COINHOARDER: Tracking a Ukrainian Bitcoin Phishing Ring DNS Style

Artsiom Holub
Cisco Umbrella
San Francisco, USA
artholub@cisco.com

Jeremiah O'Connor
Cisco Security
San Francisco, USA
jeoconno@cisco.com

Abstract— **With the price of Bitcoin ascending to new heights in 2017, the rocketing valuation of cryptocurrencies continues its momentum into 2018. Evidence of the massive growth of these digital assets can be seen in the massive spikes in new clients at companies like Coinbase, adding 100,000 users in a 24-hour period, and Binance, which recently expanded its user base by 240,000 users in just one hour.**

The financial industry and Silicon Valley are not the only groups who have caught the cryptocurrency fever. Malicious actors have discovered that cryptocurrency newbies are unwitting targets that offer a consistent stream of revenue. Through our global network visibility, Cisco has observed many of these attacks originating from bulletproof hosting infrastructures located in the Eastern European region. This area is a hotbed for crypto theft and other computer crimes such as ransomware, botnets, DDoS services and credit card fraud. Some criminals have even extended beyond the digital world by kidnapping and demanding ransoms in Bitcoin, such as the case in the reported kidnapping and ransom of Pavel Lerner. Lerner was a lead analyst at Ukraine-based digital currency exchange, Exmo, who was released by his kidnappers after a $1 million Bitcoin payment was made. The event illustrates the desperate lengths some criminals will go in order to steal cryptocurrency.

Joining the Enterprise Ethereum Alliance in 2017, Cisco is committed to protecting these new crypto technologies. Over the past year Cisco researchers have teamed up with the Ukraine Cyber Police to track a Bitcoin phishing operation dubbed the "Coinhoarder" campaign that has been tied to the theft of tens of millions of dollars worth of Bitcoin.

Credential phishing continues to be one of the biggest security challenges for internet users, and cryptocurrency phishers have found it to be a very lucrative form of attack. In 2017, Chainalysis reported Ethereum phishing as being the number one source of theft in that ecosystem with estimates placing the total amount stolen at $115 million. Google also recently published a research paper stating credential phishing is one of their top security challenges. Cisco has been proactive in detecting phishing domains in predictive fashion to help protect our customers. Additionally, we have been working with security personnel at top cryptocurrency wallets and exchanges, such as Blockchain.info and Coinbase, to help protect the cryptocurrency community members from having their tokens stolen. Introduction

I. Introduction

A. Problem

With massive growth of the price and wide adoption of crypto based cyrrencies came attention of malicious actors who start seeing users of such currencies as targets. We observe this trend through global DNS and network visibility as attacks originated from Eastern European region against users of such services as: blockchain.info, mymonero.com, binance, coindesk, etc. Attacks were very succesfull due to the new evolved methods which included the use of SSL certs, abuse of legitimate services AdSense and BingAds, targetting of specific geographical regions.

B. Detection methods

The NLP and ML based detection: Phishing campaign actors know that most means of detection rely on observing newly registered and newly launch domains and matching, typosquatting domains are fairly easy to identify, report and take down. They also familiar with most filtering approaches based on domain age, ASN and popularity, so they are gradually evolving their approaches to combat this. Recently discovered campaign was using advertising platforms as Traffic Distribution Systems (TDSs) to selectively serve content to targeted regions, limiting exposure to certain geographical locations, hours of the day, same refusing to reveal malicious content repeatedly to the same IP, and even blacklisting certain IP ranges of known scanner engines and platform like Phishtank. Leveraging services like Cloudflare phishing actors are able to hide source IPs of original phishing domains as well as get SSL certificate, which looks trustworthy for average user. Our response to these tactics is a lightweight, scalable, and globally distributed NLP system. We focus our detection specifically on global DNS data captured by Cisco Umbrella resolvers.

C. Going beyond then just research

Exposing BPH: Just to detect phishing domain isn't enough, as it is just just one component of the phishing network. Average campaign can launch up to hundreds domains over short period of time. Most of the components are reliant on an architecture of inter-connected systems, which means when you find one domain, you can find many more by pivoting around additional data, in our case it is WHOIS data. We'll use our proprietary autopivoting algorithm, which takes

978-1-5386-4922-0/18/$31.00 ©2018 IEEE

domains found with our NLP and ML based system and uses them to find new phishing websites and underlying infrastructure based on passive DNS data gathered with Cisco Umbrella resolvers.

Convinced BPH: There are a lot of phishing campaigns run by the “skids” or low level criminals, while they are usually noisy, their success is limited to very unsophisticated users and have very low conversion rate. Sophisticated phishing authors running campaign for extended periods of time with thousands of users being affected. However, to have such long running setup they can’t rely on abused domains or use regular hostings which most likely will disable domain in a timely manner. Infrastructures which were exposed in our research have modern, flexible and elusive style where hosters diversify their footprints across various spaces and jurisdictions and act as dynamic business partners for criminals that want to host illegal contents online. Global DNS and pDNS data let us to track such campaigns at scale as they still tend to reuse same techniques and parts of infrastructures.

II. COINHOARDER CAMPAIGN

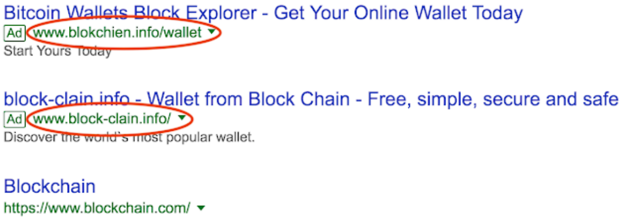
Discovery: Cisco has been tracking this bitcoin theft campaign for over 6 months using methods me mentioned in the introduction section. The campaign was discovered internally and researched with the aid of an intelligence sharing partnership with Ukraine Cyberpolice. The campaign was very simple and after initial setup the attackers needed only to continue purchasing Google AdWords to ensure a steady stream of victims. This campaign targeted specific geographic regions and allowed the attackers to amass millions in revenue through the theft of cryptocurrency from victims. This campaign demonstrates just how lucrative these sorts of malicious attacks can be for cybercriminals. And it takes copmlecated approach to battle such activity. Additionally, the revenue generated by these sorts of attacks, can then be reinvested into other cybercriminal operations.

On February 24, 2017, Cisco observed a massive phishing campaign hosted in Ukraine targeting the popular Bitcoin wallet site blockchain.info with a client request magnitude of over 200,000 client queries. This campaign was unique in that adversaries leveraged Google Adwords to poison user search results in order to steal users' wallets. Since Cisco observed this technique, it has become increasingly common in the wild with attackers targeting many different crypto wallets and exchanges via malicious ads.

Cisco identified an attack pattern in which the threat actors behind the operation would establish a "gateway" phishing link that would appear in search results among Google Ads.

When searching for crypto-related keywords such as "blockchain" or "bitcoin wallet," the spoofed links would appear at the top of search results. When clicked, the link would redirect to a "lander" page and serve phishing content in the native language of the geographic region of the victim's IP address.

978-1-5386-4922-0/18/$31.00 ©2018 IEEE



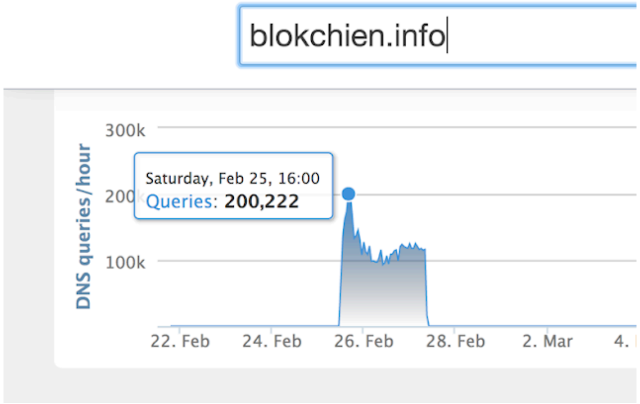
Bitcoin Wallets Block Explorer - Get Your Online Wallet Today
Ad www.blokchien.info/wallet
Start Yours Today

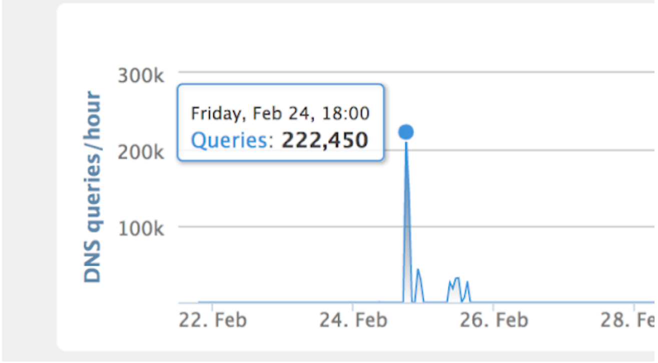
block-clain.info - Wallet from Block Chain - Free, simple, secure and safe
Ad www.block-clain.info/
Discover the world's most popular wallet.

Blockchain
https://www.blockchain.com/

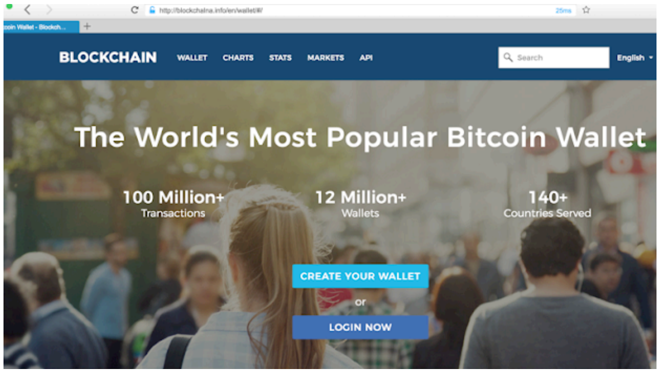
The reach of these poisoned ads can be seen when analyzing DNS query data. In February 2017, Cisco observed spikes in DNS queries for the fake cryptocurrency websites where upwards of 200,000 queries per hour can be seen during the time window the ad was displayed. Here are two examples.

The domain block-clain[.]info was used as the initial "gateway" victims would first visit. Victims would immediately be redirected to blockchalna[.]info, the landing page where the actual phishing content was hosted. These fraudulent sites are mostly hosted on bulletproof hosting providers based in Europe.



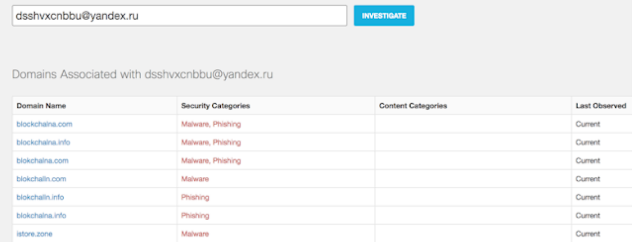


Here is what the actual lander phishing site looked like. Note how similar and convincing it is compared to a real site, with the exception of the URL:



Results of autopivoting algorithm: After discovering these domains and the activity on Google Adwords, Cisco implemented a system to flag similar domains as malicious. This resulted in DNS requests being blocked to said domains. Additionally, Cisco researchers were able to track and monitor related networks and info, such as WHOIS registrant data.

This information allowed Cisco to use DNS graph traversal techniques to uncover other phishing domains associated with the initial site. In this example, we can see the registrant dsshvxcnbbu@yandex[.]ru, which is also associated with many other phishing sites:

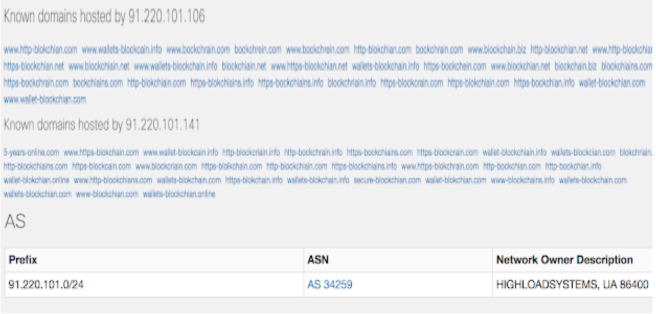


dsshvxcnbbu@yandex.ru INVESTIGATE

Domains Associated with dsshvxcnbbu@yandex.ru

Domain Name	Security Categories	Content Categories	Last Observed
blockchalna.com	Malware, Phishing		Current
blockchalna.info	Malware, Phishing		Current
blokchalna.com	Malware, Phishing		Current
blokchalln.com	Malware		Current
blokchalln.info	Phishing		Current
blokchalna.info	Phishing		Current
istore.zone	Malware		Current

Cisco also monitored the networks these domains are hosted on. Here is a snapshot of 2 of the recently active IP addresses for this campaign, 91.220.101.106 and 91.220.101.141, and the ASN associated with these domains, Highload Systems, in Ukraine.



Known domains hosted by 91.220.101.106

www.http-blokchian.com www.wallets-blockcain.info www.bockchrain.com bockchrein.com www.bockchrein.com http-blokchian.com bockchrain.com www.blockchain.biz http-blockchian.net www.http-blockchia https-blockchian.net www.blockchain.net www.wallets-blockchain.info blockchiain.net www.https-blockchian.net wallets-blockchain.info https-bockchein.com www.blockchian.net blockchain.biz blockchains.com https-bockchrain.com bockchlains.com http-blokchlain.com https-blokchlains.info https-bockchlains.info blockchrlain.info https-blockcrain.com https-blokchlain.com https-bockchian.info wallet-blockchian.com www.wallet-blockchian.com

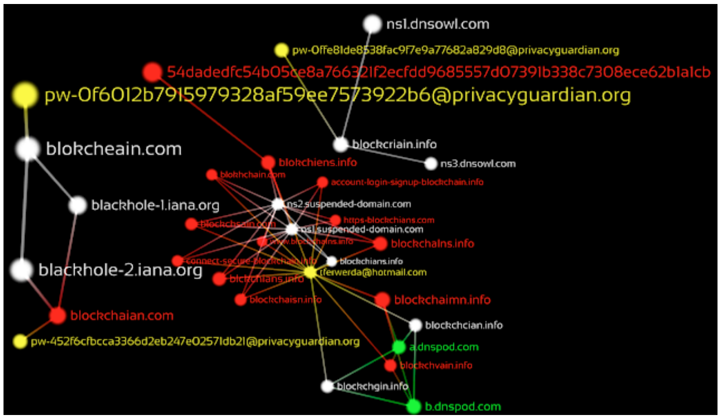
Known domains hosted by 91.220.101.141

5-years-online.com www.https-blokchain.com www.wallet-blockcain.info http-blockcrian.info http-bockchrain.info https-bockchlains.com https-blockcrain.com wallet-blockchiain.info wallets-blockcian.com blokchrlain. http-blockchlains.com https-blockcain.com www.blockcrian.com https-blokchain.com http-blockchiain.com https-blockchlains.info www.https-blokchrain.com http-bockchian.com http-bockchian.info wallet-blokchian.online www.http-blockchians.com wallets-blokchain.com https-blokchain.info wallets-blokchain.info secure-blockchian.com wallet-blokchian.com www-blockchains.info wallets-blockchain.com wallets-blockchian.com www-blockchian.com wallets-blockchian.online

AS

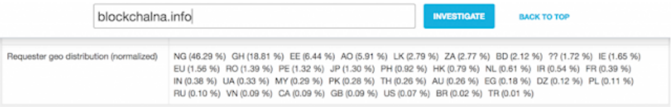
Prefix	ASN	Network Owner Description
91.220.101.0/24	AS 34259	HIGHLOADSYSTEMS, UA 86400

We can see the Second Level Domain (SLD) strings in these domains follow a similar pattern of targeting blockchain.info with many permutations of the string "blockchain", along with co-occurrences of "http", "https", "wallet" in the SLD string. Here is a graph visualization of the domains on these infrastructures:



978-1-5386-4922-0/18/$31.00 ©2018 IEEE

Geographic targeting: One of the most interesting facets to these attacks are the geographic regions of the victims. Using data from Umbrella Client Requester Distribution queries to these malicious domains, we can see a significant number of DNS resolution requests coming from countries such as Nigeria, Ghana, Estonia and many more.

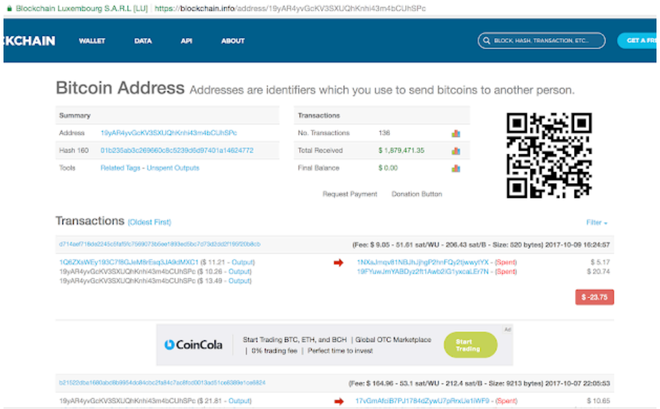


blockchalna.info INVESTIGATE BACK TO TOP

Requester geo distribution (normalized)	NG (46.29 %) GH (18.81 %) EE (6.44 %) AO (5.91 %) LK (2.79 %) ZA (2.77 %) BD (2.12 %) ?? (1.72 %) IE (1.65 %) EU (1.56 %) RO (1.39 %) PE (1.32 %) JP (1.30 %) PH (0.92 %) HK (0.79 %) NL (0.61 %) IR (0.54 %) FR (0.39 %) IN (0.38 %) UA (0.33 %) MY (0.29 %) PK (0.28 %) TH (0.26 %) AU (0.26 %) EG (0.18 %) DZ (0.12 %) PL (0.11 %) RU (0.10 %) VN (0.09 %) CA (0.09 %) GB (0.09 %) US (0.07 %) BR (0.02 %) TR (0.01 %)

This threat actors appears to be standing up phishing pages to target potential victims African countries and other developing nations where banking can be more difficult, and local currencies much more unstable compared to the digital asset. Additionally, attackers have taken notice that targeting users in countries whose first language is not English make for potentially easier targets. Based on the number of queries, this campaign is one of the biggest targeting Blockchain.info to date. Blockchain.info has been very proactive in supporting users. Kristov Atlas, a security and privacy engineer at Blockchain.info, has even gone so far to say "phishing is one of our top areas of concern in protecting our users."

Quatifiying attacker’s revenue: Cisco has evidence the COINHOARDER group has been actively pilfering Bitcoin since at least 2015. Based on our findings, we estimate this group has stolen tens of millions of USD in cryptocurrency. While working with Ukraine law enforcement, we were able to identify the attackers' Bitcoin wallet addresses and thus, we could track their activity for the period of time between September 2017 to December 2017. In this period alone, we quantified around $10M was stolen.In one specific run, they made $2M within 3.5 week period. Here we have a screenshot of one of the wallets, 19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc, related to this actor group, which has received a total of $1,894,433.09.


Blockchain Luxembourg S.A.R.L [LU] | https://blockchain.info/address/19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc
KCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FR

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc
Hash 160	01b235ab3c269660c8c5239d6d97401a14624772
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	136
Total Received	$ 1,879,471.35
Final Balance	$ 0.00

Request Payment   Donation Button

Transactions (Oldest First)   Filter

d714aef718de2245c5fa f5fc7569073b5ee1893ed5bc7d73d2dd2f195f20b8cb   (Fee: $ 9.05 - 51.61 sat/WU - 206.43 sat/B - Size: 520 bytes) 2017-10-09 16:24:57

1Q6ZXsWEy193C7f8GJeM8rEsq3JA9dMXC1 ($ 11.21 - Output)
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc ($ 10.26 - Output)
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc ($ 13.49 - Output)
➡ 1NXaJmqv81NBJhJjhgP2hnFQy2tjwwytYX - (Spent) $ 5.17
19FYuwJmYABDyz2ft1Awb2iG1yxcaLEr7N - (Spent) $ 20.74

$ -23.75

CoinCola | Start Trading BTC, ETH, and BCH | Global OTC Marketplace | 0% trading fee | Perfect time to invest   Start Trading   Ad

b21522dba1680abc8b9954dc84cbc2fa84c7ac8fcd0013ad51ce6389e1ce6824   (Fee: $ 164.96 - 53.1 sat/WU - 212.4 sat/B - Size: 9213 bytes) 2017-10-07 22:05:53

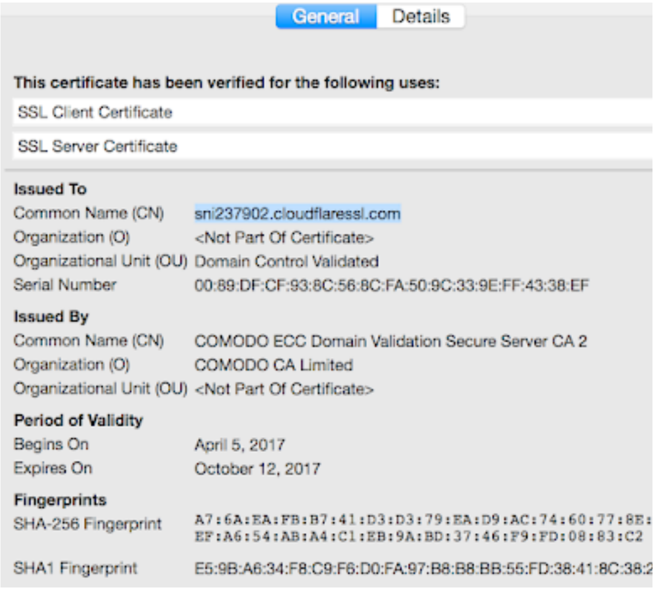
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc ($ 21.81 - Output) ➡ 17vGmAfciB7PJ1784dZywU7pRnUe1iWF9 - (Spent) $ 10.65

While identifying the individual who owns a specific wallet is extremely difficult, we still can look for open source intelligence surrounding the wallet. In December 2017, Cisco found posts on Reddit and Stack Exchange with addresses associated with stolen funds from this campaign, 13wahvu3FP8LK8P51UmEkhBUhyC7mzkrn3.

The wallet address in the screenshot above was also mentioned in a Reddit post in October 2017.

Based on our findings associated with this syndicate, we estimate the COINHOARDER group to have netted over $50M dollars over the past three years. It is important to note that the price of Bitcoin has shot up drastically over 2017, starting around $1,000 in January and hitting a high point just under $20,000 in December. While criminals were able to profit from this, it also adds a new level of complexity for criminals to convert their cryptocurrency funds to a fiat currency like US dollars. The historic price of Bitcoin during the height of this campaign would have made it very difficult to move these ill-gotten finances easily.

New effective attack techniques: Cisco has observed this threat actor evolve over time. Not only have we seen the COINHOARDER group abuse Google Adwords to generate traffic to their phishing servers, but we have also observed this group evolve to make their sites appear more legitimate. A few months after we began tracking this particular group, we observed them starting to use SSL certs issued by Cloudflare and Let's Encrypt. SSL certificate abuse has been a rising trend among phishing campaigns in general. Below is an example of a wildcard SSL certificate issued by Cloudflare for the domain bockchain[.]info.



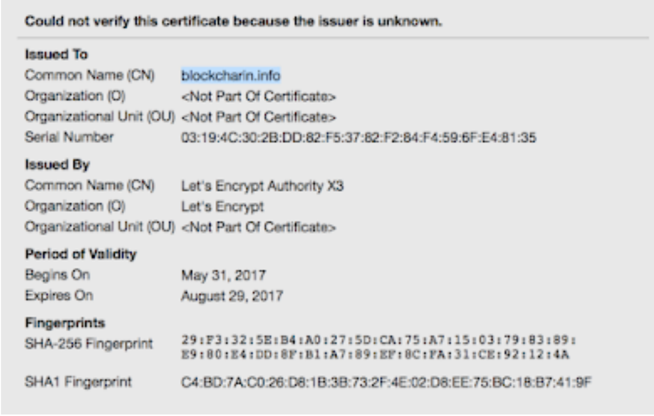
This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To	
Common Name (CN)	sni237902.cloudflaressl.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	Domain Control Validated
Serial Number	00:89:DF:CF:93:8C:56:8C:FA:50:9C:33:9E:FF:43:38:EF
Issued By	
Common Name (CN)	COMODO ECC Domain Validation Secure Server CA 2
Organization (O)	COMODO CA Limited
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	April 5, 2017
Expires On	October 12, 2017
Fingerprints	
SHA-256 Fingerprint	A7:6A:EA:FB:B7:41:D3:D3:79:EA:D9:AC:74:60:77:8E: EF:A6:54:AB:A4:C1:EB:9A:BD:37:46:F9:FD:08:83:C2
SHA1 Fingerprint	E5:9B:A6:34:F8:C9:F6:D0:FA:97:B8:B8:BB:55:FD:38:41:8C:38:2

Here is an example of one of these SSL certificates issued by Let's Encrypt associated with this campaign and the site blockcharin[.]info.


Could not verify this certificate because the issuer is unknown.

Issued To	
Common Name (CN)	blockcharin.info
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	03:19:4C:30:2B:DD:82:F5:37:82:F2:84:F4:59:6F:E4:81:35
Issued By	
Common Name (CN)	Let's Encrypt Authority X3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	May 31, 2017
Expires On	August 29, 2017
Fingerprints	
SHA-256 Fingerprint	29:F3:32:5E:B4:A0:27:5D:CA:75:A7:15:03:79:83:89: E9:80:E4:DD:8F:B1:A7:89:EF:8C:FA:31:CE:92:12:4A
SHA1 Fingerprint	C4:BD:7A:C0:26:D8:1B:3B:73:2F:4E:02:D8:EE:75:BC:18:B7:41:9F

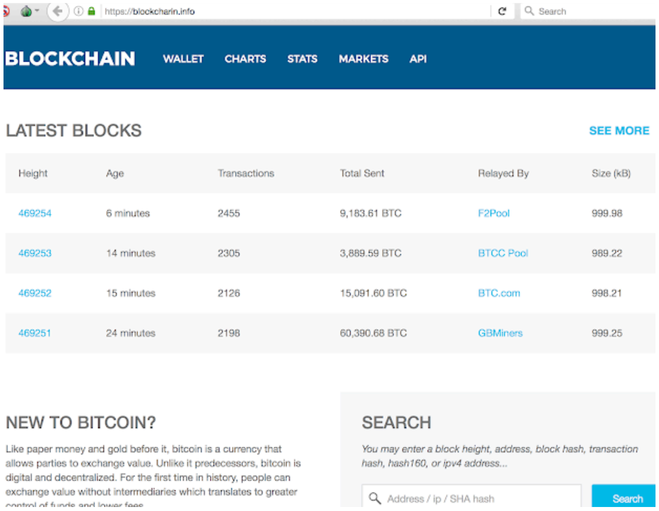
The COINHOARDER group has made heavy use of typosquatting and brand spoofing in conjunction SSL signed phishing sites in order to appear convincing. We have also observed the threat actors using internationalized domain names. These domains are used in what are called homograph attacks, where an international letter or symbol looks very similar to one in English. Here are some examples from this campaign.

The Punycode (internationalized) version is on the left, the translated (homographic) version on the right:

xn--blockchan-d5a[.]com → blockchaìn[.]com

xn--blokchan-i2a[.]info → blokchaìn[.]info

These attacks can be nearly impossible to spot with the human eye, especially when delivered on a mobile platform and using these techniques helps coax users into handing over their funds.



LATEST BLOCKS

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
469254	6 minutes	2455	9,183.61 BTC	F2Pool	999.98
469253	14 minutes	2305	3,889.59 BTC	BTCC Pool	989.22
469252	15 minutes	2126	15,091.60 BTC	BTC.com	998.21
469251	24 minutes	2198	60,390.68 BTC	GBMiners	999.25

NEW TO BITCOIN?

Like paper money and gold before it, bitcoin is a currency that allows parties to exchange value. Unlike it predecessors, bitcoin is digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees

SEARCH

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Address / ip / SHA hash

III. CONCLUSION

Crypto assets have proven to be a new, valuable financial commodity targeted by varying degrees of cyber criminals. In 2017, we observed phishers advance their tactics by utilizing new attack vectors such as Google

978-1-5386-4922-0/18/$31.00 ©2018 IEEE

Adwords combined with the use of IDNs and rogue SSL certificates to improve their probability of success, and generate millions in profit.

What is clear from the COINHOARDER campaign is that cryptocurrency phishing via Google Adwords is a lucrative attack on users worldwide. Phishers are significantly improving their attack techniques by moving to SSL and employing the use of IDNs to fool victims into handing over their credentials. We can expect to see more of these realistic looking phishes with Let's Encrypt releasing full wildcard certificate support at the end of this month. We will continue to monitor the landscape and coordinate with international law enforcement teams in 2018 to help protect users and organizations.

REFERENCES

[1] "New attacks on wallets and AdWords correlate with Bitcoin price surge" https://umbrella.cisco.com/blog/2016/12/22/protecting-bank-pocket-rise-criminal-activity-correlates-bitcoin-price-surge-holidays/

[2] "Rise in Bitcoin leads to more Phishing attacks" https://umbrella.cisco.com/blog/2017/02/28/bitcoin-phishing-attacks-gain-traction/

[3] "Changing the Standard of Phishing: Attack Trends,Tips and Tricks." https://umbrella.cisco.com/blog/2017/08/10/changing-standard-phishing-attack-trendstips-tricks/

[4] "Protecting ICOs and cryptocurrency users" https://umbrella.cisco.com/blog/2017/09/27/protecting-icos-cryptocurrency-users/

[5] 'COINHOARDER: Tracking a Ukrainian Bitcoin Phishing Ring DNS Style" http://blog.talosintelligence.com/2018/02/coinhoarder.html

[6] D. Hubbard and D. Mahjoub, "Using Large Scale Data to Provider Attacker Attribution for Unknown IOC's," https: //www.rsaconference.com/writable/presentations/file_upload/air- r04-using_large_scale_data_to_provide_attacker_attribution_for_unknown_iocs- .pdf, 2016.

[7] "Colocrossing resellers program," https://www.colocrossing.com/ services/resellers. "

[8] "Reseller partner program," https://www.leaseweb.com/partner-programs/reseller. "

[9] "Become an ovh partner," https://partners.ovh.com/become- a- partner. "

[10] "Voxility - iaas for service providers and large websites," https://www. voxility.com/info.

[11] "Whmcs web hosting billing and automation platform," https://www. whmcs.com/.

[12] "Ripe database documentation," https://www.ripe.net/manage- ips- and-asns/db/support/documentation/ripe- database- documentation/. "

[13] "Registration data access protocol (rdap)," http://rdap.afrinic.net/rdap/. "

[14] "Registration data access protocol (rdap)," http://www.lacnic.net/en/ web/lacnic/registration- data- access- protocol.

[15] D. Mahjoub, "Marauder or Scanning Your DNSDB for Fun and Profit," http://www.slideshare.net/OpenDNS/marauder- or- scanning- your-dnsdb- for- fun- and- profit- source- boston, 2014."

[16] "Cloudflare One-Click SSL" https://www.cloudflare.com/ssl/

[17] "Automatically enable HTTPS on your website with EFF's Certbot, deploying Let's Encrypt certificates." https://certbot.eff.org/

[18] "Use Google **AdSense** to make money online by placing ads on your website and YouTube channel." https://www.google.com/adsense/start/

978-1-5386-4922-0/18/$31.00 ©2018 IEEE