

# 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

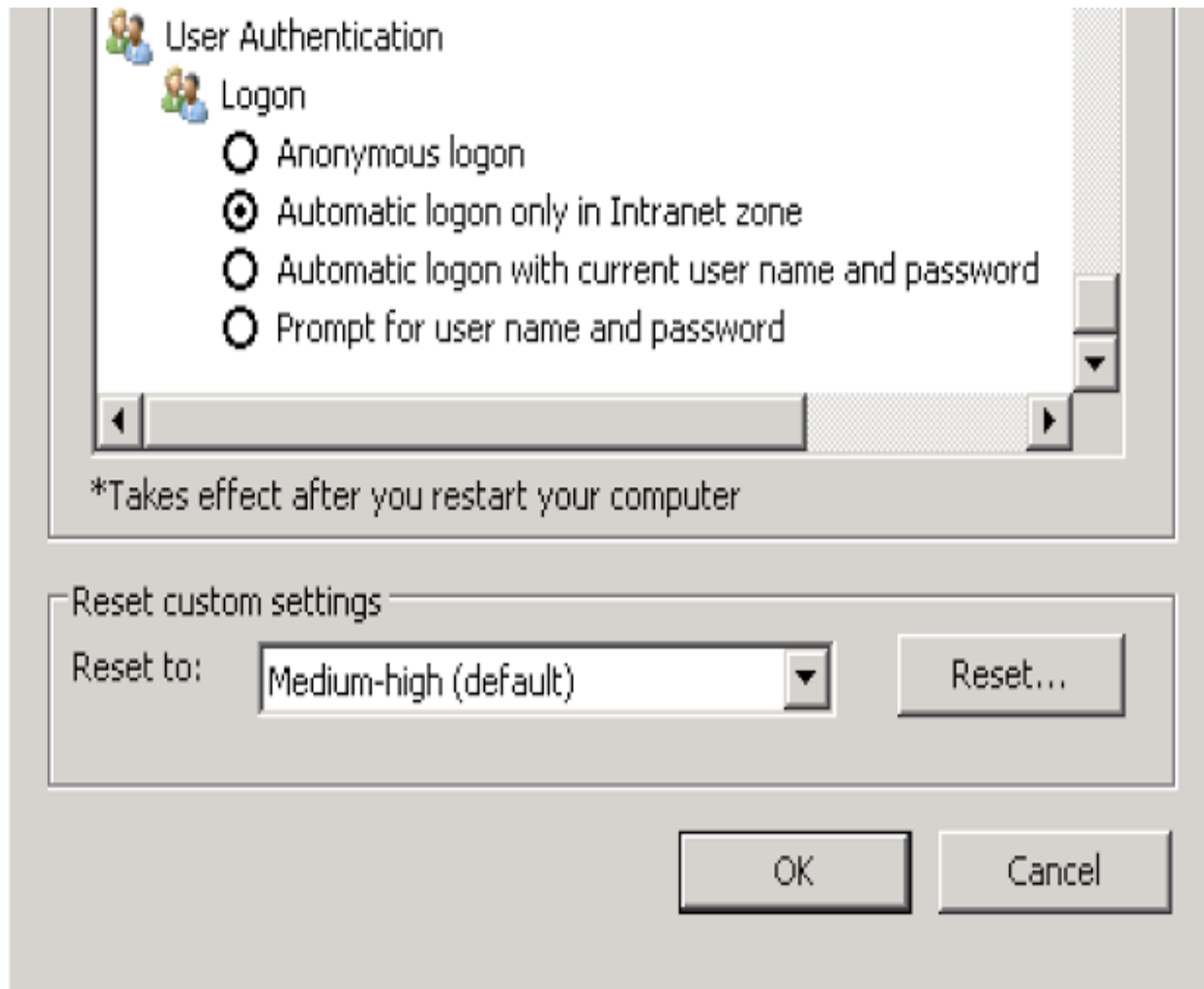
Main Assumption is Attacker is on the victim's network.

## 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

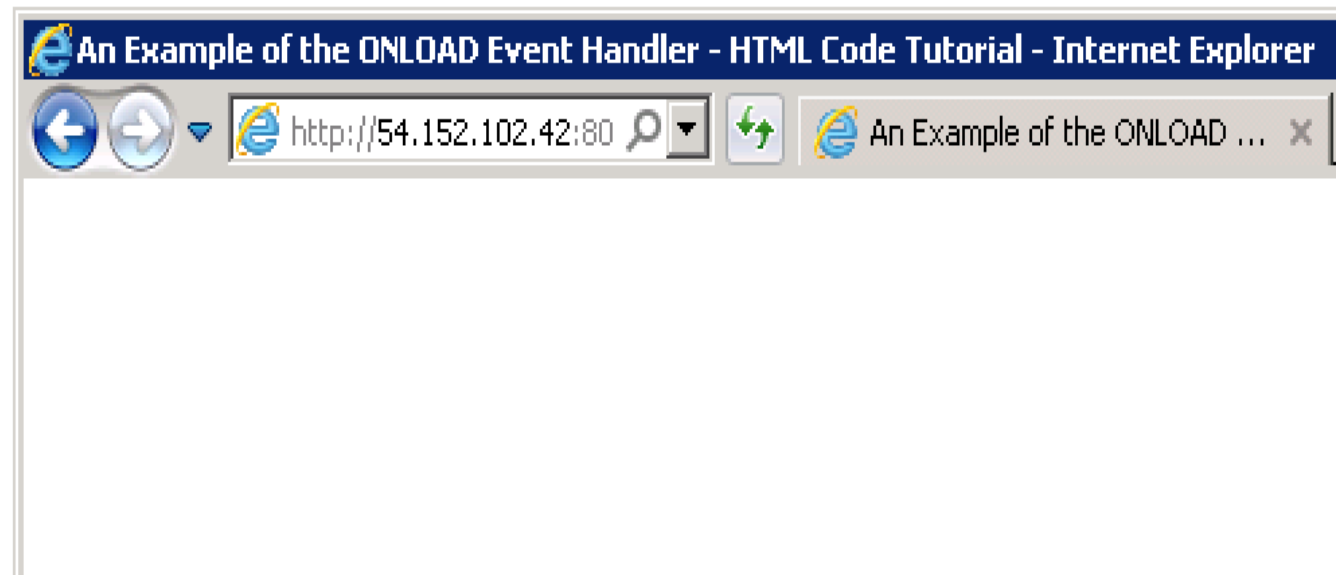
There's actually an IE setting for this :



# 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

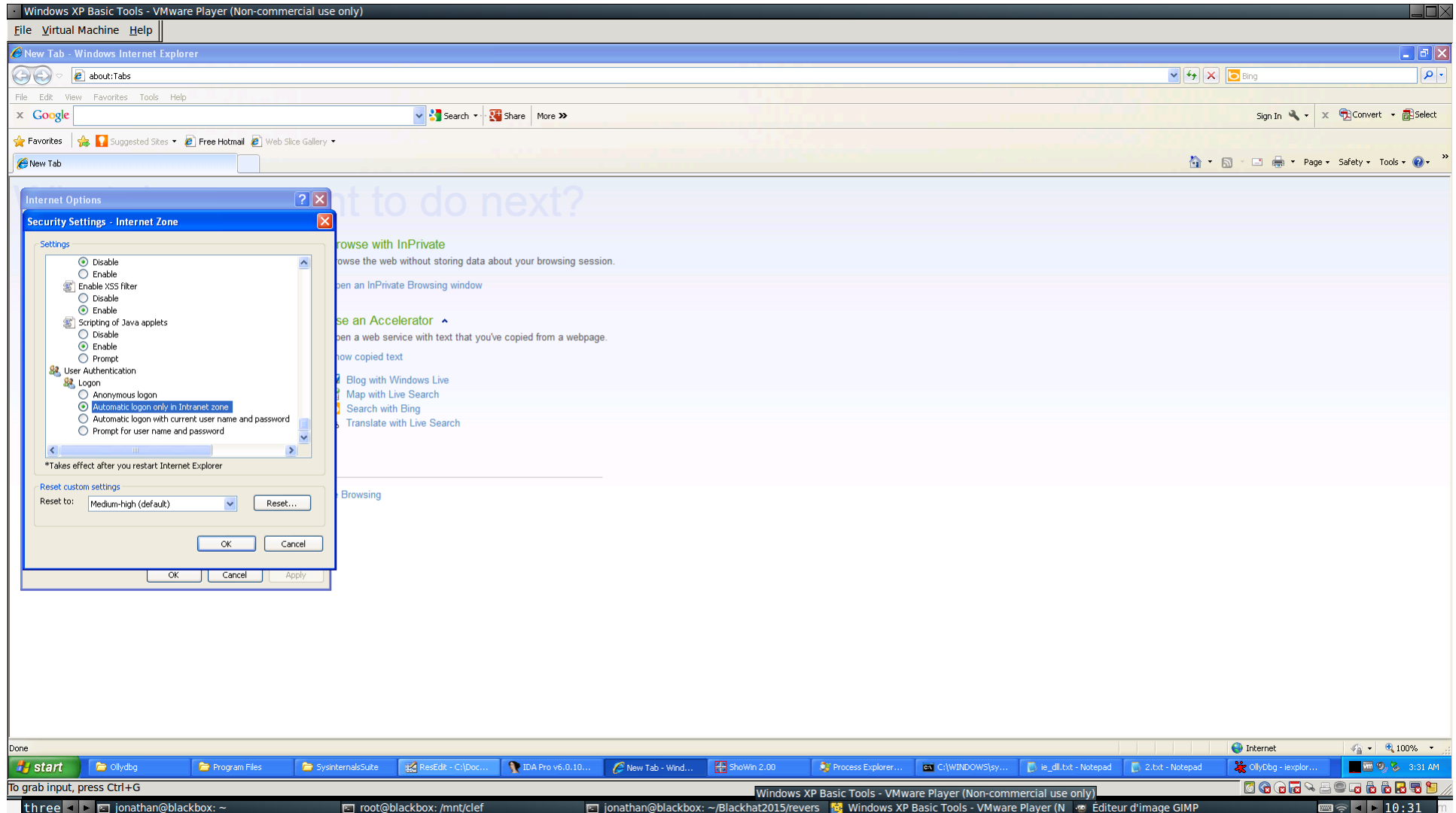
```
NTLM Message Type: NTLMSSP_AUTH (0x00000003)
⊕ Lan Manager Response: 0000000000000000000000000000000000000000000000000000000000000000
  NTLM Client Challenge: 0000000000000000
⊖ NTLM Response: 6c814b0a16fbbc86ea17370ed34521680101000000000000...
  Length: 286
  Maxlen: 286
  Offset: 162
⊖ NTLMv2 Response: 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

The screenshot displays the ResEdit application interface. The main window shows a list of resources under the 'Dialog' folder, with '118 [English (United States)]' selected. A 'Security Settings' dialog box is open, showing a list of settings: 'Expand item', 'Expand item', 'Leaf', 'Leaf', 'Collapse item', and 'Leaf'. The dialog also includes a 'Reset custom settings' section with a 'Reset to:' dropdown and a 'Reset' button. The application title bar reads 'ResEdit - C:\WINDOWS\system32\inetctl.dll'. The menu bar includes 'File', 'Edit', 'View', 'Dialog', 'Options', and 'Help'. The toolbar contains various icons for file operations and editing. The status bar at the bottom shows 'Ready' and 'To grab input, press Ctrl+G'. The taskbar at the bottom of the screen shows the Start button, 'Olydbg', 'Program Files', and 'SysinternalsSuite' icons. The system tray in the bottom right corner shows the system clock as '4:28 AM' and the date '28'.

Windows XP Basic Tools - VMware Player (Non-commercial use only)

File Virtual Machine Help

ResEdit - C:\WINDOWS\system32\inetctl.dll

File Edit View Dialog Options Help

Resources

Enter search here

Dialog

- 100 [English (United States)]
- 101 [English (United States)]
- 102 [English (United States)]
- 103 [English (United States)]
- 118 [English (United States)]
- 200 [English (United States)]
- 300 [English (United States)]
- 500 [English (United States)]
- 600 [English (United States)]
- 700 [English (United States)]
- 750 [English (United States)]
- 751 [English (United States)]
- 1000 [English (United States)]
- 1100 [English (United States)]
- 1140 [English (United States)]
- 1200 [English (United States)]
- 1620 [English (United States)]
- 4426 [English (United States)]
- 4446 [English (United States)]
- 4449 [English (United States)]
- 4450 [English (United States)]
- 4451 [English (United States)]
- 4452 [English (United States)]

Properties

118

Enter search here

Appearance

3DLook	False
Absolute Align	False
Border	Dialog Frame
Caption	Security Settings
Client Edge	False
Clip Children	False
Clip Siblings	False
Horizontal Scrollbar	False
Layout RTL	False
Left Scrollbar	False
Maximize Box	False
Minimize Box	False
Overlapped Window	False
Palette Window	False
Static Edge	False
Style	Popup

Appearance

Ready

To grab input, press Ctrl+G

three jonathan@blackbox: ~ root@blackbox: /

ResEdit - C:\WINDOWS\system32\inetctl.dll

File Edit View Dialog Options Help

Resources

Enter search here

ANSI 4:28 AM 28

# 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 view shows two side-by-side files: "prompt\_user.reg" and "automatic\_logon\_internet.reg". Both files contain registry values for "HKKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3". The files are identical except for line 222, which is highlighted in red in both panes. In the left pane, line 222 is "1A00=dword:00010000". In the right pane, line 222 is "1A00=dword:00000000".

The status bar at the bottom reads: "Comparing file file:///tmp/diff/prompt\_user.reg with file file:///tmp/diff/automatic\_logon\_internet.reg" and "1 of 1 difference, 0 applied 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' for the process 'iexplore.exe'. The list includes:

- Base: 00400000, Name: iexplore.exe, Path: C:\Program Files\Internet Explorer\iexplore.exe
- Base: 00400000, Name: Normaliz.dll, Path: C:\WINDOWS\system32\Normaliz.dll
- Base: 00400000, Name: AcroIEFavC1.dll, Path: C:\Program Files\Adobe\Acrobat\MCIETAct\AcroIEFavC1.dll
- Base: 00400000, Name: Coupon\_Down, Path: C:\Program Files\Coupon Downloader\Coupon Downloader.dll
- Base: 00400000, Name: AcroIEHlp, Path: C:\Program Files\Adobe\Acrobat\AcroIEHlp\AcroIEHlp.dll
- Base: 00400000, Name: OCHelper, Path: C:\Program Files\Microsoft\One-Click-Lover.dll
- Base: 00400000, Name: OCHelperRes, Path: C:\Program Files\Microsoft\One-Click-Lover\OCHelperResource.dll
- Base: 00400000, Name: skypeplugin, Path: C:\WINDOWS\system32\skypeplugin.dll
- Base: 00400000, Name: swg, Path: C:\Program Files\Skype\Toolsbars\Internet Explorer\skypeplugin.dll
- Base: 00400000, Name: msis31, Path: C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic\swg\_en\_004439FF6761805.dll
- Base: 00400000, Name: GoogleToolb, Path: C:\Program Files\Google\Google Toolbar\Component\GoogleToolbarDynamic\_32\_8E471B27954D28F5.dll
- Base: 00400000, Name: SkypeFnr, Path: C:\Program Files\Skype\Toolsbars\Shared\SkypeFnr.dll
- Base: 00400000, Name: GoogleToolb, Path: C:\Program Files\Google\Google Toolbar\GoogleToolbar\_32.dll
- Base: 00400000, Name: Inetctl, Path: C:\WINDOWS\system32\inetctl.dll
- Base: 00400000, Name: pnfpllt, Path: C:\WINDOWS\system32\pnfpllt.dll
- Base: 00400000, Name: wshextl, Path: C:\WINDOWS\system32\wshextl.dll
- Base: 00400000, Name: jscrip1, Path: C:\WINDOWS\system32\jscrip1.dll
- Base: 00400000, Name: WINET1, Path: C:\WINDOWS\system32\WINET1.dll
- Base: 00400000, Name: ertut1, Path: C:\WINDOWS\system32\ertut1.dll
- Base: 00400000, Name: IEFNAME, Path: C:\WINDOWS\system32\IEFRAME.dll
- Base: 00400000, Name: inetcp1, Path: C:\WINDOWS\system32\inetcp1.dll
- Base: 00400000, Name: xpshins, Path: C:\Program Files\Internet Explorer\xpshins.dll
- Base: 00400000, Name: WINTHTP, Path: C:\Program Files\Internet Explorer\WINTHTP.dll
- Base: 00400000, Name: gdiplus, Path: C:\WINDOWS\system32\gdiplus.dll
- Base: 00400000, Name: uxtheme, Path: C:\WINDOWS\system32\uxtheme.dll
- Base: 00400000, Name: NETAPI32, Path: C:\WINDOWS\system32\NETAPI32.dll
- Base: 00400000, Name: Shimg, Path: C:\WINDOWS\system32\Shimg.dll
- Base: 00400000, Name: conct132, Path: C:\WINDOWS\system32\conct132.dll
- Base: 00400000, Name: DLFC, Path: C:\WINDOWS\system32\DLFC.dll
- Base: 00400000, Name: ADUPACK, Path: C:\WINDOWS\system32\ADUPACK.dll
- Base: 00400000, Name: hnetcs1, Path: C:\WINDOWS\system32\hnetcs1.dll
- Base: 00400000, Name: rsasenh, Path: C:\WINDOWS\system32\rsasenh.dll
- Base: 00400000, Name: J23sv, Path: C:\Program Files\Java\jre6\bin\J23sv.dll
- Base: 00400000, Name: JqsPlugin, Path: C:\Program Files\Java\jre6\bin\JqsPlugin.dll
- Base: 00400000, Name: Aclayers, Path: C:\WINDOWS\AppPatch\Aclayers.DLL
- Base: 00400000, Name: mscook, Path: C:\WINDOWS\system32\mscook.dll
- Base: 00400000, Name: wshcpip, Path: C:\WINDOWS\system32\wshcpip.dll
- Base: 00400000, Name: MS2MLP, Path: C:\WINDOWS\system32\MS2MLP.dll
- Base: 00400000, Name: ws2\_32, Path: C:\WINDOWS\system32\ws2\_32.dll
- Base: 00400000, Name: VFR, Path: C:\WINDOWS\system32\VFR.dll
- Base: 00400000, Name: SURLIB, Path: C:\WINDOWS\system32\SURLIB.dll
- Base: 00400000, Name: ntlanman, Path: C:\WINDOWS\system32\ntlanman.dll
- Base: 00400000, Name: NETAPI, Path: C:\WINDOWS\system32\NETAPI.dll
- Base: 00400000, Name: NETUI1, Path: C:\WINDOWS\system32\NETUI1.dll
- Base: 00400000, Name: NETUI0, Path: C:\WINDOWS\system32\NETUI0.dll
- Base: 00400000, Name: actxprxy, Path: C:\WINDOWS\system32\actxprxy.dll
- Base: 00400000, Name: sensapi, Path: C:\WINDOWS\system32\sensapi.dll
- Base: 00400000, Name: WINSPOOL, Path: C:\WINDOWS\system32\WINSPOOL.DRV
- Base: 00400000, Name: stl, Path: C:\WINDOWS\system32\stl.dll
- Base: 00400000, Name: msctf, Path: C:\WINDOWS\system32\msctf.dll
- Base: 00400000, Name: MSCTF, Path: C:\WINDOWS\system32\MSCTF.dll
- Base: 00400000, Name: msxsl15, Path: C:\WINDOWS\system32\msxsl15.dll
- Base: 00400000, Name: CFGMR32, Path: C:\WINDOWS\system32\CFGMR32.dll
- Base: 00400000, Name: CRPFTUL, Path: C:\WINDOWS\system32\CRPFTUL.dll
- Base: 00400000, Name: msctfime, Path: C:\WINDOWS\system32\msctfimeime
- Base: 00400000, Name: NLANG, Path: C:\WINDOWS\system32\NLANG.dll
- Base: 00400000, Name: cryptnet, Path: C:\WINDOWS\system32\cryptnet.dll
- Base: 00400000, Name: dcrprov, Path: C:\WINDOWS\system32\dcrprov.dll
- Base: 00400000, Name: davsint, Path: C:\WINDOWS\system32\davsint.dll
- Base: 00400000, Name: WINSTA, Path: C:\WINDOWS\system32\WINSTA.dll
- Base: 00400000, Name: WINSOCK, Path: C:\WINDOWS\system32\WINSOCK.dll
- Base: 00400000, Name: IMH32, Path: C:\WINDOWS\system32\IMH32.DLL
- Base: 00400000, Name: conct132, Path: C:\WINDOWS\system32\conct132.dll
- Base: 00400000, Name: cryptdll, Path: C:\WINDOWS\system32\cryptdll.dll
- Base: 00400000, Name: RRSDDL, Path: C:\WINDOWS\system32\RRSDDL.dll
- Base: 00400000, Name: ntrshu1, Path: C:\WINDOWS\system32\ntrshu1.dll
- Base: 00400000, Name: USERENV, Path: C:\WINDOWS\system32\USERENV.dll
- Base: 00400000, Name: RTL, Path: C:\WINDOWS\system32\RTL.dll
- Base: 00400000, Name: WINTNT, Path: C:\WINDOWS\system32\WINTNT.dll
- Base: 00400000, Name: PSPT, Path: C:\WINDOWS\system32\PSPT.dll
- Base: 00400000, Name: WINTRUST, Path: C:\WINDOWS\system32\WINTRUST.dll
- Base: 00400000, Name: Inagapi, Path: C:\WINDOWS\system32\Inagapi.dll
- Base: 00400000, Name: IPHLPAPI, Path: C:\WINDOWS\system32\IPHLPAPI.DLL
- Base: 00400000, Name: adsiidoc, Path: C:\WINDOWS\system32\adsiidoc.dll
- Base: 00400000, Name: rtut11s, Path: C:\WINDOWS\system32\rtut11s.dll
- Base: 00400000, Name: rasan, Path: C:\WINDOWS\system32\rsasan.dll
- Base: 00400000, Name: TFP132, Path: C:\WINDOWS\system32\TFP132.dll
- Base: 00400000, Name: MSFSPT32, Path: C:\WINDOWS\system32\MSFSPT32.dll
- Base: 00400000, Name: WTSHP132, Path: C:\WINDOWS\system32\WTSHP132.dll
- Base: 00400000, Name: WLDAP32, Path: C:\WINDOWS\system32\WLDAP32.dll
- Base: 00400000, Name: CLBCATQ, Path: C:\WINDOWS\system32\CLBCATQ.DLL
- Base: 00400000, Name: CORRES, Path: C:\WINDOWS\system32\CORRES.dll
- Base: 00400000, Name: DLXOUT32, Path: C:\WINDOWS\system32\DLXOUT32.dll
- Base: 00400000, Name: conct132, Path: C:\WINDOWS\system32\conct132.dll
- Base: 00400000, Name: GDI32, Path: C:\WINDOWS\system32\GDI32.dll
- Base: 00400000, Name: SETAPI, Path: C:\WINDOWS\system32\SETAPI.dll

The taskbar shows several open applications including start, OllyDbg, Program Files, SystemStateSuite, ResEdit, C:\Doc..., IDA Pro v6.0.10..., New Tab - Wind..., ShoWin 2.00, Process Explorer..., C:\WINDOWS\sys..., ie\_dll.txt - Notepad, 2.bit - Notepad, OllyDbg - iexplor..., and a clock showing 3:35 AM.





# 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](http://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

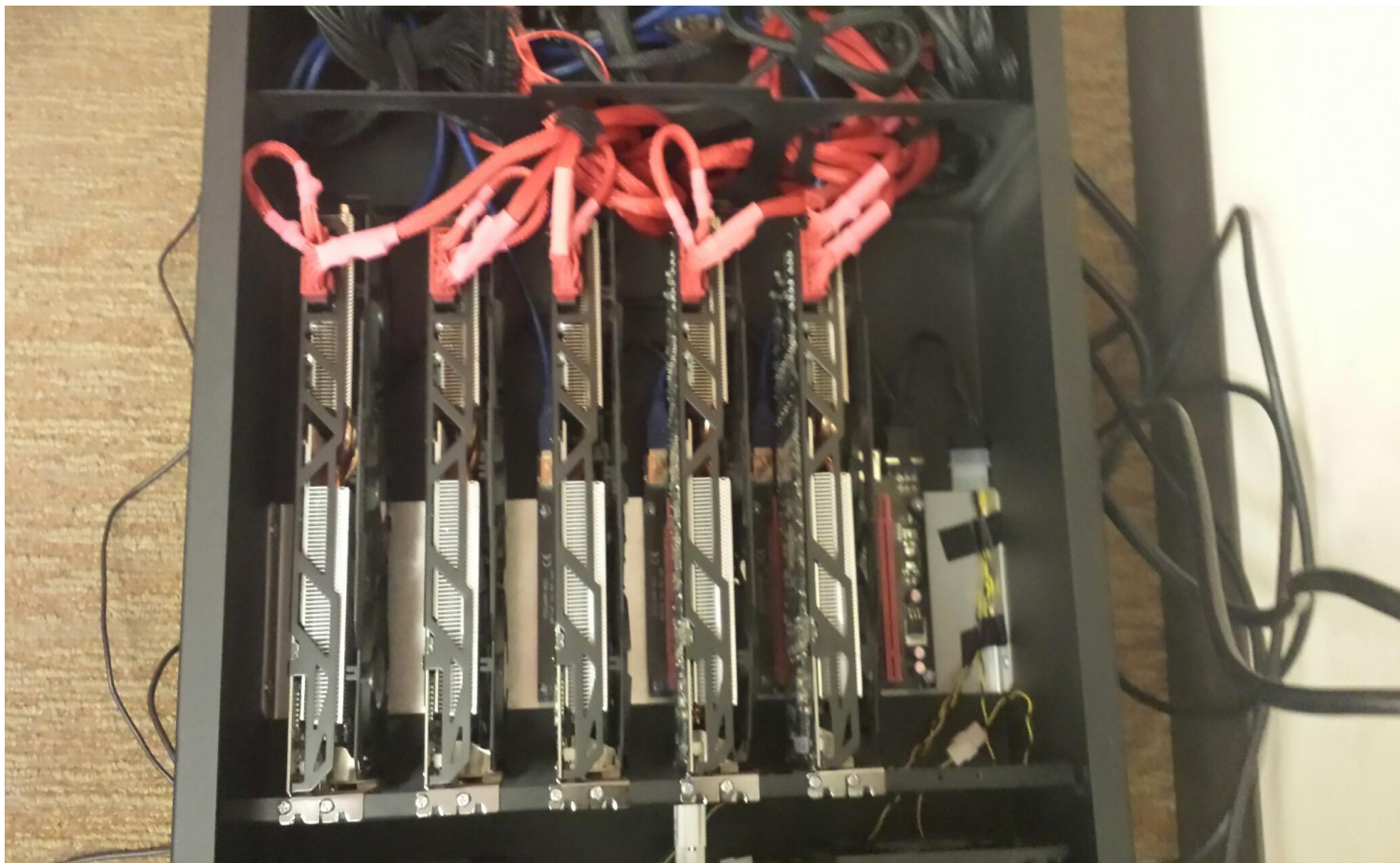
## **Hash cracking**

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 realm="SMB" Search

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	Count							
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"
		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 ?

