*What is “Koobface”?*

Koobface is a worm that primarily utilizes social media and e-mail sites to. As the security of these sites has improved, Koobface’s reliance on these sites has decreased. It is a worm in that it is capable of replicating itself and spreading to other systems via networks without the user taking any more part than originally downloading the worm. It is a Trojan horse, in that it appears as an Adobe Flash upgrade (usually), which at a cursory glance would seem legitimate, but once downloaded it creates a backdoor for the attacker and can host a variety of other malicious activity.

Koobface is a multi-component malware that, once the original worm/Trojan horse is in place, can download the other components that the attacker wants to use. These components can range from information stealers to redirection applications that send a user to malicious sites. The original applet is relatively harmless, it is the components that are later downloaded that do the real damage.

*Which Operating Systems Does It Affect?*

Koobface is capable of infecting the major operating systems: Microsoft Windows, the Mac OS X, and there is even a variant that infects Linux. Interestingly, while the infection will not be persistent on a Linux machine (as the malicious application is lost on reboot), the Linux machine may be left on long enough for the attacker to use the machine for their malicious purposes.

*What Are the Damaging/Malicious Effects?*

Koobface carries on a variety of malicious activities, the most notable being that it joins a host machine with other infected machines into a botnet that can be used by the attacker for whatever purpose the attacker might have. The botnet can be used to “install additional pay-per-install malware,” to steal search queries, display advertisements, among other things. “A study by the [Information Warfare Monitor](http://en.wikipedia.org/wiki/Information_Warfare_Monitor), a joint collaboration from SecDev Group and the Citizen Lab in the Munk School of Global Affairs at the University Toronto, has revealed that the operators of this scheme have generated over $2 million in revenue from June 2009 to June 2010.” This revenue is presumably generated by the pay-per-install malware or advertising that pays by the click.

Koobface variants may also include features that block user access to major security websites, steal passwords, or simply grant the attacker general use (usually abusive) of the infected computer.

While Koobface has been identified to gather various File Transfer Protocol (FTP) site login information, most notably for social media, it has not been observed to gather sensitive financial data.

*What Means Are Used?*

Koobface hijacks social media profiles in order to spread itself. It accesses the infected machine’s user’s contacts list and will send messages with malicious links. The most common form is a link to a false youtube video. Here the user is presented with a prompt claiming that their Adobe Flash Player needs to be updated. If the user accepts the “update,” a java applet is downloaded and installed on the system.

Once installation is complete, the system is not infected and can become a “zombie,” and thus a part of the aforementioned botnet (a botnet being a robot network that receives commands from the attacker). Once a part of the botnet, the system can be used to spam the malicious link to the user’s contacts, thus spreading the worm.

Further, since Koobface is a “multicomponent malware,” it can proceed to download and install any components the attacker specifies, and carry out further malicious activity.

*How Does One Defend Against Koobface?*

It is not recommended that individuals try to remove Koobface personally, but rather seek trusted professional help (face-to-face help if you are especially wary). Most anti-virus software is capable of removing Koobface, along with other common malwares. Individuals should be aware of soliciting phone calls and offers to remove viruses in exchange for payment that appear on the internet.

*References*

<http://nakedsecurity.sophos.com/questions-and-answers-about-koobface/>

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-real-face-of-koobface.pdf>

<http://www.webopedia.com/DidYouKnow/Internet/virus.asp>

<http://news.softpedia.com/news/New-Koobface-Variant-Infects-Linux-too-163450.shtml>

<http://news.softpedia.com/news/Linux-Java-Based-Trojan-Might-Have-Been-an-Accident-163848.shtml>

<http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Worm:Win32/Koobface.gen!F&threatid=2147631531>

<http://en.wikipedia.org/wiki/Koobface>