Written by **C. Mitchell Shaw** on May 7, 2017

WikiLeaks Exposes CIA's "Archimedes" Hacking Weapon

The latest release from WikiLeaks on the CIA's hacking program — published Friday — reveals a tool CIA hackers use to attack a computer that is part of a Local Area Network (LAN). LANs are usually used to tie all of the computers in an office into a single network for the purposes of sharing resources including those used for security. This newly revealed CIA tool — codenamed Archimedes — turns the strength of a LAN against itself by leveraging any compromised computers against all others on the network.

As the WikiLeaks press release explains:

> Today, May 5th 2017, WikiLeaks publishes "Archimedes," a tool used by the CIA to attack a computer inside a Local Area Network (LAN), usually used in offices. It allows the re-directing of traffic from the target computer inside the LAN through a computer infected with this malware and controlled by the CIA. This technique is used by the CIA to redirect the target's computers web browser to an exploitation server while appearing as a normal browsing session.
>
> The document illustrates a type of attack within a "protected environment" as the the tool is deployed into an existing local network abusing existing machines to bring targeted computers under control and allowing further exploitation and abuse.

Archimedes dates back to at least June 2011 when it was known as Fulcrum and was already in version 0.6. The most up-to-date version of the cyberweapon listed in WikiLeaks' Wednesday publication was Archimedes 1.3 dated January 13, 2014. Like many of the other hacking tools exposed in previous publications, it is not know whether Archimedes is still being developed or used.

Archimedes works as a weapon for launching a man-in-the-middle attack. It essentially allows a CIA-controlled computer (the man in the middle) to park itself between two computers and intercept all communications between them.

In a typical man-in-the-middle attack, computer A sends a data packet (which could be anything from a file to an e-mail to a VoIP telephone call) to computer B. The man-in-the-middle intercepts the data packet and relays it on to computer B, keeping a copy of the data packet in the process. The process is repeated for all packets back and forth. It is possible — even fairly common — for the packets (especially software downloads) to be altered or replaced by a man in the middle. When that happens, the file a user thinks he downloaded is easily replace by a download that is corrupted, allowing even further disintegration of security and privacy in the form of greater attacks.

Archimedes has a weakness, though. It is unable to launch a full, two-way man-in-the-middle attack. As the manual for Fulcrum/Archimedes — which is part of the WikiLeaks publication — explains:

> ARP Spoofing is a technique used on a LAN to allow an attacker's machine to intercept data frames from peer machines that were intended for other destinations. This places the attacker's machine

> in the middle of any traffic from the target's machine to any other destination and is known more commonly as the maninthemiddle. ARP Spoofing compromises the targets machine's translation of IPv4 addresses into MAC addresses by sending spoofed ARP packets which associate the attacker's MAC address with IP address of another host (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead.
>
> Fulcrum uses ARP spoofing to get in the middle of the target machine and the default gateway on the LAN so that it can monitor all traffic leaving the target machine. It is important to note that Fulcrum only establishes itself in the middle on one side of the twoway communication channel between the target machine and the default gateway. Once Fulcrum is in the middle, it forwards all requests from the target machine to the real gateway.

So, Archimedes is designed as a cyber-espionage tool and does not appear to be able to be used for cyber-sabotage, though the CIA may have other tools for accomplishing that.

In keeping with its policy in the other CIA hacking leaks, WikiLeaks has published the documents that accompanied Archimedes, but has not published the software itself. As WikiLeaks founder and public face, Julian Assange, wrote in the press release for his organization's first leak about the CIA's hacking program:

> Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published.
>
> 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.

This is a departure from the anti-secrecy website's usual policy of publishing government documents *in toto* — as was done in the infamous CableGate disclosures. Given the extreme danger of these tools, the decision to redact and anonymize makes sense. Otherwise, WikiLeaks could be guilty by journalistic zeal of what the CIA is guilty of by ineptitude: the dissemination of cyberweapons.

Because, as this writer reported in a previous article, the CIA built an arsenal of cyberweapons — of which Archimedes is only a part — to equip an army of CIA hackers and then allowed the code to get loose in the wild:

> 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.

So, while WikiLeaks' decision to redact and anonymize files and data makes sense, the CIA has already ensured that any hacker — whether state-sponsored or teen-aged — can have access to Archimedes along with all the CIA's other weapons simply by downloading them from the Internet.

As WikiLeaks continues to expose the CIA as the unaccountable agency it is, more and more of the agency's actions — which are certainly immoral and unethical and likely illegal — are coming to light. Given what is already known, is there a single good reason not to dissolve the agency?