Herding Cats:
This Ain't Yo' Daddy's Malware!

June 2011

BrandenWilliams
SECURE BUSINESS GROWTH

When I started framing up this article, I wasn't sure how far back into malware's history I should go. One of the clearest examples of the origination of debilitating malware could be the 1988 Morris Worm, largely credited as the first widespread Internet worm. While technically simple, it's creativity forced administrators to change the way they thought about this fancy thing called the Internet. Viruses and trojans were around in those days, but mostly as data destroying nuisances or things that render machines unusable. In fact, I will neither confirm nor deny that the prankster in me wrote a few of these innocent programs masquerading as versions of Doom[1]. Sure, I may have made someone laugh (or scream), but I didn't cause any permanent damage to any hardware or business process.

Things are a bit different today. Malware is both crafted in a targeted manner for hire and used in mass destruction activities designed to cause havoc across multiple industries. For those in the right circles, development kits exist for rapid malware creation. As of last month one of the biggest recent headaches' source code is now available for download[2].

"But I have anti-virus software," you might say. "I'm covered from all manner of malware according to the marketing material from my anti-virus company!" Sure you are. So are the millions of victims whose computers are members of botnets. Patching machines on some regular basis and updating anti-virus subscriptions doesn't solve the issue. Anti-virus is pretty effective when it comes to battling things it knows about. The problem is that many of these trojans change in such a way that they render anti-virus ineffective, yet users are still lulled into a false sense of security by keeping them up to date.

Think of it this way. If you were told to walk across a two-inch I-Beam suspended 100 feet in the air, would you walk across differently if there was a net right below the beam to catch you if you fell? I certainly would. I would be hugging that beam for dear life without a net, whereas with a net it would be more of a personal challenge to make it across without falling. I would feel secure in the fact that if I did fall I would get to try again without visiting a hospital. If I know I am protected from clicking on something that might compromise my machine, I am more willing to click than if I know that there is a significant chance that "clicking here" could spell my demise.

Security nay-sayers have complained about anti-virus for years—in some respects for that very reason. Browser-based attacks are becoming quite a problem and anti-virus manufacturers have not been very effective in protecting against this threat. It's not that they are not trying, but in my personal experience, the amount of CPU power required to live inside the browser makes the thing almost unusable. It's such a serious issue that companies are working on plans for disposable browsers where you could visit various sites and essentially delete their existence when complete, thus rendering any installed malware ineffective past that usage.

Now you must be thinking, "OK, so this is scary enough. What can I do?"

I'm certainly glad you asked me that.

For one, remember defense in depth. Don't rely on any one control to keep you safe. If you are deploying sophisticated anti-virus software but not performing basic egress or content filtering, you are putting all your chips behind something that is not proven to be fully effective. User experience in the workplace should be balanced by the consumerization

FOOTNOTES

[1] *If THAT doesn't take you back to the good old days, nothing will!*

[2] *Complete ZeuS sourcecode has been leaked to the masses: http://www.csis.dk/en/csis/blog/3229*

of IT and the needs of the business. Social media needs special attention because recent incidents have shown it to be a great place for malware to propagate. Most of all, focus your defense efforts on the key pieces of information that your organization needs to survive, and destroy any information that you don't need or can look up from another authoritative source. Assume your network is compromised and design your security controls around that notion.

This ain't yo' daddy's malware! Don't try to combat it the same way he did!

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH