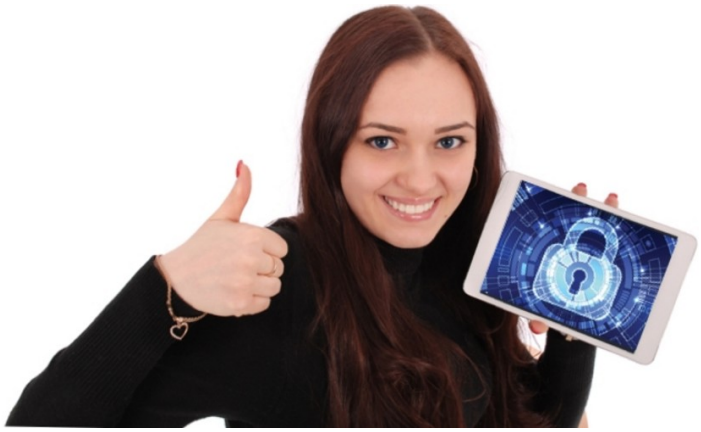
Written by **C. Mitchell Shaw** on March 13, 2017

Good News From CIA Leak: Encryption Works!

The media have spun the recent story about CIA-developed hacking tools by claiming either that there's nothing to worry about, or that the problem is so severe that it is no longer possible to protect our privacy through encryption. In reality, privacy is under attack, but encryption still works.



With WikiLeaks' recent disclosure of the CIA's secret hacking program, many are left wondering how deep the rabbit hole goes. How secure are the devices and softwares that people all over the world use and depend on every day? While the mainstream media have reported on this either as if there is nothing to it or it's the end of both privacy and encryption, the truth is that encryption can still be used effectively to protect privacy.

As *The New American* has reported in previous articles, the tools (read: cyber weapons) developed by the CIA are scarily invasive. Any hacker who is worth his weight in silicon — and who also has access to these tools — has the ability to remotely access and control devices — such as computers, mobile devices, and SmartTVs — to watch and listen to targets, as well as the theoretical (if not actual) ability to hack and control cars and trucks to disable or override steering, brakes, acceleration, and airbag controls. And thanks to the haphazard way the cyber-weapon files and documents were circulated within the CIA and its contractor companies, that could be a lot of hackers.

And despite the pooh-poohing by the intelligence community and many in the mainstream media, recent statements by the CIA and White House, coupled with the FBI's investigation into the source of the leaked CIA documents, serve as admissions that the disclosures are genuine. So regarding both the existence of the cyber weapons and the fact that the CIA lost control of them, it is really is as bad as it looks.

But that is also very good news.

Buried in the CIA documents (and WikiLeaks' analysis of those documents) is the fact that there has been a shift in the way the surveillance state gathers information. In the wake of the Snowden revelations about mass surveillance almost four years ago, many — this writer included — began to implement ways to protect themselves against mass surveillance. 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.

Apple introduced encryption by default for devices running newer versions of iOS; Google followed suit with encryption by default for all devices running newer versions of Android. Millions of people in the United States and worldwide began using encrypted communication applications. The surveillance hawks predicted the end of the world, claiming that terrorists were using those tools to "go dark." The hawks demanded back doors into the encrypted devices and softwares.

Reports of recent revelations about the CIA hacking program focus on the fact that the vulnerabilities exploited by the CIA-developed cyber weapons allow the hackers to compromise the underlying operating systems (such as iOS, Android, Windows, MacOS, Linux, Solaris, and others) to capture the data before it is encrypted. As this writer noted in an earlier article:

> Because the operating systems themselves would be compromised, all software running on those devices would be subject to corruption, as well. This would mean that privacy tools — such as those this writer uses on a regular basis — would be rendered useless. For instance, an application such as Signal — used for encrypting text messages and phone calls on mobile devices — would continue to encrypt the communications, leaving the user feeling secure. But since the keyboard would record (and report) all keystrokes before Signal could encrypt and send the text message, the communication could still be harvested by the hackers. Likewise, since the microphone itself could be activated, it would make no difference that the communication leaving the device would be encrypted; the hackers would still be able to capture the unencrypted voice recordings of both parties.

So, how is that good news? Put simply: it means that encryption works!

The surveillance state has had to change its game. As the *New York Times* reported recently:

> The 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 New American reached out to several companies and organizations involved in promoting digital liberty to ask what the CIA revelations mean for the state of privacy. What we found shows that — for users who are willing to invest the time to keep their systems and programs up-to-date — the CIA hacking tools can be effectively blocked.

Dr. Andy Yen is the CEO and one of the founders of ProtonMail, an open-source, end-to-end encrypted, Zero-Knowledge e-mail service with its servers in Switzerland. Dr. Yen told *The New American* that the CIA revelations are "the biggest intelligence leak since Snowden in 2013 and the documents released so far appear to just be the tip of the iceberg." When asked about the security of ProtonMail running on devices that may have been compromised by hackers (the government or otherwise) exploiting the devices' vulnerabilities, Dr. Yen said, "From what we have seen so far, it is clear that ProtonMail's cryptography is not compromised, so the email privacy of our users is still secure." He added, "We are encouraging users to work to harden their endpoint devices, by actively patching all the software that they run."

Part of that initiative to encourage users to "harden their endpoint devices" came in the form of a

statement ProtonMail released the same day WikiLeaks dumped the CIA documents and files. Part of that statement says:

> 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 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.

In other words, the danger is in running old software, including operating systems that are missing the most recent updates. 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."

That is because outdated operating systems (I'm looking at all of you who are still running Windows XP), software programs, and applications do not have the most up-to-date security patches. All software has vulnerabilities. As those vulnerabilities are discovered, the software developers issue updates to plug those vulnerabilities. Going over the list of the CIA's notes on how to attack different devices, operating systems, and softwares, one common denominator shines through: they all depend on exploiting unpatched vulnerabilities.

In the quote above from one of this writer's previous articles, there is a reference to Signal — an application for encrypted texts and phone calls. The company behind Signal is Open Whisper Systems. Signal has a list of endorsements from people — Ed Snowden, Laura Poitras, Bruce Schneier, and others — who have a real understanding of cryptography and the need for private communications. In a statement to *The New American*, Open Whisper Systems said:

> 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.

There again is the evidence that encryption works for those use it and keep their devices and software up-to-date.

Another open-source, end-to-end encrypted, Zero-Knowledge service is SpiderOak One, which offers an online backup service similar in function to DropBox with the distinction that everything built into SpiderOak One has the users' privacy in mind. 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 (or have any way to know) users' passphrases. In a statement published on its website, SpiderOak 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.

The take-away? Encryption works. At least for those willing to take the time and effort to make sure their endpoint devices (computers, mobile devices, routers, etc) are running up-to-date, reliable, trustworthy operating systems and software (which almost certainly excludes Microsoft Windows).

The answer to the question, "How can someone protect themselves from surveillance?" has not changed. Replace Windows with either Mac or (even better) Linux. Use open-source software and avoid proprietary software as much as you can. Encrypt everything you can, including your hard drive. Encrypt all communications, and encourage others to do the same. It's simple to do with applications such as ProtonMail and Signal. Keep your operating system and other software up-to-date. Don't store anything to an online backup service without first encrypting it — there is no cloud; it's just someone else's computer. And — most importantly — think about privacy and security. Make it a guiding principle in the way you use computers. Any chain is only as strong as its weakest link. The way you use computers — the choices you make, the programs and applications you use, and the ways you use them — are the biggest factors after following the above steps.

As for making a SmartTV secure, the best bet is to get rid of it. Period. The software is proprietary and the thing is designed as a spy tool.

Encryption has changed the game for the surveillance hawks. Now, instead of being able to conduct mass surveillance on scale, they are forced to compromise select and specific endpoint devices. If you are the specific target of a three-letter-agency, there is little you can do to avoid being spied on. For the rest of us, things are actually looking better.