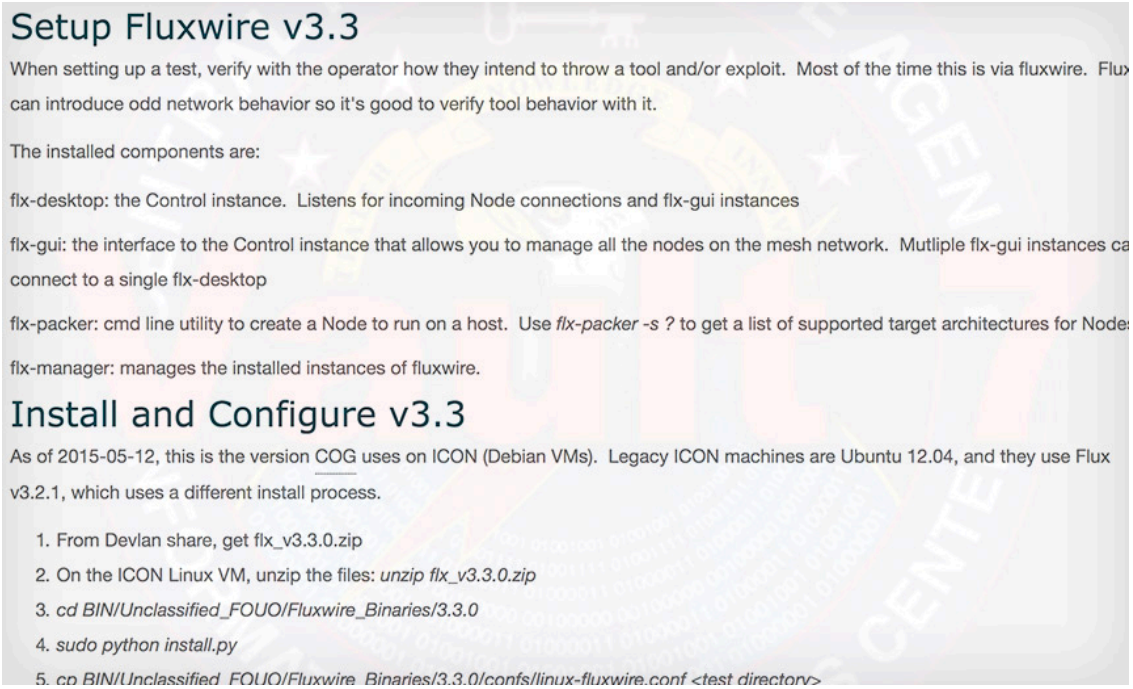
Symantec Links 'Longhorn' Group to CIA Hacking Files

By Jeremy Kirk

Archived: 2026-04-05 20:15:31 UTC

Fraud Management & Cybercrime , Next-Generation Technologies & Secure Development

Researchers Count at Least 40 Longhorn Targets Across 16 Countries (jeremy_kirk) • April 11, 2017



Malware that Symantec calls Corentry appears to correlate with Fluxwire malware described in the Vault 7 release. (Source: WikiLeaks)

Symantec sees a strong correlation between hacking techniques used by a group that it calls Longhorn, and the alleged CIA network exploitation documents released by WikiLeaks.

See Also: How Attackers Use AI to Outsmart Email Filters

Upwards of 40 targets in 16 countries appear to have been attacked by Longhorn, although Mountain View, Calif.-based Symantec did not explicitly say the group was the CIA.

The security firm says it has been blocking attacks for the last three years that it attributes to Longhorn.

"The tools used by Longhorn closely follow development timelines and technical specifications laid out in documents disclosed by WikiLeaks," security researchers at Symantec write in a blog post. "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."

Since March 7, WikiLeaks has released four batches of files from the agency, as part of a leak it calls Vault 7. The CIA hasn't confirmed the veracity of the documents. But agency spokeswoman Heather Fritz Horniak has told Reuters that the disclosures from WikiLeaks "not only jeopardize U.S. personnel and operations, but also equip our adversaries with tools and information to do us harm."

Horniak added: "It is important to note that CIA is legally prohibited from conducting electronic surveillance targeting individuals here at home, including our fellow Americans, and CIA does not do so."

WikiLeaks has claimed that the files previously circulated amongst government contractors and were leaked by someone concerned with U.S. government policies relating to software vulnerabilities.

Vault 7 differs significantly from the broader information that former National Security Agency contractor Edward Snowden passed to several media outlets in 2013. The CIA documents describe software flaws and network exploitation techniques in detail. The CIA leaks startled the intelligence community due to the strong possibility of yet another insider security breach.

SCOOBYSNACKs, Anyone?

From the start, Symantec suspected Longhorn was an outlier, saying it appeared to be different from other potential cybercrime groups. That assessment was based in part on Longhorn using a zero-day software exploit, which Symantec found embedded within a Microsoft Word document. The exploit delivered a data-stealing tool called Plexor.

"The malware had all the hallmarks of a sophisticated cyberespionage group," Symantec writes. "Aside from access to zero-day exploits, the group had preconfigured Plexor with elements that indicated prior knowledge of the target environment."

Longhorn's malware seem tuned for cyberespionage, with components for fingerprinting systems, discovering other ones and exfiltrating data, Symantec adds.

Longhorn usually targeted governments and international organizations, such as those in the financial, telecoms, energy, aerospace and information technology. "All of the organizations targeted would be of interest to a nation-state attacker," the company says.

With the benefit of hindsight, Longhorn appears to have made operational security errors as its campaigns unfolded. Code words were used to identity victims and campaigns. Symantec found ones that would likely indicate the group originated from an English-speaking North American country.

"One example was a nod to the band The Police, with the code words REDLIGHT and ROXANNE used," Symantec writes. Another example: a piece of malware was nicknamed SCOOBYSNACK - after the animated television series Scooby Doo.

Of course, it is entirely plausible that the codenames could be intended as a false flag to point suspicion in another direction.

Fluxwire vs. Corentry

But Symantec also noticed a parallel between leaked Vault 7 documents that describe malware called Fluxwire - including a list of its features and a related change log - and malware that Symantec has been tracking, which it calls Corentry, suggesting they are one in the same.

"New features in Corentry consistently appeared in samples obtained by Symantec either on the same date listed in the Vault 7 document or several days later, leaving little doubt that Corentry is the malware described in the leaked document," Symantec writes.

Until 2014, Corentry was compiled with an application called GCC. But Symantec later recovered malware that had been compiled on Feb. 25, 2015, using a different compiler - the Microsoft Visual C++ compiler, often referred to as MSVC. The Vault 7 documents, meanwhile, note that version 3.3.0 of Fluxwire switched to using the MSVC compiler on Feb. 25, 2015.

Corentry sample (MD5 hash)	Date/time of sample compilation	Embedded Corentry version number	Corentry compiler	Vault 7 changelog number	Vault 7 changelog date
N/A	N/A	N/A	N/A	2.1.0 - 2.4.1	Jan 12, 2011 - Feb 28, 2013
e20d5255d8ab1ff5f157847d2f3ffb25	23/08/2013 10:20	3.0.0	GCC	3.0.0	Aug 23, 2013
5df76f1ad59e019e52862585d27f1de2	21/02/2014 11:07	3.1.0	GCC	3.1.0	Feb 20, 2014
318d8b61d642274dd0513c293e535b38	15/05/2014 09:01	3.1.1	GCC	3.1.1	May 14, 2014
N/A	N/A	N/A	N/A	3.2.0	Jul 15, 2014
511a473e26e7f10947561ded8f73ffd0	03/09/2014 00:12	3.2.1	GCC	3.2.1	Aug 18, 2014
c06d422656ca69827f63802667723932	25/02/2015 16:50	N/A	MSVC	3.3.0	Feb 25, 2015
N/A	N/A	N/A	N/A	3.3.1 -> 3.5.0	May 17, 2015 -> Nov 13, 2015

Corentry version numbers and compilation dates compared to Fluxwire version numbers and change-log dates disclosed in Vault 7. (Source: Symantec)

Curiously, Symantec researchers were watching one time when Longhorn suddenly backed off a target.

"On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally," it writes.

The combination of valuable zero-day flaws as well as the used of advanced malware attack capabilities seen in Longhorn attacks leave little doubt that this is the work of a single group, Symantec says. "Taken in combination, the tools, techniques, and procedures employed by Longhorn are distinctive and unique to this group, leaving little doubt about its link to Vault 7."

Executive Editor Mathew Schwartz also contributed to this story.
