

SMB : SHARING MORE THAN JUST YOUR FILES

Hormazd Billimoria, Jonathan Brossard



Who are we ?

Jonathan Brossard @endrazine



Security Researcher

Presented at Blackhat/Defcon/CCC/HITB...

Co-founder of the NoSuchCon and Hackito Ergo
Sum Conferences (Paris)

Program Committee of Shakacon (Hawaii)

Check out <https://www.moabi.com>

Who are we ?

Hormazd Billimoria

Security Researcher

@hormazdb



First time speaker at Blackhat

Co-author of the first remote exploit against Windows 10

Co-author of the first remote exploit against Microsoft Edge

Agenda



Agenda

- Introduction to SMB
- Previous Work
- SMB Relay Rebooted
- Root cause analysis
- French Kiss (attack)
- Syphilis (attack)
- Ménage à Trois (attack)
- Mitigation

Introduction to SMB



Demo : Previous Work



Introduction to SMB

What is SMB ?

A network file sharing protocol

Requires Authentication

Designed for Local networks

Introduction to SMB

What is NTLM ?

NT LAN Manager: Suite of security protocols NTLMv2

Challenge response authentication protocol

Cannot be replayed

SMB Relay

Very old exploit

Known since 2001 implemented by Sir Dystic (Cult of the Dead Cow)

Very good exploits

Alberto Solino (Core Security) `smbrelayx.py`

Metasploit module

How it works

Using the hash produced to re-authenticate against another service on the (same) machine.

SMB Relay

Original attack scenario

Attacker is on local intranet

Victim visits attacker's website with file:/// in img tag

IE auto authenticates to attacker

Attacker replays the hash back to the same victim (SMB Reflection :
CVE2008-4037)

SMB Relay

Limits of this attack

Attacker needs to be on the same local network
NOT accessible over the Internet.

SMB Credential Reflection Vulnerability

(CVE2008-4037)

Microsoft issued a partial fix (MS08-068)

Prevents replay of hash to the same machine

Does not stop the attacker from

Relaying the hash to another machine

Breaking the hash

Contribution

We're extending previous research :
SMB Relaying,
Breaking hashes...

this time, remotely over the internet

SMB Relay : Rebooted



DEMO : French Kiss Attack (IE to SMB)



Affected Software

All versions of Windows are affected

First remote exploit against Windows 10

First remote exploit against Microsoft Edge

SMB Relay Rebooted

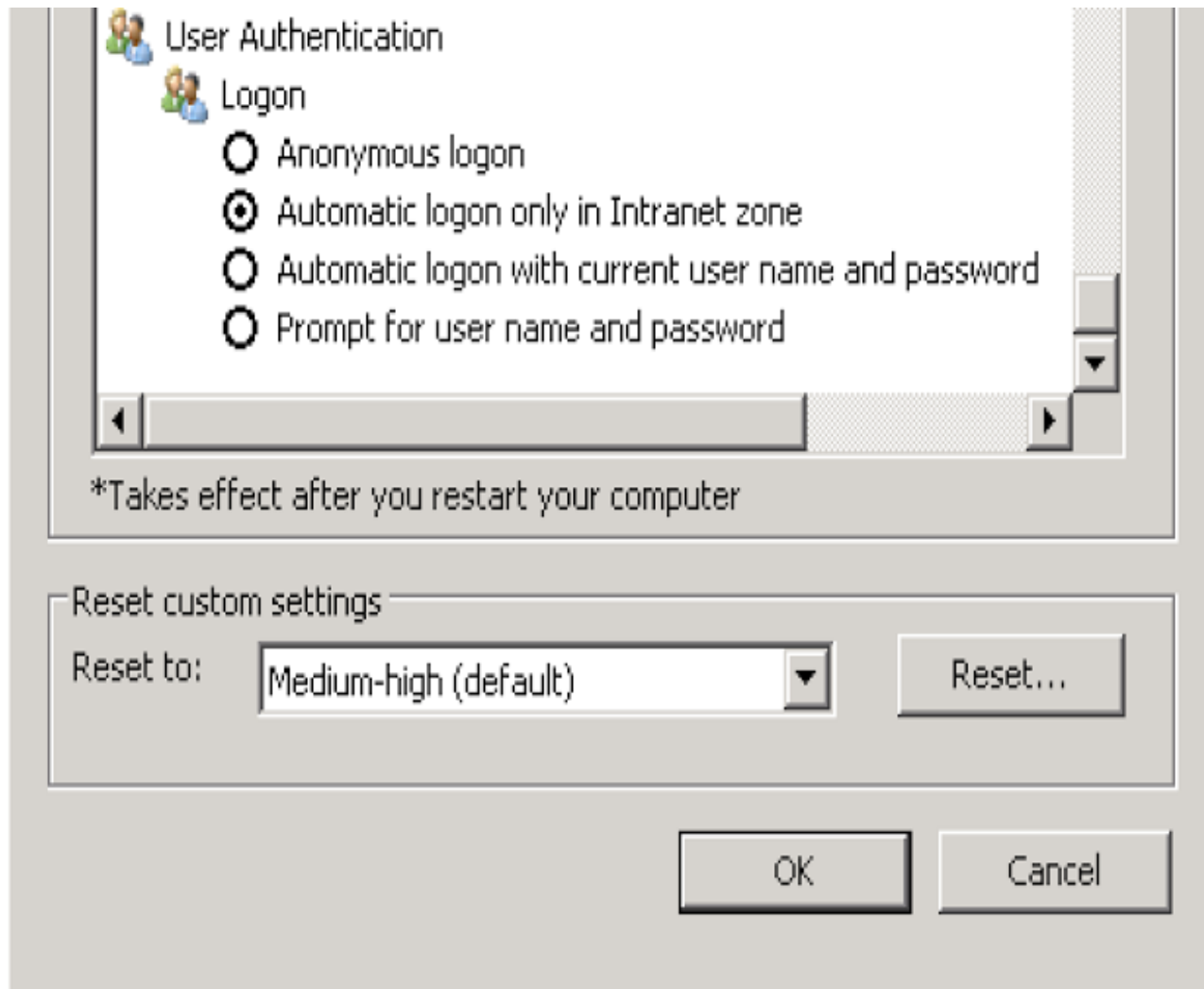
Main Assumption is Attacker is on the victim's network.

Issue Severity:

Note that attacks targeting this issue only work in the **Intranet zone** – Internet Explorer will not send credentials automatically in the Internet zone. This limits attacks to coming from within the same subnet

SMB Relay Rebooted

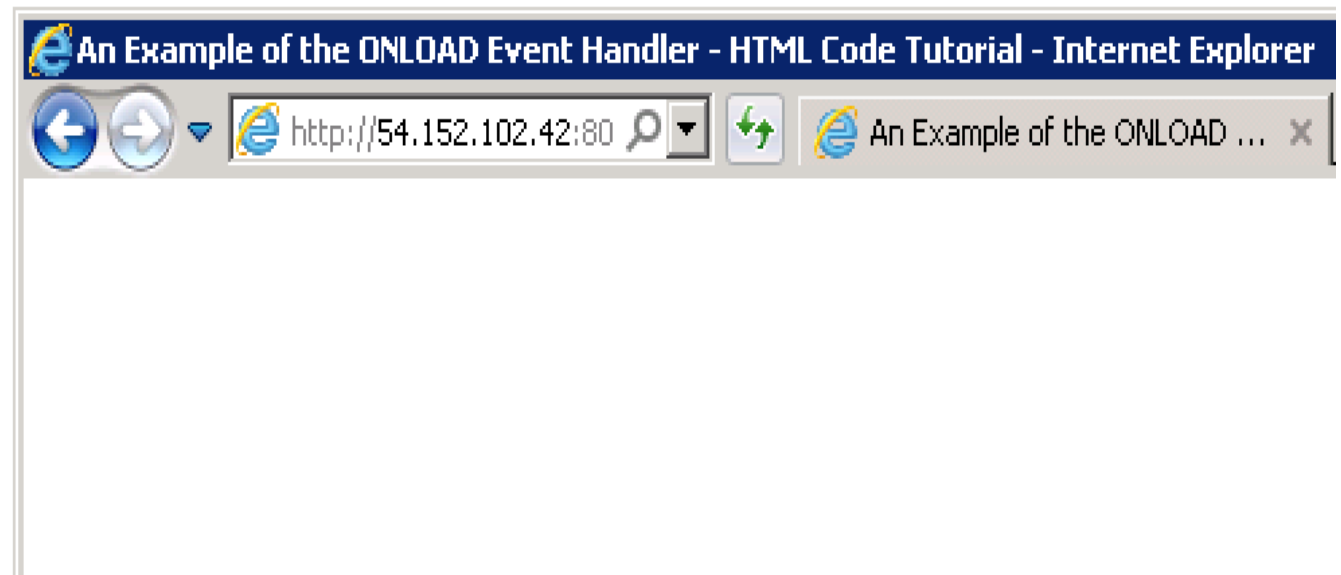
There's actually an IE setting for this :



The Mighty IMG tag

(Very) Basic trigger :

```
6  
7 <BODY >  
8   
9 </body>  
10
```



SMB Relay Rebooted

59	38.3612930	172.31.39.166	54.209.109.93	TCP	54 50998+445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
60	38.3613510	172.31.39.166	54.209.109.93	SMB	213 Negotiate Protocol Request
61	38.3624960	54.209.109.93	172.31.39.166	TCP	54 445+50998 [ACK] Seq=1 Ack=160 Win=30336 Len=0
62	38.3709730	54.209.109.93	172.31.39.166	SMB	173 Negotiate Protocol Response
63	38.3803440	172.31.39.166	54.209.109.93	SMB	193 Session Setup AndX Request, NTLMSSP_NEGOTIATE
64	38.4012130	54.209.109.93	172.31.39.166	SMB	426 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
65	38.4015660	172.31.39.166	54.209.109.93	SMB	706 Session Setup AndX Request, NTLMSSP_AUTH, User: RELAY\hormazd
66	38.4136650	54.209.109.93	172.31.39.166	SMB	120 Session Setup AndX Response

What is going on here ?

SMB Relay Rebooted

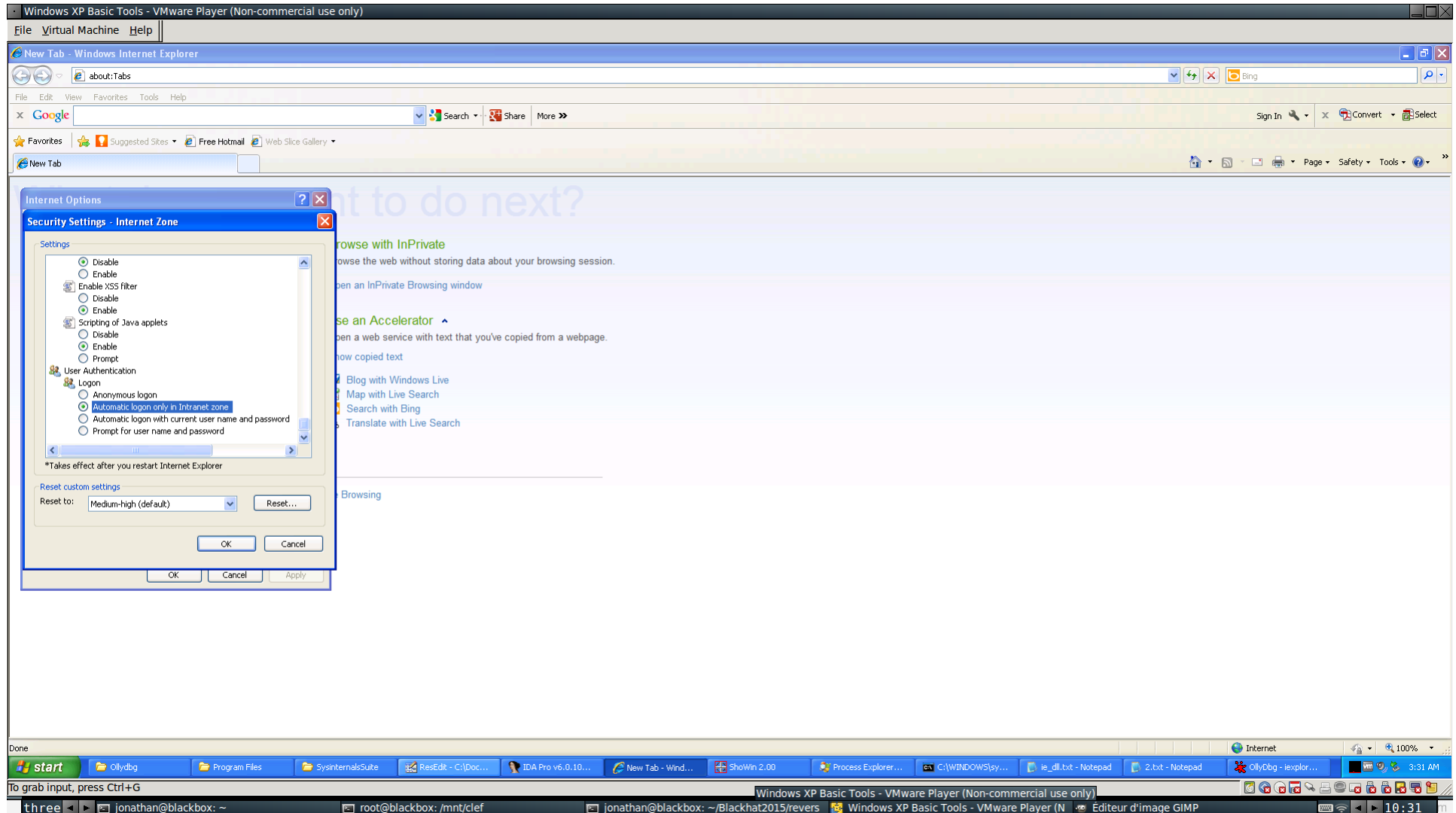
```
NTLM Message Type: NTLMSSP_AUTH (0x00000003)
⊕ Lan Manager Response: 0000000000000000000000000000000000000000000000000000000000000000
  NTLM Client Challenge: 0000000000000000
⊖ NTLM Response: 6c814b0a16fbbc86ea17370ed34521680101000000000000...
  Length: 286
  Maxlen: 286
  Offset: 162
⊖ NTLMv2 Response: 6c814b0a16fbbc86ea17370ed34521680101000000000000...
  NTProofstr: 6c814b0a16fbbc86ea17370ed3452168
  Response Version: 1
  Hi Response Version: 1
  Z: 000000000000
  Time: Jan 13, 2015 17:54:34.000000000 UTC
  Client Challenge: 9fa115478c469c4b
  Z: 00000000
⊕ Attribute: NetBIOS computer name: server_name
⊕ Attribute: NetBIOS domain name: WORKGROUP
⊕ Attribute: DNS computer name: server_name
⊕ Attribute: DNS domain name: WORKGROUP
⊕ Attribute: Timestamp
⊕ Attribute: Flags
⊕ Attribute: Restrictions
```

Authentication is actually happening silently !

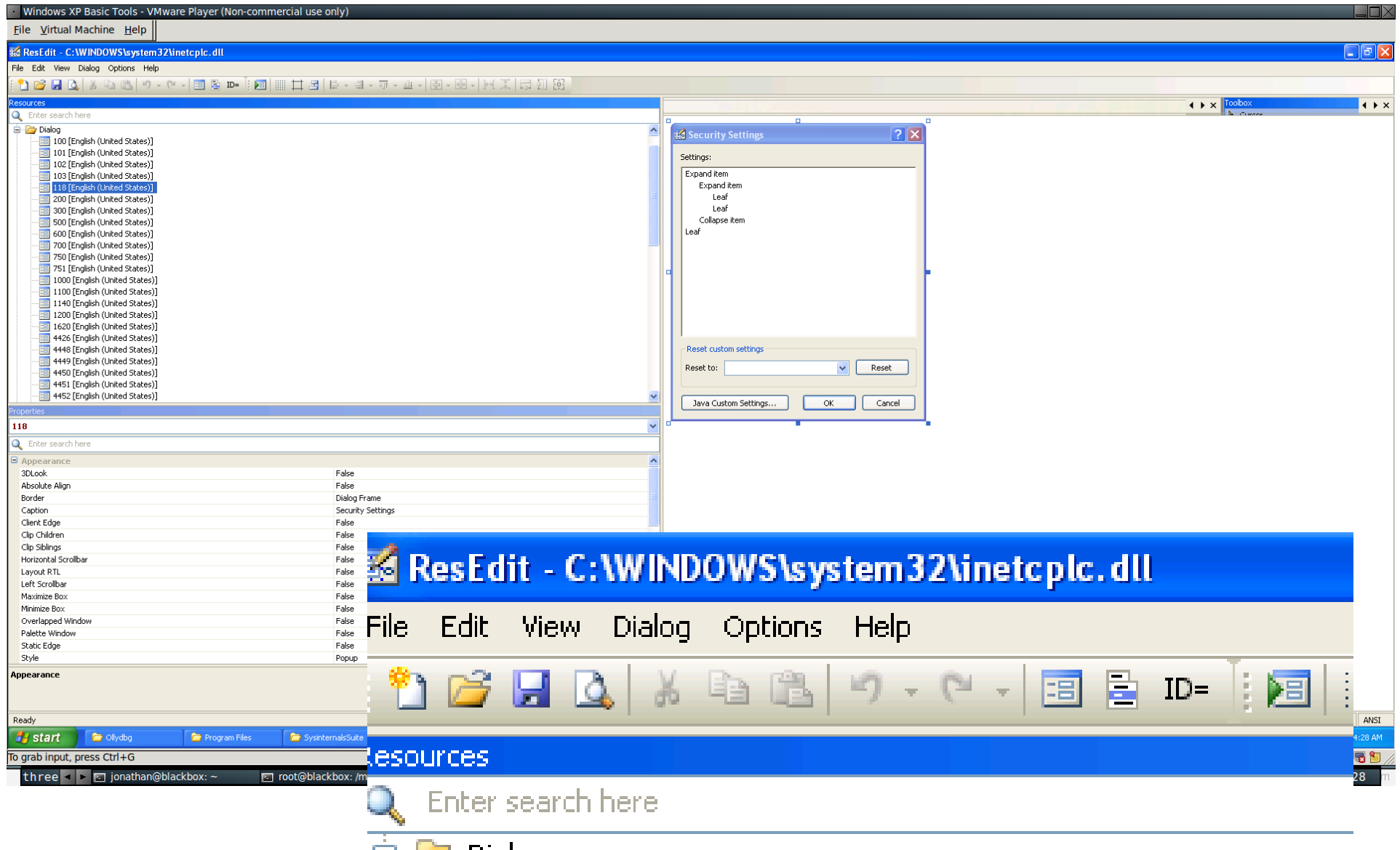
Root Cause Analysis



Root Cause Analysis



Root Cause Analysis



Diffing the registry

The screenshot shows the Kompare application window. The title bar reads "Kompare". The menu bar includes "File", "Difference", "Settings", and "Help". The toolbar contains icons for "Compare Files", "Save", "Save All", "Previous File", "Next File", "Previous Difference", "Next Difference", "Unapply All", "Unapply Difference", "Apply Difference", and "Apply All".

The "Navigation" section contains a table with the following columns: "Source Folder", "Destination Folder", "Source File", "Destination File", "Source Line", "Destination Line", and "Difference". The table shows the source file is "prompt_u..." and the destination file is "automatic_logon_internet.reg", with a difference of "Changed 1 line" at line 222.

The main diff area shows two side-by-side files: "prompt_user.reg" and "automatic_logon_internet.reg". Both files contain registry values for "Internet Settings\Zones\3". The files are identical up to line 221. At line 222, the "prompt_user.reg" file has the value "1A00" with a data type of "dword:00010000", while the "automatic_logon_internet.reg" file has the value "1A00" with a data type of "dword:00000000". This line is highlighted in red in both panes.

The status bar at the bottom indicates "Comparing file file:///tmp/diff/prompt_user.reg with file:///tmp/diff/automatic_logon_internet.reg" and shows "1 of 1 difference, 0 applied" and "1 of 1 file".

Tracing

The screenshot displays a Windows XP virtual machine running VMware Player. The main window is OllyDbg, showing the 'Executable modules' list for the process 'iexplore.exe'. The list includes various system DLLs and application DLLs, such as 'C:\Program Files\Internet Explorer\iexplore.exe', 'C:\WINDOWS\system32\user32.dll', 'C:\WINDOWS\system32\GDI32.dll', and many others. The taskbar at the bottom shows several open applications, including 'start', 'Olydbg', 'Program Files', 'SystemStateSuite', 'ResEdit', 'IDA Pro v6.0.10...', 'New Tab - Wind...', 'ShoWin 2.00', 'Process Explorer...', 'C:\WINDOWS\sys...', 'ie_dll.txt - Notepad', '2.bit - Notepad', and 'OlyDbg - iexplor...'. The system tray shows the time as 3:35 AM.

Base	Size	Entry	Name	File version	Path
00400000	000F3000	00401A25	Internet Explorer	8.00.6001.18702	C:\Program Files\Internet Explorer\iexplore.exe
01840000	000C5000	000C5000	user32.dll	6.0.6002.5512	C:\WINDOWS\system32\user32.dll
01E30000	00090000	01E31782	Normaliz.dll	6.0.6002.5512	C:\WINDOWS\system32\Normaliz.dll
02230000	00053000	02230494	AcroIEFavC1	11.0.0.379	C:\Program Files\Common Files\Adobe\Acrobat\MCIETAct\AcroIEFavClient.dll
02290000	00010000	02292F46	Coupon Down	11.0.0.379	C:\Program Files\Coupon Down\loader\Coupon Down_loader.dll
022E0000	00011000	022E7098	AcroIEHelpe	11.0.0.379	C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
02310000	00012000	451F1084	AcroIEHelpe	11.0.0.379	C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
02340000	00046000	02345D1F	OChelper.dll	4.0.7577.0 build	C:\Program Files\Microsoft Lync\OChelper.dll
02430000	00003000	024354D1	OChelperRes	4.0.7577.0 build	C:\Program Files\Microsoft Lync\OChelperResource.dll
02490000	0000E000	02498477	skypeieplugi	5.2.1.0	C:\WINDOWS\system32\skypeieplugi.dll
02550000	00124000	02558C51	skypeieplugi	5.2.1.0	C:\Program Files\Skype\Toolbars\Internet Explorer\skypeieplugin.dll
02640000	000F9000	0264D1E2	swg	5.7.9012.1008	C:\Program Files\Google\Google Toolbar\Notifer\5.7.9012.1008\swg.dll
02670000	00009000	02671108	msi31	7.0.5.1111.1711	C:\WINDOWS\system32\msi31.dll
026C0000	00479000	026C1894	GoogleToolb	7.0.5.1111.1711	C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic_32_8E471B27954D28F5.dll
02700000	000F9000	02701108	msi31	7.0.5.1111.1711	C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic_xw_en_804439F67F61805.dll
027C0000	00047000	027C1894	GoogleToolb	7.0.5.1111.1711	C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic_32_8E471B27954D28F5.dll
027F0000	000F9000	027F1108	msi31	7.0.5.1111.1711	C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic_xw_en_804439F67F61805.dll
02830000	00435000	02834F42	SkypeFav	5.2.1.0	C:\Program Files\Skype\Toolbars\Shared\SkypeFav.dll
10000000	00053000	1000E191	GoogleToolb	7.0.5.1111.1711	C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
10090000	0000C000	100929E5	Indtut1.dll	8.00.6001.18702	C:\WINDOWS\system32\Indtut1.dll
100E0000	0000E000	100E5306	pnfplitt	8.00.6001.18702	C:\WINDOWS\system32\pnfplitt.dll
3CE40000	00052000	3CE42001	whetapi	8.00.6001.18702	C:\WINDOWS\system32\whetapi.dll
3D700000	00084000	3D7080E9	jscrip1	8.00.6001.23141	C:\WINDOWS\system32\jscrip1.dll
3D900000	00004000	3D901748	WININET	6.00.6002.5512	C:\WINDOWS\system32\WININET.dll
3DFA0000	001E3000	3E0E383D	iertutil	8.00.6001.19098	C:\WINDOWS\system32\iertutil.dll
3E100000	001E3000	3E0E383D	IEFRAME	8.00.6001.19098	C:\WINDOWS\system32\IEFRAME.dll
3FDE0000	00441000	3FDE191D	inetapi	8.00.6001.19098	C:\WINDOWS\system32\inetapi.dll
42700000	001E6000	42712969	inetcp1.cpl	8.00.6001.19098	C:\WINDOWS\system32\inetcp1.cpl
42900000	00040000	42912723	msi31	7.0.5.1111.1711	C:\Program Files\Internet Explorer\iexplore.dll
451F0000	00006000	451F201C	xpshtml	8.00.6001.19098	C:\Program Files\Internet Explorer\XPS\html.dll
454F0000	00059000	454F1748	WINHTTP	6.00.6002.5512	C:\WINDOWS\system32\WINHTTP.dll
45C50000	0010B000	45C57989	gdipplus	2.2.6002.22509	C:\WINDOWS\WinSxS\x-ww_Microsoft.Windows.GDIPlus_6595b64144c0fd1f_1.0.6002.22509_x-ww_c0da2032\gdipplus.dll
53960000	00010000	53961626	uxtheme	6.00.2900.5512	C:\WINDOWS\system32\uxtheme.dll
5D070000	00038000	5D071626	uxtheme	6.00.2900.5512	C:\WINDOWS\system32\uxtheme.dll
5E860000	00055000	5E868846	NETAPI32	6.00.2900.5512	C:\WINDOWS\system32\NETAPI32.dll
62470000	00020000	62471626	Shimeng	6.00.2900.5512	C:\WINDOWS\system32\Shimeng.dll
6D090000	00090000	6D093460	conct132	6.02 (xps_sp3)	C:\WINDOWS\system32\conct132.dll
6E100000	00000000	6E100000	OLE32	6.00.6002.5512	C:\WINDOWS\system32\OLE32.dll
6E800000	0002E000	6E801496	ADUPACK	8.00.6001.18702	C:\WINDOWS\system32\ADUPACK.dll
6E830000	00059000	6E831748	hnetapi	6.00.6002.5512	C:\WINDOWS\system32\hnetapi.dll
68000000	00036000	68014E38	rsaenh	6.00.6002.5507	C:\WINDOWS\system32\rsaenh.dll
6D430000	00063000	6D435358	J23sv	6.0.230.0	C:\Program Files\Java\jre6\bin\j23sv.dll
6D4F0000	00012000	6D4F1626	uxtheme	6.00.2900.5512	C:\WINDOWS\system32\uxtheme.dll
71590000	00079000	7159C170	AcLayers	5.1.2600.5506	C:\WINDOWS\AppPatch\AcLayers.DLL
71650000	0003F000	716516C0	mswsock	6.00.6002.5512	C:\WINDOWS\system32\mswsock.dll
71A90000	00009000	71A9142E	whetapi	8.00.6001.18702	C:\WINDOWS\system32\whetapi.dll
71A00000	00009000	71A01626	MS2HELP	6.00.6002.5512	C:\WINDOWS\system32\MS2HELP.dll
71A00000	00017000	71A01273	ws2_32	6.00.6002.5512	C:\WINDOWS\system32\ws2_32.dll
71B20000	00012000	71B21248	VFR	6.00.2900.5512	C:\WINDOWS\system32\VFR.dll
71BF0000	00013000	71BF118D	SHELL32	6.00.6002.5512	C:\WINDOWS\system32\SHELL32.dll
71C10000	0000E000	71C1175E	ntlanman	6.00.6002.5512	C:\WINDOWS\system32\ntlanman.dll
71C30000	00007000	71C31075	NETAPI	6.00.6002.5512	C:\WINDOWS\system32\NETAPI.dll
71C90000	00040000	71C94445	NETUI1	6.00.6002.5512	C:\WINDOWS\system32\NETUI1.dll
71D00000	00017000	71D01029	NETUI2	6.00.6002.5512	C:\WINDOWS\system32\NETUI2.dll
71D40000	0001B000	71D412BD	actxprxy	6.00.2900.5512	C:\WINDOWS\system32\actxprxy.dll
722B0000	00009000	722B1110	senapi	6.00.6002.5512	C:\WINDOWS\system32\senapi.dll
73000000	00026000	73005485	WINSPOOL_D	6.00.6002.5512	C:\WINDOWS\system32\WINSPOOL_D
73000000	00013000	73001302	stl	6.00.6002.5512	C:\WINDOWS\system32\stl.dll
746F0000	00020000	746F1748	msctf	6.00.6002.5512	C:\WINDOWS\system32\msctf.dll
74720000	0004C000	74721305	MSCTF	6.00.6002.5512	C:\WINDOWS\system32\MSCTF.dll
74980000	00012000	74981190	msasn1	6.00.1952.0	C:\WINDOWS\system32\msasn1.dll
74E00000	00007000	74E01626	CFGHDR32	6.00.6002.5512	C:\WINDOWS\system32\CFGHDR32.dll
754D0000	00009000	754D1660	CRYPTUI	6.00.6002.5512	C:\WINDOWS\system32\CRYPTUI.dll
75C00000	0002E000	75C0FE11	msctfime_in	6.00.6002.5512	C:\WINDOWS\system32\msctfime_in
75F30000	00010000	75F316F6	NLANS	6.00.2900.5512	C:\WINDOWS\system32\NLANS.dll
75E00000	00013000	75E14200	cryptnet	6.00.6002.5512	C:\WINDOWS\system32\cryptnet.dll
75F60000	00007000	75F61121	ddrprov	6.00.6002.5512	C:\WINDOWS\system32\ddrprov.dll
75770000	00000000	7577138F	davslint	6.00.6002.5512	C:\WINDOWS\system32\davslint.dll
76360000	00010000	763610E0	WINSTA	6.00.6002.5512	C:\WINDOWS\system32\WINSTA.dll
76390000	00005000	763910E0	WINSTA	6.00.6002.5512	C:\WINDOWS\system32\WINSTA.dll
76390000	00010000	76391200	IMH32	6.00.6002.5512	C:\WINDOWS\system32\IMH32.DLL
763B0000	00049000	763B1619	conct132	6.00.2900.5512	C:\WINDOWS\system32\conct132.dll
76790000	0000C000	76791889	cryptdll	6.00.6002.5512	C:\WINDOWS\system32\cryptdll.dll
76800000	00004000	768070E3	RMSDGL	6.00.6002.5512	C:\WINDOWS\system32\RMSDGL.dll
76990000	00025000	76991075	ntshrui	6.00.6002.5512	C:\WINDOWS\system32\ntshrui.dll
769C0000	00004000	769C1654	USERENV	6.00.6002.5512	C:\WINDOWS\system32\USERENV.dll
76C00000	00011000	76C020E6	rtl	6.00.6002.5512	C:\WINDOWS\system32\rtl.dll
76840000	0002D000	76842861	WINMM	6.00.6002.5512	C:\WINDOWS\system32\WINMM.dll
768F0000	00009000	768F1108	FSPT	6.00.6002.5512	C:\WINDOWS\system32\FSPT.dll
76C00000	0002E000	76C11C25	WINTRUST	6.00.6002.5512	C:\WINDOWS\system32\WINTRUST.dll
76C00000	00020000	76C11C25	inagapi	6.00.6002.5512	C:\WINDOWS\system32\inagapi.dll
76D40000	00018000	76D42C50	IPAPI	6.00.6002.5512	C:\WINDOWS\system32\IPAPI.dll
76D00000	00019000	76D05300	IPAPI	6.00.6002.5512	C:\WINDOWS\system32\IPAPI.DLL
76E10000	00020000	76E11100	advapi32	6.00.6002.5512	C:\WINDOWS\system32\advapi32.dll
76E00000	0000E000	76E018A0	rtutils	6.00.6002.5512	C:\WINDOWS\system32\rtutils.dll
76E30000	00012000	76E31260	rsasn	6.00.6002.5512	C:\WINDOWS\system32\rsasn.dll
76E00000	0002F000	76E01300	TAPI32	6.00.6002.5512	C:\WINDOWS\system32\TAPI32.dll
76EE0000	0000C000	76EE1300	RPCRT4	6.00.6002.5512	C:\WINDOWS\system32\RPCRT4.dll
76F00000	00009000	76F03300	WSPAPI32	6.00.6002.5512	C:\WINDOWS\system32\WSPAPI32.dll
76F60000	0002C000	76F61130	MLDAP32	6.00.6002.5512	C:\WINDOWS\system32\MLDAP32.dll
76FD0000	00073000	76FD3045	CLBQATL	6.00.6002.5512	C:\WINDOWS\system32\CLBQATL.dll
77050000	00005000	77051055	CORRES	2001.12.4414.708	C:\WINDOWS\system32\CORRES.dll
77120000	00008000	77121150	OLE32	6.00.6002.5512	C:\WINDOWS\system32\OLE32.dll
773D0000	00103000	773D2520	conct132	6.0 (xps_sp3)	C:\WINDOWS\WinSxS\x-ww_Microsoft.Windows.Common-Controls-6595b64144c0fd1f_1.0.6002.22509_x-ww_61e65202\conct132.dll
774E0000	0012E000	774E1061	ole32	6.00.6002.5512	C:\WINDOWS\system32\ole32.dll
77490000	000F3000	77491E40	SETUPAPI	6.00.6002.5512	C:\WINDOWS\system32\SETUPAPI.dll

Lessons learned

It's not just IE

All Windows applications relaying on System dlls to fetch URLs are vulnerable (see C:\Windows\inetcplc.dll...).

Registry keys involved

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones*

What's happening

Inetcplc.dll does save the settings properly in the registry. Registry configuration is queried, and then ignored !

DEMO: French Kiss to Malware (Syphilis attack)



Syphilis attack

Time to attack via SMB relay

Fool user into visiting malicious website (r/netsec ?)

Relay credentials to DC on the same network

Maybe attack NTLM over HTTP server auth?

Attack Limitations

Packet signing needs to be disabled (only for relaying malware)

Recommended to improve performance

SMB outbound needs to be enabled

Failing egress filtering at Firewall level (common)

In regards to packet signing...

Home

Knowledge Center

Downloads

Service Requests

Tools

Programs and Policies

Customer Service

My Account

Knowledge Center

Search McAfee Knowledge Center | Print

SMB Signing must be disabled for Windows NTLM authentication to work

Technical Articles ID: KB74145

Last Modified: 9/25/2013

Environment

McAfee Firewall Enterprise 8.3.x, 8.2.x

Summary

According Microsoft KB article 887429 (support.microsoft.com/kb/887429), you can configure SMB signing to be OFF, ON but not required, or ON and required for clients to login.

You must disable SMB signing (in other words, set it to OFF) for NTLM authentication via the firewall to work. You cannot set it to be ON but not required; you must completely disable it on the Windows server.

Solution

For instructions about turning SMB signing off, see [PD21455](#),

Rate this document



Did this article resolve your issue?

- Yes
 No

Please provide any comments below

Optional

Submit

Affected Products

DEMO: French Kiss to RDP



French Kiss to RDP

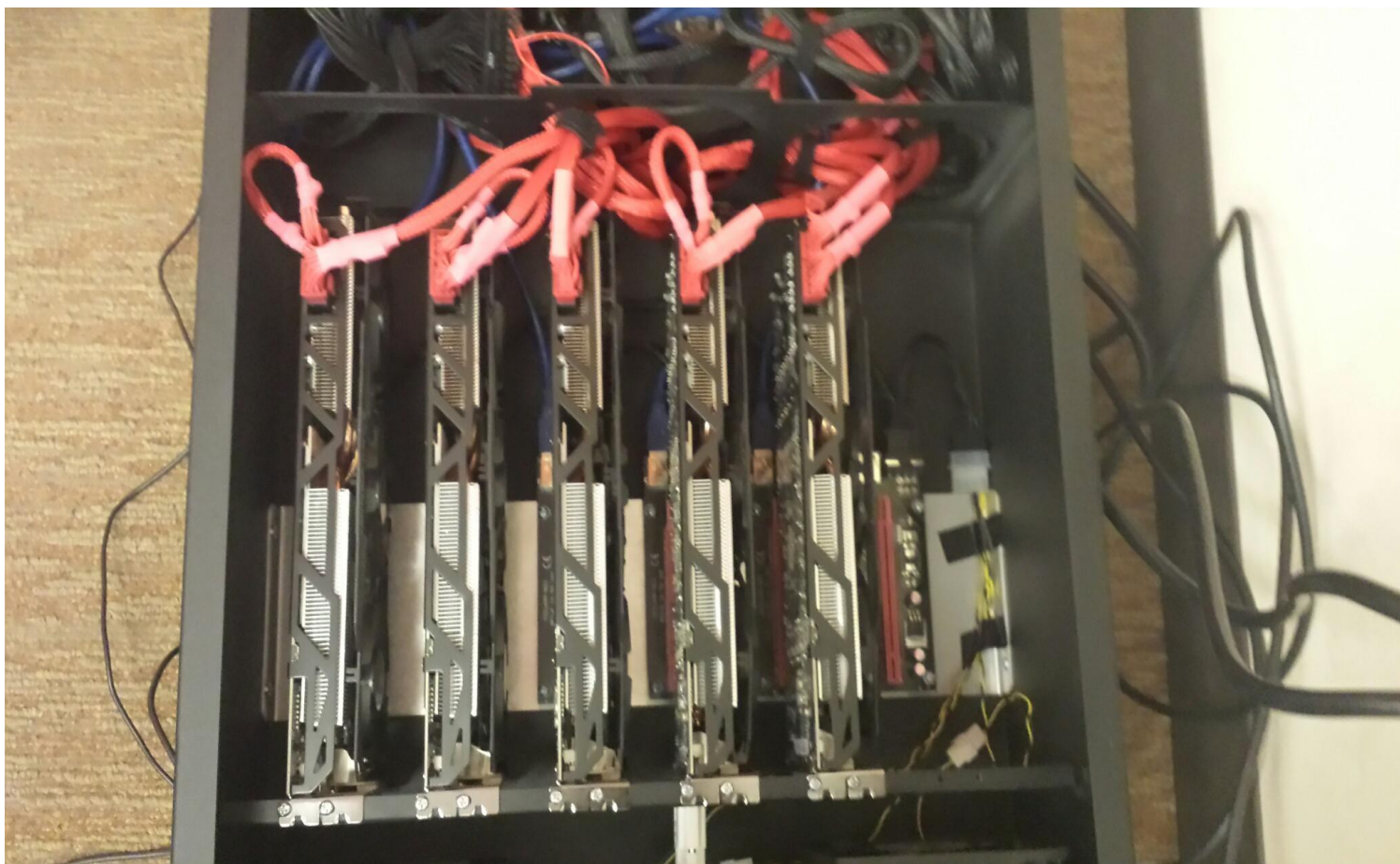
Hash cracking

GPU cracking Super fast (HashCat)

Our own cracking machine

Can crack 2.4 Billion hashes/sec

Hash Cracking Hardware



French Kiss to RDP

Key space of 68 characters

Uppercase

Lowercase

Alphanumeric

Special characters - !@#\$%&

8 Characters passwords

68^8 - 2 days and 5 hours to crack

NTLM authentication over the Internet

SHODAN

Results 1 - 10 of about 1506 for WWW-Authenticate: Basic realm="SMB"

Services	Count	IP	OS	Company	Added	Location	HTTP Status	HTTP Headers
HTTP	896	219.85.116.80	Linux 2.6.x	Sony Network Taiwan Limited	12.01.2014	Taipei	401 Unauthorized	HTTP/1.0 401 Unauthorized Pragma: no cache Content-type: text/html Date: Sun, 12 Jan 2014 14:16:20 GMT Accept-Ranges: bytes Connection: close WWW-Authenticate: Basic realm="SMB"
HTTP Alternate	574	219-85-116-80-adsl-TPE.dynamic.sonet.net.tw						
HTTPS	33							
HTTPS Alternate	3							
Top Countries								
India	1,273							
China	118							
Taiwan	102							
Mexico	5							
Hong Kong	3							
		118.166.81.94		CHTD, Chunghwa Telecom Co., Ltd.	12.01.2014	Taipei	401 Unauthorized	HTTP/1.0 401 Unauthorized Pragma: no cache Content-type: text/html Date: Sun, 12 Jan 2014 13:04:45 GMT Accept-Ranges: bytes Connection: close WWW-Authenticate: Basic realm="SMB"
		118-166-81-94.dynamic.hinet.net						
		115.244.226.75		BSES TeleCom Limited	01.01.2014	Pondicherry	401 Unauthorized	HTTP/1.0 401 Unauthorized Pragma: no cache Content-type: text/html Date: Wed, 01 Jan 2014 21:30:53 GMT

Impact

Retrieve user credentials

Username sent in plain text

Password cracked

Remote code execution

Leveraging NTLM authentication over HTTP allows us to RCE

Billions of corporate users are vulnerable

IE is the market leader in Corporate environments

Other triggers



DEMO : Video trigger



Ménage à Trois



DEMO : Ménage à trois (SMB Relay to Exchange)



Ménage à Trois

Owning the cloud(s)

Demos done on Amazon AWS, Microsoft Azure

Thousands of servers allowing NTLM over HTTP

Unsafe defaults

Extended protection isn't enabled by default

Extended protection is hard to configure

Mitigations



How to protect yourself

Egress filtering at Perimeter level

Drop outgoing SMB on ports 137/138/139/445.

Host level hardening

Drop outgoing SMB on ports 137/138/139/445 to public IPs

Enable Packet Signing

Enable Extended Protection

Take away



Impact

We forced a victim to send us their credentials

Through a website

Through an email

Through a video...

Able to upload malware

Able to replay SMB to Exchange

Able to replay to any service using NTLMSSP

And all of this was done remotely from the Internet

All versions of Windows are affected

Windows 10 and Microsoft Edge are also vulnerable

Acknowledgements



Greetings

Special thanks to MSRC for working on those vulnerabilities with us for the past 9 months.

Questions ?

