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

The CIA's Hacking Ability

WikiLeaks released thousands of pages of information provided by an informant, showing that the CIA not only developed tools to hack every major electronic device, but lost them.

In the ongoing war on encryption — which is part of a larger war on privacy — waged by the surveillance hawks in government, the stakes have never been higher than now. As the three-letter-agencies and others that work to maintain the surveillance state have run into a blind wall of encryption, they have sought new ways to violate the privacy of the targets of their surveillance.

In the almost four years since Edward Snowden revealed the depth and breadth of the mass surveillance being conducted on American citizens and others by the NSA and other three-letter-agencies, an active battle has been waged between those who would protect privacy and those who would encroach upon it. As the surveillance hawks have vacillated between denying the size and scope of the surveillance on the one hand and demanding backdoors into the encryption used by people to secure their data on the other hand, default encryption has become the standard for devices running the newer versions of both iOS and Android. Millions of people all over the world began to seek out ways to secure their data at rest (files and folders stored on a device) and their data in motion (communications).

As a response to that increased demand, more and more software developers began to offer simple-to-use applications for mobile devices and computers. Those simple-to-use applications provide impenetrable encryption both for storing data and for end-to-end encrypted communications.

The surveillance state responded with both a public relations attack (painting encryption as a "tool of terrorists") and a test case in the courts. In the wake of the terrorist attack in San Bernardino in December 2015, the Department of Justice (a misnomer if ever there was one) took Apple to court in an attempt to force the company to provide a backdoor into the iOS platform — circumventing the encryption protecting those devices. The Justice Department insisted the FBI *claimed* that the backdoor would only be used once, on one phone — the phone used by the San Bernardino shooter, Sayed Farook. Expert after expert showed that there is no such thing as a "one-time-use backdoor" and that once such a technique exists, it could be used as often (and as widely) as those using it desired.

The government's case was nothing more than an attempt to set a precedent. Apple stood firm in its refusal to compromise the encryption of its devices, and — on the brink of a court decision that seemed likely to favor Apple's position — the Justice Department dropped its case. The test case ended with no win for the surveillance state and no precedent set.

In the immediate aftermath of that failure, the surveillance hawks in Congress introduced legislation to require companies offering encrypted devices and applications to create backdoors that would allow government agencies to sidestep the encryption. That legislation also failed. In fact, it never got out of committee. This writer detailed those events in an article for the July 18, 2016 issue of The New American entitled "Government's All-access Pass to Your Privacy." That article can also be found on The New American's website.

Then the other shoe dropped.

On March 7, 2016, WikiLeaks announced the largest publication of confidential documents on the CIA ever made public. The publication of these documents and files — code-named "Vault 7" by WikiLeaks — exposes "the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of 'zero day' weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones," according to a press release by WikiLeaks.

The first part of "Vault 7" is called "Year Zero" and includes nearly 9,000 leaked documents and files detailing the CIA's arsenal of cyberweapons — including "malware, viruses, trojans, weaponized 'zero day' exploits, malware remote control systems and associated documentation" — and the hacker army of "over 5000 registered users" employed by the CIA to use those cyberweapons to compromise computers, mobile devices, SmartTVs, and automobiles. As the press release explains:

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.

In a statement to WikiLeaks the source details 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 source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.

In a subsequent press release, issued March 23, 2016, WikiLeaks published more information about the CIA's hacking program. That new information — code-named "Dark Matter" — shows that the CIA has also developed "tools" and "methods" for installing malware directly into the firmware embedded in the hardware of Mac laptops. Since these are "firmware" hacks, the surveillance weapons would remain on the devices even if the hard drive were formatted (or replaced) and the operating system reinstalled (or replaced).

The leaked information also shows that — after developing the cyberweapons — the CIA hackers

handled them in ways that violate the most basic chain of custody. As a direct result of that, the WikiLeaks press release says, "Recently, the CIA lost control of the majority of its hacking arsenal."

The inescapable conclusion of the CIA losing control of its cyberweapons is that they are now likely in the hands of others — both hostile nation-states and individuals — with even less restraint than the CIA, if that were possible. If those weapons — instead of being bits and bytes, lines of computer code — were guns and bombs, the result would be the same. And to put in the for-what-it's-worth column, this is at least as bad as that, because computer code is far easier to duplicate and modify than physical weapons. As WikiLeaks put it:

Cyber 'weapons' are not possible to keep under effective control.

While nuclear proliferation has been restrained by the enormous costs and visible infrastructure involved in assembling enough fissile material to produce a critical nuclear mass, cyber 'weapons', once developed, are very hard to retain.

Cyber 'weapons' are in fact just computer programs which can be pirated like any other. Since they are entirely comprised of information they can be copied quickly with no marginal cost.

Securing such 'weapons' is particularly difficult since the same people who develop and use them have the skills to exfiltrate copies without leaving traces — sometimes by using the very same 'weapons' against the organizations that contain them. There are substantial price incentives for government hackers and consultants to obtain copies since there is a global "vulnerability market" that will pay hundreds of thousands to millions of dollars for copies of such 'weapons'. Similarly, contractors and companies who obtain such 'weapons' sometimes use them for their own purposes, obtaining advantage over their competitors in selling 'hacking' services.

Also, "Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by peer states, cyber mafia and teenage hackers alike."

The documents and files were leaked to WikiLeaks by an unknown source who had access to them because of the haphazard way in which they were circulated within the CIA and its contractor companies. Due to the dangerous nature of the cyberweapons and instructions for their use included in the leak, and not wanting to be guilty of the further spread of the cyberweapons, WikiLeaks made a surprising decision: For perhaps the first time in its decade-long history, WikiLeaks redacted the information before publishing it.

As the press release explains:

Wikileaks has also 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.

Given that WikiLeaks considered the documents and files so dangerous as to cause the whistleblower website to depart from its policy of "release without redaction," what exactly are those cyberweapons capable of?

The "Year Zero" disclosures show that the CIA's hacking weapons allow hackers to exploit

vulnerabilities found in the 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. By exploiting those vulnerabilities (or "bugs"), a hacker using the CIA's "tools" could break in to — and control — computers and mobile devices including those running Windows, Mac, Linux, Solaris, Android, iOS, and other operating systems. Those operating systems account for nearly all computers and mobile devices worldwide.

But just how much control could the hacker gain over those devices? In short, total control.

The leaked documents show that the CIA has developed techniques to remotely activate a wide range of devices (including powering them on, if they are turned off) and control the cameras and microphones — turning them into surveillance devices that allow the hacker to both listen to and watch the victim of the surveillance.

The implications of remote control access are staggering and go far beyond the ability to watch and listen (as bad as that is). Having control over the device would also mean the hacker could access all files and folders on the device. This would not only mean that the hackers could *view* those files and folders, it would mean they could *add and delete* at will. As this writer said in an online article dated March 8, 2016:

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.

If that seems far-fetched, there is a well-documented case where this is almost exactly what happened. In 2012, CBS News correspondent Sharyl Attkisson was working on an exposé of the Obama administration regarding the Benghazi scandal. Her computer — an iMac — began making a loud noise as the fan ran at full speed, indicating that the processor was overheating. That is odd behavior for an Apple product, even more so because the same thing had happened a few days earlier to the Toshiba laptop issued to her by CBS News.

Attkisson took her computer to an expert. That expert, described by Attkisson as a "confidential source inside the government," discovered on her computer a piece of "commercial, nonattributable spyware that's proprietary to a government agency: either the CIA, FBI, the Defense Intelligence Agency, or the National Security Agency (NSA)." Not only that, but buried in the system files of her operating system (where she would be almost certain never to look) — there were three classified government documents. Attkisson could have been charged under the Espionage Act for possessing those documents. In her book *Stonewalled: My Fight for Truth Against the Forces of Obstruction, Intimidation, and Harassment in Obama's Washington* Attkisson asks rhetorically, "Why? To frame me?"

Attkisson's claims — far from being mere he-said/she-said — are well-substantiated. She points out in her book that both CBS News and Don Allison, a security specialist at Kore Logic, confirmed the presence of the government spyware on her computer. In fact, after describing an episode of watching "data in my computer file … wiping at hyperspeed before my very eyes," she says in her book:

While a great deal of data has been expertly wiped in an attempt to cover-up the deed, Don [Allison] is able to find remnants of what was once there. There's key evidence of a government computer

connection to my computer. A sort of backdoor link that leads to an ISP address for a government computer that can't be accessed by the general public on the Web. It's an undeniable link to the U.S. government.

As she recounts, Allison explained, "This ISP address is better evidence of the government being in your computer than the government had when it accused China of hacking into computers in the U.S."

So just how did the government gain that degree of control over Attkisson's computers? For that matter, how do hackers (both government and non-government) ever gain control over *any* device? The WikiLeaks disclosures of the CIA's hacking program go a long way toward answering those questions.

All software has the potential for vulnerabilities. As stated above, the arsenal of cyberweapons developed by the CIA includes malware, viruses, trojans, malware remote-control systems, and weaponized "zero day" exploits. "Zero day" exploits refer to those vulnerabilities that hackers discover but are not known to the manufacturer of the hardware or software — therefore the developer has "zero days" to patch the vulnerabilities before they are used as exploits. By exploiting these vulnerabilities, hackers at the CIA developed ways to penetrate the systems running the vulnerable software and firmware to gain control over a variety of devices, including computers running almost all operating systems; "smart" mobile devices such as iPhones, iPads, and phones and tablets running Android; SmartTVs; and automobiles. (For information on the potential uses for "hacked" cars and trucks, see "WikiLeaks: CIA May Be Hacking Cars to Murder People.")

Since the CIA's hackers require unpatched vulnerabilities to penetrate systems and devices, the CIA routinely "hoarded" those vulnerabilities by discovering them but not reporting them to the hardware and software manufacturers. While this may seem to make sense in the darkened recesses of the minds of the CIA's hacking army, the reality is that by leaving those vulnerabilities unpatched, the CIA allowed a situation that threatened the security of the very people it is sworn to protect. (For information on steps you can take to protect yourself against hackers — both government and non-government, see my article "Foiling Foul Hackers.")

The documents and files in the "Year Zero" publication show that the CIA developed hacking tools specifically geared toward Microsoft Windows (which, considering the essential spyware nature of Windows, could not have been very difficult). Since Windows maintains the dominant share of the operating system market for end users, the CIA's decision to focus much of its attention there makes logistical sense. But the hacking army did not limit its arsenal of cyberweapons to only those geared toward Windows. Hacking tools were also developed to exploit vulnerabilities found in other operating systems.

A sampling of some of the programs developed by the CIA shows just how invasive these weapons can be:

• UMBRAGE is a suite of cyberweapons that includes keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance, and survey techniques.

• Fine Dining is a "menu" that CIA case officers fill out to request the tools they need to accomplish "exfiltrating" information from computer systems.

• Improvise (JQJIMPROVISE) is "a toolset for configuration, post-processing, payload setup and

execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor). Its configuration utilities such as Margarita allow the NOC (Network Operation Center) to customize tools based on requirements from 'Fine Dining' questionnaires."

• HIVE is "a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants."

• Weeping Angel is a toolset that infests smart TVs, transforming them into covert microphones. It has a "Fake-Off mode" that allows hackers to "suppress LEDs" to fool the owner of the SmartTV into believing the device is turned off, when — in reality — it is watching (via the built-in camera) and listening (via the built-in microphone).

Even the names of these weapons are very telling. If the CIA hackers believed they were doing honorable and praiseworthy work, one would expect them to name their "tools" after virtuous things. Instead, these tools are often named after evil things — albeit based on science-fiction characters. For instance, the program "HIVE" seems to be named after a character from the television series *Marvel's Agents of S.H.I.E.L.D*. The character is an evil alien hybrid who wants to take over the world. He attempts to do so by infecting those with whom he comes into contact with a virus that brings them both under his control and into a single consciousness with him. Similarly, the program "Weeping Angel" is named after a race of malicious predatory creatures from the British television series *Doctor Who*. The Weeping Angels in *Doctor Who* are creatures who appear to be stone statues as long as they are being watched. Once their victim looks away, the Weeping Angels begin moving and doing their evil deeds.

The hacking tools in these programs — as seen in the sample list above — allow the hackers to take complete control over the target devices. It is as if the hackers are sitting at the keyboard, looking at the monitor. Worse, because the control happens surreptitiously, the owner or user of the device has no idea he or she is being watched, listened to, and otherwise spied upon.

For mobile devices, the news is perhaps even worse. Many have long known that mobile devices are the most difficult of electronics to lock down to a level of good security. This is because the very nature of smartphones depends on them always having a connection to mobile towers for both voice and data connectivity. Coupled with the GPS capabilities of the devices and the presence of built-in cameras (front-facing and rear-facing) and other sensors to detect a long list of environmental variables, this makes for an electronic device that seems designed to report on your location and activity. Any vulnerability in the system that can be exploited instantly turns such a device into a surveillance tool that is turned on its owner.

As the WikiLeaks press report states:

CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA.…

The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert

operations world-wide.

As part of that initiative, the "CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone," according to WikiLeaks' analysis in the press report.

Keep in mind that — in the more than 10 years it has been exposing the corruption and illegality of governments and organizations around the world — WikiLeaks has never been shown to have published any documents that have later been proved to be false. But in this instance, is the anti-secrecy website exaggerating in its analysis? Even just a little? No.

As this writer reported in an online article dated March 9, 2017:

The CIA documents published [March 7] contain more than 70 separate links, which account for hundreds of pages on methods developed by the MDB to exploit iPhones and another 47 links (and hundreds more pages) on Android. Since iPhone and Android make up nearly 100 percent of the smartphone market, with Android at nearly 85 percent, these exploits would affect billions of users world-wide. In fact, more than one billion Android devices were sold last year alone.

The tools (read: weapons) the CIA developed allow hackers to hack iPhones, iPads, and Android phones and tablets to defeat the device encryption — including encrypted communications — and in some cases remotely activate cameras and microphones, remotely activate location services (even if the user has disabled them), remotely access files and folders on the devices (and copy, remove, or add files and folders, and other things).

For its part, the CIA has — as per usual — addressed these leaks from both sides of its mouth. In a statement released almost immediately after the leaked material was published by WikiLeaks, the CIA said that the agency has "no comment on the authenticity of purported intelligence documents released by Wikileaks or on the status of any investigation into the source of the documents." The statement then went on to defend the agency's efforts to "aggressively collect foreign intelligence overseas to protect America from terrorists, hostile nation states and other adversaries." While neither explicitly confirming nor denying the validity of the "purported" documents and files, the statement condemns WikiLeaks' disclosure of the information, saying that it is "designed to damage the Intelligence Community's ability to protect America against terrorists and other adversaries." The statement added, "Such disclosures not only jeopardize U.S. personnel and operations, but also equip our adversaries with tools and information to do us harm."

Of course, if — as the CIA would have the American people believe — the authenticity of the leaked documents and files is questionable, then its publication could not possibly "jeopardize U.S. personnel and operations" or "equip our adversaries with tools and information to do us harm." Added to that is the fact that the FBI is investigating the leak to determine "who had access to the information," according to a report from the *New York Times*, which went on to say that the list could "include at least a few hundred people, and possibly more than a thousand." This is as good as an admission that the materials published by WikiLeaks are genuine. After all, if the leak is not genuine, what is there to investigate?

So, the CIA — in possible violation (or at least in excess) of its mandated powers — created a secret army of hackers equipped with an equally secretive arsenal of cyberweapons to hack into a wide range

of devices for the purpose of spying on the people using those devices. And while the CIA claims that it never uses its investigative tools on American citizens living in the United States, it is important to remember that the agency doesn't exactly have a stellar reputation for being truthful. And even in the off-chance that the CIA's claim about not spying on American citizens living stateside is true, it is also irrelevant because the cyberweapons developed by the agency were allowed — by ineptitude — to get loose in the world. Consequently, those weapons are right now likely in the hands of other nation-states and teenage hackers. They are certainly in the hands of the NSA, FBI, and other American spy agencies that don't even pretend to have the CIA's "restrictions" on spying on Americans living in the land of the "free" and the home of the brave.

This article is an example of the exclusive content that's available by subscribing to our print magazine.

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