The Real Lesson of the WikiLeaks Vault 7 Document Dump

by Sharon D. Nelson Esq. and John W. Simek

Some days are just more interesting than others. You could almost hear the mournful wailing of spooks (the CIA kind) as WikiLeaks released thousands of documents describing sophisticated software tools used by the Central Intelligence Agency to break into smartphones, computers and even Internet-connected televisions.

The New York Times reported that the documents, at first review, appeared to be authentic. The initial release, which WikiLeaks said was only the first part of the document collection, included 7,818 web pages with 943 attachments. The entire archive of CIA material consists of several hundred million lines of computer code according to WikiLeaks.

Initial reports overstated what the technology could do, suggesting that the encryption for popular apps such as Signal and WhatsApp had been compromised. As the details become more clear, it was noted that the apps themselves were NOT compromised. Rather, if the phone was compromised, by malware for example, encryption doesn't do you any good since the app has to decrypt the message for you to read it, thus allowing a successful attacker to read it. The real news was that both Androids and iPhones have allegedly been compromised by the CIA and allied intelligence services, meaning that apps such as Signal and WhatsApp cannot protect your privacy.

The source of the documents was not named. WikiLeaks said the documents, which it called Vault 7 (where DO they come up with these monikers?), had 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."

WikiLeaks said the source, in a statement, set out policy questions that "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, the group said, "wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons."

The documents are dated from 2013 to 2016. WikiLeaks, which has sometimes been accused of recklessly leaking information that could do harm, said it had redacted names and other identifying information from the collection. It said it was not releasing the computer code for actual, usable cyberweapons "until a consensus emerges on the technical and political nature of the C.I.A.'s program and how such 'weapons' should be analyzed, disarmed and published."

One revelation is about a program called Weeping Angel which uses Samsung "smart" televisions as covert listening devices. According to the WikiLeaks news release, even when it appears to be turned off, the television "operates as a bug, recording conversations in the room and sending them over the internet to a covert C.I.A. server." We had previously speculated that this might be true but take no pleasure in being right. As it turns out, CNET reported that the hack only works on certain versions of firmware and you have to have physical access to the TV.

Another program described in the documents, named Umbrage, is a voluminous library of cyberattack techniques that the CIA has collected from malware produced by other countries, including Russia. According to the WikiLeaks release, the large number of techniques allows the CIA to mask the origin of some of its cyberattacks and confuse forensic investigators. This is another great fear of ours. If we are under a cyberattack, how do we respond with assurance that we have traced the attack back to its true source? And God help us if we have autonomous machines with AI helpfully doing all these investigations for us. We truly "ride the lightning" in the cyberwarfare era.

Despite all the reports of the CIA's hacking ability, the real message is to make sure your devices have the most recent versions of firmware and software. In other words, update, update, update. So far, all of the reported vulnerabilities have been patched by the vendors. In fact, Apple, Google and Microsoft have said that their products are already safe from most of the tools identified in the WikiLeaks documents. An ironic outcome of the WikiLeaks dump has China very concerned that the United States has the ability to hack into devices made by Chinese companies. The WikiLeaks documents mentioned that network routers manufactured by Chinese firms Huawei and ZTE could be hacked using the CIA tools. Chinese Foreign Ministry spokesman Geng Shuangsaid said, "We urge the U.S. side to stop listening in, monitoring, stealing secrets and internet hacking against China and other countries." Apparently, what's good for the goose isn't good for the gander.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com