CHAMELEON

FOR OUR SMARTER WORLD

SSL Verification – Investigation Findings

Hamish Burnett – (222282244)

Contents

Executive Summary

The test that this report will investigate, is whether the Chameleon website's SSL Certificates are valid. SSL Certificates are used to identify webservers, and prove that they are who they say they are, and that they are not a malicious actor (Cloudflare, n.d.). They ensure that the site is secure, while browsing the website. The SSL Certificates of the Chameleon website, were then analysed, to verify that they are correct, and that they are suitable, use within the Chameleon website.

The tools used for this test, were Kali Linux, through VirtualBox, openssl, and Cyberchef. The certificates were obtained from the website, and were analysed, to prove their validity.

It was found that the certificates are valid, however, several actions could be taken, to improve the security of the Chameleon website's SSL certificates. The two fields that were found to be lacking in security, were the following fields:

- Common Name
- Subject Alternative Name

The Common Name, is the domain name, that the certificate protects (i.e. https://sit-chameleon-website-0bc2323.ts.r.appspot.com/). The Subject Alternative Name, is similar to the Common Name, and provides more web addresses, that the website covers (i.e. https://mail.sit-chameleon-website-0bc2323.ts.r.appspot.com/ These fields were found to be too liberal, in their approach, and a tighter, more restricted approach is needed. Both of these fields, only applied to a small section of the Chameleon website address and these settings should be amended. If these settings are not amended, then an attacker may be able to create an impersonation website of the Chameleon website, and utilise the Chameleon SSL Certificates, to appear authentic (Venafi, n.d.).

Introduction

SSL Certificates are used to ensure security, while on websites. HTTP was previously used as a protocol to transmit traffic between a client, and a server, without any encryption, or protections (Cloudflare, n.d.). This meant that data travelled in plaintext, between a client, and a server, which enabled attackers to view, and modify sensitive data. HTTPS was then implemented, which encrypted data between a client and a server, so that only authorised parties (the client, or the server), were able to decrypt the traffic, and read the network traffic. The encryption is completed through SSL, which ensures that the client is communicating directly with the server, and not a malicious actor, and that the network traffic is encrypted, to prevent eavesdropping.

SSL Certificates are used to identify webservers, and prove that they are who they say they are, and that they are not a malicious actor. The SSL Certificates of the Chameleon website, will now be analysed, to verify that they are correct, and that they are suitable, and not compromised, for proving the identity of the Chameleon web server.

Potential attacks including SSL Certificates, include impersonation of the Chameleon website, Man-in-the-Middle attacks, and Denial of Service attacks (Venafi, n.d.).

Tools Used

Four main tools were used, which are listed below:

- Openssl
- Cyberchef
- Kali Linux
- Virtual Box Virtual Machine

Scope of Testing

The scope of this SSL verification, was limited to the Chameleon website. Only the certificates from the Chameleon website, were analysed, and verified.

Methodology

To perform SSL verification, openssl will be used, to analyse the SSL certificates of the Chameleon website. The testing was performed in a Kali Linux Virtual Machine, which came preinstalled with openssl. Openssl will be used to request the SSL certificate from the website, which can then be analysed.

To obtain the SSL certificate, the following command was used (Bombal, 2023).

```
┌──(kali㉿kali)-[~/Documents/SIT378]
└─$ openssl s_client -connect sit-chameleon-website-0bc2323.ts.r.appspot.com:443
```

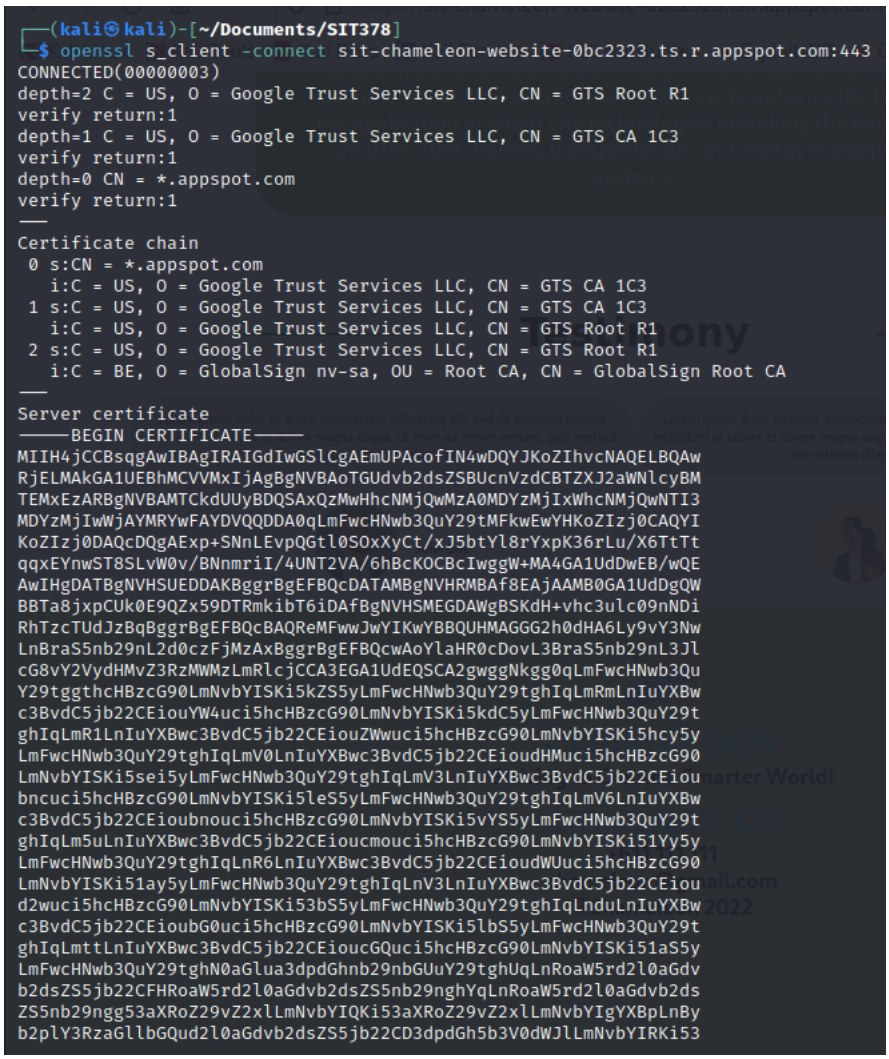
The command will be deconstructed, to identify all components.

Openssl: The application to be run.

S_client: Indicates to create a connection to a server, using SSL (The OpenSSL Project Authors, n.d.-a).

-connect sit-chameleon-website-0bc2323.ts.r.appspot.com:443: Provides the website, and the port, to connect to. The website is shown in blue, and the port, shown in green.

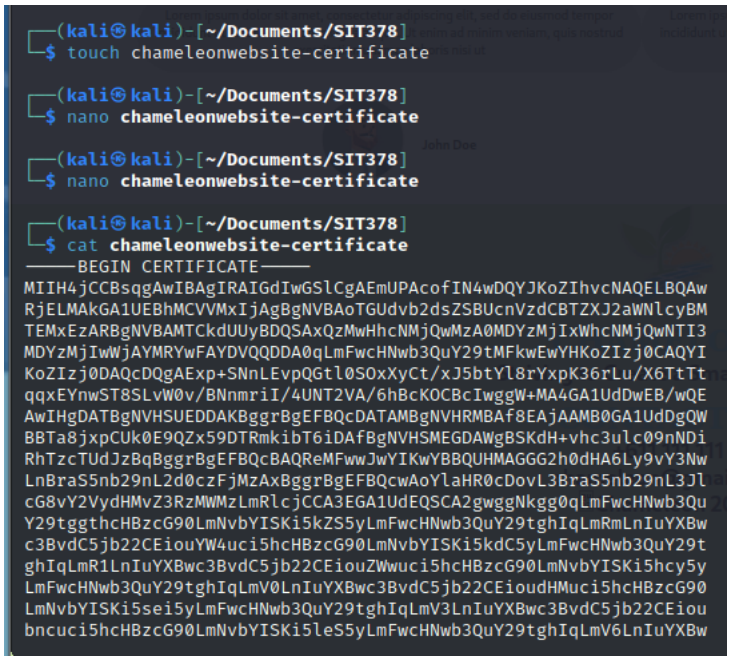
The result of this command, is shown below.



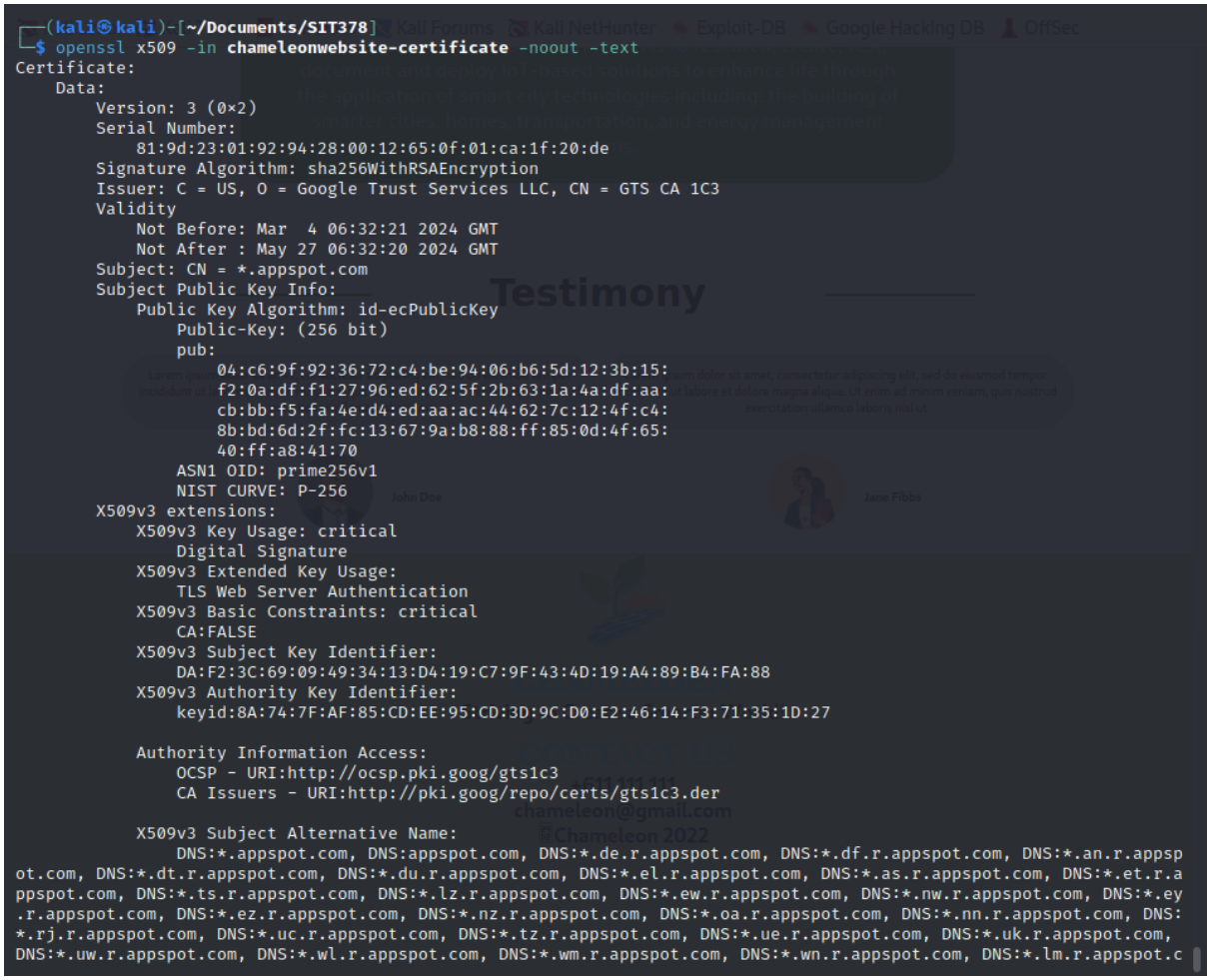
Where the output states, “BEGIN CERTIFICATE”, is where the certificate begins. At the current stage, the certificate is in a PEM format, which is used to store information about the certificate, in base 64 encoding (Heddings, 2020). The PEM format is not in a human readable form, and thus, the certificate will now be converted to a human readable format.

To convert it into human readable format, the certificate will be copied into a new file. To do this, enter the command *touch chameleonwebsite-certificate*. The *touch* command creates a new file. Edit the file, using the command *nano chameleonwebsite-certificate*, and paste the certificate into this

file. Then, use the command *cat chameleonwebsite-certificate*, to view the newly created file. See the following image, to view the output of these commands.



The following command, was then used, to convert the PEM certificate, into a human readable certificate, as shown below.



The components of the command, are as follows:

Openssl: The software application to run.

x509: Allows the certificate to be displayed to the user. This enables the certificate to be analysed, to ensure that it is valid (The OpenSSL Project Authors, n.d.-b).

-in chameleonwebsite-certificate: This indicates that the command should read the file chameleonwebsite-certificate, which contains the certificate, to be analysed.

-noout: Ensures that the output of the command, does not included the encoded version of the certificate.

-text: Outputs the certificate, in a text format, which is readable by the person examining the certificate.

Analysis of the certificate will now commence.

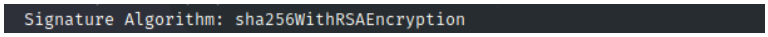
```
┌──(kali㉿kali)-[~/Documents/SIT378]
└─$ openssl x509 -in chameleonwebsite-certificate -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            81:9d:23:01:92:94:28:00:12:65:0f:01:ca:1f:20:de
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
        Validity
            Not Before: Mar  4 06:32:21 2024 GMT
            Not After : May 27 06:32:20 2024 GMT
        Subject: CN = *.appspot.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:c6:9f:92:36:72:c4:be:94:06:b6:5d:12:3b:15:
                    f2:0a:df:f1:27:96:ed:62:5f:2b:63:1a:4a:df:aa:
                    cb:bb:f5:fa:4e:d4:ed:aa:ac:44:62:7c:12:4f:c4:
                    8b:bd:6d:2f:fc:13:67:9a:b8:88:ff:85:0d:4f:65:
                    40:ff:a8:41:70
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                DA:F2:3C:69:09:49:34:13:D4:19:C7:9F:43:4D:19:A4:89:B4:FA:88
            X509v3 Authority Key Identifier:
                keyid:8A:74:7F:AF:85:CD:EE:95:CD:3D:9C:D0:E2:46:14:F3:71:35:1D:27

            Authority Information Access:
                OCSP - URI:http://ocsp.pki.goog/gts1c3
                CA Issuers - URI:http://pki.goog/repo/certs/gts1c3.der

            X509v3 Subject Alternative Name:
                DNS:*.appspot.com, DNS:appspot.com, DNS:*.de.r.appspot.com, DNS:*.df.r.appspot.com, DNS:*.an.r.appsp
ot.com, DNS:*.dt.r.appspot.com, DNS:*.du.r.appspot.com, DNS:*.el.r.appspot.com, DNS:*.as.r.appspot.com, DNS:*.et.r.a
ppspot.com, DNS:*.ts.r.appspot.com, DNS:*.lz.r.appspot.com, DNS:*.ew.r.appspot.com, DNS:*.nw.r.appspot.com, DNS:*.ey
.r.appspot.com, DNS:*.ez.r.appspot.com, DNS:*.nz.r.appspot.com, DNS:*.oa.r.appspot.com, DNS:*.nn.r.appspot.com, DNS:
*.rj.r.appspot.com, DNS:*.uc.r.appspot.com, DNS:*.tz.r.appspot.com, DNS:*.ue.r.appspot.com, DNS:*.uk.r.appspot.com,
DNS:*.uw.r.appspot.com, DNS:*.wl.r.appspot.com, DNS:*.wm.r.appspot.com, DNS:*.wn.r.appspot.com, DNS:*.lm.r.appspot.c
```

Most fields will be analysed, however, some fields will not be analysed, as they will not contribute in a meaningful manner, to this investigation.

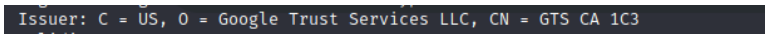
The Serial Number (shown below), is a number assigned by the issuing organisation, to uniquely identify each certificate. No other certificate that is issued by the same issuing organisation, will have the same Serial Number.

```
Serial Number:
    81:9d:23:01:92:94:28:00:12:65:0f:01:ca:1f:20:de
```

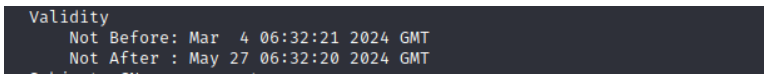
The Signature Algorithm (shown below), indicates that this certificate was signed using the SHA256 algorithm, combined with RSA. The SHA256 algorithm, is a suitable hashing algorithm, to generate a signature, as it is part of the SHA-2 class of algorithms, which are deemed secure (National Institute of Standards and Technology, 2023). RSA is also deemed secure by the Australian Government, for the purpose of verifying that the signature was generated by the owner of the website, and not a malicious actor (Australian Signals Directorate and Australian Cyber Security Centre, 2024). This signature is issued by the Certificate Authority (A body that issues certificates) (Coclin, 2021). Therefore, the signature of this certificate, will be a valid signature, due to the use of SHA256, combined with RSA.



The issuer of this certificate, is Google Trust Services. They are a reliable, and trusted issuing authority (Google Trust Services, n.d.), and thus, the issuer of the certificate is valid.



This certificate is only valid, between a certain time window, as shown below. The certificate is only valid for use, after the 4th of March, 2024, and before the 27th of May, 2024. Outside of these times (i.e. before the 4th of March 2024, and after the 27th of May 2024), this certificate is not a valid certificate. As the current date falls between these dates, the certificate is valid.



The common name, of the website, is the name of the URL, that the certificate represents (digicert, n.d.). In this instance, the * character, indicates a wild character, and that this section, can indicate any text. Therefore, this certificate, is issued to [anytext].appspot.com. For example, the common name, could be chameleon.appspot.com, or deakinuniversity.appspot.com. Given that the Chameleon website, is as follows: https://sit-chameleon-website-0bc2323.ts.r.appspot.com/ , this certificate only provides a certificate for the r.appspot.com section of the URL. This could be a vulnerability that needs patching. Given the current configuration of the common name (*.appspot.com), this website (https://sit-chameleon-website-0bc2323.ts.r.appspot.com/) should be flagged as potentially malicious, when this website is entered into a browser. This is because it should not accept that the URL has multiple subdomains, when it only has a single wildcard (*). An attacker could also create a website, that utilises the domain .appspot.com, and use the Chameleon website's certificate. This should not be valid, and should be patched.

The following screenshot, shows the public key, which is used to prove that the Chameleon website has the associated private key, through signing the signature that was generated. The public/private keys generated by the Certificate Authority, verify that the Chameleon website, is genuine, and that it is not a malicious actor, masquerading as the Chameleon website. The digital signature algorithm that is used, is elliptic curve cryptography, with a key size of 256 bits. The curve also uses the P-256 curve, generated from the National Institute of Standards and Technology (NIST). Both the key size (256 bits), and the NIST Curve (P-256), are recommended for elliptic curve cryptography, used in digital signatures, by the Australian Government (Australian Signals Directorate and Australian Cyber Security Centre, 2024). Therefore, this encryption method, is valid, for the digital certificates.

```
Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
        Public-Key: (256 bit)
        pub:
            04:c6:9f:92:36:72:c4:be:94:06:b6:5d:12:3b:15:
            f2:0a:df:f1:27:96:ed:62:5f:2b:63:1a:4a:df:aa:
            cb:bb:f5:fa:4e:d4:ed:aa:ac:44:62:7c:12:4f:c4:
            8b:bd:6d:2f:fc:13:67:9a:b8:88:ff:85:0d:4f:65:
            40:ff:a8:41:70
        ASN1 OID: prime256v1
        NIST CURVE: P-256
```

The two items that are in the following screenshot, are important for checking the validity of the SSL certificates. The Subject Key Identifier is a hash of the public and private key combination, that were used to sign this certificate, and the Authority Key Identifier, is a combination of the public and private keys, in the form of a hash, of the issuing authority. These are used to track when the keys have changed. These keys are valid, for use within the digital certificate.

```
  X509v3 Subject Key Identifier:
      DA:F2:3C:69:09:49:34:13:D4:19:C7:9F:43:4D:19:A4:89:B4:FA:88
  X509v3 Authority Key Identifier:
      keyid:8A:74:7F:AF:85:CD:EE:95:CD:3D:9C:D0:E2:46:14:F3:71:35:1D:27
```

The following two items (Key Usage, and Extended Key Usage), indicate the purpose of these keys. It can be seen that these keys are for performing digital signatures (Key Usage), for TLS Web Server Authentication (Extended Key Usage). These keys are valid are not used for encryption, or for email encryption, and are used solely for TLS certificates. Thus, the keys that are used in this certificate, are valid.

```
    X509v3 Key Usage: critical
        Digital Signature
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
```

The Subject Alternative Name, is used to allow the certificate to be used, for other domains, which are listed below. See the Subject Name highlighted in red, which is the domain name of the Chameleon website (https://sit-chameleon-website-0bc2323.ts.r.appspot.com/). This allows many other websites, to utilise the Chameleon website's SSL certificate. This would allow a malicious actor, to create a website, which uses one of the following web domains, and use the Chameleon website's SSL certificate. The attacker could create a phishing website, of the Chameleon website, to attempt to gain user credentials, when they are entered into the site, or to spread malware. These Subject Alternative Names, should be reduced, as they present a security risk.

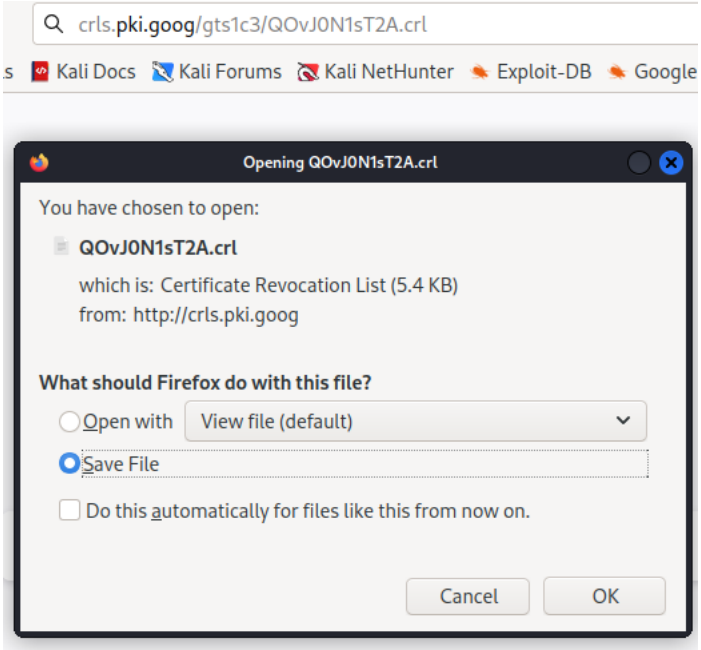
```
            X509v3 Subject Alternative Name:
                DNS:*.appspot.com, DNS:appspot.com, DNS:*.de.r.appspot.com, DNS:*.df.r.appspot.com, DNS:*.an.r.appsp
ot.com, DNS:*.dt.r.appspot.com, DNS:*.du.r.appspot.com, DNS:*.el.r.appspot.com, DNS:*.as.r.appspot.com, DNS:*.et.r.a
ppspot.com, DNS:*.ts.r.appspot.com, DNS:*.lz.r.appspot.com, DNS:*.ew.r.appspot.com, DNS:*.nw.r.appspot.com, DNS:*.ey
.r.appspot.com, DNS:*.ez.r.appspot.com, DNS:*.nz.r.appspot.com, DNS:*.oa.r.appspot.com, DNS:*.nn.r.appspot.com, DNS:
*.rj.r.appspot.com, DNS:*.uc.r.appspot.com, DNS:*.tz.r.appspot.com, DNS:*.ue.r.appspot.com, DNS:*.uk.r.appspot.com,
DNS:*.uw.r.appspot.com, DNS:*.wl.r.appspot.com, DNS:*.wm.r.appspot.com, DNS:*.wn.r.appspot.com, DNS:*.lm.r.appspot.c
```

The CRL Distribution Points (CRL being short for Certification Revocation List), indicate whether the current certificate has been revoked, due to security issues with the keys. This can occur if the encryption was hacked. This list keeps track of whether the certificate is on this list, which would

indicate that the keys need to be updated. This is particularly important to check, as malicious actors may compromise a key pair, and then redirect the user to a malicious site, while keeping the Chameleon certificate.

```
X509v3 CRL Distribution Points:
    Full Name:
      URI:http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl
```

The revocation list will now be analysed. The website was used, to obtain the revocation list. The list was then saved to the computer, as seen below.



The CRL list was then opened, using the following command: *openssl crl -in QOvJ0N1sT2A.crl -inform DER -text -noout* (Mister PKI, 2021). The results of this command, are shown below.

The switches of this command, are listed below:

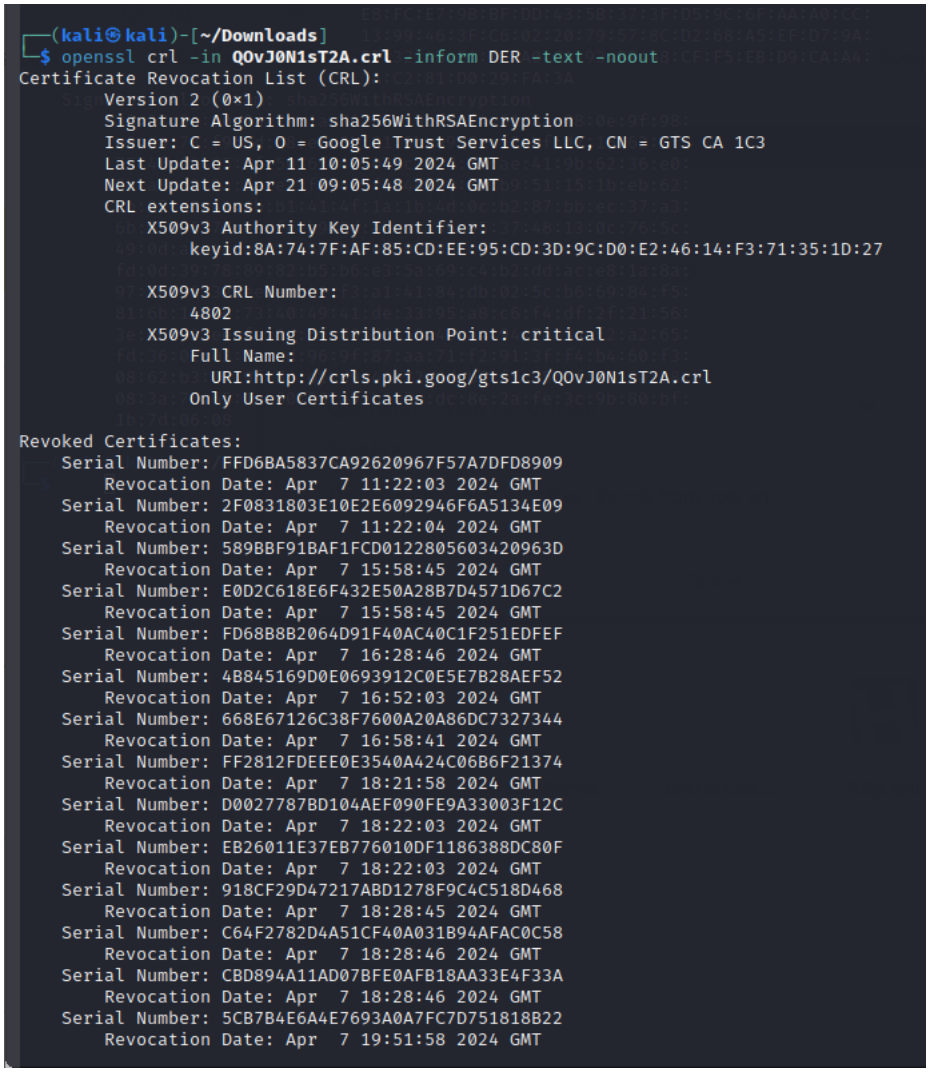
Openssl: Use the openssl application for this command.

crl: specifies that it is a crl file (earlier, x509, was used, to indicate certificate files).

-in QOvJ0N1sT2A.crl: Specifies the file to use, which contains the CRL list.

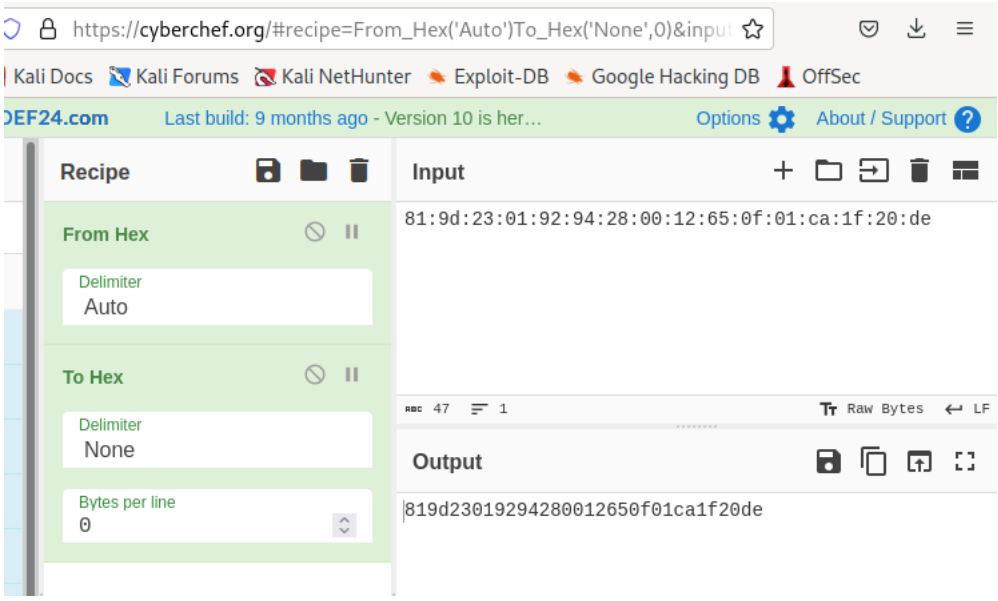
-inform DER: This ensures that the Terminal knows that it is in the form of a DER certificate.

-noout: Outputs the content of the file, to the terminal



```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl crl -in QOvJ0N1sT2A.crl -inform DER -text -noout
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Google Trust Services LLC, CN = GTS CA 1C3
        Last Update: Apr 11 10:05:49 2024 GMT
        Next Update: Apr 21 09:05:48 2024 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:8A:74:7F:AF:85:CD:EE:95:CD:3D:9C:D0:E2:46:14:F3:71:35:1D:27

            X509v3 CRL Number:
                4802
            X509v3 Issuing Distribution Point: critical
                Full Name:
                  URI:http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl
                Only User Certificates

Revoked Certificates:
    Serial Number: FFD6BA5837CA92620967F57A7DFD8909
        Revocation Date: Apr  7 11:22:03 2024 GMT
    Serial Number: 2F0831803E10E2E6092946F6A5134E09
        Revocation Date: Apr  7 11:22:04 2024 GMT
    Serial Number: 589BBF91BAF1FCD01228056034209630
        Revocation Date: Apr  7 15:58:45 2024 GMT
    Serial Number: E0D2C618E6F432E50A28B7D4571D67C2
        Revocation Date: Apr  7 15:58:45 2024 GMT
    Serial Number: FD68B8B2064D91F40AC40C1F251EDFEF
        Revocation Date: Apr  7 16:28:46 2024 GMT
    Serial Number: 4B845169D0E0693912C0E5E7B28AEF52
        Revocation Date: Apr  7 16:52:03 2024 GMT
    Serial Number: 668E67126C38F7600A20A86DC7327344
        Revocation Date: Apr  7 16:58:41 2024 GMT
    Serial Number: FF2812FDEEE0E3540A424C06B6F21374
        Revocation Date: Apr  7 18:21:58 2024 GMT
    Serial Number: D0027787BD104AEF090FE9A33003F12C
        Revocation Date: Apr  7 18:22:03 2024 GMT
    Serial Number: EB26011E37EB776010DF1186388DC80F
        Revocation Date: Apr  7 18:22:03 2024 GMT
    Serial Number: 918CF29D47217ABD1278F9C4C518D468
        Revocation Date: Apr  7 18:28:45 2024 GMT
    Serial Number: C64F2782D4A51CF40A031B94AFAC0C58
        Revocation Date: Apr  7 18:28:46 2024 GMT
    Serial Number: CBD894A11AD07BFE0AFB18AA33E4F33A
        Revocation Date: Apr  7 18:28:46 2024 GMT
    Serial Number: 5CB7B4E6A4E7693A0A7FC7D751818B22
        Revocation Date: Apr  7 19:51:58 2024 GMT
```

The Serial Number of the Chameleon website, contains “:” symbols, while the Serial Number’s of the revoked certificates, do not contain this symbol. Cyberchef was used to remove the “:” symbols, through first converting it from Hex, to the raw values, and then converting the raw values, back to Hex, but without any separator values. This is shown below.



To check whether the Chameleon certificate was among the revoked certificates, *grep* was used, to search for the Serial Number, of the Chameleon certificate. It was found, that the Chameleon certificate, was not among the revoked certificates, as it was not found, in the revocation list. Therefore, the certificate is valid. The screenshot of the *grep* search is shown below.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl crl -in QOvJ0N1sT2A.crl -inform DER -text -noout | grep -A 1 819d230192942800126 50f01ca1f20de

┌──(kali㉿kali)-[~/Downloads]
```

The Certificate Transparency (CT) of the Chameleon website's certificates were analysed. The Certificate Transparency, indicates that a record has been made to a public registry, which contains all certificates. The public registry can then be checked, to determine whether similar domains have been registered, which can be use to spot whether there are any similar domains, to the Chameleon website, which are used for phishing, or to imitate the Chameleon website. As the Chameleon certificates are listed on two databases, this certificate is valid.

```
CT Precertificate SCTs:
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70:
                    91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB
        Timestamp : Mar  4 07:32:23.277 2024 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:46:02:21:00:F5:95:03:C7:72:B9:EB:4B:C6:5C:8C:
                    37:14:FA:69:68:6E:4A:CF:C9:70:0A:F7:0A:22:78:84:
                    CC:E5:DC:9D:21:02:21:00:F6:FD:E0:13:9C:79:45:1D:
                    92:9C:32:AE:18:F3:1E:D5:FB:3C:D4:EF:55:5F:B1:00:
                    B7:C3:0E:6C:DF:F4:20:84
    Signed Certificate Timestamp:
        Version   : v1 (0x0)
        Log ID    : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2:
                    32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B
        Timestamp : Mar  4 07:32:23.017 2024 GMT
        Extensions: none
        Signature : ecdsa-with-SHA256
                    30:45:02:21:00:E0:6F:90:71:4E:B1:15:6B:3E:6A:A8:
                    E8:FC:E7:9B:BF:DD:43:5B:37:3F:D5:9C:6F:AA:A0:CC:
                    13:99:46:3F:C6:02:20:79:57:8C:D2:68:A5:EF:D7:9A:
                    5F:32:4B:E1:13:A0:CA:93:B9:58:CF:F5:EB:D9:CA:A4:
                    1A:C2:81:D0:29:FA:3A
```

The signature of the digital certificate, is shown below. This indicates that we can trust the SSL certificate, from the Chameleon website. Therefore, we can trust the Chameleon website, is who it says it is, and is not a malicious actor.

Results

From the analysis, it was found that the SSL certificate, that the Chameleon website uses, is valid, and is able to be trusted. However, it was also found that several sections of the certificate were not as secure as they should be, which may pose some security risks. In particular, the Common Name, and the Subject Alternative Name, while valid, were found to be vulnerable. Phishing attacks could be launched, through making a website that looks similar to the Chameleon website, and hosting it under a similar name, while using the Chameleon certificates.

Recommendations

The current setting of the Common Name, is set to: *.appspot.com, while the Chameleon website URL, is https://sit-chameleon-website-0bc2323.ts.r.appspot.com/ . The Common Name should be changed, to something along the lines of *.sit-chameleon-website-0bc2323.com. This would ensure that only the Chameleon website is able to use this certificate, rather than any website, that ends in .appspot.com.

The second recommendation, is to modify the Subject Alternative Name. Currently, this setting is configured to allow a wide variety of websites, to use the Chameleon certificate. Examples of these websites, include, *.de.r.appspot.com, *.app.google, and *withyoutube.com. This should be changed, to be similar to the first recommendation, to only allow websites of the name *.sit-chameleon-website-0bc2323.com.

Conclusion

While all settings of the Certificates were found to be valid, several small changes, particularly to the Common Name, and the Subject Alternative Name, can increase the security of SSL, within the Chameleon website, and prevent phishing attacks.

References

Australian Signals Directorate and Australian Cyber Security Centre (2024) *Guidelines for Cryptography*: Australian Government, accessed 2024. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography

Bombal, D (2023) *Certificates of Authority: Do you really understand how SSL / TLS works?* (2023). YouTube, accessed 2024. https://www.youtube.com/watch?v=VcV4T8cL3xw

Cloudflare (n.d.) *What is SSL? | SSL definition*, accessed 2024. https://www.cloudflare.com/learning/ssl/what-is-ssl/

Coclin, D. (2021) *What is a CA? Certificate Authorities Explained*: digicert , accessed 2024. https://www.digicert.com/blog/what-is-a-certificate-authority

digicert (n.d.) *What is a Wildcard SSL Certificate?* accessed 2024. https://www.digicert.com/faq/public-trust-and-certificates/what-is-a-wildcard-certificate

Google Trust Services (n.d.) *Google Trust Services*: Google, accessed 2024. https://pki.goog/

Heddings, A. (2020) *What Is a PEM File and How Do You Use It?* accessed 2024. https://www.howtogeek.com/devops/what-is-a-pem-file-and-how-do-you-use-it/

Mister PKI (2021) *openssl crl*, accessed 2024. https://www.misterpki.com/openssl-crl/

National Institute of Standards and Technology (2023) *Hash Functions*: U.S Department of Commerce, accessed 2024. https://csrc.nist.gov/Projects/Hash-Functions

The OpenSSL Project Authors (n.d.-a) *s_client*, accessed 2024. https://www.openssl.org/docs/man1.1.1/man1/openssl-s_client.html

The OpenSSL Project Authors (n.d.-b) *x509*, accessed 2024. https://www.openssl.org/docs/man1.1.1/man1/x509.html

Venafi (n.d.) *The Most Common SSL and TLS Attacks*, accessed 2024.https://venafi.com/machine-identity-basics/the-most-common-ssl-and-tls-attacks/