

AppRanger Blocking a Web Attack

Opening a web page can be dangerous for your desktop or server.

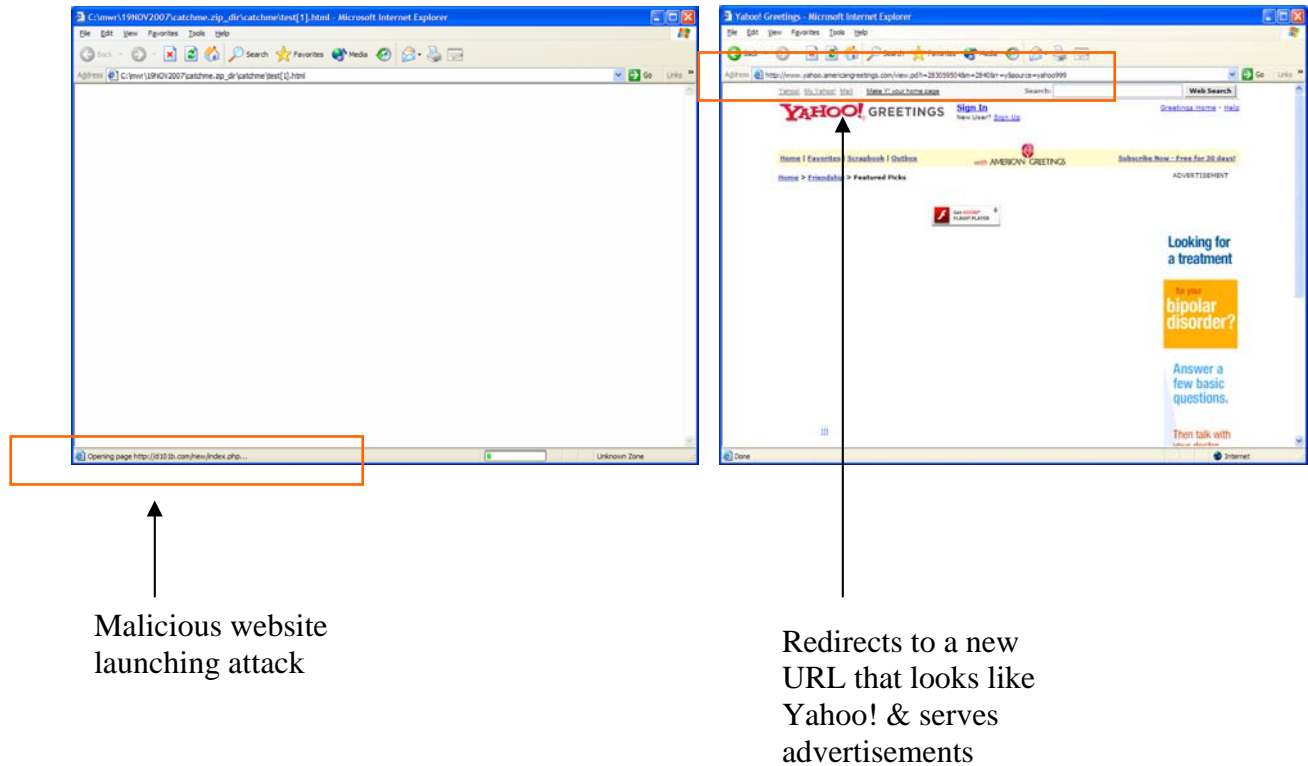
User may click on a malicious link received via e-mail or visit a website that has been compromised. An attack would be launched that would exploit vulnerabilities in the Web browser, Acrobat, media player, etc. to infect the desktop or server.

Below we show what happens when a user clicks on a malicious links.

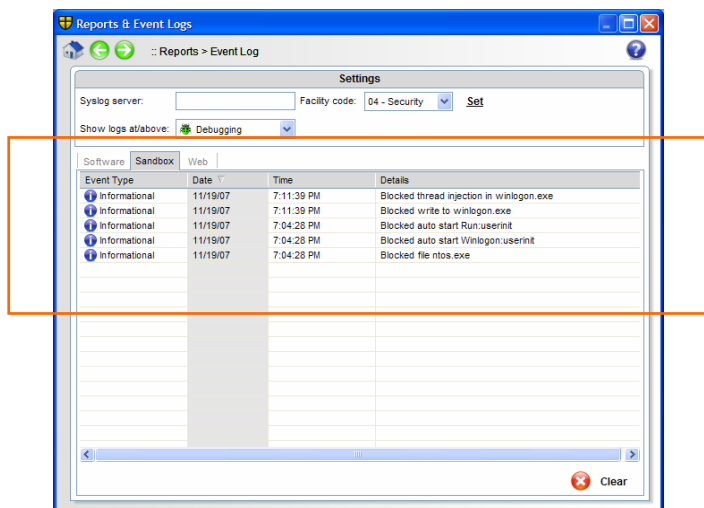
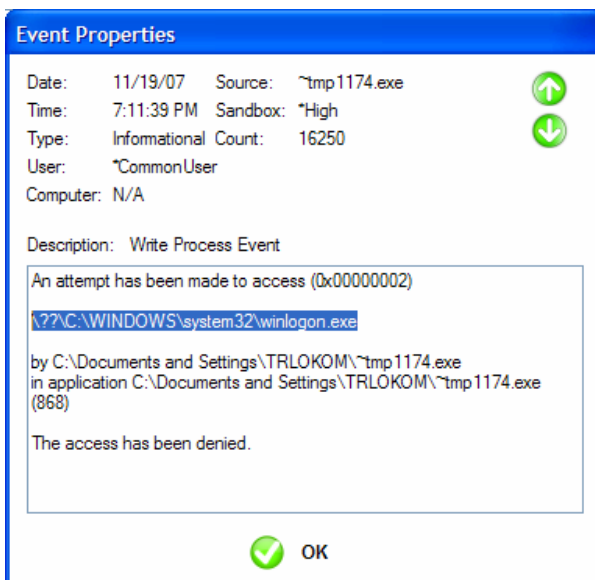
Attack Explained

Malicious code is part of a link that user receives via e-mail. Obfuscation of link makes it difficult to judge if it is a malicious or benign link. When the user clicks on the link, a malicious PHP script from a malicious website (d1o1b.com) executes a new process (tmp1174.exe) and then redirects the user to another Web page that looks like Yahoo!

The user does not have to do anything other than click on the original link received via e-mail.



The process created by the malicious PHP script (tmp1174.exe) attempts to perform several malicious actions, e.g. modify winlogon and few other files.



These actions are detected by the AppRanger and blocked.

In this particular attack, AppRanger has blocked five malicious actions:

- tmp1174.exe tries to inject a thread into winlogon.exe
- tmp1174.exe tries to modify winlogon.exe
- tmp1174.exe tries to create a few autostart registry entries
- tmp1174.exe tries to write a new malicious file called ntos.exe

If any of the above actions were successful, the computer would be very difficult to clean.