FORTCONSULT

Straight talk on IT security

SECURITY ADVISORY

ID: FCSA1204

Deal Extreme website

ExploitKit Infection

Phone: +45 70207525 Email: info@fortconsult.net Web: www.fortconsult.net

Background

From the Deal Extreme website:

“Online shopping for cool gadgets at the right price. Buy cheap computers, electronics, car accessories, cellphones, iPhone, apparels and home gadgets“

From wikipedia: (Translated by Google translate)

“Deal Extreme is a Chinese shop and one of the largest in its niche. [1] The company is based in Hong Kong and bases its business on selling cheap products to Europe and USA . The website has as of 2012 1 348 039 impressions per day. [2]

The store sells small electronics mainly to private households and is believed to be the world's cheapest online store. [3] [4] The shop sells, among other things, replicas of famous brands like iPhone under similar names such as "SciPhone", "Ifone" and "HiPhone".

In September 2011 opened the store inventories in the United States and Britain, which guarantees three days of delivery in Western Europe and North America.

Prices given in U.S. dollars, and for customers, it is especially reasonable when there is free shipping on all orders.”

PLEASE DO NOT ENTER THIS URL – hx_xp:// deal DONOTENTER extreme . com

Description

An ExploitKit is currently one of the most popular web threats. Its purpose is to deliver a malicious payload to a victim's computer.

There are many version of ExploitKits with different names and options.

Analysis

The malicious files where embedded in the deal extreme website via an Iframe or were part of a malicious advertisement a.k.a malvertisement.

From wiki: “*A malvertisement is an infected online ad. The spread of malicious ads on the Internet's top commercial websites has recently taken a turn for the worse.”*

URL information: (the links are un-clickable)

URL:

hx_xp://www . deal extreme . com

URL that linked to the URL that host the malware:

hx_xp://e. storesbay . com/www/delivery/afr.php?zoneid=1&cb=INSERT_RANDOM_NUMBER_HERE

URL that hosts the malware:

hx_xp:// prisnssas . tk/24842.jar

Malicious files:

hx_xp:// prisnssas . tk/24842.jar

Hx_xp:// prisnssas . tk/a/b.class

Hx_xp:// prisnssas . tk/a/b/class.class

Exploit

The exploit that was used is:

Java AtomicReferenceArray vulnerability

or a variant of this exploit.

It might be a part of "RedKit" exploit kit or "BlackHole" exploit kit.

CVE Reference

CVE-2012-0507: cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507

Recommendations

1. Do not enter the deal extreme website.
2. Use advertisements blockers.
3. Disable or remove Java from your machine.

Disclosure Timeline

28 May 2012 – Vulnerability found.

29 May 2012 – Vendor Notification.

30 May 2012 – Public Disclosure.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team/Yaniv Miron.

About FortConsult

FortConsult provides independent security assessment services, including penetration testing and PCI DSS assessment service internationally to customers, such as financial services companies, banks, acquirers, service providers and merchants.

See www.fortconsult.com for more information about FortConsult.

Or contact us at +45 7020 7525 or info@fortconsult.net.

Copyright and Disclaimer

The information in this advisory is Copyright FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.