Linux is Not the Answer to Security Problems

Lori MacVittie, 2009-02-10

Malicious links served up in a browser are OS agnostic. They don't care about the OS because the target is people, not technology.

In response to the problem of links and trust put forth in a recent post a reader replies that the answer to "evil links" is simply to run Linux instead of Windows.

> *the very best solution is to run something other than windows, and with ubuntu at its current state of maturity (and free-ness), why wouldn't you?*

I won't disagree with the assessment of Ubuntu and its current state of maturity. It's ***very*** nice, and I'm enjoying it immensely on my new laptop for a multitude of reasons and Don and I have always insisted that our children run a Linux distribution on their laptops just to minimize the impact (on us to cleaning up) of automatically downloaded and installed viruses and trojans. And the commenter is partially right – running a Linux-derived operating system will indeed protect many users from the automatic installation of many OS-specific (read: Windows) targeted viruses and worms. But it's not the answer to the problem of malicious content a la links because most of the time the target of the content isn't technology, it's the ***user, and*** it isn't relying on an operating system, it's relying on a browser. And unfortunately, users aren't going to change their behavior because they're running Ubuntu or a Mac or Windows or an iPhone.

WEB 2.0 and CLOUD CHANGED THE GAME

One of the great things about standards in the browser like CSS and JavaScript and XHTML is the ability to create a rich and interactive user interface ***and*** have it consistent across operating systems and browsers. With the increasing reliance on "cloud-based services" for e-mail, personal document management, photo storage and generally any consumer-oriented use of a computer that used to be associated with a fat client now being pushed out to "The Cloud" the browser is the primary interface between the user and the rest of the world.

If that interface can be, and it is all the time, leveraged by miscreants to manipulate users into providing their credentials or unknowingly assisting in the spread of links and code that can accomplish the same then the operating system upon which that browser is running is neither an advantage or a disadvantage.

And that's exactly what's happening. The benefit to miscreants today is in identity theft; in obtaining credit card and personal information that can used or sold for monetary gain. The old "destroy your computer" viruses of the 1990s are passé and not in vogue. Today it's about theft, plain and simple, and almost all viruses that are distributed are done so in the hopes of accomplishing ***that*** task. "Viruses" today are keyloggers and applications that turn consumers' desktops into part of a giant botnet that is performing mass SQL injection attacks with the intent of injecting a link that will entice a user to willingly hand over their identity.

And because it's well-known that the Web is the Way, miscreants have turned to attacks that target the browser and the trust inherent in hyperlinks, in the visual clues that users take that engender trust like, say, the logo and design of the website. Clickjacking and cloning-based attacks are predicated on the ability to exploit the trust users have for a web site. If it looks like Twitter, or Facebook, or My Banking Institution, then it must ***be*** that site. Overlaying a "virtual keylogger" using clickjacking or cloning the site and using a domain name that includes the relevant site name in it is enough to convince a user that they are indeed on the site in question and certainly it must be safe to enter their credentials.

And from that one set of credentials the rest of the integrated, collaborative Web 2.0 world is opened to the miscreant. One set of credentials begets another and if they're lucky enough to get your web-based e-mail credentials well, it's like finding a pot of gold at the end of a digital rainbow.

With the exception of trojans and viruses designed to act as part of a larger botnet, there's nothing specific to the operating system here: it's all about the browser and deception. MacOS? No problem. Ubuntu? Great. Windows? Don't care. This is social networking engineering at its finest: manipulating the trust of a user through the same rich interface technologies that have made the operating system irrelevant.

Comes the cloud and now trojans and viruses become even *less* relevant to the game. Given someone's credit card and identity a miscreant could easily leverage cloud computing to accomplish what the end-user now will not. Move every consumer to an Ubuntu desktop and miscreants will simply find another way to launch their botnet, and that way likely leads to the cloud. Scalable, on-demand, self-service. It's a miscreant's dream.

THE PROBLEM IS NOT TECHNOLOGY BUT THE SOLUTION WILL BE

The problem of links and the potentially malicious intent behind them is not one of technology in the traditional sense. Yes, technology is being manipulated to enable the use of links as a deceptive theft mechanism, but technology – whether guns or screwdrivers or clubs or lockpicks – have always had both good and bad uses. The intent of the wielder is always at the root of the issue. The problem is two-fold; first, it's financially advantageous to miscreants to perpetrate such attacks and second, users are still woefully uninformed about phishing and pharming and avoiding the deceptions inherent across the Interweb today. There doesn't seem to be much we can do about the first part of the problem and addressing the second is a never-ending battle.
Unfortunately, that's not due to a lack of trying on the part of information security advocates. Trying to explain how to spot some of these deceptions to a typical consumer is like trying to explain to me how to tell the difference between the sounds a car engine might make when it's in trouble. You can try, but I likely won't "get it" or be able to put it into practice. It seems simple to you and I because we're knee-deep in technology day after day. But for someone who just wants to get their e-mail and post a photo on Flickr and update their Facebook status…it actually *is* rocket-science and it *is* that complicated.

The solution will likely eventually be found in technology, it always is, but it won't be as simple as a change in the operating system because that variable has been largely neutralized thanks to Web 2.0 and "The Cloud."

- Excuse Me But Is That a Gazebo On Your Site?!
- Web Application Security at the Edge is More Efficient Than In the Application
- WILS: InfoSec Needs to Focus on Access not Protection
- An Unhackable Server is Still Vulnerable
- Twittergate Reveals E-Mail is Bigger Security Risk than Twitter
- Automatically Removing Cookies
- Clickjacking Protection Using X-FRAME-OPTIONS Available for Firefox
- Stop brute force listing of HTTP OPTIONS with network-side scripting
- Jedi Mind Tricks: HTTP Request Smuggling
- I am in your HTTP headers, attacking your application
- Understanding network-side scripting

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com