Browser vulnerability to Superfish

A fact-finding trip to Best Buy

Summary:

- Superfish performs HTTP MitM for IE, Chrome, and Firefox
- Superfish performs HTTPS MitM for IE and Chrome
- Superfish appears to **not** perform MitM on HTTPS connections from Firefox
- The Superfish proxy accepts its own certificate, so now that the private key has been leaked, an **attacker can mimic an arbitrary site in Chrome and IE**

I wanted to see how Superfish affects Firefox and other browsers, but needed an affected device. So I headed down to Best Buy and tested things out on their display unit, a Lenovo Yoga 2 11 Touch (YOGA2 11-59401972, Best Buy SKU 3297045).

ONLY @BEST BUY®.
Lenovo Yoga 2 11 Touc r
2-in-1 Laptop
Model: YOGA2 11- 59401972 **SKU:** 3297045

lenovo

Customer Reviews
★★★★☆ 4.07
744 Reviews
(from bestbuy.com, as of 02/13/2015)

Dimensions
11.7"w x0.7"h x8.1"l

Features

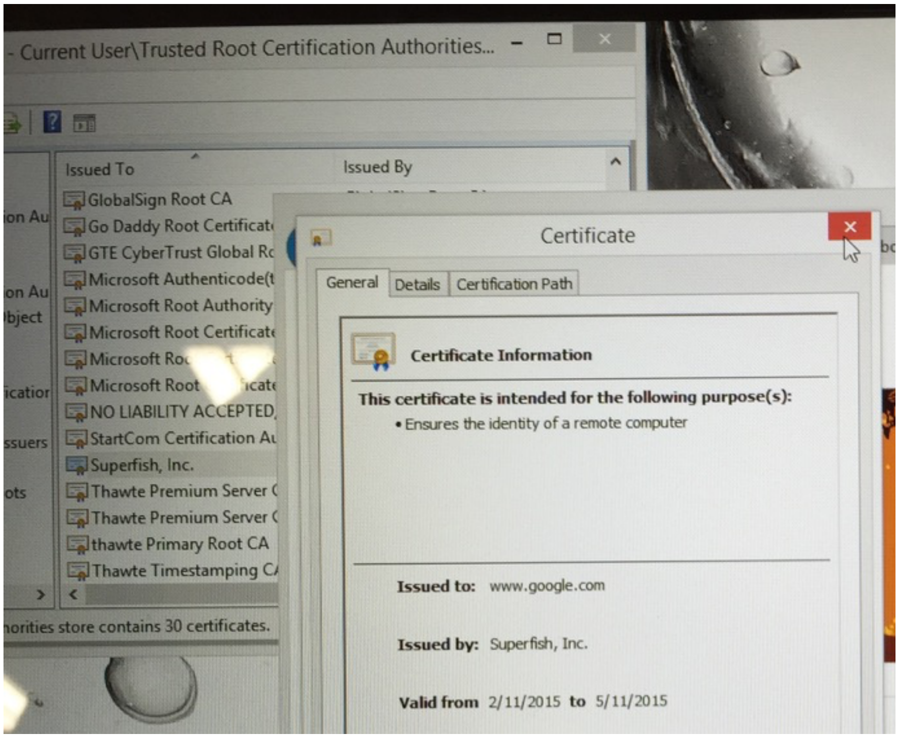
Screen Size	**11.6"**
Display Type	**HD (1366 x 768)**
Processor	**Intel® Pentium®**
Memory	**4GB**
Computer Hard Drive	**500GB**
Battery Life	**Up to 5H & 6M***

SAVE $50.00 REG. $529.99
$479.99

Geek Squad Protection (2 Year ADH): $209.99
Manufacturer's Warranty: *Battery life varies with use. See manufacturer for info on battery life. [illegible] available upon request - warranty on parts may vary

SALE 889233327807 **Printed:** 02/17 05:51 AM
POG: COCFTBL 45.06 M

When I started, the unit appeard to be cleanly initialized demo machine state. The only browser installed was Internet Explorer. So the first test I did was to verify that the Superfish certificate was present in the certificate manager and showed up when loading "https://www.google.com/". Check, and check.



Issued To	Issued By
GlobalSign Root CA	
Go Daddy Root Certificat	
GTE CyberTrust Global Ro	
Microsoft Authenticode(t	
Microsoft Root Authority	
Microsoft Root Certificate	
Microsoft Ro	
Microsoft Root icate	
NO LIABILITY ACCEPTED,	
StartCom Certification Au	
Superfish, Inc.	
Thawte Premium Server C	
Thawte Premium Server C	
thawte Primary Root CA	
Thawte Timestamping CA	

horities store contains 30 certificates.

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: www.google.com

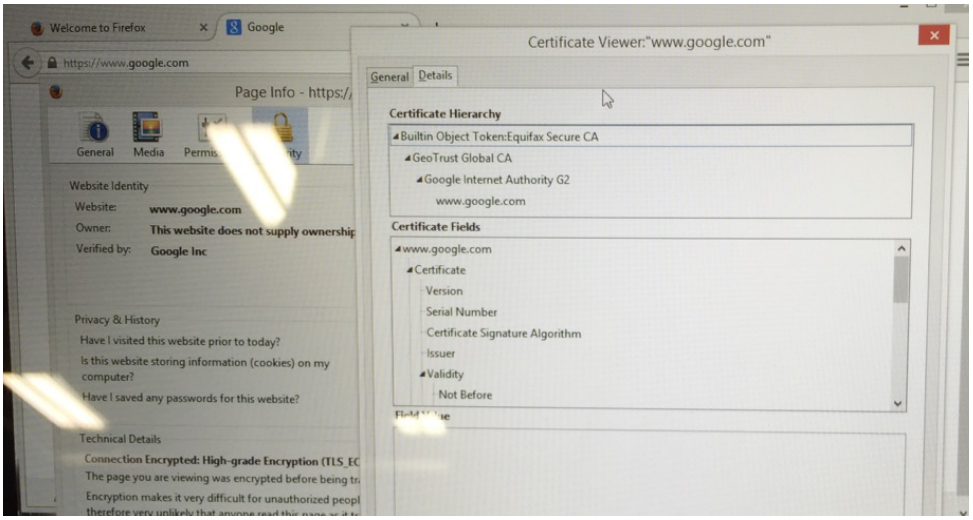
Issued by: Superfish, Inc.

Valid from 2/11/2015 **to** 5/11/2015

(But hey, on the plus side, they're only using a 3-month cert!)

I then used IE to download Firefox, and installed it. (Note that this means that Superfish had access to Firefox as it was downloaded.) On loading "https://www.google.com/" with Firefox, the certificate UI showed the normal chain for Google -- no Superfish. Likewise, looking at the list of trusted in roots showed no Superfish cert, and the add-ons screen showed no addons.

(Of course, depending on how conspiracy theory / inception you want to get here, it's possible that Superfish rewrote the Firefox UI to hide their tracks. But given that they didn't with Chrome or IE, this seems improbable.)



Welcome to Firefox

Google

https://www.google.com

Page Info - https://

General Media Permis... ...ity

Website Identity

Website: **www.google.com**

Owner: **This website does not supply ownership**

Verified by: **Google Inc**

Privacy & History

Have I visited this website prior to today?

Is this website storing information (cookies) on my computer?

Have I saved any passwords for this website?

Technical Details

Connection Encrypted: High-grade Encryption (TLS_EC

The page you are viewing was encrypted before being tr

Encryption makes it very difficult for unauthorized peopl

therefore very unlikely that anyone read this page as it tr

Certificate Viewer:"www.google.com"

General Details

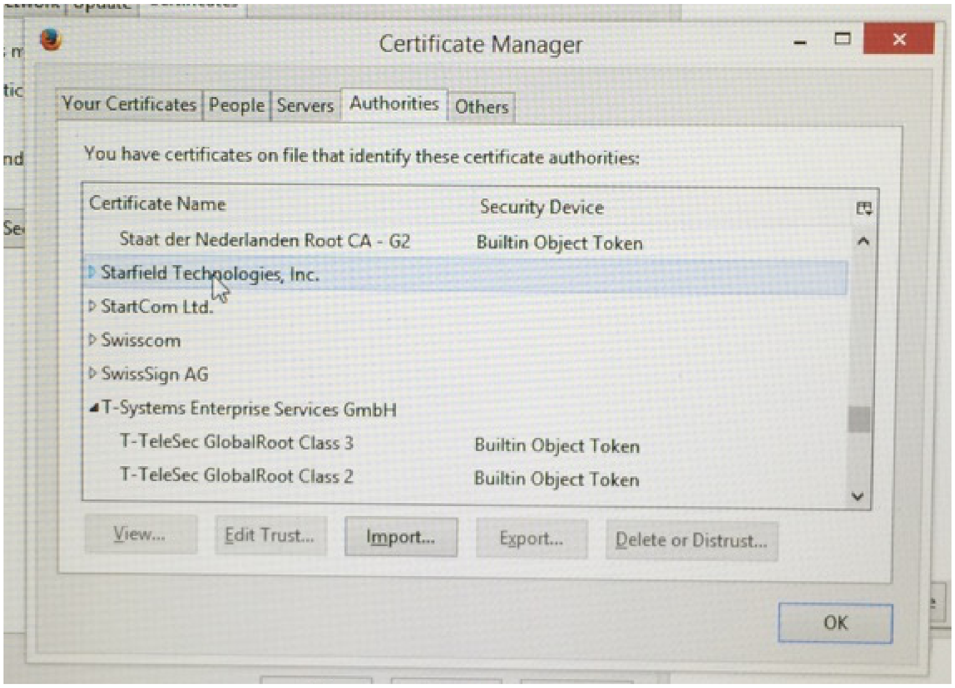
Certificate Hierarchy

```
▴Builtin Object Token:Equifax Secure CA
  ▴GeoTrust Global CA
    ▴Google Internet Authority G2
       www.google.com
```

Certificate Fields

```
▴www.google.com
  ▴Certificate
     Version
     Serial Number
     Certificate Signature Algorithm
     Issuer
    ▴Validity
       Not Before
```

Field Value

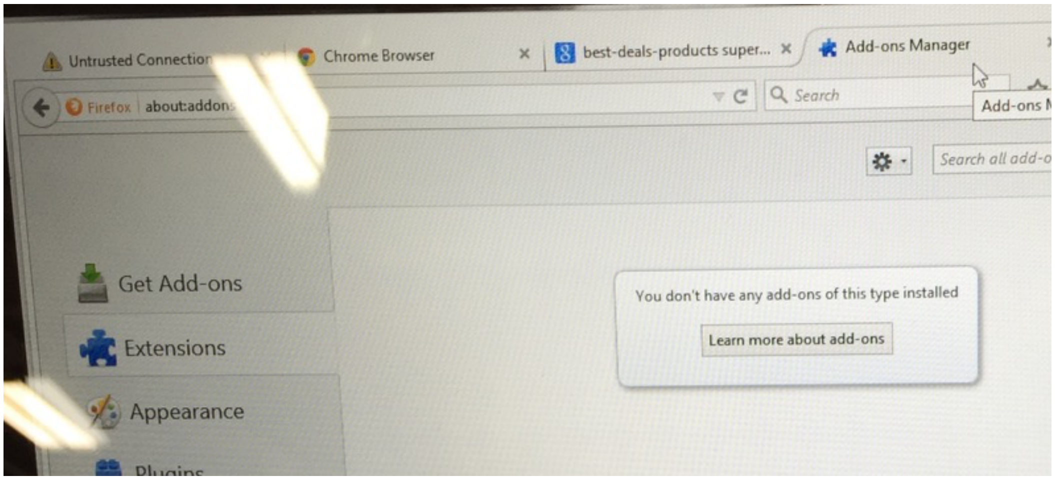


Certificate Manager

Your Certificates | People | Servers | Authorities | Others

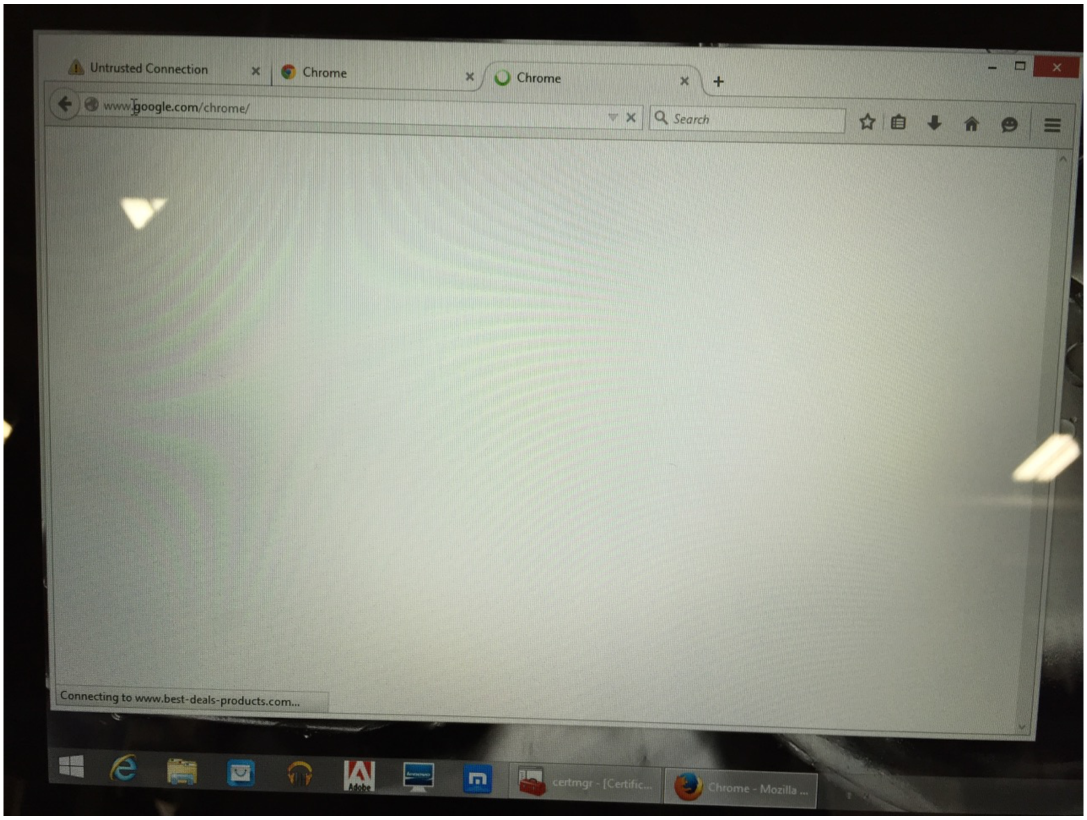
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Staat der Nederlanden Root CA - G2	Builtin Object Token
▷ Starfield Technologies, Inc.	
▷ StartCom Ltd.	
▷ Swisscom	
▷ SwissSign AG	
▴ T-Systems Enterprise Services GmbH	
T-TeleSec GlobalRoot Class 3	Builtin Object Token
T-TeleSec GlobalRoot Class 2	Builtin Object Token



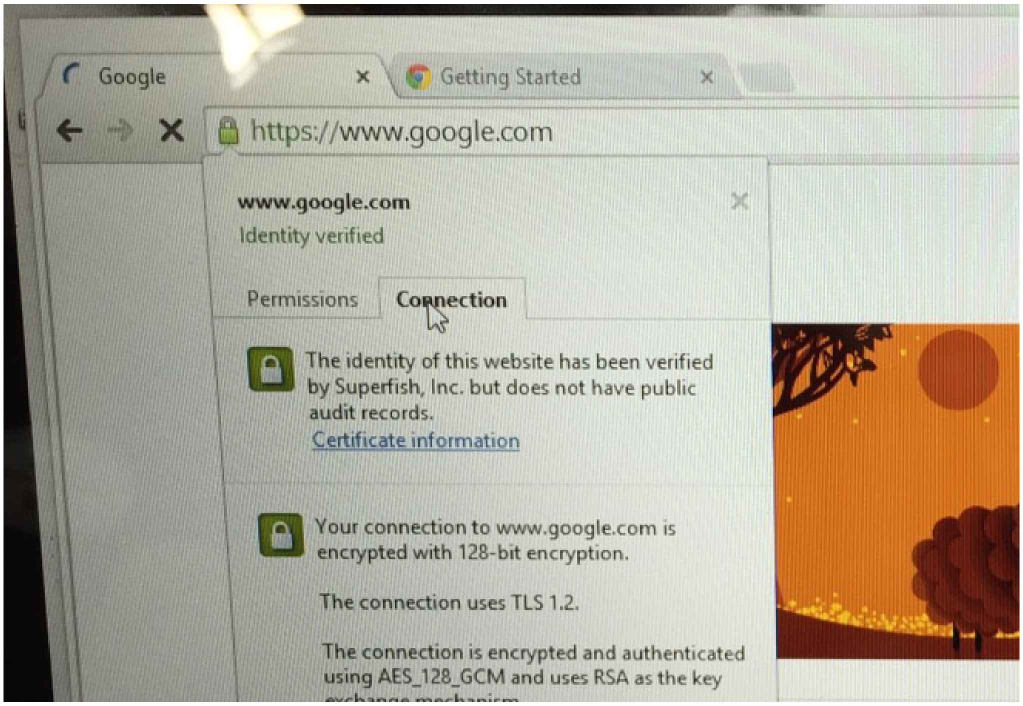
You don't have any add-ons of this type installed

When I then went to download Chrome, I accidentally entered "http://google.com/chrome", not "https". Due to the slow network at Best Buy, I was able to see status bar message "Connection to best-deals-products.com" -- a domain used by Superfish. So Superfish is injecting into HTTP. (I did not check the proxy settings to see if this was being done via configuration or intercept, but given the HTTPS exception, I suspect intercept.)



Connecting to www.best-deals-products.com...

Going back to the HTTPS version of the Chrome site, I downloaded Chrome; however, since Chrome uses a custom downloader, it was probably availble to Superfish as well. I performed the same test with Chrome as with IE, and got the same results. So Chrome is affected over HTTPS.



www.google.com

Identity verified

The identity of this website has been verified by Superfish, Inc. but does not have public audit records.

Certificate information

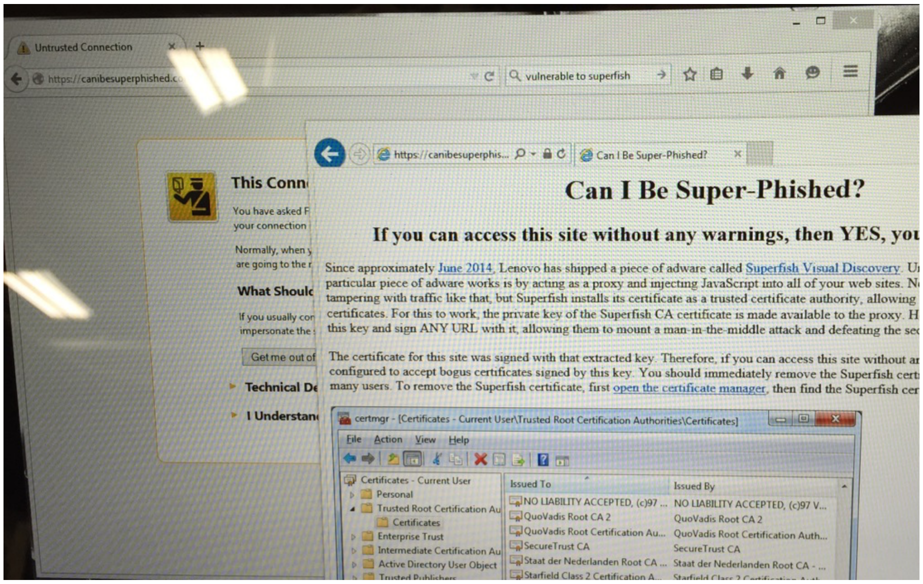
Your connection to www.google.com is encrypted with 128-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses RSA as the key exchange mechanism

I did not directly verify HTTP interference in IE and Chrome, but I assume if they're doing to Firefox, they're also doing it to IE and Chrome.

One critical question is whether an attacker can exploit the presence of the Superfish root to masquerade as an arbitrary website, now that the private key has been extracted and published. After all, given that Superfish software is a MitM in HTTPS transactions, they could be good citizens and not accept their root for the WAN-side transaction. Unfortunately, Superfish do not appear to be good citizens. The IE on a Superfish platform happily loads "https://canibesuperphished.com/", which uses a cert under the Superfish root. Firefox chokes (sec_error_unknown_issuer).



This Conn

You have asked F
your connection

Normally, when y
are going to the r

What Should

If you usually con
impersonate the

Get me out of

Technical De

I Understan

Can I Be Super-Phished?

If you can access this site without any warnings, then YES, you

Since approximately June 2014, Lenovo has shipped a piece of adware called Superfish Visual Discovery. U
particular piece of adware works is by acting as a proxy and injecting JavaScript into all of your web sites. N
tampering with traffic like that, but Superfish installs its certificate as a trusted certificate authority, allowing
certificates. For this to work, the private key of the Superfish CA certificate is made available to the proxy. H
this key and sign ANY URL with it, allowing them to mount a man-in-the-middle attack and defeating the se

The certificate for this site was signed with that extracted key. Therefore, if you can access this site without a
configured to accept bogus certificates signed by this key. You should immediately remove the Superfish cert
many users. To remove the Superfish certificate, first open the certificate manager, then find the Superfish cer

certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers

Issued To	Issued By
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...
QuoVadis Root CA 2	QuoVadis Root CA 2
QuoVadis Root Certification Au...	QuoVadis Root Certification Auth...
SecureTrust CA	SecureTrust CA
Staat der Nederlanden Root CA ...	Staat der Nederlanden Root CA - ...
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...