

Georgia State University

ScholarWorks @ Georgia State University

EBCS Reports

Evidence-Based Cybersecurity Research Group

2020

Extended Validation in the Dark Web: Evidence from Investigation of the Certification Services and Products Sold on Darknet Markets

David Maimon

Yubao Wu

Nicholas Stubler

Praneeth Sinigirikonda

Follow this and additional works at: https://scholarworks.gsu.edu/eecs_reports

Extended Validation in the Dark Web:

Evidence from Investigation
of the Certification Services
and Products Sold on
Darknet Markets

David Maimon

Yubao Wu

Nicholas Stubler

Praneeth Sinigirikonda

The Evidence-Based Cybersecurity Research Group
at Georgia State University

EXECUTIVE SUMMARY

TLS certificates fulfill two critical security functions. First, the certificate plays a key role in authenticating and verifying the identity of a host, client or application. Second, it enables the encryption of data exchanged between a client and a server. To support the sensitive operation of identity verification, SSL/TLS certificates are supposed to be issued by trusted certificate authorities (CAs) who verify and check that companies are legitimate in order to reduce the risk of fraud and establish trust in a website or service.

However, in March 2019, the Evidence-Based Cybersecurity Research Group at the Andrew Young School of Policy Studies at Georgia State University and Venafi released a detailed report, which offered evidence of the presence of a steady supply of SSL/TLS certificates on several darknet markets (Maimon et al. 2019). Specifically, we reported that SSL/TLS certificates are offered for sale either as part of crimeware services and products (for example, malicious websites and ransomware) or as a standalone product, at prices ranging from \$260 to \$1,600 (depending on the type of certificate and scope of additional services offered). In these advertisements, several vendors offered Extended Validation (EV) certificates for sale; these certificates require confirmation of the legal entity of the owner by a designated CA and are designed to confer the highest level of trust.

As a next step, we wanted to explore whether darknet vendors were able to deliver on their promise to supply EV certificates. To this end, we communicated with these vendors over various communication platforms between December 2018 and August 2019, and this report details our findings from this intensive research effort and outlines our insights.

Our findings show that the process employed by CAs to validate the true identity of companies and organizations is problematic at best and has already been outsmarted by organized crime groups that operate around the world to issue EV certificates to nonexistent retail and financial organizations.

Key research findings include:

- Posts that promise to deliver EV certificates are advertised on darknet and clearnet platforms, both as add-on services for web design projects and as standalone services.
- It is possible to buy valid EV certificates on the dark web for completely fictional companies—our researchers were able to buy three certificates from two of the top 10 CAs operating in the U.S. and U.K.
- Dark web vendors are tricking CAs by obtaining fraudulent documents and using this to obtain legitimate government documents. Our researchers received legal documentation for nonexistent companies, including “Certificate of Incorporation of a Private Limited Company” in the U.K. and “Certificate of Formation of a Limited Liability Company” in the U.S.
- Dark web vendors offering EV certificates as standalone products charge more for them than those that sell them as part of a bundle, with prices for standalone EV certificates retailing between \$1,000–\$15,000, compared with \$100–\$400 for those sold as part of a package of web services.
- Dark web vendors providing EV certificates as a standalone product are more likely to deliver. Our researchers tried to purchase an EV certificate bundled with web services, but we received a DV certificate.
- Obtaining certificates for financial services organizations is more costly (asking price ranges from \$10,000–\$15,000) than those offered for a retail website (asking price ranges from \$1,000–\$1,500).
- At least one vendor selling EV certificates is working with a sophisticated organized crime group, which operates across several countries and communicates directly with CAs.
- Although a small number of certificates were purchased as part of this research, CA business processes for evaluating identification documentation for EV certificates appear to be consistent across the industry, suggesting these tactics could be employed by a wide range of dark web vendors.

BACKGROUND

Encrypted Internet Communication, TLS Certificates and Certificate Authorities

Internet communication between clients' devices and servers is governed by various communication protocols. The Hypertext Transfer Protocol (HTTP), for example, defines how messages should be formatted and transmitted between computers connected to the internet and determines how applications and web servers should communicate and respond to queries. The Hypertext Transfer Protocol Secure (HTTPS) is the secure version of HTTP. This protocol encrypts the internet traffic between clients' browsers and the web servers they access, using one of two secure protocols: Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Both protocols use an "asymmetric" Public Key Infrastructure (PKI) system to provide confidential, encrypted communication between clients and servers by binding a "public" key and a "private" key (Kim et al. 2017). Anything encrypted with the public key can only be decrypted by the private key, and vice versa.

To facilitate confidential communications with clients, organizations need to install SSL or TLS certificates onto their web servers. These certificates bind together two important components: either a domain or server name with an organizational identity and location. When installed on a web server, the SSL or TLS certificate activates the padlock, and the HTTPS protocol allows secure connections from a web server to a browser.

To support the sensitive operation of identity verification, SSL/TLS certificates and their corresponding public and private encryption keys are issued by trusted CAs. CAs are charged with the task of employing various validation processes for different types of SSL/TLS certificates: Domain (DV), Organization (OV) and Extended (EV). DV and OV certificates require minimal validation while EV certificates require more extensive validation to ensure these higher-value certificates are issued only to legitimate companies, organizations and individuals.

Certificate Authorities' Issuing Process of EV Certificates

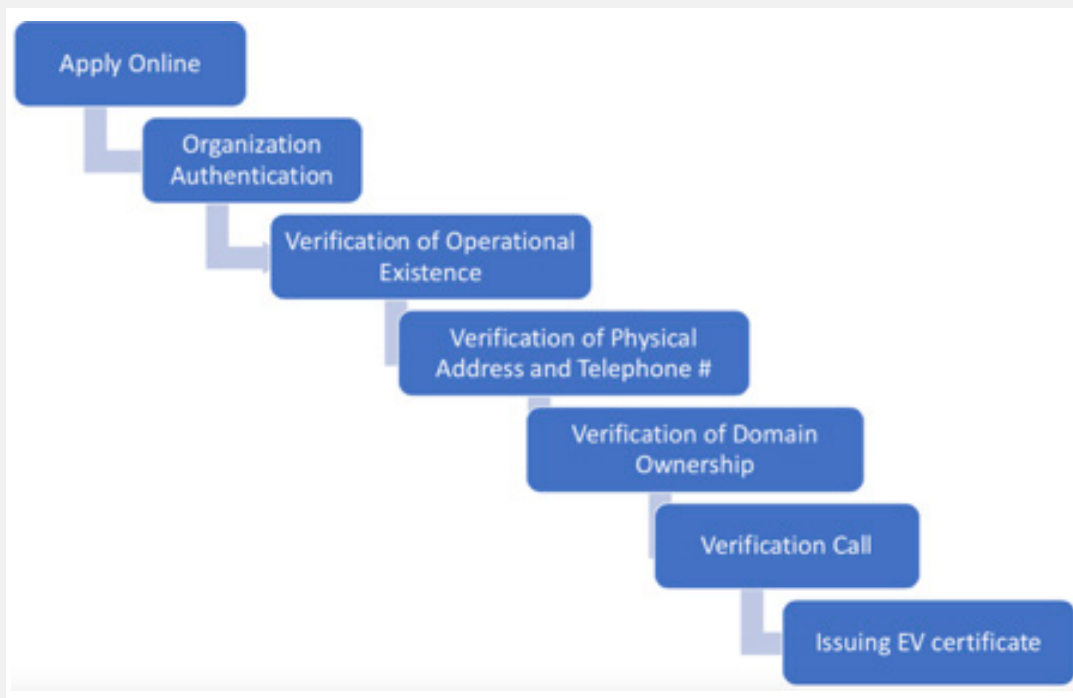
In an effort to understand CAs' issuing processes of EV certificates, we contacted 11 leading CAs—six of the top 10 in the U.S. and five of the top 10 in the U.K.—via phone and asked them to walk us through their verification process before issuing EV certificates.

CAs are required to follow a set of industry guidelines issued by the CA/Browser Forum that detail the identification process.² Figure 1 describes the various stages of the verification process. These are the steps taken by CAs and EV certificate applicants during each of stage of this process:

1. *Online Application:* Purchasers are required to complete online forms and provide basic information, including:
 - The full registered name of the company
 - Physical address of the company in the country where the certificate is to be registered
 - Direct contact information for the individual purchasing the certificate
 - Details to verify that the requesting individual works for the purchasing organization (such as a letter from HR confirming employment)
2. *Organizational Authentication:* Once the request has been submitted to the CA, the CA confirms that the information provided is correct. This can be done either through a search for official documentation (such as articles of incorporation or chartered licenses) or, in the U.S., through a Professional Opinion Letter (POL) from an attorney.
3. *Operational Existence:* In addition to legal documentation, most CAs also cross-check the information submitted by the requester against a reputable, third-party database (such as Dun & Bradstreet or Bloomberg) to confirm that the organization is currently operational. In the U.S., CAs also verify the organization has been operational for at least six months (this is also verified through a third-party database).

4. *Physical Address and Telephone Number:* The CA cross-references the information given against official government databases, such as Company House in the U.K. or state or municipal registers in the U.S., to confirm that the physical address and telephone number provided are correct.
5. *Domain Ownership:* Purchasers are required to prove they are the legal owners of the domain they are seeking to get certified. CAs can either verify this by checking a third-party database, such as who.is, or by having the applicant send an email from one of the five following email addresses:
 - Admin@YourDomainName.com
 - Administrator@YourDomainName.com
 - Webmaster@YourDomainName.com
 - Hostmaster@YourDomainName.com
 - Postmaster@YourDomainName.com
6. *Verification Call:* Finally the CA will call the purchasing individual at the number provided and reconfirm all of the information provided is correct.
7. *Issuing the Certificate:* Upon successful validation of the requesting organizations identify, an EV certificate is sent by email.

Figure 1. Validation Steps Taken by CA to Verify the Identity of EV Certificate Purchasers



If the processes used by trusted CAs to verify the identity of the requesting party can be spoofed, malicious actors can be issued an EV SSL/TLS certificate that delivers the highest levels of trust. This allows attackers to create malicious websites that appear more “trustworthy” to the

user and their browser.¹ Illegal online markets that populate the dark web may support malicious actors’ efforts to obtain authentic EV certificates and establish “legitimate” identities for the spoofed websites they build (Kim et al. 2017; Kozak et al. 2018).

¹ It is no more difficult to identify malicious traffic from a DV and OV certified website and an EV certified website. The technical challenge is the same.

The Availability of SSL/TLS Certificates on Darknet Markets

Darknet markets offer the hardware, software and materials needed to initiate all types of cybercrime (Yip et al. 2013). The first report we published from this project (Maimon et al. 2019) disclosed the presence of underground online markets for SSL/TLS certificates. Specifically, we reported that:

- Five of the Tor network markets observed by our group offered a steady supply of SSL/TLS certificates, along with a range of related services and products.
- SSL/TLS certificates are often packaged with crime-ware services and products, such as malicious websites and ransomware.
- Prices for certificates vary from \$260 to \$1,600, depending on the type of certificate and scope of additional services offered.

- At least one vendor on BlockBooth promises to issue certificates from reputable CAs. The seller also offers forged documentation, which allows attackers to present themselves as trusted U.S. or U.K. companies for less than \$2,000.

However, in the absence of a rigorous validation of both the services and products offered by these darknet vendors, it is difficult to assess the risk posed to online users by this market. Specifically, one may argue that this issue should be of lower concern if the ads on the darknet markets we have observed are posted by fraudsters who are not delivering the promised commodity than if the products are actually delivered. The second phase of our project explores whether darknet vendors deliver on their promise to supply EV certificates to interested parties, as well as assess the origin and quality of the products these vendors sell.

RESEARCH DESIGN AND METHODOLOGY

To accomplish our research objective, we applied for an Institutional Review Board² approval for this research. Once approval was granted, we dived into online markets and hacker forums that were active on the Tor network from October 2018–April 2019 and searched for “for sale” listings of TLS certificates.

Our research team discovered close to 70 relevant online market webpages on the Tor network. To explore for the presence of SSL- and TLS-related ads in each market, we typed in “TLS certificates” and “SSL certificates” in the

search bar of each market. Exhibits 1–5 present several example ads our team was able to find between January and April 2019 (i.e., followed by the publication of our first report (Maimon et al. 2019)).

Consistent with the findings reported in (Maimon et al. 2019), Exhibits 1–3 presents ads for SSL/TLS certificates which are packaged with malware and web design services. However, while Exhibits 1 and 2 present ads posted on Empire Market and Dream Market simultaneously, Exhibit 3 presents an ad posted on Bitify, a clearnet online market platform

Exhibit 1. SSL Certificates Sold Along with Malware Services on Empire Market

CodeSigning EV, EV, SSL Certificates

This is a product for those who want to make their malware undetectable, more legit and long lifespan. As the title says it is code signing...

Sold by [Vendor] February 21, 2019 Vendor Level 2 Trust level 1

Product Class	Features	Origin Country	Features
Quantity Left	Digital	Ships to	World Wide
Ends In	Unlimited	Payment	World Wide Escrow
	Never		

CodeSigning EV - 1 days - USD + 0.00 / order

Purchase price: **USD 400.00**

Qty: 1

0.096278 BTC / 6.594131 LTC / 6.940829 XMR

Description Feedback Refund policy

CodeSigning EV, EV, SSL Certificates

This is a product for those who want to make their malware undetectable, more legit and long lifespan.

As the title says it is code signing certificate. You can find more information here:

<https://www.globalsign.com/en/code-signing-certificate/ev-code-signing-certificates/>

I offer these certs and price as follows:

CodeSigning Comodo - \$ 400

CodeSigning EV GlobalSign - \$ 1500

EV SSL - \$ 400

² An institutional review board is a type of committee that applies research ethics by reviewing the methods proposed for research to ensure they are ethical.

Exhibit 2. SSL Certificates Sold Along with Web Design Services on Dream Market

Browse by category

- Services 6107
- Hacking 730
- IDs & Passports 1491
- Money 1060
- Other 907
- Cash out 1146

- Digital Goods 62724
- Drugs 84469
- Drugs Paraphernalia 465
- Services 6107
- Other 6162

Onion mirrors

uhvlt5gnqhad7.onion verified

jdlyhuwcvlvehvtd4.onion
 Ge6ly3uolmzce2.onion
 Teg7acrkuodcw3.onion
 vtpagrmvizecjo.onion
 igytrhmqj33ty5.onion
 6qocf6cjq2kyact.onion
 x3x20wb7jasax6q.onion
 bkjcpa2kdkmowwq.onion
 xyjycfmdzby22.onion
 nhb6cwf6syyqg.onion
 k3p0243s57mpa.onion

eCommerce with Private Host & Domain [+ SSL]


Vendor [REDACTED] (3)

Price [REDACTED]

Ships to Worldwide, Worldwide

Ships from PM

Escrow No



Product description

We are offering now eCommerce on one of the follow providers:

- AbanteCart
- PrestaShop
- WHMCS
- CubeCart
- osCommerce
- Zen Cart

Links

- Forum
- Help
- Conferences
- Vendor application
- Earn money

Exchange

BTC	1.0
mBTC	1000.0
BCH	28.3
USD	3618.5
EUR	3191.2
GBP	2868.9
CAD	4888.9
AUD	5048.5
mBCH	28366.0
BRL	14210.5
DKK	23828.9
NOK	31644.2
SEK	32863.2
TRY	19373.9
CNH	25019.2
HKD	28408.3
RUB	244192.9
INR	254676.1
JPY	408107.2

News

- Downtime & Recovery 13/09/2017
- Deposit delays 27/09/2015
- Forum under maintenance 12/08/2015
- Earn money by findng

Exhibit 3. SSL Certificates Sold Along with Web Design Services on Bitify

The screenshot shows a marketplace listing for an SSL certificate and web design services. At the top, there is a countdown timer showing 1 Day, 20 Hrs, 56 Min, and 33 Sec. Below the timer is a thumbnail image of a website. To the right of the timer, the listing details include: Available QTY: 8 Items; Buy Now: \$150.00 (Reference Only) and 0.011810 BTC; a 'Buy Now!' button; Item ID: #2133851; Reserve: Reserve price met; Condition: Brand New; Ending: 9/27/2019, 8:37:30 AM; Watch List: + Watch; Category: Misc (Digital Goods); Location: USA; Viewed: 63 times. At the bottom of the listing are 'Contact Seller' and 'Report Listing' buttons.

Item description

I will provide you with professional looking Custom made E-commerce Webstores! I've made thousands of websites and I know exactly what you need.

These websites can be used for ANY payment processor (PAYPAL+STRIPE+SQUARE+BRAINTREE)

You will only provide me with merchant details and I will connect it to the ecommerce website. And Bam you're ready to go!

What you will have:

- ✓ Aged domain
- ✓ Guaranteed satisfaction
- ✓ Ready to use E-commerce webstore
- ✓ Low-risk products
- ✓ professionally designed
- ✓ Hosting and Domain will be within the package
- ✓ SSL Certificate

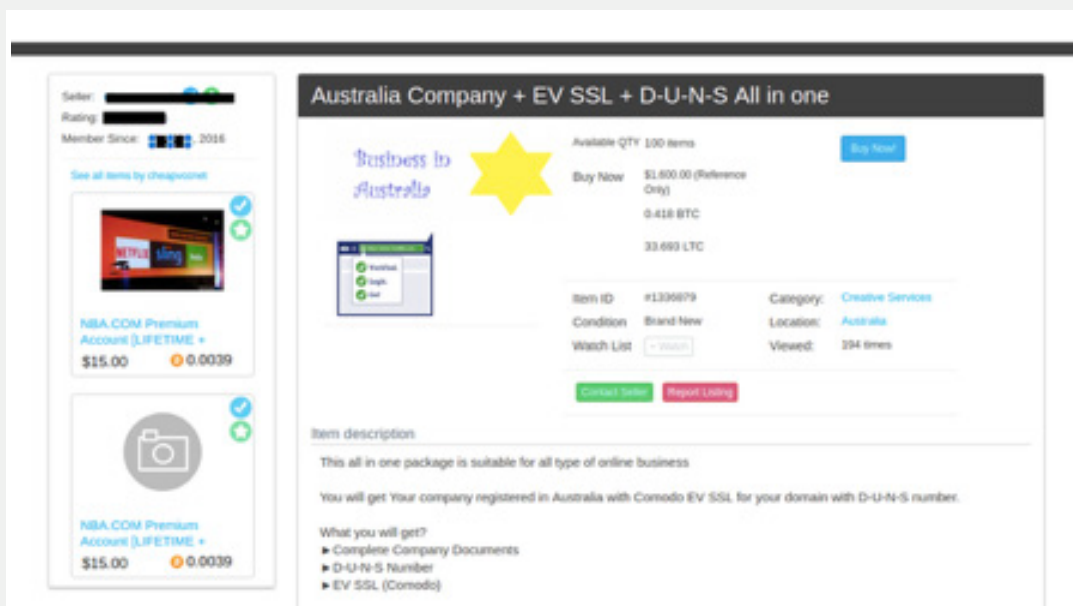
Similarly, Exhibits 4–5 present ads posted by vendors who promise to issue certificates from reputable CAs. However, while Exhibit 4 presents an ad posted on

BlockBooth, a darknet market platform, Exhibit 5 presents an ad posted on Bitify.

Exhibit 4. EV Certificates for U.K. and U.S. Companies BlockBooth—a Listing Platform on Open Bazaar



Exhibit 5. EV Certificates for Australian Companies on Bitify



Upon discovery of the above ads, as well as other ads that are not reported here but are available from the authors upon request, we randomly contacted two vendors—one who advertised the issuance of SSL/TLS certificates along with a web design service and the other who advertised EV certificate for sale—in order to assess whether their advertisements are truthful. Below, we describe our

interactions with a darknet market vendor who advertised the issuance of SSL/TLS certificates along with a web design service as well as our assessment of the product he provided to the group. Additionally, we elaborate on the interactions we had with a vendor who advertised EV certificates for sale on both clearnet and darknet underground markets, detailing our assessment of the products provided.

RESULTS

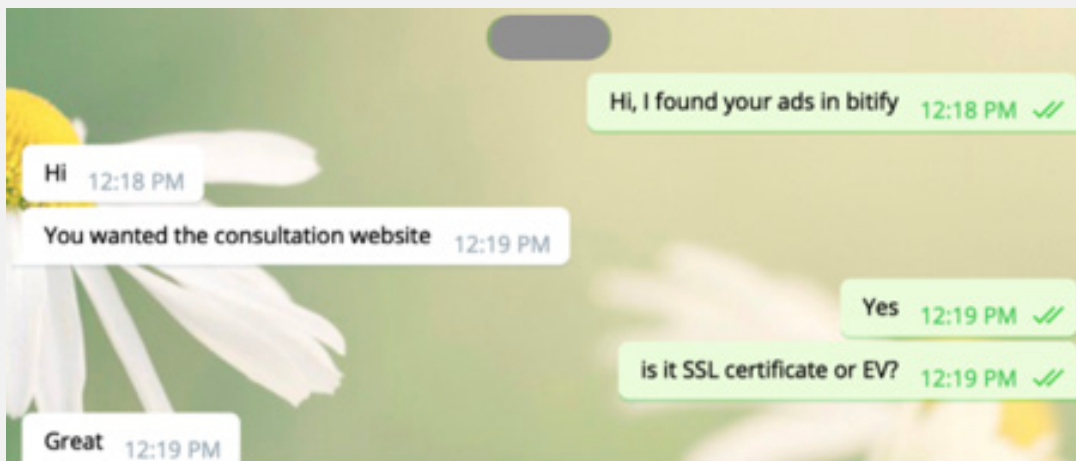
Case Study I: Web Design Service for an Online Retail Platform

Approaching and Building Trust

The vendor we approached with a request to design a retail website with an EV certificate installed on it preferred to be contacted by potential customers over Telegram. Exhibit 6 presents a screenshot of the initial interaction between our research group (in green) and the vendor (in white). Since the vendor offered several services, we

chose the package that was relevant to our needs in the context of this study and asked that our website include a function that allows a user to open an account, log in with a username and password and provide a response to a CAPTCHA.³ We also asked for an EV certificate to be installed on the website. When we asked the vendor what our new website could be used for, the response we got suggested utilizing it as a platform to run online scams and steal targets' cookies and passwords.

Exhibit 6. Approaching a Vendor Over Telegram



Negotiating

The vendor's response to our first query was prompt. After receiving our requirements for the desired website and the need for an EV certificate, the vendor mentioned that an annual fee will be required to install and maintain the certificate. An updated price (between \$200–\$400) was sent to us with an agreement to use an escrow service⁴ to complete the business transaction. The vendor promised that the complete website, including the EV certificate installed on it, would be delivered within two weeks from the time of payment. The vendor's available

methods of payment were money transfers to either a PayPal account or a Bitcoin wallet. An installment plan was agreed upon (to build trust), and the first payment was sent to the vendor.

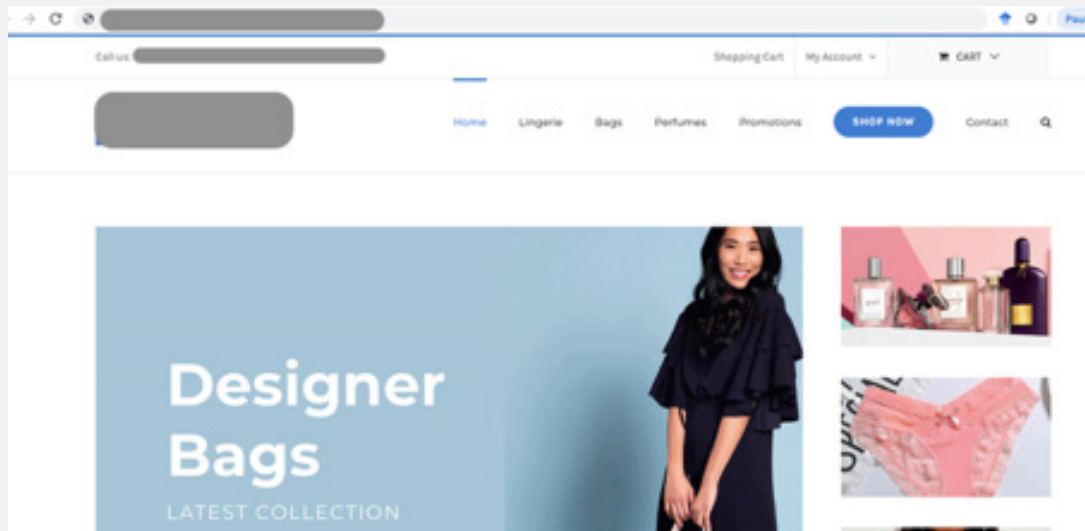
Product Arrival

A link to our newly purchased website arrived over Telegram about eight days after we sent our first payment. Exhibit 7 presents a screenshot of this website. We deleted the website URL as well as few other identifying details in effort to protect our team's safety.

³ CAPTCHA is a type of challenge–response test used in computing to determine whether the user is human or a bot.

⁴ Online escrow service is a third-party website/platform which could be used to securely conduct online transactions. Specifically, this service allows customers to avoid sending their payments directly to a seller, and instead to an Escrow company. The use of an escrow company services insure that it is only after the customer has received the product funds will be released to the seller.

Exhibit 7. Website Designed by Darknet Vendor and Delivered to Research Team



Quality and Authenticity Assessment

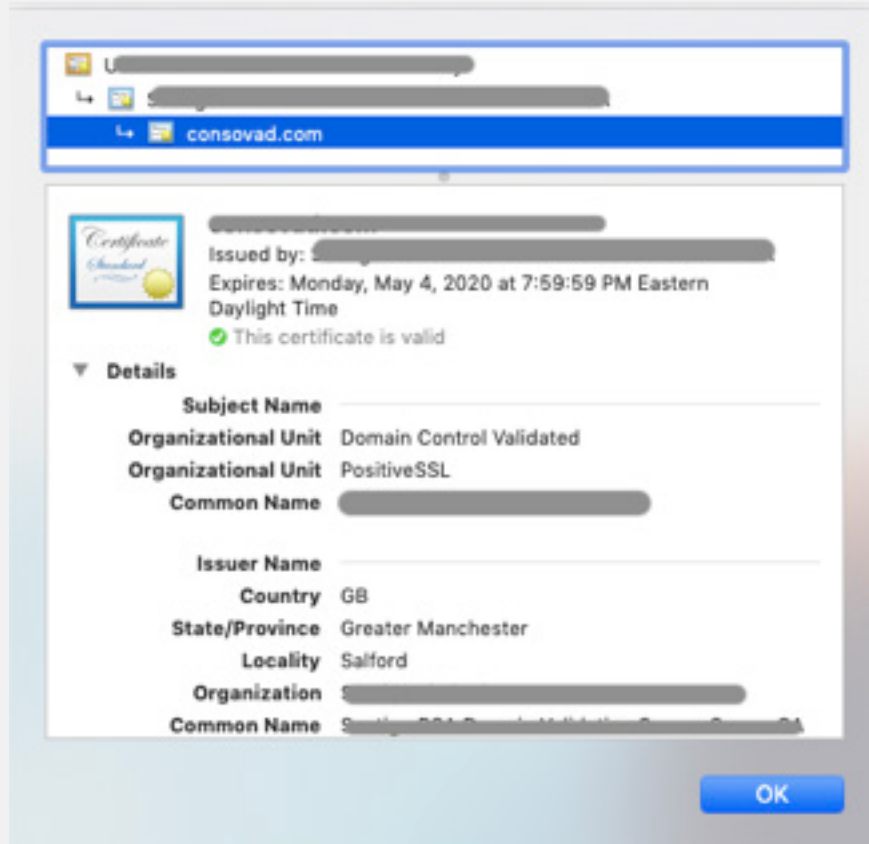
To assess the quality of the product we received from the vendor, we performed two checks. First, we attempted to establish an account on the website, and second, we examined the type of TLS certificate that was installed.

Results from these investigations yielded two key findings:

1. Although creating an account on the new website was feasible, no CAPTCHA banner was prompted to a user who attempted to log in to the account.
2. The type of TLS certificate installed on the website was of a DV type and not EV. Exhibit 8 presents a screenshot of the certificate installed on the website.

In order to assess whether the DV certificate was installed on the website by mistake, we contacted the vendor and asked him to explain why an EV certificate was not installed on the website. The vendor replied the following day and explained the DV certificate is installed on the website temporarily, until the EV certificate is delivered and installed. However, in order for the EV certificate to be installed, we were asked by the vendor to send the second payment installment directly to his Bitcoin wallet; we were promised that the funding would be used to cover the EV certificate costs. Unsurprisingly, once we paid the second installment, the vendor disappeared and stopped responding to our queries and messages.

Exhibit 8. DV Certificate Installed on the Website Designed by a Darknet Vendor



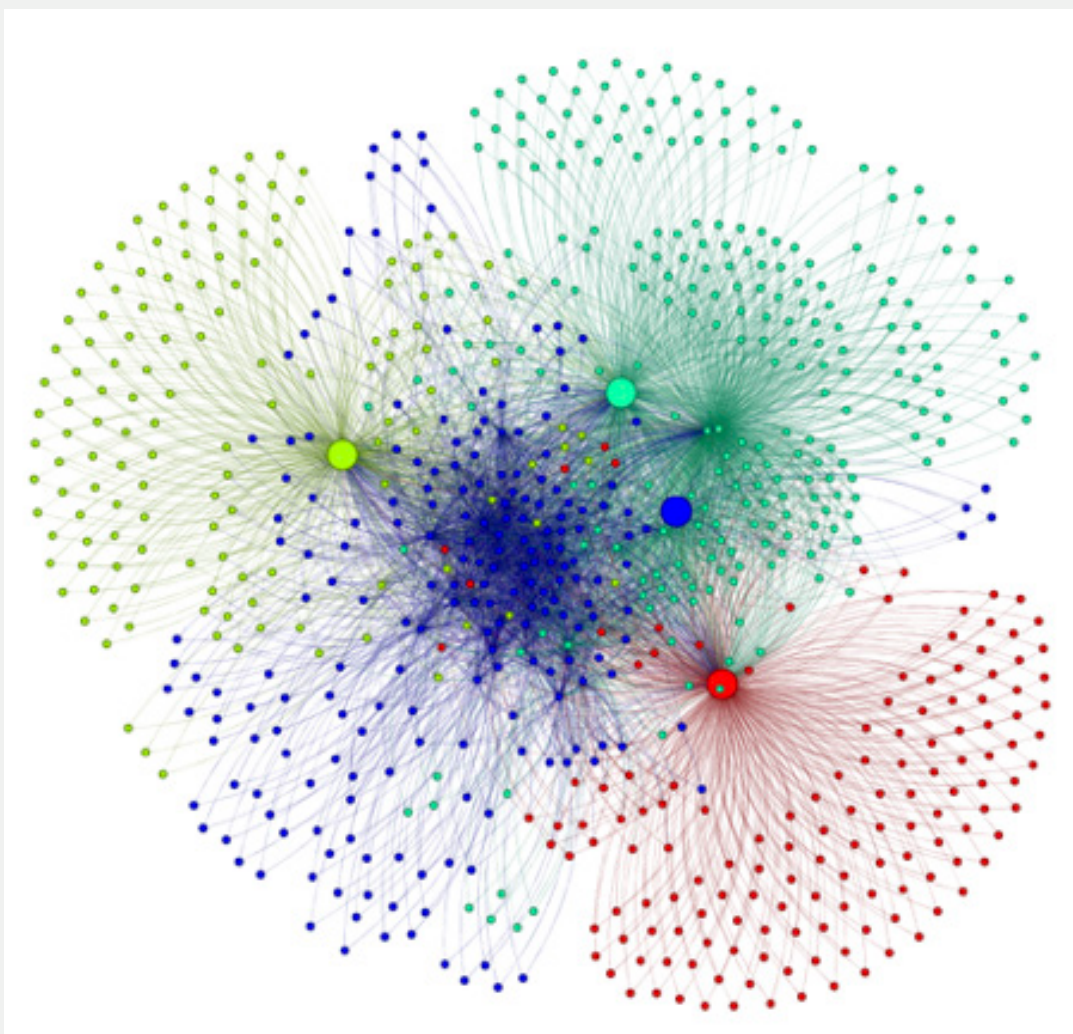
Case Study 2: Obtaining EV Certificates for U.K.-Based Organizations
Retail Website

Approaching and Building Trust

After our experience working with the previous vendor, we were keen to find a vendor with whom we could establish greater trust. Online markets allow people to rate vendors and disclose their transactions, which helps increase trust among potential customers. We were eager to find a vendor with an established presence on both clearnet and darknet markets.

The vendor we approached with a request to purchase EV certificates preferred to be contacted by potential customers via email, Skype or Telegram. By investigating this vendor's group of followers on one of the markets,⁵ our research team was able to map the online social network of the vendor and assess the online business ecosystem within which EV certificates were being sold.⁶ Figure 2 presents the first order (i.e., users followed by or being followed by the vendor directly) and second order (i.e., users followed by or being followed by the vendor's followers) connections of the vendor we approached (market with large blue circle).

Figure 2. Vendor First and Second-Order Connections (N = 742)



Nodes highlighted are those with greatest betweenness centrality. Colors indicate the communities (subgroups) that nodes belong to. Communities rely on the Girvan-Newman algorithm, which identifies groups of individuals who have in-group connections and few out-group connections.

⁵ Similar to social media platforms like Twitter, some clearnet and darknet platforms allow users to “follow” and be “followed” by other users of the platform.

⁶ Unfortunately, we couldn't create a similar social network for the first vendor discussed in Case Study 1 due to absence of relevant information in the market platform that was employed by the vendor.

All in all, the overall size of the vendor social network is composed of 742 actors; 65 vendors and customers are directly connected to the vendor and another 677 are following or are being followed by the vendor's followers. Importantly, three key vendors seem to be central to this network. Those three key vendors are represented by large red, green and light green circles. The large red circle (306 followers and following) represents a vendor who specializes in selling soft and hard illegal drugs (for example, Dutch MDMA crystals, Colombian cocaine and "Green Heineken" ecstasy). Some of the countries this vendor serves include Germany, U.K., Poland, Canada, Australia and Brazil. The large green dot (288 followers and following) represents a vendor who specializes in selling counterfeit brand products from China (for example, sunglasses and wallets). Finally, the large light green circle (238 followers and following) represents a vendor claiming to be a small business from Canada (Quebec) that specializes in selling seeds (almonds, pumpkins, cranberries and cashews). This social network demonstrates that both legitimate and illegitimate actors may have exposure to the unique underground market of TLS certificates.

Consistent with the platform used for contacting the first vendor, this vendor preferred to be contacted over Telegram. We shared a request to explore a potential purchase of an EV certificate for a U.K.-based retail website at first, and the vendor responded rapidly. He indicated that the prices advertised on the ad (between \$1,000–\$1,500) are lower than the actual prices he charges for those certificates and that the price varies based on the (1) type of retail the certificate would be used for; (2) the issuing CA and (3) the country in which the certificate will be issued. Depending on the customer's needs and the order level of complexity, the time it takes to complete an order can vary from a few days up to a month and a half. Payment could only be made using cryptocurrency coins, such as Bitcoin, Litecoin and Ethereum.

Negotiating

Drawing on our experience with the first vendor, we decided to request that the second vendor provide an EV certificate for a basic retail website we had created, which could support potential customers' online payments for various products they could buy directly from the website. We insisted on using an online escrow company service in this transaction and asked whether we could be given a discount. The vendor agreed to work with an online escrow company but refused to provide a discount, explaining that this operation is performed by a group of people. Accordingly, each member of the team is charged with handling different aspects of the operation, including verification and issuance of the certificates. The vendor assured the research team that his group is experienced and disclosed that he has successfully completed many projects in the past. Our request for an installment plan was approved.

Modus Operandi

Once agreement was reached between our group and the vendor, we were asked to provide an entity name and URL link for the website on which the EV certificate should be installed. The requested information was sent to the vendor, along with our first payment. The vendor thanked us and promised to be in touch within a few days.

Several days after we placed the order, our group received a dossier of official documents from the Registrar of Companies in England and Wales. The documents enclosed indicated the formation of a new company, which carried the entity name we provided to the vendor in the U.K. (importantly, although we received a digital copy of these documents, a hard copy version could also be mailed to a physical address). Exhibits 9 and 10 present two of the three official certificates we received from the vendor. In addition to the new company name, these documents included the names of the filing individual, as well as a physical address for the new company.⁷ Those details were cross-verified with the U.K. Companies House website (www.companieshouse.gov.uk) and were found to exist on those official databases.

⁷ We removed sensitive details from the two documents shown in Exhibits 9 and 10 in order to protect the safety and privacy of all personal involved in this research both as subjects and as researchers.

Exhibit 9. Certificate of Incorporation Document for a U.K.-Based Retail Website



**CERTIFICATE OF INCORPORATION
OF A
PRIVATE LIMITED COMPANY**

Company Number [REDACTED]

The Registrar of Companies for England and Wales, hereby certifies that
[REDACTED]

is this day incorporated under the Companies Act 2006 as a private company, that the company is limited by shares, and the situation of its registered office is in England and Wales.

Given at Companies House, Cardiff, on [REDACTED]

Exhibit 10. Certificate of Registration for U.K.-Based Retail Website

Company Number: [REDACTED] Date: [REDACTED] Certificate# 1
Shareholder: [REDACTED] Number of Shares: 1

DW PAYDAYS LIMITED
Incorporated under the Companies Act 2006

No. of Shares: **1** No. of Certificate: **1**

This is to certify [REDACTED]
of [REDACTED]
is (are) the Registered holder(s) of 1 Ordinary share(s)
of 1 GBP each fully paid, numbered 1
to 1 inclusive, of the Company, subject to the Memorandum
and Articles of Association of the Company.

Give under the Common Seal of the said Company (or executed by the signatures of the following officers)

this [REDACTED] day of [REDACTED] 2019

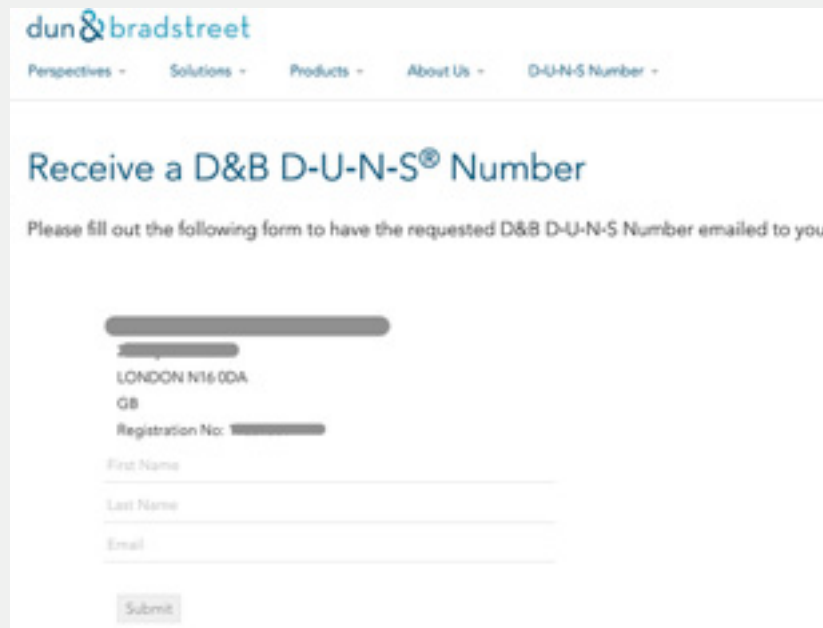
Director Director Secretary

NO TRANSFER OF THE WHOLE PORTION OF THE ABOVE SHARES CAN BE REGISTERED WITHOUT THE PRODUCTION OF THIS CERTIFICATE

In an effort to increase the legitimacy of the new retail entity he created, the vendor also obtained a Data Universal Numbering System (D-U-N-S) number from Dun and Bradstreet, a U.S.-based company that provides commercial data, analytics and insights for businesses and maintains a database of more than 300 million business

records worldwide. Exhibit 11 presents a screenshot of the new entity record on the Dun and Bradstreet website. Importantly, the physical address reported on Dun and Bradstreet's website for the entity matches the one reported on the U.K. Companies House website.

Exhibit 11. Registration of U.K.-Based Retail Company on the Dun and Bradstreet Website



The screenshot shows the Dun & Bradstreet website interface. At the top, the logo "dun & bradstreet" is displayed in blue. Below the logo is a navigation menu with links: "Perspectives -", "Solutions -", "Products -", "About Us -", and "D-U-N-S Number -". The main heading reads "Receive a D&B D-U-N-S® Number". Below this, a sub-heading states: "Please fill out the following form to have the requested D&B D-U-N-S Number emailed to you." The form contains several fields: a large greyed-out input field at the top; a field containing "LONDON N16 0DA" and "GB"; a field labeled "Registration No." followed by a greyed-out input; and three input fields for "First Name", "Last Name", and "Email". A "Submit" button is located at the bottom of the form.

Upon receiving these documents, the second installment was sent to the vendor. In addition, and per the vendor's request, we allowed the vendor access to the email server on which our website was installed. It was at that time that

an official request for an EV certificate was submitted by the vendor to the CA. Exhibit 12 presents the confirmation email we received for the EV certificate request submitted by the vendor.

Exhibit 12. Confirmation Email from CA for the Receipt of an EV Certificate Request to be Installed on a U.K.-Based Retail Website



From: [REDACTED]
To: [REDACTED]
Sent: March 20, 2019 9:00 AM
Subject: S [REDACTED]: Approve Certificate Request for [REDACTED] (Order #00000000)
Hello,

We've received a [REDACTED] certificate request for [REDACTED].

Order info:
Domain name: [REDACTED]
Order number: 40000400 [REDACTED]
Ordered on: 03/20/2019 [REDACTED]
Contact: Herman Wilson [REDACTED]
Certificate type: EV
Organization name: B [REDACTED]

Several days followed after the confirmation email, and after a series of confirmation activities taken by the vendor, we received an approval email for the issuance of

an EV certificate to our U.K.-based retail website, along with the EV certificate. Exhibit 13 presents a screenshot of the email.

Exhibit 13. Confirmation Email from CA for the Approval of an EV Certificate Request



From: [REDACTED]
To: [REDACTED]
Sent: [REDACTED]
Subject: [REDACTED]
ORDER NUMBER: [REDACTED]
COMMON NAME: [REDACTED]

Dear Herman Wilson,

Congratulations! [REDACTED] has approved your request for a [REDACTED] EV certificate. Your certificate is included at the end of this email.

INSTALLATION INSTRUCTIONS

Once the EV certificate was approved, the vendor notified the research team and asked for the final payment installment. We then installed the certificate on the website.

Exhibit 14 presents a screenshot of the website prior to the installation of the EV certificate, and Exhibit 15 shows the website after the installation of the EV certificate.

Exhibit 14. U.K.-Based Retail Website Appearance Prior to the Installation of an EV Certificate Presenting No Padlock and Company Location

The screenshot shows a web browser window with a grey address bar and no padlock icon. The page content includes a "Payment Information" section with two columns of form fields:

- Billing Address:** Full Name (John M. Doe), Email (john@example.com), Address (542 W. 10th Street), City (London), State (LDN), Country (UK), Zip (NR14 7PZ). A checkbox for "Shipping address same as billing" is checked.
- Payment:** Accepted Cards (MasterCard, Visa, American Express, Discover), Name on Card (John M. Doe), Credit card number (1000-2222-3333-4444), Exp Month (September), Exp Year (2022), CVV (123).

A red error message is displayed below the Exp Month field: "Automatic credit card filing is disabled because this form does not use a secure connection."

Exhibit 15. U.K.-Based Retail Website Appearance Presenting a Green Padlock and Company Location After the Installation of an EV Certificate

The screenshot shows the same web browser window, but now with a green padlock icon in the address bar and a search bar. The "Payment Information" section is identical to Exhibit 14, but the error message is gone. A "Cart" sidebar is visible on the right side of the page, showing a "Total" amount.


Quality and Authenticity Assessment

To assess the quality of the product we received from the vendor, we performed two checks.

First, we checked for the presence of the green padlock icon and the new entity name in the address bar. Second, we searched for the website identity and technical details of the EV certificate, which are disclosed on the website.

As may be observed in Exhibit 15, the installation of the EV certificate on our website resulted in the appearance of the green padlock in the address bar. In addition, the new entity name was also showing to the right of the green padlock (this detail is deleted from the image in order to protect the safety of both the vendor and research team). Exhibit 16 presents a screenshot of the EV certificate details, as disclosed on the website. Note that the details enclosed by this banner reveal the validity and truthfulness of the certificate.

Exhibit 16. Details of EV Certificate as It Appeared on U.K.-Based Retail Website

 Expires: Thursday, March 19, 2020 at 8:00:00 AM Eastern Daylight Time
✔ This certificate is valid

Details

Subject Name	
Business Category	Private Organization
Inc. Country	GB
Serial Number	
Country	GB
Locality	London
Organization	LIMITED
Organizational Unit	LIMITED
Common Name	
Issuer Name	
Country	US
Organization	
Organizational Unit	
Common Name	
Serial Number	
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Tuesday, March 19, 2019 at 8:00:00 PM Eastern Daylight Time
Not Valid After	Thursday, March 19, 2020 at 8:00:00 AM Eastern Daylight Time

Financial Institution

Approaching

The vendor's success in delivering an EV certificate for the U.K.-based retail website was surprising to our group. This vendor and his team obviously have a proficient process for obtaining real EV certificates for non-existent entities. We wanted to test this further by seeing if the vendor would issue a certificate for a nonexistent financial services institution, as this is a highly regulated industry. A financial services website, such as one for a bank or payday loan company, could be used to steal even more sensitive information—including salary, address, bank details and so forth. This would make it an even more valuable phishing site than a retail site.

Moreover, since the vendor advertised in his post that his team could deliver EV certificates from several CAs, we wondered if a similar modus operandi would be followed in obtaining an EV certificate from a different CA than the one used for the retail shop case. Therefore, we reached out to the vendor again and asked him to provide us with a quote for a U.K.-based online payday loan website.

The vendor responded to our inquiry by emphasizing that the verification for financial-type websites is longer than the one for the retail website and requires more work and team effort. However, he assured us that his team had experience issuing EV certificates for a wide range of websites, including shopping, digital products, hosting companies, and even investment and bank websites. The price for this work was significantly higher and ranged between \$10,000–\$15,000.

Negotiation

Similar to the negotiation we had with this vendor during the first purchase of an EV certificate, negotiation for an

EV certificate for the second website focused on the use of an online escrow company in this transaction as well as a payment installment plan. Our requests to work with an escrow company and for an installment plan were approved by the vendor. No discount was provided for the initial selling price.

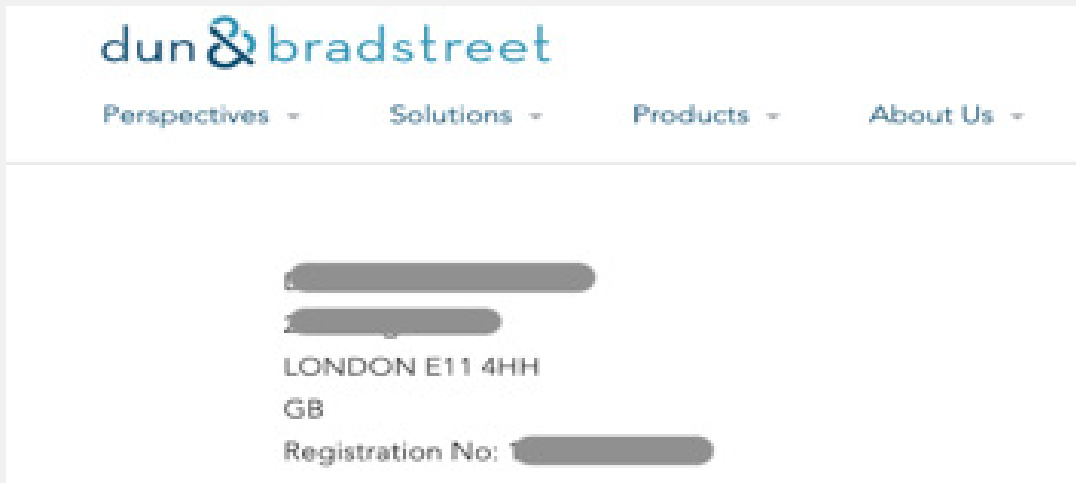
Modus Operandi

Once agreement was reached between our group and the vendor, we were asked to provide both an entity name and URL link for the website on which the EV certificate should be installed. The requested information was sent to the vendor, along with the first payment installment.

A few days after we placed the order, our group received a dossier of official documents from the Registrar of Companies in England and Wales, which indicated the formation of a new company that carried the entity name we provided to the vendor (we have not provided screenshots of those pieces of documentation in this report since they are similar to those presented in Exhibits 9 and 10). The documents included the new financial institution name and the name of the filing individual, as well as a physical address for the new company. Those details were cross-verified with the U.K. Companies House website and were found to exist on this official database.

To check whether a D-U-N-S number was issued for the new financial institution, we visited the Dun and Bradstreet website (<https://www.dnb.com/>) and searched the databases for evidence indicating the formation of our new company. Exhibit 17 presents a screenshot of the new entity record on the website. The physical address reported on the Dun and Bradstreet website for the entity was similar to the one reported on the U.K. Companies House website.

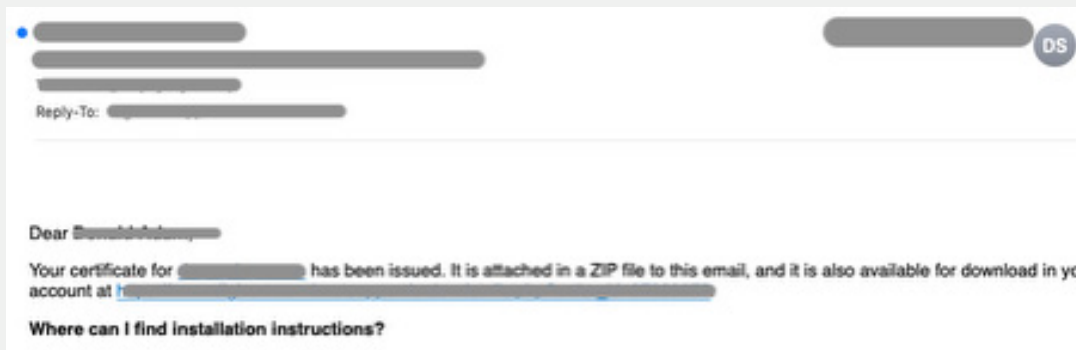
Exhibit 17. Registration of U.K.-Based Financial Institution on Dun and Bradstreet Website



Upon receipt of these documents, we sent the second installment to the vendor. In addition, and per the vendor's request, we allowed the vendor access to the email server on which our financial website was installed. It was at that time that an official request for an EV certificate was submitted by the vendor to the CA. A

few days after the confirmation email, and after a series of confirmation activities were taken by the vendor, we received an approval email for the issuance of an EV certificate to our U.K.-based financial website, along with the EV certificate. Exhibit 18 presents a screenshot of the email.

Exhibit 18. Confirmation Email from a CA for the Approval of an EV Certificate Request for a U.K.-Based Financial Institution Website



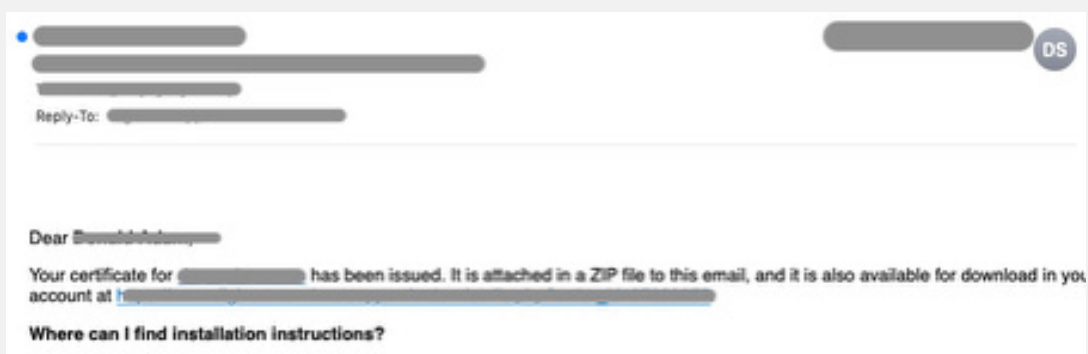
Once the EV certificate was approved, we were notified by the vendor and asked to send the final installment. We then installed the certificate on the website and checked its quality and authenticity.

Quality and Authenticity Assessment

In line with our assessment of the first EV certificate we received from the vendor, we first checked for the presence of the green padlock icon and the new entity name in the address bar.

As may be observed in Exhibit 19, the installation of the EV certificate on our website resulted in the appearance of the green padlock in the address bar. In addition, the new entity name also showed to the right of the green padlock (this detail is deleted from the image in order to protect the safety of both the vendor and research team).

Exhibit 19. U.K.-Based Financial Institution Website Appearance After the Installation of an EV Certificate



We also searched for the EV certificate details, which are disclosed on the website. Exhibit 20 presents a screenshot of the EV certificate details, as disclosed on the website.

Note that the details enclosed by this banner reveal the validity of the certificate.

Exhibit 20. Details of EV Certificate as It Appeared on U.K.-Based Financial Institution Website

Assurance EV Root CA
to Extended Validation Server CA
dlwpaydays.com

Issued by: Assurance EV Root CA
Expires: Wednesday, August 12, 2020 at 8:00:00 AM Eastern Daylight Time
This certificate is valid

Details

Subject Name	
Business Category	Private Organization
Inc. Country	GB
Serial Number	
Country	GB
Locality	London
Organization	
Organizational Unit	Marketing
Common Name	
Issuer Name	
Country	US
Organization	
Organizational Unit	
Common Name	Server CA
Serial Number	
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Wednesday, August 7, 2019 at 8:00:00 PM Eastern Daylight Time
Not Valid After	Wednesday, August 12, 2020 at 8:00:00 AM Eastern Daylight Time

Case Study 2: US

Approaching and Building Trust

The vendor's success in delivering two EV certificates for U.K.-based businesses' websites was concerning to our group. However, since the vendor advertised his team could deliver EV certificates from numerous CAs in several countries, we wondered if a similar method of operation would be employed while obtaining an EV certificate to a financial institution website that operates in the U.S. Therefore, we reached out to the vendor again and asked him to provide us with a quote for a U.S.-based online loans and payday website.

The vendor responded to our inquiry by emphasizing that the verification for a financial-type website in the U.S. would be complicated and would require a larger team than the one operated in the U.K. Verification for the company would have to be done using official documentation from Delaware, and the price for obtaining an EV certificate for a U.S.-based financial institution would range between \$6,000–\$8,500. The vendor reassured our team that his group is quite experienced working in the U.S.

Negotiating

Consistent with the negotiation we had with this vendor during our previous purchases of EV certificates,

negotiation for the purchase of an EV certificate for the U.S.-based website focused on our team's desire to use an online escrow company in this transaction as well as a payment installment plan. Our requests to work with an escrow company and for an installment plan were approved by the vendor. No discount was provided for the initial selling price.

Modus Operandi

Once an agreement was reached between our group and the vendor, we were asked by the vendor to provide both an entity name and URL link for the website on which the EV certificate should be installed. The requested information was sent to the vendor, along with the first payment. A few days after we placed the order, our group received a dossier of official documents from the Division of Corporations in Delaware, which indicated the formation of a new company that carried the entity name we provided to the vendor. Exhibits 21 and 22 present the two official documents we received from the vendor. The documents included the new financial institution name and the name of the filing individual, as well as a physical address for the new company. Those details were cross-verified with the website and were found to exist on those official databases.

Exhibit 21. Certificate of Formation Document for a U.S.-Based Financial Institution Website

State of Delaware
Secretary of State
Division of Corporations
Delivered
1/1/11

**CERTIFICATE OF FORMATION
OF**

[Redacted]

(A Delaware Limited Liability Company)

First: The name of the limited liability company is: [Redacted]

Second: Its registered office in the State of Delaware is located at [Redacted],
[Redacted], County of Sussex. The registered agent in charge thereof is [Redacted]

IN WITNESS WHEREOF, the undersigned, being fully authorized to execute and file this document have signed below and executed this Certificate of Formation on this [Redacted]

[Redacted]

Exhibit 22. Statement of Authorized Person to U.S.-Based Financial Institution Website

STATEMENT OF AUTHORIZED PERSON

IN LIEU OF ORGANIZATIONAL MEETING
FOR

[Redacted]

We, [Redacted], Inc., the authorized person of [Redacted] – a Delaware Limited Liability Company – hereby adopt the following resolution pursuant to Section 18-201 of the Delaware Limited Liability Company Act:

Resolved: That the Certificate of Formation of [Redacted] was filed with the Secretary of State of Delaware on [Redacted].

Resolved: That on [Redacted] the following persons were appointed as the initial members of the Limited Liability Company until their successors are elected and qualify:

[Redacted]

Resolved: That the undersigned signatory hereby resigns as the authorized person of the above named Limited Liability Company.

This resolution shall be filed in the minute book of the company.

[Redacted Signature Line]
[Redacted Name Line]

To check whether a D-U-N-S number was issued for the new financial institution, we visited the Dun and Bradstreet website and searched the databases for evidence indicating the formation of our new company.

Exhibit 23 presents a screenshot of the new entity record on the website. The physical address reported on the Dun and Bradstreet's website for the entity was similar to the one reported in the Delaware Division of Corporations.

Exhibit 23. Registration of U.S.-Based Financial Institution on Dun and Bradstreet Website

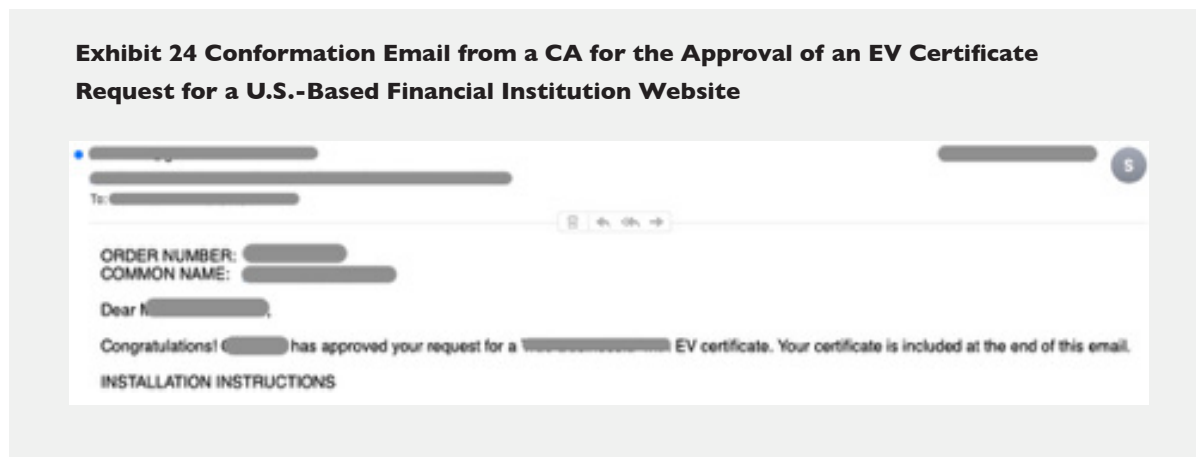
Email D&B D-U-N-S® Number

Please fill out the following form to have the requested D&B D-U-N-S® Number emailed to you.

[Redacted] LC
[Redacted]
Lewes, Delaware 19958-3608
[Redacted]

Upon receipt of these documents, we sent the second installment to the vendor. In addition, and per the vendor's request, we allowed the vendor access to the email server on which our financial institution website was installed. It was at that time that an official request for an EV certificate was submitted by the vendor to the CA.

A few days after the confirmation email and a series of confirmation activities taken by the vendor, we received an approval email for the issuance of an EV certificate to our U.S.-based financial institution website, along with the EV certificate. Exhibit 24 presents a screenshot of the approval email.



Once the EV certificate was approved, we were notified by the vendor and asked to send the final installment. We then installed the certificate on the website and checked the quality and authenticity of the certificate.

Quality and Authenticity Assessment

In line with our assessment of the previous EV certificates we received from the vendor, we first checked for the presence of the green padlock icon and the new entity name in the address bar.

As may be observed in Exhibit 25, the installation of the EV certificate on our website resulted in the appearance of the green padlock in the address bar. In addition, the new entity name also showed to the right of the green padlock (this detail is deleted from the image in order to protect the safety of both the vendor and research team). We also searched for the EV certificate details which are disclosed on the website. Exhibit 26 presents a screenshot of the EV certificate details, as disclosed on the website. Note that the details enclosed by this banner reveal the validity of the certificate.

Exhibit 25. U.S.-Based Financial Institution Website Appearance After the Installation of an EV Certificate

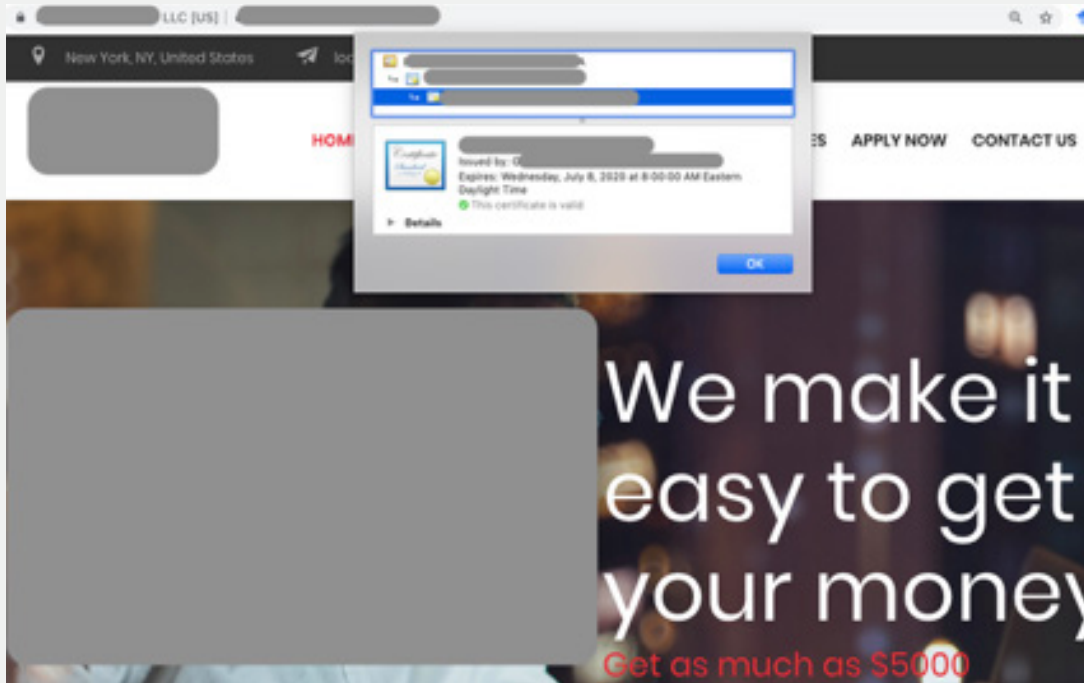


Exhibit 26. Details of EV Certificate as It Appeared on U.S.-Based Financial Institution Website

Issued by: [Redacted]
Expires: Wednesday, July 8, 2020 at 8:00:00 AM Eastern Daylight Time
This certificate is valid

Details

Subject Name	[Redacted]
Business Category	Private Organization
Inc. Country	US
Inc. State/Province	Delaware
Serial Number	[Redacted]
Country	US
State/Province	Delaware
Locality	LEWES
Organization	[Redacted]
Organizational Unit	Division of Corporations
Common Name	[Redacted]
Issuer Name	[Redacted]
Country	US
Organization	[Redacted]
Organizational Unit	[Redacted]
Common Name	[Redacted]
Serial Number	[Redacted] 1 E3
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Monday, July 8, 2019 at 8:00:00 PM Eastern Daylight Time
Not Valid After	Wednesday, July 8, 2020 at 8:00:00 AM Eastern Daylight Time

OK

DISCUSSION

An EV SSL/TLS certificate is designed to be the most trusted certificate on the market and is issued by CAs that follow a rigorous validation process aimed at identifying the requester's true identity. Specifically, the CA/Browser Forum and Microsoft guidelines for obtaining an EV certificate require that the requester provide multiple pieces of identifying information, including the company's D-U-N-S number (unique numeric identifiers assigned to a single business entity) or a letter from a certified public accountant who can verify the legitimacy of the business, when a certificate is requested. After submitting the request, the CA is required to authenticate the legal existence and identity of the requesting party by verifying the company's trade name and its operational and physical existence, as well as its ownership of the domain name.

Evidence presented in this report indicates that at least one international organized crime group has been able to exploit the unique problems embedded within the EV validation process used by CAs, and this group is able to issue EV certificates for websites of nonexistent retail and financial institutions in both the U.K. and U.S. Specifically, these online vendors harness their knowledge of CA validation processes to sell EV certificates to interested parties. This discovery is a result of an extensive research effort through which three EV certificates for nonexistent retail and financial organizations were sold to our team.

The findings presented in this report add to the ongoing debate regarding the effectiveness and necessity of EV certificates in increasing trust among internet users.

Specifically, our findings verify James Burton's (2017) experiment yet take it to the next level by exposing that at least one organized crime group now gets EV certificates from a legitimate CA and sells them on both clearnet and darknet markets. Burton's suggestion that malicious actors could get access to credentials off the dark web, use those to set up a fake company and then purchase a fake domain and an EV SSL to secure that domain, is now a reality, which law enforcement agencies and governmental agencies such as the Federal Trade Commission should address.

Based on these findings, we believe CAs could do more to validate the authenticity of individuals and organizations purchasing EV certificates to ensure they retain their value. For example, a more thorough verification of the EV certificate purchaser's physical presence could be followed. Exhibits 27 and 28 present the street view from the addresses that appeared in the registration documents and the Dun and Bradstreet database for the U.K.-based retail and financial companies. Exhibit 29 presents the street view from the address that appeared in both the Delaware Division of Corporations registration documents and the Dun and Bradstreet database for the U.S.-based financial institution. Evaluating this data could improve the EV certificate validation process. Failure to adjust these processes calls into question the necessity of purchasing EV certificates and their value in delivering additional levels of trust. Future improvements should take an evidence-based cybersecurity approach and include consistent tests that evaluate potential problems and weaknesses in the validation process.

Exhibit 27. Street View from the U.K. Retail Company's Address Submitted to Authorities by Vendor and Appeared on Certificate of Registration Document from Google Maps



Exhibit 28. Street View from U.K.-Based Financial Institution's Address Submitted to Authorities by Vendor and Appeared on Certificate of Registration Document from Google Maps



Exhibit 29. Actual Site on U.S.-Based Financial Institution's Address, Which Was Submitted to Authorities by Vendor from Google Maps



An evidence-based cybersecurity approach provides an ideal framework for conceptualizing an interdisciplinary problem like online crime because it stresses moving beyond decision makers' political, financial and social backgrounds as well as personal experiences to a model in which policy decisions are made based on scientific research findings. Moreover, this approach draws on the assumption that solutions to human behaviors may be affected by the interconnected behavior of victims, offenders and law enforcement agencies operating within

the cyber realm, and that the effectiveness of the different interventions in achieving its goals should be assessed through rigorous scientific research methods. Seeking to collect and produce evidence from each of the key junctures formed through the online interaction between the different actors that operate on the cybercrime ecosystem and drive CA online fraud victimization will result in a more effective validation process. In turn, this will allow effective prevention and mitigation of cybercrime incidents.

REFERENCES

1. Burton, J. (2017). First part of Phishing with EV. Available at: <https://www.typewritten.net/writer/ev-phishing/>
2. Kim, D., Kwon, B. J., & Dumitraş, T. (2017, October). Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1435-1448). ACM.
3. Kozák, K., Kwon, B. J., Kim, D., Gates, C., & Dumitraş, T. (2018). Issued for Abuse: Measuring the Underground Trade in Code Signing Certificate. arXiv preprint arXiv:1803.02931.
4. Maimon, D., Wu, Y., McGuire, M., Stubler, N., & Qiu, Z. 2019. SSL/TLS Certificates and Their Prevalence on the Dark Web (First Report). Available at: <https://www.venafi.com/sites/default/files/2019-02/Dark-Web-WP.pdf>
5. Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: an interdisciplinary review. *Annual Review of Criminology*, 2, 191-216.
6. Members of the CA/Browser Forum. (2007 – 2019). Guidelines For The Issuance And Management Of Extended Validation Certificates, v1.6.9. Available at: <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.6.9.pdf>
7. Yip, M., Shadbolt, N., & Webber, C. (2013). Why forums?: An empirical analysis into the facilitating factors of carding forums. Proceedings of the 5th Annual ACM Web Science Conference 453-462.