Longhorn Cyber-Espionage Group Is Actually the CIA

bleepingcomputer.com/news/security/longhorn-cyber-espionage-group-is-actually-the-cia/

Catalin Cimpanu

By
Catalin Cimpanu

- April 10, 2017
- 02:07 PM
- 0

Security researchers from Symantec have tied the CIA hacking tools leaked by WikiLeaks last month to a cyber-espionage group responsible for at least 40 hacks in 16 countries.

The group's activity came to light in 2014, when security researchers from Symantec first identified attacks from a common actor that appeared to have the backing of a North American nation.

Symantec named the group Longhorn, while Kaspersky tracked its activity under the name of Lamberts.

Vault 7 dump helped reveal group's identity

After WikiLeaks dumped Vault 7, a collection of documents allegedly stolen from the CIA, Symantec experts started going through those files, which were mostly wiki pages and manuals for all sorts of hacking tools.

WikiLeaks claimed the files belonged to the CIA, saying hackers and contractors provided the data. Following the leak, the US Department of Justice refused to admit some of the files in a US case, saying they're classified material, and inadvertently confirming their validity, even if the CIA never publicly acknowledging the leak.

Many clues support Symantec's findings

Now, following an analysis of the WikiLeaks Vault 7 documents, US cyber-security firm Symantec is sure the documents describe the modus operandi and some of the tools of the Longhorn cyber-espionage group, which they first discovered in 2014, and tracked its activity back to 2007.

The tools used by Longhorn closely follow development timelines and technical specifications laid out in documents disclosed by WikiLeaks. The Longhorn group shares some of the same cryptographic protocols specified in the Vault 7 documents, in addition to following leaked guidelines on tactics to avoid detection. Given the close similarities between the tools and techniques, there can be little doubt that Longhorn's activities and the Vault 7 documents are the work of the same group.

To sustain its conclusions, Symantec details its findings:

A trojan detected by Symantec as Trojan.Corentry has all the features of the Fluxwire tool contained in the Vault 7 dump. The Fluxwire changelog closely matches the timeline when Symantec detected new features in Corentry samples.

Up until 2014, the CIA used GCC to compile Fluxwire samples, and then switched to MSVC, a detail also observed with Corentry samples.

Early Corentry samples contained a reference to the file path for the Fluxwire program database (PDB) file, linking Corentry with Fluxwire.

The CIA Fire and Forget tool, used for the user-mode injection of a payload called Archangel resembles the modus operandi of a trojan Symantec detected as Backdoor.Plexor.

The way the CIA used cryptography for its tools matches how the Longhorn group operated:
- inner cryptography within SSL to prevent man-in-the-middle (MITM) attacks
- key exchange once per connection
- use of AES with a 32-bit key

Other Vault 7 operational manuals describe attack techniques also used by the Longhorn group:
- use of the Real-time Transport Protocol (RTP) as a means of command and control (C&C) communications
- usage of wipe-on-use as standard practice
- in-memory string deobfuscation
- use of a unique deployment-time key for string obfuscation
- use of secure erase protocols involving renaming and overwriting
- usage of a single domain and IP address combination per target for the C&C server

CIA accidentally hacked a computer in the US

According to Symantec, Longhorn malware has been linked to attacks on 40 targets in 16 countries in the Middle East, Europe, Asia, and Africa.

At one point, Longhorn infected a computer in the United States, but the group quickly removed the malware within hours.

While the Vault 7 dump helped Symantec link Longhorn with the CIA, the Shadow Brokers dump from last year helped Kaspersky link the activities of a cyber-espionage group known as the Equation Group, active since the mid-90s, to the CIA.

Related Articles:

White House: Prepare for cryptography-cracking quantum computers

'Hack DHS' bug hunters find 122 security flaws in DHS systems

US issues guidance on North Korean hackers, offers $5M reward

FTC fines Twitter $150M for using 2FA info for targeted advertising

US Senate: Govt’s ransomware fight hindered by limited reporting

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.