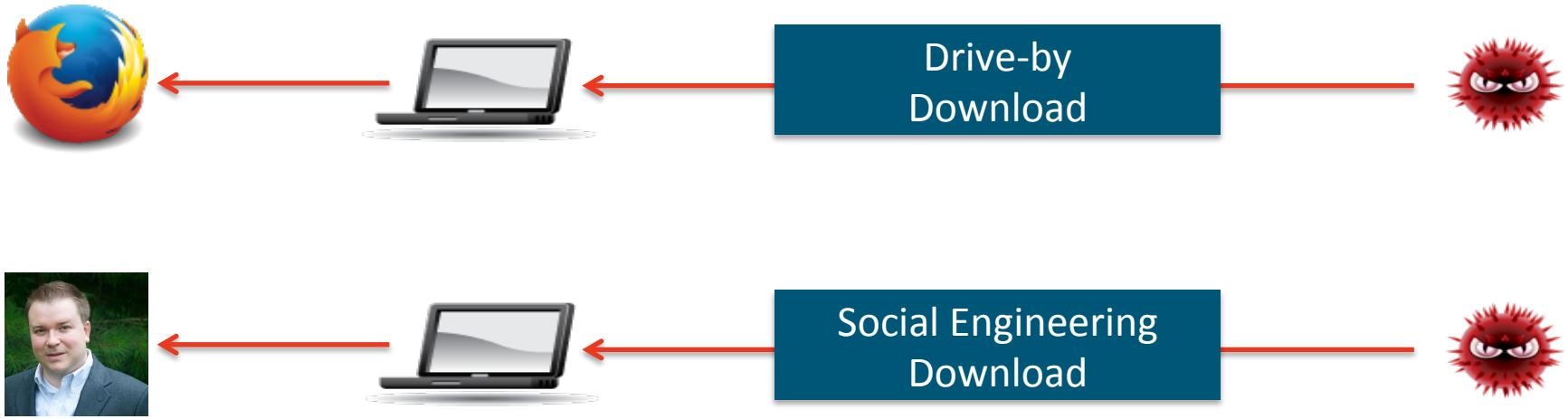
Towards Measuring and Mitigating Social Engineering Software Download Attacks

Terry Nelms[1,2], Roberto Perdici[3,1], Manos Antonakakis[1], Mustaque Ahamd[1,4]

[1]Georgia Institute of Technology
[2]Damballa, Inc.
[3]University of Georgia
[4]New York University Abu Dhabi

tnelms@gatech.edu, perdisci@cs.uga.edu, manos@gatech.edu, mustaq@cc.gatech.edu

How Modern Malware Infections Occur



Study of Web-Based Social Engineering Downloads

- Data collection on a large academic network for two months.
- Real-time deep packet inspection of network traffic.
- Maintain a data buffer of all recent HTTP transactions.
- On executable download record all web traffic from client.

Study of Web-Based Social Engineering Downloads

- Collected a total of 35,638 downloads
- 2,004 real world successful SE downloads
- Full web path reconstruction
- Extensive manual analysis

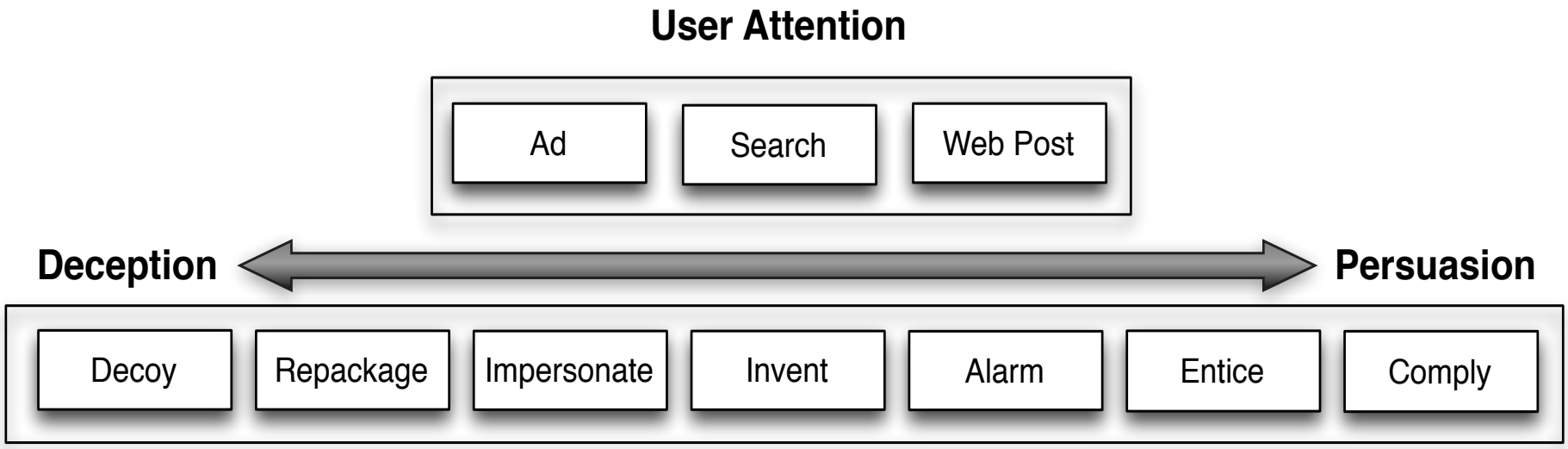
Outline

- Categorizing SE Download Tactics
- Measuring SE Download Properties
- Detecting SE Download Attacks

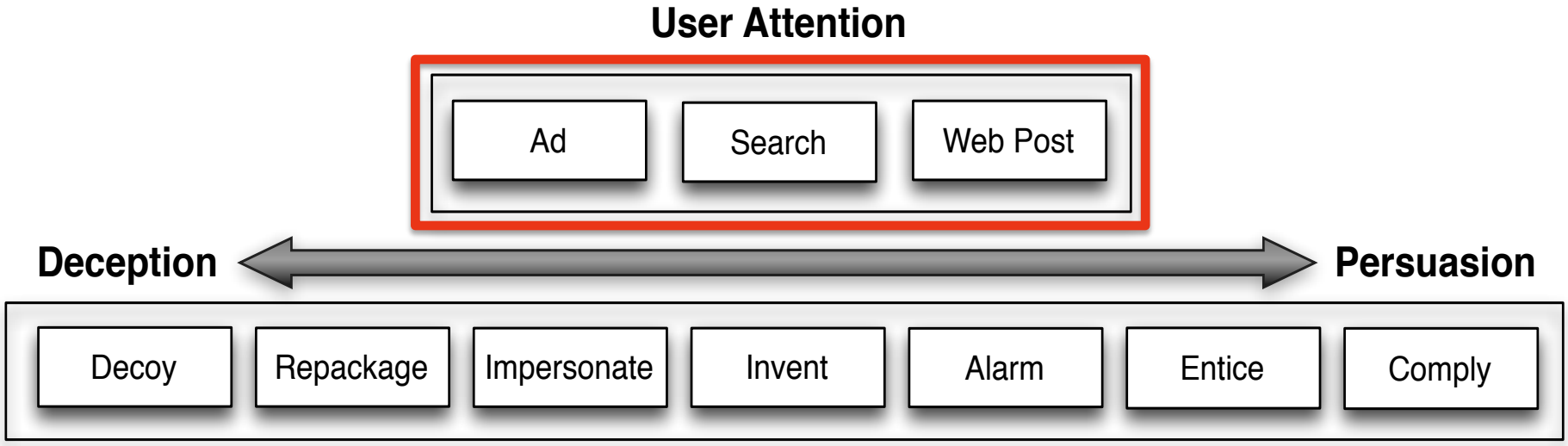
Outline

- Categorizing SE Download Tactics
- Measuring SE Download Properties
- Detecting SE Download Attacks

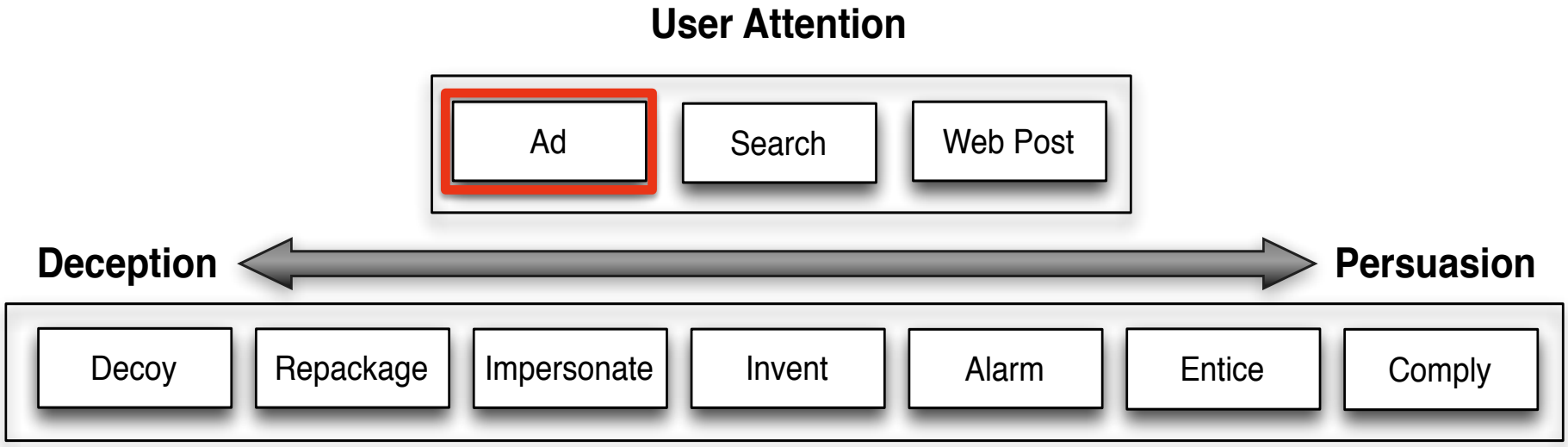
SE Download Categorization



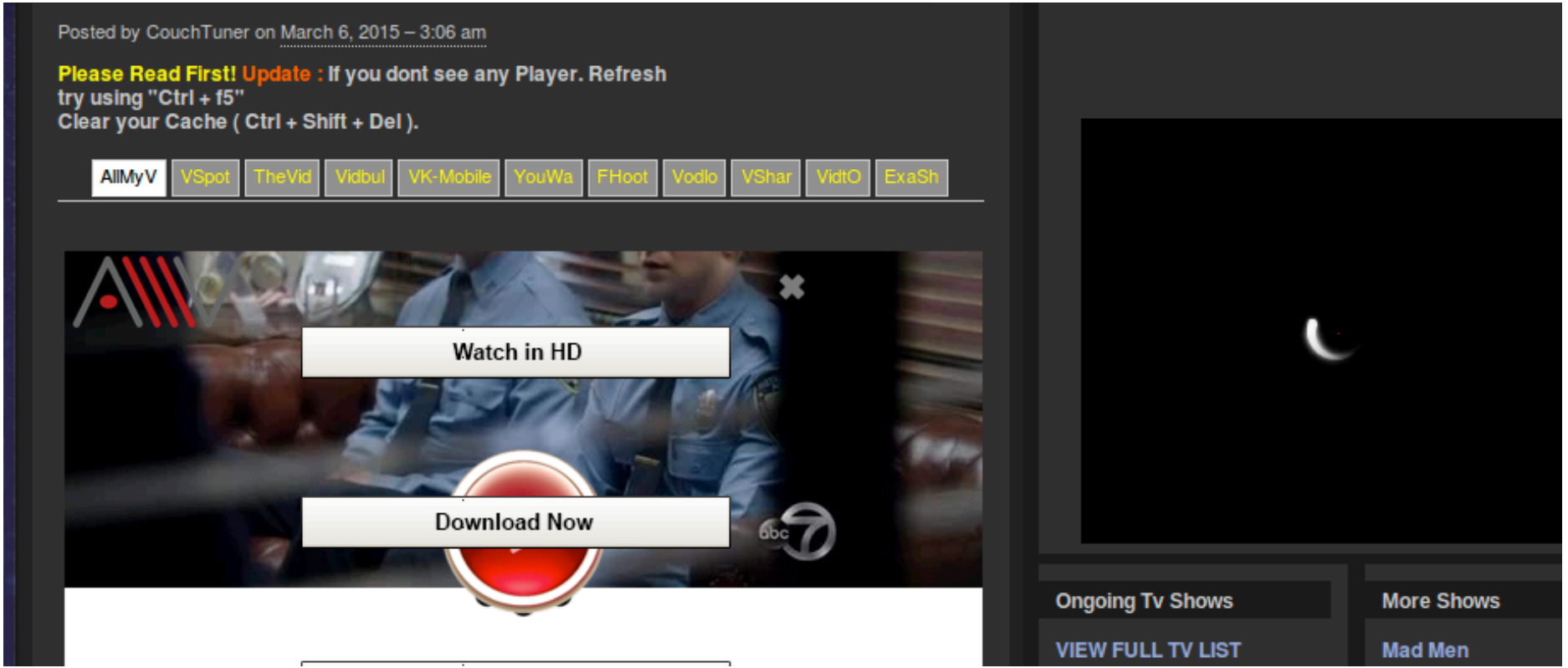
SE Download Categorization



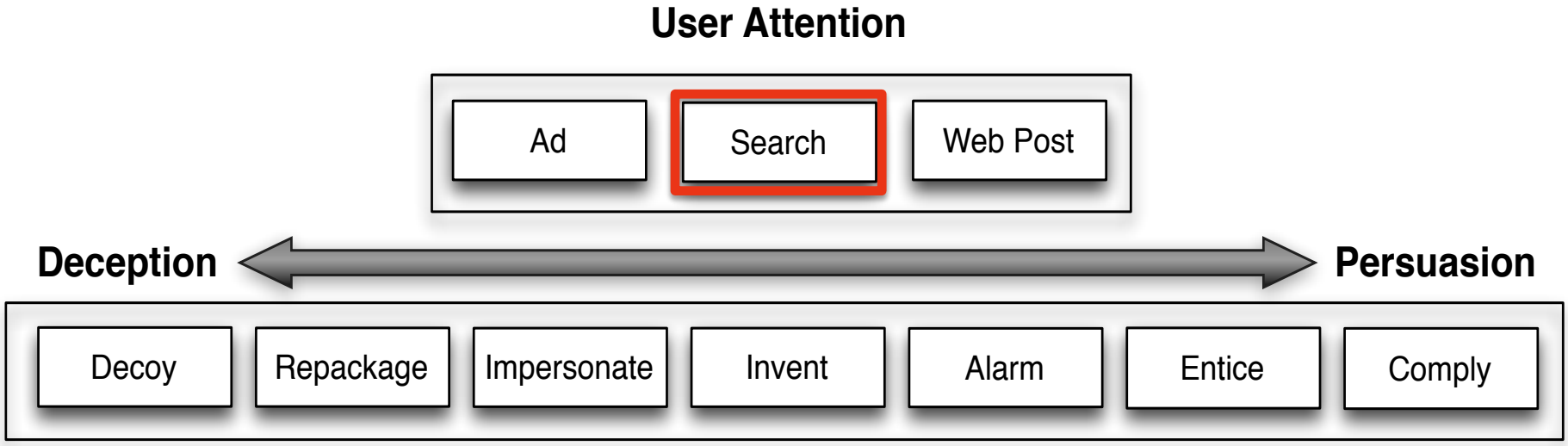
SE Download Categorization



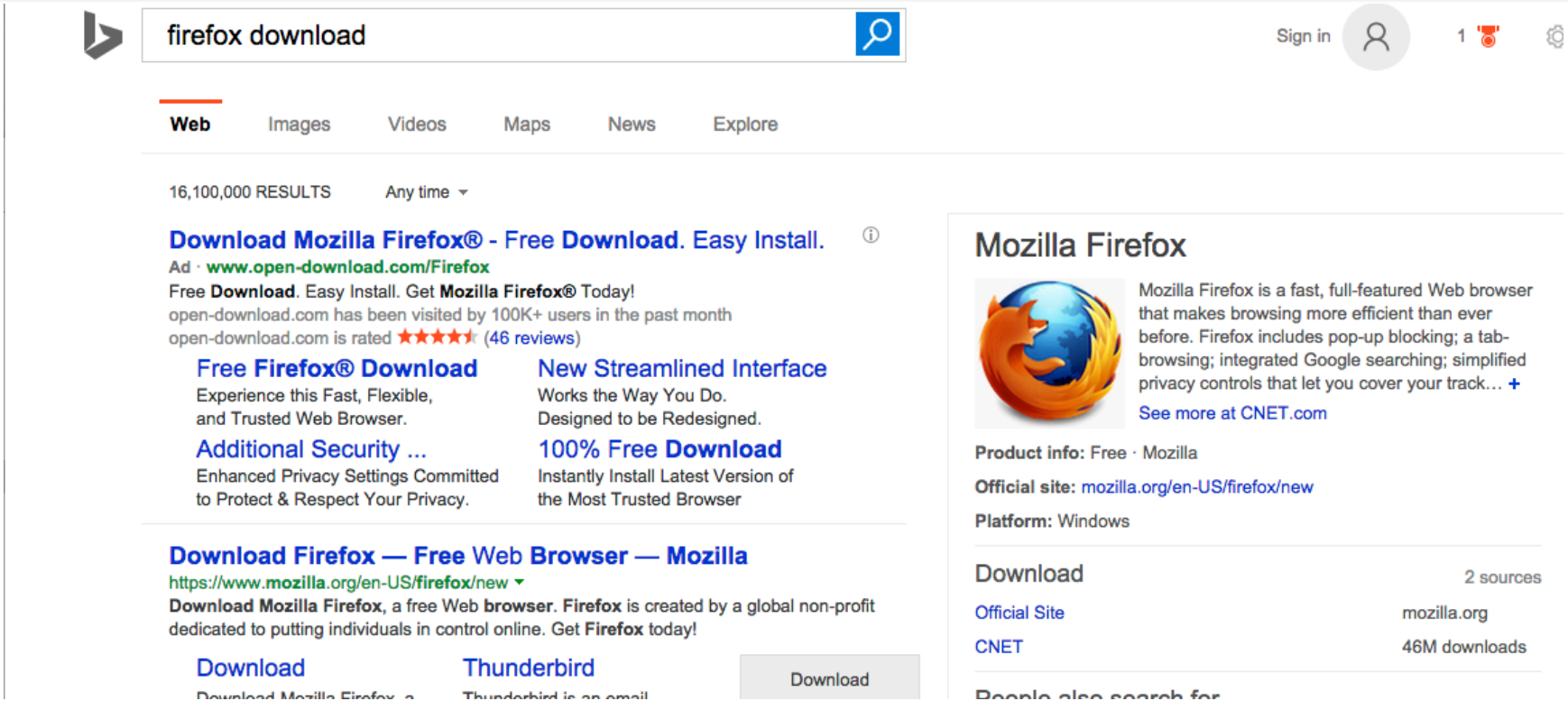
Advertisement



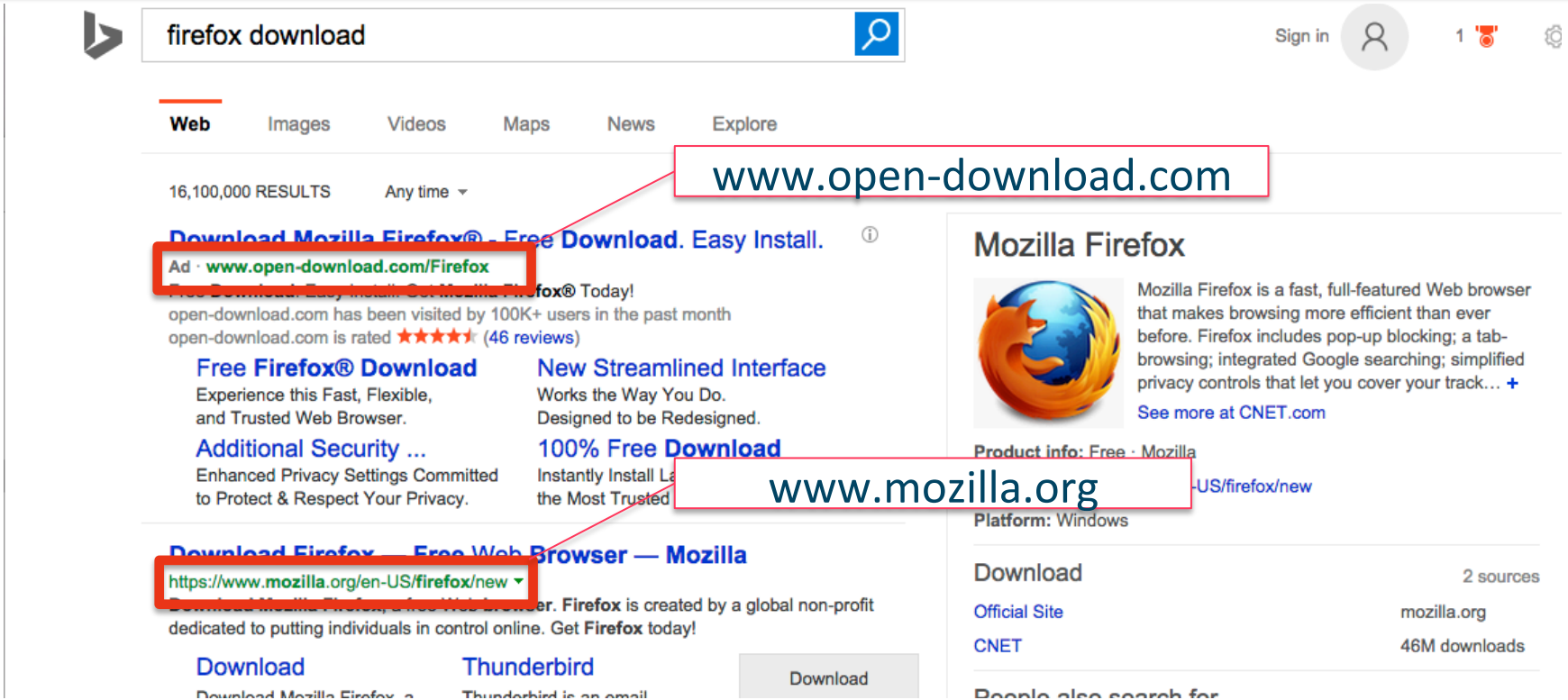
SE Download Categorization



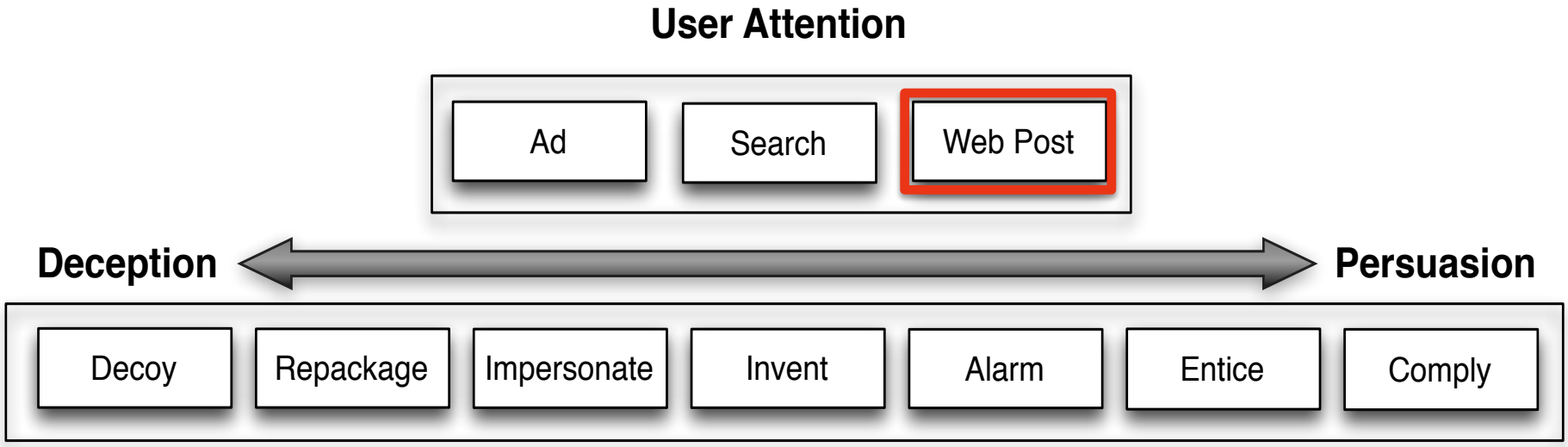
Search


firefox download
Sign in
1
Web
Images
Videos
Maps
News
Explore
16,100,000 RESULTS
Any time
Download Mozilla Firefox® - Free Download. Easy Install.
Ad · www.open-download.com/Firefox
Free Download. Easy Install. Get Mozilla Firefox® Today!
open-download.com has been visited by 100K+ users in the past month
open-download.com is rated (46 reviews)
Free Firefox® Download
Experience this Fast, Flexible, and Trusted Web Browser.
New Streamlined Interface
Works the Way You Do. Designed to be Redesigned.
Additional Security ...
Enhanced Privacy Settings Committed to Protect & Respect Your Privacy.
100% Free Download
Instantly Install Latest Version of the Most Trusted Browser
Download Firefox — Free Web Browser — Mozilla
https://www.mozilla.org/en-US/firefox/new
Download Mozilla Firefox, a free Web browser. Firefox is created by a global non-profit dedicated to putting individuals in control online. Get Firefox today!
Download
Thunderbird
Download
Mozilla Firefox
Mozilla Firefox is a fast, full-featured Web browser that makes browsing more efficient than ever before. Firefox includes pop-up blocking; a tab-browsing; integrated Google searching; simplified privacy controls that let you cover your track... +
See more at CNET.com
Product info: Free · Mozilla
Official site: mozilla.org/en-US/firefox/new
Platform: Windows
Download
2 sources
Official Site
mozilla.org
CNET
46M downloads

Search


firefox download
Sign in
1
Web
Images
Videos
Maps
News
Explore
16,100,000 RESULTS
Any time
www.open-download.com
Ad · www.open-download.com/Firefox
open-download.com has been visited by 100K+ users in the past month
open-download.com is rated (46 reviews)
Free Firefox® Download
Experience this Fast, Flexible, and Trusted Web Browser.
New Streamlined Interface
Works the Way You Do. Designed to be Redesigned.
Additional Security ...
Enhanced Privacy Settings Committed to Protect & Respect Your Privacy.
100% Free Download
www.mozilla.org
https://www.mozilla.org/en-US/firefox/new
dedicated to putting individuals in control online. Get Firefox today!
Download
Thunderbird
Download
Mozilla Firefox
Mozilla Firefox is a fast, full-featured Web browser that makes browsing more efficient than ever before. Firefox includes pop-up blocking; a tab-browsing; integrated Google searching; simplified privacy controls that let you cover your track... +
See more at CNET.com
Product info: Free · Mozilla
Platform: Windows
Download
2 sources
Official Site
mozilla.org
CNET
46M downloads

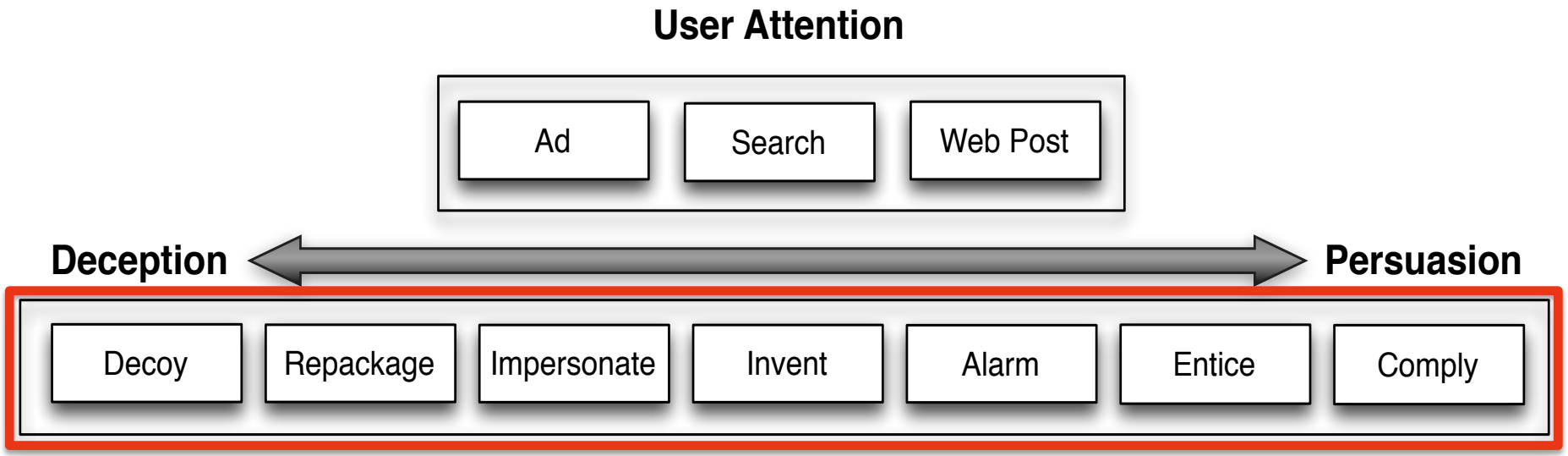
SE Download Categorization



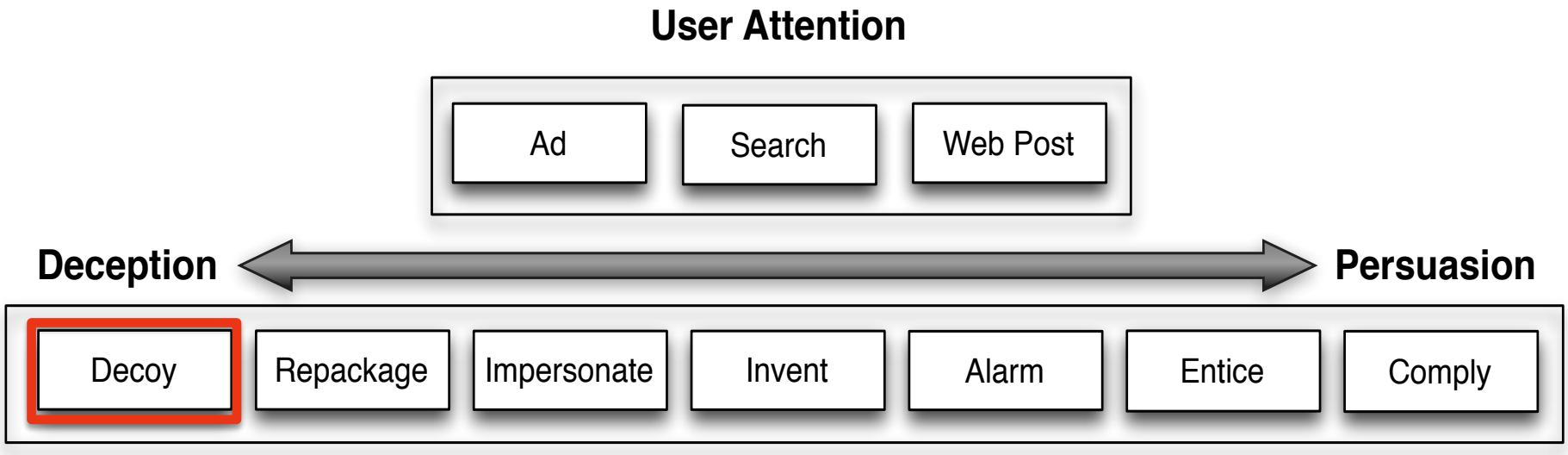
Web Post


Forums : General Discussion > Integrated Chinese Third Edition Level 1 Part 1 Answer Key
whalyol (Applicant) 8/13/2014 6:43 AM EST : Integrated Chinese Third Edition Level 1 Part 1 Answe... link
whalyol
Posts: 189
0
Like
0
Dislike
vs Primer
ill Chinese
iocheng 第三册 上
uyu
r Beginning Students
; An Invitation to Chinese 1
d Chinese
tegrated Chinese 1 (1st edition)
tegrated Chinese 1 (2nd edition)
tegrated Chinese 1 (3rd edition)
tegrated Chinese 2 (2nd edition)
tegrated Chinese 2 (3rd edition)
inese With Me
ndarin in Steps
Chinese Characters (Tuttle)
Integrated Chinese Third Edition Level 1 Part 1 Answer Key > http://tinyurl.com/p7e5jy3
MaXiHeaLZ
Earned "Your Active!" 3/21/2012 4:46 PM
TearsofSorrow
Earned "Being Involved!" 3/9/2012 1:34 PM
ullgur
Earned "Your Active!" 3/4/2012 9:51 AM
Jazamina
Earned "Cool Kids Crowd!" 2/9/2012 5:32 PM
TearsofSorrow
Earned "Your Active!" 1/22/2012 12:25 AM
1 2 3 4
Advertisement

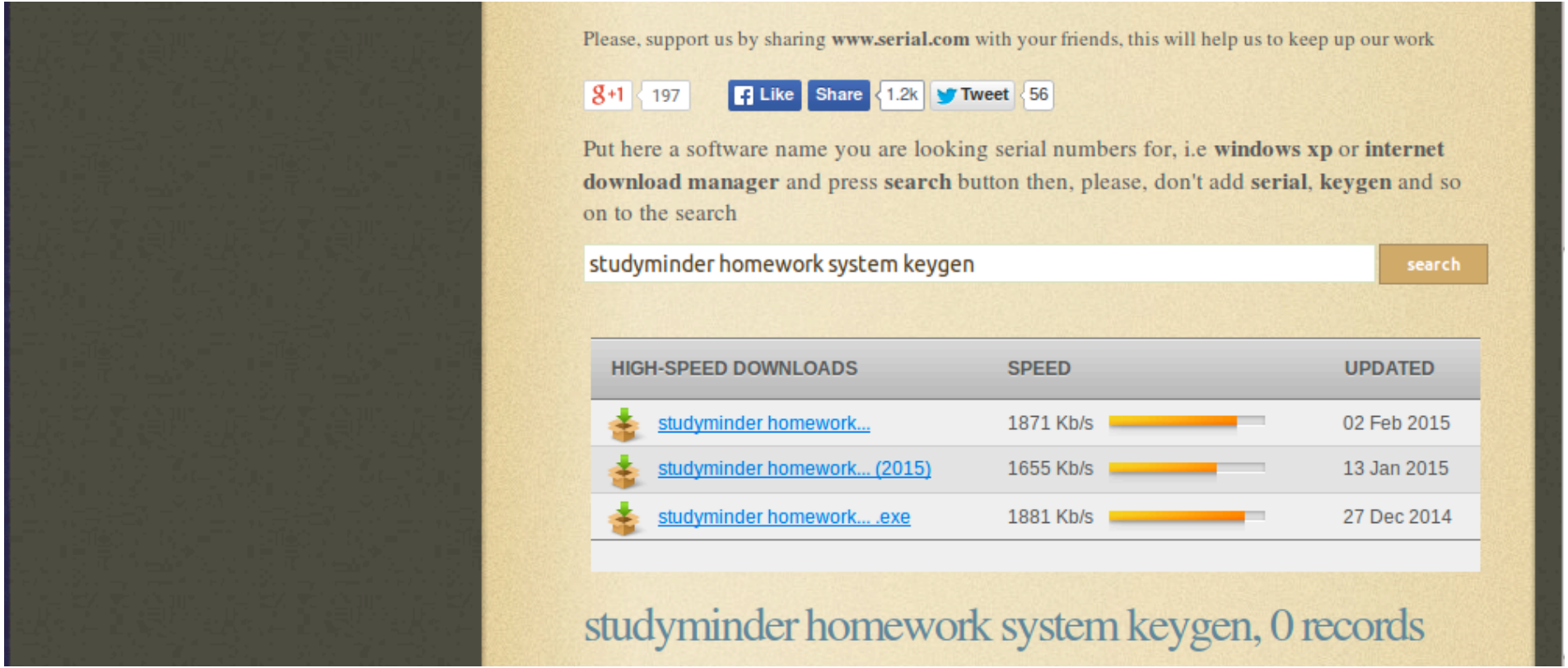
SE Download Categorization



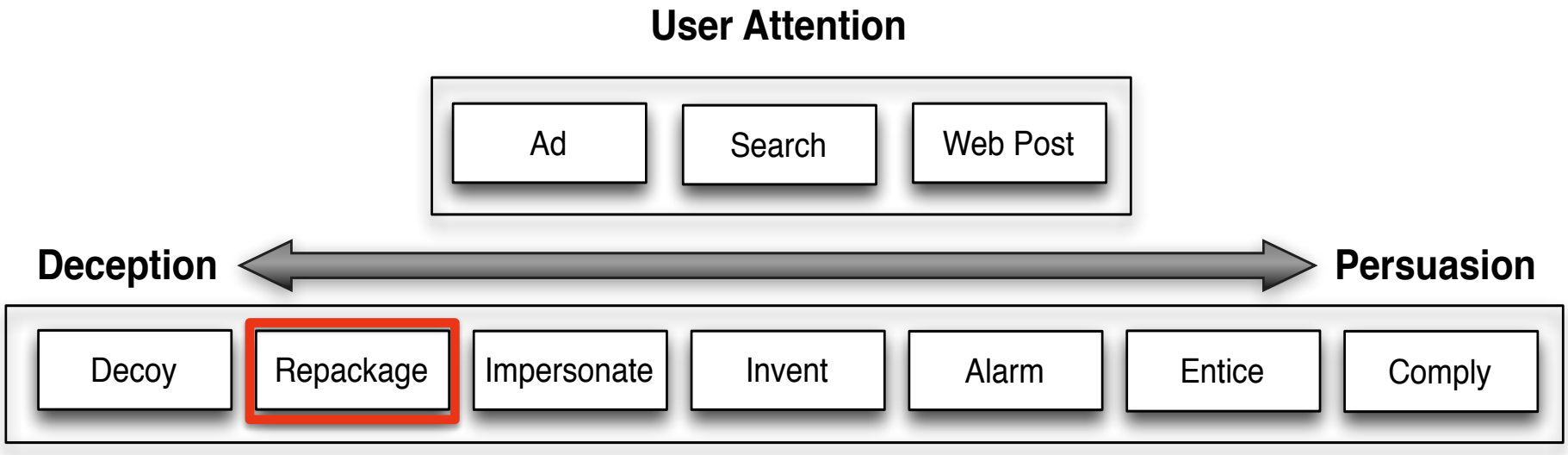
SE Download Categorization



Decoy


Please, support us by sharing www.serial.com with your friends, this will help us to keep up our work
g+1 197
Like Share 1.2k
Tweet 56
Put here a software name you are looking serial numbers for, i.e windows xp or internet download manager and press search button then, please, don't add serial, keygen and so on to the search
studyminder homework system keygen
search
HIGH-SPEED DOWNLOADS
SPEED
UPDATED
studyminder homework...
1871 Kb/s
02 Feb 2015
studyminder homework... (2015)
1655 Kb/s
13 Jan 2015
studyminder homework... .exe
1881 Kb/s
27 Dec 2014
studyminder homework system keygen, 0 records

SE Download Categorization



Repackage

Free Download

By clicking "Download" DownloadInfo distributes software **via an ad-supported download manager system**. This software may be available free elsewhere. The software is in its original form, and no affiliation with Mozilla is intended. Terms of Service | Uninstall Instructions

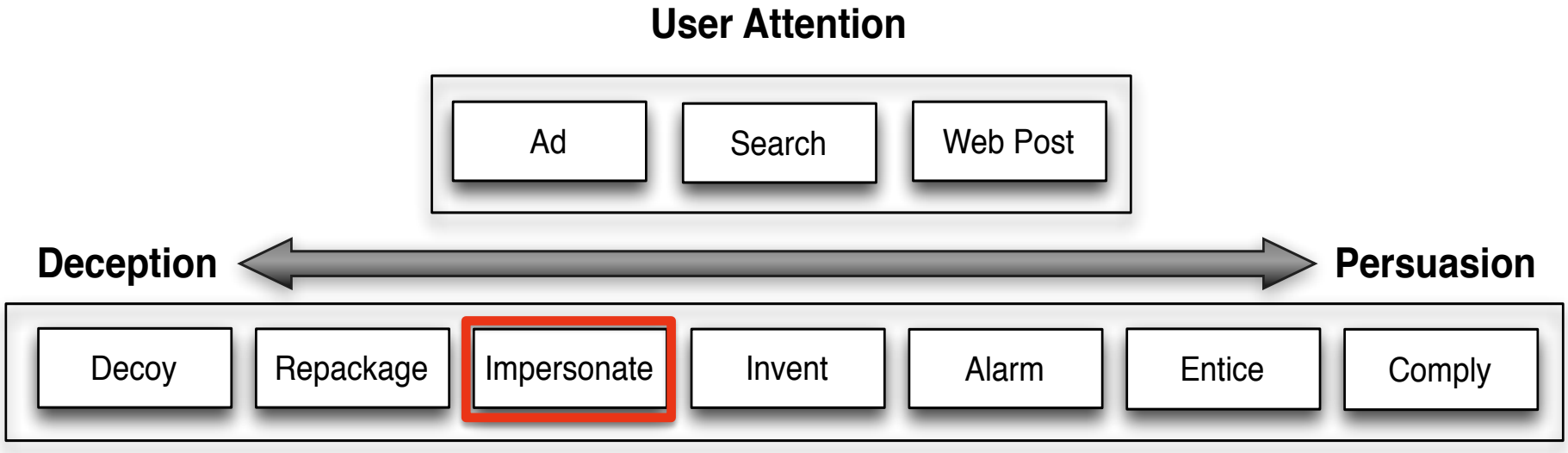
Rating:	★★★★☆
Version:	29.0.1
Price:	Free
Compatibility:	Windows XP, Windows Vista, Windows 7, Windows 8

Firefox Overview

Firefox Review

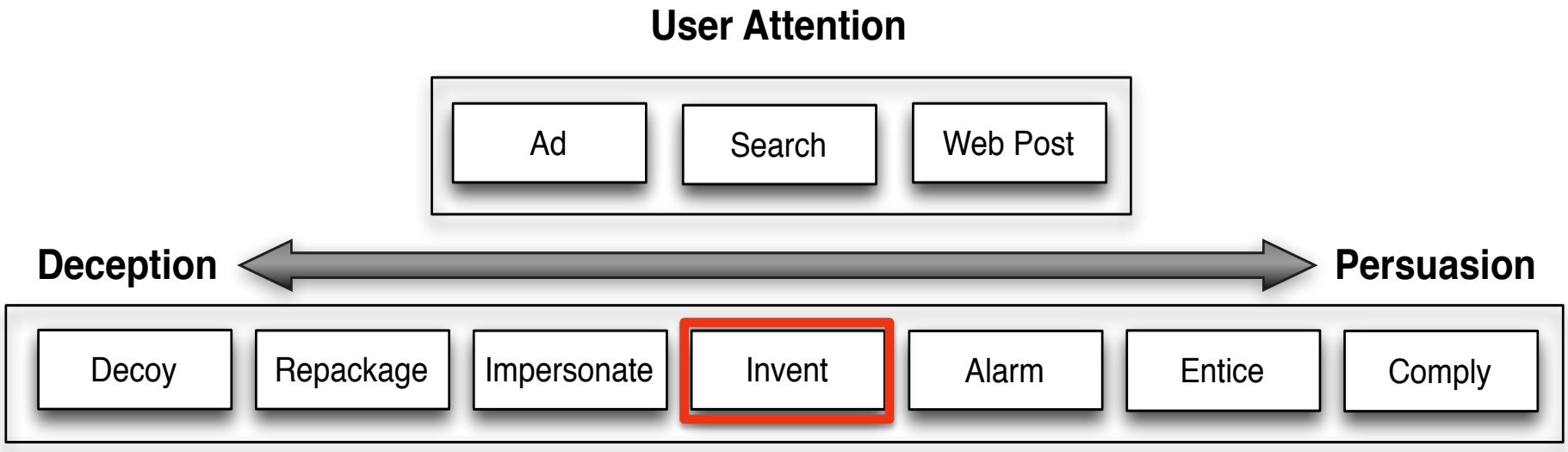
Firefox jumped into the browser wars 11 years ago, managing to offer a cleaner and faster alternative to Internet Explorer. Mozilla, the creators of Firefox, seemed to slow down after a few years though, and their browser market share dropped significantly. Now that there are 3 leading competitors in the web browser market, Mozilla has a lot of work they need to do if they want to stay or improve upon their current 25% browser usage.With Firefox version 29.0.1, Mozilla has released hundreds of improvements for their flagship browser software. The desktop version of the browser has seen a new and updated interface for its 29th iteration, and the new interface works really well. The standard design has been cleaned up significantly. Customization is the most important new feature that Mozilla wants people to know about. The menu now features a grid with 3 columns of icons instead of a vertical list of text buttons. This menu holds the options, history, print, and all other standard browser tools. It also can contain add-ons downloaded from Mozilla's download center. These options and add-ons can be rearranged in the order the user wants the buttons to appear. Buttons that the user doesn't want can be removed entirely from the menu. If this is done though, Mozilla did not leave a button to see all of the menu items. The only way to access that application or option again would be to add it to the menu first and then launch it. Additional new features in Firefox 29.0.1 include improved Firefox Sync, allowing browser history, tabs, passwords, bookmarks, and preferences. Syncing is done by either creating a Mozilla account or by pairing up

SE Download Categorization

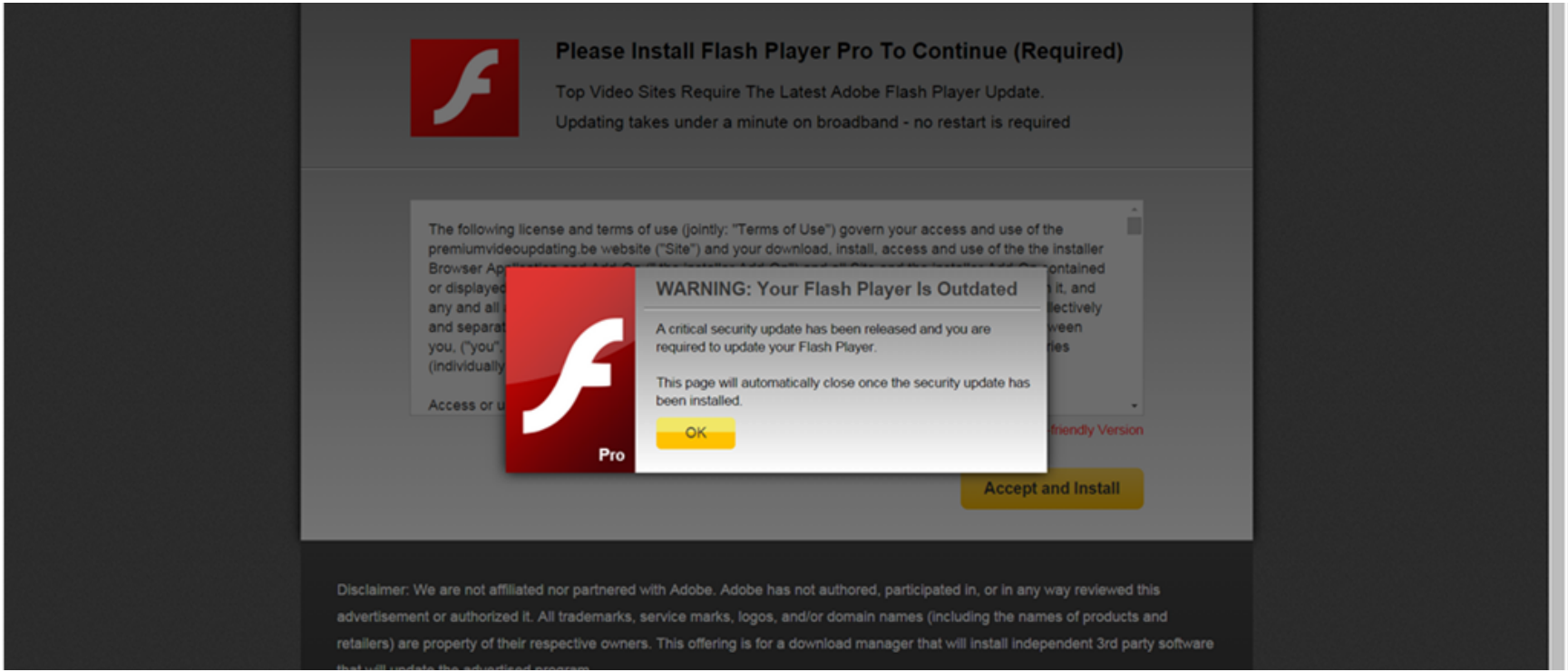


Impersonate

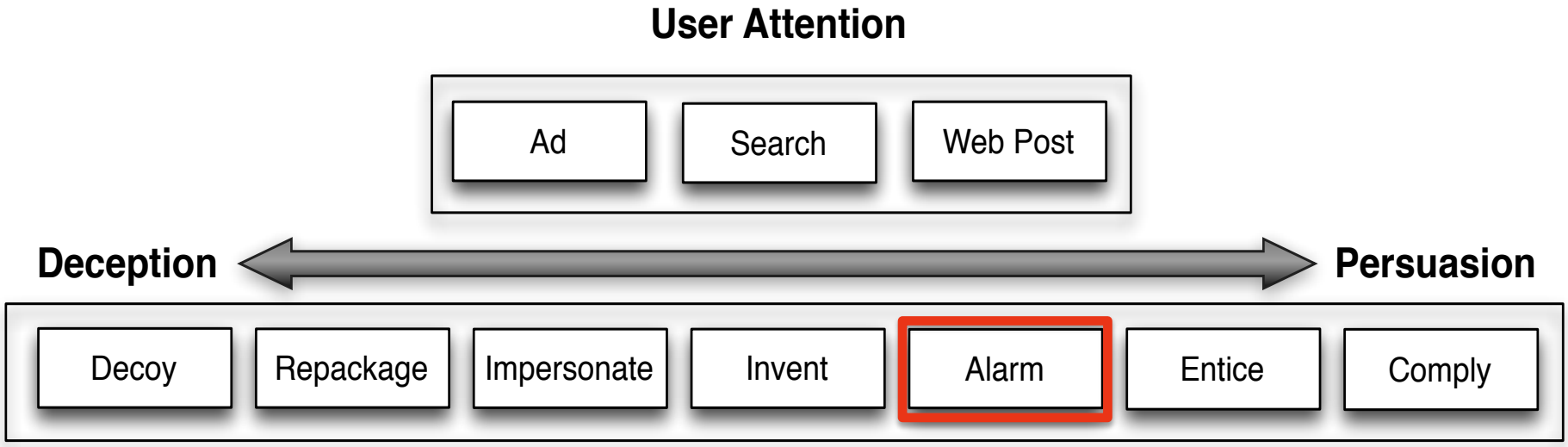
SE Download Categorization



Invent


Please Install Flash Player Pro To Continue (Required)
Top Video Sites Require The Latest Adobe Flash Player Update.
Updating takes under a minute on broadband - no restart is required
The following license and terms of use (jointly: "Terms of Use") govern your access and use of the premiumvideoupdating.be website ("Site") and your download, install, access and use of the the installer
WARNING: Your Flash Player Is Outdated
A critical security update has been released and you are required to update your Flash Player.
This page will automatically close once the security update has been installed.
OK
Pro
Accept and Install
Disclaimer: We are not affiliated nor partnered with Adobe. Adobe has not authored, participated in, or in any way reviewed this advertisement or authorized it. All trademarks, service marks, logos, and/or domain names (including the names of products and retailers) are property of their respective owners. This offering is for a download manager that will install independent 3rd party software

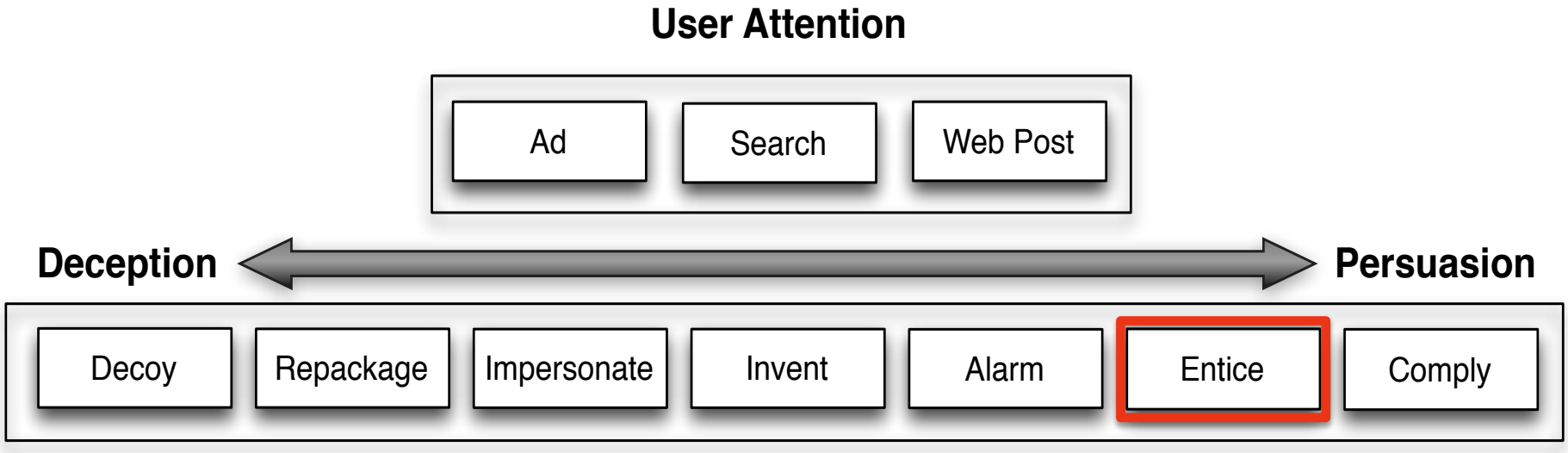
SE Download Categorization



Alarm


EBOLA EARLY WARNING SYSTEM
ARE YOU SAFE FROM EBOLA?
DON'T FALL VICTIM TO ONE OF THE DEADLIEST PLAGUES IN HISTORY!
GET INSTANTLY NOTIFIED WHEN EBOLA STRIKES NEAR YOU!
DANGER!
EBOLA ALERT NEAR YOU!!
DOWNLOAD NOW
HOW CLOSE WILL YOU BE TO THE NEXT OUTBREAK?
Over 4,500 deaths & counting

SE Download Categorization



Entice

Info

download the latest minecraft x-ray mod 1.8 / 1.8.1 .This mod is nice and useful to players who have difficult time of cave hunting or are for endless minecraft diamond search.I is easy to use and simple as 1.2.3. to install. I could say some of the features would be that you can customize almost everything you can chose what block can be hidden or whit what key you can enable x-ray mod.As well you can use it too find players, mobs , mob spawns and a lot more.
==========

Default Key bind

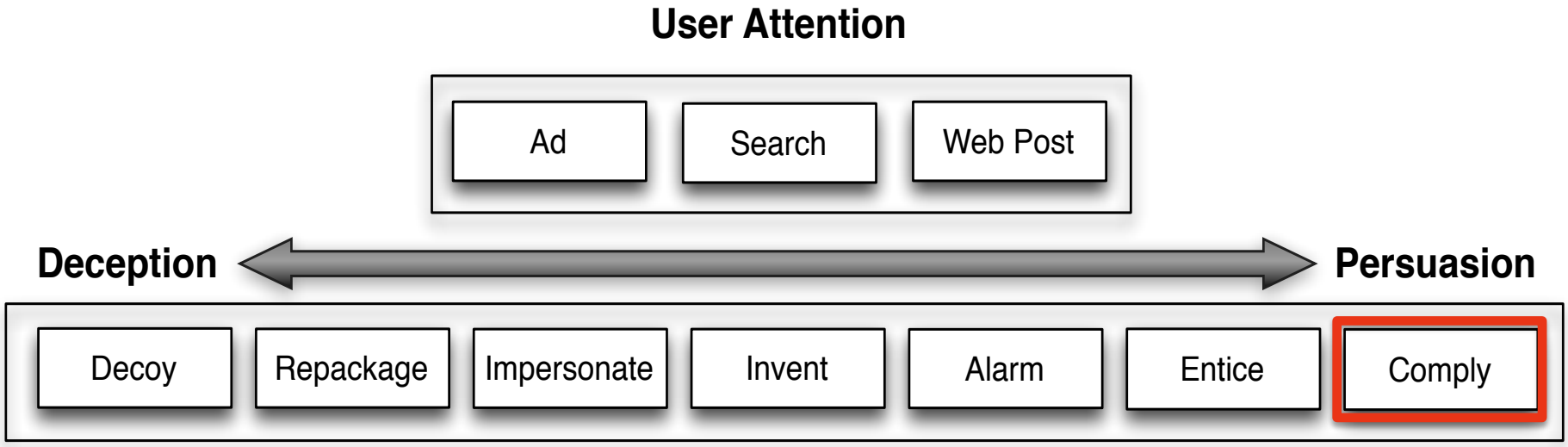
X toggles X Ray
R toggles Red stone finder
C toggles Cave finder
B toggles Fullbright
J toggles Coordinates

==========

Download

Minecraft x-ray mod 1.8 / 1.8.1

SE Download Categorization



Comply


Install Media Downloader
in order to watch videos (required)
• Watch HD videos online
• Enhanced video and audio files support
• Supports multi video formats and resolution
• Supports FLV/Flash
See details User license Agreement
Installing takes under a minute - No restart is required

Outline

- Categorizing SE Download Tactics
- Measuring SE Download Properties
- Detecting SE Download Attacks

Popularity of SE Tactics for Tricking the User

Trick	Total	Percentage
Repackage+Entice	972	48.5%
Invent+Impersonate+Alarm	434	21.7%
Invent+Impersonate+Comply	384	19.2%
Repackage+Decoy	155	7.7%
Impersonate+Decoy	46	2.3%
Impersonate+Entice+Decoy	12	0.6%
Invent+Comply	4	0.2%
Impersonate+Alarm	1	0.1%

Popularity of SE Tactics for Tricking the User

Trick	Total	Percentage
Repackage+Entice	972	48.5%
Invent+Impersonate+Alarm	434	21.7%
Invent+Impersonate+Comply	384	19.2%
Repackage+Decoy	155	7.7%
Impersonate+Decoy	46	2.3%
Impersonate+Entice+Decoy	12	0.6%
Invent+Comply	4	0.2%
Impersonate+Alarm	1	0.1%

Top 3 Responsible for over 89%.

Repackage + Entice (48.5%)

Free Download

By clicking "Download" DownloadInfo distributes software **via an ad-supported download manager system**. This software may be available free elsewhere. The software is in its original form, and no affiliation with Mozilla is intended. Terms of Service | Uninstall Instructions

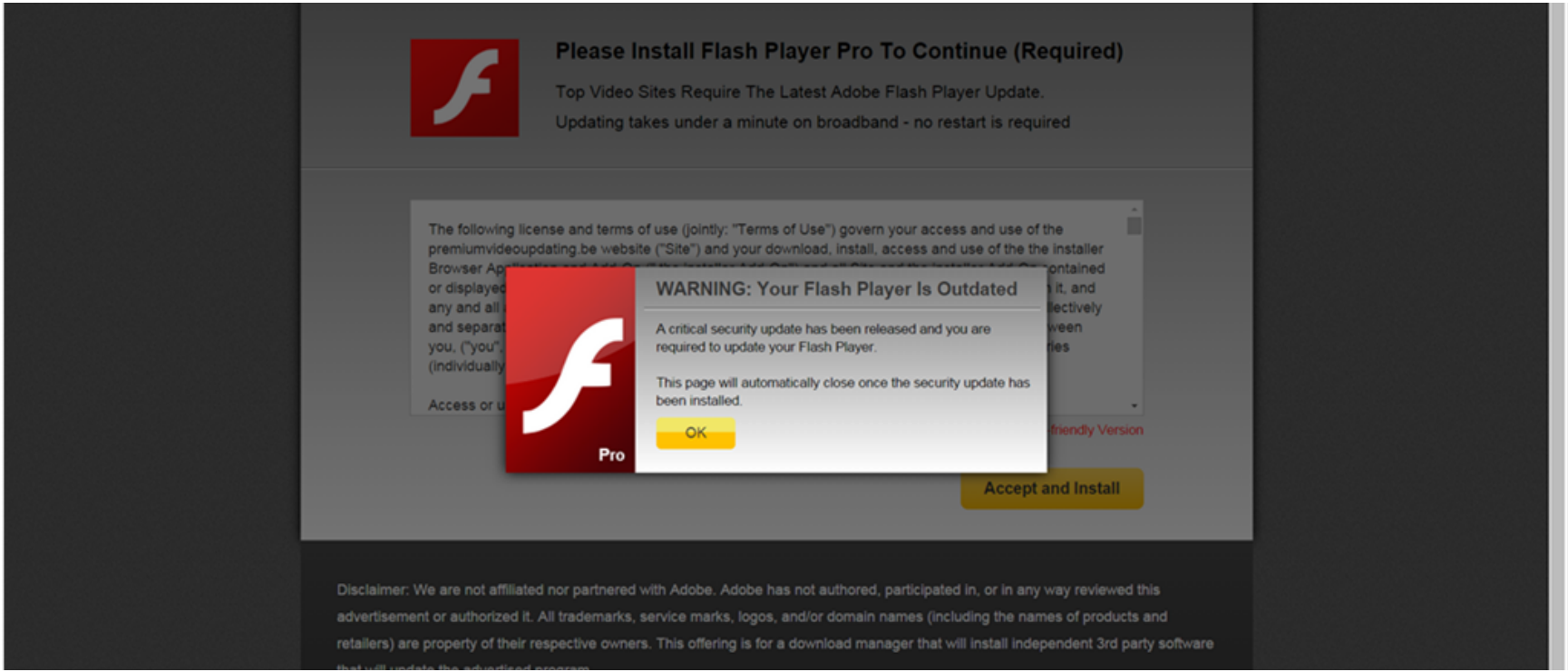
Rating:	★★★★☆
Version:	29.0.1
Price:	Free
Compatibility:	Windows XP, Windows Vista, Windows 7, Windows 8

Firefox Overview

Firefox Review

Firefox jumped into the browser wars 11 years ago, managing to offer a cleaner and faster alternative to Internet Explorer. Mozilla, the creators of Firefox, seemed to slow down after a few years though, and their browser market share dropped significantly. Now that there are 3 leading competitors in the web browser market, Mozilla has a lot of work they need to do if they want to stay or improve upon their current 25% browser usage.With Firefox version 29.0.1, Mozilla has released hundreds of improvements for their flagship browser software. The desktop version of the browser has seen a new and updated interface for its 29th iteration, and the new interface works really well. The standard design has been cleaned up significantly. Customization is the most important new feature that Mozilla wants people to know about. The menu now features a grid with 3 columns of icons instead of a vertical list of text buttons. This menu holds the options, history, print, and all other standard browser tools. It also can contain add-ons downloaded from Mozilla's download center. These options and add-ons can be rearranged in the order the user wants the buttons to appear. Buttons that the user doesn't want can be removed entirely from the menu. If this is done though, Mozilla did not leave a button to see all of the menu items. The only way to access that application or option again would be to add it to the menu first and then launch it. Additional new features in Firefox 29.0.1 include improved Firefox Sync, allowing browser history, tabs, passwords, bookmarks, and preferences. Syncing is done by either creating a Mozilla account or by pairing up

Invent + Impersonate + Alarm (21.7)



Invent + Impersonate + Comply (19.2%)

Invent + Impersonate Subclass (Tactics Popularity)

	Alarm	Comply
Fake Flash	68%	20%
Fake Java	30%	0%
Fake AV	1%	0%
Fake Browser	1%	0%
Fake Player	0%	80%

Popularity of SE Tactics for Gaining the User's Attention

User's Attention	Total	Percentage
Ad	1,616	80.6%
Search+Ad	146	7.3%
Search	127	6.3%
Web Post	115	5.7%

Popularity of SE Tactics for Gaining the User's Attention

User's Attention	Total	Percentage
Ad	1,616	80.6%
Search+Ad	146	7.3%
Search	127	6.3%
Web Post	115	5.7%

Almost 88% used advertisements.

Benign Ad Based Downloads

- 7% of all benign downloads are ad-based.
- 40% chance that an ad-based download is benign.
- Trion Worlds is the most popular followed by Spotify.

Category	Percentage
Games	32%
Utilities	30%
Music	15%
Business	11%
Video	8%
Graphics	2%
Social	2%

Top 5 Ad Entry Point Domains

Comply	Alarm	Entice
26% onclickads.net	16% adcash.com	20% doubleclick.net
10% adcash.com	7% onclickads.net	16% google.com
10% popads.net	7% msn.com	12% googleadservices.com
7% putlocker.is	6% yesadsrv.com	11% msn.com
3% allmyvideos.net	4% yu0123456.com	8% coupons.com

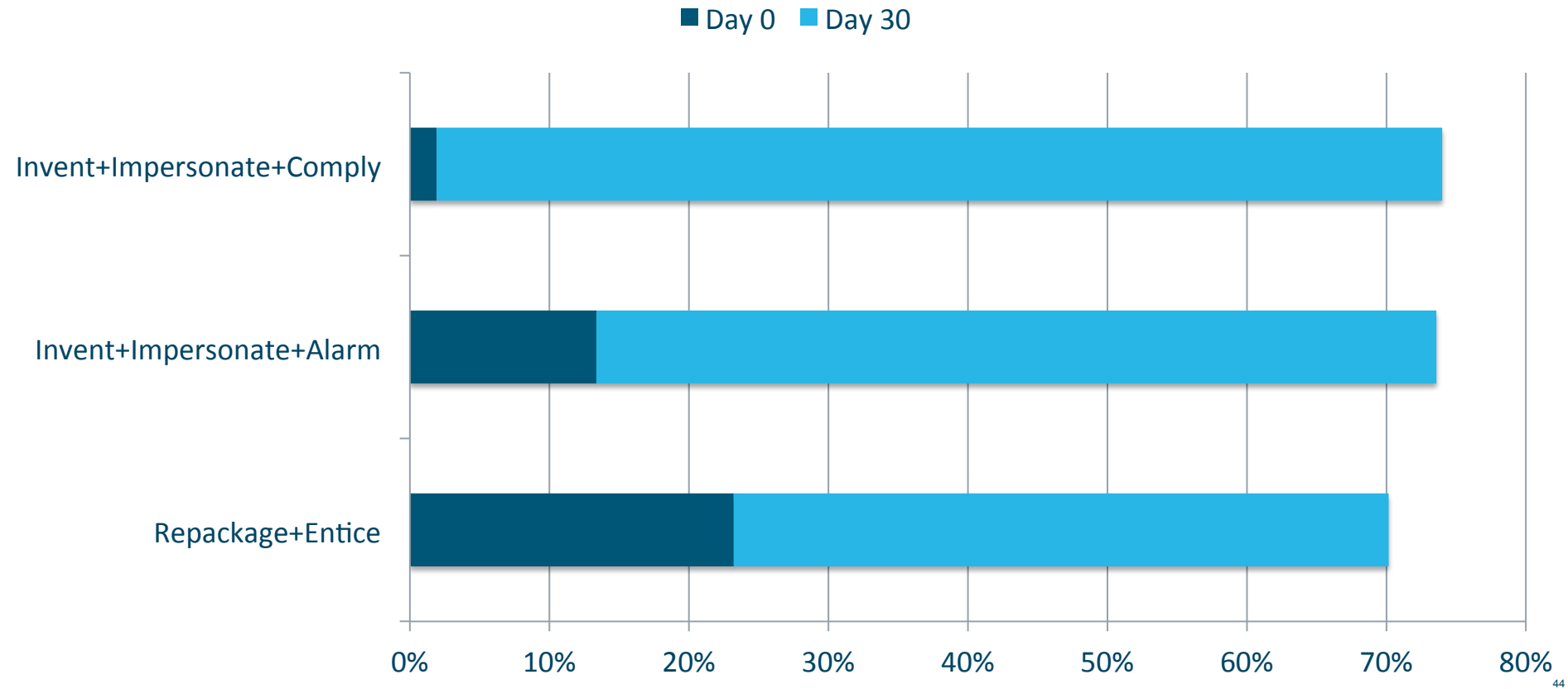
Top 5 Ad Entry Point Domains

Comply	Alarm	Entice
26% onclickads.net	16% adcash.com	20% doubleclick.net
10% adcash.com	7% onclickads.net	16% google.com
10% popads.net	7% msn.com	12% googleadservices.com
7% putlocker.is	6% yesadsrv.com	11% msn.com
3% allmyvideos.net	4% yu0123456.com	8% coupons.com

Outline

- Categorizing SE Download Tactics
- Measuring SE Download Properties
- Detecting SE Download Attacks

AV Detection (Day 0 and Day 30)



Classifying Social Engineering Downloads

- **Ad Chain Features**
  - Ad-Driven
  - Minimum Ad Domain Age
  - Maximum Ad Domain Popularity
- **Download URL Features**
  - Download Domain Age
  - Download Domain Alexa Rank

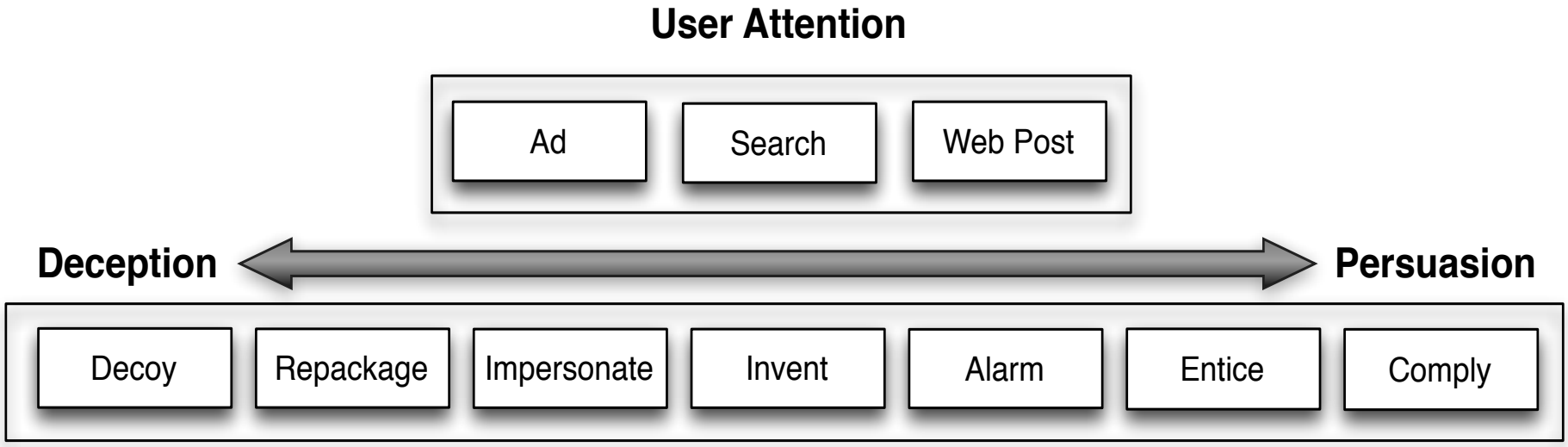
Classifying Social Engineering Downloads

	Predicted Class: Ad-Based SE	Predicted Class: Benign
Ad-Based SE	91.2%	8.8%
Benign	0.5%	99.5%

True Positive Rate

False Positive Rate

Conclusion


User Attention
Ad
Search
Web Post
Deception
Persuasion
Decoy
Repackage
Impersonate
Invent
Alarm
Entice
Comply

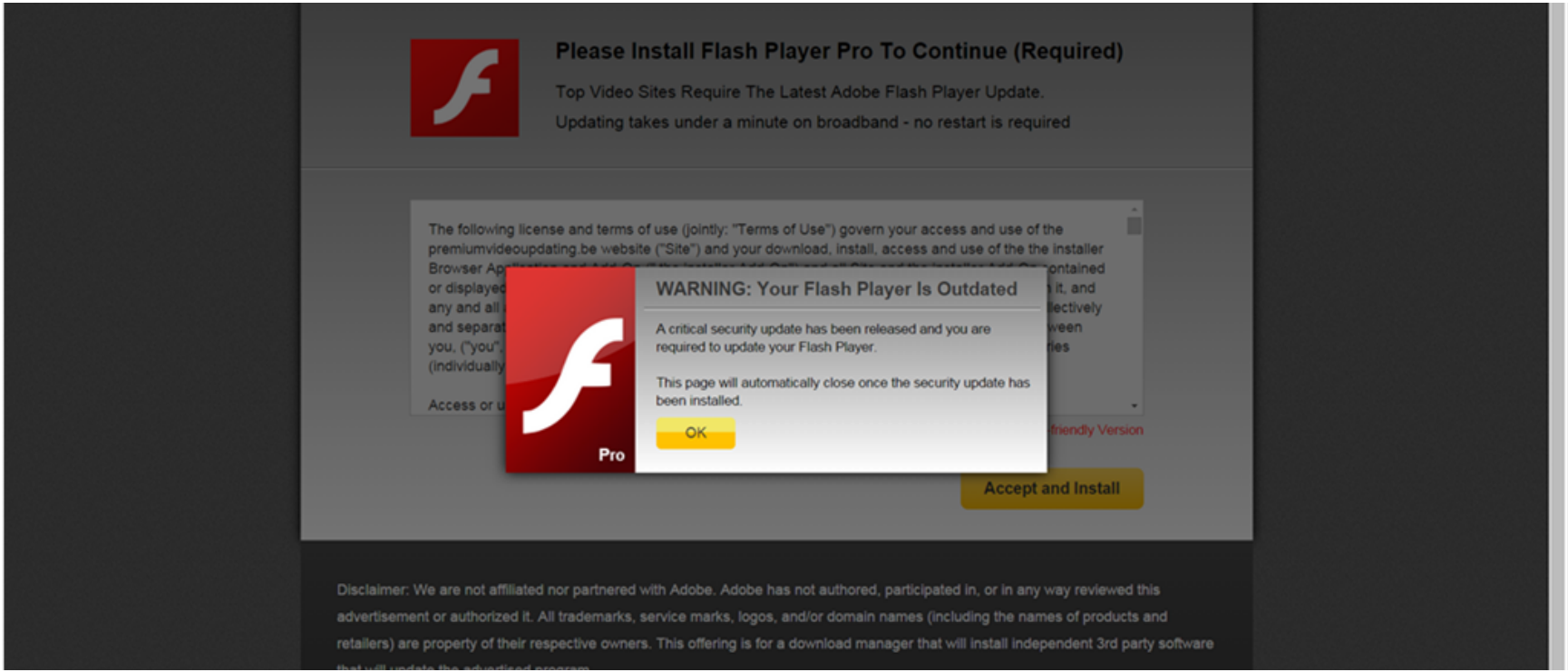
Conclusion

Trick	Total	Percentage
Repackage+Entice	972	48.5%
Invent+Impersonate+Alarm	434	21.7%
Invent+Impersonate+Comply	384	19.2%
Repackage+Decoy	155	7.7%
Impersonate+Decoy	46	2.3%
Impersonate+Entice+Decoy	12	0.6%
Invent+Comply	4	0.2%
Impersonate+Alarm	1	0.1%

User's Attention	Total	Percentage
Ad	1,616	80.6%
Search+Ad	146	7.3%
Search	127	6.3%
Web Post	115	5.7%

Comply	Alarm	Entice
26% onclickads.net	16% adcash.com	20% doubleclick.net
10% adcash.com	7% onclickads.net	16% google.com
10% popads.net	7% msn.com	12% googleadservices.com
7% putlocker.is	6% yesadsrv.com	11% msn.com
3% allmyvideos.net	4% yu0123456.com	8% coupons.com

Conclusion


Please Install Flash Player Pro To Continue (Required)
Top Video Sites Require The Latest Adobe Flash Player Update.
Updating takes under a minute on broadband - no restart is required
The following license and terms of use (jointly: "Terms of Use") govern your access and use of the premiumvideoupdating.be website ("Site") and your download, install, access and use of the the installer
WARNING: Your Flash Player Is Outdated
A critical security update has been released and you are required to update your Flash Player.
This page will automatically close once the security update has been installed.
OK
Pro
Accept and Install
Disclaimer: We are not affiliated nor partnered with Adobe. Adobe has not authored, participated in, or in any way reviewed this advertisement or authorized it. All trademarks, service marks, logos, and/or domain names (including the names of products and retailers) are property of their respective owners. This offering is for a download manager that will install independent 3rd party software

Questions?

Towards Measuring and Mitigating Social Engineering Software Download Attacks

Terry Nelms[1,2], Roberto Perdici[3,1], Manos Antonakakis[1], Mustaque Ahamd[1,4]

[1]Georgia Institute of Technology
[2]Damballa, Inc.
[3]University of Georgia
[4]New York University Abu Dhabi

tnelms@gatech.edu, perdisci@cs.uga.edu, manos@gatech.edu, mustaq@cc.gatech.edu