infosec@pjlhuillier.com
ICT GROUP
INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

February 14, 2014 Release # 253

BACKDOOR TROJAN

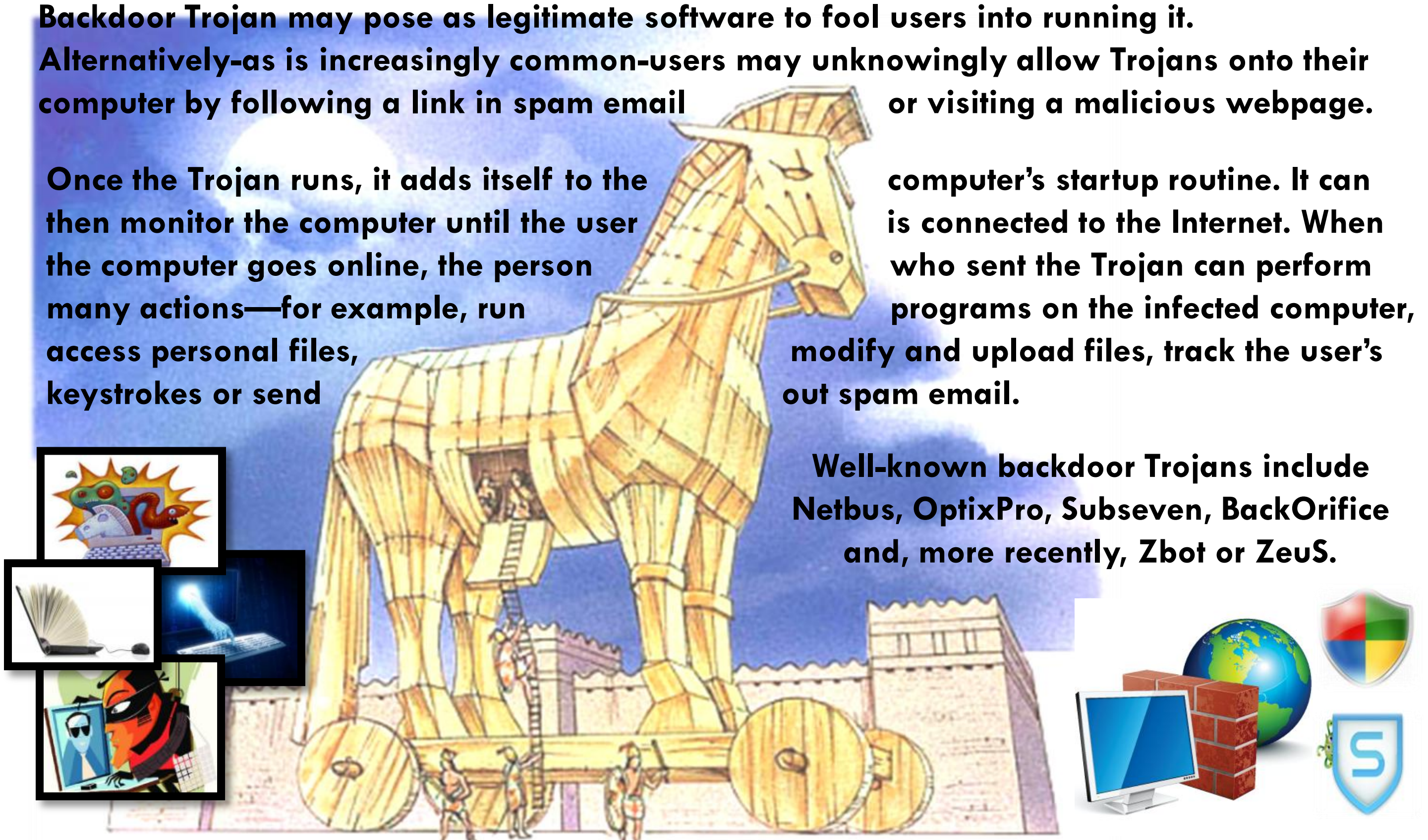
-- Begin Transmission --

A Backdoor Trojan allows someone to take control of a user's computer without permission.

Backdoor Trojan may pose as legitimate software to fool users into running it. Alternatively-as is increasingly common-users may unknowingly allow Trojans onto their computer by following a link in spam email or visiting a malicious webpage.

Once the Trojan runs, it adds itself to the computer's startup routine. It can then monitor the computer until the user is connected to the Internet. When the computer goes online, the person who sent the Trojan can perform many actions—for example, run programs on the infected computer, access personal files, modify and upload files, track the user's keystrokes or send out spam email.

Well-known backdoor Trojans include Netbus, OptixPro, Subseven, BackOrifice and, more recently, Zbot or ZeuS.



To avoid backdoor Trojans, you should keep your computers up to date with the latest patches (to close down vulnerabilities in the operating system), and run anti-spam and antivirus software. You should also use a firewall, which can prevent Trojans from accessing the Internet to make contact with the hacker.

-- End of Transmission –

Information Security: It's a Shared Responsibility
REFERENCE(S): Sophos Ltd. (2012). *Threatsaurus: The A-Z of computer and data security threats.*
Boston, USA | Oxford, UK

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.

Document Code: 2014ICT_15SECA005