# Booters and Certificates: An Overview of TLS in the DDoS-as-a-Service Landscape

Benjamin Kuhnert*, Jessica Steinberger*†, Harald Baier*, Anna Sperotto† and Aiko Pras†

*da/sec - Biometrics and Internet Security Research Group
University of Applied Sciences Darmstadt, Darmstadt, Germany
Email:{Benjamin.Kuhnert, Jessica.Steinberger, Harald.Baier}@h-da.de

†Design and Analysis of Communication Systems (DACS)
University of Twente, Enschede, The Netherlands
Email:{J.Steinberger, A.Sperotto, A.Pras}@utwente.nl

***Abstract*—Distributed Denial of Service attacks are getting more sophisticated and frequent whereas the required technical knowledge to perform these attacks decreases. The reason is that Distributed Denial of Service attacks are offered as a service, namely Booters, for less than 10 US dollars. As Booters offer a Distributed Denial of Service service that is paid, Booters often make use of Transport Layer Security certificates to appear trusted and hide themselves inside of encrypted traffic in order to evade detection and bypass critical security controls. In addition, Booters use Transport Layer Security certificates to ensure secure credit card transactions, data transfer and logins for their customers. In this article, we review Booters websites and their use of Secure Socket Layer certificates. In particular, we analyze the certificate chain, the used cryptography and cipher suites, protocol use within Transport Layer Security for purpose of security parameters negotiation, the issuer, the validity of the certificate and the hosting companies. Our main finding is that Booters prefer elliptic curve cryptography and are using Advanced Encryption Standard with a 128 bit key in Galois/Counter Mode. Further, we found a typical certificate chain used by most of the Booters.**

***Keywords*—booters; certificates; distributed denial of service as a service; mitigation; tls.**

## I. INTRODUCTION

Over the last years, Distributed Denial of Service (DDoS) attacks remain the top threat responsible for infrastructure and service outages [1]. The reason is that DDoS attacks are getting more sophisticated and more frequent whereas the required technical knowledge to perform these attacks decreases. One possibility to launch DDoS attacks is offered to non-technical users by websites referred to as Booters [2][3]. A user accesses a Booter website and chooses an attack plan that defines a number of attacks with a maximum attack duration each within a maximum period of time (expiration time) [4]. After the selection of an attack plan, the customer request is forwarded to a payment system (e.g., PayPal, BitCoin and credit card), which notifies the Booter when the amount of money is paid. This notification unblocks the customer and allows the customer to perform as many attacks as he/she wants in accordance to the attack plan. Besides the simplicity to buy and launch DDoS attacks against anyone on the Internet, Booters also use Transport Layer Security (TLS) to hide their attacks, evade detection, and bypass critical security controls [5][6]. In addition, Booters also secure their credit card transactions, data transfer and logins using TLS certificates in order to protect their customers.

The main intention of the TLS protocol and the Public Key Infractructure (PKI) is to give customers the confidence to complete their transactions using several trust indicators. However, the TLS protocol did not originally include the provision of a validated business identity within the TLS certificate and, as a result, the role of the Certification Authority (CA) is to pass trust. Moreover, CAs should have a responsibility to ensure they only ever issue TLS certificates to legitimate companies. As opposed to this, Booters that use a TLS certificate to secure their Internet transactions are intended to generate harmful traffic against a target system.

In this paper, we review the use of TLS certificates of current Booters. Further, we analyze the characteristics of the used of TLS certificates (e.g., certificate chain, used cryptography and cipher suites, negotiation protocol, issuer and the validity of the certificate). To summarize, our contributions are as follows: i) We identify and classify the used TLS certificates of Booters and generalize potential malicious certificate chains; ii) We study in detail the characteristics of the used TLS certificates (e.g., used cryptography and cipher suites, negotiation protocol, issuer and the validity of the certificate) and uncover same Booter infrastructures; iii) We discuss strategies to mitigate Booters using TLS certificates.

## II. BOOTERS AND SSL CERTIFICATES

In this section, we provide a general overview of Booters using TLS certificates. First, we define the terminology that is used throughout this paper and describe the methodology to retrieve the TLS certificate. Second, we provide information regarding the certificate chain, the used cryptography and cipher suites, protocol use within TLS for purpose of security parameters negotiation, the issuer and the validity of the certificate. We aim to shed light onto the typical TLS configuration parameters of Booter websites and discuss our findings in terms of mitigation and response to DDoS attacks.

### A. Terminology

The analysis of Booter websites has revealed that there are various terms used to describe websites that offer DDoS-as-a-Service. Namely, Booters websites are also known as

 ISBN: 978-1-61208-570-8 

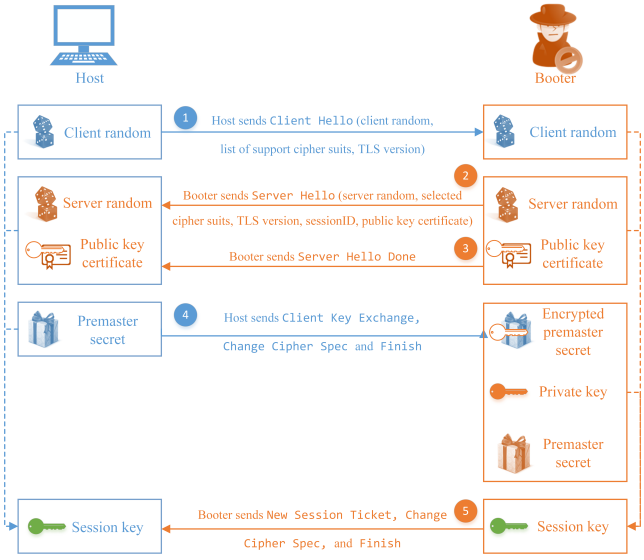


Figure 1. SSL handshake with a Booter website.

Stressers, DDoS-for-hire, DDoS-as-a-Service, and DDoSers [4]. In this paper, we adhere to the term Booter and refer to the infrastructure of a Booter presented in [4].

Further, we adhere to the definition of a CA by [7]: "A certification authority is a general designation for any entity that controls the authentication services and the management of certificates. A CA can be public commercial, private or personal. CAs are independent and define an Certification Practice Statement (CPS)."

### B. Methodology

First, we monitor the landscape of Booter websites that listen to HyperText Transport Protocol Secure (HTTPS) requests and reply with a TLS certificate to secure their Internet transactions based on the Booterblacklist [8]. To connect to a Booter website, we first used the TLS client program `s_client` of OpenSSL. However, we found that the OpenSSL program `s_client` is not always able to extract and store the certificate chain of an existing connection. To overcome missing certificate chains, we developed two different TLS client programs and performed a TLS handshake [9] as shown in Figure 1. The reason to develop two different TLS client programs is that the Booters website presents different TLS certificates during the SSL handshake based on the use of the Server Name Indication (SNI) Extension of SSL [10]. Therefore, one TLS client program makes use of the SNI Extension and the other program works without. We stored the cipher suits, TLS version, the Booters public key certificate and its certificate chain, and the Subject Alternative Name (SAN) field [11]. In addition to the TLS data, we used `whois` to query all domain name entries within the SAN field of the certificates to gather information about the hoster of the Booter websites.

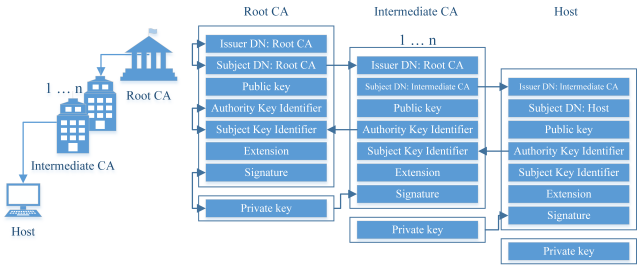


Figure 2. Certificate chain and linkages between certificates [13].

### C. The use of TLS certificates by Booter websites

Out of 434 Booters, 152 replied with a TLS certificate. Even though this amount is significantly less than the usage of TLS certificate authorities for the top 10 million websites presented in [12] (e.g., W3Techs [12] reported that 67.4% of the websites currently use TLS certificates), Gartner believes that by 2017 more than 50% of the network attacks will use SSL encryption [5]. As a result, the number of Booters that use TLS might also increase [6] .

*1) Depth of TLS certificate chain:* As described in [11], TLS certificates are built in a top down process. First, the self-signed Root CA certificate is established [13]. Next, the Root CA signs an intermediate CA certificate. This intermediate CA either create an additional intermediate CA or issues a certificate to people or hosts. To establish a valid certificate chain at least one CA is required. [13] reported that there is no theoretical maximum of certificate chains, but the average certificate chains have between two and three CAs in the hierarchy. The depth count is "level 0:peer certificate", "level 1: CA certificate", "level 2: higher level CA certificate", and so on. The last certificate is called Root certificate. In contrast to the process of building TLS certificates, the validation of TLS certificates is a bottom up approach. Both the building and verification process are shown in Figure 2. On average, Booter websites have a depth count of 4.

*2) Geographic Distribution of TLS certificates:* We examined the geographic distribution of the host, intermediate and root TLS certificates by using the subject and issuer two-letter International Organization for Standardization (ISO) country code and compared our findings with [2]. Our findings revealed a similar distribution of the top 10 two-letter ISO country code of the certificate's subject and issuer as reported by [2]. The top ranked country that issues TLS certificates to Booter websites is Sweden, followed by Great Britain. The geographical distribution of the TLS certificate by subject and issuer country is listed in Table I and shown in Figure 3. Surprisingly, the majority (74.59%) of the Booter websites that use TLS certificates provide the country code of the certificate subject and issuer. In addition to Table I, 10 certificates did not provide information about the subject and issuer country. Even though the country code is missing, the TLS certificate is still valid as the country name attribute is optional [11].

*3) Types of TLS certificates:* Besides self-signed certificates, currently three types of commercial TLS certificates

 ISBN: 978-1-61208-570-8 

TABLE I. GEOGRAPHICAL DISTRIBUTION OF THE TLS CERTIFICATE BY USING THE SUBJECT AND ISSUER COUNTRY.

| Country Name | BE | FR | GB | SE | US | ZA |
|---|---|---|---|---|---|---|
| Frequency | 27 | 3 | 222 | 230 | 69 | 24 |

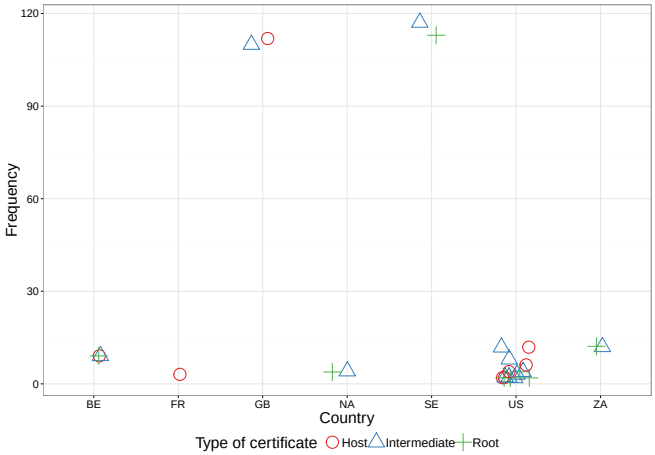


Figure 3. Geographic distribution of Booter's certificate issuer.

are available: Domain Validated (DV), Organization Validated (OV) and Extended Validation (EV).

The DV SSL certificate is the most common type of TLS certificate. The CA verifies only the domain name and typically exchanges confirmation email with an address listed in the domain's WHOIS record. DV certificates are typically verified and issued through automated processes. Human intervention is minimized and organization checks are eliminated in order to support issuing certificates in a quick and cheap manner. While the browser displays a padlock, examination of the certificate will not show the company name as this was not validated. All Booters listed on the Booter blacklist that respond to an HTTPs request make use of DV TLS certificates.

In contrast to DV certificates, CAs must validate the company name, domain name and other information through the use of public databases when issuing an OV certificate. The issued certificate will contain the company name and the domain name, for which the certificate was issued for. None of our Booter websites that use TLS certificates to secure their Internet transactions make use of a OV certificate.

The purpose of an EV certificate is to identify the legal entity that controls a website and to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. An EV certificate is only issued once an entity passes a strict authentication procedure. The Guidelines for the Issuance and Management of Extended Validation Certificates [14] present criteria established by the CA/Browser Forum for use by certification authorities when issuing, maintaining, and revoking certain digital certificates for use in Internet website commerce. As in the OV, the EV lists the company name in the certificate itself. However, a fully validated EV certificate will also show the name of the company or organization in the address bar itself, and the address bar is displayed

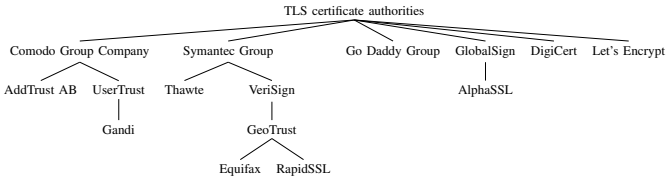


Figure 4. Relationship of TLS certificates.

in green. Further, other disambiguating information is also provided (e.g., address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number).

*4) Certificate chain:* In this section, we analyze the certificate chain of the TLS certificates used by the Booter websites. We found 585 TLS certificates used by 152 Booter websites as host, intermediate or root certificate issued by 17 different organizations. We recognized the occurrence of similar certificate chains and built an overview of relationships between CAs and their TLS certificates.

In a first step, we analyzed the root certificates and trusted CAs. At least for the European context, an EU Trusted Lists of Certification Service Providers is available. We compared the root certificates used by the Booter websites with the CAs listed on the EU Trusted List [15]. We assumed to find the majority of the root certificates used by Booter websites on the EU Trusted List as the geolocation revealed Great Britain and Sweden the top issuer countries as shown in Figure 3. However, the organization names of the root certificates of the Booter websites are not listed on the EU Trusted List of Certification Service Providers.

To answer the question of who is issuing the TLS certificates used by Booter websites, we built an overview of relationships between CAs and their TLS certificates as shown in Figure 4. The majority of the Booters intermediate and root certificates are issued by Comodo CA Limited and AddTrust AB.

However, AddTrust AB no longer exists as a company [16]. After ScandTrust, a private Swedish CA, acquired AddTrust AB, Comodo CA Limited purchased the AddTrust root certificates from ScandTrust [16]. Further, Comodo CA Limited also purchased the CA UserTrust [17], which had four roots [16]. As reported by [16], the key material was removed from its original sites of operation and transferred into Comodo's data and backup centers.

The next higher amount of TLS certificates are issued by organizations belonging to the Symantec Group. In 2000, Thawte was acquired by Symantec [18]. In the year 2006, VeriSign acquired GeoTrust [19] and bought the certificates from them. In 2010, Symantec acquired VeriSign's identity and authentication business for 1.28 billion US dollar [20] and thus owns the TLS and code signing certificate services, the managed public key infrastructure services, the VeriSign trust seal, the VeriSign identity protection authentication service and the VIP fraud detection service.

As a response to occurring security incidents in the past, some CAs are sold. Even though CAs are sold and their key material is transferred to other CAs, each of the hundreds of

 ISBN: 978-1-61208-570-8

different root CAs are equally trusted by the browsers [21].

*5) Costs of SSL certificates:* The costs of a TLS certificate depend on the type of the certificate, the value of the used intermediate and root CAs within the certificate chain and the reputation of the issuing CA.

As described in Section II-C3, the three types of commercial TLS certificates DV, OV and EV are available. The cheapest certificate is a DV certificate (e.g., starting from $8.95 for a single domain and $98 for multiple domains), followed by the OV certificate (e.g., starting from $38 for a single domain and $180 for multiple domains). The most expensive TLS certificate is EV (e.g., starting from $99 for a single domain and $269 for multiple domains), because an applying entity has to pass strict authentication procedures.

In recent years, incidents with CAs that issued bogus TLS certificate have been published and discussed. In 2008, Eddy Nigg ordered an SSL certificate for Mozilla.com on CertStar's site without having to go through any validation or verify that he was authorized to order the certificate [22][23]. In the year 2011, a Comodo affiliate RA was compromised resulting in the fraudulent issue of 9 SSL certificates to sites in 7 domains [24][25]. Later in 2011, the DigiNotar CA detected an intrusion into its CA infrastructure, which resulted in the fraudulent issuance of 531 public key certificate requests for a number of domains, including Google.com [26][27]. In 2015, Microsoft revoked an improperly issued SSL certificate for the domain `live.fi` that could be used in attempts to spoof content, perform phishing attacks, or perform man-in-the-middle attacks [28][29].

In most of the aforementioned cases, the involved CA that issued bogus TLS certificates have been sold or dissolved and their key material has been transferred to different parties. The acquiring organization recognized the lower value of such a CA, offer these TLS certificates to third party vendors that sell these at a cheaper cost as the in-house generated ones [16]. As the Booter websites main intention is to earn money, most of the Booter websites make use of low-cost TLS certificates, as they are equally trusted by the browsers.

*6) Serial numbers, wildcards and SAN of TLS certificates:* Each TLS certificate must have a serial number, which uniquely distinguishes it from all other certificates issued by the same CA. The serial number is unique only to the issuing CA and a non-negative integer [11]. We analyzed 152 Booter Unified Resource Locators (URLs) and their certificate serial number. Out of 152 Booters URLs, 18 TLS certificates provide the same serial number to different Booter URLs as listed in Table II.

To ensure that these Booter URL are related to each other, we reviewed the common name and the alternative domain name attributes as the TLS certificate could be a wildcard or a Subject Alternative Name (SAN) certificate. Wildcard TLS certificates protect unlimited subdomains with a single certificate. In contrast to wildcard TLS certificates, SAN certificates protect multiple domain names with a single certificate. For example, a SAN certificate could be issued for `abc.de`. In addition, the domain `gef.hi` is added to the SAN values

TABLE II. DUPLICATE SERIAL NUMBERS OF USED TLS CERTIFICATES.

| # | Serial number | URL |
|---|---|---|
| 1 | 1121936FEA6ABA378CA723245B8F125A7850 | booter-sales.hourb.com<br>stresser.org |
| 2 | 1121B4A4D767765C56B0224767AB1AE0767C | omega-stresser.us<br>onestress.com |
| 3 | 2FFF | darkstresser.weebly.com<br>opaquebooter.weebly.com |
| 4 | 55F2EBB7F44E0B5AC0125A5D14E72035 | buyddos.com<br>freezystresser.nl<br>getsmack.de<br>optimusstresser.com<br>superstresser.com<br>xrstresser.net |
| 5 | 9D8646B2096A20FF0C48F24CEC1810EB | equinoxstresser.net<br>riotstresser.com |
| 6 | BBBA942BA2268EF9A74B78A5D4412E8E | powerstresser.com<br>signalstresser.com |
| 7 | 109DFF6A138BB2677C35C5F6DAB7B089 | crazyamp.me<br>iddos.net |

and thus the same certificate protects multiple domains. We identified the use of one wildcard certificate by the Booter infrastructure listed in Table II row 2. Further, we assume that the remainder of Booters in Table II use SAN certificates, but do not explicitly add the different Booter URLs to the alternative domain name attributes to secure their own Booter infrastructure. As reported by [2], Booters protect themselves using DDoS Protection Services. In case, the operator of a Booter infrastructure would enter all possible alternative domain names in the SAN attributes of a TLS certificate, the Booter infrastructure itself would be more vulnerable to attacks.

*7) Certificate validity and revocation:* When a TLS certificate is issued, it is expected to be in use for its entire validation period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period (e.g., change of name, change of association between subject and CA, a compromise or suspected compromise of the corresponding private key). In any of the aforementioned circumstances, the CA needs to revoke the certificate [11].

**Common name:** The Common Name (CN) of a TLS certificate is typically composed of a String containing the host and domain name [30]. The CN must be the same as the Web address that will be accessed when connecting to a secure site. As a consequence, the TLS certificate is valid only if the request host name matches either the common name or at least one of the certificate subject alternative names. We found that the 8 Booter URLs do not match to the CN written in the TLS certificate. As a result, the connections to this Booter websites appear to be invalid within the Browser. In a second step, we analyzed what kind of third party is used as CN of the certificate and found that the entries 1 and 4 in Table II use a CN or SAN of a domain parking company instead of the Booters URL.

Domain parking is often an advertising practice that resolve to a Web page containing advertising listings and links and are not limited to benign applications. However, the revenue

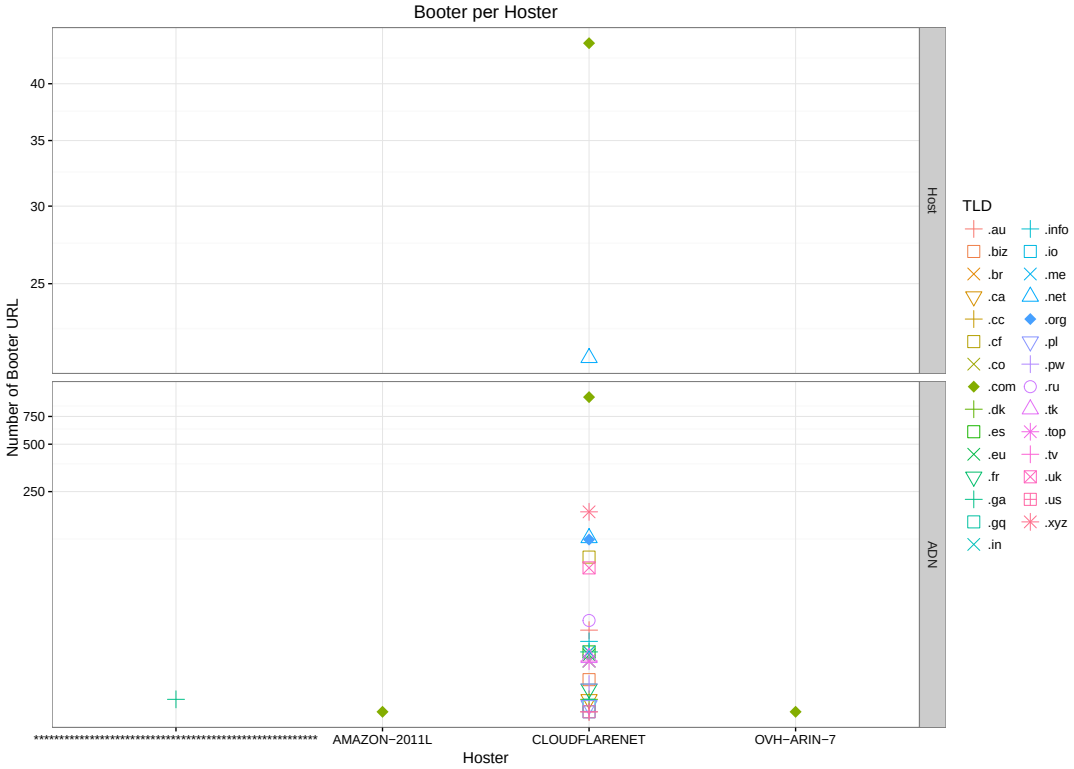


Figure 5. Distribution of Booter websites per Hoster.

generated is split between the parking service and the domain owner. As reported in [31] such domain parking monetization is a million-dollar business. In accordance with [32], we assume that domain parking is used by the owner of the Booter websites once malicious actions of these domains have been discovered and the domain has been blocked. Even though the malicious domains have been blocked, traffic from backlinks is still used to make money [32].

**SAN:** The Subject Alternative Name (SAN) field [11] within the TLS certificate specifies additional subject identifies. In case a SAN is defined, the SAN must always be used and the CN is only evaluated in case the SAN is not present. We found that Booter websites entered 21 additional subject identifies on average. Surprisingly, we also found Booter websites using more than 90 SANs in a single certificate. One possible explanation for this huge amount of SANs within a certificate is that these URLs reside in a Content Delivery Network (CDN) network. However, CDNs serve content on behalf of other companies. The servers of a CDN usually handle results of hundreds or thousands of different domains and are distributed all over the world. For reason of usability, these servers often share a single TLS certificate. Another explanation is that domains also might get compromised by Booter owners and are abused for malicious activities.

**Validity period:** Each TLS certificate contains a validity period. A validity period is described as the time interval during, which the CA warrants that it will maintain information about the status of the certificate [11]. A maximum validity period is described within the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates by the CA/ Browser Forum [33] and is set to 39 months maximum validity of OV and DV TLS certificates in order to increase TLS security. However, the TLS certificates used by Booter websites use a maximum validity of half a year to one year on average.

**Revocation:** In Section II-C5, we presented some incidents with CAs that issued bogus TLS certificate. In most of those cases, the CA creates and disseminates revocations of the bogus TLS certificates. To revoke certificates nearly every certificate contains a reference to a Certificate Revocation List (CRL). A CRL is a list of certificates that the CA has revoked for whatever reason. However, [34] reported that browsers often do not bother to check whether certificates are revoked (including mobile browsers, which uniformly never check). Out of 152 Booter websites, only one Booter used a certificate that had been revoked. Browsing this Booter website raises an error message within the Web browser.

*8) TLS protocol and cipher suites:* During the TLS handshake the used cipher suite is negotiated. Our TLS client program uses a version-flexible SSL/TLS method and thus the protocol version used will be negotiated to the highest version mutually supported by the client and server. In total, our TLS client offered 42 cipher suites [35], from which a Booter website selects the one most appropriate. Out of 152 Booter websites that use TLS, 148 make use of TLS using a cipher

 ISBN: 978-1-61208-570-8 

suite in Galois Counter Mode (GCM) [36][37]. In particular, 146 Booter websites secure their websites using the elliptic curve cipher suite `ECDHE-ECDSA-AES128-GCM-SHA256`. According to the NIST recommendations on key length [38], a 256-bit elliptic curve key provides as much protection as a 3 072-bit asymmetric key.

*9) Hoster of Booter websites:* In order to identify the hosting provider of the Booter websites, we used the Booter URLs presented in the Booter blacklist and performed a `whois` query. We found that the majority of Booter websites that are using TLS reside in the CDN of Cloudflare. Figure 5 shows the distribution of Booter URLs within the hosting provider network categorized by Host or Alternative Domain Names (ADNs). For example, the majority of Booter websites make use of the Top Level Domains (TLDs) `.com` and `.net` and reside in the network of Cloudflare. Further, Figure 5 shows, in which network the SANs are hosted. We found that the majority of SANs presented within the TLS certificate of a Booter website also reside in the network of Cloudflare.

To validate our results, we compared the preferred used TLS protocol and cipher suite of the hosting network. In Section II-C8, we showed that the majority of Booter websites are using Elliptic Curve Cryptography (ECC) and GCM. This finding is in accordance with [39], who reported Cloudflare enables their customers to use ECDSA certificates on their CloudFlare-enabled sites. As a result, the majority of Booter websites using ECC and GCM reside in the network of the content delivery network Cloudflare.

*10) TLD of Booters:* Each Booter website is accessible via an URL that is registered though a registrar at ICANN. According to [40], 1930 Generic Top-Level Domains (gTLDs) are coordinated by ICANN. We reviewed the top level domains that are used by Booters websites. Reviewing the TLDs of the Booter URLs at depth 0, the majority of Booters use `.com` and `.net` TLDs. Taking also into account the SANs within the TLS certificate of a Booter website, the majority of TLDs are registered within the `.com`, `.xyz`, `.org`, `.net` and `.cf`. However, the number of registered domains within a TLD also vary and thus we reviewed the share of Booter URLs that use TLS compared to the overall amount of registered domains. Under consideration of the overall amount of registered domains, the majority of Booter URLs that use TLS registered a `.cf` domain followed by `.xyz`, whereas `.cf` is a country-code domain sponsored by the *Société Centrafricaine de Télécommunications (SOCATEL)* and the `.xyz` is a generic domain sponsored by XYZ.COM LLC.

TABLE III. SUMMARY OF THE USE OF TLS IN THE DDOS-AS-A-SERVICE LANDSCAPE.

| Criterion | Result |
|---|---|
| Use of TLS | 152 of 434 (35%) |
| Depth of certificate chain | 4 |
| Geographic distribution of subject and issuer | Sweden, Great Britain |
| Type of TLS certificate | DV |
| Top certificate issuer | Comodo Group |
| # SANs | ∅21 |
| Validity of certificate | $0.5 - 1$ year |
| Revoked | 1 of 585 certificates |
| Preferred TLS protocol | TLSv1/SSLv3 |
| Preferred TLS cipher suite | `ECDHE-ECDSA-AES128-GCM-SHA256` |
| Preferred TLDs | `.cf`, `.xyz` |
| Hoster (Host/ADN) | Cloudflare/Cloudflare |

## III. DISCUSSION

In this section, we provide an aggregated overview of the key findings. Further, we discuss our results with regard to possible mitigation strategies. We have summarized the information presented in Section II-C in Table III.

Even though the main intention of the TLS protocol and the PKI is to give customers the confidence to complete their transactions using several trust indicators, there are no technical restrictions in place that prohibit a CA from issuing a certificate to a malicious third party [21]. Thus, both the integrity of the CA based public key infrastructure and the security users' communications depend upon hundreds of CAs around the world choosing to do the right thing. As a consequence, anyone of those CAs can become the weakest link in the chain.

In case of occurring security incidents at a CA, the affected certificates should be revoked instead of selling the issuing CAs and their key materials to third parties. As a consequence, these TLS certificates are less valuable and are sold by the acquiring companies for a lower price. However, acquiring a CA and the transfer of key materials should be transparent to the users of the PKI and well documented for later lookups.

Further, the TLS certificates and PKI should provide non-technical users the possibility to differentiate low-value TLS certificates from high-value TLS certificates in order to decide, which URL to trust. At least for the European context, a list of trusted CAs is available. In order to decide whom to trust, a global list of trusted CAs would be beneficial. Besides the differentiation of low and high-value TLS certificates, the addition of a reputation level of CAs within the trusted list should be established.

Next, we found that the majority of TLS certificates used by Booter URLs are issued by the Comodo Group Company. According to [41], Comodo indeed is leading the overall market (33.6%), however Symantec is still stronger among top ranked websites. One possible mitigation strategies might be the removal of certain certification chains, but removing intermediate and root certificates from the trust store of the browser might cause a negative impact for non-technical users. As a consequence, there is clearly a need to provide the possibility to differentiate between different levels of trust for non-technical users and to improve usability of TLS certificates.

 ISBN: 978-1-61208-570-8 

We found that in some cases Booter URLs do not match their SANs or CN within the TLS certificate. Current Web browsers raise a warning, but non-technical users might accept the exception shown in the Web browser and can access the website as expected. One approach to block the use of Booter websites and thus mitigate the effects caused by Booter attacks is to implement an automatic check and comparison of the CN and SANs with the Booters URL.

Besides the not matching SANs or CN with the Booter URL, we found that the Booter websites that use a TLS certificate specified 21 SANs on average. In total, we found 3 156 SANs specified within the TLS certificate of the Booter URLs listed on the Booter blacklist. Within these SANs, we identified further suspicious domain names that contain various terms to describe a Booter (e.g., www.beststresser.com uses also the SAN of *.bestipstressers.com). We suggest to use the SANs provided in each TLS certificate to extend the Booter blacklist. We also identified several TLS certificates that provide more than 90 SANs. One explanation might be that this Booter URL resides in a CDN network. For reasons of usability, CDN often share a single TLS certificate.

We identified numerous Booter URLs that reside in CDN networks. Even though these Booter websites carry out DDoS attacks and thus cause network traffic within the CDN network, in accordance with [42][43], we assume the amount of network traffic caused by these attacks is such that the CDN network operators might not be able to detect these DDoS attacks as their effects might be to small.

## IV. Related work

Over recent years, DDoS-as-a-Service gained an increasing research interest. [2] analyzed attacks generated by 14 distinct Booter websites. Therefore, Santanna et al. [2] analyzed the attack types, the attack volume and the geographic distribution of the Booters. They found that DDoS-as-a-Service offers non-technical skilled users the possibility to perform DDoS attacks. In total, the authors were able to achieve up to 1.6 Gbps Domain Name System (DNS)-based and up to 7.0 Gbps CharGen attack traffic. In [3], the authors provide an overview of 15 operational MySQL databases (including users, attacks and infrastructures) of Booters. Besides the operational databases, Steinberger et al. [4] presented the Booter's scenario elements and their relationships. A Booters' scenario consists of the six elements: A Booter customer, a payment system, a database, a Booter website including DDoS Protection Service, a Booter infrastructure and a target system.

To mitigate DDoS attacks performed by Booter websites, a list of Booter characteristics to detect and classify them was created in the work of [44]. An initiative to share the (most extensive) list of websites that offer DDoS attacks as a paid service is provided on http://booterblacklist.com. However, none of the aforementioned works focused on the use of TLS certificates used by Booter URLs as one possible mitigation strategy.

## V. Conclusions

In this paper, we conducted a structured analysis of the use of TLS certificates of 434 active Booter websites, which allowed us to gain insight into the certificate chain, used cryptography and cipher suites, negotiation protocol, issuer and the validity of the certificate. Our analysis revealed that an increasing number of Booter owners make use of TLS to hide their malicious activities inside encrypted traffic and thus remain undetected by current security tools. Further, we found that Booter websites predominantly use elliptic curve cryptography combined with Galois/Counter mode. We recognized that the TLS certificates of Booter websites often specify numerous SANs. Therefore, we suggest to include the SANs into the Booter blacklist in case they contain certain terms used to describe Booters (e.g., `*stresser*, *ddoser*`) as they are most likely also Booter websites.

## Acknowledgment

This work was partly supported by the German Federal Ministry of Education and Research (BMBF), the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within the Center for Research in Security and Privacy (CRISP) and by the Netherlands Organisation for Scientific Research (NWO) Distributed Denial-of-Service Defense: Protecting Schools and other public organizations (D3) Project.

## References

[1] Arbor Networks, "Worldwide Infrastructure Security Report," 2015. [Online]. Available from: https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf 2017.05.11

[2] J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Zambenedetti Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in IFIP/IEEE International Symposium on Integrated Network Management (IM), May 2015, pp. 243–251.

[3] J. Santanna, R. Durban, A. Sperotto, and A. Pras, "Inside booters: An analysis on operational databases," in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, May 2015, pp. 432–440.

[4] J. Steinberger, J. J. Santanna, E. Spatharas, H. Amler, N. Breuer, K. Graul, B. Kuhnert, U. Piontek, A. Sperotto, H. Baier, and A. Pras, ""Ludo" - kids playing Distributed Denial of Service," in TNC16, J. Bergström, G. Hórvath, and B. Schofield, Eds. GÉANT Ltd, November 2016. [Online]. Available from: http://www.eunis.org/erai/2016-2/

[5] Venafi, "Is your SSL Traffic Hiding Attacks?" 2014. [Online]. Available from: https://www.venafi.com/blog/your-ssl-traffic-hiding-attacks 2017.05.11

[6] Dell Inc., "2016 Dell Security Annual Threat Report," 2016. [Online]. Available from: https://www.sonicwall.com/whitepaper/2016-dell-security-annual-threat-report8107907 2017.05.11

[7] E. Gerck, "Overview of Certification Systems: X.509, PKIX, CA, PGP & SKIP," 2000. [Online]. Available from: http://nma.com/mcg-mirror/certover.pdf 2017.05.11

[8] "Booter (black)List." [Online]. Available from: http://booterblacklist.com 2017.06.13

[9] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 (Proposed Standard), Internet Engineering Task Force, Aug. 2008. [Online]. Available from: http://www.ietf.org/rfc/rfc5246.txt 2017.05.11

[10] D. Eastlake 3rd, "Transport Layer Security (TLS) Extensions: Extension Definitions," RFC 6066 (Proposed Standard), Internet Engineering Task Force, Jan. 2011. [Online]. Available from: http://www.ietf.org/rfc/rfc6066.txt 2017.05.11

 ISBN: 978-1-61208-570-8 

[11] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280 (Proposed Standard), Internet Engineering Task Force, May 2008. [Online]. Available from: http://www.ietf.org/rfc/rfc5280.txt 2017.05.11

[12] W3Techs, "Usage of SSL certificate authorities for websites," 2016. [Online]. Available from: http://w3techs.com/technologies/overview/ssl_certificate/all 2017.05.11

[13] B. Hein, "PKI Trust Models: Whom do you trust?" 2013. [Online]. Available from: https://www.sans.org/reading-room/whitepapers/vpns/pki-trust-models-trust-36112 2017.05.11

[14] CA/Browser Forum , "EV SSL Certificate Guidelines V1_5_9," 2016. [Online]. Available from: https://cabforum.org/extended-validation 2017.05.11

[15] European Commision, "EU Trusted Lists of Certification Service Providers," 2016. [Online]. Available from: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers 2017.05.11

[16] Anonymous, "Comments on the Article of Detecting Certificate Authority compromises and web browser collusion," 2011. [Online]. Available from: https://blog.torproject.org/blog/detecting-certificate-authority-compromises-and-web-browser-collusion 2017.05.11

[17] Comodo Group, Inc, "Secure faxing. Secure e-mail. Secure backup - Anywhere, anytime." 2004. [Online]. Available from: https://www.comodo.com/news/press_releases/12_01_04.html 2017.05.11

[18] Thawte, "About Thawte," 2016. [Online]. Available from: https://www.thawte.com/about/ 2017.05.11

[19] T. Callan, "VeriSign completes acquisition of GeoTrust," 2005. [Online]. Available from: http://www.symantec.com/connect/blogs/verisign-completes-acquisition-geotrust 2017.05.11

[20] I. Grant, "Symantec completes $1.28bn VeriSign acquisition," 2010. [Online]. Available from: http://www.computerweekly.com/news/1280093508/Symantec-completes-128bn-VeriSign-acquisition 2017.05.11

[21] C. Soghoian and S. Stamm, "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL (Short Paper)," in Proceedings of the 15th International Conference on Financial Cryptography and Data Security, ser. FC'11. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 250–259.

[22] E. Nigg, "Unbelievable!" 2008. [Online]. Available from: https://groups.google.com/forum/#!topic/mozilla.dev.tech.crypto/nAzIKSBEh78%5B1-25%5D 2017.05.11

[23] SSL Shopper, "SSL Certificate for Mozilla.com Issued Without Validation," 2008. [Online]. Available from: https://www.sslshopper.com/article-ssl-certificate-for-mozilla.com-issued-without-validation.html 2017.05.11

[24] Comodo Group, Inc, "Comodo SSL Affiliate - The Recent RA Compromise," 2011. [Online]. Available from: https://blog.comodo.com/other/the-recent-ra-compromise 2017.05.11

[25] Comodo Group, Inc , "Comodo Incident Report," 2011. [Online]. Available from: https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html 2017.05.11

[26] DigiNotar Damage Disclosure, "DigiNotar reports security incident," 2011. [Online]. Available from: https://blog.torproject.org/blog/diginotar-damage-disclosure 2017.05.11

[27] VASCO Data Security International, Inc, "DigiNotar reports security incident," 2011. [Online]. Available from: https://www.vasco.com/about-vasco/press/2011/news_diginotar_reports_security_incident.html 2017.05.11

[28] Microsoft Security TechCenter, "Improperly Issued Digital Certificates Could Allow Spoofing," 2015. [Online]. Available from: https://technet.microsoft.com/en-us/library/security/3046310.aspx 2017.05.11

[29] D. Pauli, "Microsoft scrambles to kill Live.fi man-in-the-middle diddle," 2015. [Online]. Available from: http://www.theregister.co.uk/2015/03/17/redmond_scrambles_to_kill_livefi_maninthemiddle_diddle 2017.05.11

[30] E. Rescorla, "HTTP Over TLS," RFC 2818 (Informational), Internet Engineering Task Force, May 2000. [Online]. Available from: http://www.ietf.org/rfc/rfc2818.txt 2017.05.11

[31] S. Alrwais, K. Yuan, E. Alowaisheq, Z. Li, and X. Wang, "Understanding the Dark Side of Domain Parking," in 23rd USENIX Security Symposium (USENIX Security 14). San Diego, CA: USENIX Association, Aug. 2014, pp. 207–222. [Online]. Available from: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/alrwais 2017.05.11

[32] Z. Li, S. Alrwais, Y. Xie, F. Yu, and X. Wang, "Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures," in Security and Privacy (SP), 2013 IEEE Symposium on, May 2013, pp. 112–126.

[33] CA/Browser Forum , "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates Version 1.3.7," 2016. [Online]. Available from: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.7.pdf 2017.05.11

[34] Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson, "An End-to-End Measurement of Certificate Revocation in the Web's PKI," in Proceedings of the 2015 ACM Conference on Internet Measurement Conference, ser. IMC '15. New York, NY, USA: ACM, 2015, pp. 183–196.

[35] "Ciphersuites of TLS Client." [Online]. Available from: https://www.dasec.h-da.de/staff/benjamin-kuhnert 2017.06.13

[36] J. Salowey, A. Choudhury, and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS," RFC 5288 (Proposed Standard), Internet Engineering Task Force, Aug. 2008. [Online]. Available from: http://www.ietf.org/rfc/rfc5288.txt 2017.05.11

[37] E. Rescorla, "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)," RFC 5289 (Informational), Internet Engineering Task Force, Aug. 2008. [Online]. Available from: http://www.ietf.org/rfc/rfc5289.txt 2017.05.11

[38] E. Barker, "Recommendation for Key Management - Part 1: General," 2016. [Online]. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf 2017.05.11

[39] N. Sullivan, "ECDSA: The digital signature algorithm of a better internet," 2014. [Online]. Available from: https://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet 2017.05.11

[40] namestat.org , "How many top-level domains are there now? 300? 500? No, it's 1,000," 2016. [Online]. Available from: https://namestat.org/s/gtld-program 2017.05.11

[41] W3Techs, "Comodo has become the most widely used SSL certificate authority," 2016. [Online]. Available from: https://w3techs.com/blog/entry/comodo_has_become_the_most_widely_used_ssl_certificate_authority 2017.05.11

[42] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Collaborative attack mitigation and response: A survey," in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), May 2015, pp. 910–913.

[43] J. Steinberger, L. Schehlmann, S. Abt, and H. Baier, Anomaly Detection and Mitigation at Internet Scale: A Survey. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 49–60.

[44] J. J. Santanna and A. Sperotto, "Characterizing and Mitigating the DDoS-as-a-Service Phenomenon," in Monitoring and Securing Virtualized Networks and Services: 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2014, A. Sperotto, G. Doyen, S. Latré, M. Charalambides, and B. Stiller, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 74–78.