New American

Written by **C. Mitchell Shaw** on March 10, 2017

CIA "Weapons" Let Hackers Use Your Computer, Phone, & TV to Spy on You

With the WikiLeaks disclosures Tuesday about the hacking capabilities of the CIA, it is now known that the agency can hack at least on par with the NSA and with even less accountability. One element of that is the ability to remotely access devices — such as computers, mobile devices, and televisions — to watch and listen to targets. Of course, since the CIA has lost control over its hacking tools, others now have that same ability.

As *The New American* reported Wednesday:

> On Tuesday, WikiLeaks released the first part of a "new series of leaks on the U.S. Central Intelligence Agency" that 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 arsenal of cyber "weapons" 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 mobile devices such as iPhones, iPads, and Android phones and tablets, SmartTVs, and computers running Windows, Mac, Linux, Solaris, and other operating systems.

Once the hackers have control of those devices, they can remotely activate the cameras and microphones, turning the devices into surveillance apparatus owned and operated by the subjects (read: victims) of the surveillance — all without any indication to the owners of the devices that they were being watched and listened to. No light. No indicators. Pure, surreptitious surveillance.

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, 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 which is turned on its owner.

The secret (and apparently *unauthorized*) CIA hacking program found and exploited those vulnerabilities. As the WikiLeaks press release Tuesday explained:

> 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 (see this organizational chart of the CIA for more details).
>
> 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. But is WikiLeaks guilty of overstating the case?

No.

The CIA documents published Tuesday 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 computers, the CIA developed tools for Microsoft Windows (which could not have been that difficult, considering that Windows 10 is essentially spyware) and other operating systems. Since Windows (even in the wake of the fiasco of Windows 10) maintains the dominant share of the computer market for end users, the CIA focused most of its hacking attention on that family of operating systems. But it also developed programs with names such as:

• UMBRAGE — which includes keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques;

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

• Improvise (JQJIMPROVISE) — which 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' questionairies"; and

• HIVE — which 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."

Since some of these tools also affect, to varying degrees, operating systems such as Mac, Linux, and Solaris, those — such as this writer — who have said goodbye to Microsoft still need to be aware that nothing is ever completely outside the reach of an uncountable federal agency with an agenda and a budget steeped in secrecy.

Perhaps the most invasive devices in the lives of many are those that fall into the category known as the Internet-of-Things (IoT), such as smartwatches, Internet-connected appliances, and SmartTVs. The CIA did not overlook the fact that (in fulfillment of the predictions found in *1984* and *Fahrenheit 451*) millions of consumers now purchase televisions that are not only Internet-connected, but also have cameras and microphones. This was a spy tool made-to order and the CIA's Embedded Development Branch (EDB) made sure not to let it go to waste. The press release from WikiLeaks says, "The attack against Samsung smart TVs was developed in cooperation with the United Kingdom's MI5/BTSS." One tool, known by the codename "Weeping Angel" after a race of malicious predatory creatures from the British television series *Doctor Who* (which serves to demonstrate the mindset of the people who create such tools), allows hackers to activate a "Fake-Off mode" on those televisions, fooling the user to believe the device is powered off. The first page from the CIA documents on "Weeping Angel" says it allows the hacker to "Suppress LEDs to improve look of Fake-Off mode" and "prevent updates" from being downloaded and installed on the SmartTV to prevent a security patch from removing the vulnerabilities the hackers use to activate the device remotely. After all, having a power light on would be a dead give-away and installing updates from the device manufacturer could mean the CIA's effort would be back at square one.

To that end, in the wake of these disclosures, this writer wrote Wednesday that:

> 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.

Now, *USA Today* is reporting that:

> [WikiLeaks Founder and Editor Julian] Assange said that some tech firms have reached out seeking more details about the CIA tools. He said WikiLeaks hasn't published the details because it doesn't want "journalists and people of the world, our sources, being hacked using these weapons." The best way to avoid that, he said, is to give companies such as Apple, Google and Samsung access first.
>
> "We have decided to work with them, to give them some exclusive access to some of the technical details we have, so that fixes can be pushed out," Assange said.

So, those patches are hopefully coming and the CIA (along with other hackers who now have access to the tools which never should have been created) will have to start all over.

While the CIA claims that it never uses its investigative tools on American citizens in the United States, one is reminded that the agency doesn't exactly have a stellar reputation for being truthful. Besides, how many terrorist camps in the Middle East have SmartTVs to watch their favorite programs on? The reality is that these tools are designed to penetrate the very types of devices used by ordinary citizens in Western countries.

The Third Amendment to the U.S. Constitution guarantees that "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." The reasons for this prohibition on government intrusion are numerous, but not the

least is that England had placed soldiers in the homes of American subjects to keep them under control by the surveillance that was a necessary part of their presence. The modern, digital equivalent of that is installing software on a citizen's electronic devices — without his consent — to accomplish the same end.

While the manufactures of the software and hardware affected by these cyber "weapons" work to patch those vulnerabilities, Congress should immediately investigate this crime against privacy and liberty.