The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained

A technical paper discussing the KOOBFACE botnet

Written by
Jonell Baltazar,
Joey Costoya, and
Ryan Flores

Trend Micro Threat Research

TABLE OF CONTENTS

INTRODUCTION

Nothing encapsulates the Web 2.0 concept more than social networking sites, which provide users the ability to connect, communicate, and share with others. Social networking sites also serve as a platform for the advertising industry. They allow businesses to become known globally with ease since social networking sites users are distributed in different geographical locations. They also allow business owners to have a "personal" connection with customers and a place to find and to get to know potential employees.

Leading the way through the Web 2.0 social networking revolution is *Facebook,* the world's largest social networking site. By opening the *Facebook* development platform to the public, the site also opened its doors so developers can create applications within the social network.

Facebook slowly transformed the computing landscape with its application framework. Instant messaging (IM), private messages, and interactive games replaced their desktop-based counterparts. The vision of making the browser a platform is slowly materializing with every new application developed for and by *Facebook.*

For cybercriminals, the shift from desktop-based applications to Web-based ones, particularly those on social networking sites, presents a new vector for abuse. As more and more people communicate through social networks, the more viable social networks become malware distribution platforms.

These types of paradigm shifts in malware distribution have occurred before. Viruses piggybacked on files because people exchanged floppy disks frequently back then. Email as a delivery platform was abused by spammers and email-based worms. The same was true for IM applications.

Now, as we see another shift in technology and user behavior, with social networking sites becoming a dominant medium, it is no surprise that a new type of malware—KOOBFACE—rides on this new means of propagation.

KOOBFACE is a revolutionary malware, being the first to have a successful and continuous run propagating through social networks. Its success can, unfortunately, set a precedent for other malware families to abuse social networking sites.

In this paper, we attempt to dissect KOOBFACE by component in order to allow users to understand what the KOOBFACE threat is and what it does.

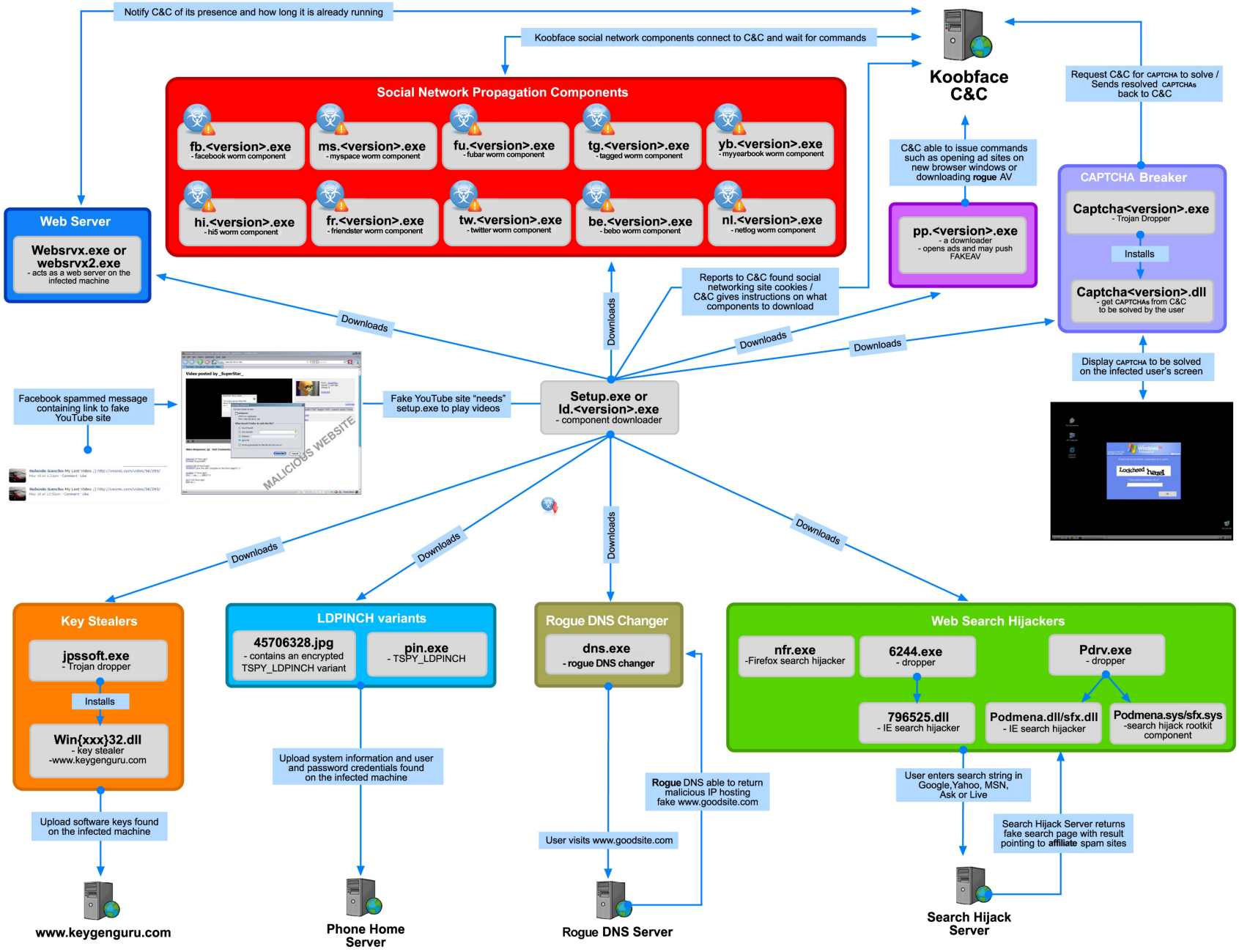

Figure 1. An overview of the KOOBFACE botnet

OVERVIEW

KOOBFACE is composed of various components, each with specific functionalities. While most malware cram their functionalities into one file, KOOBFACE divides each capability into different files that work together to form the KOOBFACE botnet (see Figure 1).

A typical KOOBFACE infection starts with a spam sent through *Facebook, Twitter, MySpace,* or other social networking sites containing a catchy message with a link to a "video."

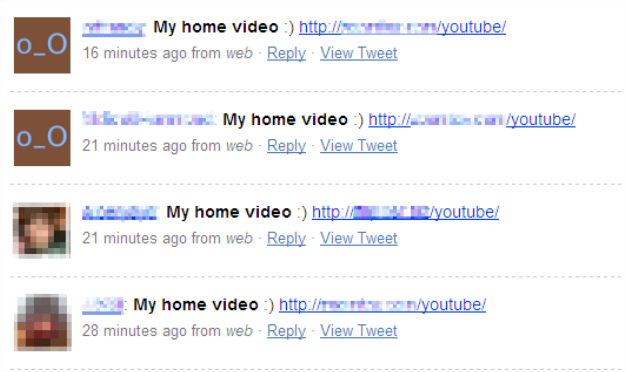

Figure 2. Sample KOOBFACE* Twitter *spam

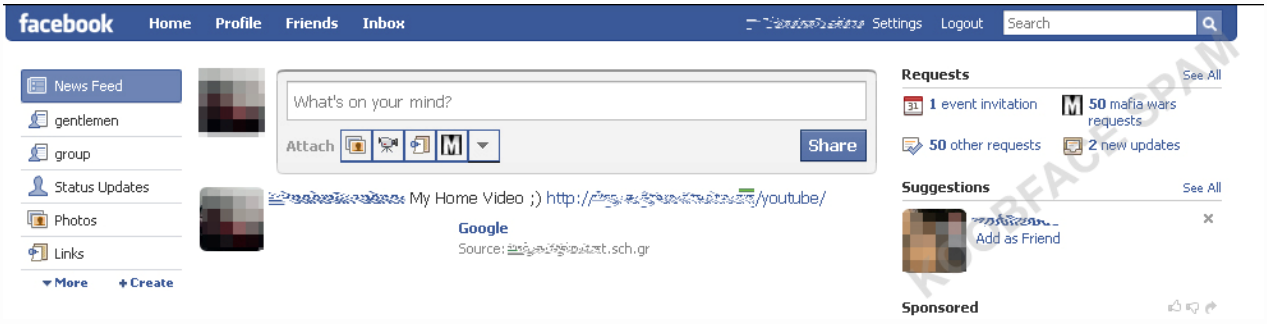

Figure 3. Sample* Facebook *status message spam

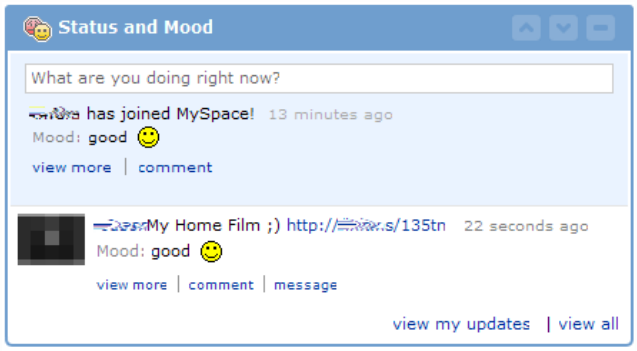

Figure 4. Sample* MySpace *status update spam

KOOBFACE can also send messages to the inbox of a user's social network friend.

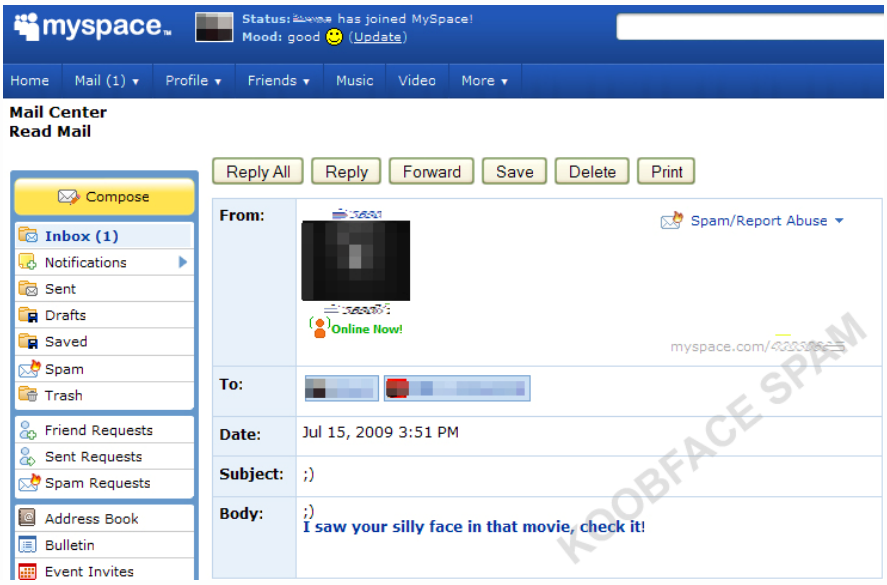

Figure 5. Sample **MySpace** *spammed message in a user's inbox*

Clicking the link will redirect the user to a website designed to mimic *YouTube* (but is actually named *YuoTube*), which asks the user to install an executable (.EXE) file to be able to watch the video.

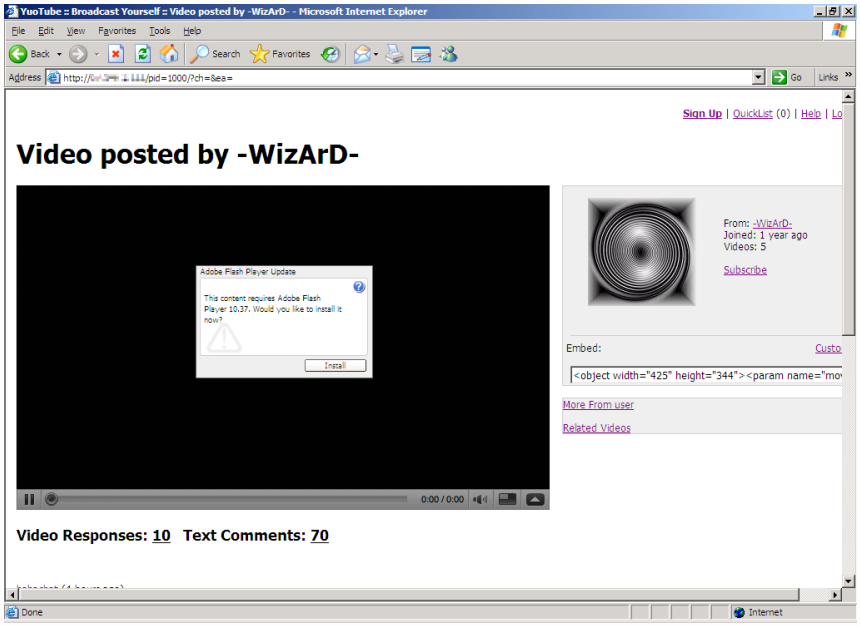

Figure 6. Copycat **YouTube** *site that leads to the KOOBFACE downloader*

The .EXE file is, however, not the actual KOOBFACE malware but a downloader of KOOBFACE components. The components may be subdivided into the following:

- KOOBFACE downloader
- Social network propagation components
- Web server component
- Ads pusher and rogue antivirus (AV) installer
- CAPTCHA breaker
- Data stealer
- Web search hijackers
- Rogue Domain Name System (DNS) changer

The following sections discuss the KOOBFACE components in more detail.

KOOBFACE Downloader

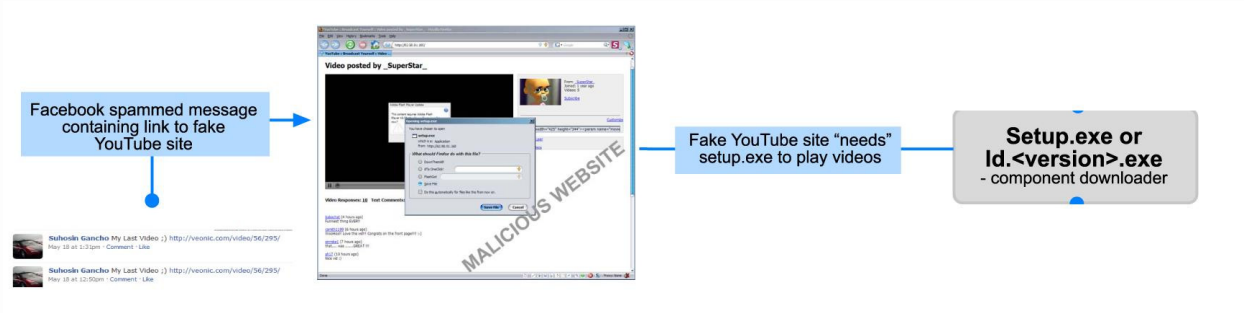

Figure 7. KOOBFACE downloader component routine

The KOOBFACE downloader is also known as the fake "Adobe Flash component" or video codec the fake *YouTube* site claims you need to view a video that turns out to be nonexistent. The downloader's actual purpose includes the following:

- Determine what social networks the affected user is a member of
- Connect to the KOOBFACE Command & Control (C&C)
- Download the KOOBFACE components the C&C instructs it to download

In order to determine what social networks the affected user is a member of, the KOOBFACE downloader checks the Internet cookies in the user's machine. As of this writing, the KOOBFACE downloader checks the cookies for the following social networking sites:

- *Facebook*
- *MySpace*
- *Hi5*
- *Friendster*
- *myYearbook*
- *Tagged*
- *Bebo*
- *Netlog*
- *fubar*
- *Twitter*

The presence of cookies means the user has logged in to any of the above-mentioned social networking sites. The KOOBFACE downloader then reports all found social networking site cookies to the KOOBFACE C&C.

Depending on the social network cookies found, the KOOBFACE C&C then determines what additional components the KOOBFACE downloader needs to download. For instance, if the affected user has *Facebook, MySpace,* and *Twitter* accounts, the KOOBFACE downloader reports the presence of these sites' cookies to the KOOBFACE C&C. The KOOBFACE C&C then instructs the KOOBFACE downloader to download the social network propagation KOOBFACE components responsible for sending out messages in *Facebook, MySpace,* and *Twitter.*

Apart from the necessary social network propagation components, the KOOBFACE C&C may also instruct the KOOBFACE downloader to download and install other KOOBFACE malware that act as Web servers, ads pushers, rogue AV installers, CAPTCHA breakers, data stealers, Web search hijackers, and rogue DNS changers.

Social Network Propagation Components

The social network propagation components of KOOBFACE may be referred to as the actual KOOBFACE worm since these are responsible for sending out messages in social networking sites that eventually lead to the KOOBFACE downloader.

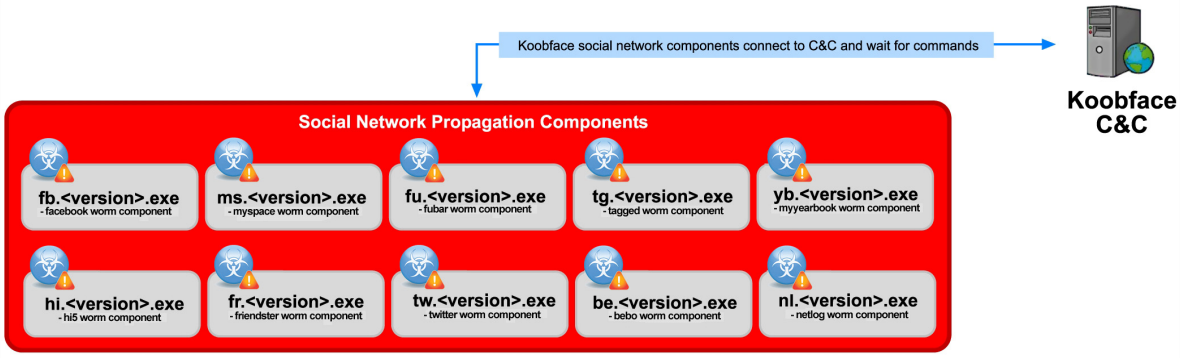

Figure 8. KOOBFACE social network propagation component routine

In general, each social network module is designed to do the following:

- Contact the KOOBFACE C&C
- Get the related messages and URLs from the KOOBFACE C&C
- Post the messages and URLs to the social networking site
- Retrieve text messages and URLs from the KOOBFACE C&C and to mail these to the social network inboxes of the affected user's friends

The social network propagation components of KOOBFACE comprise several binaries. Each of these binaries has been especially built to handle a particular social networking site. The social network component contacts one of many KOOBFACE C&Cs, which then issues commands that the component executes on the affected user's machine. The C&C commands contain messages and URLs that are posted in the affected user's social network shout-outs/status messages or sent to his/her social network friends' inboxes.

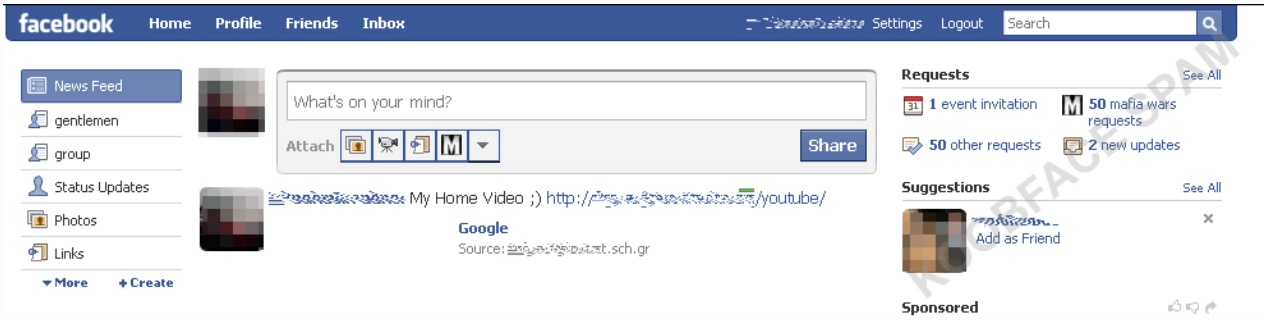

Figure 9.* Facebook *status message spam generated by the* Facebook *social network propagation component of KOOBFACE

Web Server Component

The KOOBFACE Web server component makes the infected machine an unwitting Web server that is part of the KOOBFACE botnet.

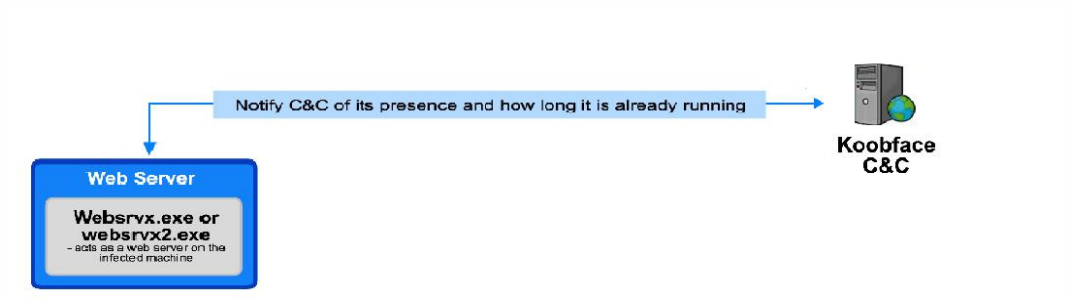

Figure 10. KOOBFACE Web server component routine

Once the system is turned into a Web server, it notifies the KOOBFACE C&C that it is already operable. It also tells the C&C how long it has been running. In turn, the KOOBFACE C&C instructs the Web server to act as a proxy or a relay server to distribute other KOOBFACE components.

The Web server component then serves the fake *YouTube* pages, which lead to the KOOBFACE downloader.

Ads Pusher and Rogue Antivirus Installer

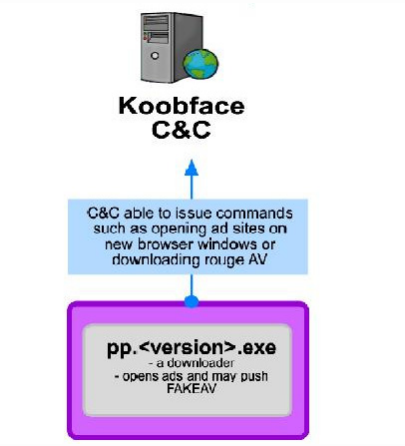

Figure 11. KOOBFACE ad pusher/rogue antivirus component routine

This KOOBFACE component connects to the KOOBFACE C&C, which then instructs it to download rogue antivirus software from a particular URL. It also opens new browser windows that have the ability to push ads or misleading warnings commonly employed by rogue antivirus.

CAPTCHA Breakers

The CAPTCHA-cracking component of KOOBFACE does not solve CAPTCHA image tests through the use of sophisticated computer algorithms. Instead, it gets the infected user himself/herself to solve the challenge-response tests.

The CAPTCHA image that needs to be cracked is fetched from one of KOOBFACE's C&C servers. When the image is downloaded, it is presented to the user, along with a panic-inducing message.

Figure 12. How KOOBFACE makes the user solve CAPTCHA image tests

The "Time before shutdown" is a countdown clock, counting down from the three-minute mark. It provides a sense of urgency for the user to solve the displayed CAPTCHA image within the given time frame.

KOOBFACE does not shut a user's machine down when the countdown timer finishes. It instead waits until the user solves the CAPTCHA test. It has more to do with session timeouts wherein websites impose a certain time limit for a user to solve the CAPTCHA test.

After the user solves the CAPTCHA image test, KOOBFACE relays the solution to one of its C&C servers.

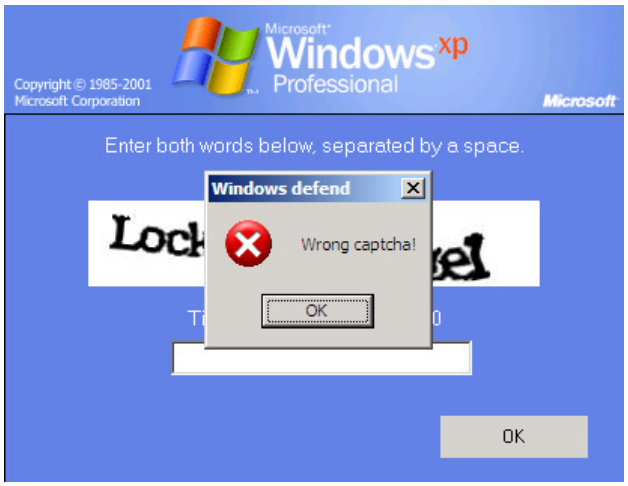

Figure 13. Error message if the CAPTCHA test solution entered did not pass validation

KOOBFACE does not really check whether the CAPTCHA solution is correct or not. Instead, it implements a simple regular expression-based check of the given solution. For instance, if the given CAPTCHA test requires a two-word solution, KOOBFACE will check if the solution given is in fact made up of two words. If the given solution did not pass validation, KOOBFACE displays the following "error" message.

If the given solution is, however, validated as correct, KOOBFACE closes the CAPTCHA dialog box and "allows" the user to continue using his/her Windows machine.

Data Stealers

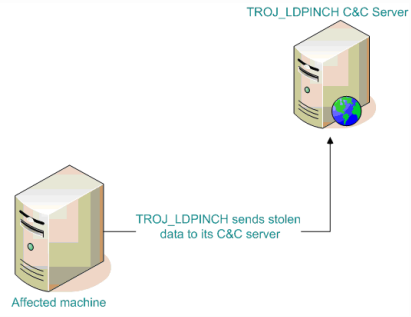

Figure 14. KOOBFACE data stealer component routine

The data stealer component is a variant of the **TROJ_LDPINCH** malware family, which steals Windows digital product IDs, Internet profiles, email credentials, FTP credentials, and IM application credentials. The stolen data is then encrypted and sent to the Trojan's C&C server. The following lists the software that this binary checks and steals credentials for:

- FTP server and client software:
  - Total Commander
  - cuteFTP
  - Ipswitch
  - SmartFTP
  - Coffeecup Software
  - FTP commander (Pro, Deluxe)
  - FlashFXP
  - FileZilla
- Internet profiles
  - Windows Live and Passport.NET profiles
  - Opera saved profiles
  - Mozilla saved profiles
- Email clients:
  - Eudora
  - Becky! Internet Mail
  - RITLabs The Bat! Email client
  - Microsoft Outlook and Outlook Express
  - Mozilla Thunderbird
- Instant messengers:
  - GAIM
  - ICQ
  - QIP
  - Trillian
  - Mail.ru Agents
- Other checked software credentials
  - Punto Switcher
  - Rapidshare
  - Depositfiles
  - Megaupload
  - Universal Share Downloader
  - Rapget

Interestingly enough, this data stealer binary is usually embedded in a .JPG image file, which is hosted using a popular image-hosting site, increasing the chances of the data stealer component to pass through the usual network defenses.

Web Search Hijackers

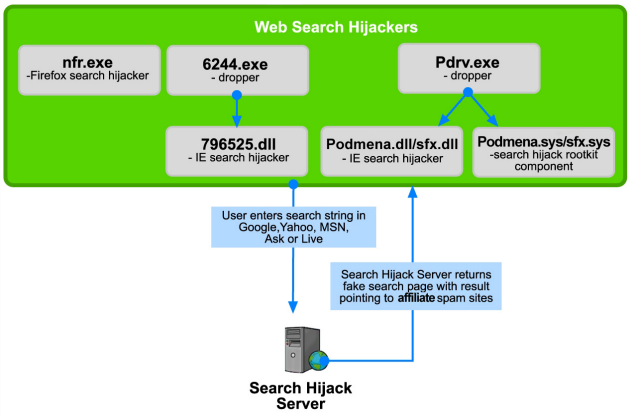

Figure 15. KOOBFACE web search hijacker component routine

Web search hijackers have the ability to intercept search queries to *Google, Yahoo, MSN, Ask,* or *Live* and to redirect them to dubious search portals. These dubious search portals then serve rigged results by returning only the websites of affiliate companies with dubious reputations.

Rogue DNS Changers

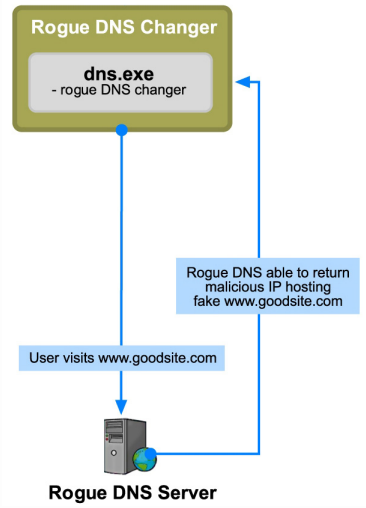

Figure 16. KOOBFACE rogue DNS changer component routine

A rogue DNS changer modifies the DNS server of the affected machine by pointing its DNS to a rogue instead of a legitimate DNS server.

The rogue DNS server then intercepts the websites a user visits and serves malware or phishing pages instead of the legitimate web pages the user originally wants to visit.

A rogue DNS server also blocks a user's access to certain AV or security websites.

SUCCESSFUL SOCIAL ENGINEERING

Components of the KOOBFACE botnet owe their continued proliferation to gratuitous link-sharing behaviors seen commonly on social networking sites. In a study by *AddtoAny,* people are now using *Facebook* and *Twitter* to share links more than they use email. This report proves that social networks have become as viable as—or even more engaging a communication medium than—email or IM.

Figure 17. The dangers of social networking threats are really just one click away.

Facebook unwittingly supported this then-growing trend by initiating a drastic redesign in March 2009 that further enabled and encouraged this behavior. The redesign highlighted status updates on user homepages instead of new connection or relationship updates as was the site's previous format. These status updates often included feeds about newly uploaded photos and shared videos. Touted as a risky move, the rehash nevertheless paid off, as people actively used the feature to share information.

Fortunately for cybercriminals, content shared on social networks often resides on other sites like *Flickr* for photos or *YouTube* for videos. Users, therefore, have come to expect that browsers will open to locations outside the social networking sites when clicking shared links.

Furthermore, links related to certain hot, timely, or interesting content in fact tend to reach viral status such that URLs to a single online resource find themselves plastered onto several users' status messages, shout-outs, wall messages, and updates within a relatively short period of time. A recent socially relevant example would be how the online protests against the Iran election achieved viral status by being circulated across social networks via involved users who posted these protests, raised awareness about it, and thereby won over other users to post them as well.

These behaviors brewed the perfect storm for cybercriminals. The prevalence of KOOBFACE in social networks has caused enough disturbances that have forced site owners to take action. On July 9, 2009, as we reported an increase in KOOBFACE activity on *Twitter, Twitter* decided to temporarily suspend infected accounts in order to curb the infection, demonstrating the vast propagation potential of a social network malware.

SUMMARY AND CONCLUSIONS

The KOOBFACE threat comprises several component malware files that work together to form and maintain the KOOBFACE botnet. This threat model enables KOOBFACE to update its existing components on an affected system, add new ones, or stop updating nonworking modules.

KOOBFACE's update capability makes it a dynamic and therefore formidable threat. It can target new social networking sites by simply adding a new social network propagation component. What started as a malware originally designed to propagate through *Facebook* and *MySpace* now branches out to eight other social networking sites, including *Twitter,* largely due to its modular design and update capability.

KOOBFACE further extends its update or download and execute capability by pushing other malware onto an affected system. KOOBFACE appears to be monetizing this capability by implementing a pay-per-install model where other malware groups can pay the KOOBFACE group to install their malware into KOOBFACE-infected systems. So far, there can be as many as three types of malware utilizing KOOBFACE's pay-per-install service, namely, search hijackers, data stealers, and rogue AV installers.

Since most social network sites employ heuristic rules to distinguish human from spam activity, KOOBFACE will most likely be challenged by a CAPTCHA while spamming a user's social network. KOOBFACE cleverly goes around this by having other KOOBFACE-infected users solve the CAPTCHA for them, a pretty good technique that does not require complex CAPTCHA-breaking algorithms or employing a herd of CAPTCHA breakers.

KOOBFACE cleverly uses social networking sites' Internet cookies to identify what sites an affected user is a member of to access the user's social network account and to send KOOBFACE-related messages to the affected social networking site. After checking what social networking sites a user is a member of, KOOBFACE only downloads the components applicable to the affected system, thus minimizing the download of and exposure to other irrelevant KOOBFACE components.

Using the existing user session, KOOBFACE is able to send messages to the social networking site on the user's behalf, which works to the malware's advantage for the following reasons:

- It eliminates the need to create a fake account on the target social networking site to be able to send malicious URLs to other users.

- It leverages the implied trust that exists between the sender (affected user) and the sender's contacts, increasing the likelihood of the sender's contacts clicking the malicious URL.

The success KOOBFACE is enjoying proves the viability of abusing social networking sites for malware propagation. KOOBFACE has taken advantage of how social networking sites work and how people use them. It constantly tricks victims into downloading malware components through its video-sharing ruse—which mimics what the majority of social network users do online.

A year has passed since the discovery of the first KOOBFACE variant but the malware is still going strong, successfully extending its reach to other social networking sites and paving the way for a new generation of malware that spreads through social networking sites.

REFERENCES

- *Andrew Martin.* (May 29, 2009). "Inside the Massive Gumblar Attack." http://www.martinsecurity.net/2009/05/20/inside-the-massive-gumblar-attacka-dentro-del-enorme-ataque-gumblar/ (Retrieved July 2009).
- *CNN.com/US.* (June 17, 2009). "Iranian-Americans 'Hungry' for Updates Amid Tumult in Iran." http://edition.cnn.com/2009/US/06/16/iranian.americans/ (Retrieved July 2009).
- Baltazar, Jonell. (July 22, 2008). *TrendLabs Malware Blog.* "New KOOBFACE Upgrade Makes It Takedown-Proof." http://blog.trendmicro.com/new-koobface-upgrade-makes-it-takedown-proof (Retrieved July 2009).
- Baltazar, Jonell. (June 25, 2009). *TrendLabs Malware Blog.* "Koobface Tweets." http://blog.trendmicro.com/koobface-tweets (Retrieved July 2009).
- Costoya, Joey. (May 3, 2009). *TrendLabs Malware Blog.* "Koobface Tries CAPTCHA Breaking." http://blog.trendmicro.com/koobface-tries-captcha-breaking (Retrieved July 2009).
- *FireEye Malware Intelligence Lab.* (June 17, 2009). "Killing the Beast… Part II." http://blog.fireeye.com/research/2009/06/killing-the-beastpart-ii.html (Retrieved July 2009).
- Flores, Ryan. (July 9, 2009). *TrendLabs Malware Blog.* "Koobface Increases Twitter Activity." http://blog.trendmicro.com/koobface-increases-twitter-activity (Retrieved July 2009).
- Flores, Ryan. (June 28, 2009). *TrendLabs Malware Blog.* "New Koobface Component: A DNS Changer." http://blog.trendmicro.com/new-koobface-component-a-dns-changer (Retrieved July 2009).
- *Kaspersky Lab.* (July 31, 2008). "Kaspersky Lab Detects New Worms Attacking *MySpace* and *Facebook."* http://www.kaspersky.com/news?id=207575670 (Retrieved July 2009).
- *NCS-Tech.* (February 22, 2008). "Social Networking Sites Are Not the Problem… Behaviors (and Bad Statistics) Are! http://www.ncs-tech.org/?p=1161 (Retrieved July 2009).
- Owyang, Jeremiah. *Web Strategy.* (January 11, 2009). "A Collection of Social Network Stats for 2009." http://www.web-strategist.com/blog/2009/01/11/a-collection-of-soical-network-stats-for-2009/ (Retrieved July 2009).
- Schonfled, Erick. *TechCrunch.* (December 31, 2008) http://www.techcrunch.com/2008/12/31/top-social-media-sites-of-2008-facebook-still-rising/ (Retrieved July 2009).
- *TechCrunch.* "The True Value of Social Networks: 2009." http://www.techcrunch.com/the-true-value-of-social-networks-2009/ (Retrieved July 2009).
- *TheFutureBuzz.* (January 12, 2009). "Social Media, Web 2.0, and Internet Stats." http://thefuturebuzz.com/2009/01/12/social-media-web-20-internet-numbers-stats/ (Retrieved July 2009).
- *ThreatFire Research Blog.* (May 26, 2009). "Virut Distributing KOOBFACE, Ad Clickers, and Spam Bots." http://blog.threatfire.com/2009/05/virut-distributing-koobface-ad-clickers.html (Retrieved July 2009).

- *ThreatFire Research Blog.* (June 3, 2009). "*Softwarefortubeview* Moves to a New Home at 65.110.50.141." http://blog.threatfire.com/2009/06/softwarefortubeview-moves-to-new-home.html (Retrieved July 2009).
- *ThreatFire Research Blog.* (June 16, 2009). "*Streamviewers'* .GIF Images Embedded with Encrypted Malware." http://blog.threatfire.com/2009/06/streamviewers-gif-images-embedded-with.html (Retrieved July 2009).
- *ThreatFire Research Blog.* (June 18, 2009). "Podmena, *podmena.dll* and *podmena.sys* = Spoof, *spoof.dll, spoof.sys.*" http://blog.threatfire.com/2009/06/podmena-podmenadll-and-podmenasys-spoof.html (Retrieved July 2009).
- *Twitter Status* (July 9, 2009). "Koobface Malware Attack." http://status.twitter.com/post/138789881/koobface-malware-attack (Retrieved July 2009).
- *WebProNews.* (July 21, 2009). "Report: Facebook the Most Popular Link-Sharing Tool." http://www.webpronews.com/topnews/2009/07/21/report-facebook-the-most-popular-link-sharing-tool (Retrieved July 2009).