## Malicious Social Networking: Koobface Worm

Author: Joel Yonts

The popularity of social networking sites such as MySpace and Facebook has sky rocketed in recent years. Today nearly everyone has a profile and established friends lists that are used to keep tabs on your two hundred closest friends. For most, the motive behind these sites lies somewhere between a genuine interest in keeping in touch with friends and family to keeping up with the latest gossip. This popularity hasn't gone unnoticed to the malcode authors. To these authors, social engineering is a key tactic used to get their wares installed on unsuspecting victims. Social networking sites makes socially engineering victims almost too easy.

The authors of the Koobface ( an anagram of Facebook ) worm implemented an ingenious system that plays on a victim's interest in getting the dirt on one of their friends. At a high level, an infected user has a new wall post added or messages (Figure 1) are sent to all their friends with words such as "Check out these embarrassing videos of me…". Included with the post is a link where a user can click to get all the juicy photos or video.

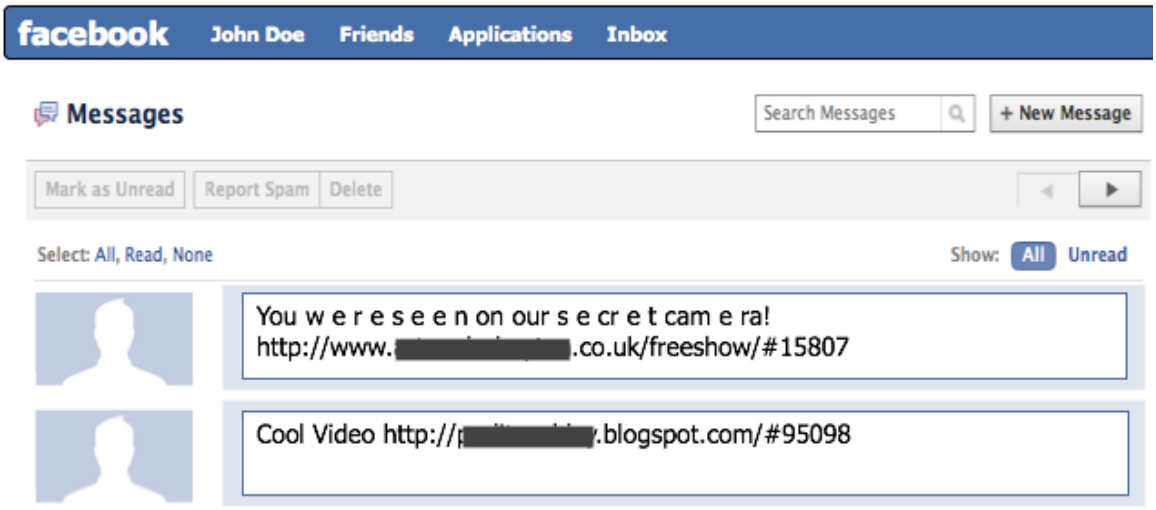


Figure 1: Facebook Messages with Links to Koobface

The embedded link takes you to a dropper site hosting a fresh copy of Koobface ready to be installed on its next victim.

One variant of the infection process highlighted above involves getting a friend request or private message from an unknown individual wanting to become friends or chat. In most cases the profile picture is a scantily clad female looking to share compromising photos of herself and includes a link to her private website. If you haven't guessed already, the link takes you to a dropper site where you can get your personal copy of Koobface.

In most cases the malicious link mentioned above takes you to a YouTube like site that pops a message that you need to install Adobe Flash, a new video codec, or some other plug-in to view the video. Figure 2 is screenshot of a Koobface infection site using this technique.


**Figure 2: Koobface Worm Delivered Under the Guise of Adobe Flash**

Installing the "update" downloads and infects a new system/user and the cycle continues.

**Malware Payload**

The Koobface family of malware was first documented by researchers in mid 2008 and has trended as one of the top infectors throughout 2009 up to the current date in early 2010. Koobface's primary propagation method is through social networking sites such as Facebook, Twitter, MySpace, and Friendster. Even though the infection process remains largely the same, the payload and malicious behaviors documented as part of the Koobface infection has varied slightly over this period. Below is a list of some of these behaviors:

- Stealing login credentials and sessions stored in website cookies
- Stealing web browser saved passwords

**TABLE 1: FORENSIC TIMELINE SHOWING COOKIES BEING ACCESSING DURING INFECTION**

```
Thu Apr 22 2010 21:25:44  326 .a.. <data omitted> ./Cookies/administrator@google[2].txt
                          500 .a.. <data omitted> ./Cookies/administrator@www.msn[1].txt
                          191 .a.. <data omitted> ./Cookies/administrator@atdmt[2].txt
                          178 .a.. <data omitted> ./Cookies/administrator@ad.wsod[2].txt
                           68 .a.. <data omitted> ./Cookies/administrator@c.msn[1].txt
                          460 .a.. <data omitted> ./Cookies/administrator@msn[2].txt
                          680 .a.. <data omitted> ./Cookies/administrator@rad.msn[2].txt
```

- **Irrelevant data was omitted for formatting purposes**

- Trick users into solving CAPTCHAs in automated attacks against other systems (*Figure 3*)
- Installation of malicious proxy settings used for Ad Hijacking and Click Fraud
- SPAM and malware distribution
- Installation of a rogue webserver for command and control (*Figure 4*)
- Rogues security software delivery (*Figure 5*)


**Figure 3: CAPTCHAs Served via Koobface**

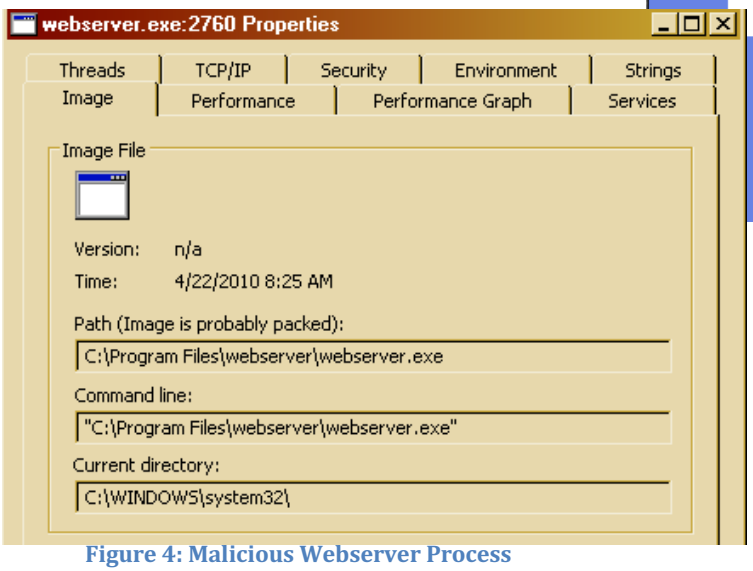


**Figure 4: Malicious Webserver Process**

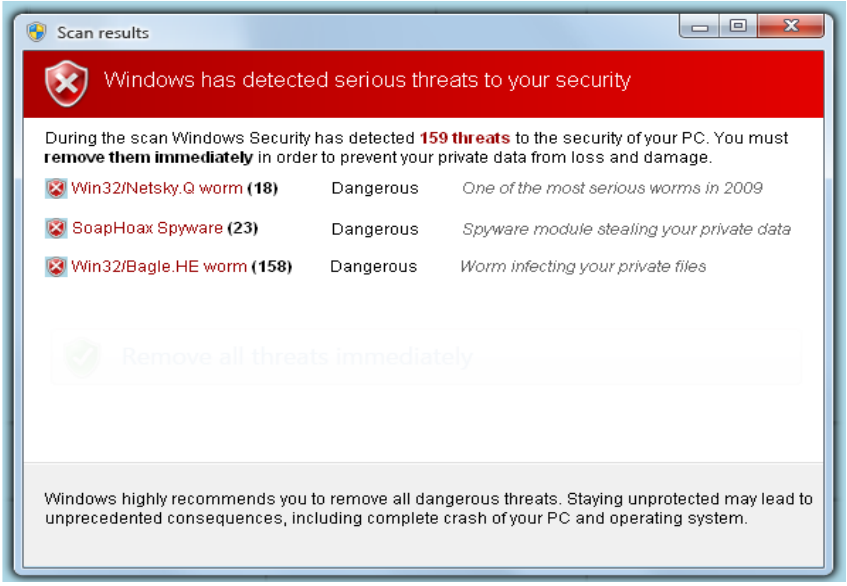


**Figure 5: FakeAV Pop-up Displayed on Compromised Host**

## Koobface Defense

A good first line of defense against this family of malware is security awareness. If users are trained to avoid clicking links from unsolicited or suspicious posts and approach installing plug-ins with caution, the social engineering infection vector is severely limited. Trained users combined with reputation based network filtering and locally installed Anti-Malware solutions rounds out a good defense against Koobface. For corporate entities, a ban on non-work related social networking sites may limit the corporate exposure to this family.

## Appendix A: Infection Artifacts

The details listed in the previous sections are based in part on research data gathered during the analysis of a recent sample of Koobface:

*loader.exe: 441d525538ec30002b0581373c3b7623*

The infection process also yielded the follow system and network infection artifacts.

**TABLE 2: DROPPER SITE INTERACTION**

```
TCP_HIT/200 72192 GET http://216.xxx.xxx.xxx/.sys/?getexe=loader.exe
TCP_HIT/200 49152 GET http://70.xxx.xxx.xxx/.xm29oep/?getexe=ploader.exe
TCP_HIT/200 259584 GET http://64.xxx.xxx.xxx/.dzhm5b/?getexe=p.exe
TCP_HIT/200 36864 GET http://70.xxx.xxx.xxx/.xm29oep/?getexe=v2captcha21.exe
TCP_HIT/200 103424 GET http://70.xxx.xxx.xxx/.xm29oep/?getexe=cmd.exe
TCP_HIT/200 13824 GET http://70.xxx.xxx.xxx/.xm29oep/?getexe=ws.exe
```

**TABLE 3: FILESYSTEM ADDITIONS**

```
c:/Program Files/webserver/webserver.exe
c:/WINDOWS/bill108.exe
c:/WINDOWS/bk23567.dat
c:/WINDOWS/fdgg34353edfgdfdf
```

Joel Yonts, jyonts@gmail.com

```
c:/WINDOWS/system32/btw_oko.dll
c:/WINDOWS/system32/captcha.dll
c:/WINDOWS/system32/drivers/USBSTOR.SYS
c:/WINDOWS/system32/drivers/etc/hosts
c:/WINDOWS/system32/drivers/klifoko.sys
c:/Documents and Settings/Administrator/Desktop/win_protection_update.exe

(deleted):1.bat
(deleted):3.reg
(deleted):SelfDel.bat
(deleted):win_protection_update.exe
(deleted):rdr_1271939089.exe
(deleted):rdr_1271939101.exe
(deleted):1924656.exe
(deleted):1924656.exe.exe
(deleted):captcha.bat
(deleted):nlokobmove.bat
(deleted):zpskon_1271948510.exe
(deleted):dxxdv34567.bat
```

**TABLE 4: SIGNIFICANT REGISTRY MODIFICATIONS**

```
Keys Added
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_FLTOKOMGR
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_FTDISOKO
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WEBSERVER
HKLM\SYSTEM\ControlSet001\Services\captcha
HKLM\SYSTEM\ControlSet001\Services\FltOkoMgr
HKLM\SYSTEM\ControlSet001\Services\Ftdisoko
HKLM\SYSTEM\ControlSet001\Services\webserver
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_FLTOKOMGR
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_FTDISOKO
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_WEBSERVER
HKLM\SYSTEM\CurrentControlSet\Services\captcha
HKLM\SYSTEM\CurrentControlSet\Services\FltOkoMgr
HKLM\SYSTEM\CurrentControlSet\Services\Ftdisoko
HKLM\SYSTEM\CurrentControlSet\Services\webserver

Values Added
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\sysfbtray:
"c:\windows\bill108.exe"
```

**TABLE 5: NEW SERVICES**

```
SERVICE_NAME: FltOkoMgr
DISPLAY_NAME: Partition Protected Standard
(null)
       TYPE               : 20 WIN32_SHARE_PROCESS
       STATE              : 4  RUNNING
                               (NOT_STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
       WIN32_EXIT_CODE       : 0  (0x0)
       SERVICE_EXIT_CODE : 0  (0x0)
       CHECKPOINT         : 0x0
       WAIT_HINT          : 0x0

SERVICE_NAME: captcha
DISPLAY_NAME: captcha
(null)
       TYPE               : 120 WIN32_SHARE_PROCESS INTERACTIVE_PROCESS
       STATE              : 1  STOPPED
```

```
                            (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT      : 0x0
        WAIT_HINT       : 0x0

SERVICE_NAME: webserver
DISPLAY_NAME: webserver
(null)
        TYPE            : 20 WIN32_SHARE_PROCESS
        STATE           : 4  RUNNING
                            (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT      : 0x0
        WAIT_HINT       : 0x0
```

**TABLE 6: MALICIOUS FIREWALL PORT OPENINGS**

| Port | Protocol | Mode | Name |
|---|---|---|---|
| 8085 | TCP | Enable | VMware FilterPort |
| 877 | TCP | Enable | webserver |
| 4000 | TCP | Enable | webserver |
| 53 | TCP | Enable | webserver |

## Additional Material

A wealth of additional material is available on Koobface. Below is an abbreviated list that can add an additional perspective of this popular malware family.


**Win32/Koobface**
McAfee, Inc.
http://vil.nai.com/vil/content/v_148955.htm

**W32.Koobface**
Symantec, Inc.
http://www.symantec.com/security_response/writeup.jsp?docid=2008-080315-0217-99

**Koobface variant worms across social networking sites**
The Register
http://www.theregister.co.uk/2009/03/02/koobface_worm_returns