SUPERFISH

Jonathan Ng
Minying Lu
Philip Zhang
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

Monitor user activity

Analyze and extract user preference

Superfish’s Database

Targeted images/ads

Injecte ads/img to webpage
SUPERFISH CERT IN ROOT STORE
Verify superfish as CA

Lenovo computer with superfish installed in root store

Real cert
Subject: BOA
Issuer: Verisign

“fake” cert
Subject: BOA
Issuer: SuperFish

The Man-in-the-Middle Attack

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

Actively monitor user activity and collect data

Bank of America
OOPS
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

Affected machine

Super.dmp
Binary file: 10011010001.....

“Strings” function

Super.txt
Convert binary to human readable string

Search for “PRIVATE KEY”, and got result

Binary file: 10011010001.....

Convert binary to human readable string

Store private key into .pem file

Super.pem

Try to look at it

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

Try OpenSSL and password prompted

Try OpenSSL and password prompted

Dictionary attack

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

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Found password: “komodia”

Affected machine

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack

Decrypted private key with password and obtain the superfish certificate

Dictionary attack
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxJBAkghkqkhkG9w0BBQwwMzAbBkgwhhkiG9w0BBQwwDgQIDHhHyAEZQoICAggA
MBQGClqG1b3DQMjHMEg+MCYQ3ASACoDvGvFRHvkt0bSRc0f31bVqevUwS5z
xQn+rzLiHw6b0a1mbFs6tGkacVz/LFE7L14de/CSQ6pzZCCyfDzovemPuGye
SeAe7hbacl+1/3Wf3vBn3vTFbLPf17wSmk6lcKq7YfckJz//sUJGpeX9r6rayWYyFx
f+EdTr348d0ez8uHkURY1cvSHaIDITALKChOnoAYT685V1ghTeB6x0CwdfsHxH+X
3QbhomY2C1xfj1AozZ/LndcpDaEf0rVrrxF0XXr1bmeDEyDQj16Avn19uuaaj71
N1O3zrnxqsfvdVfPAaYRQonSa02jXxk4ho17z2/c/MpM6c6dwsf5V3R7SmRngxgy8N
1GLyVfHHR7538tIaDgJ18d8j8t890/v0eE0Kx666jKkRGo+Vpq6+bshh7vThPC/gS
1d1Fvn5s1v2eknuhD0hJ5XkYQ6Hjnioae4Ae/0ARLqzaID8Itt//PRB0OMSkutd
z1px9d2Z8pSoRAOAcBwUSaFaw9u+txxvzrPMT3zomu8yQyVMNLmVpGNDJ0z6JPJ1
jaZHWT7U67j380H/b6K7Ug/ybrJGn0mPP4h2/ug675Ekfot0USrsvKWruetQh01
TCHn9h1t3cxxtnXtQz243RHM7Mturq+6fql1f3bb9bWarMBu3C3gprqyyXeM0QQg
VlyKLWuAumF2c7t7uqjaNmVg6vbwhHEbR6njiJ1L7j4w6D2YQvcarcS35Mb/K0
SK5S4HNvBFXuXa1iP7y3t0Bom7QFkFakxju0JP+AJmneHrReokS2u420HXBWEDE8
Vrhw7/1tXxs3kJbCQ9M/rqsvyQ4xVhXDAkXfPmS25uJyKjEvGvCQok4F/t
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICCAIBAwIBAgIJDANL84epRZnnaEARCSCg6lBQszd3QEBBQUAMSxzGDAWBGNg
BAoTbD11nC1GvZmLrAzWw5jJkJGMAKAIUEBxMCU0YVczAJBGvNBBgTACKBBQsZw
CQQVQQGUEjW3VU3EYMY8GALUEAxMjPU3VzX2maXGoLCBBjbrMmB4XhD0MDw4MjeE2
MJUyNLoXDTM0DwUsN2E2MjuJwIY4z8xkEYMY8GALUEChMjPU3VzX2maXGoLCBBjbrMmB4
MQS5VQQtVQvH9ewT7RjELMAKAIUEC8NCQ9ExAJBGvNBBgTALKTMR9gwFyvYDQQe
Ew97tXbICmZpc2gsElvuyY4zwBQYJazhvcNAQEBBQAgYmAMIGcAoG0aj8jz
Shh2Xyk/sC9y6X9DBmVwDQf5/xm5e8mRmIIXKFJ2r8QUL5jg41dgnsSsAYj3b
1Tnm3Hh/n+7U+hFm6pE8FX/aFAXYqVc4XoufPlar/2FwPr5TvGAGVYV8x375sB
3b2MptTrhD2/g3xpBtmQoDQus81c/ZJZocPnQoETAgMBAAGjgAcwbg6wDAYDVR0T
BAUASMWE8/zAD8g6VNH54EFGuQ+51ZU3URC70tU7JMj404oaYYwG0yGAIUDsWb
hTBC8goAu+51u38URC70tU7JMj404oaYYwG0yGAIUDsWb
ZmlzaW51Ww5jJkJGMAKAIUEBxMCU0YVczAJBGvNBBgTACKBBQsZw
UzEYMY8GALUEChMjPU3VzX2maXGoLCBBjbrMmB4
AQEFBQAgYHb7Ap7Kp33EcwcjzOyL3jyNCJl+35k1X2m0xUQ0sU766450j
1IIsYyWtw6sA9ZTRMz5T4Q4vFQQra81cLqYpPsPMuPC+FCxKuF51bDN5w1/0xK33XH
TICQ5Wql9t9JEOFv3ктW+zn2Or7Y4Li0MW7GEUI+88VAw4q9XyNL/ycf0--
-----END CERTIFICATE-----
Simply search for “PRIVATE KEY” in super.txt

```
pc2g&h
IhvcD
Unknown error
equence
operation
SocketAsync

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBAbgkqhkiG9w0BBQ0wFwMzAbBgkqhkiG9w0BBQwwGgQIDHhAIAZQoICAaggA
MBQGCCqGSIb3DQMHBAnHEg+MCYQ30ASCAoDEvGvFRHvTw0b5Rc0f3lbVKqeUvWSz
xQn+rZELHnb6baolmbFcsi6XkacVzL/EF7Ll4de/CSQ6pZZCCvfDzov0mPOuGve
SAe7hbAcol7+JWVfzbnVTblPfoi7mSwK61cKq7YfcKJ2os/uJGpe9zraywWyFx
f+EdTr348d0ez8uHkURY1cvHSdITALKChOonAYT68SVighTeB6x0CwfmsHx+X
3Qbhom2YCIxfJiaOoz2/LndCpDaEfOrVrxXFOXXrIbmeDEyjDQj16AVni9uuaj7l
NiO3zrrqxsfdVINPaAYRKQns102jXqkh01z72c/MpMMC6dwZswF5V3R7RSXngyBn
```
View the encrypted certificate chain using OpenSSL

C:\dev>openssl rsa -in super.pem -text
Enter pass phrase for super.pem:
Password must be in memory dump as well
Use a dictionary of all the (lowercase) words in the memory dump: 2203

FOUND PASSWORD
With the password, “komodia”, Graham was able to decode the private key.
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.”
Intercept traffic

“Shape”, block or redirect traffic

Return manipulated data

Komodia’s SSL Hijacker

Komodia’s Redirector

Computer

Web server
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 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.”
LENNOVO: “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:

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

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

- Double check that it was removed by uninstalling SuperFish VisualDiscovery
- Go to Manage Certificates and remove the Superfish certificate from Trusted Root CA store
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/
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 MIICxjBABBgkqhkiG9w0BBQw0MzAbBgkqhkiG9w0BBQwwDgQIDHhxyAEZQoICAghA
4852 MBQGCcQGSIb3DQMHBAlHEg+MCYQ30AASCAD0DEyGvFRHvtW0b5Rc0f3lbbVqeUvWSz
4853 xQn+rZELHnwb6baolmbFcs6XkacVzL/EF7l4de/CSQ6pZZCCvfDzov0mPOuGve
4854 SAe7hbAcol7+JWVfzbmVTblPfoi7mwSvK61cKq7YfcKJ2os/uJGepeX9zraywlyFx
4855 f+EdTr348d0ez8uHkUryY1cvSHsIDITALkJh0onAYT68SVighTeB6xOCwmsHx+X
4856 3Qbhom2YCIxfJiaAoz2/LndCpDaEfOrVrxXF0KXRbmeDEyjDQj16AVni9uuaj7l
4857 Ni03zrrqsfdVINPaAYRKQn5102jXqKHO1z72c/MpMMC6dwZswF5V3R7RSXngybN
```
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
- US-CERT official alert: https://www.us-cert.gov/ncas/alerts/TA15-051A
- 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://marcrogers.org/2015/02/19/will-the-madness-never-end-komodia-ssl-certificates-are-everywhere/
- http://www.kb.cert.org/vuls/id/529496