SSL/TLS Certificates and Their Prevalence on the Dark Web (First Report)

David Maimon
Yubao Wu
Michael McGuire
Nicholas Stubler
Zijie Qiu

Georgia State University | Andrew Young School of Policy Studies

Executive Summary

As organizations focus on the digital transformation of their businesses, the importance of encryption as the cornerstone of security and privacy is increasingly vital. In 2018, over 70 percent of internet traffic was encrypted. Experts believe that this figure is expected to rise to 80 percent in 2019 (Google, 2019). Secure Sockets Layer (SSL, an older standard) and Transport Layer Security (TLS, a newer standard) certificates are essential to encryption because they authorize all encrypted communication between machines. SSL/TLS certificates are instrumental in protecting privacy and improving security, providing each machine with a unique machine identity. They control the flow of sensitive data to authorized machines and are used in everything from website transactions and mobile devices to smart city initiatives, robots, artificial intelligence algorithms and containers in the cloud.

Despite the pivotal role encryption plays in our digital economy and across the internet, the processes needed to protect digital certificates are not well understood or widely followed. As a result, SSL/TLS certificates are often poorly protected, making them attractive targets for attackers. In fact, illegitimate access to SSL/TLS certificates has played a key role in several high-profile, high-impact breaches—such as Snowden, Sony and Equifax.

To shine a light on the availability of SSL/TLS certificates on the dark web, the Evidence-based Cybersecurity Research Group at the Andrew Young School of Policy Studies at Georgia State University and the University of Surrey spearheaded a research program, sponsored by Venafi. This report details the preliminary findings of the research and outlines the volume of SSL/TLS certificates for sale on the dark web, including information on how they are packaged and sold to attackers. These certificates can be used to eavesdrop on sensitive communications, spoof websites, trick consumers and steal data. The long-term goal of this research is to gain a more thorough understanding of the role SSL/TLS certificates play in the economy of the dark web as well as how they are being used by attackers.

This is the first of three reports—the first of their kind—focused on the underground SSL/TLS marketplace and its role in the wider cybercrime economy. This report will show that there is a machine identity-as-a-service marketplace on the dark web, where fraudulent TLS certificates are readily available for purchase.

Key findings:

- Five of the Tor network markets observed—Dream Market, Wall Street Market, BlockBooth, Nightmare Market and Galaxy3—offer a steady supply of SSL/TLS certificates, along with a range of related services and products.
- One representative search of these five marketplaces uncovered 2,943 mentions for "SSL" and 75 for "TLS." In comparison, there were only 531 mentions for "ransomware" and just 161 for "zero day" exploits.
- SSL/TLS certificates are often packaged with crimeware services and products, such as malicious websites and ransomware.
- Certain marketplaces, like Dream Market, appear to specialize in the sale of SSL/TLS certificates and related services.
- Some underground marketplaces focus on packaging services with SSL/TLS certificates. For example, some sellers offer "aged" domains, after-sale support and integration with a range of legitimate payment processors—including Stripe, PayPal and Square.
- At least one vendor on BlockBooth promises to issue certificates from reputable certificate authorities. 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.
- Prices for certificates vary from $260 to $1,600, depending on the type of certificate and scope of additional services offered.

The Hypertext Transfer Protocol and TLS Certificates

The internet is made up of a large number of globally connected computer networks (Tanenbaum and Wetherall 2011). To allow easy communication among these computer networks and to support the transmission of data between clients and servers, common communication protocols have been developed. Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web to support users' access to the internet. HTTP 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. For example, when you type `google.com` in your browser, your computer sends an HTTP command to the Google web server and directs it to fetch and transmit the requested webpage. Hypertext Transfer Protocol Secure (HTTPS) is the secure version of HTTP. This protocol encrypts the communication 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) with a SSL/TLS certificate issued by a certificate authority. 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 certificate authorities. Certificate authorities are charged with the task of employing stringent validation processes to ensure SSL/TLS certificates are issued only to legitimate companies, organizations and individuals. An extended validation (EV) SSL/TLS certificate is designed to be the most trusted certificate on the market. EV certificates create verified identities and are only issued after the certificate authority verifies the identity of the requester using robust specifications laid out by the CA/Browser forum and Microsoft. These guidelines require that the requester provide several pieces of identifying information, including the company's DUNS 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 certificate authority 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. EV certificates should be issued only after these steps are successfully completed. Importantly, other types of SSL/TLS certificates—uch as organization validated (OV) and domain validated (DV)—are also used to authorize encrypted communication. However, the verification information required by certificate authorities for these types of SSL/ TLS certificates varies, and once they are in use by the requester, the security feedback to users about the validity of their certificates from browsers may also vary.

The keys and certificates issued by certificate authorities are used during the beginning of each encrypted communication to authenticate the identity of the machines. However, if these certificates are fraudulent, compromised, forged or tampered with, they can be powerful tools for attackers.

Specifically, if a trusted certificate authority is breached and private keys are stolen from it, the stolen certificates could be sold in the online underground market on the dark web to malicious parties. In turn, they could use them to move silently between trusted machines, "listen" to encrypted traffic, and escalate privileges to access sensitive data (Gu and Gu 2015). Moreover, if the verification processes used by trusted certificate authorities to verify the identity of the requesting party can be circumvented or spoofed, malicious actors can be issued a SSL/TLS certificate that delivers the highest levels of trust (i.e., an EV certificate). This allows attackers to create "trustworthy" spoofed or malicious websites and encrypt the traffic between malicious servers to targeted users, making it more difficult to identify problematic behavior.

Are SSL/TLS Certificates for Sale on the Dark Web?

Malicious actors can get information on either stolen machine identities or code-signing certificates and can even establish "legitimate" identities for the spoofed websites they build in an effort to victimize their targets (Kim et al. 2017; Kozak et al. 2018) through the illegal online markets that populate the dark web. Online environments that support the convergences of cybercriminals, enablers, targets and guardians exist on both the surface web (which contains all the websites and computers that are accessible to anyone with an internet connection) and on the deep web (which is up to 500 times larger than the surface web and consists of websites that are not searchable, including innocuous sites like business intranets and medical databases; Kremling & Parker 2017). The dark web (also known as the "darknet") forms a subset of the deep web. Due to the extended anonymity that it allows, the dark web provides an attractive online platform for the development of networks and allegiances between criminals and enablers, as well as for the initiation and development of illegal activities (Maimon and Louderback 2019). A dark web market is a commercial website that operates via anonymous networks, such as The Onion Router (Tor) or the Invisible Internet Project (I2P).

Online forums and market users who employ public communication platforms over the dark web often create unique public threads that aim to ask a question or advertise a service or a product (Hutchings and Clayton 2016). The posting entity gives a description of the service or product (either needed or provided) and includes details on pricing information, payment and contact information (Holt and Lampke 2010). These markets offer the hardware, software and materials needed to initiate all types of cyber-dependent crimes (i.e., illegal activities that can only be performed using a computer, computer networks or other forms of information communication technology (McGuire and Dowling 2013)), as well as the sensitive data harvested from victims of cyber-dependent crimes—like Social Security numbers, credit card numbers, names and addresses (Yip et al. 2013).

The premise for this research project is that among the wide range of illegal commodities that are offered for sale on these online markets and forums, it may be possible to find evidence for the sale and purchase of compromised, fraudulent and forged TLS certificates. Specifically, Kim and colleagues (2017) have recently alerted to the presence of a code-signing certificate (i.e., certificates that guarantee the authenticity of a software publisher and integrity of the software) market over the darknet. Kozak and associates (2018) have further documented the operation of four dark web vendors that issue code-signing certificates for the purpose of abuse. However, we are not aware of any previous research that provides evidence for the existence of a market for compromised, stolen and forged SSL/TLS certificates in the dark web. Therefore, our research objective was to seek evidence of their existence in underground markets and assess the prevalence of SSL/TLS certificates as a commodity in the dark web.

Research Design and Methodology

To accomplish our research objective, we dived into online markets and hacker forums that were active on the Tor network, I2P and the Freenet during the data collection period from October 2018–January 2019 and searched for "for sale" listings of stolen, fake and forged TLS certificates. Our research team discovered close to 60 relevant online market webpages on the Tor network, 17 webpages on I2P, and no relevant webpages on the Freenet (see Appendices A and B for the list of dark web markets we monitored). 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. We performed 16 weekly searches across all 60 websites during the project period.

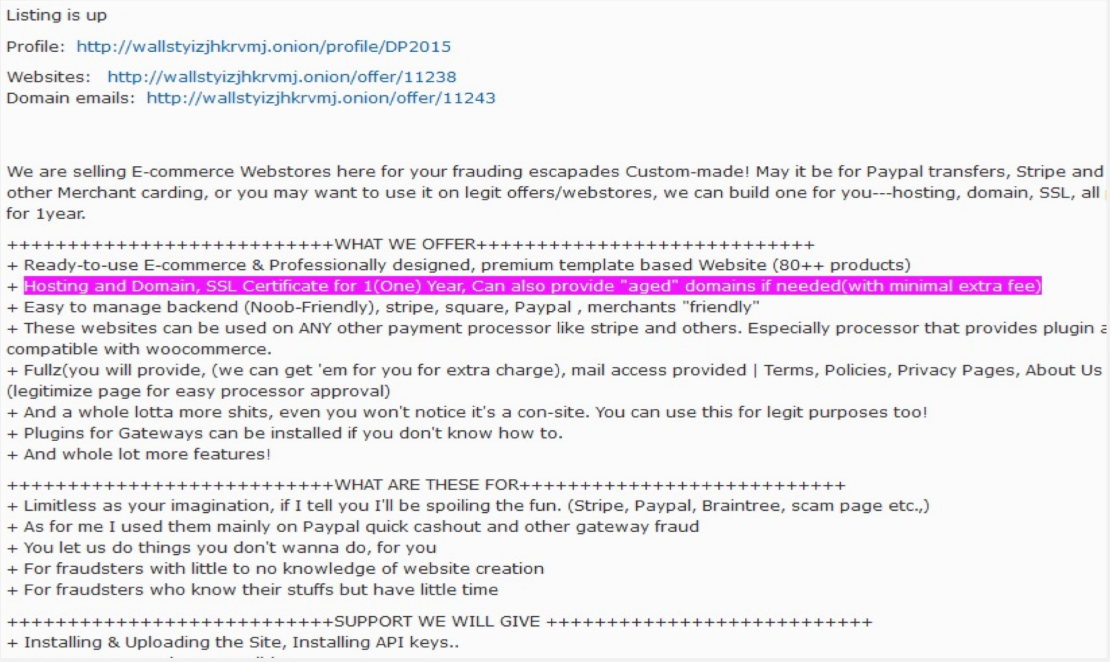
Results

We observed evidence for the relevance of SSL/TLS certificates in the cybercrime ecosystem in five of the Tor network markets we observed: Dream Market, Wall Street Market, BlockBooth, Nightmare Market and Galaxy3. Table 1 presents a typical summary from one of our weekly searches on the number of mentions of SSL and TLS certificate listings. Note that the number of mentions we observed did not vary significantly throughout the duration of the project. For comparison purposes, in this table, we juxtapose the number of SSL/TLS certificates mentions with the number of mentions for two other popular products on these markets: ransomware and zero-day exploits. As may be observed in the table, there is a considerable variation with respect to the number of mentions of SSL/TLS certificates across the markets observed. While the number of mentions of SSL/TLS certificates is high on the Dream Market, it is lower on the Wall Street Market and Galaxy3, and it's even lower on BlockBooth and the Nightmare Market. Interestingly, the number of mentions of SSL certificates is significantly higher than the number of mentions for both ransomware and zero-day exploits in three out of the five markets.

Table 1. Mentions Count for Search Perfomed on December 3rd

Web Name	SSL Certificates	TLS Certificates	Ransomware	Zero-Day Exploits
Dream Market	2912	64	512	160
Wall Street Market	10	4	13	1
BlockBooth	3	1	0	0
Nightmare Market	2	0	5	0
Galaxy3	16	7	1	0

Figure 1 presents a screenshot of a typical ad in which SSL certificates were mentioned in the Wall Street Market. Note that some of the commodities offered for sale on this market are malware, security vulnerabilities and exploits, as well as stolen accounts and credit card credentials. The vendor in this ad provides the design of "trustworthy" e-commerce stores aimed to support the operation of online fraudulent activity. SSL certificates are mentioned second in the list of services offered by this vendor, along with "aged domains" (i.e., websites that have been registered and active for a long period of time, which makes the site appear to be more legitimate. SSL/TLS certificates and aged domains are used to convey trust to website visitors and search engines.



Listing is up

Profile: http://wallstyizjhkrvmj.onion/profile/DP2015

Websites: http://wallstyizjhkrvmj.onion/offer/11238
Domain emails: http://wallstyizjhkrvmj.onion/offer/11243

We are selling E-commerce Webstores here for your frauding escapades Custom-made! May it be for Paypal transfers, Stripe and other Merchant carding, or you may want to use it on legit offers/webstores, we can build one for you---hosting, domain, SSL, all for 1year.

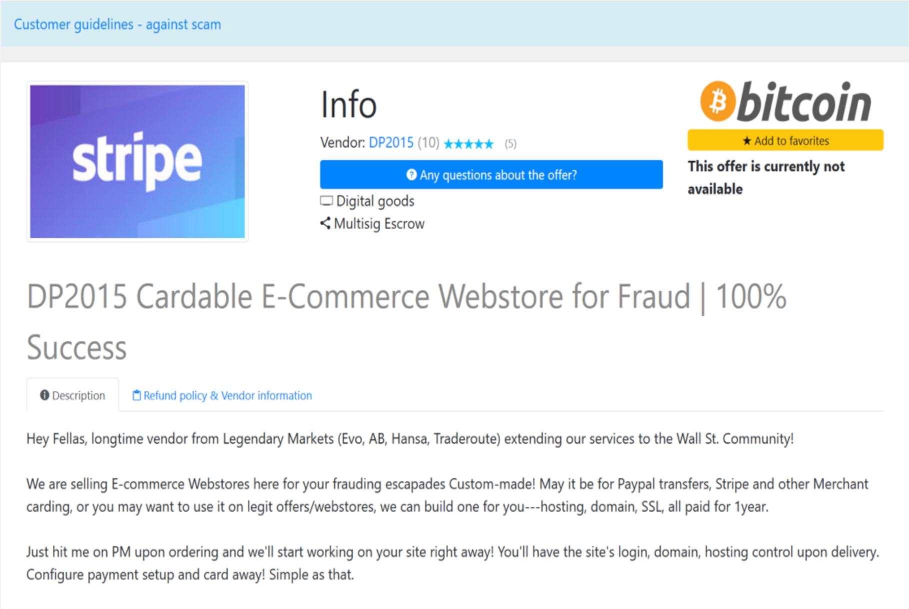
```
++++++++++++++++++++++++++++WHAT WE OFFER+++++++++++++++++++++++++++++
+ Ready-to-use E-commerce & Professionally designed, premium template based Website (80++ products)
+ Hosting and Domain, SSL Certificate for 1(One) Year, Can also provide "aged" domains if needed(with minimal extra fee)
+ Easy to manage backend (Noob-Friendly), stripe, square, Paypal , merchants "friendly"
+ These websites can be used on ANY other payment processor like stripe and others. Especially processor that provides plugin a
compatible with woocommerce.
+ Fullz(you will provide, (we can get 'em for you for extra charge), mail access provided | Terms, Policies, Privacy Pages, About Us
(legitimize page for easy processor approval)
+ And a whole lotta more shits, even you won't notice it's a con-site. You can use this for legit purposes too!
+ Plugins for Gateways can be installed if you don't know how to.
+ And whole lot more features!

++++++++++++++++++++++++++++WHAT ARE THESE FOR++++++++++++++++++++++++++++
+ Limitless as your imagination, if I tell you I'll be spoiling the fun. (Stripe, Paypal, Braintree, scam page etc.,)
+ As for me I used them mainly on Paypal quick cashout and other gateway fraud
+ You let us do things you don't wanna do, for you
+ For fraudsters with little to no knowledge of website creation
+ For fraudsters who know their stuffs but have little time

++++++++++++++++++++++++++++SUPPORT WE WILL GIVE ++++++++++++++++++++++++++++
+ Installing & Uploading the Site, Installing API keys..
```

Figure 1. SSL Certificates Sold along with Website Design Services (Wall Street Market)

A visit to this vendor's website reveals important details about the operation. Figure 2, for example, discloses more details about the vendor, along with an explicit statement regarding the proposed website's goal (i.e., online fraud). Figure 3 presents a more detailed list of services than those presented in Figure 1, as well as a list of services that will not be provided by the vendor under this umbrella. Finally, Figure 4 shows the asking price for the vendor's service ($170), the number of products already sold (10) and customer ratings (which seems to be very high).



Customer guidelines - against scam
stripe
bitcoin
★ Add to favorites
Any questions about the offer?
Description
Refund policy & Vendor information

Info

Vendor: DP2015 (10) ★★★★★ (5)

Digital goods

Multisig Escrow

This offer is currently not available

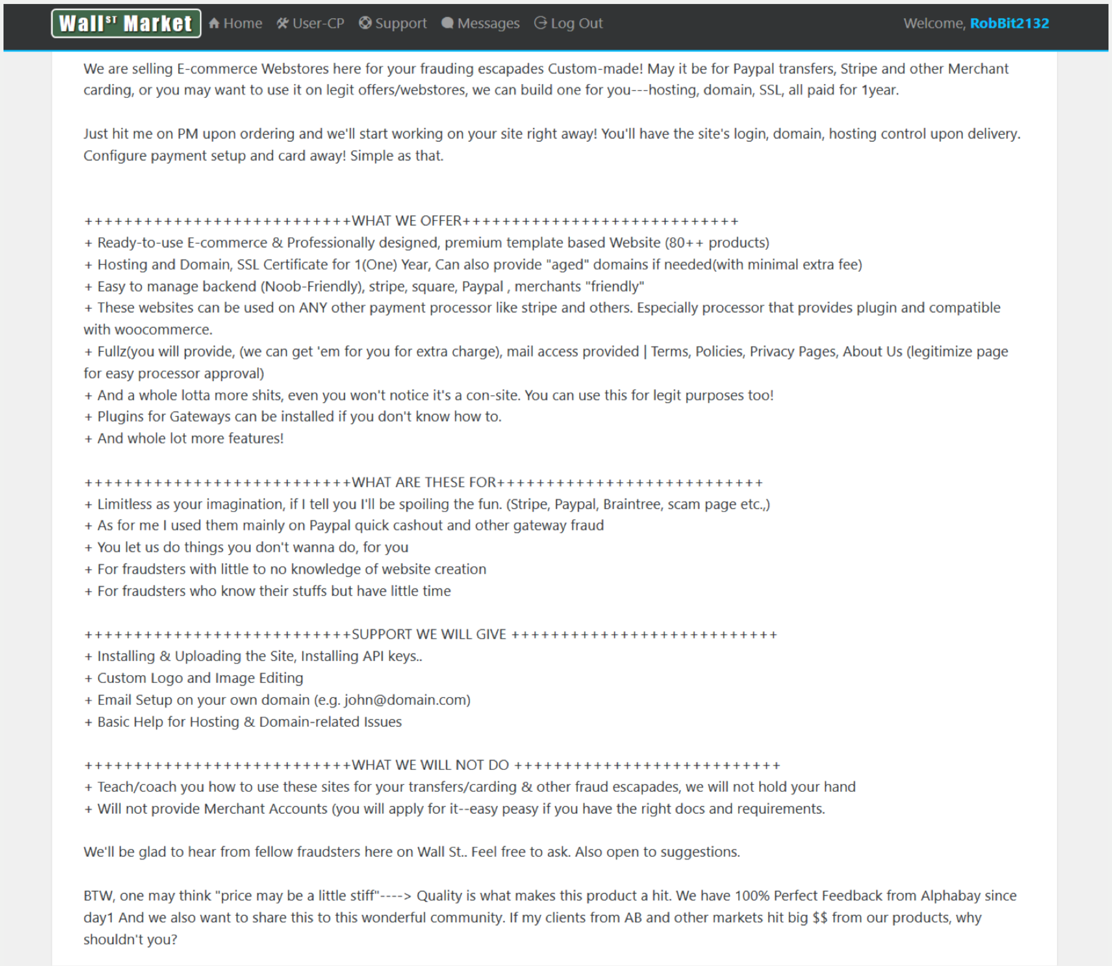
DP2015 Cardable E-Commerce Webstore for Fraud | 100% Success

Hey Fellas, longtime vendor from Legendary Markets (Evo, AB, Hansa, Traderoute) extending our services to the Wall St. Community!

We are selling E-commerce Webstores here for your frauding escapades Custom-made! May it be for Paypal transfers, Stripe and other Merchant carding, or you may want to use it on legit offers/webstores, we can build one for you---hosting, domain, SSL, all paid for 1year.

Just hit me on PM upon ordering and we'll start working on your site right away! You'll have the site's login, domain, hosting control upon delivery. Configure payment setup and card away! Simple as that.

Figure 2. SSL Certificates Sold to Create Fraudulent Website for E-Commerce



We are selling E-commerce Webstores here for your frauding escapades Custom-made! May it be for Paypal transfers, Stripe and other Merchant carding, or you may want to use it on legit offers/webstores, we can build one for you---hosting, domain, SSL, all paid for 1year.

Just hit me on PM upon ordering and we'll start working on your site right away! You'll have the site's login, domain, hosting control upon delivery. Configure payment setup and card away! Simple as that.

+++++++++++++++++++++++++WHAT WE OFFER++++++++++++++++++++++++++
+ Ready-to-use E-commerce & Professionally designed, premium template based Website (80++ products)
+ Hosting and Domain, SSL Certificate for 1(One) Year, Can also provide "aged" domains if needed(with minimal extra fee)
+ Easy to manage backend (Noob-Friendly), stripe, square, Paypal , merchants "friendly"
+ These websites can be used on ANY other payment processor like stripe and others. Especially processor that provides plugin and compatible with woocommerce.
+ Fullz(you will provide, (we can get 'em for you for extra charge), mail access provided | Terms, Policies, Privacy Pages, About Us (legitimize page for easy processor approval)
+ And a whole lotta more shits, even you won't notice it's a con-site. You can use this for legit purposes too!
+ Plugins for Gateways can be installed if you don't know how to.
+ And whole lot more features!

+++++++++++++++++++++++++WHAT ARE THESE FOR+++++++++++++++++++++++++
+ Limitless as your imagination, if I tell you I'll be spoiling the fun. (Stripe, Paypal, Braintree, scam page etc.,)
+ As for me I used them mainly on Paypal quick cashout and other gateway fraud
+ You let us do things you don't wanna do, for you
+ For fraudsters with little to no knowledge of website creation
+ For fraudsters who know their stuffs but have little time

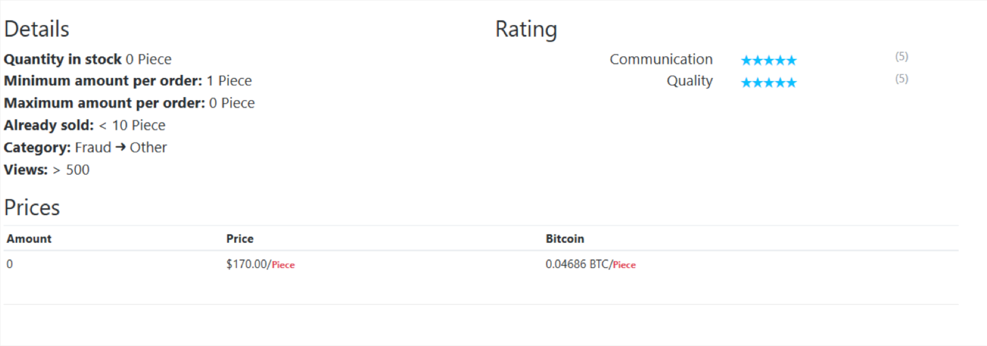
+++++++++++++++++++++++++SUPPORT WE WILL GIVE +++++++++++++++++++++++++
+ Installing & Uploading the Site, Installing API keys..
+ Custom Logo and Image Editing
+ Email Setup on your own domain (e.g. john@domain.com)
+ Basic Help for Hosting & Domain-related Issues

+++++++++++++++++++++++++WHAT WE WILL NOT DO +++++++++++++++++++++++++
+ Teach/coach you how to use these sites for your transfers/carding & other fraud escapades, we will not hold your hand
+ Will not provide Merchant Accounts (you will apply for it--easy peasy if you have the right docs and requirements.

We'll be glad to hear from fellow fraudsters here on Wall St.. Feel free to ask. Also open to suggestions.

BTW, one may think "price may be a little stiff"----> Quality is what makes this product a hit. We have 100% Perfect Feedback from Alphabay since day1 And we also want to share this to this wonderful community. If my clients from AB and other markets hit big $$ from our products, why shouldn't you?

Figure 3. SSL Certificates and Services to Create Fraudulent Websites (Wall St. Market)



Details

Quantity in stock 0 Piece
Minimum amount per order: 1 Piece
Maximum amount per order: 0 Piece
Already sold: < 10 Piece
Category: Fraud ➔ Other
Views: > 500

Rating

Communication	★★★★★	(5)
Quality	★★★★★	(5)

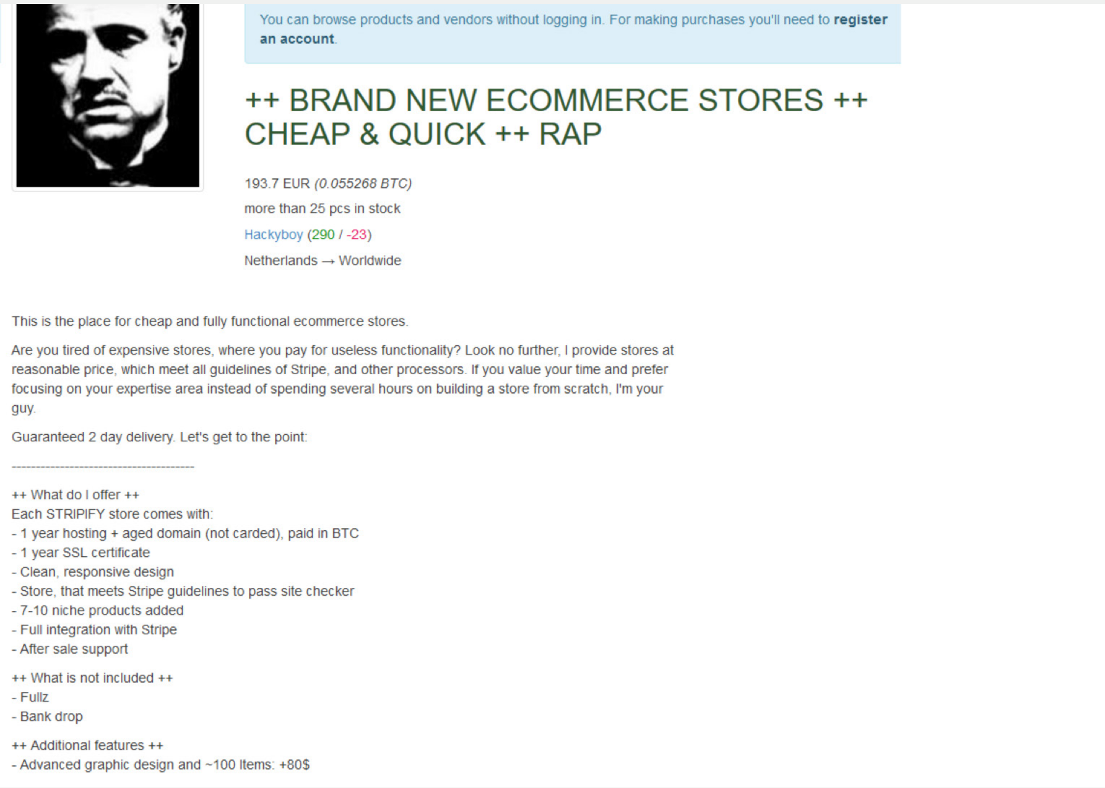
Prices

Amount	Price	Bitcoin
0	$170.00/Piece	0.04686 BTC/Piece

Figure 4. Price, Previous Sales and Customer Ratings of Fraudulent Websites with SSL/TLS Certificates

Similarly, Figure 5 presents evidence for another vendor on the Dream Market. This vendor's ad, and many others like it, mentions the issuance of SSL certificates and the use of aged domains as key services provided by this vendor.

Two insights are worth mentioning. First, this vendor's presentation of the service provided is subtle and implied (unlike the language used in the previous ad). And second, the price for this service is less than €200.



You can browse products and vendors without logging in. For making purchases you'll need to **register an account**.

++ BRAND NEW ECOMMERCE STORES ++ CHEAP & QUICK ++ RAP

193.7 EUR *(0.055268 BTC)*
more than 25 pcs in stock
Hackyboy (290 / -23)
Netherlands → Worldwide

This is the place for cheap and fully functional ecommerce stores.

Are you tired of expensive stores, where you pay for useless functionality? Look no further, I provide stores at reasonable price, which meet all guidelines of Stripe, and other processors. If you value your time and prefer focusing on your expertise area instead of spending several hours on building a store from scratch, I'm your guy.

Guaranteed 2 day delivery. Let's get to the point:

++ What do I offer ++
Each STRIPIFY store comes with:
- 1 year hosting + aged domain (not carded), paid in BTC
- 1 year SSL certificate
- Clean, responsive design
- Store, that meets Stripe guidelines to pass site checker
- 7-10 niche products added
- Full integration with Stripe
- After sale support

++ What is not included ++
- Fullz
- Bank drop

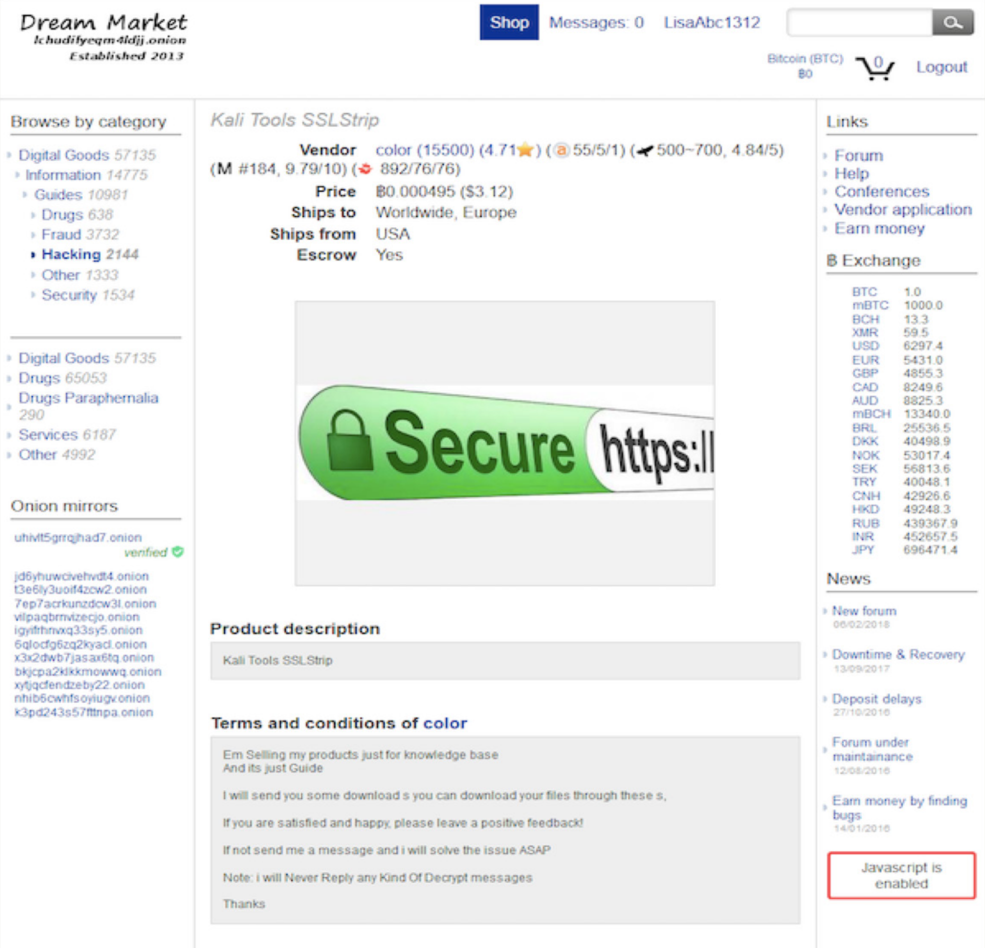
++ Additional features ++
- Advanced graphic design and ~100 Items: +80$

Figure 5. SSL Certificates Sold With Website Design Services (Dream Market)

SSL/TLS certificates were also mentioned in various tutorials produced by anonymous authors. In addition, we found evidence of the availability of SSL stripping tools in the Dream Market. SSL stripping is a specific type of man-in-the-middle attack in which an attacker can prevent a web browser from upgrading to an SSL connection to HTTP or HTTPs. These attackers typically go unnoticed by users.

SSL strip tools allow attackers to strip away the encryption offered by HTTPS links, and they also make it possible to redirect and map those links to homograph-similar HTTPS links.

Figure 6 presents a For Sale ad of a Kali SSL Strip tool for less than $5.



Browse by category

- Digital Goods 57135
  - Information 14775
    - Guides 10981
      - Drugs 638
      - Fraud 3732
      - **Hacking** 2144
      - Other 1333
      - Security 1534

- Digital Goods 57135
- Drugs 65053
- Drugs Paraphernalia 290
- Services 6187
- Other 4992

Onion mirrors

uhivlt5grrqjhad7.onion
verified

jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

Kali Tools SSLStrip

Vendor color (15500) (4.71⭐) (ⓐ 55/5/1) (✈ 500~700, 4.84/5) (M #184, 9.79/10) (892/76/76)
Price Ƀ0.000495 ($3.12)
Ships to Worldwide, Europe
Ships from USA
Escrow Yes

Product description

Kali Tools SSLStrip

Terms and conditions of color

Em Selling my products just for knowledge base
And its just Guide

I will send you some download s you can download your files through these s,

If you are satisfied and happy, please leave a positive feedback!

If not send me a message and i will solve the issue ASAP

Note: i will Never Reply any Kind Of Decrypt messages

Thanks

Links

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

Ƀ Exchange

BTC	1.0
mBTC	1000.0
BCH	13.3
XMR	59.5
USD	6297.4
EUR	5431.0
GBP	4855.3
CAD	8249.6
AUD	8825.3
mBCH	13340.0
BRL	25536.5
DKK	40498.9
NOK	53017.4
SEK	56813.6
TRY	40048.1
CNH	42926.6
HKD	49248.3
RUB	439367.9
INR	452657.5
JPY	696471.4

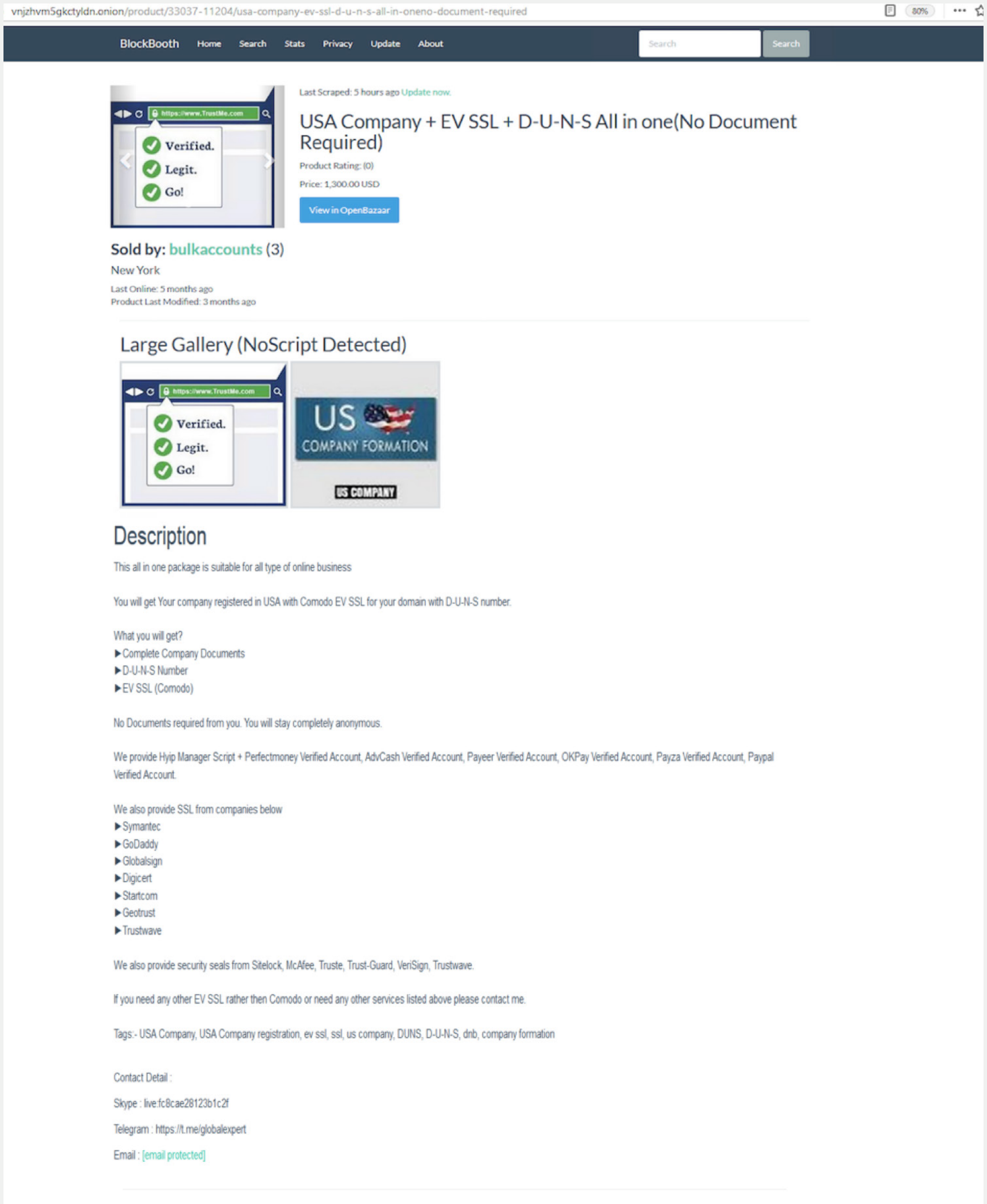
News

- New forum
  06/02/2018
- Downtime & Recovery
  13/09/2017
- Deposit delays
  27/10/2016
- Forum under maintainance
  12/08/2016
- Earn money by finding bugs
  14/01/2016

Javascript is enabled

Figure 6. Kali SSL Strip Tool (Dream Market)

Although SSL certificate mentions in both Dream Market and Wall Street Market are primarily packaged as either website design services or for stripping encryption of HTTPS links, the mentions on BlockBooth typically offer a standalone service that provides EV certificate issuance for interested parties. In Figure 7, we present a screenshot of an ad posted by the vendor 'bulkaccounts' that advertises the vendor's ability to issue EV certificates for U.S. companies without asking potential clients for any verifying information. The cost for each certificate starts at $1,300. In the description section of the ad, more details are provided about the types of services offered. One notable finding from this section is the vendor's promise to supply EV certificates from reputable and trusted certificate authorities. Additionally, the vendor promises to provide full documentation for forged companies, including D-U-N-S numbers.



Last Scraped: 5 hours ago Update now.

USA Company + EV SSL + D-U-N-S All in one(No Document Required)

Product Rating: (0)

Price: 1,300.00 USD

Sold by: bulkaccounts (3)

New York

Last Online: 5 months ago
Product Last Modified: 3 months ago

Large Gallery (NoScript Detected)

Description

This all in one package is suitable for all type of online business

You will get Your company registered in USA with Comodo EV SSL for your domain with D-U-N-S number.

What you will get?
▶Complete Company Documents
▶D-U-N-S Number
▶EV SSL (Comodo)

No Documents required from you. You will stay completely anonymous.

We provide Hyip Manager Script + Perfectmoney Verified Account, AdvCash Verified Account, Payeer Verified Account, OKPay Verified Account, Payza Verified Account, Paypal Verified Account.

We also provide SSL from companies below
▶Symantec
▶GoDaddy
▶Globalsign
▶Digicert
▶Startcom
▶Geotrust
▶Trustwave

We also provide security seals from Sitelock, McAfee, Truste, Trust-Guard, VeriSign, Trustwave.

If you need any other EV SSL rather then Comodo or need any other services listed above please contact me.

Tags:- USA Company, USA Company registration, ev ssl, ssl, us company, DUNS, D-U-N-S, dnb, company formation

Contact Detail :

Skype : live:fc8cae28123b1c2f

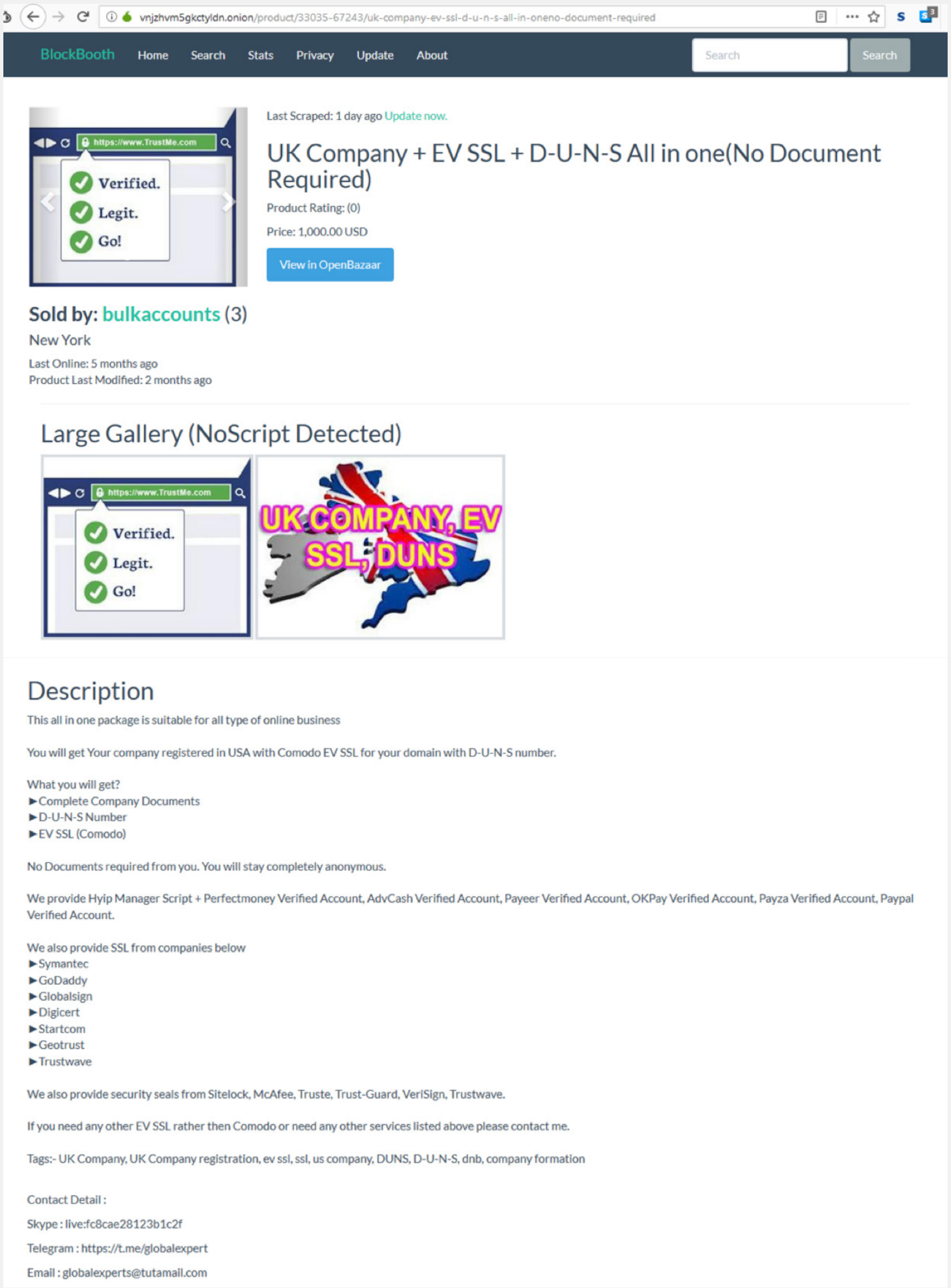
Telegram : https://t.me/globalexpert

Email : [email protected]

Figure 7. EV Certificates of US Companies—No Doc or Verification Required

Figure 8 presents a screenshot of an ad posted again by bulkaccounts. In it, the vendor advertises issuance of EV certificates for U.K. companies without asking potential clients for any verifying information. The advertised cost for each certificate starts at $1,000. However, after contact with the vendor, it seems that the true asking price for this product is closer to $1,600. After reading through the description section of the ad, we find similar details to those offered for the issuance of its EV certificates for U.S. companies: The vendor promises to supply EV certificates from reputable and trusted certificate authorities, along with documentation for the forged companies. Importantly, since registration of a U.K. company seems to be more complicated than that of a U.S. company, the vendor also offers company formation services.

Figure 8 presents a screenshot of the post advertising this service.



Last Scraped: 1 day ago Update now.

UK Company + EV SSL + D-U-N-S All in one(No Document Required)

Product Rating: (0)

Price: 1,000.00 USD

Sold by: bulkaccounts (3)

New York

Last Online: 5 months ago
Product Last Modified: 2 months ago

Large Gallery (NoScript Detected)

Description

This all in one package is suitable for all type of online business

You will get Your company registered in USA with Comodo EV SSL for your domain with D-U-N-S number.

What you will get?
►Complete Company Documents
►D-U-N-S Number
►EV SSL (Comodo)

No Documents required from you. You will stay completely anonymous.

We provide Hyip Manager Script + Perfectmoney Verified Account, AdvCash Verified Account, Payeer Verified Account, OKPay Verified Account, Payza Verified Account, Paypal Verified Account.

We also provide SSL from companies below
►Symantec
►GoDaddy
►Globalsign
►Digicert
►Startcom
►Geotrust
►Trustwave

We also provide security seals from Sitelock, McAfee, Truste, Trust-Guard, VeriSign, Trustwave.

If you need any other EV SSL rather then Comodo or need any other services listed above please contact me.

Tags:- UK Company, UK Company registration, ev ssl, ssl, us company, DUNS, D-U-N-S, dnb, company formation

Contact Detail :

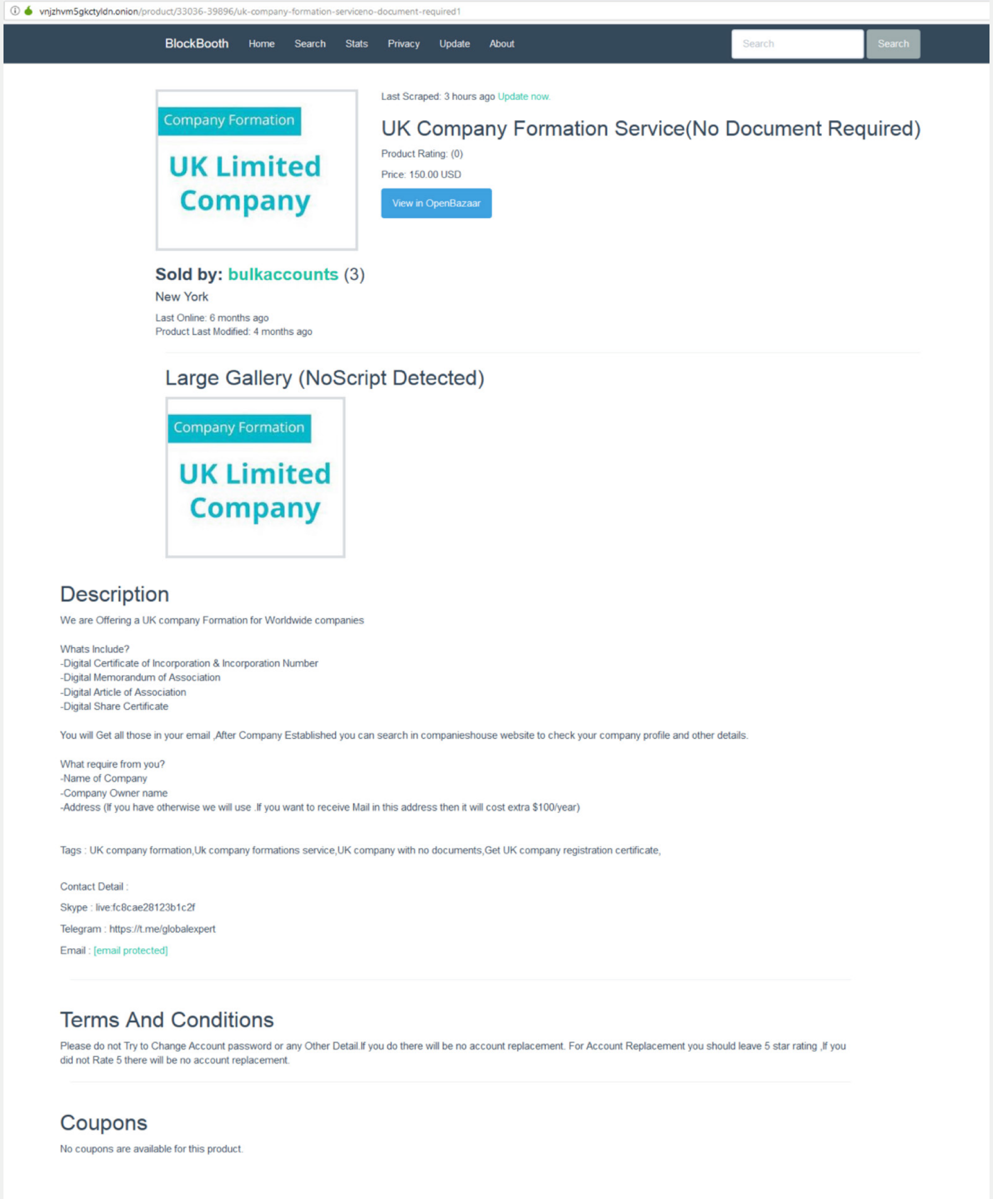
Skype : live:fc8cae28123b1c2f

Telegram : https://t.me/globalexpert

Email : globalexperts@tutamail.com

Figure 8. EV Certificates for U.K. companies—No Doc or Verification Required

As indicated in Figure 9, the vendor offers full support in establishing a company's identity in the U.K., in addition to all of the required legal documentation associated with this process. The client only needs to provide the company and owner names as well as some form of physical address. The charge for this service is $150. If buyers don't have a physical address, the vendor offers to provide one for an extra $100.



Last Scraped: 3 hours ago Update now.

UK Company Formation Service(No Document Required)

Product Rating: (0)

Price: 150.00 USD

Sold by: bulkaccounts (3)

New York

Last Online: 6 months ago
Product Last Modified: 4 months ago

Large Gallery (NoScript Detected)

Description

We are Offering a UK company Formation for Worldwide companies

Whats Include?
-Digital Certificate of Incorporation & Incorporation Number
-Digital Memorandum of Association
-Digital Article of Association
-Digital Share Certificate

You will Get all those in your email ,After Company Established you can search in companieshouse website to check your company profile and other details.

What require from you?
-Name of Company
-Company Owner name
-Address (If you have otherwise we will use .If you want to receive Mail in this address then it will cost extra $100/year)

Tags : UK company formation,Uk company formations service,UK company with no documents,Get UK company registration certificate,

Contact Detail :

Skype : live:fc8cae28123b1c2f

Telegram : https://t.me/globalexpert

Email : [email protected]

Terms And Conditions

Please do not Try to Change Account password or any Other Detail.If you do there will be no account replacement. For Account Replacement you should leave 5 star rating ,If you did not Rate 5 there will be no account replacement.

Coupons

No coupons are available for this product.

Figure 9. U.K. Company Formation Service

Discussion

SSL and TLS certificates issued by trusted certificate authorities are designed to serve as machine identities, ensuring confidential communication between servers and clients. Before issuing these certificates, and especially before issuing EV certificates, certificate authorities are obligated to employ a stringent set of validation data of the requesting party designed to verify their identity. Although prior research has suggested ways to detect fake SSL and TLS certificates (Gu and Gu 2015), as well as the way they can be used by adversaries to generate attacks (Birge-Lee et al. 2017), we are not familiar with any past research that provides evidence of fake and stolen certificate markets. This project provides evidence of the existence of an online underground market for TLS certificates, specifically the presence of vendors on online underground markets that are promising to issue EV certificates for U.S. and U.K. companies for less than $2,000. At this point, we are not sure how large this market is, whether the quality of goods offered matches vendor listings, or which parties are interested in purchasing these commodities. However, we plan to continue our research and keep investigating this issue.

References

1. Google. Transparency Report. HTTPS Encryption on the Web. (Data retrieved January 2019.)
2. Birge-Lee, H., Sun, Y., Edmundson, A., Rexford, J., & Mittal, P. (2017). Using BGP to acquire bogus TLS certificates. HotPETS'17.
3. Gu, X., & Gu, X. (2015). On the detection of fake certificates via attribute correlation. Entropy, 17(6), 3806-3837.
4. Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. Criminal Justice Studies 23:33-50.
5. Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. Taylor & Francis Online.
6. Hutchings, A., & Holt, T. J. (2015). A Crime Script Analysis of the Online Stolen Data Market. British J. of Criminology 55: 596-614.
7. 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.
8. 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.
9. Kremling, J., & Parker, A.M. (2017). Cyberspace, Cybersecurity, and Cybercrime. Thousand Oaks CA: SAGE Publications.
10. Maimon, D., & Louderback, E. R. (2018). Cyber-Dependent Crimes: An Interdisciplinary Review. Annual Review of Criminology, (0).
11. McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report: United Kingdom. Report 75: 1-34.
12. Tanenbaum, A. & Wetherall, D. (2011). Computer Networks 5th Edition.
13. 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.

Appendix A. Tor Network Markets Monitored

Dream Market
Wall Street
Empire Market
Silk Road 3.1
Rapture
Tochka/Point
Cannazon
CGMC
Berlusconi Market
AltBay
The Majestic Garden
Olympus
Midland City
Black Market
Cave Tor

Valhalla
Under Market
BlockBooth
Apollon
DutchDrugz's
Psychedelicum
Dutch Magic
CarlieUK Cocaine
Pushing Taboo
Cocaine Market
The French Connection
Glasswerkz Australia
AlphaBay
Zion
Drug Market

Green Road
EuCanna
The Peoples Drug Store
Smokeables
CannabisUK
Nightmare
Fresh Onion
0day forum
Hidden Wikis
Hacking forum
Free Hacks
The Hub
Dread
DNMAvengers
LINKS Onion

OnionDir
Amazon GC
Hidden Answers
Stack Wolfs
Imperial
Black White
Hacker Group
Rent-A-Hacker
Chinese Darknet Market
PlaceMarket
German-Plaza
Galaxy 3

Appendix B. I2P Network Markets Monitored

Legwork
Eepstatus
Exchanged
Lifebox
Black market
Visibility

Dumpteam
Hidden Answers
Chan
Anongw
Anonsfw
Difracker

Darknetnow
Dark realm
Dead
Hidden Answers
I2P forum