the Availability Digest

www.availabilitydigest.com
@availabilitydig

# Epidemic of Certificate-Related Outages

April 2017

The use of digital certificates is skyrocketing as companies use more cloud services, IoT devices, and DevOps automation. A digital certificate is an electronic document used to prove ownership of a public key. It is issued by a certificate authority (CA) and allows software to communicate securely with the certificate's subject. A certificate's subject may be a person or an organization, or it may be a computer or other device (used in TLS – Transport Layer Security – a cryptographic protocol that provides communications security over a computer network).

Certificates and their corresponding keys are the foundation of all cyber security. They are the identity and access management facilities for machines, just like user names and passwords are for humans. Certificates allow machines to communicate securely.

One of the primary drivers in the increase in digital certificates is the explosion of IP-connected devices on business networks. The increase in certificates and their corresponding keys compounds the serious security vulnerabilities associated with cryptographic key and digital certificate management. When a digital certificate expires, the related public key is no longer effective. Communication with the certificate's encrypted subject is no longer possible. The encrypted subject is effectively lost. This is a certificate-related outage.

Most businesses do not have the visibility or tools necessary to manage this element of cybersecurity.

## The Epidemic of Certificate-Related Outages

Venafi, Inc. is a cybersecurity company that develops software to secure and protect cryptographic keys and digital certificates. According to Venafi in a study released February 2, 2016, four out of five businesses suffered certificate-related outages in 2016. It points out that the outages were due to inadequate cryptographic controls.

The leading cause of the outages was the expiry of digital certificates. Venafi's study showed that most companies do not have an automated process for certificate renewals. Even worse, almost two-thirds of the companies surveyed had no central record of digital certificates. The average company has over 16,000 keys and certificates of which they are unaware.

As the use of encryption grows, challenges associated with effective key and certificate management have proliferated. The Venafi survey showed that:

- 79% of respondents suffered at least one certificate-related outage in 2016.
- Over a third suffered more than six such outages in 2016.
- 4% suffered 100 or more certificate-related outages in 2016.
- Almost two-thirds could not respond to a certificate-related security event in less than six hours.

## What Should Companies Do?

Organizations must automate the discovery, issuance, lifecycle, and remediation of all keys and certificates from the data center to the cloud to the IoT edge of their network. This process must start with a central record of digital certificates and their keys. Facilities must be in place to provide notification about the expiration of certificates so that they can be renewed in a timely fashion.

Tracking down 16,000 unknown keys will not be a simple task. But if this is not done, the epidemic of certificate-related outages will undoubtedly continue.

## Acknowledgements

Information for this article was obtained from the following sources:

Businesses experiencing an epidemic of certificate-related outages, *Information Age*; February 2, 2017.
80% of businesses hit by certificate-related outages, study shows, *SC Magazine*; February 2, 2017.
Certificate-Related Outages Affect 79 Percent of Businesses, *Business Wire*; February 2, 2017.
Certificate-Related Outages Impact Most Businesses, *APM Digest*; March 1, 2017.
Public Key Certificates, *Wikipedia*