

# 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 attackers 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

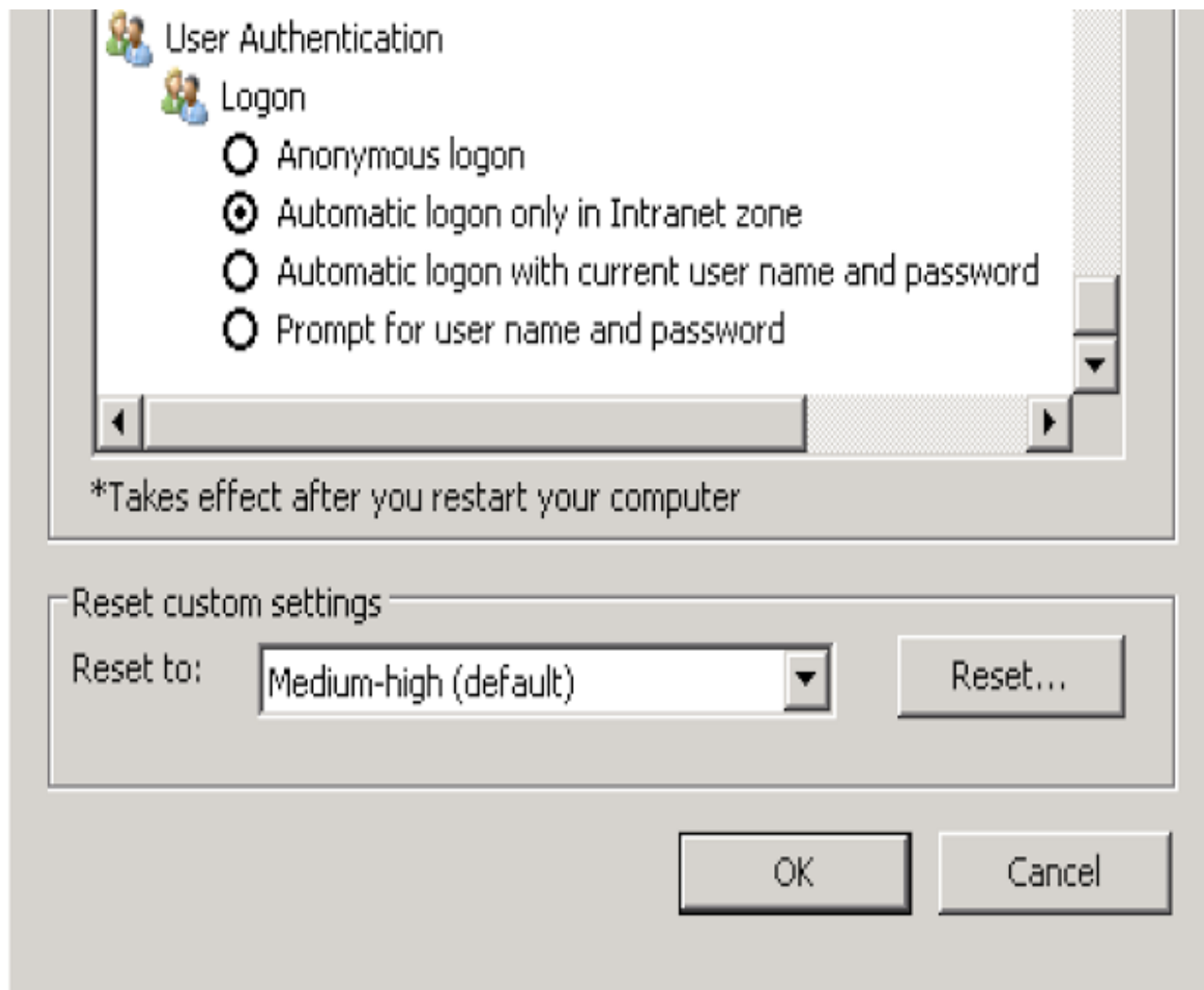
Main Assumption is Attacker is on the victim's network.

## 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

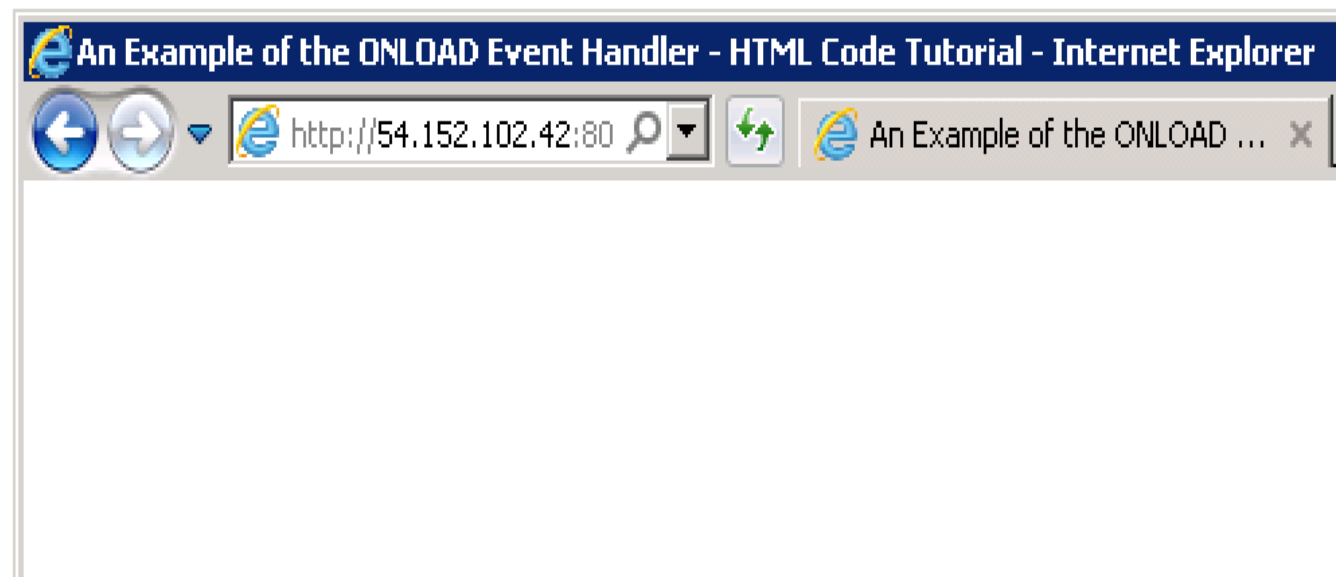
There's actually an IE setting for this :



# 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

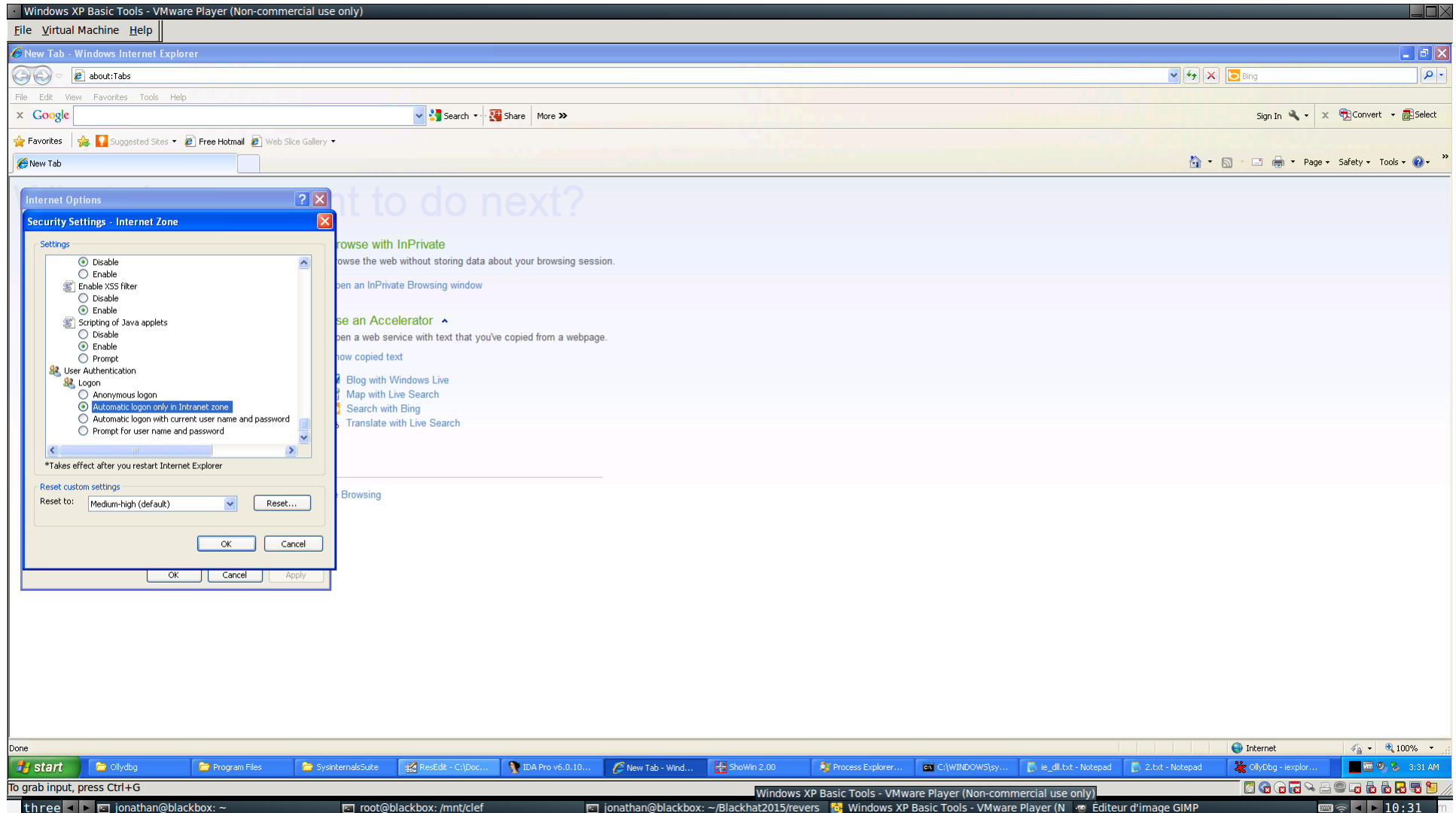
```
NTLM Message Type: NTLMSSP_AUTH (0x00000003)
⊕ Lan Manager Response: 0000000000000000000000000000000000000000000000000000000000000000
  NTLM Client Challenge: 0000000000000000
⊖ NTLM Response: 6c814b0a16fbbc86ea17370ed34521680101000000000000...
  Length: 286
  Maxlen: 286
  Offset: 162
⊖ NTLMv2 Response: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



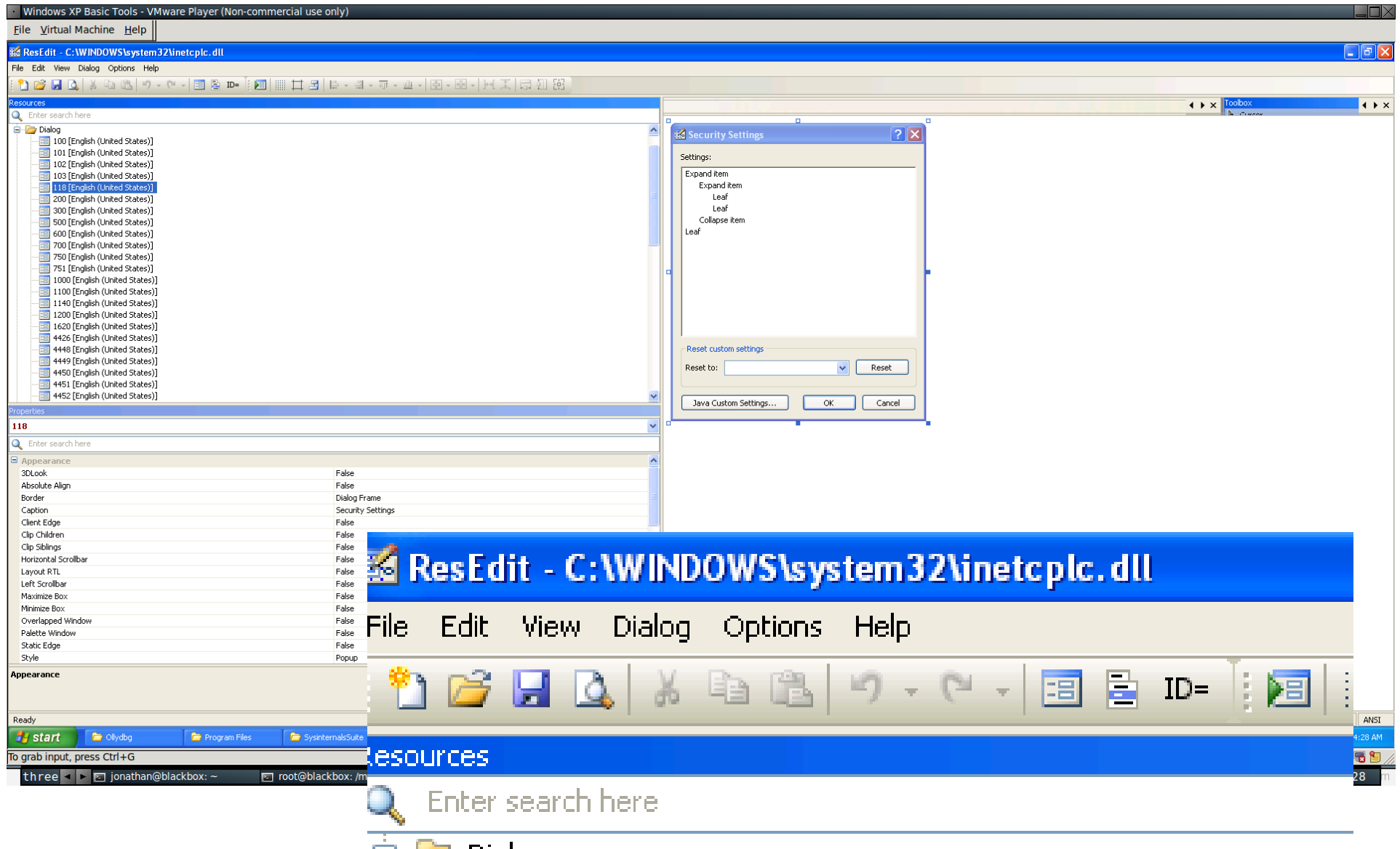
# Root Cause Analysis





[illegible]

# Root Cause Analysis



# Diffing the registry

The screenshot shows the Kompare application window. The top menu bar includes File, Difference, Settings, and Help. Below the menu is a toolbar with 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 main window is divided into several panes. The 'Navigation' pane on the left shows the 'Source Folder' and 'Destination Folder' both set to '/tmp/diff/'. The 'Source File' pane shows 'prompt\_u...' and the 'Destination File' pane shows 'automatic\_logon\_internet.reg'. The 'Source Line' and 'Destination Line' panes both show '222', and the 'Difference' pane shows 'Changed 1 line'. The main diff view shows two side-by-side text files. The left file is 'prompt\_user.reg' and the right file is 'automatic\_logon\_internet.reg'. Both files contain registry values for 'HKEY\_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 files. In the left file, line 222 is '"1A00"=dword:00010000'. In the right file, line 222 is '"1A00"=dword:00000000'. The status bar at the bottom indicates 'Comparing file file:///tmp/diff/prompt\_user.reg with file:///tmp/diff/automatic\_logon\_internet.reg' and '1 of 1 difference, 0 applied 1 of 1 file'.

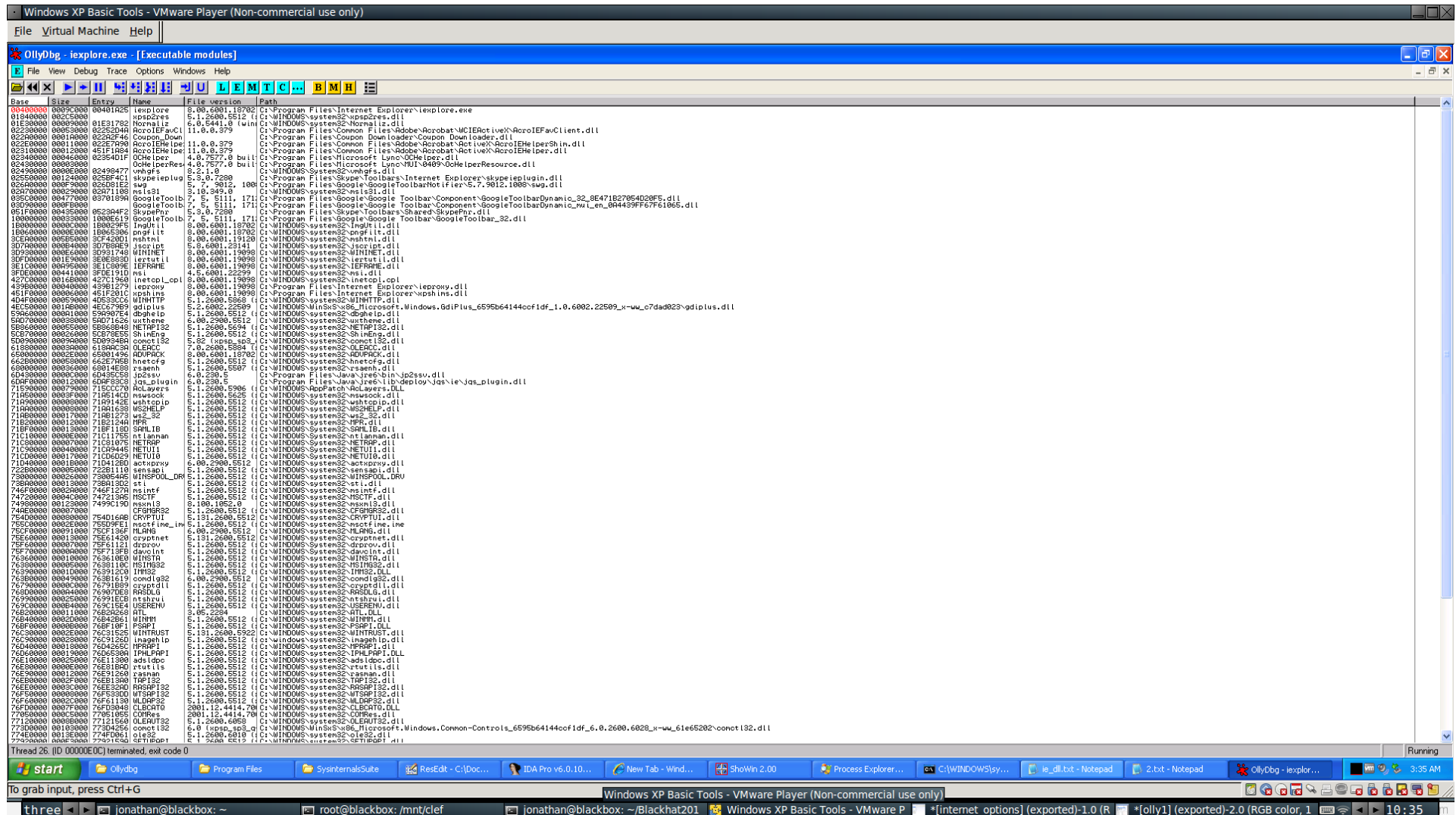
Source Folder	Destination Folder	Source File	Destination File	Source Line	Destination Line	Difference
/tmp/diff/	/tmp/diff/	prompt_u...	automatic_logon_internet.reg	222	222	Changed 1 line

```
prompt_user.reg
187 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
188 @="
189 "DisplayName"="Internet"
190 "Description"="This zone contains all websites you haven't placed in o
191 "Icon"="inetctl.cpl#001313"
192 "CurrentLevel"=dword:00000000
193 "MinLevel"=dword:00011000
194 "RecommendedLevel"=dword:00011000
195 "Flags"=dword:00000001
196 "1001"=dword:00000001
197 "1004"=dword:00000003
198 "1200"=dword:00000000
199 "1201"=dword:00000003
200 "1206"=dword:00000003
201 "1400"=dword:00000000
202 "1402"=dword:00000000
203 "1405"=dword:00000000
204 "1406"=dword:00000003
205 "1407"=dword:00000001
206 "1601"=dword:00000000
207 "1604"=dword:00000000
208 "1605"=dword:00000000
209 "1606"=dword:00000000
210 "1607"=dword:00000003
211 "1608"=dword:00000000
212 "1609"="0"
213 "1800"=dword:00000001
214 "1802"=dword:00000000
215 "1803"=dword:00000000
216 "1804"=dword:00000001
217 "1805"=dword:00000001
218 "1806"=dword:00000001
219 "1807"=dword:00000001
220 "1808"=dword:00000000
221 "1809"=dword:00000000
222 "1A00"=dword:00010000
223 "1A02"=dword:00000000
224 "1A03"=dword:00000000
225 "1A04"=dword:00000003
226 "1A05"=dword:00000001
227 "1A06"=dword:00000000
228 "1A10"=dword:00000001
229 "1C00"=dword:00010000

automatic_logon_internet.reg
187 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3]
188 @="
189 "DisplayName"="Internet"
190 "Description"="This zone contains all websites you haven't placed in other zones"
191 "Icon"="inetctl.cpl#001313"
192 "CurrentLevel"=dword:00000000
193 "MinLevel"=dword:00011000
194 "RecommendedLevel"=dword:00011000
195 "Flags"=dword:00000001
196 "1001"=dword:00000001
197 "1004"=dword:00000003
198 "1200"=dword:00000000
199 "1201"=dword:00000003
200 "1206"=dword:00000003
201 "1400"=dword:00000000
202 "1402"=dword:00000000
203 "1405"=dword:00000000
204 "1406"=dword:00000003
205 "1407"=dword:00000001
206 "1601"=dword:00000000
207 "1604"=dword:00000000
208 "1605"=dword:00000000
209 "1606"=dword:00000000
210 "1607"=dword:00000003
211 "1608"=dword:00000000
212 "1609"="0"
213 "1800"=dword:00000001
214 "1802"=dword:00000000
215 "1803"=dword:00000000
216 "1804"=dword:00000001
217 "1805"=dword:00000001
218 "1806"=dword:00000001
219 "1807"=dword:00000001
220 "1808"=dword:00000000
221 "1809"=dword:00000000
222 "1A00"=dword:00000000
223 "1A02"=dword:00000000
224 "1A03"=dword:00000000
225 "1A04"=dword:00000003
226 "1A05"=dword:00000001
227 "1A06"=dword:00000000
228 "1A10"=dword:00000001
229 "1C00"=dword:00010000
```

Comparing file file:///tmp/diff/prompt\_user.reg with file:///tmp/diff/automatic\_logon\_internet.reg 1 of 1 difference, 0 applied 1 of 1 file

# Tracing





# Tracing

[illegible]

# 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**

Inetcpplc.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

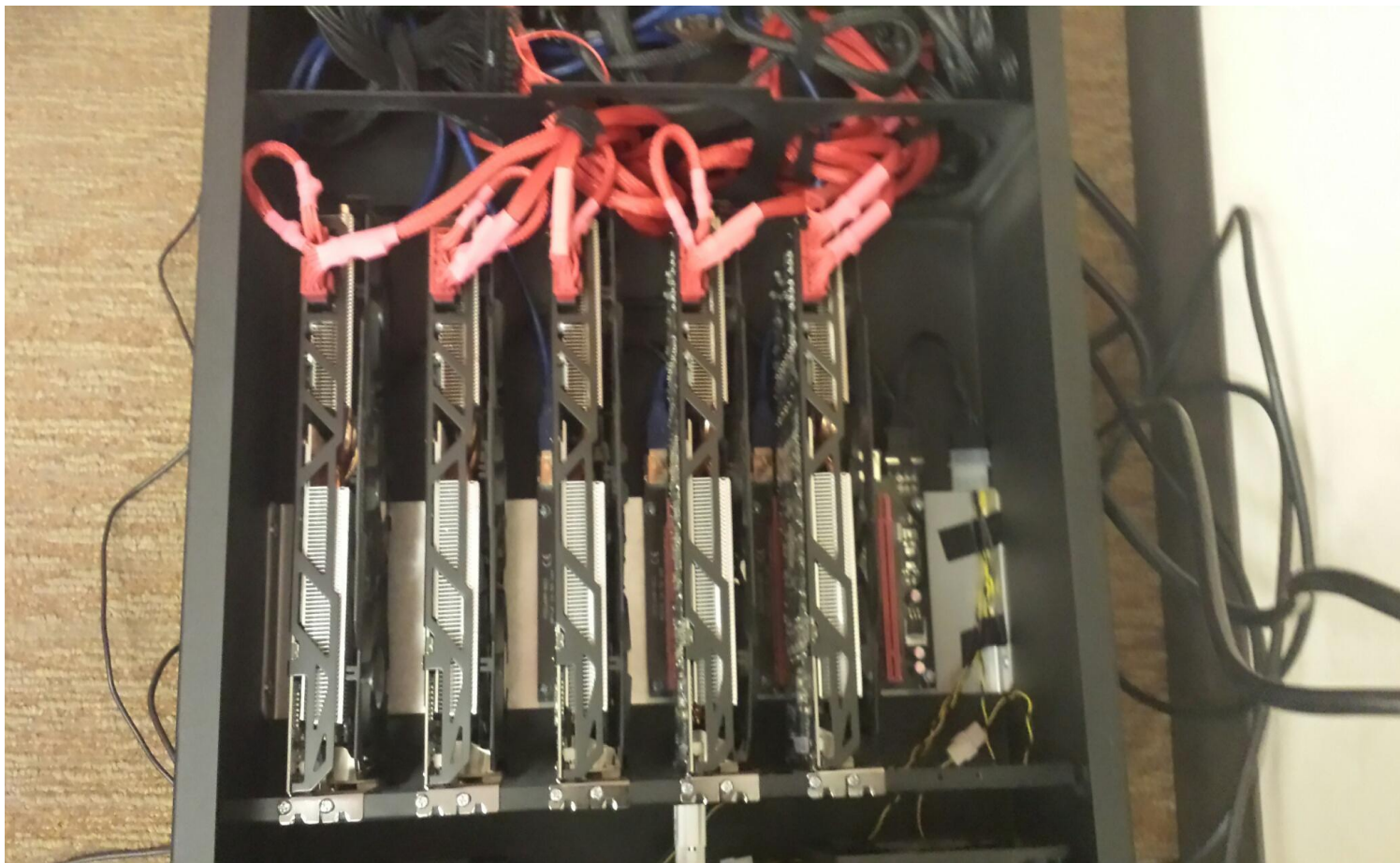
## **Hash cracking**

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



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

Services

HTTP

896

HTTP Alternate

574

HTTPS

33

HTTPS Alternate

3

Top Countries

India

1,273

China

118

Taiwan

102

Mexico

5

Hong Kong

3


401 Unauthorized

219.85.116.80

Linux 2.6.x

Sony Network Taiwan Limited

Added on 12.01.2014

 Taipei

219-85-116-80-adsl-TPE.dynamic.sonet.net.tw

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"

401 Unauthorized

118.166.81.94

CHTD, Chunghwa Telecom Co., Ltd.

Added on 12.01.2014

 Taipei

118-166-81-94.dynamic.hinet.net

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"

401 Unauthorized

115.244.226.75

BSES TeleCom Limited

Added on 01.01.2014

 Pondicherry

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 ?

