Executive Brief

2016 CIO Study

Reveals growing concern about threats to keys and certificates

How widespread is the abuse of keys and certificates?

A 2016 survey conducted by Vanson Bourne, an independent technology market research provider, asked 500 enterprise CIOs in the U.S., U.K., France and Germany how the increased demand for encryption is impacting their cyber security efforts. As the use of encryption increases, so does the number of cryptographic keys and digital certificates. These keys and certificates make up machine identities, which are needed to authenticate machines in the encryption process—similar to how usernames and passwords authenticate people. The results of the survey show IT executives acknowledge the risks associated with the cryptographic keys and digital certificates, but are largely unprepared to counter them.

87% of CIOs believe their security controls do not fully protect their business

Today's security controls are designed to blindly trust the keys and certificates that comprise machine identities and control encrypted traffic. Even with layered security defenses, respondents believe their security controls are less effective because they cannot inspect for malicious activity or data exfiltration inside encrypted traffic.

90% of CIOs have been or expect to be attacked by threats hidden in encryption

Most are already experiencing attacks that use unprotected keys and certificates to disguise malicious actions in encrypted traffic. Attackers routinely misuse machine identities to hide attacks, evade detection, and bypass critical security controls. If this malicious activity goes undetected, cyber criminals can gain elevated privileges necessary to access critical systems and data for extended periods of time.

85% of CIOs anticipate criminal misuse of keys and certificates will get worse

As enterprises expand IT initiatives around Encryption Everywhere, DevOps, IoT, enterprise mobility and other agile, Fast IT strategies, the explosion of keys and certificates provides cyber criminals with more opportunity to compromise these keys and certificates and hijack machine identities for use in their attacks.

86% of CIOs expect keys and certificates to be the next big market for hackers

Keys and certificates are desirable to attackers because of their importance, lack of protection, and the ability for cyber criminals to monetize them quickly, according to Intel's Matthew Rosenquist.[1] In addition, IBM Security's X-Force research team has found that large numbers of code-signing certificates are also now a hot commodity in the black market.[2]

79% of CIOs expect the speed of DevOps to make it difficult to know what should be trusted

As DevOps quickly delivers new IT services, the number of keys and certificates used to establish machine identities and secure those services is growing exponentially. But when developers, and not security professionals, are left to manage and secure machine identities, the organization is exposed to security blind spots and new vulnerabilities.

Unless key and certificate issuance and revocation are automated using secure systems, not just any framework or open source tool, DevOps becomes another significant area of risk.

What is driving the increasing risk to keys and certificates?

Organizations are implementing IT initiatives such as Fast IT, DevOps and Encryption Everywhere strategies, which are responsible for a nearly 100% increase in encrypted traffic. This is causing a dramatic rise in the sheer numbers of keys and certificates, up 34% between 2013 and 2015, with over 23,000 keys and certificates in today's average enterprise. And 54% of security professionals admit to not knowing where all of their keys and certificates are located, who owns them, or how they are used.[3] This lack of visibility into the status of the machine identities that control the flow of encrypted data leaves many organizations exposed to attack and business disruption from certificate-related outages.

What are the best strategies for protecting your encryption assets?

To lower the risk of attack, your organization must protect keys and certificates in the datacenter, on desktops, on mobile and IoT devices, and in the cloud. The entire certificate issuance and renewal process should be automated with policy enforcement and workflows, which will help you quickly scale new encryption-dependent applications. This approach to key and certificate protection also supports Fast IT. Plus, it improves your security posture by increasing visibility, threat intelligence and policy enforcement for machine identities.

With the proper visibility of keys and certificates, you will be equipped to inspect SSL/TLS traffic, stop certificate-based outages, complete SHA-2 migration and deliver fast security for cloud computing, DevOps and IoT. Taking control of keys and certificates—the foundation of your security—will help you strengthen all of the security controls that are built on that foundation. By securing machine identities across your organization, you'll help maximize your security investments and protect your customers, business, data and brand.

ABOUT VANSON BOURNE

Vanson Bourne is an independent specialist in market research for the technology sector. Its reputation for robust and credible research-based analysis is founded upon rigorous research principles and the ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

ABOUT VENAFI

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

[1] Rosenquist, Matthew. Intel IT Expert Blog. Stealing Certificates to Sign Malware will be the Next Big Market for Hackers. December 23, 2014.

[2] Kessem, Limor. IBM Security Intelligence Article. Certificates-as-a-Service? Code Signing Certs Become Popular Cybercrime Commodity. September 9, 2015.

[3] Ponemon Institute. 2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point. 2015.