the Availability Digest

www.availabilitydigest.com
@availabilitydig

Google and Symantec Spar Over Digital Certificates

April 2017

Symantec is judged to be the largest digital certificate authority (CA) on the Internet. A CA issues digital certificates that authenticate the ownership of public keys used by organizations for encryption. A digital certificate allows software to communicate securely with the certificate's subject – typically another computer. For instance, digital certificates are used by TLS – Transport Layer Security, a cryptographic protocol that provides communications security over a computer network.

Symantec and the brands that it controls (such as VeriSign) account for 30 percent of the valid certificates used on the Internet.

Symantec's History with Improper Digital Certificates

However, Symantec has an unfortunate history of issuing improper digital certificates. In 2015, it terminated several employees involved in issuing unauthorized certificates for Google web pages. This prompted Google to warn Symantec to take additional steps to validate certificates.

In early 2017, an independent researcher determined that Symantec had issued 108 invalid TLS certificates. 99 were issued to companies with data that was obviously fraudulent. Nine were issued without the knowledge or permission of the affected domains.

Symantec said that it was investigating the incident and would report on the resolution, cause analysis, and corrective actions taken. Most of the improperly issued certificates were revoked within an hour of being issued. All were revoked within 24 hours.

Symantec said that the certificates were issued by one of its audited partners. It revoked the authority of that partner to issue further certificates.

A software engineer on the Google Chrome team said that an investigation into 127 mis-issued certificates ballooned into at least 30,000 issued over a several-year period

Google Has Lost Patience with Symantec

Google's Chrome development team is fed up with Symantec as a CA. Over the past 18 months, Google has tangled repeatedly with Symantec over the way it issues TLS certificates. Google believes that Symantec has been improperly issuing security certificates for tens of thousands of websites.

Google plans to no longer trust TLS certificates issued by Symantec and will force Symantec to re-issue certificates faster. Otherwise, you will not be able to visit websites with old, untrustworthy documentation without Chrome giving you plenty of warnings.

Chrome will stop recognizing Symantec's Extended Validation (EV) certificates. EV certificates are supposed to convey the highest assurance of a site's authenticity. Chrome will recognize that the site has a certificate, but it will not treat the certificate as EV. Chrome will not accept any newly issued certificates from Symantec that have a validity period of longer than nine months. However, instead of acting by an arbitrary deadline, Google will decrease the maximum age of Symantec-issued certificates to nine months.

Google requires CAs to perform a number of critical functions:

- Properly ensure that domain control validation is performed for all server certificates.
- Frequently audit logs for evidence of unauthorized issuance.
- Protect their infrastructure to minimize the possibility of fraudulent certificates being issued.

According to Google:

- Symantec allowed at least four parties access to their infrastructure.
- Symantec did not properly oversee this access.
- Symantec failed to disclose such information in a timely manner.

Summary

Mis-issued certificates pose a critical threat to the Internet because certificate holders can impersonate legitimate sites. To protect themselves and their customers, every organization needs to be able to quickly detect unauthorized certificates issued by any CA and remove or replace them. Businesses that are unprepared to detect and respond to CA errors threaten the integrity of encrypted and authenticated Internet traffic.

Acknowledgements

Information for this article was taken from the following sources:

Symantec caught issuing illegit certificates for second time in two years, *SC Network Security*; January 23, 2017.
Google to Symantec: We don't trust you anymore, *Infoworld*; March 24, 2017.
Google and Symantec go to war over our Internet Security, *Engadget*; March 28, 2017.