Broken Trust

Exposing the Malicious Use of Digital Certificates and Cryptographic Keys

iSIGHT PARTNERS & VENAFI RESEARCH WHITE PAPER

Table of Contents

Executive Summary

Digital certificates and cryptographic keys are used to establish trust between entities. They ensure that data at rest or in transit is secure and the entities sending and receiving information are who they claim to be. This trust, however, is established through faith in the entities that provide certificates and keys and malicious actors can exploit this trust by hijacking the technologies through theft or forgery and using them for malicious schemes. These actors utilize compromised digital signatures for a bevy of illicit activities, which frequently include cyber criminal activities as well as cyber espionage. For example, malicious actors seeking nation-building resources or industry-specific technology often seek a competitive edge by accessing competitor's proprietary information. Financially motivated actors seek to access financial account information and other data that can be monetized. Malicious actors can abuse Public Key Infrastructure (PKI) and digital certificates to carry out all of these activities.

Introduction

This white paper provides an overview of the motivations and tactics, techniques, and procedures (TTPs) of cyber threat actors who misuse digital certificates and cryptographic key technologies for malicious purposes. The paper includes two main sections: the first section describes digital certificates and the role of PKI in establishing trust between two entities; the second section examines the cyber threat landscape from an attacker-oriented perspective, offering several brief real-world examples of how malicious actors have utilized digital certificates and cryptographic keys to achieve their ends. The paper concludes with a brief assessment of the implications of these threats, pointing out emerging trends and suggesting visibility into and control over PKI assets as a company's best strategy in minimizing its attack surface.

Cyber threat intelligence, case studies and analysis are contributed by iSIGHT Partners.

Keys and Certificates Make Everyday Life Possible

Overview

Private enterprises and government agencies utilize thousands of certificates and keys, which are usually provided by trusted third parties known as certificate authorities (CAs). Organizations worldwide rely on these trust-based relationships to secure their data transmissions.

Public Key Infrastructure (PKI)

PKI refers to any set of procedures, policies, and technologies that enable entities to use asymmetric encryption keys to validate their identities and secure their communications with other entities. PKI refers to the system that distributes public key information and enables users to validate signatures.

PKI relies on public key cryptography—a cryptographic system that uses two mathematically linked keys, a public key and a private key, for encryption and decryption. The two keys are related such that the data can only be decrypted with the private key of the corresponding public key used to encrypt the data. This unique relationship between the keys enables entities to "sign" data. An entity that wants to prove that it has sent particular data signs that data with its unique and secret private key. It distributes the decrypting public key to any entity that wants to validate the "signed" data.
Of course, the second entity needs to trust that the entity distributing the public key is who it claims to be.

Digital certificates are essentially electronic documents that automate this process by binding an identity with a public key. The certificate itself is signed by the private key of the entity, asserting the relationship between the public key and the identity. A certificate can be self-signed—that is, signed by the private key corresponding to the public key in the certificate. However, to trust a self-signed certificate, an entity would need to verify on its own that the certificate owner truly is who it claims to be. Conversely, CA-signed certificates enable users everywhere to trust that network communications originate from the parties from which they claim to originate.

For example, when a user performs secure online banking, the user's browser establishes a secure session with the bank's server via Secure Sockets Layer (SSL). When the user's browser connects to the bank's website, the bank's web server sends the browser its SSL certificate. To determine if it should trust this SSL certificate, the browser checks the signature. Because the certificate is CA-signed, the signature must match the CA's root certificate, which has been installed within the browser's trust store.

Certificates also provide secure, encrypted communications. Once the user's browser validates the bank web server's SSL certificate, the browser creates a session key, encrypts the session key with the bank's public key, and sends the encrypted key back to the bank server. Only the private key, which only the bank server knows, can decrypt the session key; therefore, only the user's browser and the bank's server can obtain the session key, which then encrypts data for the remainder of the session.

This process (depicted in figure 1 on page 5) verifies that the user is, indeed, accessing the bank's official web site. The bank may also utilize such certificates to determine that the user attempting to access this account is the real and valid customer. In that case, the user's browser would need an SSL certificate of its own, signed by an entity that the bank's server trusts.

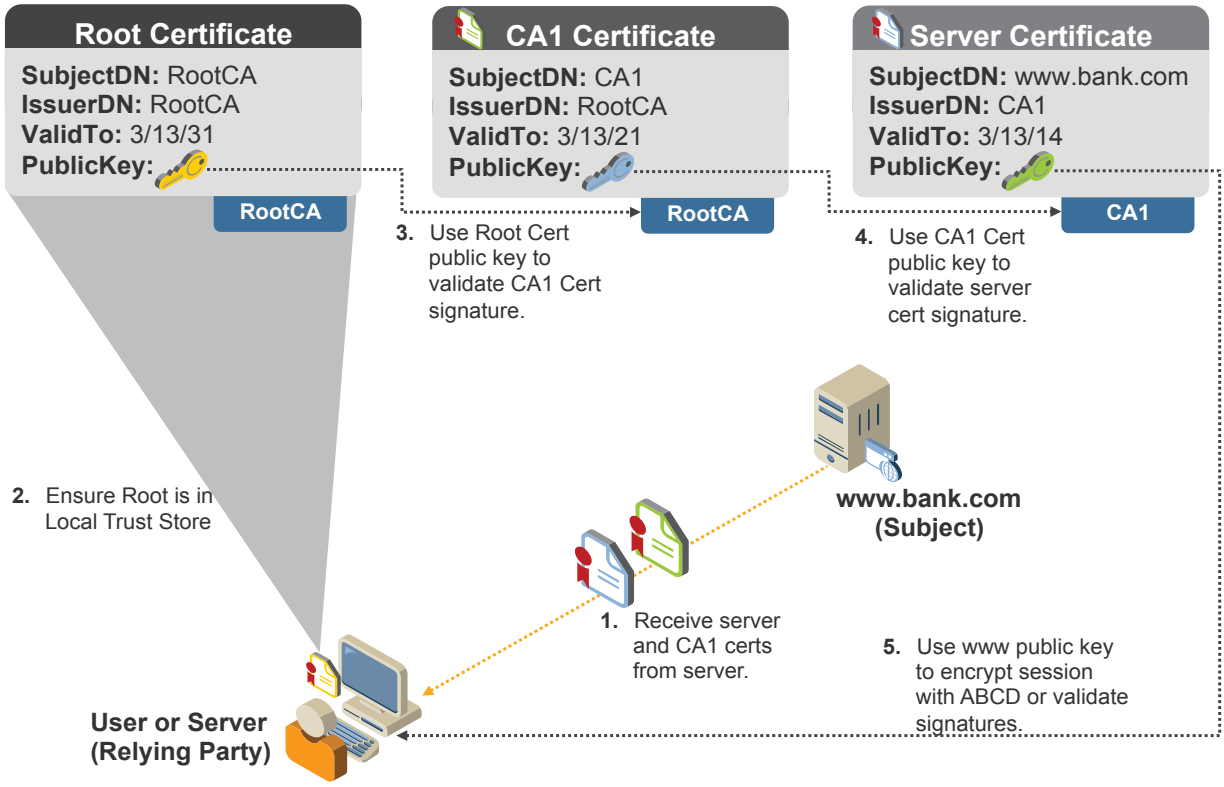

Figure 1 — Establishing trust with certificates

Secure Shell (SSH)

SSH allows for secure remote communications between two hosts. The most widely deployed SSH authentication model utilizes public key cryptography. In this model, the receiving host, or server, maintains an up-to-date public key for each trusted sender, or client. As long as the SSH server has a public key in its trusted key store, it automatically trusts communications from the client with the matching private key. SSH alleviates the need for trusted CAs that validate identities, but its security depends on carefully regulating which public keys are installed on particular servers and who can access the corresponding private keys—particularly, because SSH also allows for elevated privileges and the bypassing of authentication mechanisms on hosts.

The following example (depicted in figure 2 on page) demonstrates how SSH works. A system administrator can log on to Server 1 and Server 2 because the administrator's public key has been stored as a trusted key on Server 1 and Server 2. Moreover, Server 2 can authenticate to Server 1 because Server 2's public key has been stored on Server 1.

Summary

Because public key cryptography is such a secure and established encryption method, organizations and individual users generally trust that information is not altered in the communication exchange. However, simple weaknesses in the storage and management of keys and certificates can result in the compromise of these technologies.

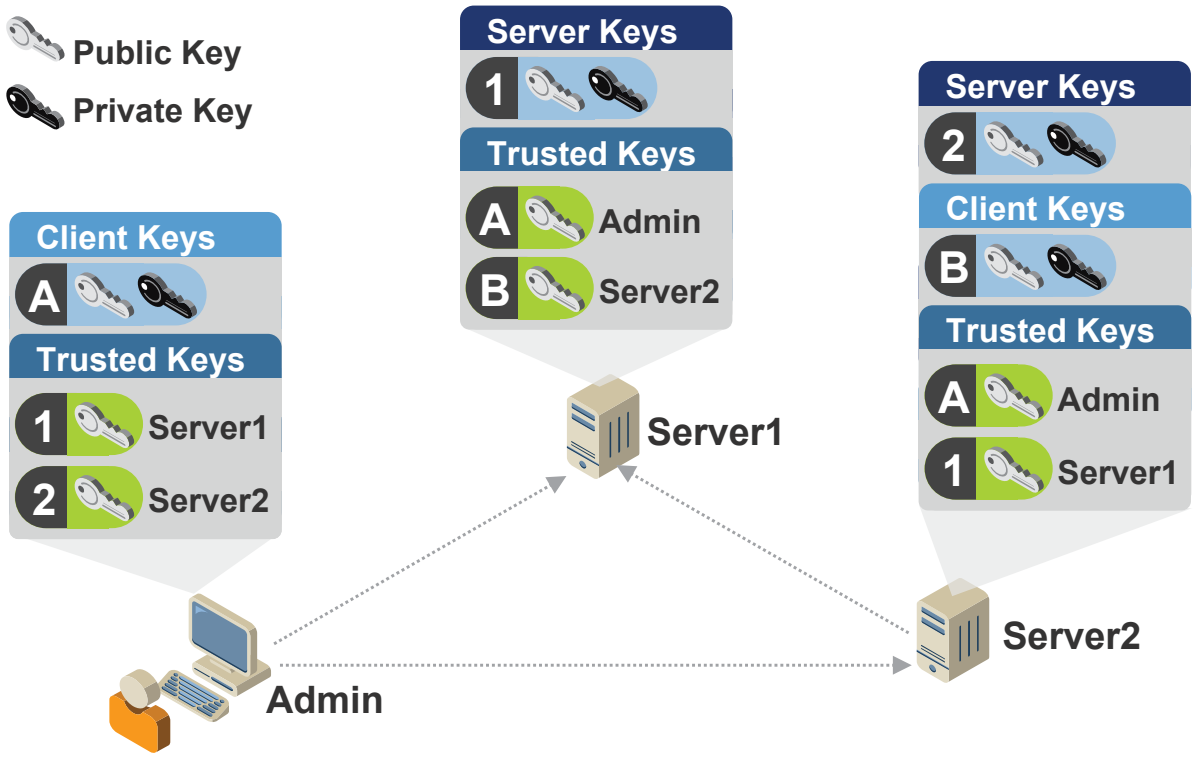

Figure 2 — SSH authentication

Current Cyber Threat Landscape

Overview

The cyber threat landscape consists of malicious actors who have a variety of motivations: some seek financial gain, some seek strategic information, and others promote their ideological views or to establish or build upon their own reputation. These malicious actors can impact public and private sector organizations in many ways, depending upon their skill level, intention, available resources and the methodologies they utilize.

Based on current cyber threat activity, it appears that the primary categories of actors using digital certificates and keys in malicious activity are financially motivated and/or targeting proprietary information. Presently, evidence does not indicate a significant number of actors who participate in cyber activism or ego-focused campaign activities abusing these technologies. This section examines the primary motivations of actors actively abusing these technologies and provides several case studies illustrating these threats, outlining the relationship between the actors' motivations, TTPs, and the types of flaws that make digital signatures and keys vulnerable to attack.

Cyber Threat Actors

The malicious actors who use certificates and keys to launch attacks can be grouped into the following categories: cyber crime actors, cyber espionage actors, and other threat actors.

Cyber Criminals

Cyber crime actors are primarily motivated by financial gain and typically target sources of data that can be used in fraudulent activity or sold for a profit. Targeted data typically includes account credentials or other sensitive personally identifiable information (PII).

Cyber criminals frequently use e-mail spam campaigns to distribute malicious attachments or to redirect users to malicious websites. Common malware payloads of spam campaigns include credential theft malware and ransomware. Cyber criminals also frequently target vulnerabilities that exist in the web application layer of an organization's system. Stolen legitimate certificates are used in campaigns to sign malware to increase the likelihood of infection on a victim machine.

Cyber Espionage Actors

Cyber espionage actors are characterized by their intent to collect information that can be used for strategic purposes within a competitive landscape. Their intelligence-collection campaigns are often designed to support state intelligence priorities—gathering information that provides advantages in the political, economic, diplomatic and military arenas.

Cyber espionage actors typically use spear-phishing e-mails with socially engineered lures to entice victims to download malware (such as a Remote Access Trojan, or "RAT") by clicking hostile links or opening malicious, attached files. Malware used in cyber espionage campaigns is typically designed to give the malicious actors persistent access to a targeted system or network, often opening a backdoor for additional damaging activities, such as privilege escalation, network reconnaissance, and data exfiltration. Watering hole attacks, which involve compromising a specific site with the explicit aim of infecting a targeted group within the site's regular readership, are also common.

Data suggests cyber espionage actors often use stolen valid digital certificates and expired digital certificates in spear-phishing campaigns and watering hole attacks in the process of exploiting system vulnerabilities to install data exfiltration malware on a victim's machine. There is also information suggesting cyber espionage actors use certificates to obfuscate and encrypt network traffic between compromised machines and command and control servers during the exfiltration stage of an attack. Certificates that are accepted by a target machine as valid will generate fewer user notifications warning users that the file they are accessing may be a security risk.

Other Threat Actors

Other threat actors are motivated by various ideologies, religions, and political sentiments. Known as cyber activists, or "hacktivists," they target organizations they perceive as directly or indirectly associated with an opposing ideology or as dangerous to their own. Hacktivist activity is commonly characterized by opportunistic targeting of unsecured websites; the effects of this activity are typically limited to low-impact defacement and leakage of data. These actors commonly utilize low-sophistication TTPs to compromise sites directly (including activities such as cross-site scripting, SQL injection or embedded iFrames). They might also purchase automated tools or services that enable them to employ more sophisticated methodologies, such as distributed denial-of-service (DDoS) or more targeted vulnerability exploitation.

This category of threat actor also includes groups and individuals who are motivated by image promotion and ego, rather than by specific ideological motives, because these actors exemplify similar TTPs and often associate themselves with larger ideological movements for the publicity. At this time, little indicates these types of actors actively use digital certificates and/or cryptographic key technology in even a minority of their activities.

Use of Certificates and Keys in Malicious Activity

The following examples illustrate some of the ways in which cyber actors actively misuse PKI and SSH. Each case study occurred between November 2012 and July 2013 and was selected to demonstrate typical attack paths associated with actors compromising and utilizing digital signatures. It is important to note that these case studies are by no means the only ways in which PKI and SSH can be compromised; rather, these cases are provided to illustrate some of these TTPs and the motivations typically associated with these methodologies, as well as the complex steps and resources needed to successfully conduct an attack using these technologies.

Use of Certificates in Spam Campaigns

The following two incidents illustrate the use of valid certificates in financially motivated attacks. This paper will focus on the phases of the attacks that most prominently use stolen certificates, highlighting how the attackers compromised the certificates and then operationalized them as tools in other phases of the attack.

Between August 27 and September 11, 2012, Portuguese-speaking actors obtained a signed digital certificate from a legitimate CA by copying the name of a well-known Brazilian company and registering the domain with falsified information. The stolen certificates were then used to sign credential collection malware. The actors successfully executed their campaign for more than two weeks before the CA revoked the certificate. Unfortunately, certificate revocation did not resolve the problem immediately; many modern browsers ignore certificate revocation lists (CRLs) based on user behavior, resulting in further proliferation of the signed malware.

A similar scheme involving Portuguese-speaking actors took place between August and November 2012. A group of actors reportedly obtained a valid digital certificate from a legitimate CA, named a signed payload file after a legitimate software company, and registered domains using a front company. While the actual method used to obtain the certificate is unclear, the actions taken after compromise are better established. The actors leveraged the stolen certificate to sign malware distributed through socially engineered spam messages, increasing the likelihood that the malware would successfully bypass both concerned users and their security software to infect targeted machines.

These cases illustrate one way in which financially motivated actors are actively targeting CAs to obtain valid certificates. They also demonstrate how these actors combined the use of valid certificates with social engineering techniques to increase the effectiveness of malware distribution spam campaigns.

Use of Certificates for Pharming

On February 12, 2013, the Korea Financial Telecommunications and Clearings Institute (KFTC) disclosed to South Korean media sources that an unspecified group of actors used pharming activities to compromise 461 authentication certificates issued by a KFTC subsidiary—likely Yessign, one of the largest authorities under KFTC. Pharming is a type of malicious scheme in which an attacker redirects a victim's web session to a malicious URL masquerading as a legitimate website; this redirection can occur by corrupting a DNS server and pointing a URL to the masquerading website's IP. The attacker may infect victims by distributing spam messages with malware that causes the browser redirection to occur. Once the victim has visited the masquerading website, transactions may be mimicked and information like login credentials may be collected and sent to the attacker. In this case, users with accounts at a number of Korean banks, including Shinhan Bank, Kookmin Bank, and Woori Bank, were re-directed to attacker-controlled duplicates of legitimate pages that appeared to be their primary banking portal. The pages collected user information in addition to KFTC-authorized certificates, which are legally required for all online bank accounts in South Korea.

This case study features another trust-based relationship that relies on certificates: instead of utilizing PKI to prove the legitimacy of a site to a user, certificates here authenticate the user to the site, verifying that the user is who he or she claims to be. Customers download their KFTC-authorized certificates as digital files, which then become permanently associated with the local machine or removable storage device on which they are stored, allowing the certificate to function essentially as a secondary authentication measure directly between the banking institution and the user.

The theft of these certificates demonstrates that certificate security is a concern not only for institutions, but also for users who often lack the resources and technical knowledge necessary to adequately protect their private digital signatures. Although compromising user account credentials through pharming requires sophisticated redirection and certificate theft capabilities, this incident shows that cyber criminals have the motivation and ability to launch such attacks. With attacks such as these, they can harvest and monetize an extensive amount of user data, which they can then use for fraudulent activity.

Pharming incidents undermine the credibility of institutions and the trust-based relationships that undergird online transactions. As in other cases

discussed, however, secure certificate usage on the part of the banking institutions could have mitigated the attack by alerting users that the site they had accessed, despite its matched DNS entry, was not genuine.

The methodology utilized in this case can also be applied to watering hole attacks—a TTP highlighted earlier as an attack typically employed by cyber espionage actors to collect proprietary data. Watering hole attacks enable malicious actors to target broad groups of individuals based on probable habits. This tactic allows actors to compromise members of targeted groups or ideologies who are likely to visit specific websites, reducing the actors' dependence on social engineering techniques as well as exposure of their methods to security researchers. Stolen or forged certificates can increase the effectiveness of the watering hole campaign by minimizing the chance that a user infected by the malware sees or heeds a warning.

Use of SSH to Access to a Targeted Environment

Malicious actors can also use SSH to gain access to a targeted environment. In March 2013, malware known as the Jokra Trojan infected South Korean banks and media outlets in an incident referred to as DarkSeoul. Analysis of the malware revealed that it uses a dropper to install itself on targeted machines and then proceeds to install four files. The malware searches the victims' folders for two pieces of software commonly used by system administrators. If either is found, the malware searches these folders for any saved sessions that contain SSH credentials. If any sessions are found, the malware establishes a connection to those systems, uploads a malicious BASH shell script to them, and executes the script.

The initial infection vector for this malware is unknown, but patch management servers used by AhnLab Policy Center (APC), a South Korean network security solutions provider were found to be compromised and were likely leveraged by the malicious actors to disseminate the malware. The discovery of AhnLab APC as a propagation vector highlights the threat posed by systems designed to aid policy and patch management. In this instance, two factors appear to have contributed to creating a vulnerable environment. First, to accommodate off-site employees, some companies deployed these servers as Internet-facing assets (as opposed to restricting access via the local intranet). Second, a software design flaw seems to have enabled the attackers to hijack the accessible servers for their own purposes.

Attackers probably chose this method due to the ease of access as well as the lure of a system designed for mass propagation. Although Jokra was used in a targeted effort, it is reasonable to assume any actor seeking to achieve similar outcomes could employ a similar methodology.

Use of SSL for Secure, Covert Communication

While this use case demonstrates how digital signatures can be utilized to gain illegitimate access to a system (via signed malware or through otherwise leveraging the trust that inherently underpins digital signatures), SSL can also be utilized to create a covert channel of communication. Several malware families utilize SSL in this way. On December 6, 2012, a NATO advisor was targeted in a phishing attack that sought to install a variant of Enfal that included this feature. The e-mail, titled "Did Global Warming Contribute to Hurricane Sandy's Devastation?" included a malicious attachment containing exploit code for the Microsoft Office 2010 RTF Stack-Based Buffer Overflow Vulnerability (CVE-2010-3333) that was utilized to install the Enfal payload. SSL-encrypted communications were used to obfuscate network traffic and evade detection by network analysts. Using SSL not only encrypts traffic, but it is also more likely to be treated as legitimate by network administrators, decreasing the likelihood of compromise discovery – particularly if the certificate appears to have been signed by a legitimate CA.

This technique contributes greatly to the malware's capability to avoid detection on victim machines. As a result, a number of malware families will utilize SSL in this way.

This technique demonstrates another frequent use-case of malicious actors for this form of technology to undermine the trust that operators place in the type of traffic being exchanged, and this also must be considered in assessing the role of digital signatures during an incident.

The Underground Marketplace

These case studies help to establish a general trend of malicious actors using digital certificates for illicit purposes. The underground market for digital certificates has also been maturing, and the role of compromised digital signatures within the overall underground economy has been slowly increasing over the last year. An active underground marketplace has developed for stolen certificates, forged certificates, and compromised keys. The market also offers tools that help other malicious actors to gather information, to compromise digital signatures, and then to use those signatures for illicit purposes.

For example, in early June 2013, Severa (the handle of a well-known spammer and malware developer) advertised a tool known as Northern Fairy Tale, which to an underground forum. This tool allegedly enables actors to conduct and administer mass iFrame injections. It also automates privilege-escalation attacks more easily than competitor products. The tool includes two components related to digital signatures: it checks for and manages SSH credentials on compromised servers and it attempts automated privilege-escalation by checking for well-established exploits. Although this tool does not use any novel techniques, it combines them at a price much lower than that of similar illicit tools. In addition, the Northern Fairy Tale panel features a well-developed graphical user interface, making it more useable and accessible for low sophistication actors.

Other incidents similarly exemplify a maturating underground market with increasingly sophisticated tools. An actor recently advertised a tool that could purportedly sign executable malware with certificates from CAs. A rogue hosting provider, active in markets in Asia, Europe and North American, offered fake SSL certificates that spoof legitimate CAs.

These few examples, in addition to many others, indicate a greater trend of malicious actors interested in obtaining and exploiting legitimate authentication technology. This underground activity demonstrates that actors can and do use these technologies for various purposes, most often related to financial gain or the collection of proprietary data for strategic use.

Conclusion

Malicious actors misuse trust-based cryptographic technology as part of many schemes. Because organizations can best protect themselves by understanding the real threats to their network, they must understand the attack vectors most likely to be used by the threat actors motivated to steal their data. Malicious actors who target sensitive and/or proprietary data, whether as part of a financially motivated crime or a cyber espionage plot, often misuse digital certificates and keys to enhance the effectiveness of their attacks.

As illustrated by the examples in this white paper, these actors abuse these technologies in a range of attack vectors, depending on their particular objective. Although lack of visibility into how cyber espionage actors plan and execute their attacks limits the assessments of trends in this area, one particular trend of note is the increase in use of stolen certificates in cyber crime malware schemes over the past several years. Underground marketplace activity further indicates that malicious actors remain interested in these technologies and that they intend to continue abusing these technologies. A maturing underground marketplace may contribute to an increase in the abuse of these technologies in both the near future and the long term.

Organizations that use digital certificates and SSH keys must understand how they are using these technologies to regulate trusted communications. They need a comprehensive inventory of their particular assets and a centralized insight into and control over the trust relationships. They can then become proactive in preventing compromise on all attack surfaces.

About iSIGHT Partners

Since 2007, Dallas-based iSIGHT Partners has been recognized as the leader in global cyber threat intelligence delivering intelligence and insight to leading enterprises in business and government. With a global network of security analysts and geographic risk management centers in Washington DC, The Netherlands, Brazil, Ukraine, India and China, iSIGHT Partners is uniquely positioned to monitor and mine the cyber threat ecosystem and deliver proprietary intelligence products and services specific to the threats its clients face. With iSIGHT Partners, enterprises can be empowered through an intelligence-led security strategy that connects intelligence directly to their business.

Find iSIGHT Partners on the web at www.iSIGHTpartners.com.

About Venafi

Venafi is the inventor of and market leader in Enterprise Key and Certificate Management (EKCM) solutions. Venafi delivered the first enterprise-class solution to discover all keys and certificates, connect these assets to the people responsible for them, report on and audit their use to prove compliance, enforce policy to reduce risk and errors, and automate all operations to eliminate security risks, downtime and compliance failures. Venafi also publishes best practices for effective key and certificate management at www.venafi.com/best-practices. Venafi customers include the world's most prestigious Global 2000 organizations in financial services, insurance, high tech, telecommunications, aerospace, healthcare and retail. Venafi is backed by top-tier venture capital funds, including Foundation Capital, Pelion Venture Partners and Origin Partners. For more information, visit www.venafi.com.

Part number: 1-0017-0913

Contact Venafi

If your enterprise is experiencing challenges related to controlling trust, specifically with securing and protecting cryptographic keys and digital certificates, Venafi can assist. For more information about our products and services, visit us online at www.venafi.com or contact us at info@venafi.com.

www.venafi.com