ONCE MORE UNTO THE DATA BREACH

Steve Miller

2,122+ data breaches in 2014

-Verizon DBIR

The average cost of a data breach will be $150 million by 2020

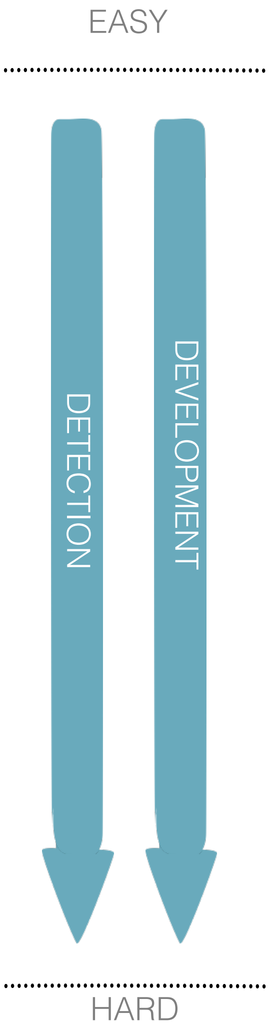
-Juniper Research

Today I will pontificate on…

- The attacker toolset ⚔
- A data breach ◕︵◕
- Common failures ಠ_ಠ
- Changing the equation ∆

The evolving attacker toolset

Progression of C2 protocols

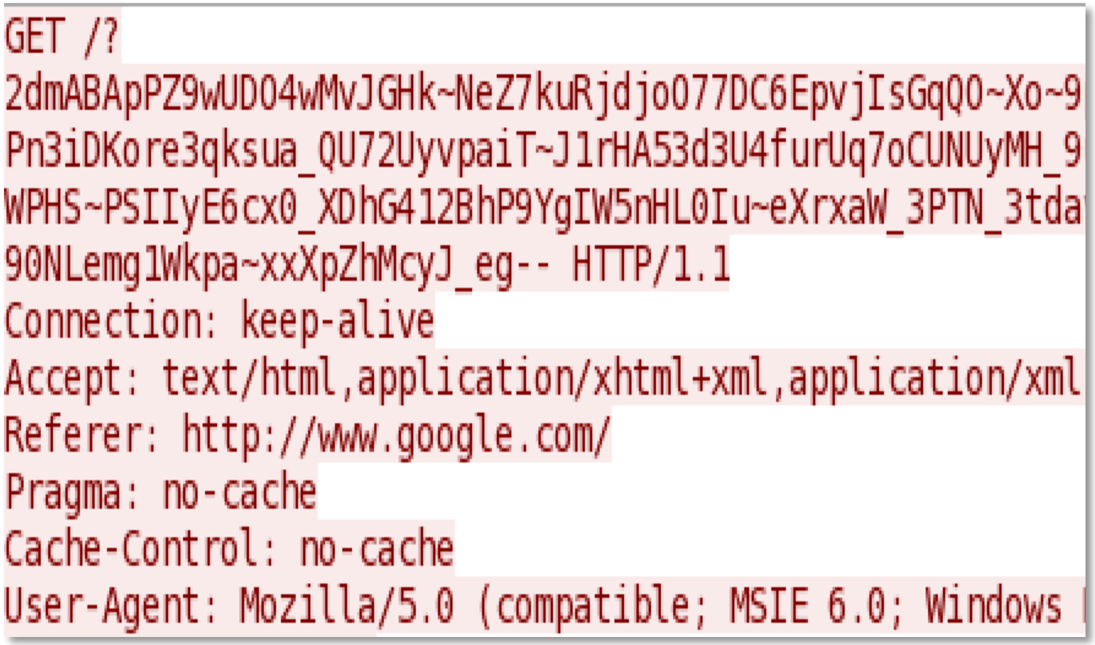


HTTP

Self-signed SSL

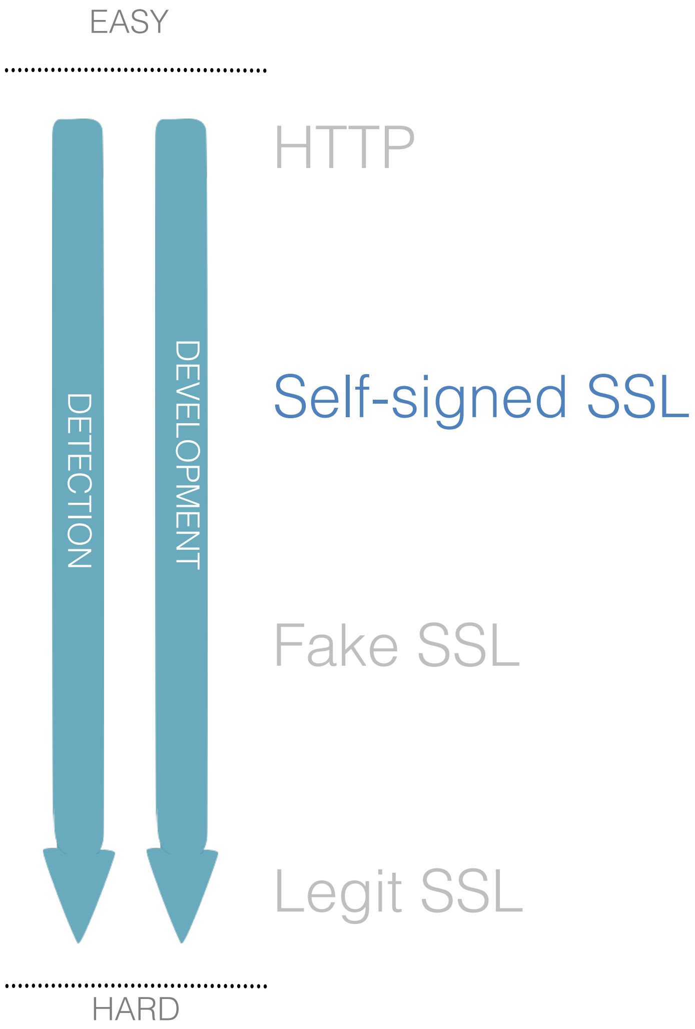
Fake SSL

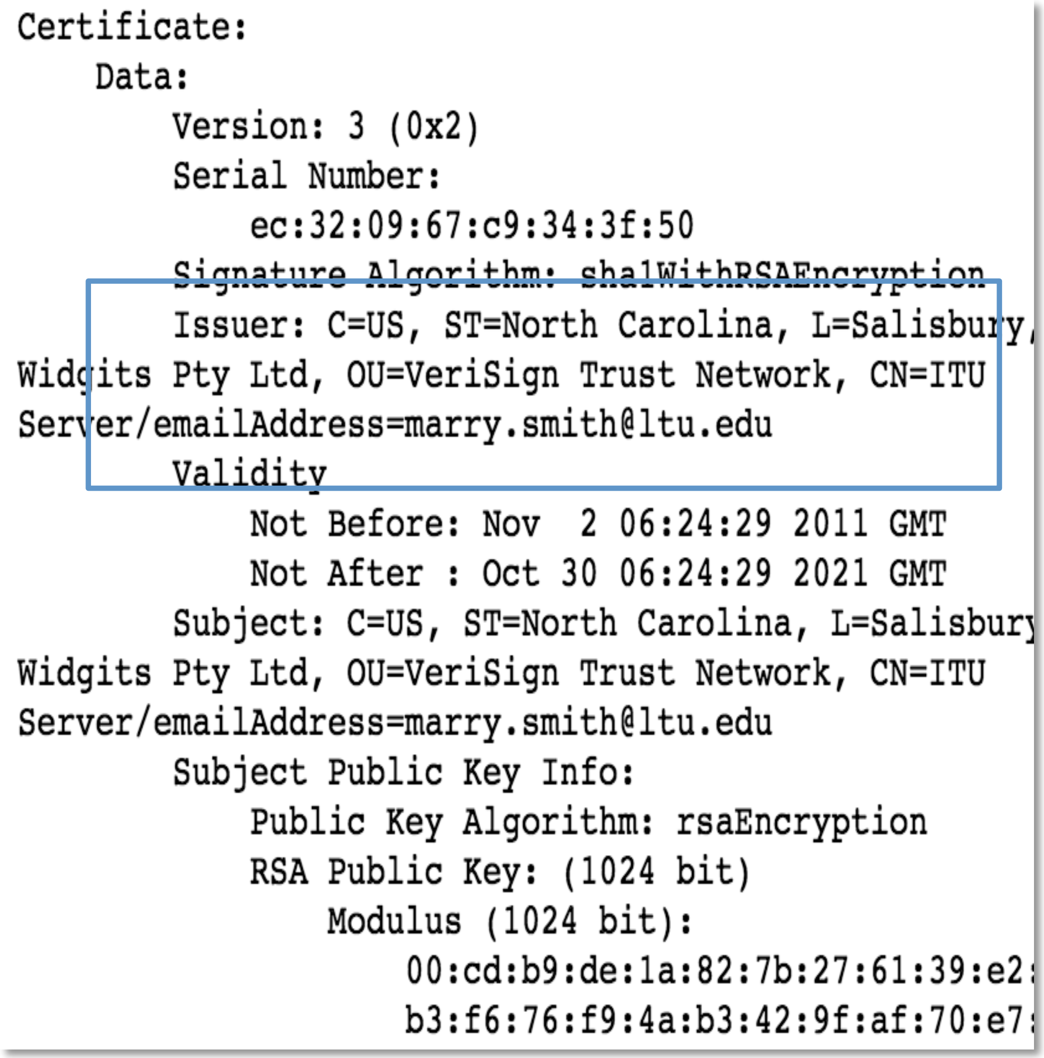
Legit SSL



```
GET /?
2dmABApPZ9wUD04wMvJGHk~NeZ7kuRjdjo077DC6EpvjIsGqQ0~Xo~9
Pn3iDKore3qksua_QU72UyvpaiT~J1rHA53d3U4furUq7oCUNUyMH_9
WPHS~PSIIyE6cx0_XDhG412BhP9YgIW5nHL0Iu~eXrxaW_3PTN_3tda
90NLemg1Wkpa~xxXpZhMcyJ_eg-- HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows
```

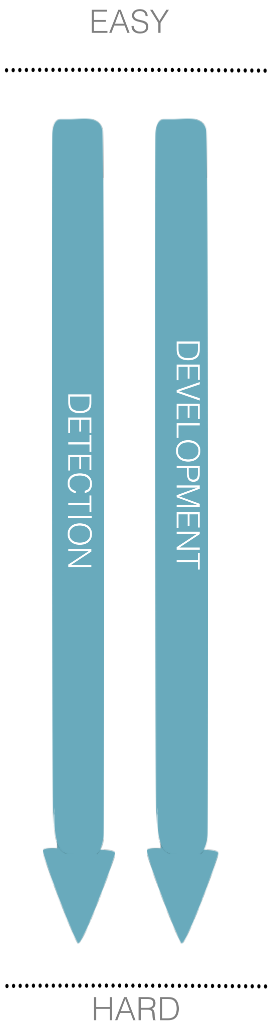
Progression of C2 protocols





```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ec:32:09:67:c9:34:3f:50
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=North Carolina, L=Salisbury,
Widgits Pty Ltd, OU=VeriSign Trust Network, CN=ITU
Server/emailAddress=marry.smith@ltu.edu
        Validity
            Not Before: Nov  2 06:24:29 2011 GMT
            Not After : Oct 30 06:24:29 2021 GMT
        Subject: C=US, ST=North Carolina, L=Salisbury
Widgits Pty Ltd, OU=VeriSign Trust Network, CN=ITU
Server/emailAddress=marry.smith@ltu.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:cd:b9:de:1a:82:7b:27:61:39:e2:
                    b3:f6:76:f9:4a:b3:42:9f:af:70:e7:
```

Progression of C2 protocols

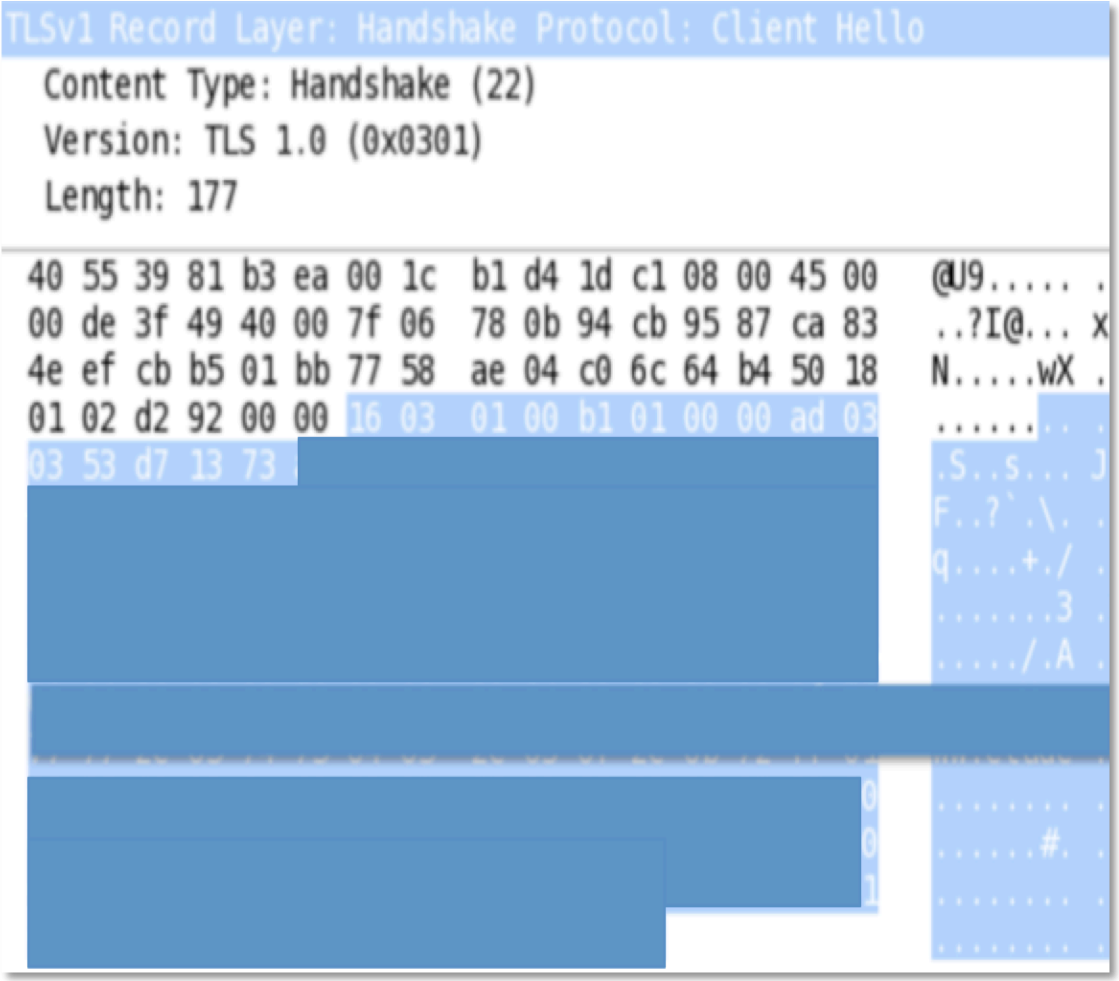


HTTP

Self-signed SSL

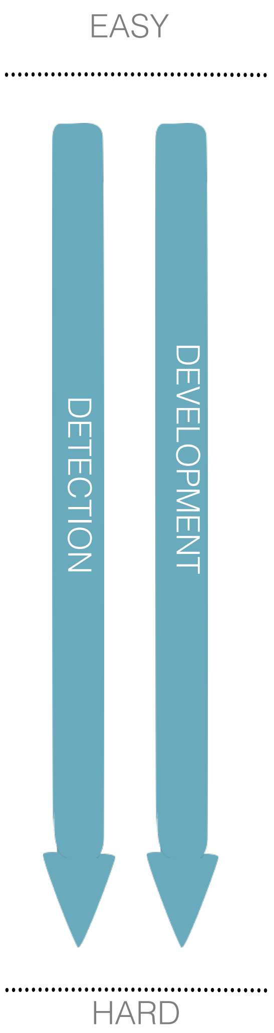
Fake SSL

Legit SSL



```
TLSv1 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 177

40 55 39 81 b3 ea 00 1c  b1 d4 1d c1 08 00 45 00   @U9..... .
00 de 3f 49 40 00 7f 06  78 0b 94 cb 95 87 ca 83   ..?I@... x
4e ef cb b5 01 bb 77 58  ae 04 c0 6c 64 b4 50 18   N.....wX .
01 02 d2 92 00 00 16 03  01 00 b1 01 00 00 ad 03   ...... .. .
03 53 d7 13 73 [redacted]                          .S..s... J
                                                   F..?`.\. .
                                                   q....+./ .
                                                   ........3 .
                                                   ...../.A .
[redacted]
                                                   ........ .
                                                   ......#. .
                                                   ........ .
                                                   ........ .
```

Progression of C2 protocols



EASY

DETECTION

DEVELOPMENT

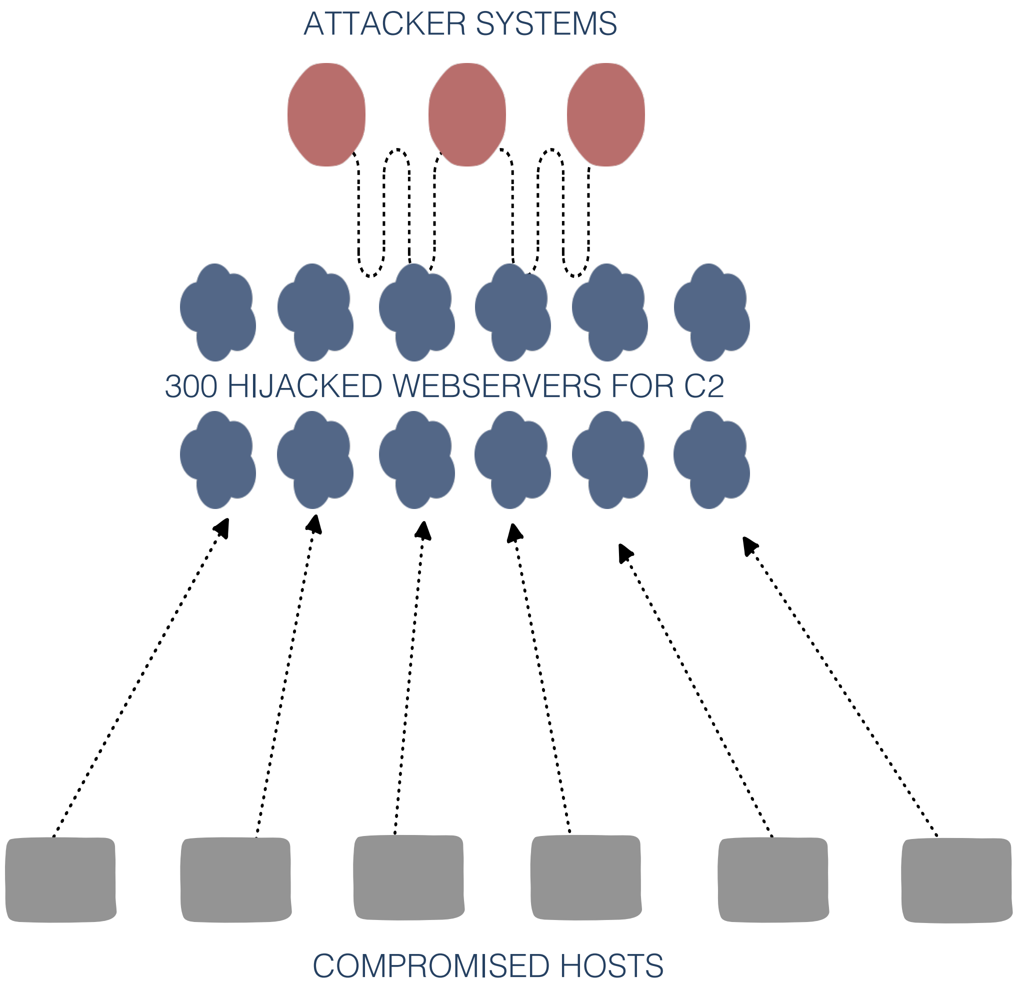
HARD

HTTP

Self-signed SSL

Fake SSL

Legit SSL



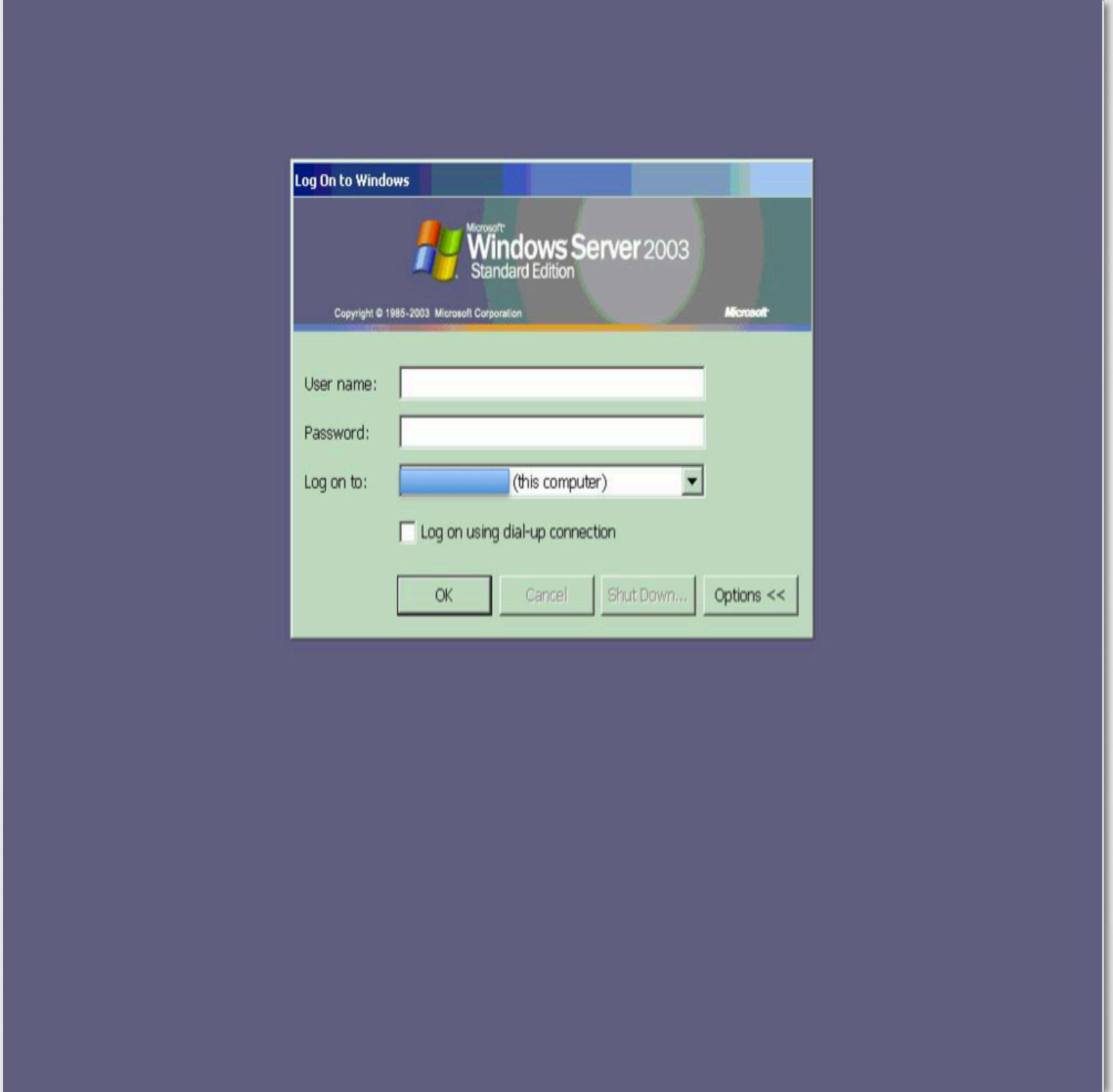
ATTACKER SYSTEMS

300 HIJACKED WEBSERVERS FOR C2

COMPROMISED HOSTS

The exemplar data breach

◕︵◕



Log On to Windows
Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft

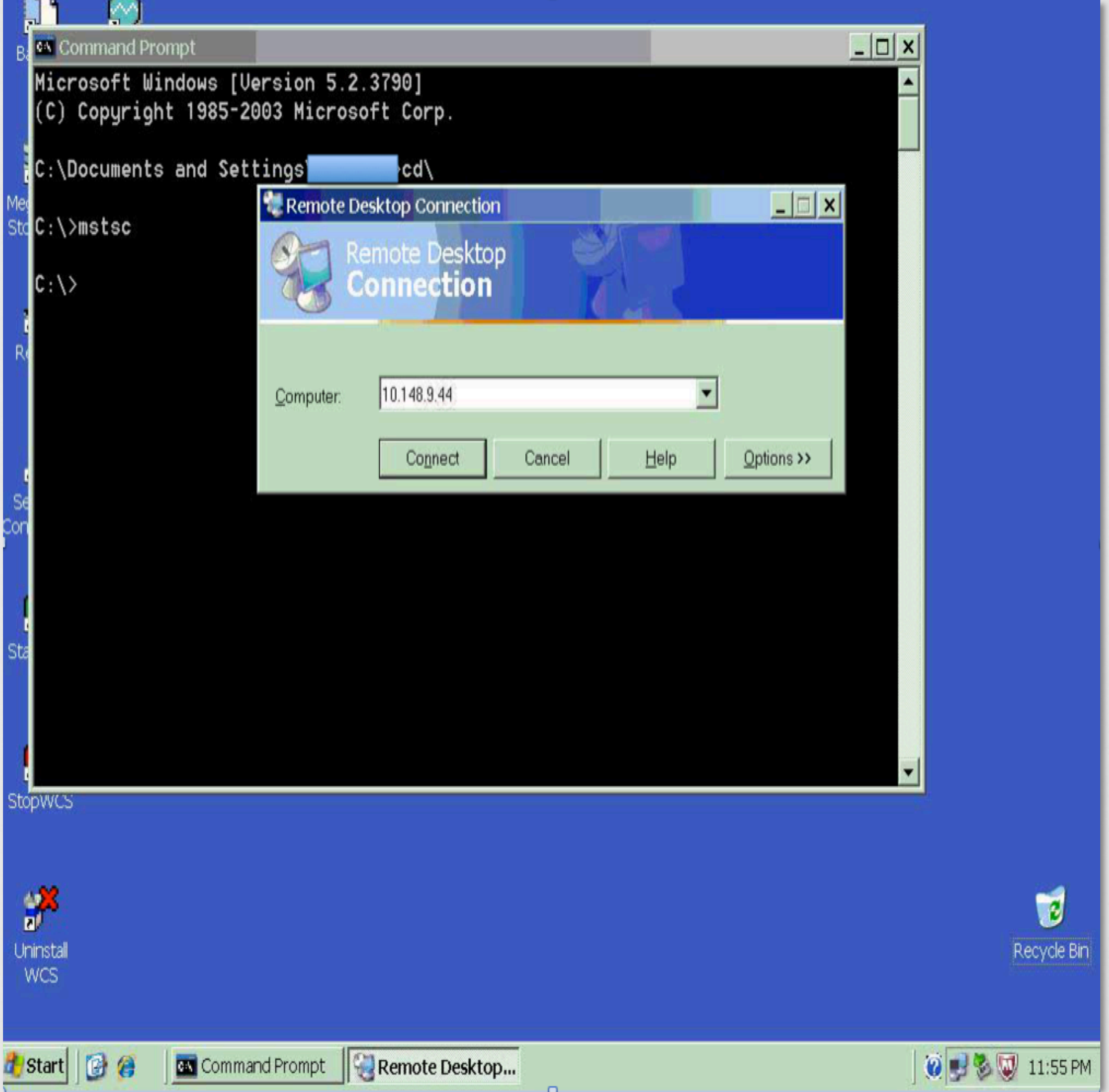
User name:

Password:

Log on to: (this computer)

☐ Log on using dial-up connection

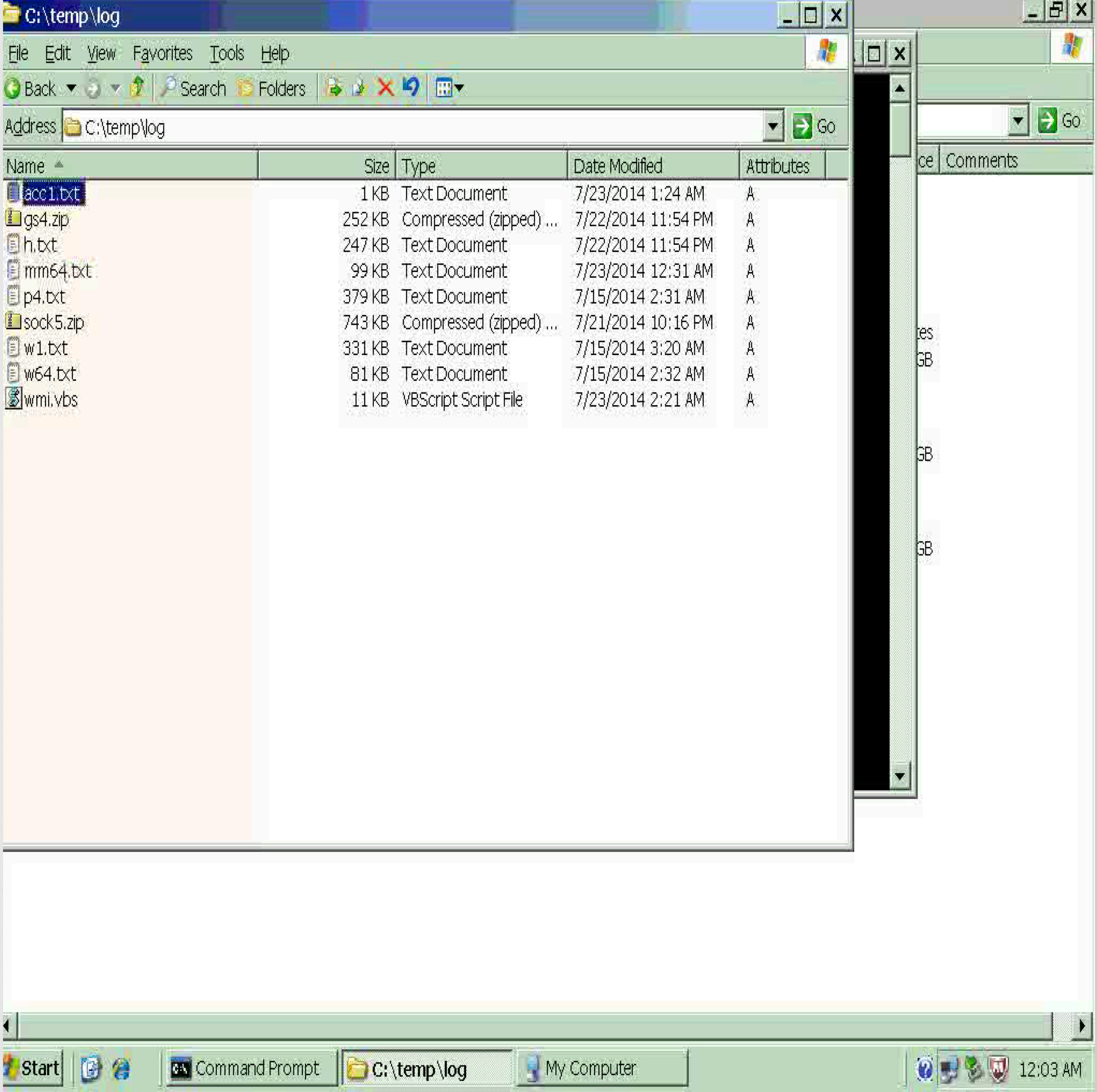
OK
Cancel
Shut Down...
Options <<



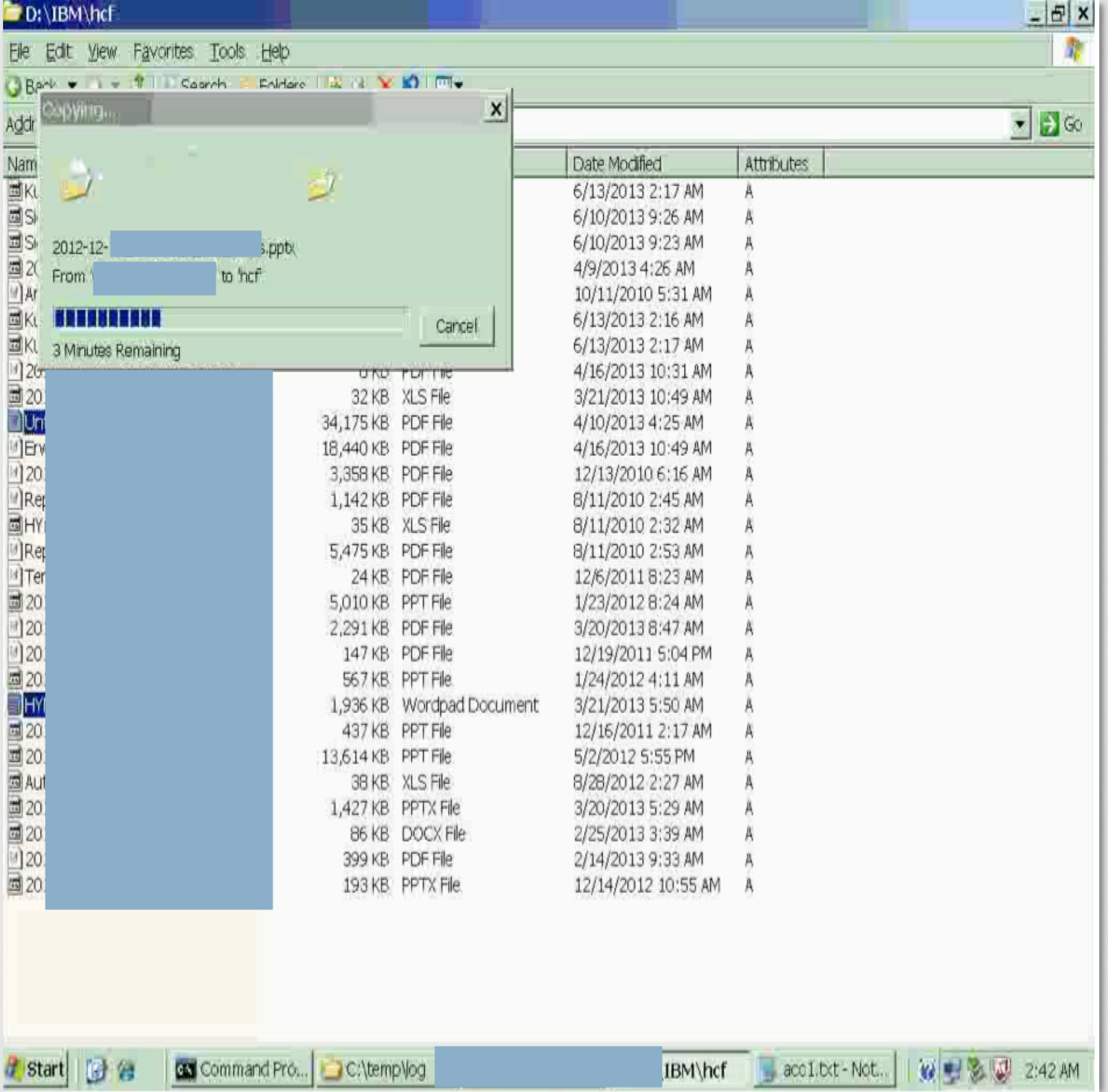
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\[redacted]>cd\

C:\>mstsc

C:\>
```

Remote Desktop Connection

Computer: 10.148.9.44



Name	Size	Type	Date Modified	Attributes
acc1.txt	1 KB	Text Document	7/23/2014 1:24 AM	A
gs4.zip	252 KB	Compressed (zipped) ...	7/22/2014 11:54 PM	A
h.txt	247 KB	Text Document	7/22/2014 11:54 PM	A
mm64.txt	99 KB	Text Document	7/23/2014 12:31 AM	A
p4.txt	379 KB	Text Document	7/15/2014 2:31 AM	A
sock5.zip	743 KB	Compressed (zipped) ...	7/21/2014 10:16 PM	A
w1.txt	331 KB	Text Document	7/15/2014 3:20 AM	A
w64.txt	81 KB	Text Document	7/15/2014 2:32 AM	A
wmi.vbs	11 KB	VBScript Script File	7/23/2014 2:21 AM	A



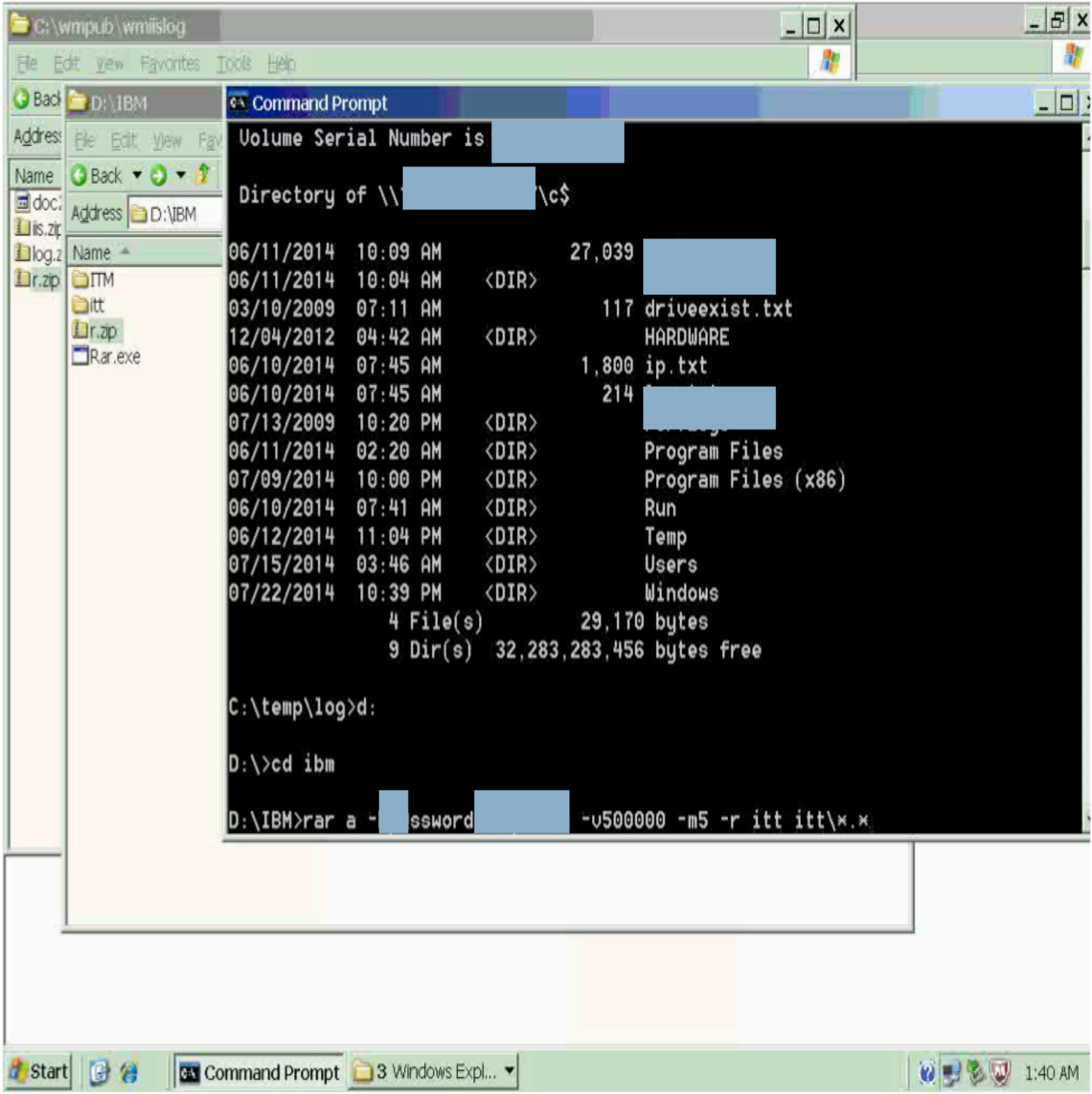
Copying...

2012-12-[redacted]s.pptx

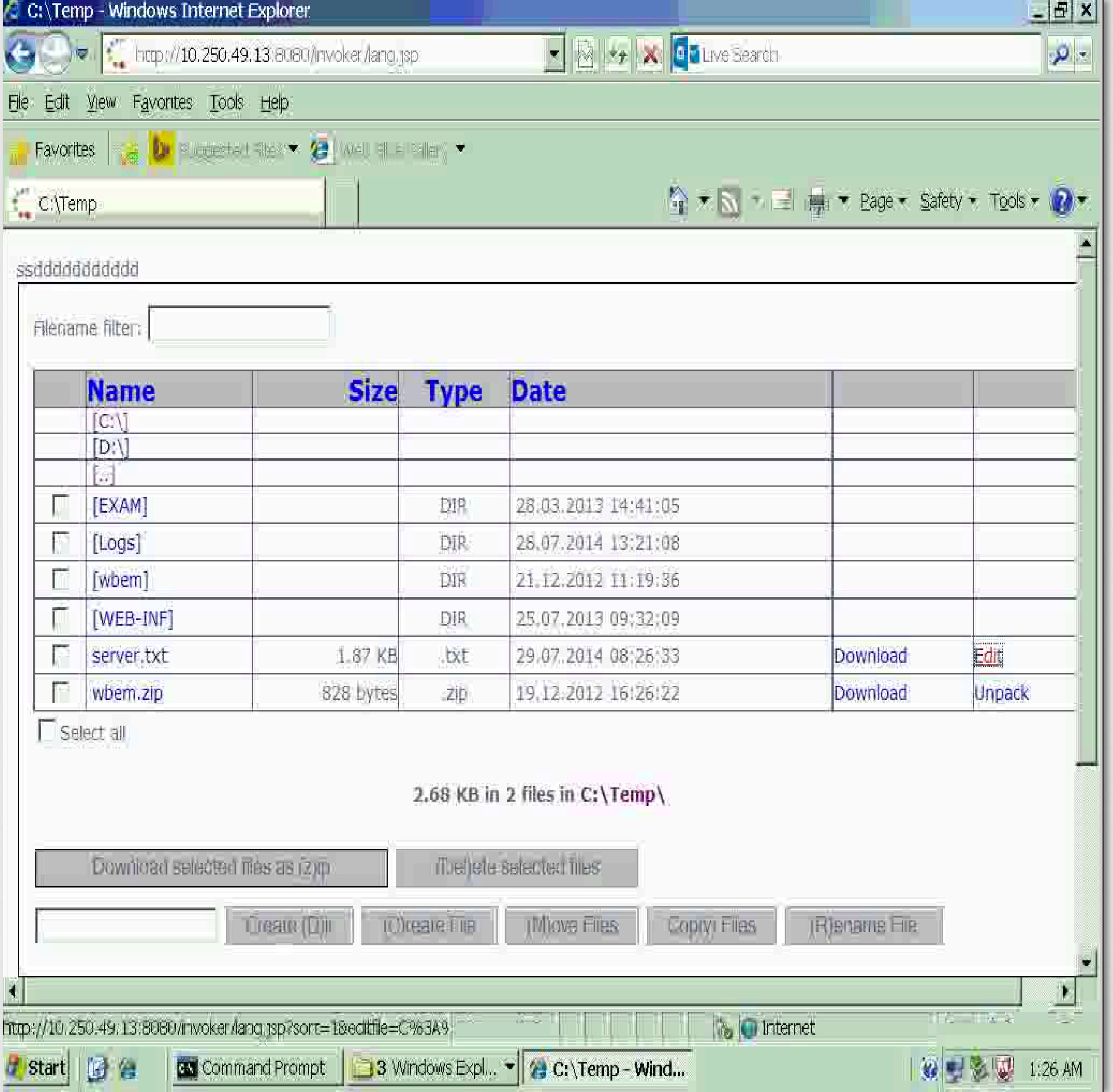
From '[redacted] to 'hcf'

3 Minutes Remaining

Nam			Date Modified	Attributes
Kl [redacted]			6/13/2013 2:17 AM	A
Sl [redacted]			6/10/2013 9:26 AM	A
Sl [redacted]			6/10/2013 9:23 AM	A
20 [redacted]			4/9/2013 4:26 AM	A
Ar [redacted]			10/11/2010 5:31 AM	A
Kl [redacted]			6/13/2013 2:16 AM	A
Kl [redacted]			6/13/2013 2:17 AM	A
20 [redacted]	0 KB	PDF File	4/16/2013 10:31 AM	A
20 [redacted]	32 KB	XLS File	3/21/2013 10:49 AM	A
Un [redacted]	34,175 KB	PDF File	4/10/2013 4:25 AM	A
Erv [redacted]	18,440 KB	PDF File	4/16/2013 10:49 AM	A
20 [redacted]	3,358 KB	PDF File	12/13/2010 6:16 AM	A
Rep [redacted]	1,142 KB	PDF File	8/11/2010 2:45 AM	A
HY [redacted]	35 KB	XLS File	8/11/2010 2:32 AM	A
Rep [redacted]	5,475 KB	PDF File	8/11/2010 2:53 AM	A
Ter [redacted]	24 KB	PDF File	12/6/2011 8:23 AM	A
20 [redacted]	5,010 KB	PPT File	1/23/2012 8:24 AM	A
20 [redacted]	2,291 KB	PDF File	3/20/2013 8:47 AM	A
20 [redacted]	147 KB	PDF File	12/19/2011 5:04 PM	A
20 [redacted]	567 KB	PPT File	1/24/2012 4:11 AM	A
HY [redacted]	1,936 KB	Wordpad Document	3/21/2013 5:50 AM	A
20 [redacted]	437 KB	PPT File	12/16/2011 2:17 AM	A
20 [redacted]	13,614 KB	PPT File	5/2/2012 5:55 PM	A
Aut [redacted]	38 KB	XLS File	8/28/2012 2:27 AM	A
20 [redacted]	1,427 KB	PPTX File	3/20/2013 5:29 AM	A
20 [redacted]	86 KB	DOCX File	2/25/2013 3:39 AM	A
20 [redacted]	399 KB	PDF File	2/14/2013 9:33 AM	A
20 [redacted]	193 KB	PPTX File	12/14/2012 10:55 AM	A



```
 Volume Serial Number is [redacted]

 Directory of \\[redacted]\c$

06/11/2014  10:09 AM            27,039 [redacted]
06/11/2014  10:04 AM    <DIR>
03/10/2009  07:11 AM               117 driveexist.txt
12/04/2012  04:42 AM    <DIR>          HARDWARE
06/10/2014  07:45 AM             1,800 ip.txt
06/10/2014  07:45 AM               214 [redacted]
07/13/2009  10:20 PM    <DIR>
06/11/2014  02:20 AM    <DIR>          Program Files
07/09/2014  10:00 PM    <DIR>          Program Files (x86)
06/10/2014  07:41 AM    <DIR>          Run
06/12/2014  11:04 PM    <DIR>          Temp
07/15/2014  03:46 AM    <DIR>          Users
07/22/2014  10:39 PM    <DIR>          Windows
               4 File(s)         29,170 bytes
               9 Dir(s)  32,283,283,456 bytes free

C:\temp\log>d:

D:\>cd ibm

D:\IBM>rar a -[redacted]ssword[redacted] -v500000 -m5 -r itt itt\*.*
```



http://10.250.49.13:8080/invoker/lang.jsp

ssdddddddddd

	Name	Size	Type	Date		
	[C:\]					
	[D:\]					
	[..]					
□	[EXAM]		DIR	28.03.2013 14:41:05		
□	[Logs]		DIR	26.07.2014 13:21:08		
□	[wbem]		DIR	21.12.2012 11:19:36		
□	[WEB-INF]		DIR	25.07.2013 09:32:09		
□	server.txt	1.87 KB	.txt	29.07.2014 08:26:33	Download	Edit
□	wbem.zip	828 bytes	.zip	19.12.2012 16:26:22	Download	Unpack

□ Select all

2.68 KB in 2 files in C:\Temp\

http://10.250.49.13:8080/invoker/lang.jsp?sort=1&editfile=C%3A%

The data stolen

- The attacker was interested in **fuel cells**
- Key words in file names:

  - Shipping plan
  - Project marketing
  - Distribution providers
  - Market strategy
  - Regional sales plan
  - Advertising
  - 2015 marketing
  - Product roadmap

  - ~~Technical details~~
  - ~~Schematics~~
  - ~~Engineering diagrams~~
  - ~~CAD files~~

The numbers

- 20 compromised systems
- 10 compromised accounts
- 7 custom utilities
- 1 piece of malware
- “Anti-forensics” techniques

Common failure points

ಠ_ಠ

ಠ_ಠ

Sometimes it’s hard to…

- Patch vulnerabilities
- Know all your egress points
- Block IPs and domains
- Reset accounts

Changing the equation

Δ

What if the attackers are kinda like us?

- They divide tasks groups
- They have their own recruiting departments
- They have goals and KPIs
- They outsource work when it makes sense
- They love their jobs
- They research and continuously innovate

What are some good assumptions?

- The attack surface is bigger than think
- Attackers evolve way faster than you do
- Your goal is to not to prevent the breach

How do I become more nimble?

- Inventory your knowledge and get smarter
- Find technology that can learn and grow
- Come up with a plan and practice

Thanks errybody!