[Template:Pp](/wiki/Template:Pp" \o "Template:Pp) [Template:Infobox computer virus](/wiki/Template:Infobox_computer_virus)

**Koobface** is a network worm that attacks [Microsoft Windows](/wiki/Microsoft_Windows), [Mac OS X](/wiki/Mac_OS_X), and [Linux](/wiki/Linux) platforms.[[1]](#cite_note-1)[[2]](#cite_note-2)[[3]](#cite_note-3) This worm originally targeted users of networking websites like [Facebook](/wiki/Facebook), [Skype](/wiki/Skype), [Yahoo Messenger](/wiki/Yahoo_Messenger), and email websites such as [GMail](/wiki/GMail), [Yahoo Mail](/wiki/Yahoo_Mail), and [AOL Mail](/wiki/AOL_Mail). It also targets other networking websites, such as [MySpace](/wiki/MySpace), [Twitter](/wiki/Twitter),[[4]](#cite_note-4) and it can infect other devices on the same local network.[[5]](#cite_note-5) This infection allows an attacker to access users' personal information such as banking information, passwords, or personal identity ([IP address](/wiki/IP_address)). It is considered a security risk and should be removed from the network.[[6]](#cite_note-6) Koobface is also used by [technical support scammers](/wiki/Technical_support_scam) to fraudulently claim to their intended victims that they have a virus on their computer.[[7]](#cite_note-7)[[8]](#cite_note-8)[[9]](#cite_note-9)

## Contents

* 1 Infection[[edit](/index.php?title=(none)&action=edit&section=1)]
* 2 Hoax warnings[[edit](/index.php?title=(none)&action=edit&section=2)]
* 3 References[[edit](/index.php?title=(none)&action=edit&section=3)]
* 4 External links[[edit](/index.php?title=(none)&action=edit&section=4)]

## Infection[[edit](/index.php?title=(none)&action=edit&section=1)]

Koobface ultimately attempts, upon successful infection, to gather login information for [FTP](/wiki/FTP) sites, Facebook, Skype, and other social media platforms, and any sensitive financial data as well.[[10]](#cite_note-10) It then uses compromised computers to build a peer-to-peer [botnet](/wiki/Botnet). A compromised computer contacts other compromised computers to receive commands in a peer-to-peer fashion. The botnet is used to install additional pay-per-install malware on the compromised computer and hijack search queries to display advertisements. Its peer-to-peer topology is also used to show fake messages to other users for the purpose of expanding the botnet.[[11]](#cite_note-11)It was first detected in December 2008 and a more potent version appeared in March 2009.[[12]](#cite_note-12) A study by the [Information Warfare Monitor](/wiki/Information_Warfare_Monitor), a joint collaboration from SecDev Group and the Citizen Lab in the Munk School of Global Affairs at the [University of Toronto](/wiki/University_of_Toronto), has revealed that the operators of this scheme have generated over $2 million in revenue from June 2009 to June 2010.[[10]](#cite_note-10) Koobface originally spread by delivering Facebook messages to people who are "friends" of a Facebook user whose computer had already been infected. Upon receipt, the message directs the recipients to a third-party website (or another Koobface infected PC), where they are prompted to download what is purported to be an update of the [Adobe Flash](/wiki/Adobe_Flash) player. If they download and execute the file, Koobface can infect their system. It can then commandeer the computer's search engine use and direct it to contaminated websites. There can also be links to the third-party website on the Facebook wall of the friend the message came from sometimes having comments like LOL or YOUTUBE. If the link is opened the trojan virus will infect the computer and the PC will become a [Zombie](/wiki/Zombie_(computer_science)) or Host Computer.

Among the components downloaded by Koobface are a DNS filter program that blocks access to well known security websites and a proxy tool that enables the attackers to abuse the infected PC. At one time the Koobface gang also used Limbo, a password stealing program.

Several variants of the worm have been identified:

* Worm:Win32/Koobface.gen!F[[13]](#cite_note-13)\* Net-Worm.Win32.Koobface.a, which attacks [MySpace](/wiki/MySpace)
* Net-Worm.Win32.Koobface.b, which attacks [Facebook](/wiki/Facebook)[[14]](#cite_note-14)\* WORM\_KOOBFACE.DC, which attacks [Twitter](/wiki/Twitter)[[15]](#cite_note-15)\* W32/Koobfa-Gen, which attacks [Facebook](/wiki/Facebook), [MySpace](/wiki/MySpace), [hi5](/wiki/Hi5_(website)), [Bebo](/wiki/Bebo), [Friendster](/wiki/Friendster), myYearbook, Tagged, Netlog, [Badoo](/wiki/Badoo) and fubar[[16]](#cite_note-16)[[17]](#cite_note-17)\* W32.Koobface.D[[18]](#cite_note-18)\* OSX/Koobface.A, a [Mac](/wiki/Mac_OS_X) version which spreads via social networks such as Facebook, MySpace and Twitter.[[19]](#cite_note-19)[[20]](#cite_note-20)

In January 2012, the *New York Times* reported[[21]](#cite_note-21) that Facebook was planning to share information about the Koobface gang, and name those it believed were responsible. Investigations by German researcher Jan Droemer<ref name=sophos>[Template:Cite web](/wiki/Template:Cite_web)</ref> and the University of Alabama at Birmingham's Center for Information Assurance and Joint Forensics Research<ref name=UAB>[Template:Cite web](/wiki/Template:Cite_web)</ref> were said to have helped uncover the identities of those responsible.

Facebook finally revealed the names of the suspects behind the worm on January 17, 2012. They include [Stanislav Avdeyko](/wiki/Stanislav_Avdeyko) (leDed), Alexander Koltyshev (Floppy), Anton Korotchenko (KrotReal), Roman P. Koturbach (PoMuc), Svyatoslav E. Polichuck (PsViat and PsycoMan). They are based in [St. Petersburg](/wiki/St._Petersburg), [Russia](/wiki/Russia). The group is sometimes referred to as Ali Baba & 4 with Stanislav Avdeyko as the leader.[[22]](#cite_note-22) The investigation also connected Avdeyko with [CoolWebSearch](/wiki/CoolWebSearch) spyware.<ref name=sophos/>

## Hoax warnings[[edit](/index.php?title=(none)&action=edit&section=2)]

The Koobface threat is also the subject of many hoax warnings designed to trick social networking users into spreading misinformation across the Internet. Various anti-scam websites such as Snopes.com and ThatsNonsense.com have recorded many instances where alarmist messages designed to fool and panic Facebook users have begun to circulate prolifically using the widely publicized Koobface threat as bait.[[23]](#cite_note-23)[[24]](#cite_note-24) The "[Barack Obama](/wiki/Barack_Obama)-Clinton Scandal" hoax which was popular in 2010 is an example.

Other misconceptions have spread regarding the Koobface threat, including the false assertion that accepting "hackers" as Facebook friends will infect a victim's computer with Koobface, or that Facebook applications are themselves Koobface threats. These claims are untrue. Other rumours assert that Koobface is much more dangerous than other examples of malware and has the ability to delete all of your computer files and "burn your hard disk." However, these rumours are inspired by earlier fake virus warning hoaxes and remain false.[[23]](#cite_note-23)

## References[[edit](/index.php?title=(none)&action=edit&section=3)]

[Template:Reflist](/wiki/Template:Reflist)

## External links[[edit](/index.php?title=(none)&action=edit&section=4)]

* [The Koobface malware gang - exposed!](http://nakedsecurity.sophos.com/koobface), research by Jan Droemer and Dirk Kollberg.
* [The Real Face of KOOBFACE](http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf), analysis by Trend Micro.
* [Researchers Take Down Koobface Servers](http://yro.slashdot.org/story/10/11/13/1732205/Researchers-Take-Down-Koobface-Servers?from=rss), Slashdot article.

[Template:Botnets](/wiki/Template:Botnets)

[Category:Computer worms](/wiki/Category:Computer_worms) [Category:Facebook](/wiki/Category:Facebook) [Category:Myspace](/wiki/Category:Myspace) [Category:Trojan horses](/wiki/Category:Trojan_horses) [Category:Hacking in the 2000s](/wiki/Category:Hacking_in_the_2000s)