Cyber-warfare Has Just Moved Into The Realm Of Reality

Ever since computers became popular, there have been those who wanted to hack their way in and find their secrets. For most of those early hackers, the thrill was in the chase, and the victory was in breaking in.

Most of their work was benign, with hackers being content to have succeeded in doing what they weren't supposed to be able to do.

As computer use grew, so did hacking. But it changed as well.

With the massive connectivity and easy access that the internet offers, more and more hackers found their niche in life. These newer hackers weren't content with merely breaching security for the sake of breaching security, they had nefarious intent in their work.

Whether that was the spread of viruses, identity theft or simply data mining for profit, it looked at the millions of computers connected to the internet as targets for attack, not just for play.

Malware has become a major threat on the Internet today, with countless hackers and even companies creating and distributing it across the world. While some is merely created for commercial purposes, placing ads on people's computers, there is much more that spells real danger to individuals and companies worldwide.

It couldn't stay that way though. Governments everywhere hold with the idea that only they can pursue illegal activities. While they work to keep their citizens from committing those acts, they are quick to adopt them themselves, and use them covertly to further their country or political party's agenda.

Such has been the case of hacking and malware in general. The first to see the value of it were the Chinese, who created a cyber-warfare branch in their army. They immediately started working to find ways into other countries computers, especially those of opposing governments and their military branches.

They didn’t limit it to that. They sought out ways to attack critical infrastructure, such as disabling power plants or bypassing the failsafes on nuclear power plants.

While China got a head start on the rest of the world, other countries have been working to catch up, including the United States of America.

Rather than making cyber-warfare a branch of the military, it seems that we’ve left it up to our intelligence organs, most especially the CIA and the NSA.

Once it moved behind the walls of intelligence operations, any efforts towards U.S. development of cyber-warfare became very hush-hush. Few knew about it, and even fewer admitted it was happening.

The vast majority of Congress was left in the dark, as they had no oversight of intelligence operations. And with Congress in the dark, the American people were totally cut out of what was happening.

Vault 7, the US Government and Cyber-warfare

The most recent Wikileaks dump, cryptically called Vault 7, has breached the secrecy of US government involvement in cyber-warfare for the very first time.

Specifically, the first 8,761 documents demonstrate the CIA’s involvement in creating millions of lines of malware code,

including viruses, Trojans, weaponized “zero day” exploits, remote control systems and other forms of malware.

In total, there were over 1,000 different hacking systems, Trojans, viruses and other “weaponized” malware. While the actual code does not seem to be part of the data dump (and that’s a good thing), documentation about its existence and descriptions of its capability have been released.

All of this was produced by the Center for Cyber Intelligence (CCI), a sub-agency of the CIA’s Directorate for Digital Innovation (DDI). This directorate, the most recent addition to the CIA’s organization chart, comprises over 5,000 registered users, many of whom are programmers and expert hackers.

The release of this information is a major blow against American cyber-warfare; but apparently it’s one that needed to happen. I say that, even though I’m not entirely comfortable about it, because according to Wikileaks, the CIA has recently lost control of the majority of their digital arsenal.

This extremely dangerous code has been circulated amongst former U.S. government hackers and contactors in an unauthorized manner.

Notice that I said “former,” not current. That’s the information that Wikileaks has, and also the means by which they were given access to this amazing data. Apparently one of those former workers felt the public needed to know what was going on behind closed doors.

The Malware Market

Should this code make it out into the dark Internet, the results could be disastrous. Apparently there is quite a market for all sorts of malware, with customers willing to pay large sums, even into the millions for programs which will

permit them access to things they shouldn’t have access too.

But that’s not the biggest problem. The big one is that once out in the open, this malware could spread around the globe in mere minutes, used and targeted by an army of individual hackers.

Unlike other weapons systems, electronic weapons don’t explode and disappear. If anything, their “explosion” causes them to multiply across computers and networks, infecting more and more as they go.

While it may be possible to take them off a particular computer, usually by scrubbing the hard drive and doing a global reinstall, they never really go away. The same electronic weapons can be used over and over again.

This code got out into the open, we can’t count on the good graces of the people who have it. While some of those CIA contractors and employees will act responsibly with what they have, invariably there will be those who will see an opportunity to use it for nefarious ends or perhaps for personal gain.

There’s another aspect of this, which is even scarier than what hackers will do with the CIA’s digital arsenal. That’s what the CIA themselves have done with it.

In 2013, Edward Snowden came forth as a whistleblower, informing the country that the NSA was spying on American citizens, in contrary to the law. This new batch of information tells us that the NSA aren’t the only ones doing that. The CIA is doing so as well.

There have always been rivalries between the various intelligence agencies. FDR created the OSS during World War II to combat this problem. Yet the OSS and later the CIA haven’t managed to eliminate that rivalry. Rather, they’ve become part of it.

One of the results of these rivalries is overlaps in areas of responsibility and multiple departments performing the same task. Such seems to be the case here, with the CIA performing its own version of the NSA's work. Yet without knowing who ordered the CIA to do this or when it was ordered, there's no real way of knowing whether this is an authorized operation or not.

Video first seen on Fox News.

But there's more than just the CIA spying on our communications, like the NSA does. Apparently they've developed malware that targets iPhones, Android phones, smart TVs and even Microsoft Windows. This malware invokes thoughts of Orwell's 1984, if anything does. With it, the CIA can turn on these devices and use them to spy on their owners.

For some reason, Samsung TVs in particular have been targeted by the CIA. Their malware, called "Weeping Angel," which was developed in conjunction with the United Kingdom's MI5, allows the television to operate in a "fake off" mode, where it appears to be off to the owner, but a microphone in the unit is recording everything said in the room and forwarding it to the CIA, via the internet.

This is just one example of the types of "back door" malware programs which the CIA has developed. Similar malware can be used to hack in to smartphones allowing the CIA to determine the owner's location, read their e-mail, their text messages, search the phone's memory and activate both the camera and microphone.

Quite literally, they can spy on anyone, anywhere, anytime they choose, and we can't do a thing about it.

Even encryption won't help, as the CIA has means of accessing the data, before it is encrypted. So much for the various communications platforms out there, which claim to encrypt

your communications. If the CIA can access the information before it is encrypted, the encryption is useless. The government will know what's in your communications, perhaps even before you do.

Before We Panic

All of this capability was probably developed with the best of intentions. The CIA, like other intelligence agencies, is involved in the war on terror. As terrorists tend to hide in the population and use the same communications that many of us do, it is necessary to develop the means of penetrating those communications to investigate the actions of those terrorists.

But where does it stop? What's to say that they aren't amassing files on each one of us? It's already been reveled that the NSA is doing that, storing all of our communications in their massive data storage facilities. Snowden told us how that information is misused by analysts breaking the rules.

Those analysts aren't the real issue though; the real issue is the government that is stealing our privacy. Spying on American citizens is a clear betrayal of our Fourth Amendment rights against unlawful search and seizure.

Yet we, the American people, are routinely subjected to a level of surveillance that the Founding Fathers couldn't have imagined. Even those of us who are not doing anything illegal have things in our lives, which we would rather not have known.

Even if the CIA can demonstrate that they haven't broken our Fourth Amendment rights, how can we trust them? There is literally nobody who has access to their files. So there is no way to prove that they are telling the truth.

The only information we would have access to, is that which they release, with the intention of demonstrating their

innocence. Not exactly something you could take to a court of law.

There is only one solution for those of us who want privacy. That's to foreswear the use of all modern means of communications. While not exactly practical, there may come a day when we need to; especially if the government starts misusing our information.

I just know one thing. I'm going to be careful about what I put out over the Internet, over my phone and through any other electronic means of communications I find myself using. There's no reason to give anyone ammunition, which might find its way back, being used against me on some future date.

*This article has been written by **Bill White** For Survivopedia.*

References:

http://www.foxnews.com/tech/2017/03/08/cia-cyber-spying-toolkit-now-in-hands-hackers-worldwide-wikileaks.html

https://wikileaks.org/ciav7p1/

http://www.wired.co.uk/article/cia-files-wikileaks-vault-7