

Potentially Malicious URLs



13lackc4t

13lackc4t@naver.com

13lackc4t.blog.me



1. First Get Permission If Needed

2. Unshortening

3. Obfuscating

- URI Tricks
- IP Obfuscation
- URL Encoding

4. Deobfuscating

5. Challenge!

- Manual Safe Deconstruction
- Automatic Safe Deconstruction
- Obfuscation Process
- Tracing the Click
- Browser Compatibility
- Conclusion

First Get Permission If Needed



Major issues

- You don't always know if that data you are transmitting is sensitive
- There is no expectation of privacy when utilizing a third party site

Unshortening



URL shorteners

| Name | URL | Ex |
|-------------------|---|---|
| TinyURL | http://tinyurl.com/ | http://tinyurl.com/bpb94s3 |
| Tiny | http://tiny.cc/ | http://tiny.cc/vorjsw |
| Bitly | https://bitly.com/shorten/ | http://bit.ly/WMyu8O |
| Google Shortener | http://goo.gl/ | http://goo.gl/ICq6o |
| Ow.ly | http://ow.ly/ | http://ow.ly/hK9YQ |
| Twitter Shortener | http://t.co | http://t.co/xxxx |
| is.gd | http://is.gd/ | http://is.gd/PliCom |
| McAfee Shortener | http://mcaf.ee/ | http://mcaf.ee/26tw9 |

URL unshorteners

- Unshorten.it

- <http://unshorten.it/>

The screenshot shows the Unshorten.It! website in a browser window. The URL bar shows 'unshorten.it'. The page has a navigation bar with links: Home, Browser Extensions, Explaining Unshorten.It!, API, and Contact Us. The main heading is 'Unshorten.It!'. Below it is a search bar containing 'http://goo.gl/Gmzqv' and a blue 'Unshorten It!' button. A message below the search bar says: 'Not got a short URL to try? Here's one: <http://bit.ly/QVBQJ5>'.

The results are displayed in two columns. The left column shows the 'Destination URL: http://en.wikipedia.org/wiki/URL_shortening' and a 'Description:' box that says 'This web page does not provide a description.' Below this is a 'Safety Ratings (Provided by Web of Trust)' section with four metrics: Trustworthiness (97), Vendor reliability (95), Privacy (95), and Child safety (91), all rated as 'Excellent'. A button at the bottom of this section says 'View full Web of Trust Scorecard'. At the very bottom is a blue button that says 'Go to http://en.wikipedia.org/wiki/URL_shortening'.

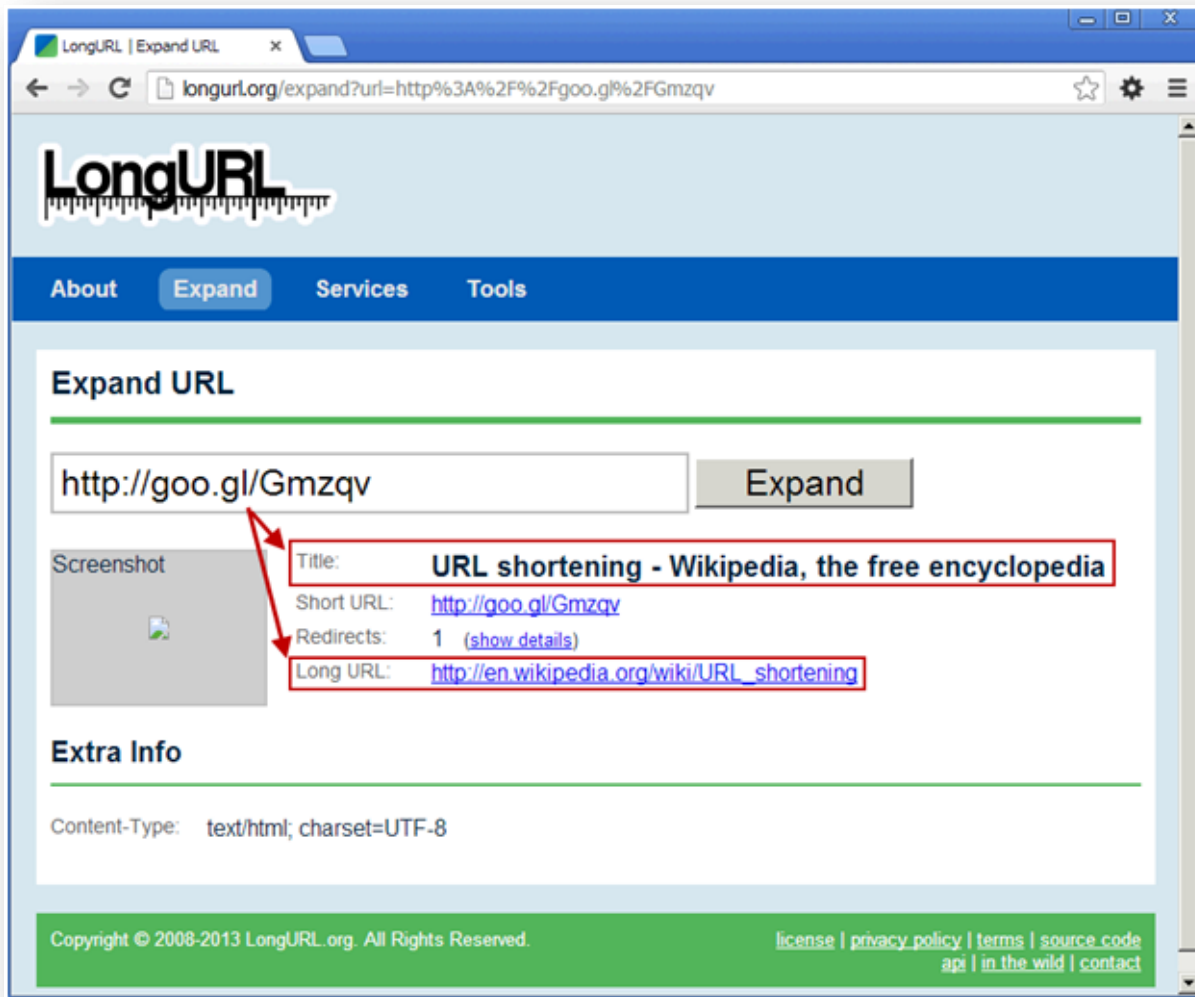
The right column shows a preview of the destination page, which is the Wikipedia article 'URL shortening'. A red box highlights the 'pagepeeker' logo in the bottom right corner of the preview. Below the preview is a green box with the text: 'Blacklists: This website was not found in any blacklists.'



URL unshorteners

- LongURL

- <http://longurl.org/>



URL unshorteners

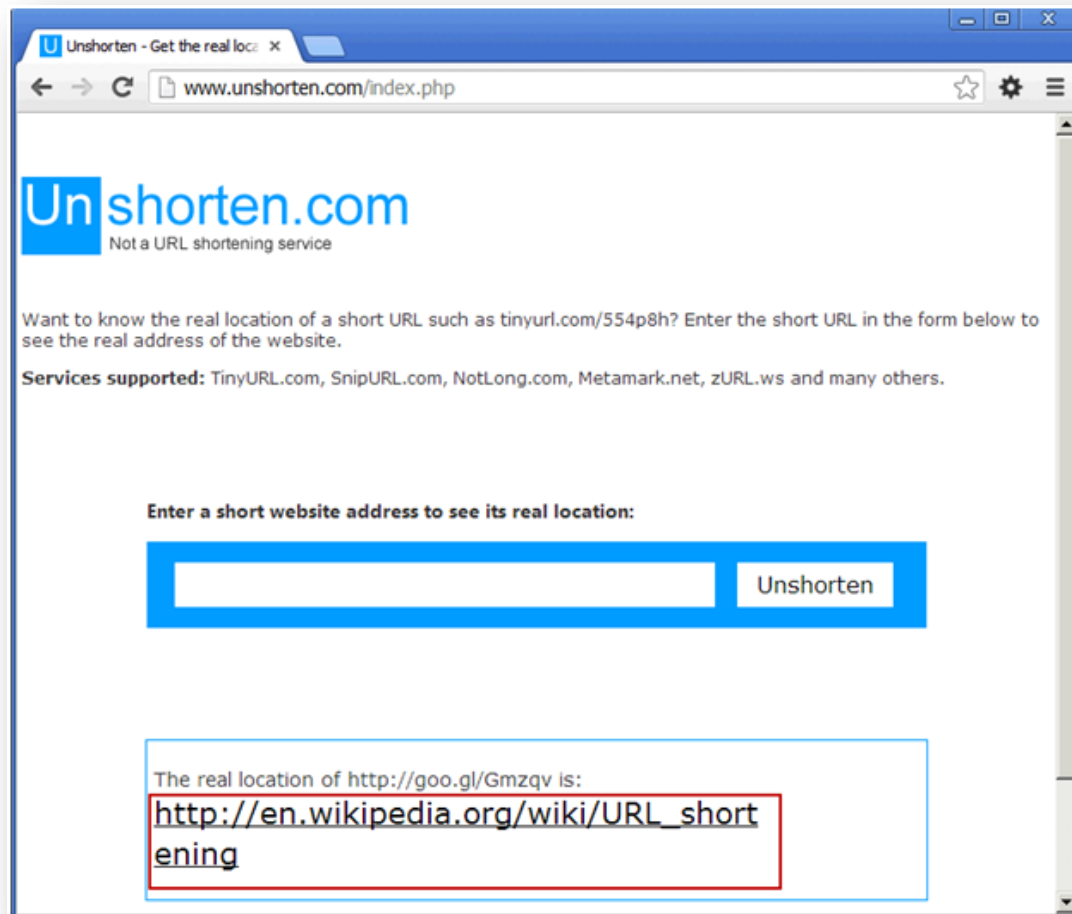
- Unshort.me
 - <http://unshort.me/>





URL unshorteners

- Unshorten.com
 - <http://www.unshorten.com/>



Obfuscating

- URI Tricks
- IP Obfuscation
- URL Encoding



URI Tricks

- **The general URL format**

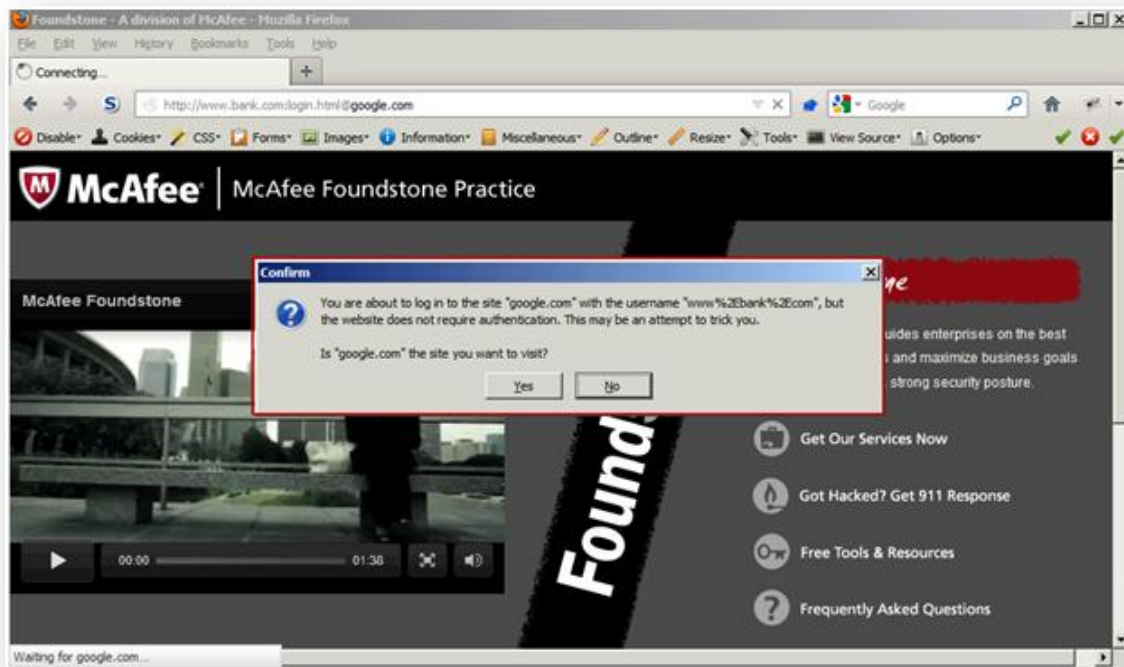
- `protocol://username:password@host:port/resource`

- **Simple examples**

- 1) `http://www.example.com/a/page.html`
- 2) `https://www.attacker.com:8443/attackscript.js`
- 3) `https://www.bank.com:login.html@phisher.cn/`

URI Tricks

- **Chrome v23**
 - Understood the URL and correctly sent us
- **Internet Explorer 8, 9, 10**
 - Not working (only 3.0 – 6.0)
- **Firefox 17.0.1**
 - Warning





IP obfuscation

▪ 74.125.131.105 (one of Google's IP addresses)

- `http://www.bank.com:login.html@74.125.131.105`

- `http://www.bank.com:login.html@1249739625/`

- ✓ DWORD conversion

- $(((((74 \times 256) + 125) \times 256) + 131) \times 256) + 105 = 1249739625$

- `http://www.bank.com:login.html@0x4a.0x7d.0x83.0x69/`

- ✓ Hex conversion

- $74 = 0x4a \quad 125 = 0x7d \quad 131 = 0x83 \quad 105 = 0x69$

- `http://www.bank.com:login.html@0112.0175.0203.0151/`

- ✓ Octal conversion

- $74 = 0112 \quad 125 = 0175 \quad 131 = 0203 \quad 105 = 0151$



URL Encoding

- converts characters into a format that can be transmitted over the Internet
- Be used in URLs to confuse the user and hide intention
 - `ftp://foo:foo%40example.com@ftp.example.com/pub/a.txt`
 - ✓ `%40` -> `'@'`

Deobfuscating

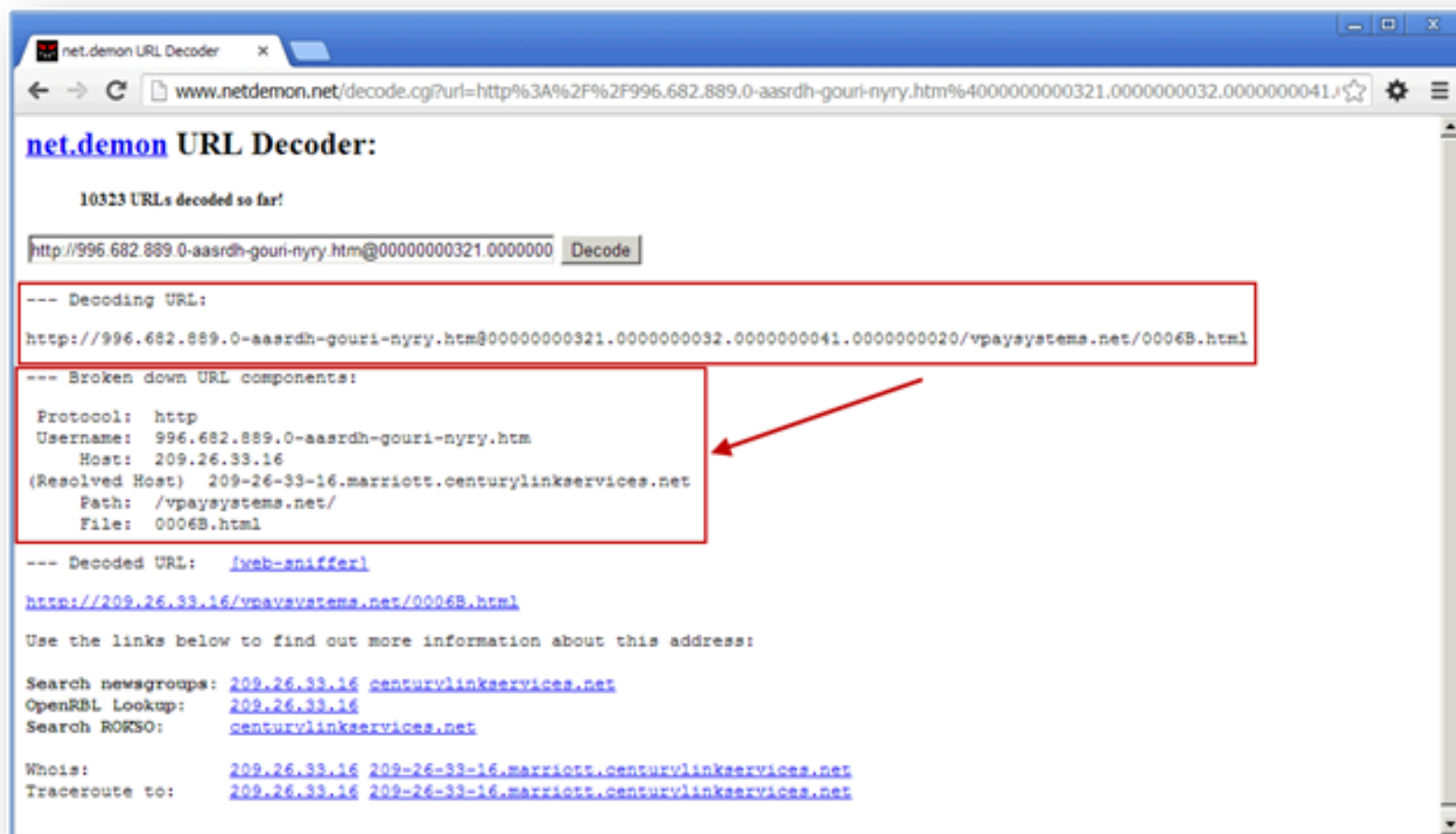


- **http://225.116.453.0-bank-login.htm@00000112.00000175.00000203.00000151**
 - These can still be done by hand, but can be time consuming
 - There are some third-party sites that will help you figure out what the URL is doing



▪ Netdemon

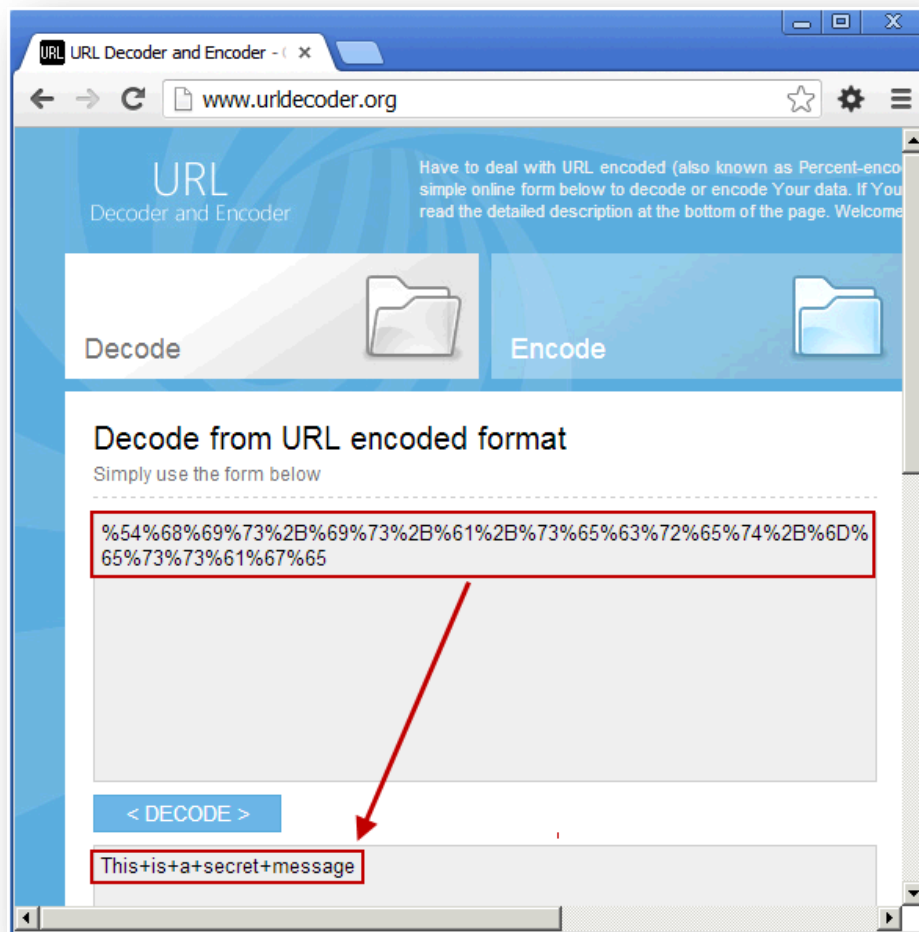
- <http://www.netdemon.net/decode.cgi>





- URL decoder

- <http://www.urldecoder.org/>

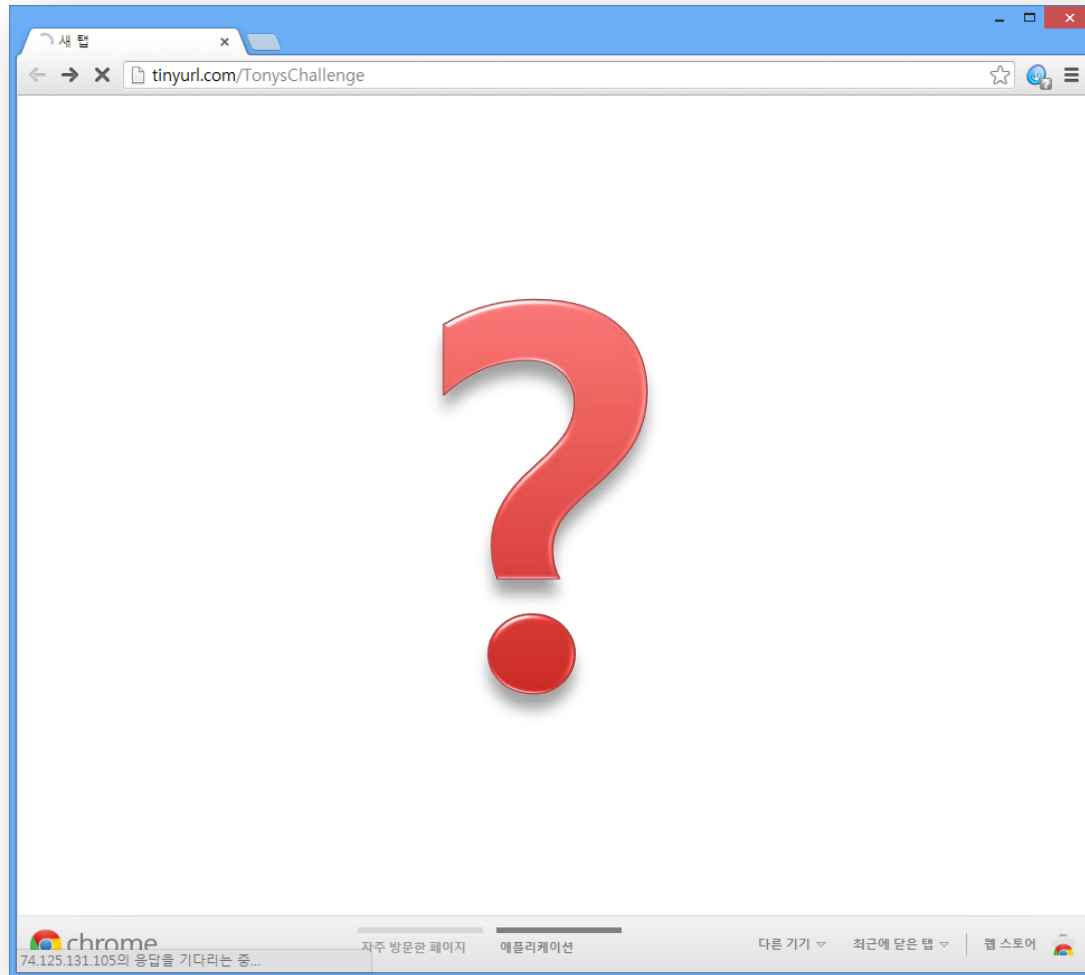


Challenge!

- **Manual Safe Deconstruction**
- **Automatic Safe Deconstruction**
- **Obfuscation Process**
- **Tracing the Click**
- **Browser Compatibility**
- **Conclusion**



- <http://tinyurl.com/TonysChallenge>





Manual Safe Deconstruction

1. Unshorten the URL
2. Discard URL trickery
3. Convert Octal to Decimal
4. URL decode
5. WHOIS attribution

Manual Safe Deconstruction

- **Unshorten the URL**
 - Use one of the URL shorteners called tinyurlchecker





Manual Safe Deconstruction

- **Unshorten the URL**

- Result

- ✓ http://225.116.453.0-bank-

- login.htm@00000112.00000175.00000203.00000151/%75%72%6C?%73%61=%74&%75%72%6C
=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D
%2F%77%61%74%63%68%3Fv%3%44%6F%48%67%35%53%4A%59%52%48%41%30



Manual Safe Deconstruction

- **Discard URL trickery**

- Remove anything from the http:// up to and including the '@'.

- Result

✓ `http://00000112.00000175.00000203.00000151/%75%72%6C?%73%61=%74&%75%72%6C=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D%2F%77%61%74%63%68%3Fv%3%44%6F%48%67%35%53%4A%59%52%48%41%30`



Manual Safe Deconstruction

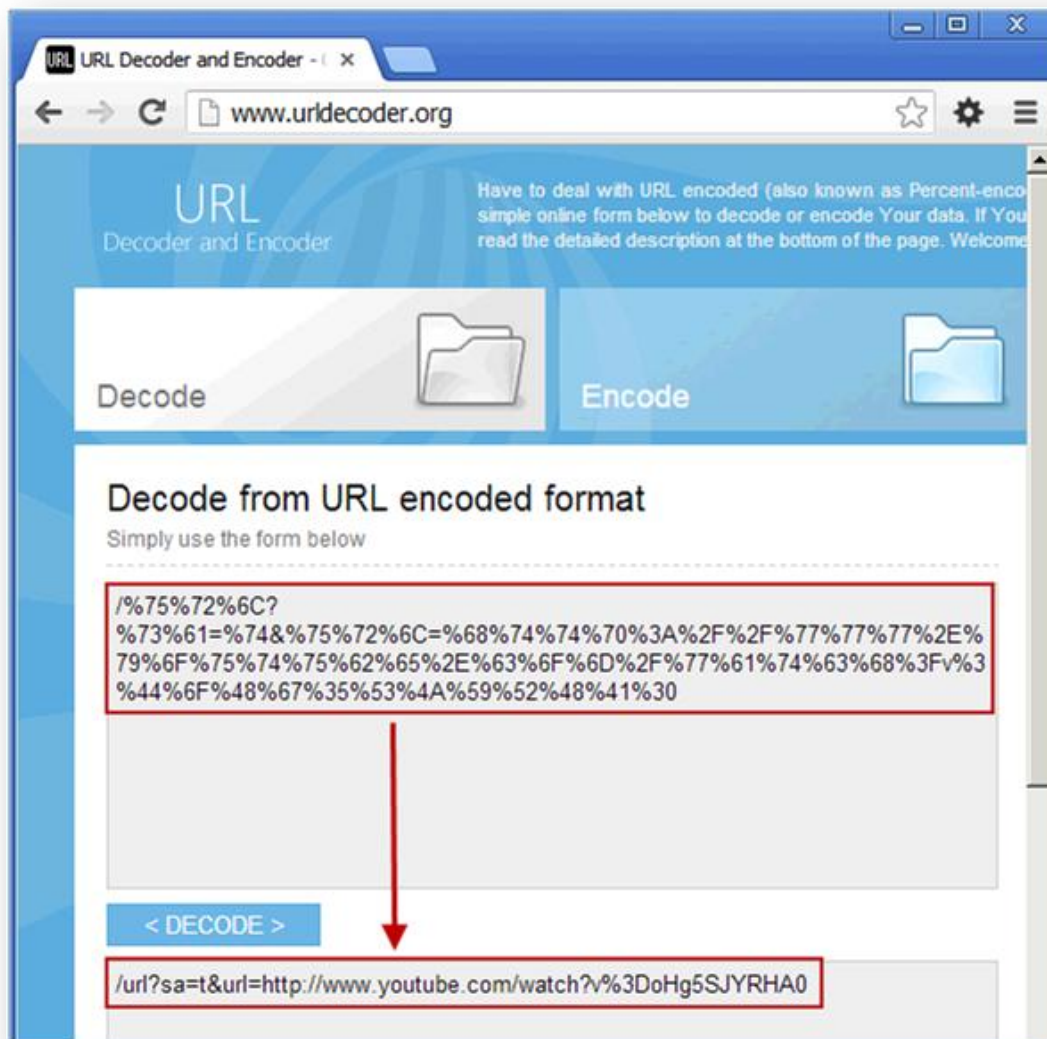
▪ Convert Octal to Decimal

- Address: `http://00000112.00000175.00000203.00000151`
- Convert: `00000112 = 74` `00000175 = 125` `00000203 = 131` `00000151 = 105`
- Becomes: `http://74.125.131.105`
- Result
 - ✓ `http://74.125.131.105/%75%72%6C?%73%61=%74&%75%72%6C=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D%2F%77%61%74%63%68%3Fv%3%44%6F%48%67%35%53%4A%59%52%48%41%30`



Manual Safe Deconstruction

- URL decode





Manual Safe Deconstruction

- URL decode

- Result

- ✓ <http://74.125.131.105/url?sa=t&url=http://www.youtube.com/watch?v%3DoHg5SJYRHA0>



Manual Safe Deconstruction

- WHOIS attribution

74.125.131.105/vc-in-f105. x

whois.domaintools.com/74.125.131.105

Open a FREE Account | Log in | Help ?

74.125.131.105 Whois Search Search

HOME RESEARCH MONITOR BUY DOMAINS LEARN OPEN AN ACCOUNT

IP Information for 74.125.131.105

IP Location: United States Mountain View Google Inc.

ASN: AS15169

Resolve Host: vc.in-f105.net Hostname is not helpful

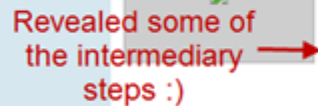
IP Address: 74.125.131.105 W R P D T

NetRange: 74.125.0.0 - 74.125.255.255
CIDR: 74.125.0.0/16
OriginAS:
NetName: **GOOGLE**
NetHandle: NET-74-125-0-0-1
Parent: NET-74-0-0-0
NetType: Direct Allocation
RegDate: 2007-03-13
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-74-125-0-0-1

OrgName: Google Inc.
OrgId: GOGI
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2011-09-24
Ref: http://whois.arin.net/rest/org/GOGI

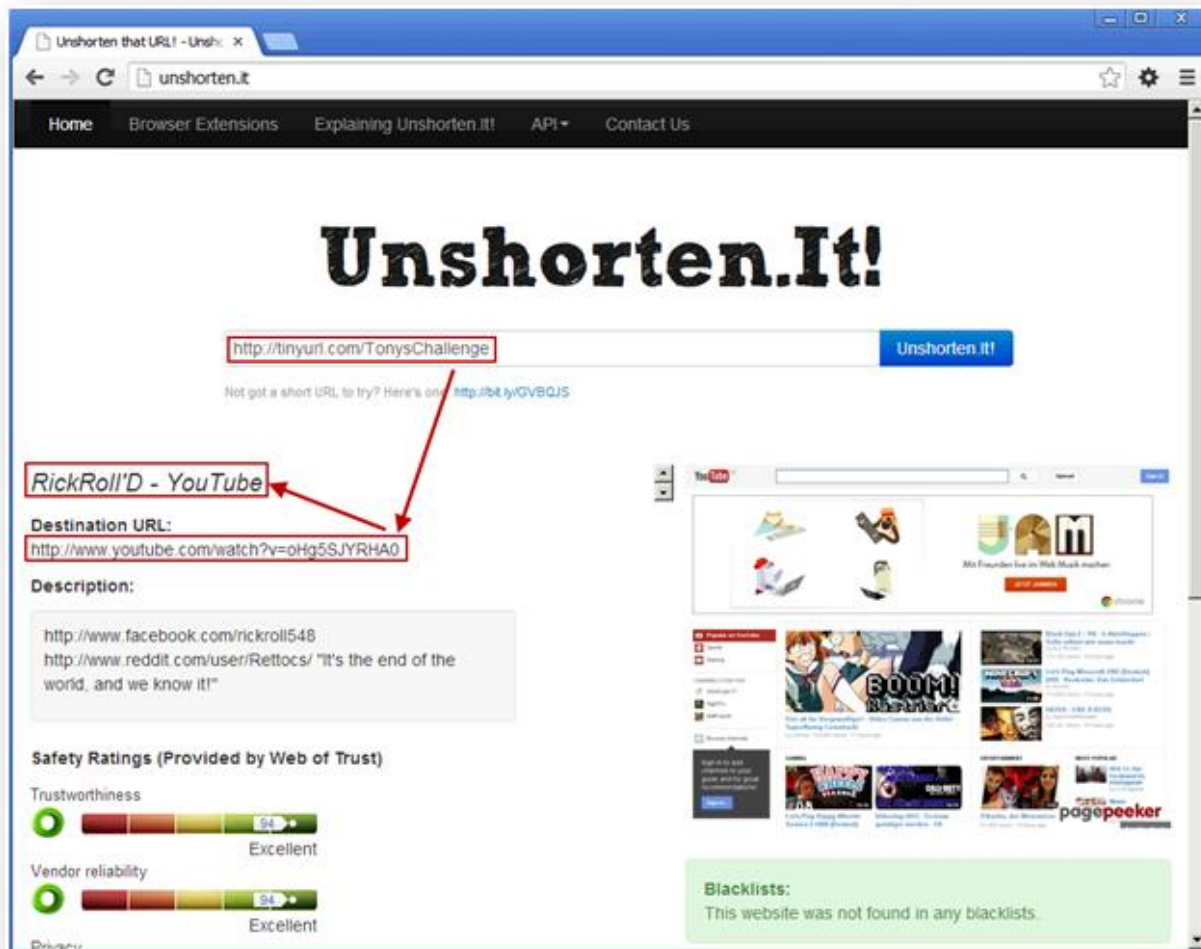
Registration is helpful

- LongURL



Automatic Safe Deconstruction

- Unshorten.it





Obfuscation Process

- URL Redirection
- Octal IP Representation
- URL Encoding
- URL Trickery
- URL Shortening



Obfuscation Process

▪ URL Redirection

- An application that accepts a parameter that allows the end user to be redirected to another page
- It happens so quickly that the user does not have time to react and stop the next page from loading
- A simple example of a URL redirect:
 - ✓ `http://www.vulnerablesite.com?URL=http://www.attacker.com`

Obfuscation Process

■ URL Redirection

- The URL redirect we used in our special link is against Google (with their gracious permission for educational purposes):

✓ <http://www.google.com/url?sa=t&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DoHg5SJYRHA0>





Obfuscation Process

▪ Octal IP Representation

1. nslookup www.google.com resolved one of Google's web servers to 74.125.131.105.
 2. Using Microsoft's Calculator, we converted the IP address - 74 = 0112 125 = 0175 131 = 0203 105 = 0151.
 3. After adding some zero padding (any number of zeros can be used), we come up with
`http://00000112.00000175.00000203.00000151`
 4. Replace "www.google.com" in our redirect URL
- Result :
 - ✓ `http://00000112.00000175.00000203.00000151/url?sa=t&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DoHg5SJYRHA0`



Obfuscation Process

- URL Encoding

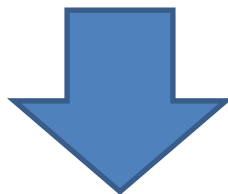
| ASCII | URL Encoded |
|-----------------|---|
| url | %75%72%6C |
| sa | %73%61 |
| t | %74 |
| http | %68%74%74%70 |
| www.youtube.com | %77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D |
| watch | %77%61%74%63%68 |
| DoHg5SJYRHA0 | %44%6F%48%67%35%53%4A%59%52%48%41%30 |



Obfuscation Process

- **URL Encoding**

- `http://00000112.00000175.00000203.00000151/url?sa=t&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DoHg5SJYRHA0`



- `http://00000112.00000175.00000203.00000151/%75%72%6C?%73%61=%74&%75%72%6C=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D%2F%77%61%74%63%68%3Fv%3%44%6F%48%67%35%53%4A%59%52%48%41%30`



Obfuscation Process

- **URL trickery**

- Chrome is the only browser that will send the user to the destination page without a warning when the URL is formatted as follows:

- ✓ `http://www.bank.com:login.html@google.com/`



Obfuscation Process

- URL trickery

- `http://00000112.00000175.00000203.00000151/%75%72%6C?%73%61=%74&%75%72%6C=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D%2F%77%61%74%63%68%3Fv%3%44%6F%48%67%35%53%4A%59%52%48%41%30`



- `http://225.116.453.0-bank-login.htm@00000112.00000175.00000203.00000151/%75%72%6C?%73%61=%74&%75%72%6C=%68%74%74%70%3A%2F%2F%77%77%77%2E%79%6F%75%74%75%62%65%2E%63%6F%6D%2F%77%61%74%63%68%3Fv%3%44%6F%48%67%35%53%4A%59%52%48%41%30`



Obfuscation Process

▪ URL Shortening

- Used TinyUrl because it allows us to specify a memorable link such as TonysChallenge

Welcome to TinyURL!™

Are you sick of posting URLs in emails only to have it break when sent causing the recipient to have to cut and paste it back together? Then you've come to the right place. By entering in a URL in the text field below, we will create a tiny URL that ***will not break in email postings*** and ***never expires***.

Enter a long URL to make tiny:

Custom alias (optional):
http://tinyurl.com/
May contain letters, numbers, and dashes.

- Result :
 - ✓ <http://tinyurl.com/TonysChallenge>

Tracing the Click

The screenshot shows a Wireshark packet capture of an HTTP session. The packet list on the left shows several requests to tinyurl.com and youtube.com. The packet details pane on the right shows the raw HTTP data for a 302 redirect from tinyurl.com to a long URL. The packet bytes pane at the bottom shows the HTML response from Google.

Step 1) User first hits TinyURL which redirects them to the URL tricky address

Step 2) The browser figures out that the authentication is unnecessary and navigates to the octal address

Step 4) User follows Location header from the server and navigates to youtube for musical enjoyment

3) The octal address is Google and there is a redirect in the URL. The server returns the location of youtube with an interesting video

Browser Compatibility

- Only Chrome!



