

Re: Identity P/W and Security question

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-08/0915.html>

From: Frode (news_at_mascot.REMOVETOREPLY.dyndns.org)

Date: 08/29/03

Date: Fri, 29 Aug 2003 17:13:23 +0200

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

mt0 wrote:

- >> *complex uses than just "block everything". It's very simple, no arguing*
- >> *that. But for simple use that's all that's needed.*
- > *But IS there such a thing as "simple use" anymore? Or a "simple" home*
- > *system these days? 24/7 always on cable/DSL connections, home networks,*
- > *etc.*

If all you use the permanent connection for is surfing, yeah. My family members are perfect examples. They use the net to send mail, chat, surf and not much else. They never use software that requires specific ports to be open/forwarded etc. A firewall that just blocks all incoming connections and a virus scanner to take care of the mail worms is all they've ever needed.

- > *Spyware busters ie Spybot Search & Destroy and AdAware block or remove*
- > *incoming malware but do nothing whatever to prevent outgoing*
- > *communications from extant programming between runs.*

Agreed. However other measures are taken to prevent the programs from getting in in the first place. So if they block them that's sufficient. Also, if the mail is handled securely (html off, not executing attachments), the firewall is on and IE up to date, there aren't many ways left that common malware tries to get in through.

- > *Far too many antivirus programs operate strictly on known virus*
- > *definition patterns – spyware is not a "virus" thus no definitions are*
- > *included.*

Aye. If you're the sort of person that install everything you find "just to test" you might want to run something that'll block outgoing connections from unapproved programs. If you show some prudence in what you install it's not really necessary however, is my point. The OP was quite clear on the subject of being careful so it ought not be an issue for him.

alt.computer.security: Re: Identity P/W and Security question

- > *It is also a very nice way sometimes to prevent infection in the first*
- > *place. Example – MBlaster.*

It gets in by connecting to a port. A port it won't be able to connect to even through a simple firewall like XP's built-in one.

- > *been reported to ID the pattern.) It takes only a minute or so to pick*
- > *through the info for a new virus that hasn't reached you yet and*
- > *proactively combat it by blocking the port it uses or writing a message*
- > *rule to deliver it to the trash.*

The default rule for any decent firewall = all ports blocked and you then open any you specifically need to let through (for virtually all casual users that equals 0).

- >> *I repeat, it's a very simple firewall. But for people just running*
- >> *around the net surfing news sites or whatever it does the job.*
- > *I have to *strongly* disagree with you on this one.*

By all means. Would be boring if everybody agreed all the time :)

- > *every nasty I've seen in the last year or so has come from a "safe" news*
- > *site – msnbc, cnet, download.com, foxnews – all the places one would*
- > *least expect. Some of these particular sites are so bad that I won't even*
- > *visit them without everything disabled – no java, no scripts, no activeX,*
- > *no nothing.*

Can you name an example of a virus or trojan that has propagated via ads on a major news site? Every nasty I've heard of for the past few years have virtually always been one of two: IIS exploit or Email worm. Can't remember any infecting major webpages and propagating that way. Curious about what you're referring to.

- > *Whether or not you want to see the notification is a preference. When*
- > *your machine no longer functions normally because you were innocent &*
- > *trusting enough to think a "firewall" was keeping it safe (as it surely*
- > *will sooner rather than later if you are just a "simple" user visiting*
- > *news sites) then it can be a whole lot of work to trace a problem that a*
- > *firewall log might have revealed almost immediately.*

I don't follow your logic here. For one, I've never heard of a virus spreading via popups or otherwise from major news sites. Assuming that IS the case I fail to see how your firewall logs would show it since it would undoubtedly come in via packets you've requested (an ad or a script for example) and the firewall log would show nothing out of the ordinary since it would just be one of any number of legit packets from that site.

- > *No, no – ZAP doesn't just block pop-ups. It blocks ALL the ads. I*
- > *literally never see an ad for anything except those rare few that are*
- > *text ads. Once in a great while I *do* want the popup – sometimes sites*
- > *put*

Re: Identity P/W and Security question

> *things that aren't ads in a small popup.*

Ah, you're more picky than me then. I don't care about an ad in the margin of the window and stuff like that. I just don't look at them and they don't impede my browsing nor pop up to block what I want to look at. The few sites that do use ads that temporarily show up on top of the article text I visit so rarely it's not a bother to me either. Certainly not enough to make me install a program to avoid it.

>> *features than they provide then use other programs. However, for most casual users, the XP firewall and toolbar popup blocking will suffice imo.*

> *If you access the Internet, you need more features than these two programs provide.*

A few hundred million internet users would likely disagree. I have a hardware firewall that came with my adsl subscription so I don't run one on my main box, in addition to that a popup killer to make surfing liveable is all I really feel I absolutely need. Virusscanner is an added piece of security just in case I get a mail from someone I know with an attachment containing a virus.

> *If cost is a consideration, there are several decent firewalls available that are free to home users, ranging from user-friendly Zone Alarm to fairly complex programs that you can write your own rules for.*

No argument there. All I'm saying is that for most people they don't have a need for it. Assuming they follow a few simple rules. Firewall enabled. View HTML mail as plain text enabled. Don't open attachments. Keep IE updated (or use another, more secure, browser). Don't install every piece of crap software on the net without having some notion of what it is first. Chances are low it carries a virus payload but malware abounds.

Follow that and chances are your virus scanner will never pick up a virus (unless it pops in as an attachment with a mail you wouldn't have opened anyways) and your spyware-firewall won't ever catch an unsolicited outgoing connection since no malware will have a way to get installed. Although installing one just to keep tabs on what programs access the net is of course a valid reason. Same for "just to be on the safe side" with every other product that's been mentioned. But essential? Not in my opinion.

> *And you might want to investigate that Google toolbar popup blocking – there are a number of reports that it in itself is spyware.*

Yeah, I've heard that too. I fail to see how software that prior to downloading forces you to choose the version with "spyware" (reports your URLs to Google in order to provide page ranking display in the toolbar) or without, and also pops up a message box very clearly stating the privacy concerns if you enable it.

alt.computer.security: Re: Identity P/W and Security question

-- --
Frode

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0.2

iQA/AwUBP09tkuXIGBWTt1afEQLNPACfWOiQva0s3ChcO0WJ6XNH1dUgNQY AoJ5Z
O3sxY/tEK2FWWkwoXVZIZWBv
=IeKD

-----END PGP SIGNATURE-----