Longhorn: Tools used by cyberespionage group linked to Vault 7

April 10, 2017

Spying tools and operational protocols detailed in the recent Vault 7 leak have been used in cyberattacks against at least 40 targets in 16 different countries by a group Symantec calls Longhorn. Symantec has been protecting its customers from Longhorn's tools for the past three years and has continued to track the group in order to learn more about its tools, tactics, and procedures.

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.

Who is Longhorn?

Longhorn has been active since at least 2011. It has used a range of back door Trojans in addition to zero-day vulnerabilities to compromise its targets. Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker.

Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. 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.

#Vault7 linked #Longhorn group infiltrated governments, international orgs, other targets

The link to Vault 7

A number of documents disclosed by WikiLeaks outline specifications and requirements for malware tools. One document is a development timeline for a piece of malware called Fluxwire, containing a changelog of dates for when new features were incorporated. These dates align closely with the development of one Longhorn tool (Trojan.Corentry) tracked by Symantec. 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.

Early versions of Corentry seen by Symantec contained a reference to the file path for the Fluxwire program database (PDB) file. The Vault 7 document lists removal of the full path for the PDB as one of the changes implemented in Version 3.5.0.

Up until 2014, versions of Corentry were compiled using GCC. According to the Vault 7 document, Fluxwire switched to a MSVC compiler for version 3.3.0 on February 25, 2015. This was reflected in samples of Corentry, where a version compiled on February 25, 2015 had used MSVC as a compiler.

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
5d-f76f1ad59e019e52862585d27f1de2	21/02/2014 11:07	3.1.0	GCC	3.1.0	Feb 20, 2014
318d8b61d642274d-d0513c293e535b38	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
511a473e26e7f10947561d-ed8f73ffd0	03/09/2014 00:12	3.2.1	GCC	3.2.1	Aug 18, 2014
c06d422656-ca69827f63802667723932	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

Table. Corentry version numbers and compilation dates compared to Fluxwire version numbers and changelog dates disclosed in Vault 7

A second Vault 7 document details Fire and Forget, a specification for user-mode injection of a payload by a tool called Archangel. The specification of the payload and the interface used to load it was closely matched in another Longhorn tool called Backdoor.Plexor.

A third document outlines cryptographic protocols that malware tools should follow. These include the use of inner cryptography within SSL to prevent man-in-the-middle (MITM) attacks, key exchange once per connection, and use of AES with a 32-byte key. These requirements align

with the cryptographic practices observed by Symantec in all of the Longhorn tools.

Other Vault 7 documents outline tradecraft practices to be used, such as use of the Real-time Transport Protocol (RTP) as a means of command and control (C&C) communications, employing wipe-on-use as standard practice, in-memory string de-obfuscation, using a unique deployment-time key for string obfuscation, and the use of secure erase protocols involving renaming and overwriting. Symantec has observed Longhorn tools following all of these practices. While other malware families are known to use some of these practices, the fact that so many of them are followed by Longhorn makes it noteworthy.

Global reach: Longhorn's operations

While active since at least 2011, with some evidence of activity dating back as far as 2007, Longhorn first came to Symantec's attention in 2014 with the use of a zero-day exploit (CVE-2014-4148) embedded in a Word document to infect a target with Plexor.

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

To date, Symantec has found evidence of Longhorn activities against 40 targets spread across 16 different countries. Symantec has seen Longhorn use four different malware tools against its targets: Corentry, Plexor, Backdoor.Trojan.LH1, and Backdoor.Trojan.LH2.

Before deploying malware to a target, the Longhorn group will preconfigure it with what appears to be target-specific code words and distinct C&C domains and IP addresses for communications back to the attackers. Longhorn tools have embedded capitalized code words, internally referenced as "groupid" and "siteid", which may be used to identify campaigns and victims. Over 40 of these identifiers have been observed, and typically follow the theme of movies, characters, food, or music. One example was a nod to the band The Police, with the code words REDLIGHT and ROXANNE used.

Longhorn's malware has an extensive list of commands for remote control of the infected computer. Most of the malware can also be customized with additional plugins and modules, some of which have been observed by Symantec.

Longhorn's malware appears to be specifically built for espionage-type operations, with detailed system fingerprinting, discovery, and exfiltration capabilities. The malware uses a high degree of operational security, communicating externally at only select times, with upload limits on exfiltrated data, and randomization of communication intervals—all attempts to stay under the radar during intrusions.

For C&C servers, Longhorn typically configures a specific domain and IP address combination per target. The domains appear to be registered by the attackers; however they use privacy services to hide their real identity. The IP addresses are typically owned by legitimate companies offering virtual private server (VPS) or webhosting services. The malware communicates with C&C servers over HTTPS using a custom underlying cryptographic protocol to protect communications from identification.

Prior to the Vault 7 leak, Symantec's assessment of Longhorn was that it was a well-resourced organization which was involved in intelligence gathering operations. This assessment was based on its global range of targets and access to a range of comprehensively developed malware and zero-day exploits. The group appeared to work a standard Monday to Friday working week, based on timestamps and domain name registration dates, behavior which is consistent with state-sponsored groups.

Symantec's analysis uncovered a number of indicators that Longhorn was from an English-speaking, North American country. The acronym MTWRFSU (Monday Tuesday Wednesday ThuRsday Friday Saturday SUnday) was used to configure which day of the week malware would communicate with the attackers. This acronym is common in academic calendars in North America. Some of the code words found in the malware, such as SCOOBYSNACK, would be most familiar in North America. In addition to this, the compilation times of tools with reliable timestamps indicate a time zone in the Americas.

Distinctive fingerprints

Longhorn has used advanced malware tools and zero-day vulnerabilities to infiltrate a string of targets worldwide. 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.

Throughout its investigation of Longhorn, Symantec's priority has been protection of its customers. Through identifying different strains of Longhorn malware, connecting them to a single actor, and learning more about the group's tactics and procedures, Symantec has been able to better defend customer organizations against this and similar threats. In publishing this new information, Symantec's goal remains unchanged: to reassure customers that it is aware of this threat and actively working to protect them from it.

Protection

Symantec and Norton products have been protecting against Longhorn malware for a number of years with the following detections: