Real-world Attack Case Study: Misuse of Keys and Certificates Bypass Critical Security Controls

Demonstration of How Attackers Use Stolen Keys and Certificates to Breach a Behind-the-Firewall System

Who Should Read this Paper?

This technical case study addressing key and certificate security issues is designed for security conscious enterprises to understand real-life attack scenarios that threaten their businesses in today's world. This white paper demonstrates a recent attack that used cryptographic keys and digital certificates as well as guidance on how to protect certificates and keys and quickly discover and remediate breaches. This paper should be read by more technical IT security staff who are interested in detailed attack methods and remediation tactics. The executive summary is intented for IT Security leaders (CISOs and their direct reports) and addresses the proof-of-concept attack impacts on the business.

The attack scenario described in this technical white paper is based on a reproduction of a real-world attack in a Raxis test environment that simulated an enterprise security infrastructure.

Table of Contents

Executive Summary

Large corporations and organizations are currently under attack from organized hacking groups located around the world. These large-scale attack campaigns have demonstrated that many companies are not prepared to properly defend or remediate against these threats. As these attacks escalate, Raxis—a white hat penetration testing firm—teamed up with Venafi—the leader of key and certificate security—to learn more about how these attacks are occurring, as well as provide instruction on applying secure configurations and remediating after a breach.

Weaponized Heartbleed attack code was available to hacking groups for at least five months before the Heartbleed vulnerability was made public. In addition to Heartbleed, thousands of malware variants have exploited unprotected keys and certificates. With this extensive exposure, organizations need to practice good security hygiene with keys and certificates that quickly discovers and remediates breaches. Without this protection, compromised keys and certificates can be used to steal data or impersonate web servers.

To analyze attack methods using keys and certificates, Raxis created a test environment and reconstructed an attack scenario modeled after a current real-world attack that breached a Global 200 business. The steps used by the attackers can be summarized in four main objectives:

1. Stealing digital certificates and private keys
2. Gaining access to the organization using stolen keys, certificates, and credentials
3. Expanding access with stolen or created Secure Shell (SSH) keys, VPN credentials, and other backdoors
4. Exfiltrating stolen data using SSL to bypass security controls and stolen keys to decrypt the data

The Raxis analysis concludes that, when attackers use these steps, they can undermine traditional security controls and breach organizations. The various traditional security tools currently on the market are not enough to effectively reduce risk and protect organizations. According to the Verizon Data Breach Investigations Report, most attacks are not discovered by company Intrusion Detection and Prevention Systems (IDS/IPS) or managed security services. Instead, attacks are most often discovered and communicated by a third party that has been affected by the breach or has noticed unusual activity. Without key and certificate security, attackers can use keys and certificates to bypass traditional security controls and hide their activities—often stealing data undetected for extended periods of time.

To defend against these attacks, organizations need comprehensive key and certificate security that issues, protects, and rotates keys and certificates in datacenters, on workstations and mobile devices, and even in the cloud. When architecting this security, it should protect certificates and private keys, recognize when these have been compromised, and automate the process to prevent misuse and increase remediation speed. This key and certificate security approach bolsters other security controls and protects the business against trust-based attacks that leverage keys and certificates.

Introduction

As reported by Time, Bloomberg, and others, known Chinese cyber-espionage operator, APT18, compromised a Fortune 200 American health services organization and stole data on 4.5 million patients. This case study outlines a reconstruction of how the Chinese APT18 group could have breached this Fortune 200 company to successfully steal data and maintain a long-term foothold.

While it is not known exactly how the attack happened, the Raxis team has attempted to recreate the attack based on information that was made publicly available. The scenarios in the case study include an approach that was likely taken by the attackers and uses real attack capabilities and technologies.

Each situation has been performed in a simulated environment using actual enterprise-grade security controls, servers, and networking equipment that may have been used by the compromised company and represents a network architecture used by many enterprises. The security penetration testing engineers at Raxis recreated these scenarios based on real-world systems as seen on assessments all across North and Central America.

There are three separate perspectives included in this case study:

- The hacker, outlining the four steps used to breach a major organization
- Company A, showing the staff's reaction to the attack without the support of key and certificate security
- Company B, demonstrating a response to the attack with key and certificate security in place

This case study provides insights as to how the misuse of keys and certificates undermines security controls that organizations expect will mitigate threats. By misusing keys, certificates, and credentials throughout the attack chain, Chinese APT18 operators were able to use these stolen assets to gain access, expand their foothold, and exfiltrate data.This white paper is intended to assist technical managers and personnel as they architect and implement a plan to protect their digital certificates and private keys.

Attack Scenario

APT18 Hacker: Meng (a.k.a. PowerMonkey)
Meng is a twenty-three-year-old hacker who works for the Chinese government. While at a school for computer science, she was recruited by the Chinese government to break into American companies and government agencies.

Meng, a.k.a PowerMonkey, has learned that she is rewarded for classified information about American companies. The government highly approves of this as a way to weaken United States market power.

Having worked for the government for five years, PowerMonkey most recently was assigned to a highly focused hacking unit that operates Advanced Persistent Threats (APTs) against American companies. Their goal is to capture confidential data while maintaining an indefinite foothold in American IT environments. The long-term goals of the sustained access are unknown to her, but her leaders stress the importance of maintaining that access. Her target list is clear; her leaders demand a foothold into every single Fortune 500 business in the United States.

After multiple spear-phishing attempts and impersonation attacks, PowerMonkey has had little success with Company A. While she is running an nmap scan to see if anything has changed on Company A's external footprint, she notices an email arrive concerning a new, currently unpublicized, or zero-day, vulnerability. Whenever a zero-day vulnerability is released, every unit works overtime to make the best use of it before the window closes. This newly found vulnerability will later be coined Heartbleed and affects OpenSSL, a very popular encryption library used on many commercial and public-facing systems. Heartbleed provides a memory dump of active memory in the web server when a properly delivered HTTPS heartbeat request is performed.

Name	Meng, a.k.a PowerMonkey
Occupation	Hacker, Chinese Gov't
Age	23
Specialties	Penetrating security defense systems; Privilege escalation

1. Stealing Digital Certificates and Private Keys

PowerMonkey feels certain that Company A has an SSL VPN, so she checks her APT unit's network topology documents on the company, and she is right. Company A is using a Juniper VPN running Junos Pulse software, a very popular SSL VPN package, to allow its employees remote access while working at home. Fortunately for PowerMonkey, her government also provides custom-developed python scripts to exploit systems quickly. PowerMonkey allows these scripts to run overnight in the hopes that Americans, who are awake and working during those hours, will log in to the VPN to work from home. Her goal is to catch any sort of credentials from memory and find them in the output file the next morning. This requires little work for her, and she feels that it is the most promising approach.

The next morning, PowerMonkey uses the tools provided by her research team to search the Juniper memory output for prime numbers, which signifies the presence of a cryptographic key. Once the primes are located, she is able to extract the Juniper VPN's private key from the data that was gathered overnight. Success! With the private key, PowerMonkey knows she can perform a Man-in-the-Middle (MITM) attack against Company A to gather credentials and other data because she can use the private key to decrypt the communication.

Figure 1: SSL Private Key Extracted from Juniper VPN Using Heartbleed

2. Gaining Access to the Organization Using Stolen Keys, Certificates, and Credentials

While manually sifting through the memory dump file, PowerMonkey notices something that makes everything easier for her. She finds a username and password for a user named “Alice” who is working remotely. Instead of performing a complex MITM attack that would require more phishing or perhaps a compromise of some ISP network equipment, PowerMonkey can now just use Alice’s credentials to successfully log into Company A’s Juniper SSL VPN.

```
mpuckett@exch1:~/mpvenafi$ xxd  junos2-dump.bin |grep password@4 -B
00624d0: 0000 0000 0000 6a75 6e6f 732e 7261 7869  ......junos.raxi
00624e0: 7363 6c6f 7564 2e63 6f6d 001b 2208 5828  scloud.com..".X(
00624f0: 2208 6828 2208 0c00 0000 0100 0000 0000  ".h("...........
0062500: 0000 0000 0000 6c6f 6769 6e48 6f73 7441  ......loginHostA
0062510: 6464 7200 0000 3139 322e 3136 382e 3130  ddr...192.168.10
0062520: 2e37 0000 0000 9028 2208 a028 2208 0800  .7.....("..("...
0062530: 0000 0100 0000 0000 0000 0000 0000 6e65  ..............ne
0062540: 7477 6f72 6b49 4600 0000 0000 0000 696e  tworkIF.......in
0062550: 7465 726e 616c 001a 2208 0000 0000 c828  ternal..".......(
0062560: 2208 d828 2208 0800 0000 0100 0000 0000  "..("...........
0062570: 0000 0000 0000 7061 7373 776f 7264 4034  ......password@4
0062580: 0008 0000 0000 4730 3064 4f6e 6521 0000  ......G00dOne!..
0062590: 0000 0000 0000 0029 2208 1029 2208 0a00  .......)"..)"...
00625a0: 0000 0100 0000 0000 0000 0000 0000 6e74  ..............nt
00625b0: 646f 6d61 696e 4034 0000 0000 0000 5241  domain@4......RA
00625c0: 5849 5343 4c4f 5544 0000 0000 0000 3829  XISCLOUD......8)
00625d0: 2208 4829 2208 0500 0000 0100 0000 0000  ".H)"...........
00625e0: 0000 1200 0000 6e74 7573 6572 4034 0003  ......ntuser@4..
00625f0: 0000 0000 0000 616c 6963 6500 0000 6829  ......alice...h)
0062600: 2208 182a 2208 0a00 0000 0100 0100 0000  "..*"...........
0062610: 0000 0000 0000 6e74 646f 6d61 696e 00ff  ......ntdomain..
mpuckett@exch1:~/mpvenafi$
```

Figure 2: User and Password Extracted from Juniper VPN Using Heartbleed

Now that PowerMonkey has access to the corporate VPN, she realizes the hard part is now over. Once she breaches a perimeter and has gained network access, there are always vulnerabilities or misconfigurations available.

3. Expanding Access with Stolen or Created SSH keys, VPN Credentials, and Other Backdoors

Mapping the Network

The first thing PowerMonkey does is an Nmap scan of the network range that was assigned by the VPN, and, subsequently, several ping scans of network ranges that she assumes may be in use. After a few hours of research using tools like nmap, ping, and nbtstat, and a basic web browser, she is able to build a network topology map indicating the server subnet, workstations, and even some branch offices. This information is exactly what she needs to continue her mission.

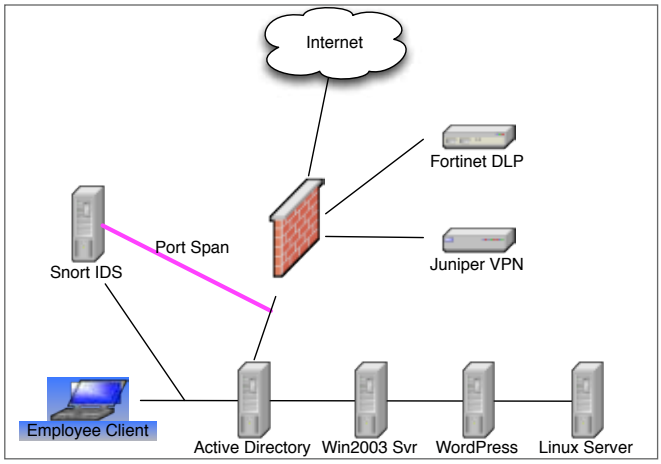


Figure 3: Network Map Created by PowerMonkey Using Basic Tools

Accessing Administrator Credentials

One of the hosts she locates in her research has an operating system fingerprint of a Windows 2003 server. When companies use old operating systems to support legacy applications, the systems are often unpatched due to risk to the application (i.e., application vendors do not support new patches to the underlying systems), and the company is either unwilling to pay for the upgrades or no upgrades exist. Regardless of why Company A uses this server, she knows this is the place to start.

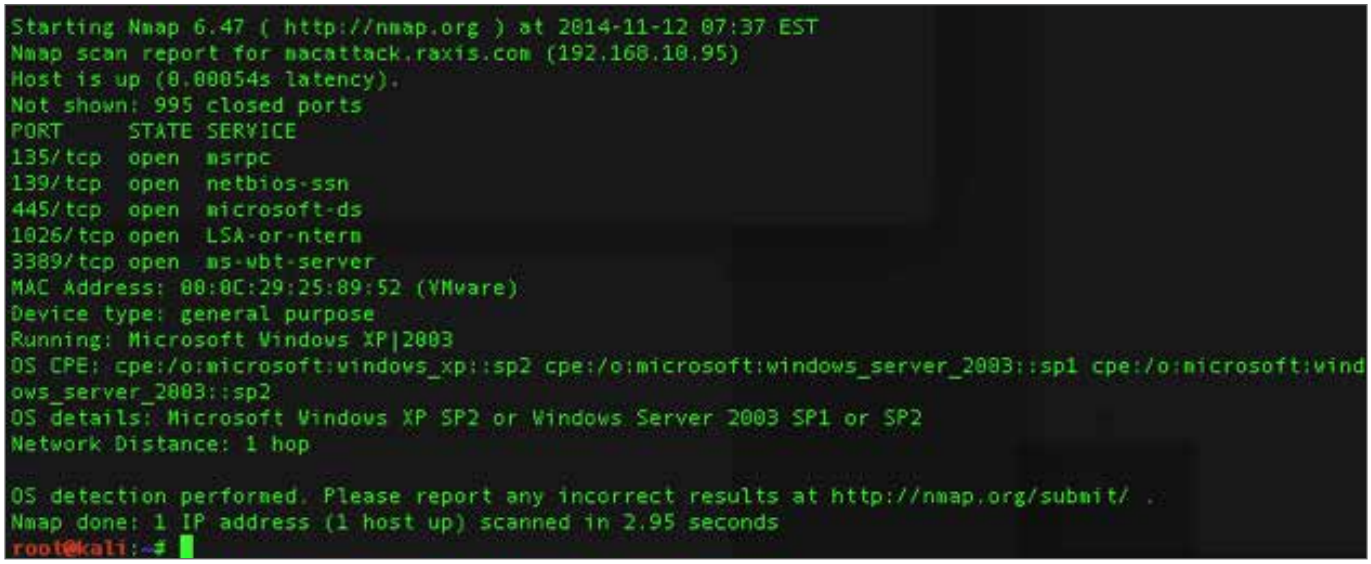


Figure 4: Internal Windows 2003 Server Located

Metasploit, penetration-testing software, fires up on her Kali Linux VM session. Unless it is a new zero-day tool that her research team has developed, many of the tools she uses are available to anyone online. PowerMonkey creates a few configuration settings for Metasploit, including loading the MS08-067 exploit module. She has used this exploit at least 20 times in the past two years, so it is easy to do. After execution, she has a Meterpreter prompt. Using Meterpreter, PowerMonkey attempts to pull down the cached credentials stored on the system. She realizes that the Windows 2003 server is not part of the domain, further reinforcing her suspicion that it is an unpatched system due to application incompatibility. The company does not want to risk the production domain with this weak system. However, PowerMonkey knows that if she can find administrator credentials on this system, these credentials are often also used on systems on the production domain that host confidential information.

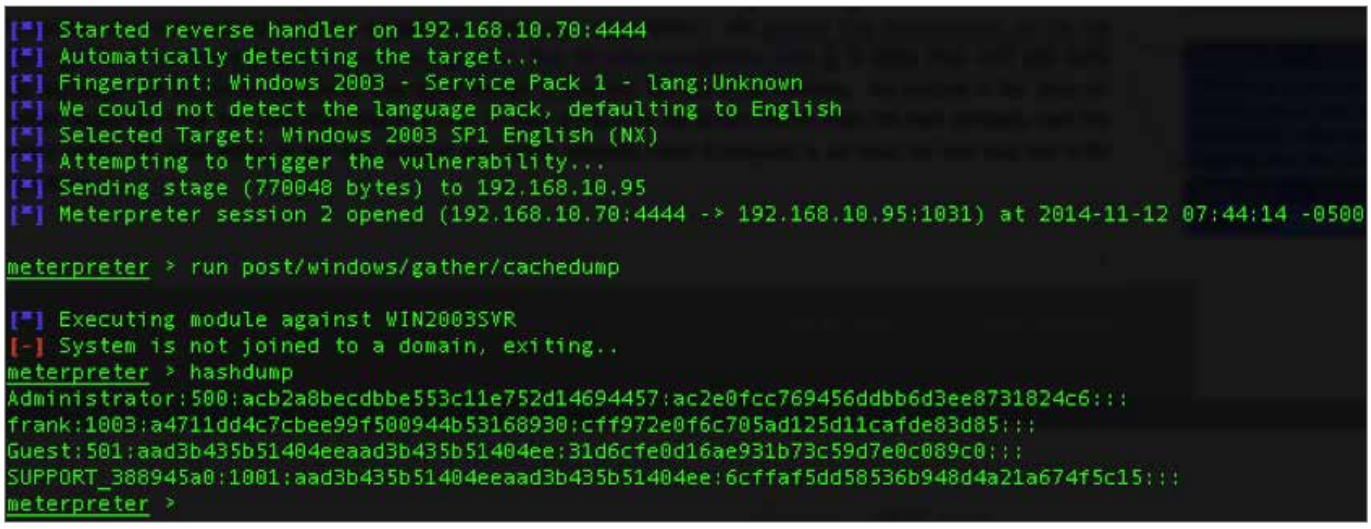


Figure 5: Local Windows 2003 Server Hashes Accessed

She discovers a user "Frank" who is likely a domain administrator since he has a local account. In order to see where these credentials can take her, PowerMonkey sends the credentials off to the hash cracking team within her organization. The hash cracking team has specialized hardware with multiple GPUs for performing advanced rule-based dictionary attacks. She knows they use hashcat, which is available to anyone for free. In this case, they used a LANMAN hash, so it would not be a tough password to crack—in a matter of minutes, she receives an email with the password. She later learns it took the team 39 seconds to break Frank's password.

```
cff972e0f6c705ad125d11cafde83d85:f00tb@ll
[s]tatus [p]ause [r]esume [b]ypass [q]uit =>


INFO: approaching final keyspace, workload adjusted


Session.Name...: cudaHashcat
Status.........: Exhausted
Rules.Type.....: File (rules/toggles5.rule)
Input.Mode.....: File (rockyou.txt)
Hash.Target....: File (win2003hashes.txt)
Hash.Type......: NTLM
Time.Started...: Wed Nov 12 07:54:42 2014 (39 secs)
Time.Estimated.: 0 secs
Speed.GPU.#1...:   948.7 MH/s
Speed.GPU.#2...:   934.7 MH/s
Speed.GPU.#*...:  1883.4 MH/s
Recovered......: 2/4 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.......: 70898912128/70898912128 (100.00%)
Skipped........: 0/70898912128 (0.00%)
Rejected.......: 7903857/70898912128 (0.01%)
HWMon.GPU.#1...:  0% Util, 44c Temp, N/A Fan
HWMon.GPU.#2...:  0% Util, 51c Temp, N/A Fan

Started: Wed Nov 12 07:54:42 2014
Stopped: Wed Nov 12 07:55:24 2014
```

Figure 6: Dual GPU Password Cracker and Hashcat Breaks Password in 39 Seconds

Creating Additional Administrator Credentials

PowerMonkey opens up Remote Desktop on her computer and connects to an Active Directory (AD) domain controller she has mapped out using Frank's newly obtained password. As she suspected, he used the same password for both systems. She has more tools she could use to gain domain access, but she sees something this simple over and over. Using access to the domain controller, she quickly creates an account for herself and assigns it to the NetworkAdmin group she found earlier, stopping short of adding herself as a domain administrator. She has access to everything else though, including shares and management of some other servers. Companies frequently audit the domain administrators group, but she is not worried as there are many other ways she can retrieve it again if needed. This will be a huge step in maintaining long-term access to Company A for the Chinese government once she is done.

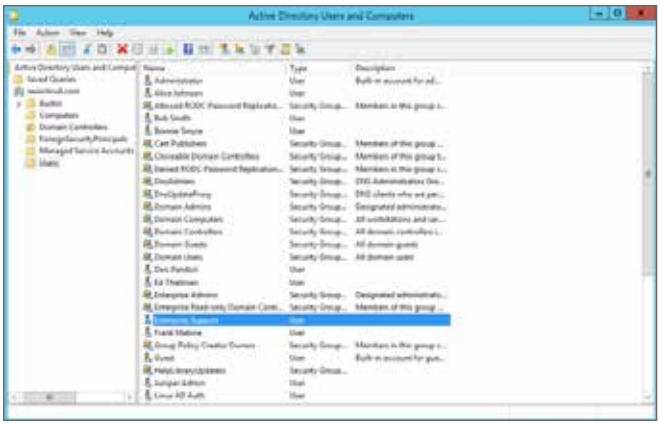


Figure 7: PowerMonkey Creates a User Account Called "Enterprise Support" with Access to Network Devices

Using Administrator Credentials to Steal Private Keys that Connect to Remote Systems

Since Frank is a domain administrator, he probably has access to other systems as well, so she searches for his workstation and locates it within the domain. Using his domain credentials, she connects to his personal laptop and searches for private keys. She finds several .pem files, which are private keys, to connect to remote systems. From her network scans, it appears that Company A uses a Virtual Private Cloud (VPC), and Amazon typically uses .pem files to connect to cloud hosted servers. After trying a few Linux systems she finds one that she believes is a VPC subnet. She finds that the key works on VAppSrv1, which is exactly the system she wants to access.

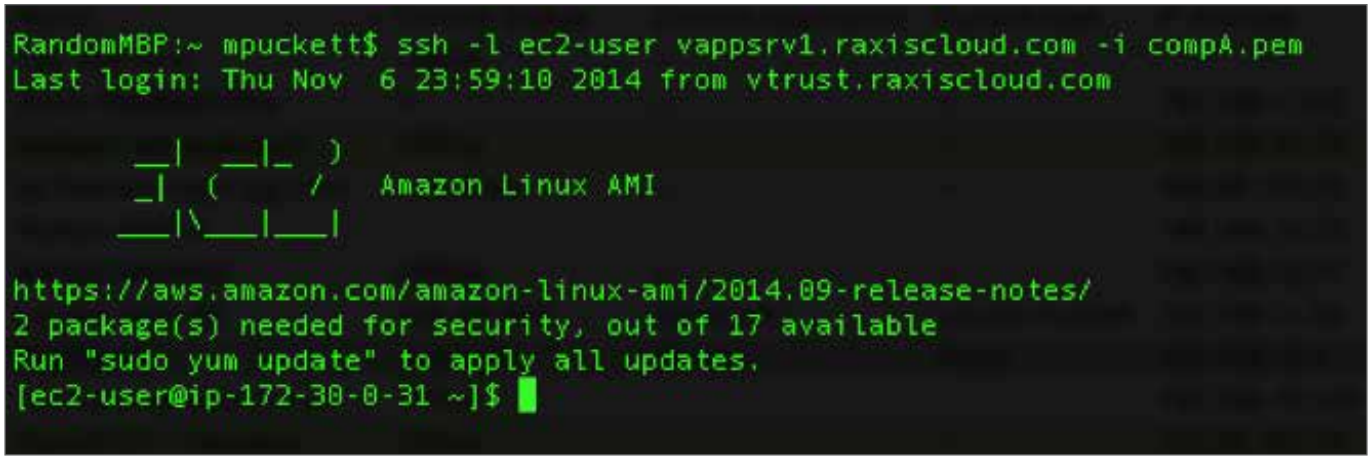


Figure 8: Access Gained to an Internal Linux Server via Stolen Private Key

Using the VPN Private Key to Decrypt Traffic and Access All Passwords

To deepen the foothold within Company A, PowerMonkey really wants to capture more passwords. She can certainly dump all of the hashes out of the Active Directory domain controller, but she thinks there may be a better way to get all of the passwords. Ideally, if she can use the Juniper private key to decrypt all of the traffic, she can get everyone's passwords, and then she will have, not only a stronger foothold, but also a way to log them all into the government password database for future use on other sites.

She connects to the Juniper VPN device management web interface and goes immediately to the troubleshooting tools. There she is able to configure tcpdump to capture traffic and decrypt it using the Juniper VPN's own private key. As the Juniper SSL VPN will be providing actual copies of the network traffic before it is processed by the server, this effectively allows PowerMonkey to conduct a man-in-the-middle attack and capture detailed logs of every single connection made.

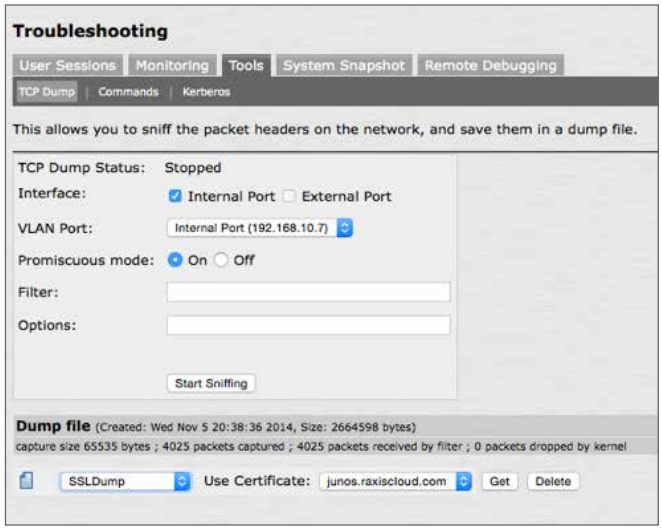


Figure 9: Juniper Tcpdump Utility and Certificate Decryption

Expanded Foothold with Stolen Keys and Credentials

Since the private key was used to decrypt the traffic, she can see everything inside the VPN sessions now. Particularly, she can see the VPN authentication, itself, along with the username and password. Now PowerMonkey has access to additional usernames and passwords without the need to exploit Heartbleed again. In the event the Heartbleed vulnerability gets patched, the decryption of the live traffic will continue to expose critical data.

```
    value           close_notify
16    0.1824 (0.0000)  C>S  TCP FIN
15 15 2.4622 (2.3588)  C>S  application_data
    ---------------------------------------------------------------
    POST /dana-na/auth/url_default/login.cgi HTTP/1.1
    Host: junos.raxiscloud.com
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:33.0) Gecko/20100101 Firefox/33.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Accept-Language: en-US,en;q=0.5
    Accept-Encoding: gzip, deflate
    Referer: https://junos.raxiscloud.com/dana-na/auth/url_default/welcome.cgi
    Cookie: lastRealm=Users; DSSIGNIN=url_default; DSSignInURL=/
    Connection: keep-alive
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 79

    tz_offset=-300&username=alice&password=C00dOne%21&realm=Users&btnSubmit=Sign+In----------
New TCP connection #18: 192.168.10.7(34205) <-> 172.30.0.172(389)
0.0294 (0.0294)  C>S
---------------------------------------------------------------
30 58 02 01 01 63 53 04 00 0a 01 00 0a 01 00 02    0X...cS.........
01 00 02 01 0f 01 01 00 87 0b 6f 62 6a 65 63 74    ..........object
63 6c 61 73 73 30 33 04 0f 6c 64 61 70 53 65 72    class03..ldapSer
76 69 63 65 4e 61 6d 65 04 0b 63 75 72 72 65 6e    viceName..curren
74 54 69 6d 65 04 13 73 63 68 65 6d 61 4e 61 6d    tTime..schemaNam
69 6e 67 43 6f 6e 74 65 78 74                      ingContext
---------------------------------------------------------------
```

Figure 10: Username and Password Revealed in Decrypted Traffic

Establishing New SSH Keys to Create Additional Backdoors to Targeted Systems

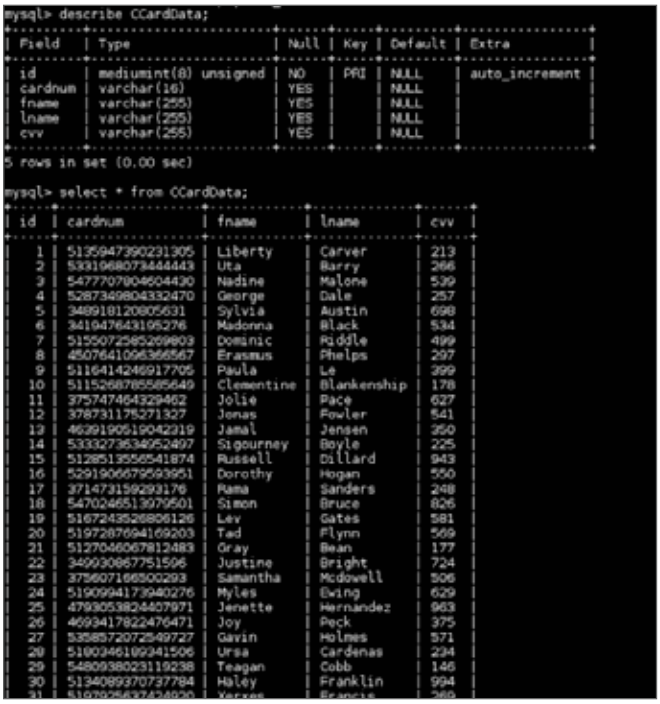
PowerMonkey is quite happy now; she has access to everything within Company A. Since they operate hospitals, she expects that they store both medical and financial data about their customers. She refers to the map she made of their infrastructure and websites, and she looks at the back-end servers until she finds that one houses databases. She maps out the database and quickly finds a large one that holds customer information. Now she is ready to perform data exfiltration of some confidential information to please her superiors. From her network topology map, she uses Frank's private key to access a Company A database server. She creates her own SSH private key and adds it to the authorized keys file in root's home directory. This will make sure she has access in the future if needed.

```
[root@ip-172-30-0-31 .ssh]# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCspuYgyM4KufuYfb0XzCCb+sGOvdzkqGG2WFWMJEbkvbUbfbivBPnFRE
7UoYeOI8CusDOoeHmc5rHgx6gC5vwnSNuNNLnhTOp/faiCADaYZ1d4BeMtXue6egKw+MzT1ZlDBbY3RwlytPpi7Gh7502V
C5QIjR1Gf8BAbSria4CGKWY4tALPrBQGSHJXWB+bckmxg9YIxut2yxRFVakz+aySH1qVjtXpeFar9XyS8k7hfvjqmnevDH
WqhLb0FMFM76mDWPAUhrkXOyh4X+Yw3HWAhgLpO594bsMgASHp8/iqkE3F3pcjvO5JzR51UfsUzA0tGfP8u6X5rycy+EM4
qK9T glacier
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCqIouh0tJsWdLGK3cxMGDOZ7xkOvdzb4iPKf2KLuMRZ2VyKxvNjGVYJv
yNX0OjSrG+/l6mKzAwqlVfjHQOAPV7EsrQTiN+IzSV/KAM/OAFuGOJ+5Ld4vn+WcCM0XaL0kVQSt5gmULQmG0z7zqxfVMg
13nMnk4DXEtiYp/NootyuFxzXnN93+rQzN/TFhyUc4SlxN/zOAhGXXKMpLbFgN27lI9Zj3Wz32VA/UvRvqxNbYqtGZ/x9P
Ivat78ATiIRQNeiNoE2zYDD9dqfoei1lucsWYwcNW7ZdckoIi9ey1d6O1VHozWjkNtR7VAiFckyRP1xp3YABd5HWxgmYNU
q72F entsup
[root@ip-172-30-0-31 .ssh]#
```

Figure 11: New "Entsup" Key Added for Future Access

4. Exfiltrating Data Using SSL to Bypass Security Controls and Stolen Keys for Decryption

Now that the foothold is solid, PowerMonkey starts looking around the database on this server. A quick "show databases" command reveals several databases, including one called "payment_info." After running a few more commands, she finds that there is indeed some valuable information here that is worth capturing.

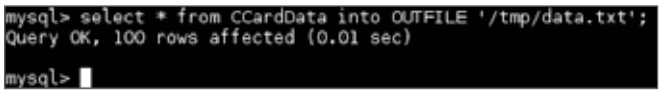


```
mysql> describe CCardData;
+---------+-----------------------+------+-----+---------+----------------+
| Field   | Type                  | Null | Key | Default | Extra          |
+---------+-----------------------+------+-----+---------+----------------+
| id      | mediumint(8) unsigned | NO   | PRI | NULL    | auto_increment |
| cardnum | varchar(16)           | YES  |     | NULL    |                |
| fname   | varchar(255)          | YES  |     | NULL    |                |
| lname   | varchar(255)          | YES  |     | NULL    |                |
| cvv     | varchar(255)          | YES  |     | NULL    |                |
+---------+-----------------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)

mysql> select * from CCardData;
+-----+------------------+-----------+-------------+-----+
| id  | cardnum          | fname     | lname       | cvv |
+-----+------------------+-----------+-------------+-----+
|   1 | 5135947390231305 | Liberty   | Carver      | 213 |
|   2 | 5331068073444443 | Uta       | Barry       | 266 |
|   3 | 5477707804604430 | Nadine    | Malone      | 539 |
|   4 | 5287349804332470 | George    | Dale        | 257 |
|   5 | 348918120805631  | Sylvia    | Austin      | 698 |
|   6 | 3419476431082276 | Madonna   | Black       | 534 |
|   7 | 5155072585269803 | Dominic   | Riddle      | 499 |
|   8 | 4507641096366567 | Erasmus   | Phelps      | 297 |
|   9 | 5116414246917705 | Paula     | Le          | 399 |
|  10 | 5115268788585649 | Clementine| Blankenship | 178 |
|  11 | 375747464329462  | Jolie     | Pace        | 627 |
|  12 | 378731175271327  | Jonas     | Fowler      | 541 |
|  13 | 4639190519042319 | Jamal     | Jensen      | 350 |
|  14 | 5333273634952497 | Sigourney | Boyle       | 225 |
|  15 | 5128513556541874 | Russell   | Dillard     | 943 |
|  16 | 5291906679593951 | Dorothy   | Hogan       | 550 |
|  17 | 371473159293176  | Rama      | Sanders     | 248 |
|  18 | 5470246513079501 | Simon     | Bruce       | 826 |
|  19 | 5167243528806126 | Lev       | Gates       | 581 |
|  20 | 5197287694169203 | Ted       | Flynn       | 569 |
|  21 | 5127046067812483 | Gray      | Bean        | 177 |
|  22 | 349930867751506  | Justine   | Bright      | 724 |
|  23 | 375607166300293  | Samantha  | Mcdowell    | 506 |
|  24 | 5190994173940276 | Myles     | Ewing       | 629 |
|  25 | 4793053824407971 | Jenette   | Hernandez   | 983 |
|  26 | 4693417822476471 | Joy       | Peck        | 375 |
|  27 | 5388572072549727 | Gavin     | Holmes      | 571 |
|  28 | 5190346109341506 | Ursa      | Cardenas    | 234 |
|  29 | 5480938023119238 | Teagan    | Cobb        | 146 |
|  30 | 5134089370737784 | Haley     | Franklin    | 994 |
|  31 | 5197025637434020 | Xerxes    | Francis     | 269 |
```

Figure 12: Credit Cards Revealed from Database

PowerMonkey outputs the newly found data to a file, along with other data on patient records, customer addresses, and budgeting information. This information certainly will earn respect with her teammates and superiors.



```
mysql> select * from CCardData into OUTFILE '/tmp/data.txt';
Query OK, 100 rows affected (0.01 sec)

mysql>
```

Figure 13: Credit Card Data Exported to File

Thanks to Frank's original key, PowerMonkey exfiltrates the data using a new private key she creates on Company A's third-party SFTP server just for the job. She can now write a script to pull down data as she needs it and export it to the third-party server. She can then extract it remotely with very little suspicion, as the third-party server normally handles remote connections and will not be detected easily. She realizes that new connections using SFTP, SCP, or anything unusual from internal servers to the outside will be considered suspicious, but their own third-party server will not be suspected. The DLP system will certainly catch her if she does not encrypt the exfiltration data. So exfiltrating the data as encrypted traffic will conceal her actions, and, to be safe, she knows using her own key would be best.

Figure 14: New Private Key Created to Move Data to the Third-party Server

At this point, PowerMonkey has access to the database that houses Company A's most private data. She realizes that Company A owns and operates hospitals around the United States. They consolidate most of their medical and financial records in the system to which she has gained access. She downloads data pertaining to over four million patients and presents them to her manager. He passes the information on to his management for their goals of compromising American companies, and they are very pleased with the wide range of data that has been gathered as well as the ability to regain access. A few months later they request more data from Company A. The access methods still work and it appears that the previous breach was not even noticed. After the success of this attack, they decide to use these same methods with other American companies. These methods can easily be used on a larger scale to cause harm to the American economy.

Company A:
Breached Organization without Key and Certificate Security

Company A owns and operates over two hundred hospitals, and it continues to grow. The company saves money and increases efficiency by centralizing its computer systems. Because of the sensitive nature of the medical records that it houses in its databases, Company A has a number of security controls in place to protect its perimeter and endpoints.

The systems at Company A are similar to many other companies in the Fortune 500. The company has Snort IDS on the inside, a Fortinet based DLP solution to monitor for data theft, and a Juniper VPN solution for remote workers. The company operates a traditional firewall model to separate the outside Internet from its internal systems, and it utilizes a DMZ for Internet-facing servers.

Discovery of the Breach

On this particular morning, Bob, an IT security manager, alerts the entire IT management team that he received a call from their bank processor indicating that there appeared to be a large number of fraudulent charges made from cards that were used previously at Company A. Often a third-party, and not the victimized company, initially discovers a breach by noticing suspicious or unusual transactions.

Bob and his colleagues subsequently search logs to see what other systems have been affected and how often. The logs show them very little; they see some connections to servers by their systems administrator, Frank, but nothing appears out of the ordinary.

As Bob has always stayed on top of IT security trends and has been quick to implement the latest tools for boundary and endpoint protection, including firewalls, DLP, AV, IAM, VPN, and IPS/IDS systems, he is left wondering how this could have happened. Was this an Advanced Persistent Threat, and, if so, why and how did they get in? He knows that modern threats are far more advanced than what they were just a few years ago, but he thought his layers of security controls would protect the company. Regardless of who did this hack, he is now faced with having to figure out how to get the hackers completely eradicated from Company A.

Bob and the management team at Company A quickly alert the authorities and hire a forensics firm to handle the internal investigation. They work closely with their public relations department to build a strategy to contact and calm customers whose data may have been stolen. The cost to Company A cannot be calculated until the forensics firm assesses the amounts and types of data that were stolen and until time goes by and shows how much of a PR backlash occurs.

A Strong Foothold within the Corporate Network

The forensics firm finds evidence in system logs that someone has been logging into their corporate VPN with a Chinese source IP address. They have no evidence on how the breach happened, as the Juniper VPN software was completely up to date with all patches at the time of the login, and it had been regularly updated for quite some time. The forensics team found the username “Alice” was used to gain access to the VPN. Upon review of Alice’s workstation, she has all patches, the antivirus product is working and updated, and Alice has not once used her laptop to click on any links that were outside of the company. The forensics firm determined that phishing was not the method of intrusion, and cited the method used to obtain Alice’s password to the VPN as unknown.

In order to determine the extent of the breach, the forensics firm pours through logs from every server and system. The forensics firm begins correlating time with events on multiple systems and is able to find connections from a VPN reserved IP for user “Alice” logging into some servers as “Frank.” The command history and database log files were cleaned up, but there was enough suspicious behavior by the person using the Chinese source IP to conclude that she was doing something that she wanted to hide. Whoever this was, she reached the credit card database and possibly other databases, and she was extremely careful in covering her tracks. As the analysis is completed, the forensics team notes that a legacy Windows 2003 server may have been the source of Frank’s password.

Bypassed Critical Security Controls

How did they get in? Other than a few connections from their third-party SFTP server and some firewall logs on the VPN, there wasn't much left behind other than a Chinese IP address. After searching back through firewall and Juniper SSL VPN logs, connections from China were noted to the VPN system over port 443 and there were correlating VPN valid logins using the username "Alice." Another piece of interesting data is that the firewall reported connections to 443 for at least an entire day before the valid login occurred in the Juniper SSL VPN logs. How could this happen? By default, the Juniper SSL VPN was recording every login and failed login connection to the SSL VPN, but the logs weren't showing any correlating attempts until "Alice" connected 24 hours later. Bob knew that Alice had no reason to be connecting from China, so he felt certain that was the entry point.

Why did his Data Loss Prevention (DLP) and Intrusion Detection System (IDS) not catch these events? Bob had DLP set up to capture and stop any transmission of credit card data to outside of the company, but, still, the hacker dumped actual credit card numbers out and DLP never produced a single alert. Encryption immediately comes to mind as he found the rogue keys on the SFTP server. *The hacker must have encrypted everything using rogue keys to and from the SFTP system to ensure DLP couldn't pick it up!* The hacker issued a self-signed key as well to avoid any key escrowed configuration on the DLP server.

Bob uses a Snort based IDS with a subscribed feed to ensure he has the latest signatures. This IDS system is located just behind the firewall and monitors all traffic that is permitted through the firewall. IDS did not show anything out of the ordinary on the inside, and his Managed Security Service reported nothing out of the ordinary over the past several months. However, these systems also do not monitor encrypted traffic.

Developing a Recovery Plan that Includes New Keys and Certificates

With the forensics report, Bob begins to plan how systems need to be rebuilt from known clean backups or by completely rebuilding the system. Active Directory servers, Unix password files, DMZ hosts, and the VPN system are certainly the first systems he must examine. But he also realizes that every single cryptographic key in his organization is now considered compromised. If he builds new servers with the old keys, they cannot be trusted. What if the hacker created new keys too, and those keys got migrated over to the new server? There is not an easy way to tell the difference between rogue keys and real keys. He must start over from the beginning by establishing all new keys and certificates.

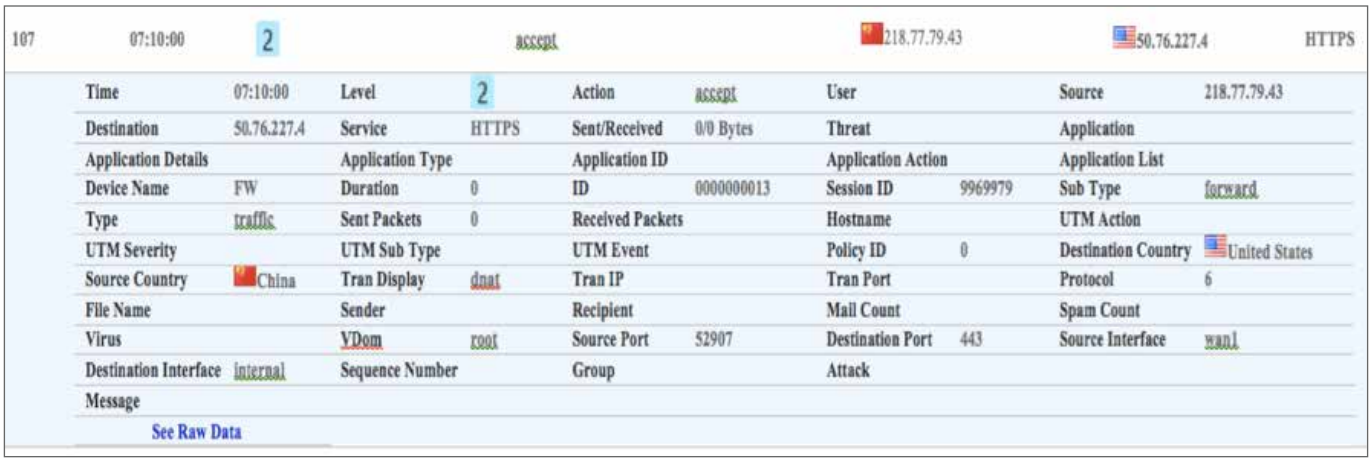
Every certificate, every key...how would he replace them all in a reasonable amount of time? To help with remediation, and determined not to make the same mistake twice, Bob immediately begins to search for a better solution to manage his keys and certificates, as well as to provide discovery for rogue keys.

The Aftermath

Bob still has no idea what hit Company A so hard. It took his organization months to remediate and issue new keys and certificates across the network. But how did they get in? There wasn't much left behind other than a Chinese IP address. He knows the data was exfiltrated as the bank processor had hard evidence that the leak originated from Company A. Somehow, this hacker got inside Company A from the outside, but left no trace of her entry point.

Bob was juggling several potential theories in his head when it occurred to him…*since our infiltrator had used a valid account to the Juniper SSL VPN 24 hours after the first hits were received on the firewall, could this have been from a zero-day flaw?*

The password policy at Company A is very stringent. They require 90-day password rotations and complex passwords, and Alice's password was just changed the week before the access occurred. The chances of an attacker reusing Alice's password from some untrusted website is unlikely. Yet the attacker was able to connect to the VPN on the first attempt and gain access. This was not some sort of brute force access, and, with the very recent password change, Bob feels it could not have been a prior compromise that caused this. This stumps Bob and his IT team, until he is watching the news one morning and learns something new.



107	07:10:00	2		accept		218.77.79.43		50.76.227.4	HTTPS

Time	07:10:00	Level	2	Action	accept	User		Source	218.77.79.43
Destination	50.76.227.4	Service	HTTPS	Sent/Received	0/0 Bytes	Threat		Application	
Application Details		Application Type		Application ID		Application Action		Application List	
Device Name	FW	Duration	0	ID	0000000013	Session ID	9969979	Sub Type	forward
Type	traffic	Sent Packets	0	Received Packets		Hostname		UTM Action	
UTM Severity		UTM Sub Type		UTM Event		Policy ID	0	Destination Country	United States
Source Country	China	Tran Display	dnat	Tran IP		Tran Port		Protocol	6
File Name		Sender		Recipient		Mail Count		Spam Count	
Virus		VDom	root	Source Port	52907	Destination Port	443	Source Interface	wan1
Destination Interface	internal	Sequence Number		Group		Attack			
Message									

See Raw Data

Figure 15: Fortinet UTM Firewall Logs Showed Connections to Juniper SSL VPN Over 24 Hours before the First Valid Login

Heartbleed Vulnerability Announced

On April 7, 2014, Bob learns about a security vulnerability, called "Heartbleed," that impacts OpenSSL which secures customer information on some systems. Remembering that the very first connections from China were on the Juniper SSL VPN and the attacker did not connect until about 24 hours later, his suspicions grow quickly. Juniper announced their devices were affected and was able to confirm that log entries were not recorded for Heartbleed attempts.

Bob is relieved to finally solve the puzzle, but then he is left discouraged when he realizes that there was nothing he could have done to detect or stop this attack. However, Bob then realizes that he can update his security measures so that if this type of attack happens again, he can avoid the manual remediation efforts that took months to finalize. He begins looking for a solution that will provide a more proactive defense and automated remediation of key and certificate issues for any future breaches.

Company B:
Attacked Organization that Uses Venafi Trust Protection Platform

Company B, like Company A, relies heavily on keys and certificates to encrypt and secure its customers' private financial and medical records. Company B also implemented similar security controls—IDS, DLP, Juniper VPN, firewalls, and a DMZ.

However, there is one significant difference in the companies' security environments. Company B's IT security manager, John, has implemented an automated key and certificate management and security solution. He recognized that if (or when) a breach occurs, the process to replace all keys and certificates would be a slow, manual one that could shut down hospitals and cancel critical care. He sought a key and certificate management and security solution that would eliminate these manual processes and deliver fast remediation when needed.

After researching the company's options, John implemented Venafi Trust Protection Platform™. He deployed Venafi TrustAuthority™ and Venafi TrustForce™, as part of the Trust Protection Platform for complete visibility into Company B's key and certificate inventory. The TrustAuthority discovery tool was implemented. Once the company's complete key and certificate inventory was created, John used Venafi to establish a baseline of normal usage so that any misuse, including an attack, would be recognized quickly. The Trust Protection Platform is used to enforce Company B's policies and is ready to respond immediately and remediate key and certificate misuse. John realizes that this significantly reduces risk to Company B as he has control of the encrypted traffic used within the company.

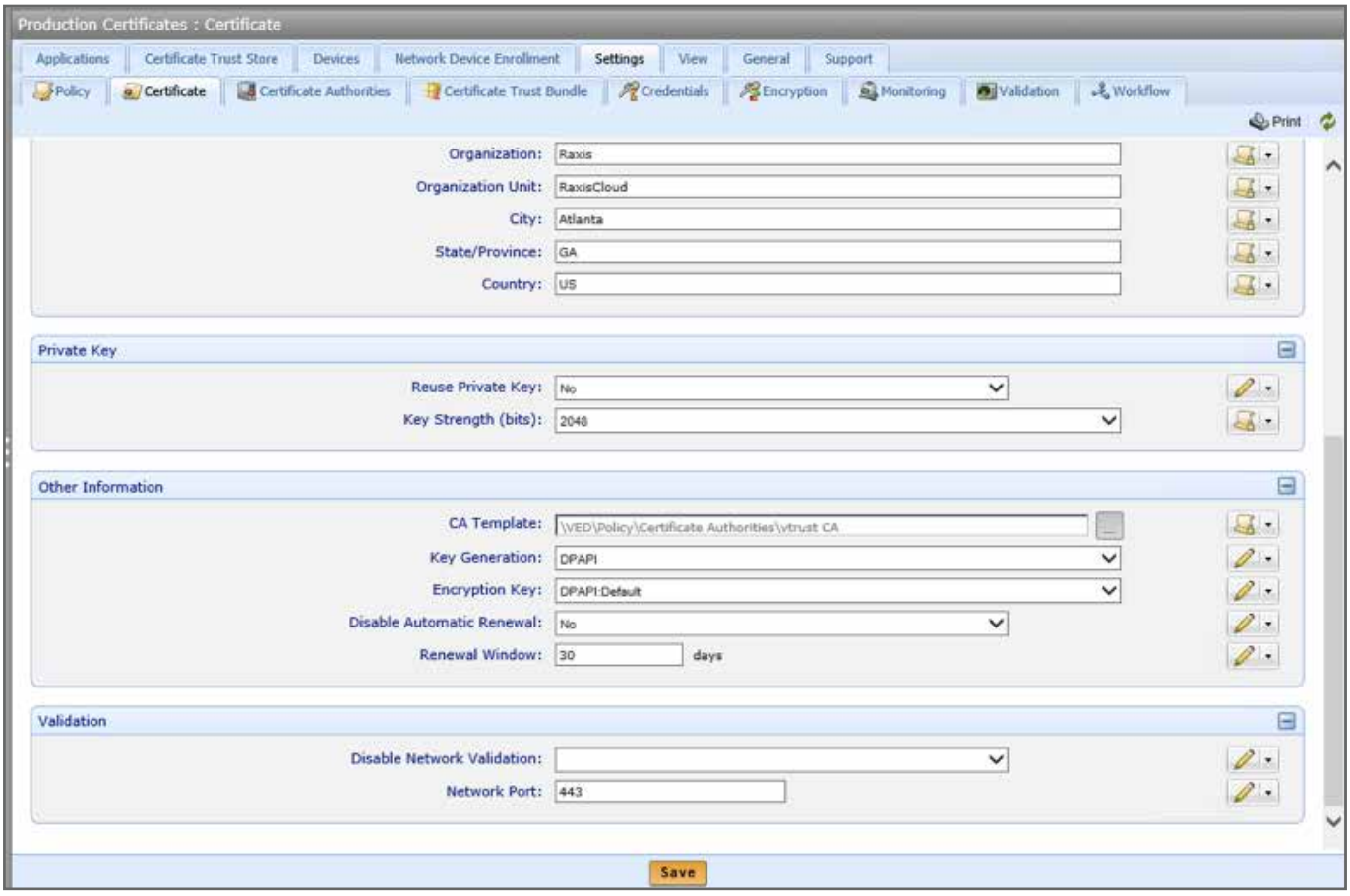


Figure 16: Certificate Defaults Configured for Company B

During the deployment process, John configured the certificate policy to enforce a number of elements, such as key strength and approval workflow processes. This ensures that the certificates used within Company B adhere to the company's security policy.

Discovery of the Breach and Immediate Remediation

When a similar attack is made on Company B, John alerts the entire IT management team that he received a call from the company's bank processor that a large number of fraudulent charges were made from cards that were used prior at Company B. John and his colleagues subsequently search logs to see what other systems have been affected and how often.

While the research on the potential breach is continuing, John decides to rotate all of the keys and certificates used within Company B while also resetting all passwords. After a breach, everyone knows to reset all of the passwords, as the hashes were likely stolen for offline cracking and subsequent password reuse. Since certificates are another important authentication control, it is clear to John that every single certificate and private key should be considered compromised as well, especially with phishing and mobile attacks on the rise.

Although John does not yet know how the hackers gained access, John knows keys and certificates can be misused to breach Company B. By compromising a workstation that accesses Company B, attackers can then capture traffic from a man-in-the-middle attack. The captured data could be decrypted using Company B's keys. The complete replacement of all keys and certificates is the only way John can have certainty that his authentication and encryption controls are healthy once again. But with hundreds, if not thousands, of certificates across Company B, without Venafi, he would have delayed this remediation until he had received breach confirmation and forensic guidance—leaving the company vulnerable during this time.

Fortunately John had installed Venafi. Each and every certificate is managed, configured properly, and included in a comprehensive inventory. Before there is even confirmation of a breach, John is able to use Venafi TrustForce to automatically issue new keys and certificates and revoke old ones—in just a few clicks and in just a few hours John has prevented any further traffic from being monitored by attackers.

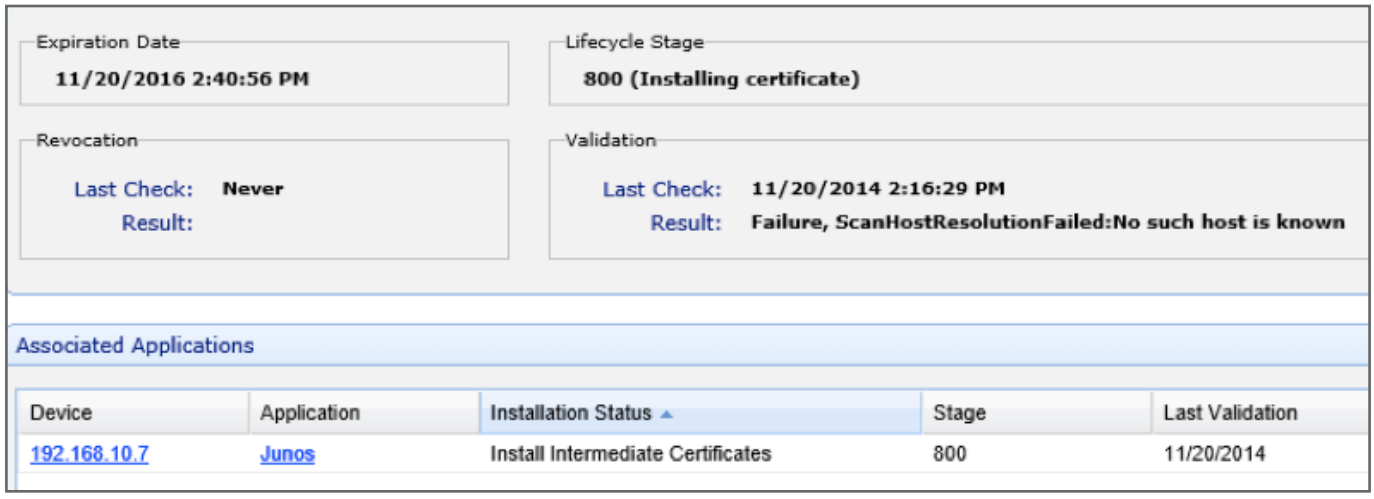


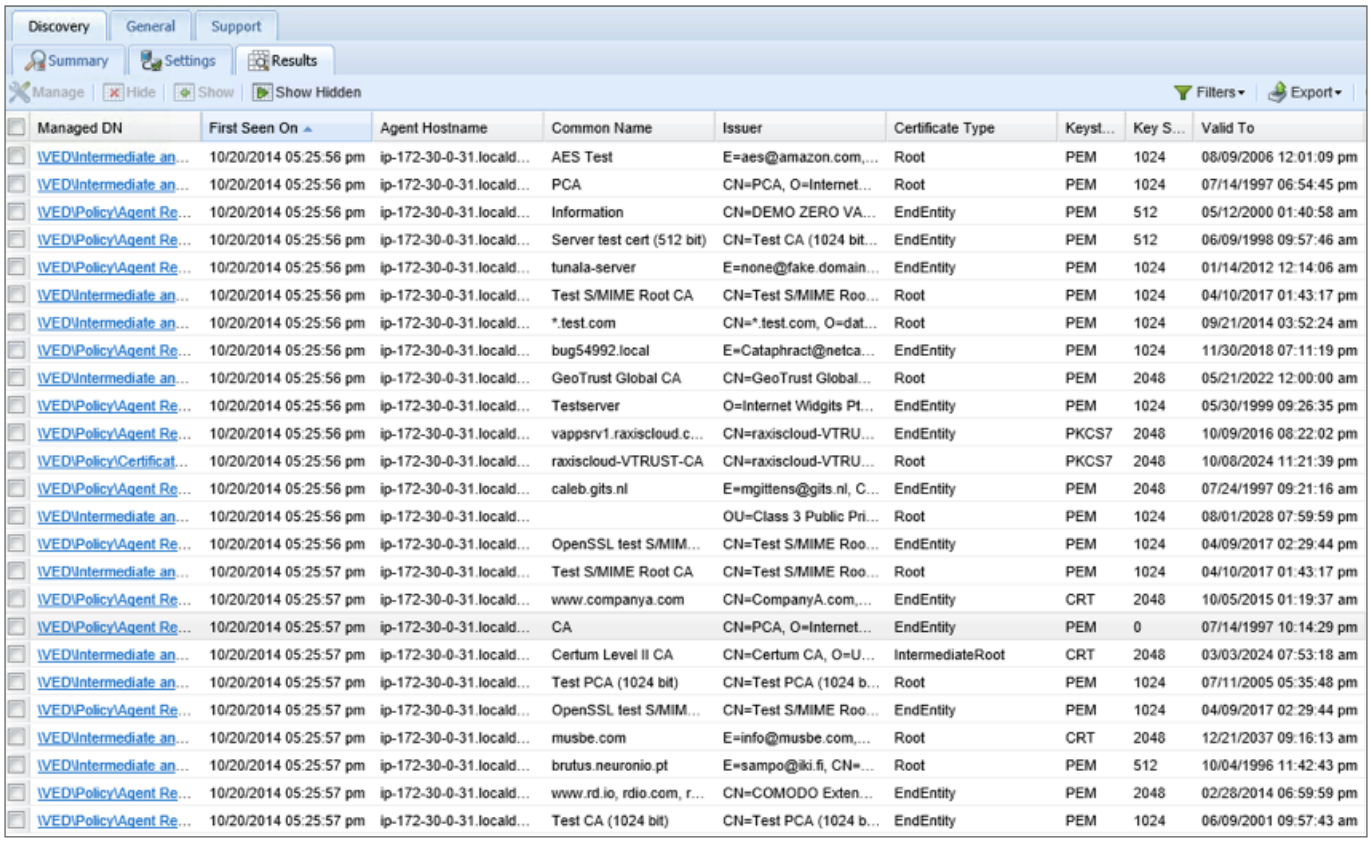
Figure 17: Certificate Re-issued for Juniper VPN Results of Forensic Efforts

Results of Forensic Efforts

John receives the results from the research, including reports from Venafi. With Venafi, he easily discovers that two rogue certificates were installed on Company B's systems because they violated Company B's certificate policies and were identified as anomalous compared to the company's baseline use. One unauthorized certificate was on the third-party SFTP server. The second certificate was installed on an SSH server to allow for shell access without using the VPN. These actions show that this hacker was persistent and wanted to remain in Company B's environment for the long term.

Bolstering Protection

John could have used Venafi to target his remediation efforts to the rogue certificates. Venafi Trust Protection Platform identifies rouge self-signed certificates, allowing John to remove these from the system. However in this case, John had already rotated all keys and certificates, blocking the attackers from any further use of keys and certificates to breach the organization.



Discovery | General | Support

Summary | Settings | Results

Manage | Hide | Show | Show Hidden | Filters | Export

Managed DN	First Seen On	Agent Hostname	Common Name	Issuer	Certificate Type	Keyst...	Key S...	Valid To
\VED\Intermediate an...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	AES Test	E=aes@amazon.com,...	Root	PEM	1024	08/09/2006 12:01:09 pm
\VED\Intermediate an...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	PCA	CN=PCA, O=Internet...	Root	PEM	1024	07/14/1997 06:54:45 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	Information	CN=DEMO ZERO VA...	EndEntity	PEM	512	05/12/2000 01:40:58 am
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	Server test cert (512 bit)	CN=Test CA (1024 bit...	EndEntity	PEM	512	06/09/1998 09:57:46 am
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	tunala-server	E=none@fake.domain...	EndEntity	PEM	1024	01/14/2012 12:14:06 am
\VED\Intermediate an...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	Test S/MIME Root CA	CN=Test S/MIME Roo...	Root	PEM	1024	04/10/2017 01:43:17 pm
\VED\Intermediate an...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	*.test.com	CN=*.test.com, O=dat...	Root	PEM	1024	09/21/2014 03:52:24 am
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	bug54992.local	E=Cataphract@netca...	EndEntity	PEM	1024	11/30/2018 07:11:19 pm
\VED\Intermediate an...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	GeoTrust Global CA	CN=GeoTrust Global...	Root	PEM	2048	05/21/2022 12:00:00 am
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	Testserver	O=Internet Widgits Pt...	EndEntity	PEM	1024	05/30/1999 09:26:35 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	vappsrv1.raxiscloud.c...	CN=raxiscloud-VTRU...	EndEntity	PKCS7	2048	10/09/2016 08:22:02 pm
\VED\Policy\Certificat...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	raxiscloud-VTRUST-CA	CN=raxiscloud-VTRU...	Root	PKCS7	2048	10/08/2024 11:21:39 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	caleb.gits.nl	E=mgittens@gits.nl, C...	EndEntity	PEM	2048	07/24/1997 09:21:16 am
\VED\Intermediate an...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...		OU=Class 3 Public Pri...	Root	PEM	1024	08/01/2028 07:59:59 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:56 pm	ip-172-30-0-31.locald...	OpenSSL test S/MIM...	CN=Test S/MIME Roo...	EndEntity	PEM	1024	04/09/2017 02:29:44 pm
\VED\Intermediate an...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	Test S/MIME Root CA	CN=Test S/MIME Roo...	Root	PEM	1024	04/10/2017 01:43:17 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	www.companya.com	CN=CompanyA.com,...	EndEntity	CRT	2048	10/05/2015 01:19:37 am
\VED\Policy\Agent Re...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	CA	CN=PCA, O=Internet...	EndEntity	PEM	0	07/14/1997 10:14:29 pm
\VED\Intermediate an...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	Certum Level II CA	CN=Certum CA, O=U...	IntermediateRoot	CRT	2048	03/03/2024 07:53:18 am
\VED\Intermediate an...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	Test PCA (1024 bit)	CN=Test PCA (1024 b...	Root	PEM	1024	07/11/2005 05:35:48 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	OpenSSL test S/MIM...	CN=Test S/MIME Roo...	EndEntity	PEM	1024	04/09/2017 02:29:44 pm
\VED\Intermediate an...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	musbe.com	E=info@musbe.com,...	Root	CRT	2048	12/21/2037 09:16:13 am
\VED\Intermediate an...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	brutus.neuronio.pt	E=sampo@iki.fi, CN=...	Root	PEM	512	10/04/1996 11:42:43 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	www.rd.io, rdio.com, r...	CN=COMODO Exten...	EndEntity	PEM	2048	02/28/2014 06:59:59 pm
\VED\Policy\Agent Re...	10/20/2014 05:25:57 pm	ip-172-30-0-31.locald...	Test CA (1024 bit)	CN=Test PCA (1024 b...	EndEntity	PEM	1024	06/09/2001 09:57:43 am

Figure 18: Certificate Discovery Can Locate Rogue or Unauthorized Keys

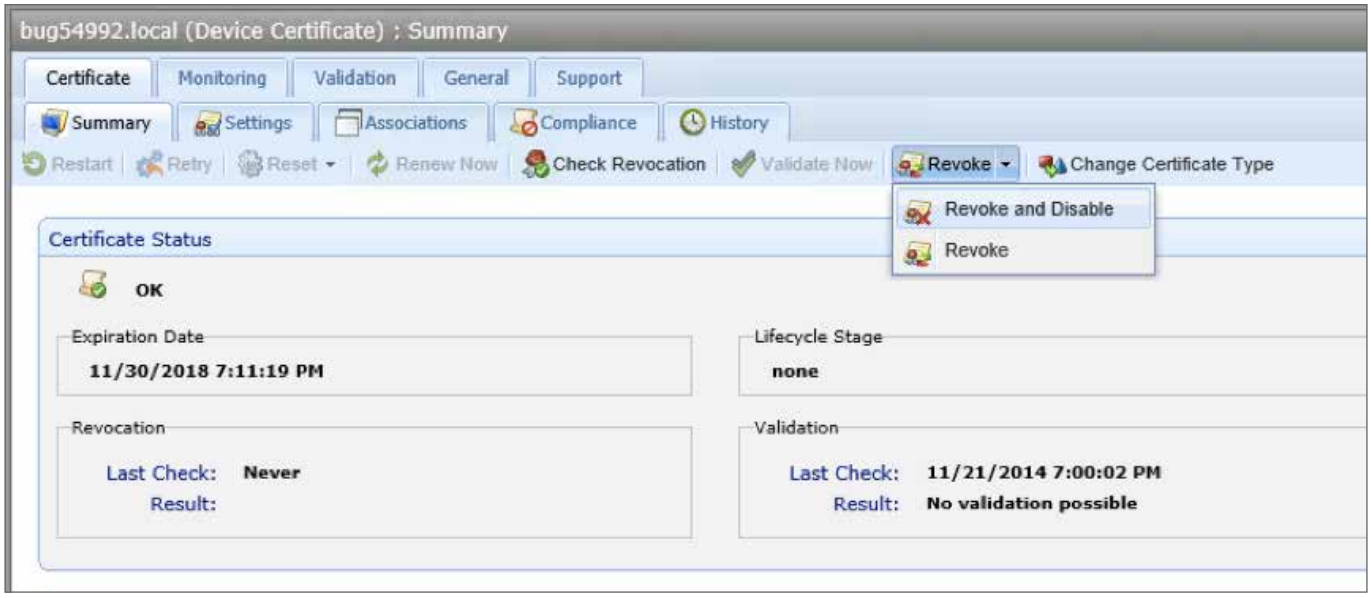


Figure 19: Revoking and Disabling an Unauthorized Certificate

It occurs to John that the rogue certificate and keys on the third-party SFTP server may have been used to exfiltrate data found within the company. The logs do not show anything, but the logs could have been cleared, or the hackers could have used a different mechanism and simply left the key for a path back in.

With Venafi certificate and key management and security in place, John had been planning an SSL/TLS traffic decryption project. After realizing that the attackers in this recent breach could have been using SSL encryption to hide their actions and exfiltrate data, John decides to expedite the project. Venafi integrates with his dedicated decryption appliance and his security systems. He will use Venafi to automatically distribute and validate private key delivery to these systems, allowing him to decrypt SSL traffic and pass the content to security devices for further processing, analysis, and policy administration. This will eliminate Company B's SSL/TLS security blind spot in its threat detection strategy.

John has also heard that Venafi now offers a new certificate reputation service. He learns that Venafi TrustNet™ is a global key and certificate reputation service that identifies rogue or anomalous key and certificate usage. With the certificate reputation established, TrustNet then enables immediate remediation by whitelisting trusted CAs and certificates, and blacklisting untrusted ones. With TrustNet, John can ensure that certificates issued by his enterprise are not misused and can also protect Company B against misused certificates from external sources as well.

John decides to deploy Venafi TrustNet for a more proactive security approach and to enable accelerated remediation in the event of another breach through its blacklisting capabilities. TrustNet will enhance the deployment of the other Venafi products, providing certificate reputation intelligence to the key and certificate management and security processes. With TrustNet, John will be better able to protect the business and retain trust in the company's brand.

Heartbleed Vulnerability Announced

After the Heartbleed vulnerability announcement, John's team immediately begins locating impacted systems. They upgrade code on all impacted systems and patch the vulnerability. To ensure they do not miss anything, they implement the Heartbleed plugin for Venafi TrustAuthority that detects systems subject to the vulnerability and scan the entire environment. John's team also rotates all of their certificates and keys to ensure full remediation. John's team is able to conduct the full Heartbleed remediation in just one week.

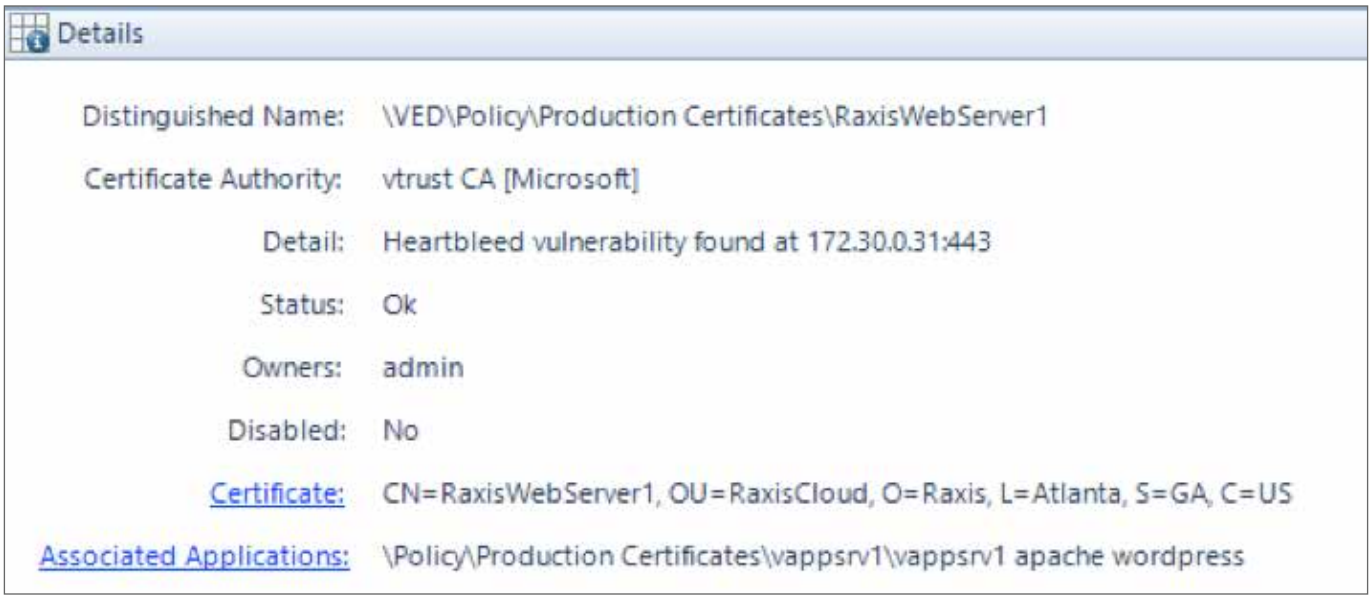


Figure 20: Venafi TrustAuthority Plugin for Detecting Systems Vulnerable to Heartbleed

There was still an open investigation with the FBI; however, John knew that there was not much anyone could do since the attack originated from China. However, since John remediated all of the vulnerable systems, revoked the unauthorized certificates, and effectively removed all back doors created by the unauthorized user, John could confidently close this issue.

Traditional Security Controls Are Not Enough

Protecting Keys and Certificates is an Everyday Business Requirement

The rise in cyberattacks and the growing concerns and regulations over data privacy are combining to compel the increased use of cryptographic keys and digital certificates. Whether used with internal networks, client-server, mobile, or cloud-based, certificates and keys are the foundation of trust for all critical systems and interactions with customers and partners. As an integral part of daily operations, keys and certificates are now a common practice across any business that wants to conduct transactions over the Internet.

However, attackers are now turning to keys and certificates as an often-unprotected source of attack that provides the trusted status bad guys need. Most organizations do not know how many keys and certificates they have, where they are located, how they are used, or who owns them. They have no formal business process or tools to keep track of how encrypted traffic and keys are used throughout the company. Many employ manual tracking methods such as spreadsheets, vulnerability scanners, or a Certificate Authority (CA), and are unable to successfully track the growing number of certificates or enforce policies. Even more troubling, security administrators are unable to recognize and respond to trust-based attacks that misuse keys and certificates.

Based on our testing and demonstrated remediation, we recommend Venafi Trust Protection Platform as a solution to these problems.

Venafi Trust Protection Platform

Venafi Trust Protection Platform™ manages and secures keys and certificates in the datacenter, on desktops, on mobile devices, and in the cloud. The platform supports Venafi TrustAuthority™, Venafi TrustForce™, and Venafi TrustNet™ and provides native integration with thousands of applications and common APIs for the extensive security ecosystem.

Venafi TrustAuthority

TrustAuthority identifies all keys and certificates across enterprise networks, out to the cloud, and for numerous Certificate Authorities (CAs). And this applies to multiple types of encryption assets, including SSL keys and certificates, SSH keys, and mobile and user certificates. TrustAuthority identifies key and certificate vulnerabilities, enforces policies and workflows, and detects anomalies with ongoing monitoring, establishing a well-regulated and visible state in which misuse can be easily detected.

Venafi TrustForce

TrustForce automates complex activities, such as rekeying and recertification. TrustForce also responds to suspicious anomalies by automatically replacing the vulnerable key or certificate. It replaces a certificate in seconds, integrating with dozens of CAs, and it remediates across thousands of certificates in just hours in the event of a CA compromise or new vulnerability such as Heartbleed. In addition, certificate whitelists are used to eliminate unnecessary risk from digital certificates signed by untrusted CAs. And TrustForce enables organizations to scale encryption-dependent applications by quickly and automatically deploying supporting keys and certificates.

Venafi TrustNet

TrustNet is a global key and certificate reputation service that identifies rogue or anomalous key and certificate usage. Certificate reputation is determined by a global sensor network, customers and partner feeds, and a highly refined scoring algorithm that is constantly tuned to address changes in the threatscape. With the reputation established, TrustNet then enables immediate remediation by whitelisting trusted CAs and certificates, and blacklisting untrusted ones. Organizations can ensure that certificates issued by their enterprise are not misused and can also protect themselves against misused certificates from external sources.

Together the platform and products provide Next Generation Trust Protection and enable enterprises to gain complete visibility into their key and certificate inventory, establish a baseline of normal usage, enforce enterprise policies and workflows, and respond to and remediate key and certificate anomalies.

Enterprises often view cryptographic keys and digital certificates as an operational issue. Venafi Trust Protection Platform does solve key and certificate management issues—such as preventing outages due to expired certificates, implementing PKI refreshes, managing mobile and user certificates, and much more. But enterprises need to start protecting keys and certificates as part of their

core security strategy. Otherwise, the trust their business depends on to operate is undermined, opening the door to successful attacks as demonstrated by our research. When keys and certificates are left unprotected, cybercriminals use them to be authenticated, evade detection, and keep their activities cloaked—these actions need to be quickly identified and remediated.

As shown in this case study, Venafi Trust Protection Platform enables enterprises to quickly detect any misuse of keys and certificates. Once detected, organizations can either apply focused remediation through blacklisting and automatic reissuance, or automate the rotation of all keys and certificates with the ability to reissue new ones and revoke old ones in just hours. Venafi also integrates with dedicated decryption appliances and security systems, enabling SSL/TLS inspection and revealing the numerous attacks that are hiding in SSL/TLS traffic.

Enterprises need to secure and protect their keys and certificates from all types of misuse—whether from errors, policy violations, or malicious intent. Vulnerabilities, like Heartbleed, are opening the door for attackers to access keys and certificates, and tools are readily available that enable APT operators to crack credentials in just seconds. Attackers are using these vulnerabilities and tools to bypass security controls that enterprises expect will mitigate these risks.

When protected, your keys and certificates preserve your trusted communications for all of your critical systems and your organization's interactions with customers and partners. Without Venafi, critical security controls are undermined, do not mitigate risk as expected, and do not achieve their intended goals. This is why security frameworks like SANS 20 have been updated to include requirements for understanding which keys and certificates are trusted and enforcing policies to secure them. With Next Generation Trust Protection from Venafi with powerful automated security, enterprises can now ensure critical controls are not undermined, increasing the effectiveness and value of an organization's overall security strategy.

About Raxis

Since 2005, the Raxis team of consultants are a unique group of highly specialized hackers, developers, and network engineers that together offer security services that are difficult to match. Our elite security experts serve customers in multiple industries, including energy, financial services, government, healthcare and retail. All of our customers regard us as a trusted partner and rely on us to provide solutions that enable them to meet and maintain compliance with industry regulations, increase IT security, maximize operational efficiency, manage security threats and control risk.

About Venafi

Venafi is the market leading cybersecurity company in Next-Generation Trust Protection. As a Gartner-recognized Cool Vendor, Venafi delivered the first trust protection platform to secure cryptographic keys and digital certificates that every business and government depend on for secure communications, commerce, computing, and mobility. Venafi customers are among the world's most demanding, security-conscious organizations.

Part number: 1-0038-0215