



Veneratio Diligentia Vires

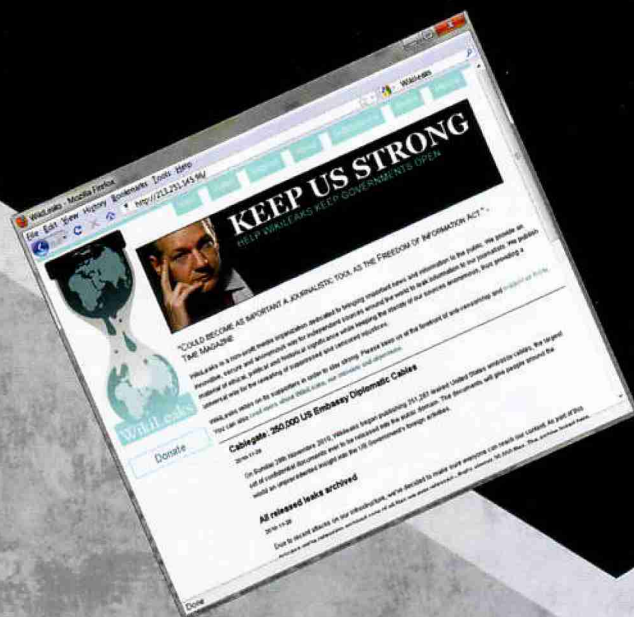
The Journal of Counterterrorism & Homeland Security International

Lessons Learned From The WikiLeaks Fiasco

By David Gewirtz



(Editor's Note: Articles are written for this Journal several months before publication, so it's entirely possible that the ongoing Wikileaks situation will have changed by the time you read this.)



T

here are three important homeland security lessons that you and your organizations should take to heart from the Wikileaks situation.

Lesson 1

Personal electronic devices should be absolutely banned from secured locations.

I have said this before, both in this publication and in mainstream media. Personal electronic devices are a massive national security risk. They must not be allowed, under any circumstances, in secured facilities. Period.

Let's run the numbers again. Last year, in "USB: The Trojan Horse of Digital Technology," I wrote that you could fit 376,000 copies of this magazine on a typical 16 gigabyte iPhone.

Bradley Manning's alleged entire "take" of secret diplomatic cables was estimated to be 1.6 gigabytes. A basic iPhone can hold 10 times the information stolen, causing heartburn among diplomatic and security professionals worldwide.

The prevailing argument against a complete lockdown of personal electronics is generally that employees want their toys.

Some of their jobs are tedious, and iPods and the like make those jobs easier to tolerate.

It doesn't matter. We will see repeated leaks and breaches (not only of information coming out, but malware and attack software going in) if we allow these devices inside our secured walls.

Lesson 2

Once leaked, the information genie can't be put back in the bottle.

Wikileaks, itself, is merely a Web site. Web sites can be shut down. Access to a Web site is controlled by a number of technologies that can be influenced and controlled by legal entities. The domain name (like "wikileaks.org") is controlled by digital data records in the domain name system, domain registrars, and domain name servers. These records can be expunged or disabled, and the name will no longer route to the Web server.

The Web servers themselves can be shut down. The actual server is generally a box running at some hosting provider's site. Sometimes there are multiple boxes, but the hosting provider can be instructed to shut down the Web site's account.

The network connection to the Web server can also be shut down. If the site runs out of a home or a physical location, the network connection is often provided by a communications service provider. These, too, can be terminated for just cause. And yet. Here's the thing. A Web site is merely a collection of files. These files are typically organized in a Web site-friendly manner, or just stored as PDFs, Word files, text documents and the like.

Files are pretty much the easiest thing to move and copy around the Internet. Mirroring (completely duplicating) a collection of files is child's play to





Veneratio Diligentia Vires

almost anyone with basic Internet skills. There are billions of computers online, and any one of these (along with, as we've shown, thumb drives, smartphones, and the like) can store copies of leaked documents.

Once leaked, if the documents have gotten out "in the wild," it is entirely unlikely that they will ever be completely retrieved and expunged from public distribution. Therefore, it's important that those who secure documents remain aware that their information may not forever be secured. They should take extra precautions to both secure the information from any possible leaks (see my first point above), and try to conduct business in a manner that if those documents do get leaked, they're not embarrassing to their owners.

Lesson 3

Organized attacks will come from actors without national, political, or financial affiliations. Security and military professionals are accustomed to fighting actual enemies. Initially, it was nation states. Then, with terrorism, the enemy became terrorist groups. Business interests and organized crime can also choose to attack resources of interest.

But we're now seeing a new form of attack. As various financial providers stopped providing funding services to Wikileaks, those providers found themselves on the receiving end of distributed denial-of-service (DDoS) attacks. We've talked about DDoS attacks before here in this publication.

These are digital attacks by thousands (and often

millions) of zombified computers, each sending network messages with the purpose of overwhelming and eventually crashing the recipient systems. These networks of zombie computers are called "botnets" and they're often controlled by commercial interests, organized crime entities, terrorist organizations, and even teenagers who managed to download the right software from less-than-savory Web sites.

The attack on the financial providers who cut off services to Wikileaks wasn't a for-profit effort. Instead, it was initiated as a political message, a message sent by Wikileaks' supporters to indicate their disapproval of the financial providers' actions. It was, essentially, a very large, very disruptive crank call, repeated millions of times. DDoS attacks can

Eventually, the target will fall. Distributed denial of service attacks continue to be difficult to fight. It is often impossible to stop the actual attack. Instead, most cybersecurity professionals have taken to deflecting the attacks, using tools that can mitigate the strength of the attacks, and working with network security professionals at all levels of the Internet's infrastructure to shunt the attacks away from vulnerable resources.

This stuff isn't fun, the game is constantly changing, and digital weapons of mass destruction are now in the hands of cranky pranksters with twisted senses of humor. If it ended there, it'd all be annoying, but manageable.

Unfortunately, there is a true terrorism angle to these attacks. Many of the groups who use DDoS attacks as political commentary devices are comprised of anonymous members. People who belong have no idea about the real identities of their fellow

jump on, in a bandwagon effect. It's here that the terrorism risk becomes valid.

Because members don't know each other, these groups can be very easy for terrorist organizations to infiltrate. Since the concurrence of a small number of members is enough to start the ball rolling on an attack or disruptive prank, terrorist organizations merely have to infiltrate a small group of separate people (or, more accurately, access the group using computers with different Internet addresses).

Once inside, the terrorist organizations can incite the group members to attack targets they might not otherwise have considered. Most group members participate for the "lulz" (the prank value) and would be horrified if these attacks caused lasting damage or death. On the other hand, terrorist organizations have no such sense of right or wrong, and can use these anonymous pranksters to initiate real, lasting damage.

So there's the challenge. It's impossible to track down all members of these anonymous prank groups. Instead, we need to continue to build up tools and resources to help resist and deflect DDoS attacks as they occur.

About the Author

David Gewirtz is director of the U.S. Strategic Perspective Institute and editor-in-chief of the ZATZ technical magazines. He regularly writes commentary and analysis for CNN's Anderson Cooper 360, and has written more than 700 articles about technology. David is a former professor of computer science, has lectured at Princeton, Berkeley, UCLA, and Stanford, has been awarded the prestigious Sigma Xi Research Award in Engineering, and was a candidate for the 2008 Pulitzer Prize in Letters. He is the Cyberterrorism Advisor for IACSP.

David's personal Web site is at DavidGewirtz.com. Read his blog at CNN Anderson Cooper 360 for politics, policy, and analysis. Read his blog at CBS Interactive's ZDNet Government where tech meets politics and government. Or Follow him on Twitter at @DavidGewirtz



These are digital attacks by thousands (and often millions) of zombified computers, each sending network messages with the purpose of overwhelming and eventually crashing the recipient systems. These networks of zombie computers are called "botnets" and...

Seeking the Edge Through Education, Training, and Technology

ruin your whole day. These attacks are exceptionally asymmetrical in their assault profile. Millions of computers, scattered all across the world, often owned and operated by people who have no idea they're cannon fodder, are all aimed at one point, all pounding on one element of a computer system or network.

pranksters. That's a big part of the appeal. They can cause trouble in the digital world, and it's not visible to their friends and neighbors.

Often, an attack or pranking scheme is initiated by one of the members and the other members



The Journal of Counterterrorism & Homeland Security International