit a particular vulnerability is immediately detected and blocked. The solution is highly scalable in that the intrusion prevention system can protect thousands of unpatched systems with a single virtual patch.
TippingPoint's expertise is recognized worldwide: 300,000 administrators, executives, and security professionals subscribe to the SANS @RISK report, which is authored by TippingPoint security analysts. The same analysis feeds our Digital Vaccine filter developers to prioritize how best to protect our customers. New Digital Vaccines are typically released on a weekly basis, but are turned in a matter of hours in emergency situations. The speed with which we deliver new filters makes this a powerful weapon in the patch race.
Threat Level 1
(as of 3/27/09 7:00 PM)
Top Threats
(as of 3/27/09 7:00 PM)
(1) CRITICAL: Microsoft GDIPlus EMF 'GpFont.SetData()' Buffer Overflow Vulnerability
(2) CRITICAL: Adobe Reader and Acrobat JBIG2 Processing Multiple Vulnerabilities (APSA09-04)
(3) CRITICAL: HP OpenView Network Node Manager Multiple Vulnerabilities
(4) HIGH: Multiple Mozilla Products Memory Corruption Vulnerability
(5) HIGH: Sun Java JDK/JRE Multiple Vulnerabilities
TMC Version 2.6.7.153 | ©2008 3Com Corporation. All rights reserved. Terms & Conditions


Threat Management Center - Windows Internet Explorer
https://tmc.tippingpoint.com/TMC/ShowFolder?contentId=digital_vaccine
Google
File Edit View Favorites Tools Help
Links 3COM TippingPoint PR Elisa Dictionaries Google SEO Marketing Resources News Networking Search Engines Menus Magazines Show Sites Translations
Search Find Check Sign In
Threat Management Center
TippingPoint
Friday 3/27/2009
elisal | Logout | Preferences
Home Releases Documentation Support My Account ThreatLinQ
Entire Site
Search
Digital Vaccine
Product Documentation /
Misc
Email Attachment Policy Filter Coverage (download)
IRC Bot Filter Coverage (download)
Instant Messaging Application Filter Coverage (download)
Peer-to-Peer Application Filter Coverage (download)
Phishing Campaign Filter Coverage (download)
Spyware Application Filter Coverage (download)
TippingPoint Event Taxonomy (download)
TippingPoint Vulnerability Filter Coverage for Microsoft Advisories - December - 2007 (MS-DOC Format) (download)
TippingPoint Vulnerability Filter Coverage for Microsoft Advisories 2004/2005 (download)
TippingPoint Vulnerability Filter Coverage for Microsoft Advisories 2006 (download)
TippingPoint Vulnerability Filter Coverage for Microsoft Advisories 2007 (download)
TippingPoint Vulnerability Filter Coverage for Microsoft Advisories 2008 (download)
TippingPoint Vulnerability Filter Coverage for Microsoft Advisories 2009 (download)
Why SMTP Filters are not Recommended (download)
TMC Version 2.6.7.153 | ©2008 3Com Corporation. All rights reserved. Terms & Conditions


Threat Management Center - Windows Internet Explorer
https://tmc.tippingpoint.com/TMC/ShowFolder?contentId=dv.2
Google
File Edit View Favorites Tools Help
Links 3COM TippingPoint PR Elisa Dictionaries Google SEO Marketing Resources News Networking Search Engines Menus Magazines Show Sites Translations
Search Find Check Sign In
Threat Management Center
TippingPoint
Friday 3/27/2009
elisal | Logout | Preferences
Home Releases Documentation Support My Account ThreatLinQ
Entire Site
Search
DV
Integration /
DV2319.zip (download)
DV2437.zip (download)
DV2480.zip (download)
DV2503.zip (download)
DV2533.zip (download)
DV2606.zip (download)
DV2643.zip (download)
DV2736.zip (download)
DV2792.zip (download)
DV2819.zip (download)
DV2897.zip (download)
DV2969.zip (download)
DV3051.zip (download)
DV3137.zip (download)
DV3176.zip (download)
DV3210.zip (download)
DV3274.zip (download)
DV3309.zip (download)
DV3362.zip (download)
DV3493.zip (download)
DV3534.zip (download)
DV3587.zip (download)
DV3736.zip (download)
DV3841.zip (download)
DV3894.zip (download)
DV3973.zip (download)


Threat Management Center - Windows Internet Explorer
https://tmc.tippingpoint.com/TMC/ShowFolder?contentId=dv_pod_casts
Google
File Edit View Favorites Tools Help
Links 3COM TippingPoint PR Elisa Dictionaries Google SEO Marketing Resources News Networking Search Engines Menus Magazines Show Sites Translations
Google Search Find Check Sign In
Threat Management Center
TippingPoint
Friday 3/27/2009
elisal | Logout | Preferences
Home Releases Documentation Support My Account ThreatLinQ
Entire Site
Search
Digital Vaccine PodCasts
Product Documentation /
DV_PodCast_20061207 (download)
DV_PodCast_20061212 (download)
DV_PodCast_20061214 (download)
DV_PodCast_20061218 (download)
DV_PodCast_20070109 (download)
DV_PodCast_20070119 (download)
DV_PodCast_20070126 (download)
DV_PodCast_20070202 (download)
DV_PodCast_20070209 (download)
DV_PodCast_20070302 (download)
DV_PodCast_20070316 (download)
DV_PodCast_20070330 (download)
DV_PodCast_20070410 (download)
DV_PodCast_20070427 (download)
DV_PodCast_20070508 (download)
DV_PodCast_20070628 (download)
DV_PodCast_20070710 (download)
DV_PodCast_20070727 (download)
DV_PodCast_20070814 (download)
DV_PodCast_20070821 (download)
DV_PodCast_20070828 (download)
DV_PodCast_20070904 (download)
DV_PodCast_20070911 (download)
DV_PodCast_20070919 (download)
DV_PodCast_20070925 (download)
DV_PodCast_20071002 (download)


Threat Management Center - Windows Internet Explorer
https://tmc.tippingpoint.com/TMC/Content/misc/tmc_updates.doc
Google
File Edit View Favorites Tools Help
Links 3COM TippingPoint PR Elisa Dictionaries Google SEO Marketing Resources News Networking Search Engines Menus Magazines Show Sites Translations
Google Search Find Check Sign In
Threat Management Center
TippingPoint
Friday 3/27/2009
elisal | Logout | Preferences
Home Releases Documentation Support My Account ThreatLinQ
Entire Site
Search
tippingpoint_snort.txt
This document contains a list of TippingPoint filters that are based on Snort filters. Note that most of these filters detect "reconnaissance" probes and are not turned on in the "recommended" settings. These filters were developed prior to August 2002.
97 TFN: Spawn Shell Command Acknowledgement (General)
117 Stacheldraht: Agent Outbound Spoofability Test (General)
118 Stacheldraht: Master Spoofability Test Response (General)
119 Stacheldraht: Agent-to-Master Ping (General)
120 Stacheldraht: Master-to-Agent Pong (General)
121 Stacheldraht: Agent Finder Gag Scanner (General)
122 Stacheldraht: Agent ID Check, Agent Response (General)
333 DoS: Land Attack
337 HTTP: Apache PHF Access
340 HTTP: Shell Command Execution (ls -l)
341 HTTP: Shell Command Execution (cd ..)
343 HTTP: Shell Command Execution (/bin/ps)
345 HTTP: Shell Command Execution (uname -a)
346 HTTP: Shell Command Execution (id command)
347 HTTP: Shell Command Execution (;id command)
348 HTTP: Shell Command Execution (echo command)
349 HTTP: Shell Command Execution (kill command)
350 HTTP: Shell Command Execution (chmod command)
351 HTTP: Shell Command Execution (chgrp command)
352 HTTP: Shell Command Execution (chown command)
353 HTTP: Shell Command Execution (chsh command)
356 HTTP: Shell Command Execution (mail)
358 HTTP: Shell Command Execution (ls|)
359 HTTP: Shell Command Execution (ls)
360 HTTP: Protected Directory Access (~root)
361 HTTP: Protected File Access (/etc/passwd)
363 HTTP: Protected File Access (/etc/motd)
364 HTTP: Protected File Access (/etc/shadow)
367 HTTP: Shell Command Execution (gcc)
369 HTTP: Shell Command Execution (cc)
371 HTTP: Shell Command Execution (cpp)
373 HTTP: Shell Command Execution (g++)
375 HTTP: Shell Command Execution (nasm)
377 HTTP: Shell Command Execution (python)
379 HTTP: Shell Command Execution (tclsh)
384 HTTP: Shell Command Execution (ping)
387 HTTP: Shell Command Execution (xterm command)
401 HTTP: Web-ColdFusion CFUSION_DECRYPT Attempt
402 HTTP: Web-ColdFusion CFUSION_ENCRYPT Attempt
411 HTTP: Web-ColdFusion /cfdocs application.cfm
412 HTTP: Web-ColdFusion /cfdocs onrequestend.cfm Access
413 HTTP: Web-ColdFusion getfile.cfm Access