Automatic Update: Good or Bad?

del.icio.us

Discuss in Forums {mos_smf_discuss:Wilson}

By Brian Wilson, CCNA, CCSE, CCAI, MCP, Network+, Security+, JNCIA

In this paper I would like to bring light to an area of security that most people do not think about or maybe have blind trust in this aspect of security. What I am talking about is software with automatic update functions. Most of us think about Windows when you hear the term "Auto-Update," but there are a lot of different kinds of software that have auto-updates and some times it is enabled without your knowledge. Now auto-updates features can be very helpful to non technical users and when it comes to windows or other Operating Systems, it is very important to have your auto-updates features turned on.

The problems with auto-updates start when the software makers use these convenient functions to push updates in an unsecured manor. I have herd reports from many sources (one was from http://www.sploitcast.com/) that some games are using peer based networks for updates, kind of like a torrent with the update files coming from other clients computers. This issue here is that if someone with malicious intent decided to inject malicious code into the update they could build a very large bot-net or just about any other kind of exploit to a large group of computers.

Let's now look at how this kind of attack could happen. Let's say I was to download a copy of game-x and go onto an online gaming community. I would need to get updates from the game server to play the game online, and this is where the auto update issues can start to happen. There are a lot of game makers now that push updates to your games without you knowing, and a lot of them use peer networks to push the updates. Sometimes these companies use servers that belong to third parties that they have limited control over. So the problem that comes up is who is monitoring what is pushed out to the clients and is the process of updating secure? If someone was able to figure out how the update process worked in the peer to peer schema and wanted to infect other users with malicious code, would there be a way to identify it and how would you stop this?

Now one way to stop this kind of attack would be to have the vendors code digitally singed so that any other code would not be accepted (this is how some of the game companies do there updates). Now you might think, "I have a firewall, so this dose not affect me." But if your computer makes the connections directly to a server that routes your connections to the other clients, then you now have an established session to that computer. The firewall now trusts this connection until it is probably closed. Once the session is open it is a direct link from them to you without your firewall getting involved. This statement also applies to NAT firewalls and any other firewall that allows established connects.

One way to see what's going on is to run Netstat from your Windows command line. This will show you the established

connections to your computer and also the ports and protocols being used. Another way to see what is happening is to run a protocol sniffer like Wireshark (formerly Ethereal) and look at the packet traffic to see what your computer is doing. You will be surprised at what your different programs send back to the vendors server, and, most of the time, you have agreed to this release of your personal information by clicking the agree button when you installed the software.

The safest thing to do is not use programs that you do not need, and, if you feel you need to use a certain game or application, make sure it is not a warez copy. A lot of warez software is loaded with Trojans, not to mention it is stealing. I feel it's just a matter of time before the gaming community sees an attack similar to this one, and when it happens we are at the mercy of the vendors and anti-virus companies to make a fix. Hopefully with newer versions of Windows such as Vista, we will see better security. But when you think about it, the true responsibility of computer security is the owner of the computer. We need to make sure we all educate our less technical friends, family, and users.

To hear a pod cast that covers a lot of what I have discussed here and that was the inspiration for me to write little paper please visit http://www.sploitcast.com/ Sploitcast Episode #17.

Brian Wilson (bwilson@ethicalhacker.net) has over 12 years experience in IT starting with a tour in the United States Army. He has worked in and out of the US Government in many different organizations and technical roles including a stint as a Cisco Certified Instructor. Currently he works for one of the largest US broadband providers (ISP) as a Senior Data/Voice Engineer supporting over 3 million High Speed Internet/ VoIP subscribers. He has attained a number of industry credentials covering many aspects of IT including CCNA, CCSE, CCAI, MCP, JNCIA, Network+, Security+, and many DoD Certifications. He also uses his knowledge of IT to benefit a number of charitable organizations. Clearly Brian's knowledge and interests are wide, and his affinity for philanthropy will be the overiding theme of his vast set of articles and videos.