New American

Written by **C. Mitchell Shaw** on April 17, 2017

Published in the April 17, 2017 issue of the New American magazine. Vol. 33, No. 08

Foiling Foul Hackers

In the wake of WikiLeaks' recent revelations of the CIA's (formerly) secret hacking program, many are left with the feeling that this is the end of privacy. As The New American highlighted in our last issue's Inside Track column, the truth is that privacy has probably never been in better shape than it is in right now, because the CIA hacking program shows that encryption works. Sometimes, the first part of good news is bad news. In this case, the bad news is very bad; but the good news is *great.*

First, the bad news is detailed in my article "The CIA's Hacking Ability." In short, the CIA spent the post-9/11 years building an arsenal of powerful hacking tools — cyberweapons — and a formidable army of hackers to use those weapons. Then, in a move that would make the Keystone Kops look brilliant by comparison, the CIA somehow managed to let those weapons loose in the world. Now, the only safe assumption is that any script-kiddie, teenaged hacker who spends his days in his mother's basement eating cold pizza, playing video games, and stealing credit card numbers has access to government-level hacking tools.

By exploiting vulnerabilities in operating systems and the software running on those operating systems, a hacker using these cyberweapons can compromise the security of a plethora of devices — such as computers, mobile devices, and SmartTVs — and use them to watch and listen to anyone in the range of the built-in cameras and microphones. That hacker — whether state-sponsored or teenaged — can access files and folders, steal (or plant) data, and otherwise wreak havoc.

So, yes, it's bad. But that bad news relies on something *completely* in the control of almost anyone living in the digital age: unpatched vulnerabilities. Before we get into what that means and what can be done to protect your devices and your privacy, let's spend a few minutes looking at how we got here.

Mass Surveillance vs. Targeted Surveillance

The Snowden revelations of almost four years ago confirmed what many had long suspected: U.S. government agencies were routinely conducting mass surveillance on everyone, including American citizens. Using programs with names such as PRISM, MYSTIC, Boundless Informant, and Xkeyscore, the NSA and other three-letter-agencies were intercepting everything from phone calls and texts to e-mails and browsing histories and everything in between. It was also revealed that nosy corporations (Google, Microsoft, Facebook, etc.) were doing their own data mining.

In the months and years that followed, more and more people demanded software tools to shutter the tools of mass surveillance. The free market replied to that demand with a trove of tools to protect users' data. As we said in the Inside Track in our last issue:

The most effective tool for that is encryption. By encrypting data at rest (files and folders stored on a device), the owners of that data can be assured that it can only be accessed by someone with the

encryption key or password. By encrypting data in motion (communications), the parties to those communications have the same assurances.

As more and more people began to employ powerful encryption tools, the surveillance hawks — who have built their careers building the surveillance state — found themselves harvesting unintelligible gibberish. Since the only way to decrypt any piece of data after it has been encrypted is to use the correct decryption key (which is mathematically impossible to break), the surveillance state had to change its game. What the leaked CIA documents and files show is that — because of the growing use of encryption — the scales have tipped in the favor of those who value their privacy enough to take appropriate measures to protect it. As a result of that, the surveillance hawks have — for the biggest part — shifted from mass surveillance to targeted surveillance of selected devices.

In other words, the use of encryption in the hands of ordinary citizens has pushed back against the surveillance state and moved the line. Instead of casting surveillance nets, the three-letter-agencies are forced to fish with a rod and reel. One fish at a time. This is much more costly (in both dollars and effort), and that serves as a deterrent to random fishing expeditions.

Protecting Your Privacy in the Digital Age

For computer users who are concerned about how to protect their privacy, the first step is to make sure their endpoint devices (computers, mobile devices, routers, etc.) are running up-to-date, reliable, trustworthy operating systems and software. In fact, when The New American reached out to companies and organizations involved in promoting digital liberty to ask what the CIA revelations mean for the state of privacy, one recurring theme in their answers was that those users who keep their devices up-to-date are at the very least risk.

Dr. Andy Yen, CEO and co-founder of ProtonMail, told The New American that ProtonMail is "encouraging users to work to harden their endpoint devices, by actively patching all the software that they run." Fortunately — as mentioned above — this is something that is completely in the control of those who own and use computers and other devices. Following Dr. Yen's advice, users should download and install the most recent versions of all software along with all new security patches.

Dr. Yen's advice carries considerable weight when one understands who he is and what he does. ProtonMail is an open-source, end-to-end encrypted, zero-knowledge e-mail service with its servers located in Switzerland. His company's decision to build and secure its software the way it has is no accident. It was designed — from the ground up — to protect its users' privacy. Since it is built on open-source software, there is no way for anything nefarious to be hidden in the code. Since it is end-to-end encrypted, even the administrators don't have access to the users' data. Since it is zero-knowledge, the administrators don't know, and have no way to know, users' passphrases. With its servers located in Switzerland, they are outside of the jurisdiction of both the United States and the European Union.

Anyone concerned about privacy should consider switching to ProtonMail. Say goodbye to Gmail's data mining and hello to ProtonMail's encrypted privacy. As more people begin using encrypted services, the more pervasive and normal they will become. The result is that everyone is more secure.

In a public statement about the CIA leaks, ProtonMail said:

We can state unequivocally that there is nothing in the leaked CIA files which indicates any sort of crack of ProtonMail's encryption. And despite claims to the contrary, there is also no evidence that

Written by **C. Mitchell Shaw** on April 17, 2017

Published in the April 17, 2017 issue of the New American magazine. Vol. 33, No. 08

Signal/Whatsapp end-to-end encryption has been breached. Here's what we do know:

Over the past three years, the CIA has put together a formidable arsenal of cyberweapons specially designed to gain surveillance capabilities over end-user devices such as mobile phones and laptop/desktop computers. These advanced malwares enable the CIA to record actions such as keystrokes on a mobile device, allowing them to conduct surveillance without breaking encryption. Through this technique, US intelligence agencies can gain access to data before they have been encrypted. This is in fact the only way to achieve data access, because cracking the cryptography used in advanced secure communication services such as ProtonMail and Signal is still impractical with current technology.

We asked Dr. Yen if a user running the most recent patches for their operating system and other software could be at risk using ProtonMail. He answered, "There can never be zero risk, so the way I would put it is, a user who has fully updated all his software would be at lowest risk of CIA hacking."

Of course, updating all of the software on a computer could be very expensive. And — depending on the trustworthiness of the operating system — it could also be pointless. Not all operating systems are created equal, and they do not all value the privacy of their users. Since Microsoft has — with the advent of Windows 10 — essentially converted its operating system into a suite of spywares designed to harvest users' data and send it back to Microsoft, users concerned about privacy should consider switching to another operating system. While it is theoretically possible to lock Windows down to a secure level, it would require much more effort than most people have the time or inclination to give.

Any chain is only as strong as its weakest link, and Windows is a very weak link in the chain of privacy.

Mac is better, especially since Apple seems at least willing to stand its ground against the surveillance hawks demanding backdoors into the encryption protecting its iOS platform for iPhones. Apple has had its own issues with user privacy, though, and the most recent revelations from WikiLeaks show that the CIA has developed ways of embedding malware into the firmware of Mac laptops, so there are still concerns of government surveillance.

One solution is to replace Windows or Mac with Linux. Of course, since the CIA malwares designed for Mac laptops are "firmware" hacks that would persist even after the operating system was replaced — and it has to be assumed that similar hacks exist for laptops designed for Windows — simply replacing Mac or Windows with Linux in a computer infected with those malwares would not be enough. In the good-news column, though, those hacks require physical access to the device. So the best course of action would be to always buy your computers in person instead of online. That way, you know it has not been intercepted and injected with malware. Oh, and if a government agent ever has access to your computer (for instance, a TSA agent steps into another room with your laptop) — you should destroy the hard drive and sell the computer for parts. Never use it again. Don't even turn it on. Replace it and restore your data from your backup. You *are* backing up your data, right?

An Operating System That Values Your Privacy

Linux is a great alternative to Windows for those seeking a more secure and liberty-friendly operating system. Because it is open-source, there are many different "flavors" (called distributions) available. Two of the most popular distributions are Ubuntu and Fedora. Both are available as free downloads and can be found with a quick Internet search.

Written by **C. Mitchell Shaw** on April 17, 2017

Published in the April 17, 2017 issue of the New American magazine. Vol. 33, No. 08

Just don't Google it; in fact, if privacy matters to you, never Google anything again. Switch to a privacy-friendly search engine such as DuckDuckGo or StartPage. Both of these search engines focus on privacy by not tracking users or caching searches.

Your DuckDuckGo search for the privacy features of Linux will likely lead you to an online article this writer wrote for The New American last year. That article quotes Mark Shuttleworth — the man behind Canonical, which sponsors the Ubuntu Linux distribution — saying that Canonical "will never backdoor Ubuntu; we will never weaken encryption." Shuttleworth's claim does not require the blind faith required to accept Microsoft's promise in its Privacy Agreement that says, "Your privacy is important to us." Because of the open-source nature of Ubuntu, millions of computer professionals and enthusiasts alike have access to the source code. If there were backdoors, they would be discovered.

And while installing or using Windows requires accepting Microsoft's End User License Agreement (EULA) — which states, "Finally, we will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary" — Ubuntu has no EULA. And it's free (as in free beer) as well as free (as in free speech).

Furthermore, most of the applications available for Ubuntu are free, as well. It comes with LibreOffice (an open-source office suite comparable in function features to Microsoft Office) preinstalled, and there are open-source alternatives to almost any proprietary program. In fact, this writer does all of his work on a laptop running Ubuntu 16.10 and has no proprietary software apps installed at all.

Encrypt Everything

Ubuntu — like most Linux distributions — allows for full disk encryption as part of the installation process. This makes it simple to follow the advice of many privacy advocates: encrypt everything. The first part of that "everything" should certainly include the hard drives in your computers and the data on your smartphones. Fortunately, both Android and iPhone come with encryption by default.

The protection offered by encrypting your hard drives and devices is only as strong as your password. While the encryption cannot be broken, a weak password can be broken within minutes using a brute-force attack. A good password should be long, random, and include uppercase and lowercase letters, numbers, and symbols. As an example, a password such as 3cl!ps3dF3@+h3r5 would take a desktop computer one trillion years to crack, according to www.howsecureismypassword.net.

As long as it is protected by a good, strong password, the importance of encryption cannot be overstressed. In fact, in response to our questions about the CIA leaks, Open Whisper Systems provided the following statement to The New American:

These leaks are confirmation that ubiquitous encryption provided by WhatsApp and Signal are forcing intelligence agencies to use malware, pushing them from undetectable mass surveillance to high risk targeted attacks.

Open Whisper Systems — which is funded by donations — produces the Signal app for encrypted texts, voice calls, and video calls for both Android and iPhone. It is endorsed by people such as Edward Snowden who understand both the need for private communication tools and the technology behind them.

So it is the presence of "ubiquitous encryption" — such as that found in Signal — that has held the surveillance state at bay. No wonder the surveillance hawks pretend that encryption in the hands of ordinary citizens is a cause for concern. This writer addressed the attitude the philosopher kings in the surveillance state have toward encryption in a previous online article:

For all the ostensible reasons that the intelligence and law-enforcement communities give for wanting to limit the ability of ordinary citizens to encrypt their data and communications, the real reason is that those in power love power and want a monopoly on it. Government officials — who use encrypted systems for both data storage and communications — don't want private citizens to use that same technology. These are the same individuals who go about their daily lives surrounded by armed police officers, military personnel, and private security guards while decrying the evils of an armed society. This double standard is more than mere hypocrisy; it is tyranny.

The CIA leaks seem to confirm that those in power do not hold that what is good for the goose is good for the gander. They use powerful encryption tools to hide their footprints while hacking the endpoint devices of their targets, but cry bloody murder when ordinary citizens use that same encryption to protect themselves from that hacking. If they ever wonder why people have trust issues where government agencies are concerned, they need look no further than the nearest mirror.

Reinforcing the importance of encryption as the best hope for pushing back against the surveillance hawks and their war on privacy, SpiderOak released a statement in the wake of the CIA leaks that said:

The latest leak of the Vault 7 files includes many exploits, but unlike previous leaks, initial analysis seems to indicate that they are entirely for attacks against endpoints.

This transition from network level to endpoint-focused attack is an interesting trend that points to an interesting hypothesis: Encryption is working.

Encryption — and particularly end-to-end encryption — fundamentally changes the cost of attacks. No longer can an adversary simply sniff network traffic, either locally or globally. To eavesdrop on communications they must take the more expensive and risky approach of compromising endpoints.

SpiderOak has a vested interest in stopping the surveillance hawks. The company is behind SpiderOak One, an open-source, end-to-end encrypted, zero-knowledge alternative to DropBox. Considering that DropBox has Condoleezza Rice (who as secretary of state defended President Bush's NSA mass-surveillance programs) on its board of directors, SpiderOak One is a clear choice for those who value privacy. The company also offers Encryptr, a free password vault for helping users keep up with all the long, strong, random passwords they need to protect their privacy.

And, as even the *New York Times* reported recently:

The [CIA] documents indicate that because of encryption, the agency must target an individual phone and then can intercept only the calls and messages that pass through that phone. Instead of casting a net for a big catch, in other words, C.I.A. spies essentially cast a single fishing line at a specific target, and do not try to troll an entire population.

"The difference between wholesale surveillance and targeted surveillance is huge," said Dan Guido, a director at Hack/Secure, a cybersecurity investment firm. "Instead of sifting through a sea of information, they're forced to look at devices one at a time."

The inescapable conclusion is that because of encryption, the surveillance state has been set back to its

pre-9/11 days and ways. Encryption is the key ingredient in any recipe for digital liberty in the age of surveillance. For those who use encrypted devices and communication tools and keep those devices and tools up-to-date, the CIA revelations really serve as little more than an opportunity to encourage others to do the same.

The surveillance state is both a political problem and a technological problem. What is needed is a two-pronged solution. While applying pressure to elected officials at both the state and federal levels to demolish the surveillance state, it is also incumbent upon every concerned citizen to apply the technological solutions to these problems. After all, you are the best guardian of your own privacy.

New American

Written by **C. Mitchell Shaw** on April 17, 2017

Published in the April 17, 2017 issue of the New American magazine. Vol. 33, No. 08