CONTENTS

Introduction .............................................................................................................................................. 3
I. FAKEAV .................................................................................................................................................. 4
   A. Installation ....................................................................................................................................... 4
   B. FAKEAV Programs ............................................................................................................................. 7
   C. FAKEAV Affiliates .............................................................................................................................. 10
II. Click Fraud ........................................................................................................................................ 21
   A. Hooking the HTTP Traffic ................................................................................................................... 21
   B. Actual Search Hijacking ...................................................................................................................... 22
III. Information Stealer .............................................................................................................................. 24
   A. Stolen Information Drop Zone ........................................................................................................... 24
   B. Targeted Applications .......................................................................................................................... 26
IV. Online Dating .................................................................................................................................... 28
Conclusions ............................................................................................................................................. 29
References ................................................................................................................................................ 31
INTRODUCTION

A lot of technical analyses and media hype surrounds how a malware spreads. KOOBFACE, for its part, has gained media traction because it was the first social network worm to achieve notable success in terms of operation.

However, beyond spreading and infection vectors, a more nagging question needs to be answered—what is this all about? What happens after getting infected?

Writing a piece of malware is already time consuming, sustaining a piece of malware—making sure it is undetected by antivirus scanners, updating its functionality, and maintaining its command and control (C&C) server—takes time and concerted effort on the part of a group of cybercriminals.

Surely, there must be something for them, too, lest all their investments go to waste.

With that in mind, this third installment of our KOOBFACE research paper series attempts to dig deeper as to how the cybercriminals behind KOOBFACE are monetizing their botnet—using campaigns and employing a whole gamut of techniques from scareware to spyware/adware activities—in order to earn a lot of money.
I. FAKEAV

One of the ways by which the group behind KOOBFACE monetizes the botnet is through the installation of FAKEAV.

We have set up monitoring systems to gather FAKEAV URLs that are being pushed by the KOOBFACE botnet. Based on the FAKEAV URLs that we have gathered so far, we found that the KOOBFACE botnet pushes binaries from at least five FAKEAV affiliate programs.

A. Installation

A FAKEAV is installed in an infected system via the KOOBFACE module, *pp.12.exe*. This module is installed together with the KOOBFACE botnet's other social networking modules. The *pp.12.exe* module:

- Acts as a FAKEAV downloader
- Triggers the display of online dating popup ads

As such, the *pp.12.exe* module is essentially one of the money-making modules of the KOOBFACE botnet.

**Figure 1.** This diagram illustrates how the KOOBFACE botnet’s FAKEAV module communicates with C&C servers to install the FAKEAV binary into an affected system.
Show Me the Money!
The Monetization of KOOBFACE

Upon execution:
• The KOOBFACE FAKEAV module contacts the C&C server using a simple HTTP GET request.
• The C&C server issues commands that tell the FAKEAV module to go to another URL.
• The FAKEAV module receives and follows the C&C server’s command.

The first thing that KOOBFACE’s FAKEAV module does is to contact its C&C server. This is done via a simple HTTP GET request.

```
GET /sys/?action=ppgen&a=0%0a%0a&v=12&pid= HTTP/1.1
Host: v=x=x.x.x.x age.com
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; na; )
Content-type: application/x-www-form-urlencoded
Connection: close

HTTP/1.1 200 OK
Connection: close
Date: wed, 28 oct 2009 09:20:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: Pleskwin
X-Powered-By: ASP.NET
X-Powered-By: PHP/5.2.3
Content-type: text/html

#BLACKLABEL
#PID 1000
URL=http://ek<x>ip<x>ads.se./sys/?action=viewgen&v=12
WIDTH=800
HEIGHT=600
INTERVAL=15
REFERER=http://gogle.com
BACKGROUND=0
#CACHE
MD5=e1c5b6d26053b98ac9e0ee6ac464b08
```

*Figure 2.* The KOOBFACE FAKEAV module contacts its C&C server via a simple HTTP GET request.

The C&C server then replies with commands instructing the FAKEAV module to visit another URL. Upon receiving the command, the FAKEAV module visits the URL specified in the C&C server’s command.

```
GET /sys/?action=viewgen&v=12 HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://gogle.com
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: ek<x>ip<x>ads.se
Connection: Keep-Alive

HTTP/1.1 200 OK
```

*Figure 3.* This shows how the FAKEAV module’s HTTP GET request is sent to the URL.
The C&C server then replies to this HTTP request with a JavaScript program. Embedded within the JavaScript program is a set of URLs.

Upon execution:
- The C&C server replies to the HTTP request with a JavaScript program that contains a set of URLs.
- The JavaScript program selects one of the URLs then opens a browser window.

In the specific example, the C&C server returned a set of six URLs—five FAKEAV URLs and one online dating affiliate site.

The JavaScript program selects one URL then opens an Internet Explorer window showing the selected URL.

Figure 4. This shows an example of a set of URLs that the C&C returns.

Figure 5. In this example, a FAKEAV URL was chosen and opened in Internet Explorer.
After the bogus FAKEAV scan is completed, the user will be pressured to download and install a FAKEAV binary.

B. FAKEAV Programs

This section shows some of the FAKEAV programs that can be downloaded onto a KOOBFACE-infected computer. It was usual for the FAKEAV programs to feign scanning the system for malware infections. Of course, cleaning the supposedly detected malware and accessing other features of the product requires the user to buy the “full version.”

To get the full version of a FAKEAV program, the user needs to pay a certain amount via a payment portal where the user is asked to enter credit card information.

Apart from being victimized by paying for useless FAKEAV licenses, users are also scammed into giving out credit card information to cybercriminals.
The following are some of the FAKEAV programs that the KOOBFACE botnet pushes:

- **Safety Center.** This offers two types of license:
  - **One-year license:** This is worth US$59.95.
  - **Lifetime license:** This is worth US$79.95.

**Figure 7.** Safety Center offers two types of license.

**Figure 8.** It even offers discounted rates!
To obtain a *Safety Center* license, a user needs to use his/her credit card. Besides shelling out money, the user also has to give out his/her complete credit card information to the cybercriminals behind the FAKEAV.

- **Security Tool.** This FAKEAV program sports a sleek user interface (UI) that is compatible with the UI style used by Windows 7. It also smoothly runs in a Windows 7-operated PC.

![Security Tool sports a sleek UI that is compatible with that used by Windows 7.](image)

*Figure 9. Security Tool sports a sleek, Windows 7-compatible UI.*

Like *Safety Center*, **Security Tool** also offers two types of license:

- **Two-year license:** This is worth US$49.95.
- **Lifetime license:** This is worth US$79.95.
Show Me the Money!
The Monetization of KOOBFACE

Figure 10. Also like Safety Center, users are also offered discounts for availing of a Security Tool license.

As with Safety Center, paying for a useless license requires a user to input his/her credit card information into a payment portal.

C. FAKEAV Affiliates

In the course of our KOOBFACE monitoring, we gathered almost 150 unique FAKEAV URLs. These URLs had telltale patterns, suggesting that they were affiliated with FAKEAV programs.

The URLs had parameters that looked like affiliate identification (ID) numbers. From the URLs we gathered, we saw the following URL parameters:

- affidavit=02942
- affidavit=12400
- pid=312&sid=4db12f
- uid=13300
- PHPSESSID=88354926d0f0a49fc589ac0a7ccdf44f
It looks like the KOOBFACE botnet is an active member of five different FAKEAV affiliates. It is, however, most unfortunate that we were unable to trace the said affiliated programs.

- **Affiliate 1 (affid=02942).** The URLs from this affiliate have the following form:
  
  \[
  \text{http://domain.tld/hitin.php?land=20&affid=02942}
  \]

  So far, we have seen KOOBFACE use the following domains from this affiliate:
  
  - chilisoft.in
  - dapohsoft.eu
  - dapohsoft.in
  - daposft.eu
  - daposft.in
  - ejremover.eu
  - igsof.eu
  - jastaspy.in
  - ktsoft.eu
  - lastspy.in
  - mexcleaner.in
  - piremover.eu
  - pivocleaner.in
  - pusoft.eu
  - qjcleaner.eu
  - ratspywawe.in
  - samosoft.in
  - softodrom.in
  - worldbestsecurity.com

  These URLs were found to be hosted on the following IP addresses:
  
  - 95.211.27.154
  - 212.117.161.142
  - 91.212.127.18

- **Affiliate 2 (affid=12400).** The URLs from this affiliate have the following form:
  
  \[
  \text{http://domain.tld/hitin.php?land=20&affid=12400}
  \]

  So far, we have seen KOOBFACE use the following domains from this affiliate:
  
  - airtoolsltd.com
  - auditcashing.com
  - auditexperiment.com
  - audittest.com
  - banktestonline.com
  - bartonsecurityservices.com
Show Me the Money!
The Monetization of KOOBFACE

- bestexamine.com
- blackhomesonline.com
- bloodexperiment.com
- bloodquiz.com
- certhomeinspect.com
- cuttingutilities.com
- drivingexperiment.com
- drivingtrial.com
- examinedan.com
- examinedesign.com
- experimentalways.com
- experimentalways.net
- experimentreg.com
- freeonlinedirect.com
- germansecuritygroup.com
- globalsecuritymonitor.com
- greatsecuritygroup.com
- greatsecurityservice.com
- homelandstability.com
- homescanllc.com
- indiasecurityworld.com
- inspectallrealty.com
- inspectourhouse.com
- nationalinternetsecurity.com
- nationalstability.com
- nightwaresoftware.com
- onlinechipguide.com
- onlineworldcar.com
- onlineworldtech.com
- ourtestdomain.com
- personalitytrial.com
- pricecheckcompany.com
- pricecheckjapan.com
- protectourpledge.com
- rosesecuritygroup.com
- safecheckcard.com
- scanmantech.com
- skyscantime.com
- superexamine.com
- testcashing.com
- testequipmentlight.com
- testexperiment.com
- theprotectour.com
- thesecuritylawyers.com
- updateexperiment.net
- widgetsutilities.com
- yourexamine.com
- yourstability.com
- aboutbillgates.com
- yourtoolscheap.com
These KOOBFACE FAKEAV domains resolved to the following IP addresses:

- 62.90.136.237
- 93.174.95.135

The two above-mentioned IP addresses were also shared by the following domains, all of which install a FAKEAV into an affected system:

- bestsecurityjobs.com
- bestwebsitesecurity.com
- businesssecuritytool.com
- cheapsecurityscan.com
- easynettest.com
- examinedan.com
- greatsecuritytestinternet.com
- handutilities.com
- internetprotectioncheck.com
- netmedtest.com
- netsecuritycode.com
- newtoolsonline.com
- safetyscantool.com
- safetystestinternet.com
- scantoolsite.com
- securitycheckeast.com
- securitycodereviews.com
- securityjobtest.com
- securityread.com
- securityscantooldirect.com
- securityscantoolguide.com
- securityscantoolworld.com
- securitysupplycenter.com
- securitytestnetonline.com
- securitytoolsavailable.com
- securitytoolworld.com
- thesecuritylawyers.com
- toolsdirectnow.com
- www.businesssecuritytool.com
- www.cheapsecurityscan.com
- www.securitycodereviews.com
- www.securitysupplycenter.com
- www.yoursecuritynetwork.com
- yoursecuritynetwork.com

- **Affiliate 3 (pid=312s01&sid=4db12f).** The URLs from this affiliate have the following form:

  http://domain.tld/?pid=312s01&sid=4db121

The URLs from the third affiliate (pid=312s01&sid4db12t) were all hosted on .CN domains.
Interestingly, all of the URLs we gathered from this affiliate were hosted on .CN domains. So far, we have seen KOOBFACE use the following URLs:

- accruingtechs.cn
- anthelion2.cn
- army-wives.cn
- baby2boy.cn
- be-spoken.cn
- bebleep.cn
- caddy-shack.cn
- cellostuck.cn
- chinagossips.cn
- circulargone.cn
- cooperinc.cn
- cross-cover.cn
- danny-dyer.cn
- destinybeijing.cn
- discounts2009.cn
- exponentials.cn
- factor2009.cn
- franchisingcorp.cn
- genusbiz.cn
- having-fun2.cn
- heedlessinfo.cn
- high0heels.cn
- howtotutorials.cn
- infabouthacks.cn
- interposition.cn
- kangaroocar.cn
- moral-theology.cn
- northern-pole.cn
- outperformoly.cn
- pericallis.cn
- poltergeist2000.cn
- programmingfun.cn
- rainbowlike.cn
- retrocession2.cn
- sapesoft.in
- semi-smile.cn
- sestiad2.cn
- skewercall.cn
- sneak-peak.cn
- spreadingnews.cn
- stinkingthink.cn
- suspensory-glue.cn
- tegan-and-sara.cn
- transmitteron.cn
- trifoms.cn
- uncrown3.cn
- uninpressive3.cn
- uninformed2.cn
Unlike the FAKEAV sites associated with two of the previous affiliates, the URLs for the third affiliate served as redirectors to actual sites that served FAKEAV binaries.

The final landing sites retained the URL parameter pid=312s01. So far, we have seen the following domains host the final landing sites:

- antivirusm.com
- antivirusn.com
- bestantispyware09.com
- detect-spyware5.com
- detect-spyware7.com
- detect-spyware9.com
- ftp.dot5productions.com
- kill-virusc.com
- mypc-scanner11.com
- mypc-scanner9.com
- top-scanner04.com
- top-scanner11.com
- top-scanner9.com
- virus-detect01.com
- virus-detect08.com
- yourmalwarescan8.com

These domains were found to be hosted at the following IP addresses:

- 83.133.119.154
- 85.12.24.12
- 91.212.107.7

The final FAKEAV binary is downloaded from the following URL:

http://212.117.160.18/setup.exe
The IP address 212.117.160.18 is also shared by the following FAKEAV domains:

- ejremover.eu
- fast-spyware-cleaner.com
- fast-spyware-cleaner.net
- fast-spyware-cleaner.org
- free-spyware-checker.net
- malware-online-scanner.com
- online-scanner-malware.net
- pivocleaner.in
- porn-tube-for-free.org
- pusoft.eu
- qjcleaner.eu
- spyware-remover-free.org
- spyware-scanner.org
- world-tube-free.biz
- www.fast-spyware-cleaner.org
- www.malware-online-scanner.com
- www.online-scanner-malware.net
- www.spyware-scanner.org
- www.world-tube-free.biz

- Affiliate 4 (uid=13300). The URLs from this affiliate have the following form:

  http://domain.tld/?uid=13300

So far, we have only seen two domains from this particular affiliate program, namely:

- goscandir.com
- goscanhand.com

The above-mentioned domains resolved to the IP address 91.212.107.103, which is also shared by a lot of other FAKEAV domains such as:

- afront.info
- asbro.info
- atquit.info
- bagse.info
- bedrid.info
- besort.info
- bettev.info
- bettre.info
- brawns.info
- brisky.info
- cafropy.cn
- cakevy.cn
- cheir.info
- cuique.info
- daphni.info
- data-saver.org
Show Me the Money!
The Monetization of KOOBFACE

- databackuper.com
- dislik.info
- dolet.info
- dovzyag.cn
- dozabes.cn
- ducyqan.cn
- dusyti.cn
- dutfij.cn
- dutsyvi.cn
- duvaba.cn
- duvegy.cn
- dwbiec.cn
- duxsoez.cn
- duzebyn.cn
- dybapi.cn
- dyqkuam.cn
- dyqunu.cn
- dytrevu.cn
- dyzani.cn
- ebaetu.cn
- ebeoxuw.cn
- ebeozag.cn
- engirt.info
- epuneyv.cn
- epuvyiz.cn
- eqadozu.cn
- eqaofed.cn
- eqaone.cn
- eqayweh.cn
- eqibuyym.cn
- eqidadx.cn
- eqiovak.cn
- eqoabce.cn
- eqoumiv.cn
- eqouwy.cn
- eqoxyda.cn
- eraumble.cn
- erauso.cn
- ereuqba.cn
- eruqale.cn
- eruqav.cn
- esuteyb.cn
- etuacwo.cn
- etuexyp.cn
- etyawjo.cn
- etykauw.cn
- evaolux.cn
- evaopsu.cn
- evyns.info
- fedar.info
- fliht.info
- freiny.info
Show Me the Money!
The Monetization of KOOBFACE

- g-antivirus.com
- general-antivirus.com
- general-av.com
- generalantivirus.com
- generalavs.com
- gicke.info
- girded.info
- gobackscan.com
- gobarscan.com
- godirscan.com
- godoerscan.com
- goeachscan.com
- goeasescan.com
- gofatescan.com
- gofowlscan.com
- gohandscan.com
- goherdscan.com
- goironscan.com
- gojestscan.com
- golimpscan.com
- golookscan.com
-gomendscan.com
- gomutescan.com
- gonamescan.com
- goneatscan.com
- gopickscan.com
- goroomscan.com
- gosakescan.com
- goscanadd.com
- goscanback.com
- goscanbar.com
- goscancode.com
- goscandeck.com
- goscandir.com
- goscanfowl.com
- goscanherd.com
- goscanjest.com
- goscanlike.com
- goscanlimp.com
- goscanmend.com
- goscanneat.com
- goscanpick.com
- goscanref.com
- goscanrest.com
- goscanroom.com
- goscansake.com
- goscanslip.com
- goscansole.com
- goscantoil.com
- goscantrio.com
<table>
<thead>
<tr>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>goscanxtra.com</td>
</tr>
<tr>
<td>gosolescan.com</td>
</tr>
<tr>
<td>goterm.info</td>
</tr>
<tr>
<td>gotoilscan.com</td>
</tr>
<tr>
<td>gotrioscan.com</td>
</tr>
<tr>
<td>gowellscan.com</td>
</tr>
<tr>
<td>goxtrascan.com</td>
</tr>
<tr>
<td>hiloa.info</td>
</tr>
<tr>
<td>ia-pro.com</td>
</tr>
<tr>
<td>iantivirus-pro.com</td>
</tr>
<tr>
<td>iantiviruspro.com</td>
</tr>
<tr>
<td>iav-pro.com</td>
</tr>
<tr>
<td>ignomy.info</td>
</tr>
<tr>
<td>in5cs.com</td>
</tr>
<tr>
<td>in5ct.com</td>
</tr>
<tr>
<td>in5it.com</td>
</tr>
<tr>
<td>inavpro.com</td>
</tr>
<tr>
<td>kebfoki.cn</td>
</tr>
<tr>
<td>kebquty.cn</td>
</tr>
<tr>
<td>kebugac.cn</td>
</tr>
<tr>
<td>keturma.cn</td>
</tr>
<tr>
<td>kevsopi.cn</td>
</tr>
<tr>
<td>kiwraux.cn</td>
</tr>
<tr>
<td>kixyhce.cn</td>
</tr>
<tr>
<td>lavolt.info</td>
</tr>
<tr>
<td>lequel.info</td>
</tr>
<tr>
<td>lowatt.info</td>
</tr>
<tr>
<td>meanly.info</td>
</tr>
<tr>
<td>midid.info</td>
</tr>
<tr>
<td>mobled.info</td>
</tr>
<tr>
<td>monast.info</td>
</tr>
<tr>
<td>moont.info</td>
</tr>
<tr>
<td>nnight.info</td>
</tr>
<tr>
<td>nroof.info</td>
</tr>
<tr>
<td>opaque.info</td>
</tr>
<tr>
<td>octian.info</td>
</tr>
<tr>
<td>odest.info</td>
</tr>
<tr>
<td>orifex.info</td>
</tr>
<tr>
<td>pante.info</td>
</tr>
<tr>
<td>pasio.info</td>
</tr>
<tr>
<td>pplay.info</td>
</tr>
<tr>
<td>qward.info</td>
</tr>
<tr>
<td>realfly.info</td>
</tr>
<tr>
<td>rogero.info</td>
</tr>
<tr>
<td>scanatom6.com</td>
</tr>
<tr>
<td>sigeia.info</td>
</tr>
<tr>
<td>spinge.info</td>
</tr>
<tr>
<td>squach.info</td>
</tr>
<tr>
<td>suivez.info</td>
</tr>
<tr>
<td>sundery.info</td>
</tr>
<tr>
<td>swoln.info</td>
</tr>
<tr>
<td>taulus.info</td>
</tr>
</tbody>
</table>
The URLs in the fifth affiliate were of the form http://domain.tld/index.php?PHPSESSID=88354926d0f0a49fc589ac0a7ccd4d4f.

So far, we have seen the following domains from this particular affiliate program:

- malware-online-scaner.biz
- malware-online-scaner.com
- malware-online-scaner.info
- malware-online-scaner.net
- malware-online-scaner.org
- spyware-online-scaner.com
- spyware-remover-free.com
- spyware-remover-free.org

We found that the domains above were hosted in the following IP addresses:

- 212.117.160.18
- 95.211.129.30
II. CLICK FRAUD

One of the most critical components the KOOBFACE botnet uses to monetize infections are search hijackers. Search hijackers monitor HTTP traffic for Web searches using popular search engines such as Google, Yahoo!, or Bing. Clicking any result returned by the Web search engines result in a redirection either to a valid Web page though not the one returned by the search engine, which results in click fraud or to a FAKEAV page.

A. Hooking the HTTP Traffic

Various versions of the KOOBFACE worm are related to search hijackers that use different techniques to monitor HTTP traffic. So far, the following two techniques are used by search hijackers to monitor HTTP traffic:

- **Installing a driver.** A driver designed to hook TCP and User Datagram Protocol (UDP) is installed into the infected machine. This driver then forwards HTTP sessions to the actual search hijacker, which acts as a proxy server for the infected machine.

- **Acting as a Browser Helper Object (BHO).** Alternatively, a BHO can be used to monitor browsing activity. Installed BHOs work hand in hand with the proxy component to complete the search hijack.

*6244.exe -> %system%\796525\796525.dll is a BHO which works hand in hand with NFR.exe -> %system%\sysdll.exe (sysdll.exe is installed as a local proxy and is responsible for redirecting network traffic to the BHO)
**B. Actual Search Hijacking**

The search hijacker installs itself as a local proxy with the HTTP traffic forwarded by the driver or the BHO component.

In *Internet Explorer*, this is carried out by creating the following registry entry:

```plaintext
(HKLM or HKCU)\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings ProxyServer = "http=localhost:<monitored port>"
```

Alternatively, Firefox’s `prefs.js` file is modified with the following to achieve the same effect:

```plaintext
user_pref("network.proxy.http", "localhost");
user_pref("network.proxy.http_port", <monitored port>);
user_pref("network.proxy.type", 1);
```

Acting as a local proxy, the search hijacker is now able to see HTTP traffic. The actual search-hijacking process works in the following manner:

1. The search hijacker monitors strings in URL requests that are related to Web search engines.
2. If a Web search engine-related string is found in the URL, the search hijacker attempts to obtain the search string the user provided.
3. The search hijacker sends a query using the user’s search string to a KOOBFACE search hijack domain (e.g., yy-dns.com, zz-dns.com, and bit-find.com).
4. The KOOBFACE search hijack domain returns a URL that is stored in the search hijacker.
5. Once the user clicks a search result, the search hijacker intercepts the request and instead requests for the URL the KOOBFACE search hijack domain provided to send to the search hijacker.
6. The user is redirected to a page he/she does not want to go to and click fraud is committed.

**Figure 12.** The search hijacker queries the string “cars” on bit-find.com, which is hosted on the IP address 85.13.236.154.
Show Me the Money!
The Monetization of KOOBFACE

5. Once the user clicks a search result from Google, Yahoo!, or Bing, the search hijacker intercepts the request and instead requests for the URL the KOOBFACE search hijack domain provided to send to the search hijacker (the URL in Figure 13).

6. At this point, the user is redirected to a page he/she does not want to go to and click fraud is committed.

It is important to note that the URLs the KOOBFACE search hijack domain returns vary. There are times when the domain remains dormant (does not return any URL for click fraud schemes). Thus, users of infected machines may not notice anything peculiar when they are surfing the Web. However, there are also times when the KOOBFACE domain seems to be involved in click fraud attacks wherein users are redirected to sites related to the search strings they used.

KOOBFACE search hijack domains are always hosted on the following IP addresses:

- 85.13.236.154
- 85.13.236.155

Performing reverse Domain Name System (DNS) tracking on the two IP addresses revealed several fake search engine domains that were being used in click fraud schemes.

As of this writing, the KOOBFACE search hijack domain has been involved with FAKEAV redirections wherein FAKEAV pages were served to users no matter what search strings they used or what search results they clicked (as discussed in section I).

To better understand how search hijacking or click fraud works, you may view a short screen capture at http://www.youtube.com/watch?v=rzPmGpNMe2g. In this example, a user searches for “jobs” in Google and clicks the monster.com link from the search results. Instead of landing on his/her chosen page, however, he/she is redirected to the site efinancialcareers.sg instead.
III. INFORMATION STEALER

The KOOBFACE botnet also makes money from selling the information it has stolen from infected machines. Such information includes FTP, Gmail account, and other saved credentials for popular Web browsers. The botnet may also use stolen FTP credentials to upload malicious codes into compromised servers and to serve updated KOOBFACE binaries.

The KOOBFACE botnet installs a variant of the LDPINCH Trojan malware into an affected system. The LDPINCH malware is responsible for stealing user names and passwords from targeted applications and sends the stolen information to a C&C server. LDPINCH is a modularized made-to-order Trojan, which costs about US$10 in the cybercriminal underground market.

When we started our KOOBFACE botnet investigation, we saw the KOOBFACE loader download an encrypted copy of the LDPINCH malware, which was embedded in a .JPG picture file. However, beginning July 2009, the loader component started downloading the LDPINCH malware in the form of an executable file.

A. Stolen Information Drop Zone

The C&C drop zones we extracted from the LDPINCH binaries we collected through our KOOBFACE monitoring include:

- gdehochesh.com
- 61.235.117.83
- xtsd20090815.com

Note, however, that gdehochesh.com no longer resolves to an IP address. On the other hand, we noticed that xtsd20090815.com resolves to the IP address 61.235.117.83, hinting that those responsible for the KOOBFACE botnet use a single C&C drop zone for stolen user names and passwords. The IP address was located in China.

```
inernet:       61.235.117.0 - 61.235.117.255
netname:       CRGdSzsS
country:       CN
descr:         China Railcom Guangdong Shenzhen Subbranch
                Telecommunication Company
                Shenzhen City, Guangdong Province
admin-c:       LQ112-AP
tech-c:        LM273-AP
status:        ASSIGNED NON-PORTABLE
changed:       hanb@crc.net.cn 20030731
mnt-by:        MAINT-CN-CRTC
source:        APNIC
```
The malware sends the stolen information in encrypted form via an HTTP POST request to the C&C drop zone and uses the word malware as a User-Agent. It sends the HTTP POST request to the /adm/index.php page of the C&C drop zone.

For the more adventurous researcher, the KOOBFACE botnet uses an administrator page, which can act as a portal where cybercriminals can retrieve stolen information.

![Figure 14. The KOOBFACE botnet’s administrator page acts as a portal where cybercriminals can retrieve stolen information.](image)

### B. Targeted Applications

The LDPINCH component used to retrieve user names and passwords from email, FTP, and instant messaging (IM) applications and Web browsers. As of this writing, the LDPINCH the KOOBFACE botnet used targeted FTP applications, Web browsers, and Gmail accounts. It retrieves a user’s Gmail account credentials by urging the affected user to log in to his/her account.
The LDPINCH malware was found to target the following applications:

- FTP applications
  - File and Archive Manager FTP-Plugin: http://www.farmanager.com
  - Ghisler FTP Total Commander: http://www.ghisler.com/
  - Ipswitch WS_FTP: http://www.ipswitch.com/
  - FlashFXP: http://www.flashfxp.com/
  - FileZilla: http://filezilla-project.org/
  - Bullet Proof FTP: http://www.bpftp.com/
  - SmartFTP: http://www.smartftp.com/
  - TurboFTP: http://www.turboftp.com/

- Saved Web browser user names and passwords
  - Mozilla Firefox
  - Opera
  - Internet Explorer 7 (including Internet cookies)

- Gmail accounts

The LDPINCH malware deletes itself from the affected system after executing its information-stealing routine to evade detection. After all, the malware does not have to be present once it gets all the information it needs. This is also a way for the malware to evade detection by most antivirus products since it does not leave its binary in the affected machine.
IV. ONLINE DATING

The creators of the KOOBFACE botnet also dabbled in the online dating affiliate scene. KOOBFACE variants popped Flash animations of “chat windows.”

![Flash animations of chat windows](image-url)

**Figure 15.** Clicking any of the Flash animations above will lead a user to the AdultFriendFinder site.

So far, we have only seen the KOOBFACE botnet use the following URL:

```plaintext
```

The domain www.onlinelovedating.com is hosted on the IP address 63.218.226.67, which is also shared by the following domains:

- currentdating.com
- datefunclub.com
- enormousdating.com
- giantdating.com
- ibestdate.com
- onlinelovedating.com
- worldbestdate.com
- worlddatinghere.com
CONCLUSIONS

What we have presented in this research paper are ways by which the cybercriminal minds behind KOOBFACE are making money off their botnet.

While some botnets were primarily designed to send out spam and to download other malware, the KOOBFACE gang has been employing novel ways to cash in on their creation.

The search hijacking that leads to the commission of click fraud is a unique way to increase artificial traffic and to earn from ads. The traffic originates from actual users and will most likely qualify as valid traffic to advertising program providers.

It seems that AdultFriendFinder is also back to its old ways, serving unsolicited adult-oriented ads using malicious software. In December 2007, AdultFriendFinder has agreed with the Federal Trade Commission (FTC)’s mandate, which barred it from displaying sexually explicit online ads (http://www.ftc.gov/opa/2007/12/afriendfinder.shtm). However, as can be gleaned from our research, the site has revived its former practice.


This discovery suggests it is not farfetched for “legitimate” entities that used to create spyware and adware in the past to completely turn to the dark side and to become part of the underground cybercriminal network.

With regard to FAKEAV, which is probably the most “in” thing among cybercriminals today, we found that KOOBFACE was affiliated with five different FAKEAV groups, each of which serves a different kind of FAKEAV (in terms of look and feel and pricing). This reveals the challenge that FAKEAV poses to the security industry, which does not have anything to do with the complexity of the malware but on the business models their makers employed.

FAKEAV programs have begun outsourcing their propagation to botnets with ready installed bases, allowing the cybercriminals behind them to concentrate instead on coming up with effective scare tactics and pay-per-install models. The success of this business model paved the way for other cybercriminals to create other FAKEAV programs and for other cybercriminal groups to device ingenious ways to promote the malicious programs apart from hiring botnets to utilize the pay-per-install model.

Last but not least, the KOOBFACE botnet installs a variant of the LDPINCH information stealer which, apart from being able to sell stolen credentials, can also be used to compromise sites using the said stolen FTP account user names and passwords. In turn, compromised sites can be rented out or used by the cybercriminals behind KOOBFACE to host phishing sites or malicious scripts.
Botnets can be monetized in various ways—by using borrowed techniques from spyware and adware or by using “hot” items such as FAKEAV.

In sum, we have seen a myriad of ways by which a botnet can be monetized—with techniques borrowed from spyware and adware and with the use of “hot” items such as FAKEAV. This just shows the various options a bot master has. It also highlights the fact that malware infections are not just minor inconveniences for users. Not only is an infected user in danger of potentially being scammed by FAKEAV perpetrators, he/she also becomes a direct participant in perpetrating fraudulent activities and cybercrimes as part of a botnet.

It also shows the communal nature of the Internet, that in one way or another, everyone is connected to everyone else. As such, the effect of a malware infection is not limited to an infected computer, thus making security everyone’s responsibility.
REFERENCES
