Written by **C. Mitchell Shaw** on March 8, 2017

WikiLeaks: CIA Cyber "Weapons" Are Loose in the Wild

On Tuesday, WikiLeaks released the first part of a "new series of leaks on the U.S. Central Intelligence Agency" which shows the CIA has been secretly building an arsenal of hacking tools and an army of hackers to rival — if not exceed — the hacking capabilities of the NSA. The leaked documents also show that the CIA — in a move reminiscent of the Keystone Kops — "lost control of the majority of its hacking arsenal" allowing it to fall into the hands of hackers who have even less moral constraint than the CIA (if that were possible).

The WikiLeaks disclosures — code-named "Vault 7" by the whistleblower website — "is the largest ever publication of confidential documents on the [CIA]," according to a press release issued by WikiLeaks. In a departure from previous releases — including the infamous CableGate disclosures — which were published *in toto*, WikiLeaks announced that they have:

> decided to redact and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks.

WikiLeaks — which has released millions of documents since its founding more than 10 years ago, and has never been found to publish any fake documents — says these documents and files come from a source who, like others, had access to them because they were handled and circulated in ways that violated the basic chain of custody for such documents.

The source told WikiLeaks that he (or she) was making the documents and files available because there are "policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency." The release of the material is intended to "initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons," according to the statement the source made to WikiLeaks.

In explaining the size and scope of the hacking capabilities of the CIA, the press release says:

> Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.
>
> By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for

> Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.

The first installment of "Vault 7" was released Tuesday and named "Year Zero." That installment contains almost 9,000 documents and files. Those documents show that the CIA created software tools including malware, viruses, trojans, weaponized "zero day" exploits, malware remote-control systems, and associated documentation. Those software tools allow the hacker using them to break into — and control — computers and mobile devices including those running the Android, iOS, Windows, Mac OS X, Linux, Solaris, and other operating systems. Those operating systems account for nearly all computers and mobile devices worldwide.

The tools that the CIA developed depend on certain vulnerabilities, or bugs, found in software and firmware (software embedded into the hardware of electronic devices) in a plethora of consumer electronics made by some of the biggest names in electronics — such as Apple, Microsoft, Google, and others. The documents show that, rather than disclose those vulnerabilities to the manufacturers, the CIA kept them secret and "hoarded" them so that its hackers could continue to use them to gain control over targeted devices.

But, just how much control could be gained?

The documents released by WikiLeaks show that the tools the CIA developed would allow its hackers to remotely activate those devices (including powering them on, if they are turned off) and control the cameras and microphones — turning any device under the hackers' control into surveillance devices to be used at will.

Since the hackers would then have remote access control over any such device, all files and folders would be available to the hacker. Worse yet, having control of the device would also allow the hacker to either remove or add files and folders. If the hacker wanted to bring an adversary down, it would be a simple matter to create a hidden folder containing illegal files — including child pornography — on the victim's device to be "discovered" at a later date by investigators serving a warrant. Such a sting operation would look — for all the world — like a legitimate law-enforcement activity. Even if it did not end in a prosecution and prison, the victim could be branded for life. After all, this is almost exactly what happened to former CBS News correspondent Sharyl Attkisson. In her case, the hidden files that were secretly placed on her computer were classified government documents for which Attkisson could have been charged under the Espionage Act for possessing.

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.

The documents also show that hackers using these tools are able to use "Smart TVs" to listen to and watch the victim of their surveillance via the built-in microphones and cameras. This is a subject *The New American* covered in a previous article, though it was not known then that the CIA had cultivated this ability. Another new twist to this is that the hackers can activate the microphones and cameras even while the TV appears to be turned off.

Since all modern automobiles — to one degree or another — use computers to control everything from emissions to brakes to airbags to steering, the CIA has been looking at ways to develop methods for controlling those systems. While the documents themselves do not specify the potential use of such tools, WikiLeaks points out that they "would permit the CIA to engage in nearly undetectable assassinations." This writer has difficulty imagining any other use the CIA would have for such capabilities.

All of this would be bad enough were these tools only in the hands of an uncountable federal agency which has been shown to be untrustworthy. But it's worse than that. As the press release states:

> Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

As Julian Assange, the founder and editor-in-chief of WikiLeaks, wrote:

> There is an extreme proliferation risk in the development of cyber "weapons." Comparisons can be drawn between the uncontrolled proliferation of such "weapons", which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective.

With these "weapons" now loose in the wild, the press release makes the salient point that their danger has grown exponentially. "Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike," the press release states.

Take a good, long look at the computer or mobile device on which you are reading this article. Given what is now known, can you trust it? Because, if WikiLeaks' analysis of these documents is correct, a hacker in Bangladesh or Tel Aviv could be watching you read this. Or he could be in his mother's basement next door eating Doritos and playing Resident Evil as he uses the weapons the CIA never should have developed in the first place and somehow managed to lose.

The single upside to this is that the "public debate" that will inevitably spring from these disclosures will lead to software manufactures patching the vulnerabilities used by these tools — essentially plugging the holes used to spy on the innocent and the guilty alike.

This is a developing story and *The New American* will continue to cover it and keep our readers informed.