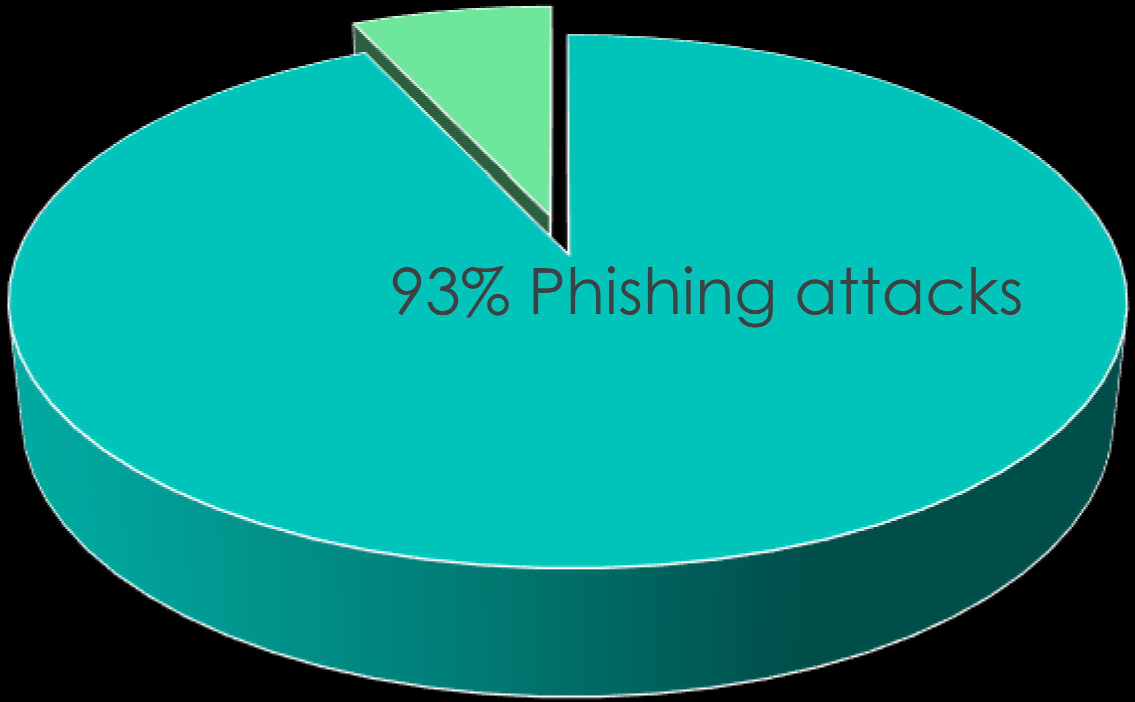
Phishing Attacks and Preventions in Blockchain Based Projects

A.A. Andryukhin
KCD LLC
Moscow, Russia

What is phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

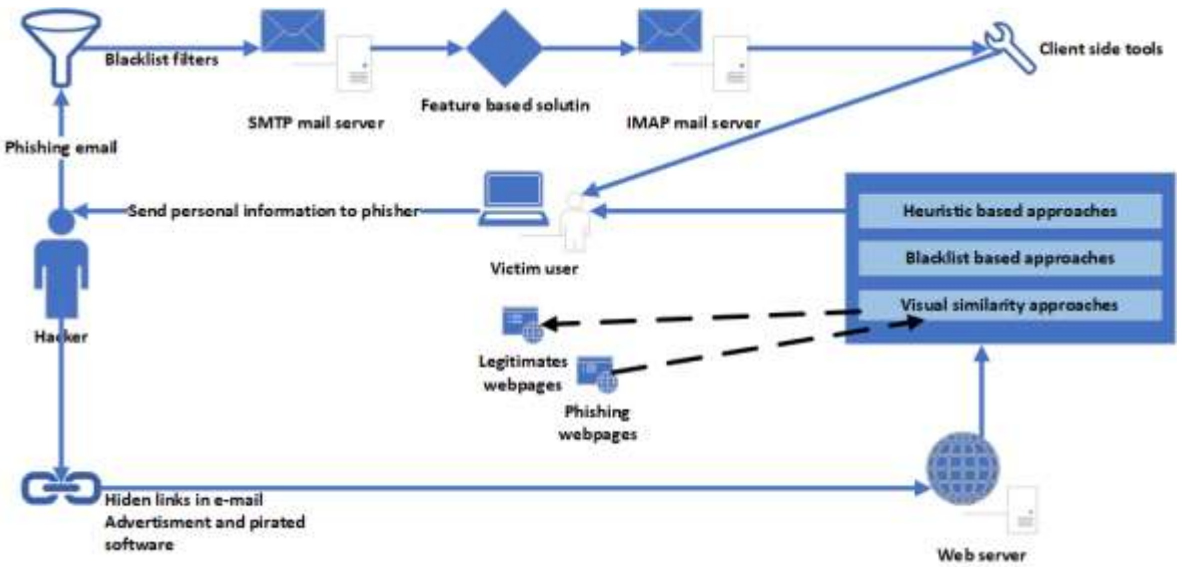
Social attacks in Q2 2018*



* Verizon Enterprise "2018 Data Breach Investigations Report"

TYPES OF PHISHING ATTACKS

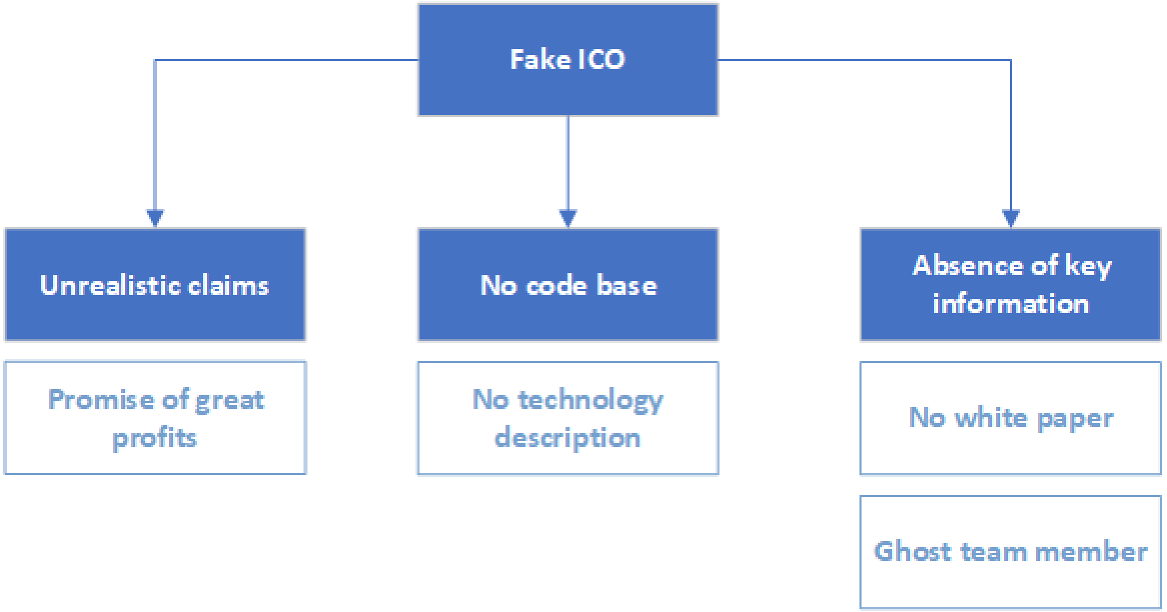
Example of the phishing scheme



Conventionally, all phishing attacks can be divided into two types: social engineering schemes and technical schemes. Social engineering schemes are based on deception and subsequent independent wrong actions of the victim, while technical schemes use vulnerabilities and imperfections of software and infrastructure.

Social Engineering Schemes - *Fake ICO*

Project	Description
PlexCoin, Ecoin	Projects did not own either the technologies that were claimed, nor the teams that could create the product. $15 million of PlexCoin ICO were frozen by SEC.



Fake ICO

Unrealistic claims

Promise of great profits

No code base

No technology description

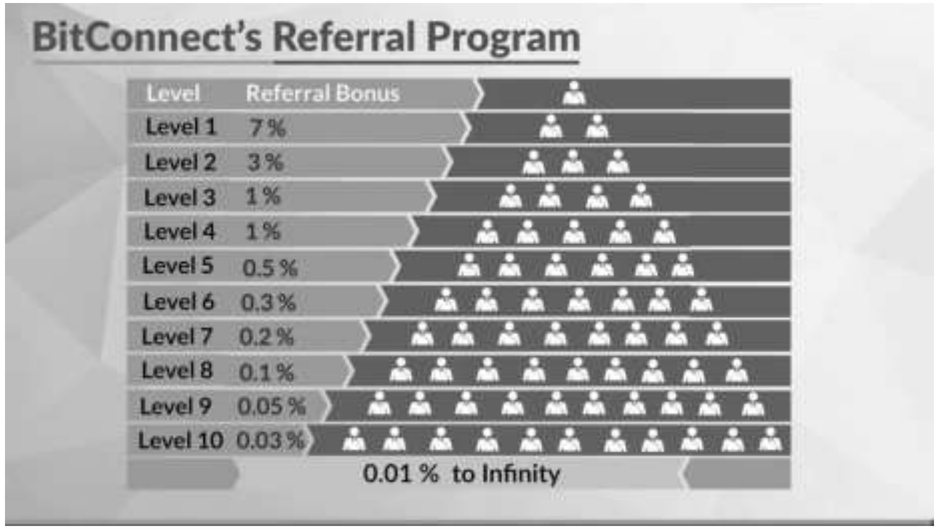
Absence of key information

No white paper

Ghost team member

Social Engineering Schemes - Pyramids, Ponzi

Project	Description
Bitcoin, Bitconnect	The organizer of an alleged Ponzi scheme advertised a Bitcoin "investment opportunity" in an online Bitcoin forum. Investors were allegedly promised up to 7% interest per week and that the invested funds would be used for Bitcoin arbitrage activities in order to generate the returns. Instead, invested Bitcoins were allegedly used to pay existing investors and exchanged into U.s. dollars to pay the organizer's personal expenses. Bitconnect promised 1% per day growth of invested funds.

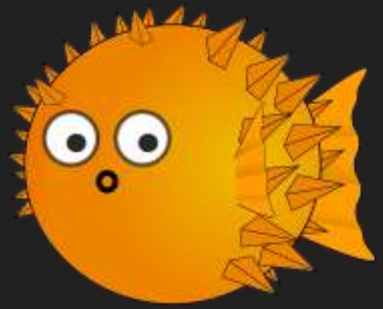


BitConnect's Referral Program

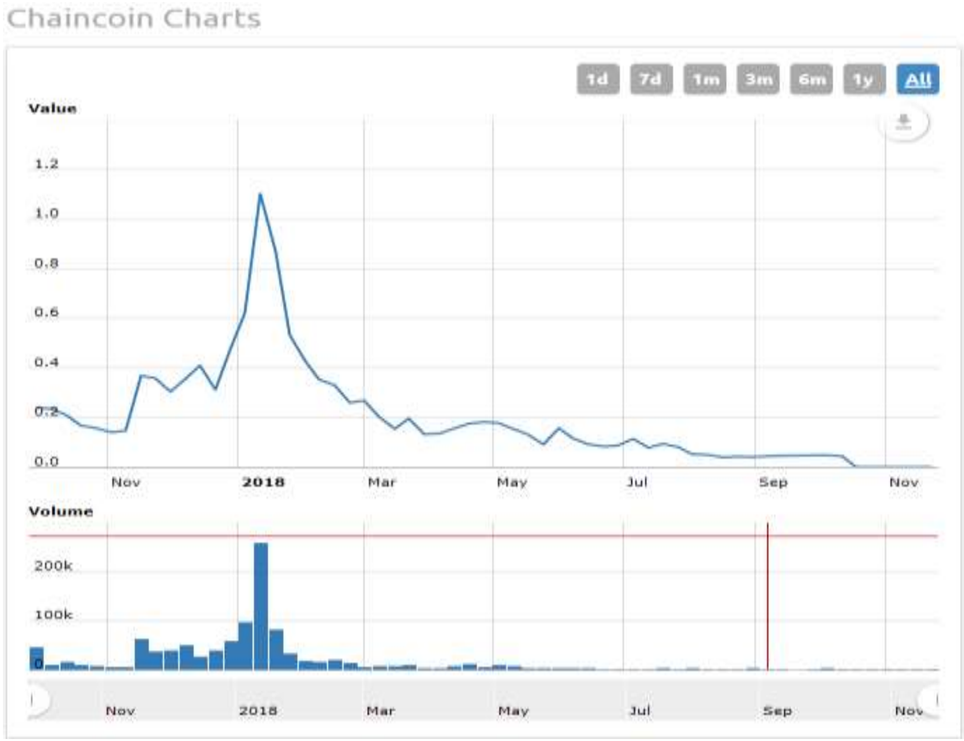
Level	Referral Bonus
Level 1	7 %
Level 2	3 %
Level 3	1 %
Level 4	1 %
Level 5	0.5 %
Level 6	0.3 %
Level 7	0.2 %
Level 8	0.1 %
Level 9	0.05 %
Level 10	0.03 %

0.01 % to Infinity

Social Engineering Schemes - ***Bloating***



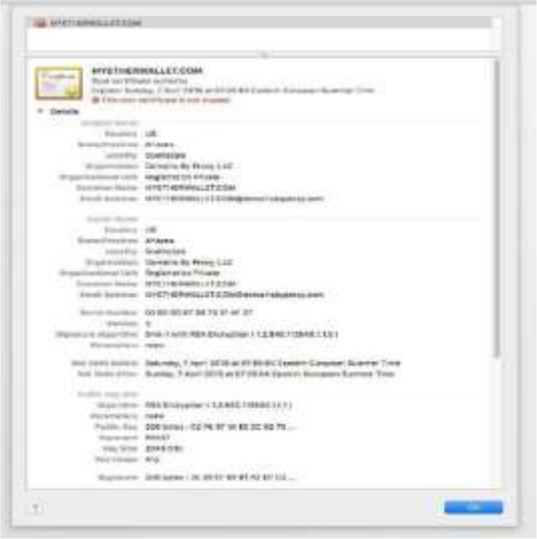
Project	Description
ChainCoin, HighCoin	Artificially created demand, aggressive advertising in the media and social networks led to an unprecedented growth and the subsequent sharp drop in the rate of the Crypto-currency



Social Engineering Schemes - Clones

Project	Description
Blockchain.info, MyEtherWallet, Binance, IOTA	Scammers use homograph attack to create a clone, advertising campaign and distribution. $50 million were stolen on the fake Blockchain.info site. A phishing website to generate private IOTA wallet seed passphrases, collected wallet keys, with estimates of up to $4 million worth of MIOTA tokens stolen.

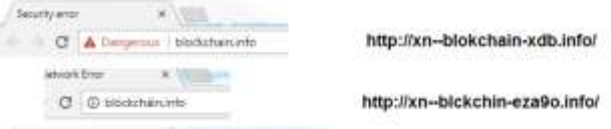
SSL of clone website



MYETHERWALLET.COM

Details

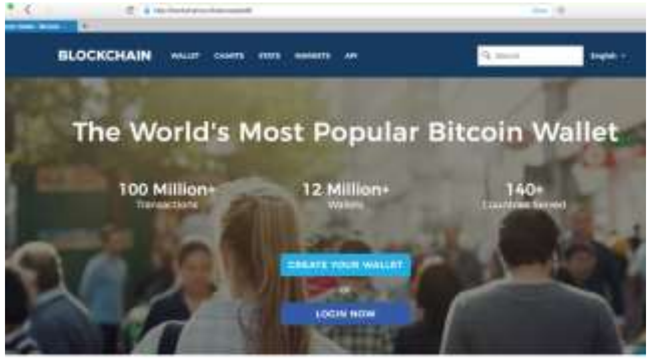
Homograph attack



http://xn--blokchain-xdb.info/

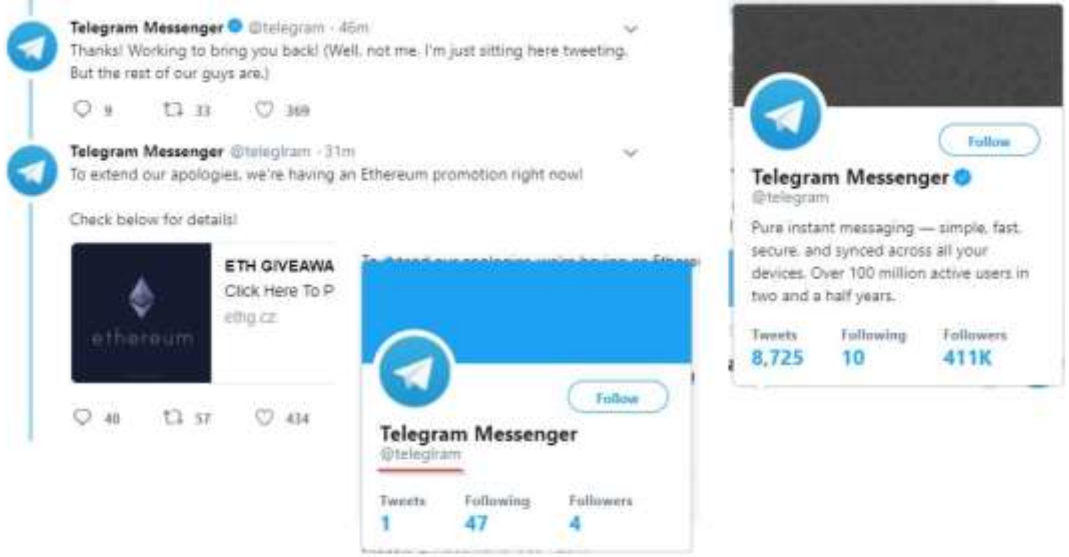
http://xn--blckchin-eza9o.info/

Clone website



Social Engineering Schemes - Social networking

Project	Description
Telegram, Blockchain.info	Scammers create fake accounts in social networks posing as well-known projects



Telegram Messenger @telegram · 46m

Thanks! Working to bring you back! (Well, not me. I'm just sitting here tweeting. But the rest of our guys are.)

9 33 369

Telegram Messenger @teleglram · 31m

To extend our apologies, we're having an Ethereum promotion right now!

Check below for details!

ETH GIVEAWA
Click Here To P
ethg.cz

40 57 434

Telegram Messenger @teleglram

Tweets 1 Following 47 Followers 4

Telegram Messenger @telegram

Pure instant messaging — simple, fast, secure, and synced across all your devices. Over 100 million active users in two and a half years.

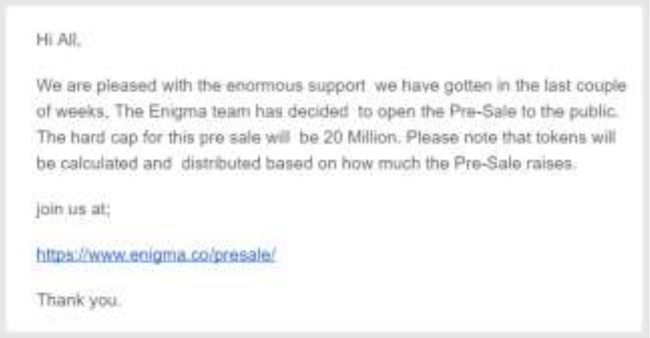
Tweets 8,725 Following 10 Followers 411K

https://twitter.com/kaspersky/status/979292135777361922?s=20

Social Engineering Schemes - ***Aimed phishing***

Project	Description
Enigma, Bee, Seele	The hackers got access to the email of Enigma CEO Gaius Ziskind. As a result, all the investors were sent messages with the offer to participate in reselling the tokens and the account details for transferring funds and $500 000 has been stolen. $1 million (Bee) and $1.8 million (Seele) were stolen using hacking of companies official e-mail lists.

Letter sent by hackers to investors from hacked mail of Enigma CEO Gaius Ziskind



Hi All,

We are pleased with the enormous support we have gotten in the last couple of weeks. The Enigma team has decided to open the Pre-Sale to the public. The hard cap for this pre sale will be 20 Million. Please note that tokens will be calculated and distributed based on how much the Pre-Sale raises.

join us at;

https://www.enigma.co/presale/

Thank you.

Check Wallet

Fake wallet - 0x29d7d1dd5b6f9c864d9db560d72a247c178ae86b

Technical schemes-Malware

Project	Description
Cryptoexchanges	Hackers from Lazarus Group (North Korea) chatted, posing as "key people" in the crypto currency industry, and during the conversation they published a small piece of code that was actually malware. They also sent out software by email. If the user downloaded this code, the hacker had the opportunity to enter his system and steal the crypto-currencies.

Indicators of Compromise

File Hashes (malicious documents, trojans, emails, decoys)

Trojanized installer and payload
9e740241ca2acdc79f30ad2c3f50990a celastradepro_win_installer_1.00.00.msi
4126e1f34cf282c354e17587bb6e8da3 celastradepro_win_installer_1.00.00.msi
0bdb652bbe15942e866083f29fb6dd62 CelasTradePro-Installer.msi
48ded52752de9f9b73c6bf9ae81cb429 celastradepro_mac_installer_1.00.00.dmg
b054a7382adf6b774b15f52d971f3799 Updater.exe
ffae703a1e327380d85880b9037a0aeb Updater.exe
bbbcf6da5a4c352e8846bf91c3358d5c Updater.exe
0a15a33844c9df11f12a4889ae7b7e4b msn.exe
E1ed584a672cab33af29114576ad6cce uploadmgrsvc.dll
D8484469587756ce0d10a09027044808 uploadmgr.dat
D7089e6bc8bd137a7241a7ad297f975d
Same RC4 key Fallchill
Same C&C server Fallchill

File path

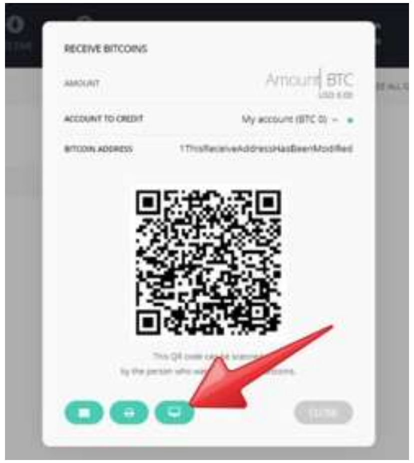
C:\Recovery\msn.exe
C:\Recovery\msndll.log
C:\Windows\msn.exe
C:\WINDOWS\system32\uploadmgrsvc.dll
C:\WINDOWS\system32\uploadmgr.dat

Domains and IPs

www.celasllc[.]com/checkupdate.php (malware distribution URL)
196.38.48[.]121
185.142.236[.]226
80.82.64[.]91
185.142.239[.]173

*Technical schemes- **Session hijacking***

Project	Description
Hardware wallet manufacturer Ledger	Attackers replace the code responsible for creating the recipient's address with its own address, as a result of which all future deposits will be sent to the attacker

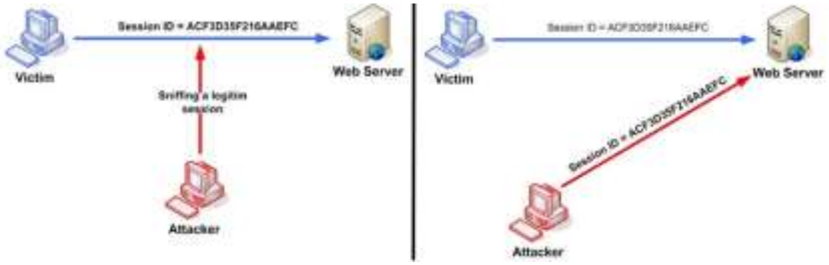


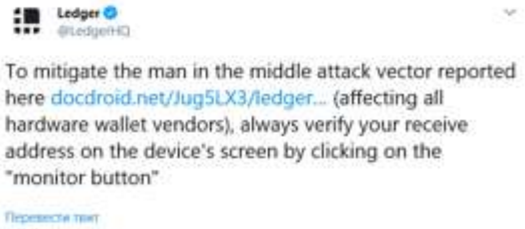
RECEIVE BITCOINS

AMOUNT Amount BTC

ACCOUNT TO CREDIT My account (BTC 0)

BITCOIN ADDRESS 1ThisReceiveAddressHasBeenModified


Victim
Session ID = ACF3D35F216AAEFC
Web Server
Sniffing a logitim session
Attacker
Victim
Session ID = ACF3D35F216AAEFC
Web Server
Session ID = ACF3D35F216AAEFC
Attacker



Ledger
@LedgerHQ

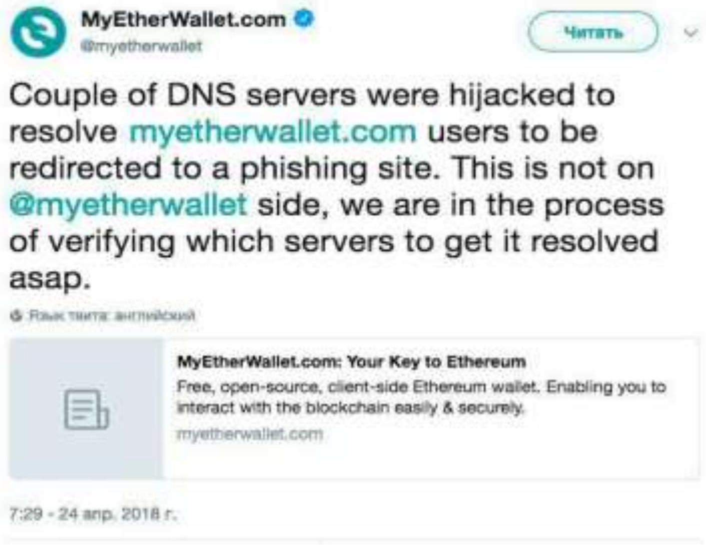
To mitigate the man in the middle attack vector reported here docdroid.net/Jug5LX3/ledger... (affecting all hardware wallet vendors), always verify your receive address on the device's screen by clicking on the "monitor button"

Перевести твит

Эта фотография, автор: Неизвестный автор, лицензия: CC BY

Technical schemes- DNS based

Project	Description
Blockchain.info, MyEtherWallet	Substitution of DNS data, users were targeted at malicious sites



MyEtherWallet.com
@myetherwallet

Couple of DNS servers were hijacked to resolve myetherwallet.com users to be redirected to a phishing site. This is not on @myetherwallet side, we are in the process of verifying which servers to get it resolved asap.

Язык твита: английский

MyEtherWallet.com: Your Key to Ethereum
Free, open-source, client-side Ethereum wallet. Enabling you to interact with the blockchain easily & securely.
myetherwallet.com

7:29 - 24 апр. 2018 г.

Technical schemes- *Key loggers*

Project	Description
Blockchain.info, Electrum wallet	Thousands of Bitcoins were stolen using keyloggers. Example of a keylogger capable of tracking up to 2.3 million addresses. The program is part of the package All-Radio 4.27 Portable, distributed now by scammers. The infection occurs after the D3DX11_31. DLL program module is placed in the Windows/Temp system folder. When infected, the module is added to the startup procedure, where it appears under the inscription "DirectX 11".

Methods of Prevention

Scheme	Type	Solution	
Social engineering phishing	Fake ICO Bloating Pyramids, Ponzi	Checking projects documentation and site traffic; avoiding risky financial investments	Using bookmarks instead links; the use of browsers with anti-phishing extension, the installation of anti-phishing software, the prohibition of clicking through links and downloading questionable attachments; authentication of the SSL certificate before using the services; inform about phishing, launch off-line copies of cryptowallets, use of two-factor authentication, complex passwords (minimum 14 symbols), refusal of public Wi-Fi, use of secure gateway.
	Clones Aimed phishing Social networking	Protection of mail servers, databases of employees, customers, investors; tracking activity on corporate pages and community pages	
Technical phishing	DNS based	Develop a DNS alternative, for example, ENS (the Ethereum name service)	
	Hijacking	Verify receive and send address	
	Malware	Do not open and install attachments	
	Key loggers	Monitor processes on task manager of device, check signatures, use on-screen keyboards, password wallets.	

Q&A

A.A. Andryukhin

KCD LLC

Moscow, Russia

Alexandr@kcdigital.ru