The Intercept_

WIKILEAKS FILES SHOW THE CIA REPURPOSING HACKING CODE TO SAVE TIME, NOT TO FRAME RUSSIA

Kim Zetter

March 8 2017, 2:28 p.m.

IN HONOR OF THOSE MEMBERS
OF THE CENTRAL INTELLIGENCE AGENCY
WHO GAVE THEIR LIVES IN THE SERVICE OF THEIR COUNTRY
UNITED STATES
AMERICA

Photo: Martin H. Simon/Press Pool/Getty Images

Attributing hacking attacks to the correct perpetrators is notoriously difficult. Even the U.S. government, for all its technical resources and expertise, took warranted criticism for trying to pin a high-profile 2014 cyberattack on North Korea, and more recently faced skepticism when it blamed Russia for hacks against top Democrats during the 2016 election.

In those cases, government officials said they based their attribution in part on software tools the hackers employed, which had been used in other cyberattacks linked to North Korea and Russia. But that sort of evidence is not conclusive; hackers have been known to intentionally use or leave behind software and other distinctive material linked to other groups as part of so-called false flag operations intended to falsely implicate other parties. Researchers at Russian digital security firm Kaspersky Lab have documented such cases.

On Tuesday, Wikileaks published a large cache of CIA documents that it said showed the agency had equipped itself to run its own false-flag hacking operations. The documents describe an internal CIA group called UMBRAGE that Wikileaks said was stealing the techniques of other nation-state hackers to trick forensic investigators into falsely attributing CIA attacks to those actors. According to Wikileaks, among those from whom the CIA has stolen techniques is the Russian Federation, suggesting the CIA is conducting attacks to intentionally mislead investigators into attributing them to Vladimir Putin.

“With UMBRAGE and related projects, the CIA can not only increase its total number of attack types, but also misdirect attribution by leaving behind the ‘fingerprints’ of the groups that the attack techniques were stolen from,” Wikileaks writes in a summary of its CIA document dump

It’s a claim that seems intended to shed doubt on the U.S. government’s attribution of Russia in the DNC hack; the Russian Federation was the only nation specifically named by Wikileaks as a potential victim of misdirected attribution. It’s also a claim that some media outlets have accepted and repeated without question.

"WikiLeaks said there's an entire department within the CIA whose job it is to 'misdirect attribution by leaving behind the fingerprints' of others, such as hackers in Russia," CNN reported without caveats.

It would be possible to leave such fingerprints if the CIA were re-using unique source code written by other actors to intentionally implicate them in CIA hacks, but the published CIA documents don't say this. Instead they indicate the UMBRAGE group is doing something much less nefarious.

They say UMBRAGE is borrowing hacking "techniques" developed or used by other actors to use in CIA hacking projects. This is intended to save the CIA time and energy by copying methods already proven successful. If the CIA were actually re-using source code unique to a specific hacking group this could lead forensic investigators to mis-attribute CIA attacks to the original creators of the code. But the documents appear to say the UMBRAGE group is writing snippets of code that mimic the functionality of other hacking tools and placing it in a library for CIA developers to draw on when designing custom CIA tools.

"The goal of this repository is to provide functional code snippets that can be rapidly combined into custom solutions," notes a document in the cache that discusses the project. "Rather than building feature-rich tools, which are often costly and can have significant CI value, this effort focuses on developing smaller and more targeted solutions built to operational specifications."

Robert Graham, CEO of Errata Security, agrees that the CIA documents are not talking about framing Russia or other nations.

"What we can conclusively say from the evidence in the documents is that they're creating snippets of code for use in other projects and they're reusing methods in code that they find on the internet," he told The Intercept. "Elsewhere they talk about obscuring attacks so you can't see where it's coming from, but there's no concrete plan to do a false flag operation. They're not trying to say 'We're going to make this look like Russia'."

The UMBRAGE documents do mention looking at source code, but these reference widely available source code for popular tools, not source code unique to, say, Russian Federation hackers. And the purpose of examining the source code seems to be for purposes of inspiring the CIA code developers in developing their code, not so they can copy/paste it into CIA tools.

It's not unusual for attackers of all persuasion — nation-state and criminal — to copy the techniques of other hackers. Success breeds success. A month after Stuxnet was discovered in June 2010, someone created a copycat exploit to attack the same Windows vulnerability Stuxnet exploited.

Components the UMBRAGE project has borrowed from include keyloggers; tools for capturing passwords and webcam imagery; data-destruction tools; components for gaining escalated privileges on a machine and maintaining stealth and persistent presence; and tools for bypassing anti-virus detection.

Some of the techniques UMBRAGE has borrowed come from commercially available tools. The documents mention Dark Comet, a well-known remote access trojan, or RAT, that can capture screenshots and keystrokes and grab webcam imagery, among other things. The French programmer who created Dark Comet stopped distributing it after stories emerged that the Syrian government was using it to spy on dissidents. Another tool UMBRAGE highlights is RawDisk, a tool made by the commercial software company Eldos, which contains drivers that system administrators can use to securely delete information from hard drives.

But legitimate tools are often used by hackers for illegitimate purposes, and RawDisk is no different. It played a starring role in the Sony hack in 2014, where the attackers used it to wipe data from Sony's servers.

It was partly the use of RawDisk that led forensic investigators to attribute the Sony hack to North Korea. That's because RawDisk had been previously used in 2011 "Dark Seoul" hack attacks that wiped the hard drives and master boot records of three banks and two media companies in South Korea. South Korea blamed the attack on North Korea and China. But RawDisk was also used in the destructive Shamoon attack in 2012 that wiped data from 30,000 systems at Saudi Aramco. That attack wasn't attributed to North Korea, however; instead U.S. officials attributed it to Iran.

All of this highlights how murky attribution can be, particularly when focused only on the tools or techniques a group uses, and how the CIA is not doing anything different than other groups in borrowing tools and techniques.

"Everything they're referencing [in the CIA documents] is extremely public code, which means the Russians are grabbing the same snippets and the Chinese are grabbing them and the U.S. is grabbing," says Graham. "So they're all grabbing the same snippets of code and then they're making their changes to it."

The CIA documents do talk elsewhere about using techniques to thwart forensic investigators and make it hard to attribute attacks and tools to the CIA. But the methods discussed are simply proper operational security techniques that any nation-state attackers would be expected to use in covert operations they don't want attributed to them. The Intercept wasn't able to find documents within the WikiLeaks cache that talk about tricking forensic investigators into attributing attacks to Russia. Instead they discuss do's and don'ts of tradecraft, such as encrypting strings and configuration data in malware to prevent someone from reverse engineering the code, or removing file compilation timestamps to prevent investigators from making correlations between compilation times and the working hours of CIA hackers in the U.S.

Researchers at anti-virus firms often use compilation times to determine where a malware's creators might be located geographically if their files are consistently compiled during work hours that are distinctive to a region. For example, tools believed to have been created in Israel have shown compilation times on Sunday, which is a normal workday in Israel.

The bottom line with the CIA data dump released by Wikileaks is that journalists and others should take care to examine statements made around them to ensure that they're reporting accurately on the contents.

Top photo: Shadows are cast on the wall at the Central Intelligence Agency (CIA) headquarters in Langley, Va., in 2011.

RELATED

WikiLeaks Dump Shows CIA Could Turn Smart TVs into Listening Devices

The CIA Didn't Break Signal or WhatsApp, Despite What You've Heard

CIA Has an "Impressive List" of Ways to Hack Into Your Smartphone, WikiLeaks Files Indicate

Intercepted Podcast: Ready to Lie