Dokąd zmierza bezpieczeństwo

Adam Haertle

aruba CLOUD

ZAUFANA TRZECIA STRONA.PL

ASUS
COLOR SLIDES

APT REPORTS

Operation ShadowHammer

By GReAT on March 25, 2019. 1:01 pm

Earlier today, Motherboard published a story by Kim Zetter on Operation ShadowHammer, a newly discovered supply chain attack that leveraged ASUS Live Update software.

While the investigation is still in progress and full results and technical paper will be published during SAS 2019 conference in Singapore, we would like to share some important details about the attack.

In January 2019, we discovered **a sophisticated supply chain attack involving the ASUS Live Update Utility**. The attack took place between June and November 2018 and according to our telemetry, it affected a large number of users.

ASUS Live Update is an utility that is pre-installed on most ASUS computers and is used to automatically update certain components such as BIOS, UEFI, drivers and applications. According to Gartner, ASUS is the world's 5th-largest PC vendor

.kaspersky.com/advert/small-business-security?redef=1&THRU&...

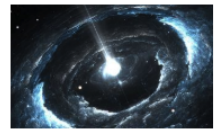
IN THE SAME CATEGORY

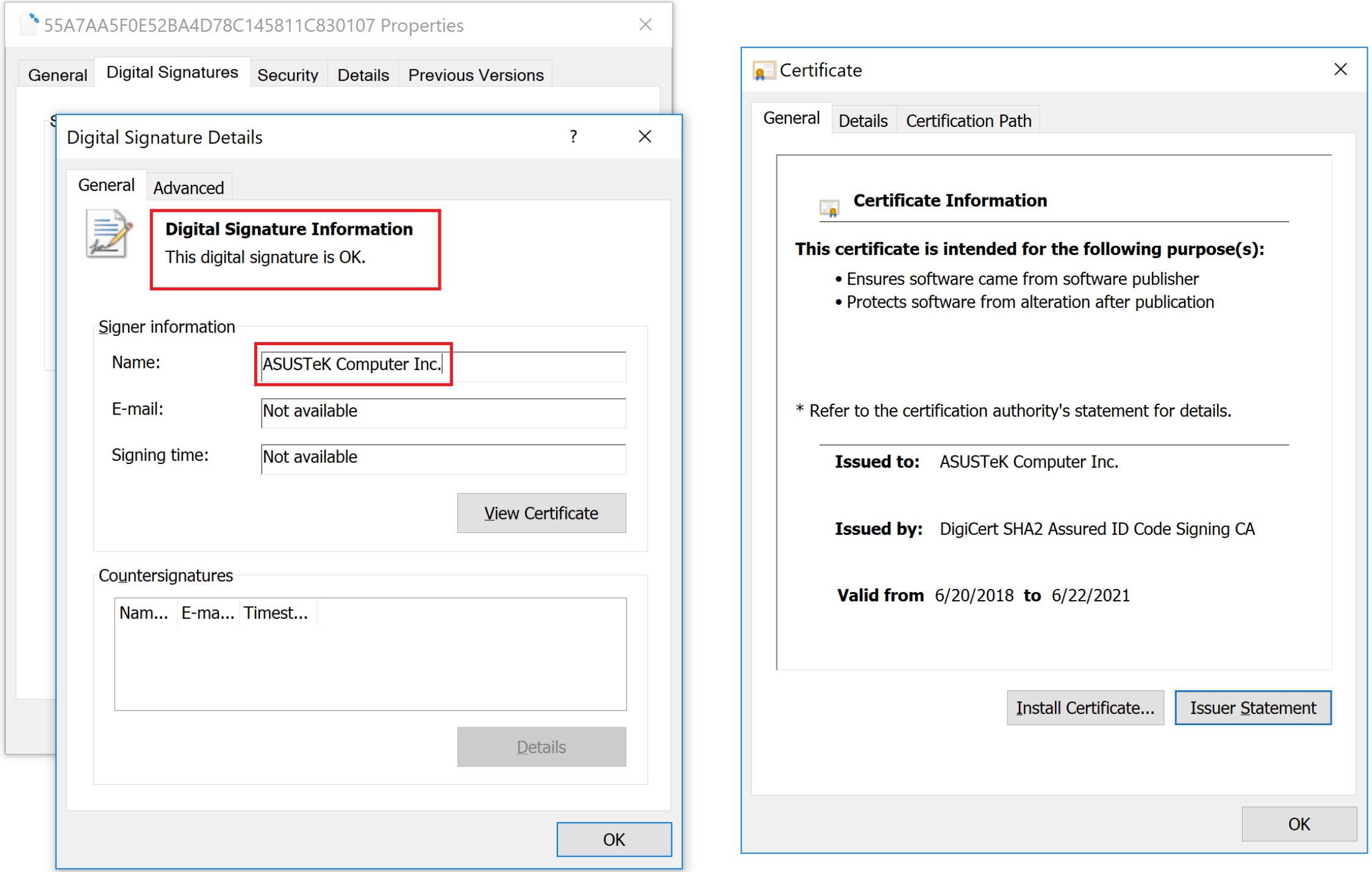
Chafer used Remexi malware t
Iran-based foreign diplomatic

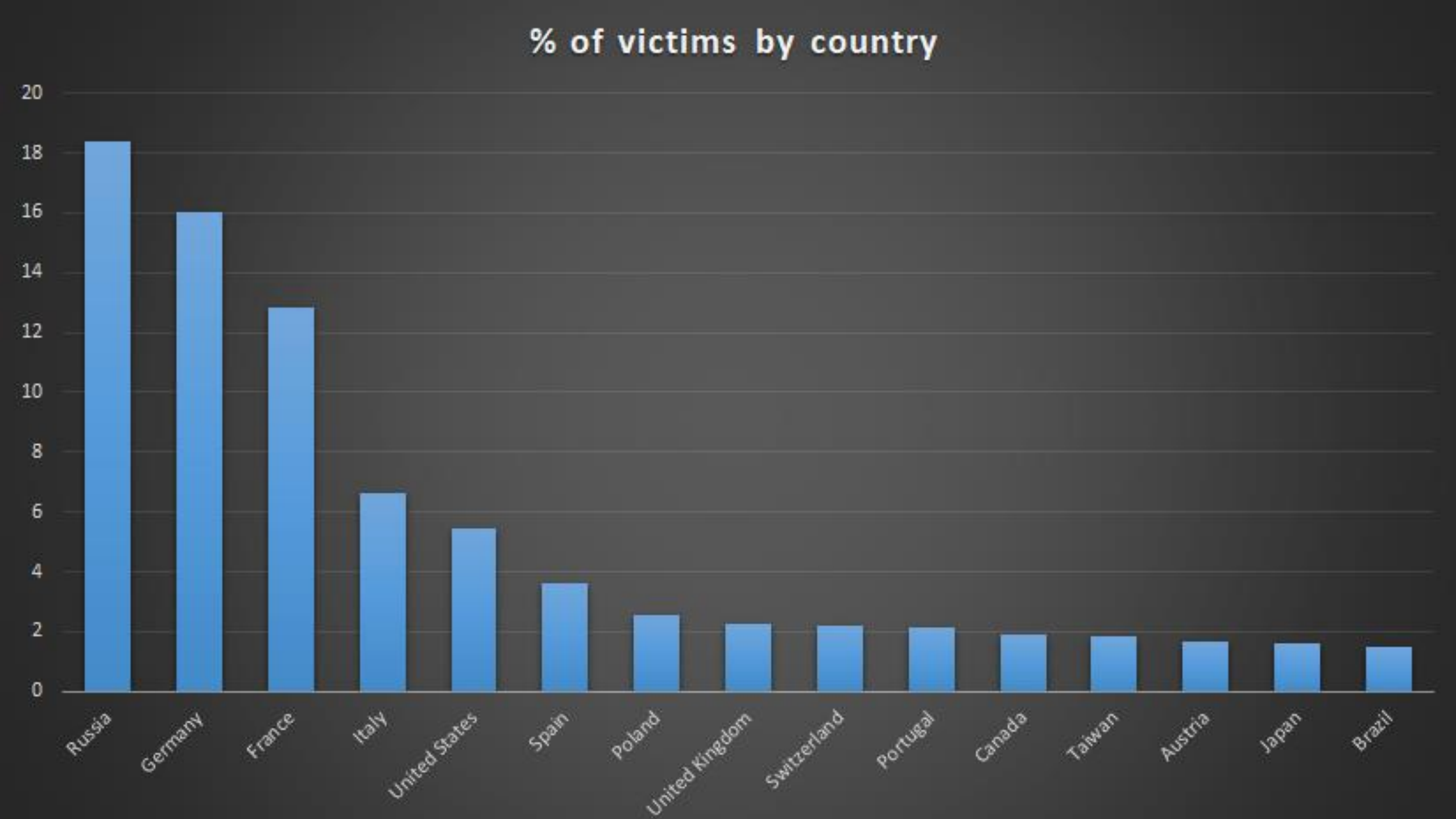
GreyEnergy's overlap with Zeb

A Zebrocy Go Downloader

APT review of the year


DarkPulsar FAQ


55A7AA5F0E52BA4D78C145811C830107 Properties
General
Digital Signatures
Security
Details
Previous Versions
Digital Signature Details
General
Advanced
Digital Signature Information
This digital signature is OK.
Signer information
Name:
ASUSTeK Computer Inc.
E-mail:
Not available
Signing time:
Not available
View Certificate
Countersignatures
Nam...
E-ma...
Timest...
Details
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: ASUSTeK Computer Inc.
Issued by: DigiCert SHA2 Assured ID Code Signing CA
Valid from 6/20/2018 to 6/22/2021
Install Certificate...
Issuer Statement
OK

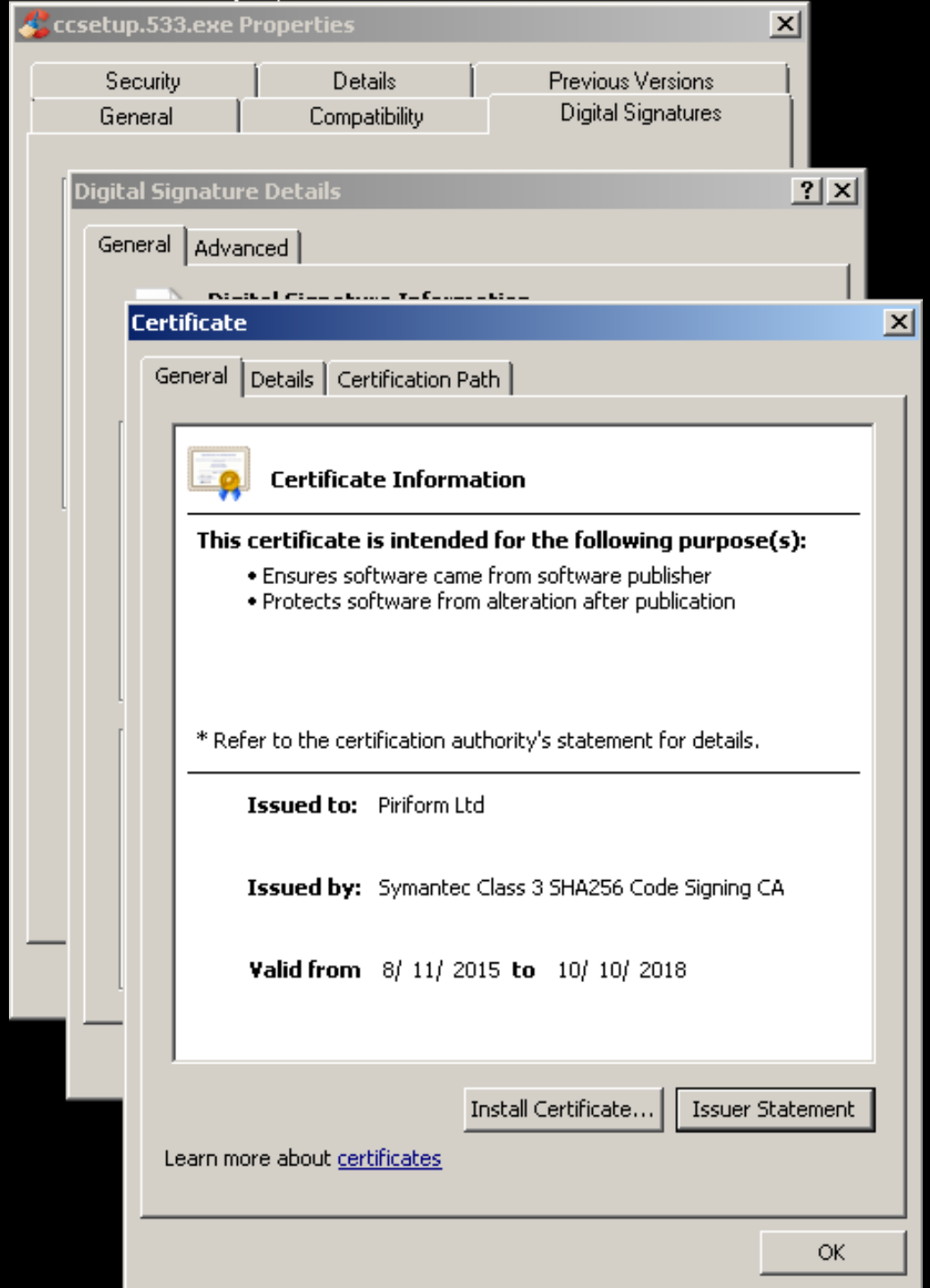

% of victims by country
20
18
16
14
12
10
8
6
4
2
0
Russia
Germany
France
Italy
United States
Spain
Poland
United Kingdom
Switzerland
Portugal
Canada
Taiwan
Austria
Japan
Brazil

Speed up & Optimize your PC with CCleaner®

CCleaner has been downloaded over 2 billion times!

Buy CCleaner Pro!

Free Download


ccsetup.533.exe Properties
Security
Details
Previous Versions
General
Compatibility
Digital Signatures
Digital Signature Details
General
Advanced
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: Piriform Ltd
Issued by: Symantec Class 3 SHA256 Code Signing CA
Valid from 8/ 11/ 2015 to 10/ 10/ 2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK

Domain	Industry	Country	Number of impacted PCs
cht.com.tw	Telco	Taiwan	13
nsl.ad.nec.co.jp	Tech	Japan	10
samsung samsung.sk samsung.sepm	Tech	Korea	5
corpnet.asus paskey.corpnet.asus	Tech	Taiwan	2
ad.fip.fujitsu.com domain.ftsp.ten.fujitsu.com	Tech	Japan	2
am.sony.com	Tech	Japan	2
infoview2u.dvrdns.org	Internet	USA	1
uk.pri.o2.com	Telco	UK	1
gg.gauselmann.com	Gaming	Germany	1
singtel	Telco	Singapore	1
intel.com	Tech	USA	1
vmware.com	Tech	USA	1

Samsung
Electronics Poland...

Domain	Industry	Country	Number of impacted PCs
htcgroup.corp	Tech	Taiwan	0
linksys	Tech	USA	0
apo.epson.net	Tech	Japan	0
vf-es.internal.vodafone.com	Telco	UK	0
ntdev.corp.microsoft.com	Tech	USA	0
dlink.com	Tech	Taiwan	0
hq.gmail.com	Tech	USA	0
dfw01.corp.akamai.com	Internet	USA	0
msi.com.tw	Tech	Taiwan	0
cisco.com	Tech	USA	0
cyberdyne.jp cyberdyne.local cyberdyne.root	Tech	Japan	0
tti-ecm.local tti.local tti.on.ca	Military	Canada	0
godaddy	Internet	USA	0

Hydro

Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

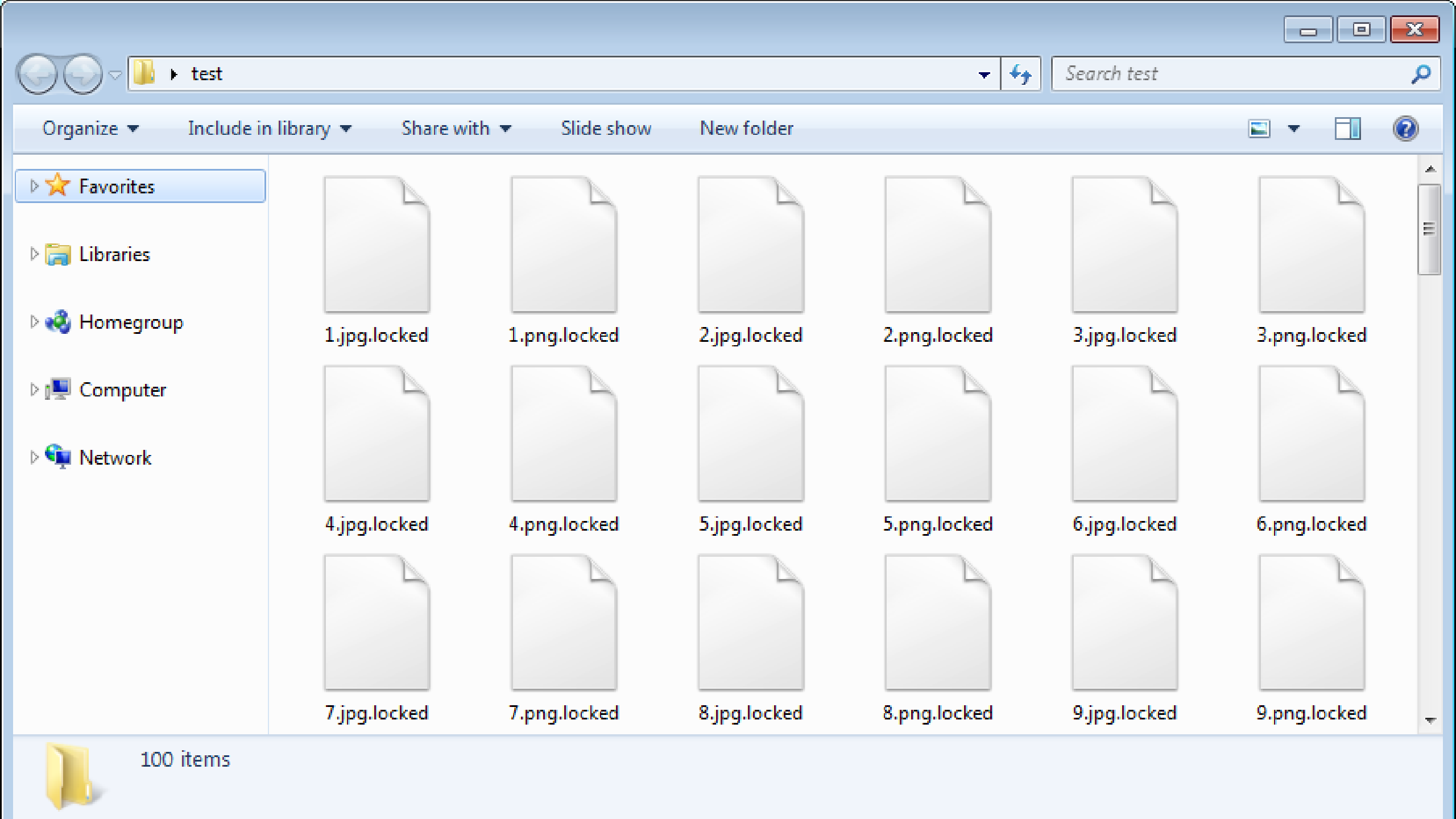
To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

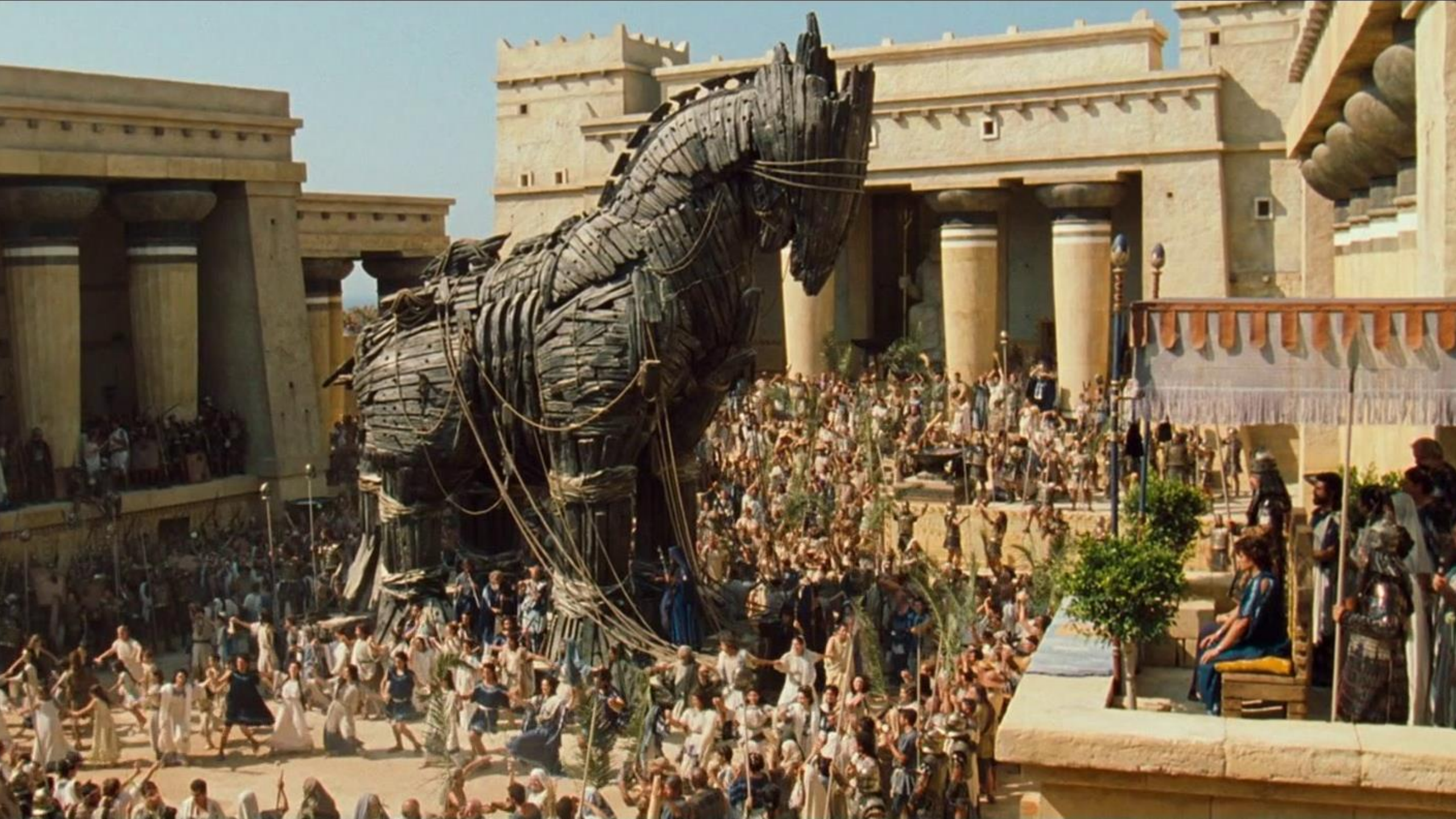
We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:
SuzuMcpherson@protonmail.com
AsuxidOruraep1999@o2.pl

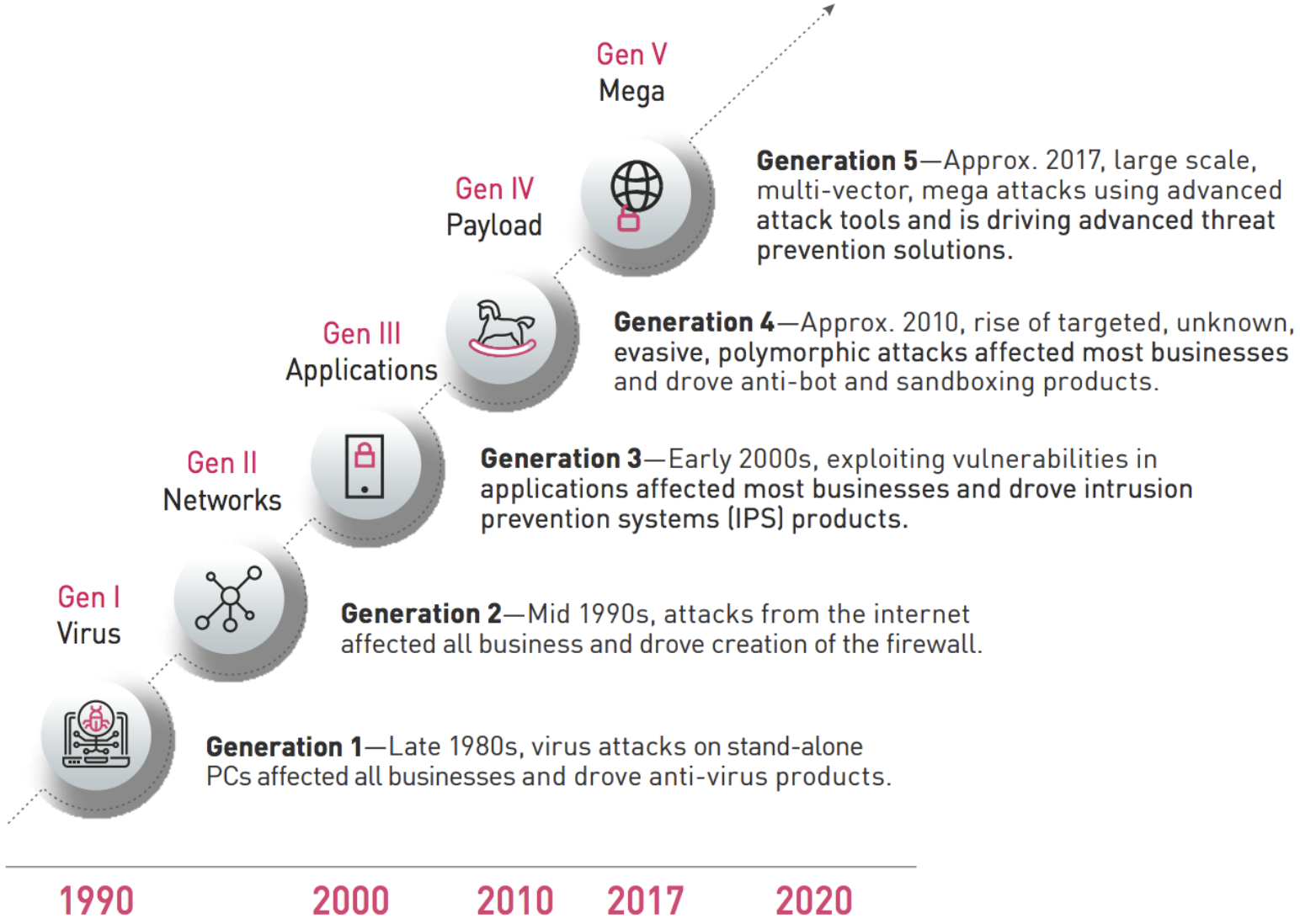

test
Search test
Organize
Include in library
Share with
Slide show
New folder
Favorites
Libraries
Homegroup
Computer
Network
1.jpg.locked
1.png.locked
2.jpg.locked
2.png.locked
3.jpg.locked
3.png.locked
4.jpg.locked
4.png.locked
5.jpg.locked
5.png.locked
6.jpg.locked
6.png.locked
7.jpg.locked
7.png.locked
8.jpg.locked
8.png.locked
9.jpg.locked
9.png.locked
100 items



5TH GENERATION CYBER ATTACKS ARE HERE AND MOST BUSINESSES ARE BEHIND

A New Model For Assessing and Planning Security

GEN V



"Only 5% of enterprises are using Gen 5 Cyber Security"

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book

Fifth generation cyberattack

From Wikipedia, the free encyclopedia

A major contributor to this article appears to have a close connection with its subject. It may require cleanup to comply with Wikipedia's content policies, particularly neutral point of view. Please discuss further on the talk page. *(August 2018) (Learn how and when to remove this template message)*

A **fifth generation cyberattack** is a type of bullshit that was made up by Cindy J Wilson beginning in 2017. This term is not used outside of Checkpoint marketing and should die a cold death.

They do not take advantage of information and tools leaked from government entities like the National Security Agency and the Central Intelligence Agency to rapidly spread around the world, impacting global businesses and communities.[1]

Computer security experts generally do not describe cyberattacks in terms of five *generations*, tracking their evolution from simple computer viruses in the early 1980s, and growing in sophistication and scale in the decades since.[2][3][4][5][6][7] The NotPetya and WannaCry ransomware attacks of 2017 marked the beginning of what is now described as the fifth generation.[8]

In recent years, the scale and robustness of cyberattacks has increased rapidly, as observed by the World Economic Forum in its 2018 report: "Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents."[9] Researchers found that 2017's WannaCry and NotPetya represented a growth in the frequency, sophistication and malice of cyberattacks on businesses.[10]

Shortly after the WannaCry attack, it was identified by the UK National Crime Agency as a "signal moment" for awareness of the impact of cyber crimes. Commentators were hopeful that organizations would respond with a more serious approach to security.[11] The European Police Commission highlighted the tendency of organized crime to adopt new technology.[12] In October 2017, Bad Rabbit, a variant of NotPetya, spread across Europe.[13]

Defining characteristics [edit]

- Made up by Checkpoint marketing
- Designed to scare stupid people
- Based on no actual research

ufoludek-zkosmosu 2 tyg. temu via Android

+626 +

#bezpleczenstwo

źródło: 1544101838159.jpg

+: TwojStaryToKorniszon, totalski +624 innych

odpowiedz ulubiony zgłoś udostępnij

‹ embed ›

Benchmark.pl

6 grudnia o 21:29 ·

Dziś na naszym fan page pojawił się mem o treści „Twoja historia przeglądarki z trybu incognito jest przechowywana w folderze system32. Dla bezpieczeństwa usuń go.". JEST TO INFORMACJA NIEPRAWDZIWA. Nie usuwajcie folderu system32. Publikując tego mema, uznaliśmy za oczywiste, że nie należy tego robić i jest to gag. Niestety dostaliśmy wiele wiadomości typu „nie mogę usunąć tego folderu". Przepraszamy za podanie nieprawdziwej informacji i mamy nadzieje, że Wasze Windowsy wciąż działają.

475 Komentarze: 71 13 udostępnień

Lubię to! Komentarze Udostępnij

Zach Latta

Secure https://mail.google.com/mail/u/0/#inbox/15bcf9777720353b

Google

Streak

Mail

More

2 of 13

COMPOSE

Inbox
Starred
Sent Mail
Drafts (251)
All Mail
Snoozed
Pipelines + New
Assistant (60)
Backlog
Bankruptcy (26)
BitBot (2)
Contracting
GitHub
Hack Club
Notes
More

Jennifer Worshek has shared a document on Google Docs with you

Inbox x

jworshek@swmetro.k12.mn.us 11:34 AM (14 minutes ago)
to hhhhhhhhhhhhh., bcc: zach

Jennifer Worshek has invited you to view the following document:

Open in Docs

Click here to Reply to all, Reply, or Forward

10.52 GB (8%) of 130 GB used
Manage

Program Policies
Powered by Google

Last account activity: 0 minutes ago
Open in 1 other location Details

People (2)

jworshek

Add to circles

Show details

https://tradeit.cash

TRADEIT.CASH
SELL YOUR SKINS

How it works | Bonus | FAQ | Blog | Buy skins | Partnership

STEAM LOGIN

USD

EN

Sell CSGO skins

Sell CS:GO skins • Sell Dota 2 items • Sell TF2 items • Sell PUBG skins • Sell H1Z1 skins

Sign in via Steam. Choose and sell CS:GO skins. Get cash.

GET CASH NOW

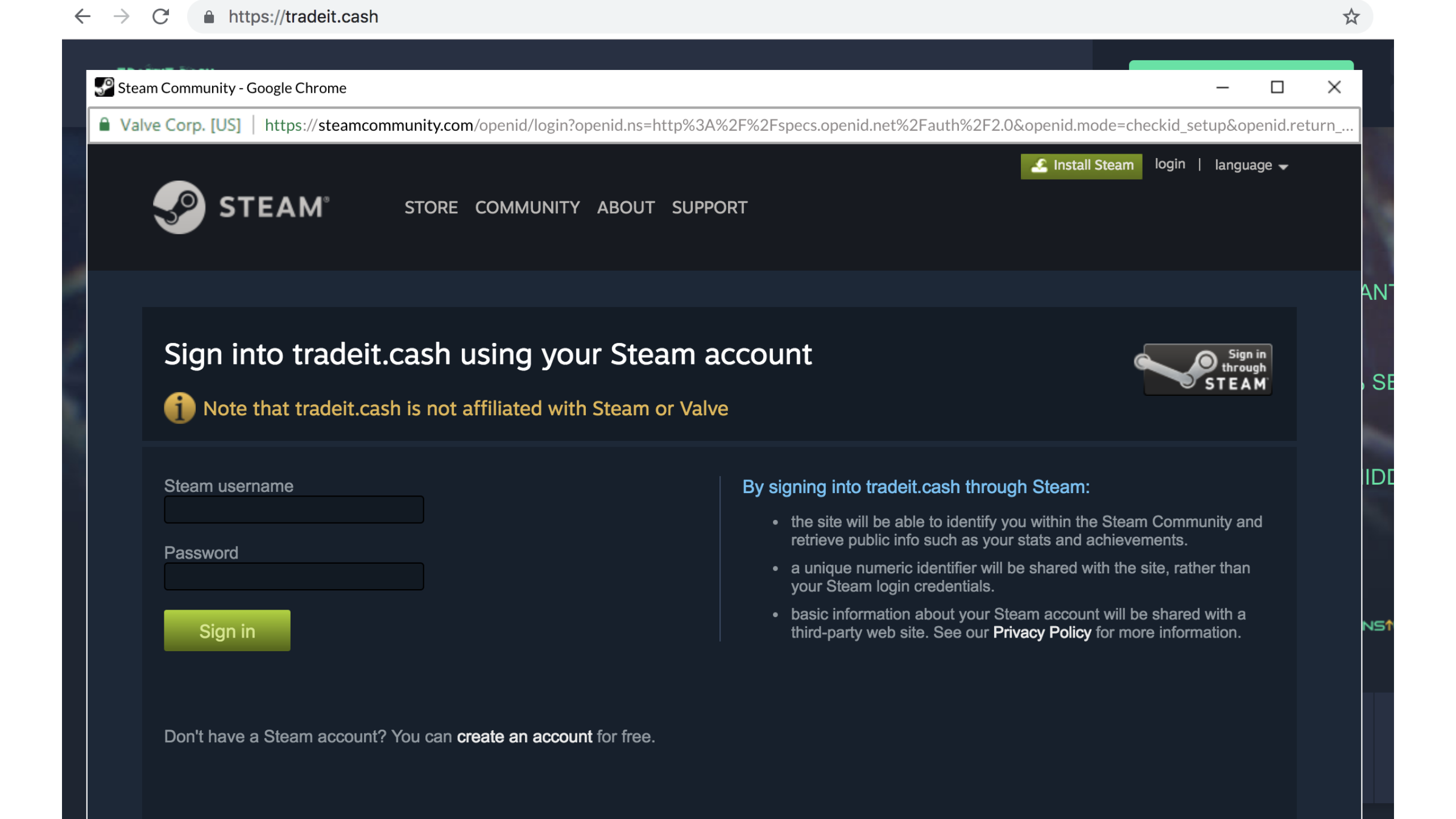
INSTANT CASH

100% SECURE

NO HIDDEN FEES

PayPal | СБЕРБАНК | QIWI | WebMoney | VISA | ПОПОЛНИТЬ ТЕЛЕФОН | Яндекс Деньги | Skrill | PAYEER | SKINSTUP | Dmarket tokens

LIVE DEALS	€ 0.37	₴ 226.38	₽ 906.23	₽ 1230.56	€ 0.06	€ 1.01	29602880
	by алек***др	by ⌐╦******	by Mi******	by Je****	by алек***др	by huma**********on	skins sold
	19 m ago	20 m ago	21 m ago	22 m ago	27 m ago	31 m ago	


https://tradeit.cash
Steam Community - Google Chrome
Valve Corp. [US] | https://steamcommunity.com/openid/login?openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=checkid_setup&openid.return_...
Install Steam
login | language
STEAM
STORE COMMUNITY ABOUT SUPPORT
Sign into tradeit.cash using your Steam account
Sign in through STEAM
Note that tradeit.cash is not affiliated with Steam or Valve
Steam username
Password
Sign in
By signing into tradeit.cash through Steam:
the site will be able to identify you within the Steam Community and retrieve public info such as your stats and achievements.
a unique numeric identifier will be shared with the site, rather than your Steam login credentials.
basic information about your Steam account will be shared with a third-party web site. See our Privacy Policy for more information.
Don't have a Steam account? You can create an account for free.

Girls HairStyle (Offl
100 Million Downloads

★★★★★

Blouse Designs Offl
100 Million Downloads

★★★★★

Mehndi Designs 20
100 Million Downloads

★★★★★

Sports Wallpapers 2
100 Million Downloads

★★★★☆

All-In-One Kids: Lea
100 Million Downloads

★★★☆☆

Virat Kohli : The App
100 Million Downloads

Love Messages - 20
100 Million Downloads

RTO Exam: Driving L
100 Million Downloads

Nani Teri Morni Offl
100 Million Downloads

Java Tutorial And Pi
100 Million Downloads

Remote Play for PS
5,000,000,000+

FREE

super kirby original
5,000,000,000+

FREE

LOL Super Surprise
5,000,000,000+

FREE

PF: photo filters

Alex Carrol Photography

★ ★ ★ ★ ★ 354

PEGI 3

Offers in-app purchases

This app is compatible with your device.

Add to Wishlist Install

Add cool filters, text, paint with custom brush and add beautiful frames!

Google Play

Premium Features
PF: photo filters

Free
3 day trial

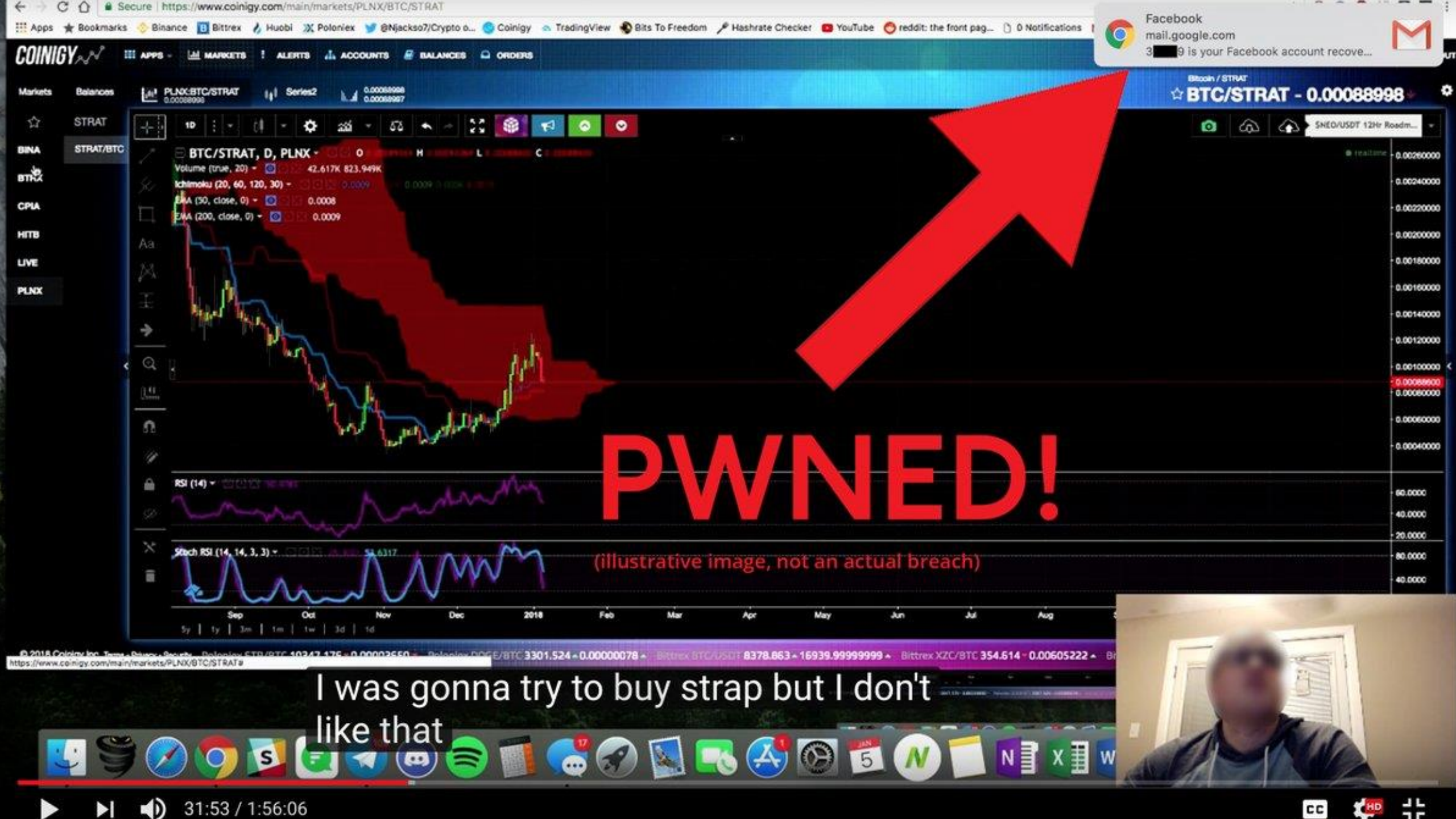
After free trial
starting Feb 7, 2019

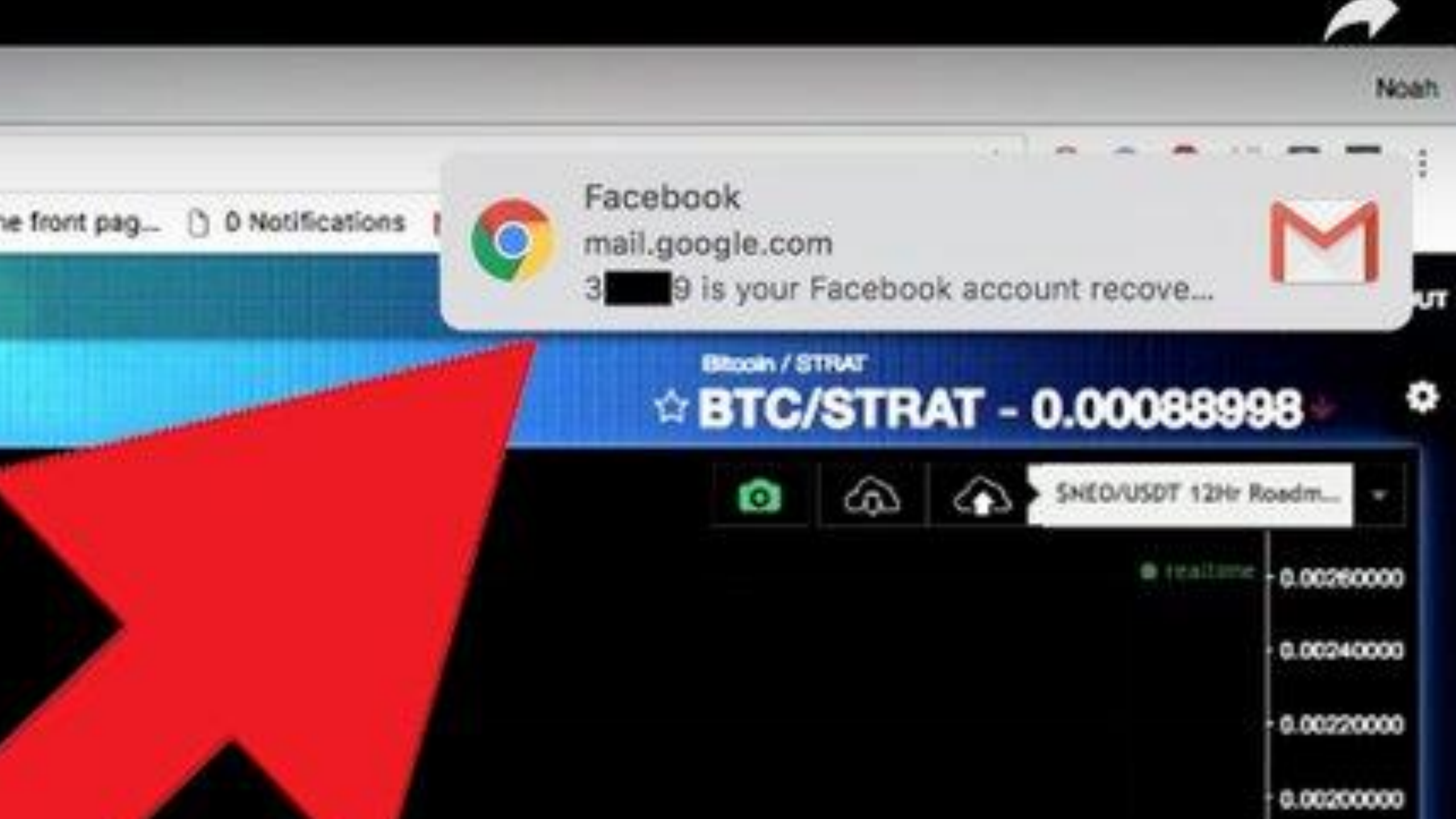
€49.99/week

G Pay Payment method needed

- Cancel anytime in Google Play
- You won't be charged if you cancel before Feb 7, 2019

CONTINUE


Facebook
mail.google.com
3[redacted]9 is your Facebook account recove...
COINIGY
BTC/STRAT - 0.00088998
BTC/STRAT, D, PLNX
PWNED!
(illustrative image, not an actual breach)
I was gonna try to buy strap but I don't like that
31:53 / 1:56:06


Noah
0 Notifications
Facebook
mail.google.com
3[redacted]9 is your Facebook account recove...
Bitcoin / STRAT
BTC/STRAT - 0.00088998
SNEO/USDT 12Hr Roadm...
realtime
0.00260000
0.00240000
0.00220000
0.00200000

ethereum

Elon Musk @PantheonBooks

I'm giving 10 000 Bitcoin (BTC) to all community!

I left the post of director of Tesla, thank you all for your support!

I decided to make the biggest crypto-giveaway in the world, for all my readers who use Bitcoin.

Participate in giveaway - musk.plus

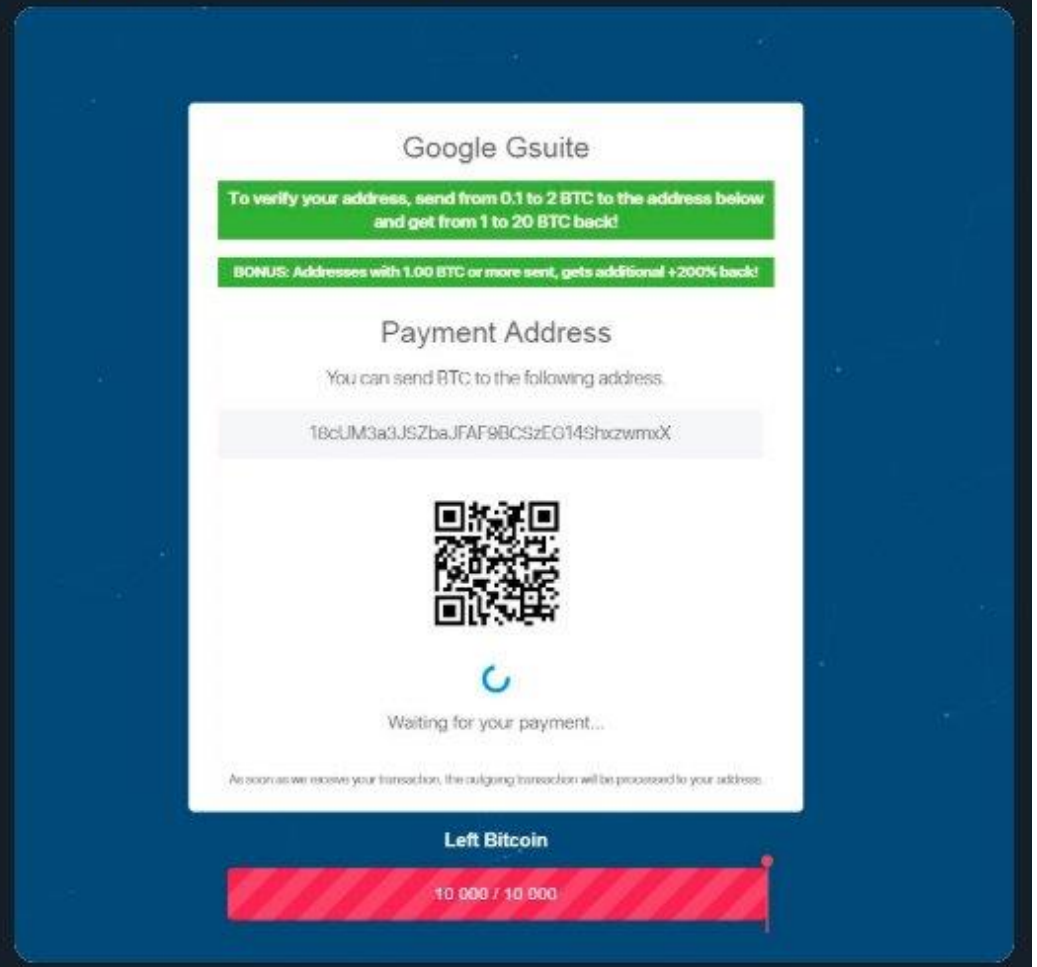
G Suite @gsuite · 20m

Google is giving 10 000 Bitcoin (BTC) to all community!

We decided to make the biggest crypto-giveaway in the world!

Now you can make payments in Gsuite using cryptocurrency!

Participate in giveaway - m-tesla.pw



25 12 27

Promoted

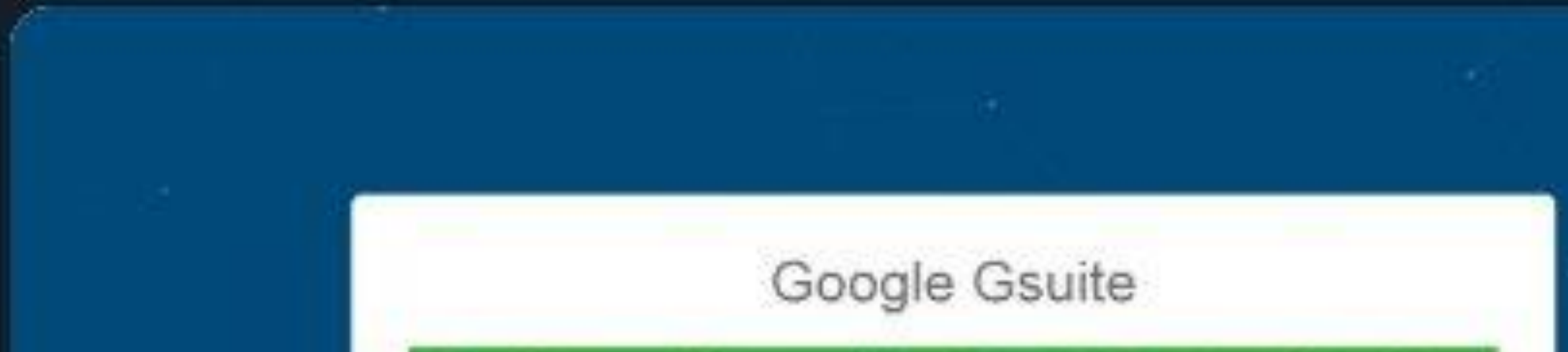
G Suite @gsuite · 20m

Google is giving 10 000 Bitcoin (BTC) to all community!

We decided to make the biggest crypto-giveaway in the world!

Now you can make payments in Gsuite using cryptocurrency!

Participate in giveaway - [redacted]



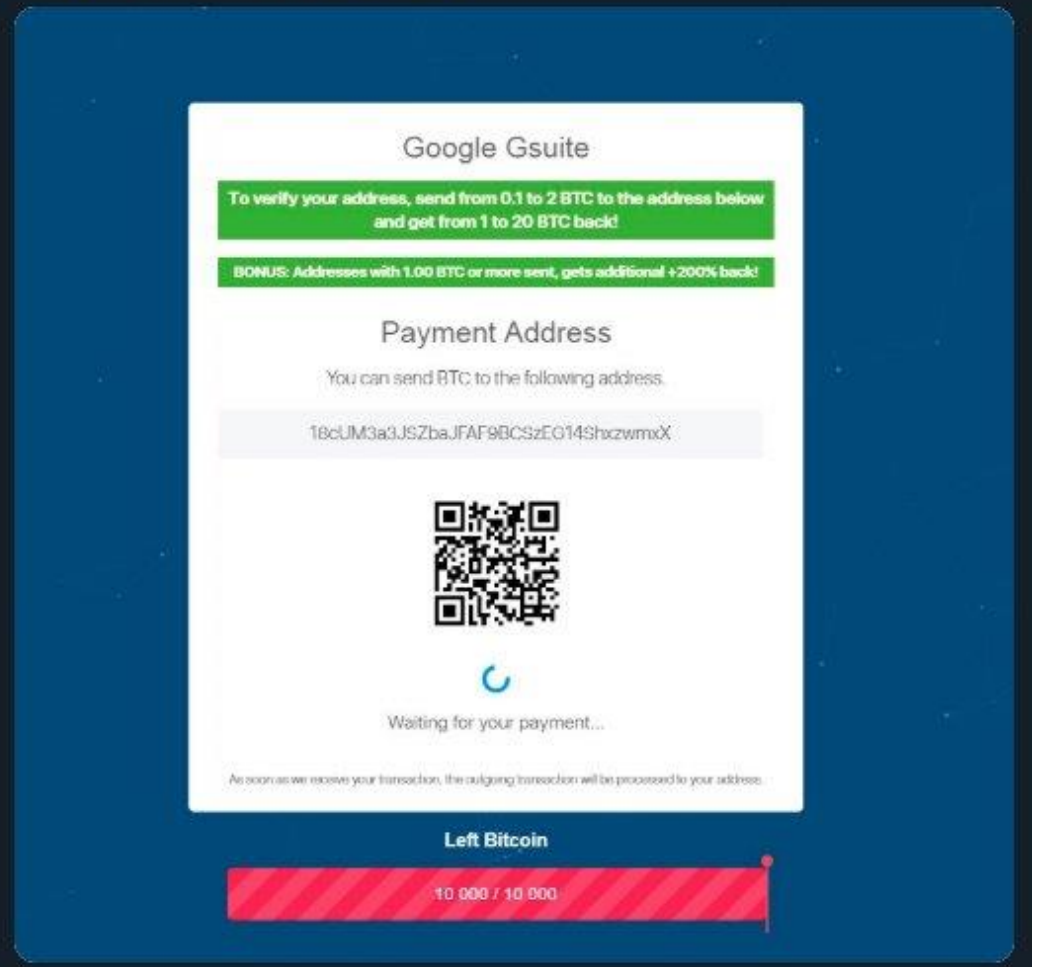
G Suite @gsuite · 20m

Google is giving 10 000 Bitcoin (BTC) to all community!

We decided to make the biggest crypto-giveaway in the world!

Now you can make payments in Gsuite using cryptocurrency!

Participate in giveaway - m-tesla.pw



25 12 27

Promoted

Left Bitcoin

10 000 / 10 000

25 12 27

Promoted

Elon Musk

To verify your address, send from 0.1 to 2 BTC to the address below and get from 1 to 20 BTC back!

BONUS: Addresses with 0.30 BTC or more sent, gets additional +200% back!

Payment Address

You can send BTC to the following address.

1KAGE12gtYVfizicQSDQmnPHYfA29bu8Da

Waiting for your payment...

As soon as we receive your transaction, the outgoing transaction will be processed to your address.

Adres Bitcoin Adresy są identyfikatorami, których używasz, aby wysłać bitcoiny do kogoś innego.

Podsumowanie	
Adres	1KAGE12gtYVfizicQSDQmnPHYfA29bu8Da
Hash 160	c732b75b9d3d75f2ed267002bec9a94324c3fc46

Transakcje		
Liczba transakcji	405	
Razem otrzymano	28.21896379 BTC	
Ostateczny stan	0 BTC	

Żądanie płatności Przycisk dotacji

Transakcje (Najpierw starsze)

Filtr

3baf77d38e8e78e7a3524d32b390af57bdf04616878b051201f11ebd908d3bd8			**2018-11-11 00:25:02**
1KAGE12gtYVfizicQSDQmnPHYfA29bu8Da	→	1HCqTD6gpAiizXiV5V3KH5NgYuPc93yKkj 37PffEpMmX3QyMWv7pXtmQ85sWbbHu5Sse	0.17708948 BTC 3.14638063 BTC
			-3.03696863 BTC
618b455dc162caeeb437fd49d3ba1e0769d0b044ea09559b8cf852c11bc65a9b			**2018-11-09 10:41:17**
1KAGE12gtYVfizicQSDQmnPHYfA29bu8Da	→	1AMbF4WQLSruw1mzCttk2RjGPxiqE5YY1S 37PffEpMmX3QyMWv7pXtmQ85sWbbHu5Sse	0.29362334 BTC 1.57330417 BTC
			-1.71814034 BTC

Transakcje

Liczba transakcji	405	
Razem otrzymano	28.21896379 BTC	
Ostateczny stan	0 BTC	

Żądanie płatności Przycisk dotacji

Home Moments Notifi

Elon Musk
@elonmusk

Joined June 2009

Elon Musk
@elonmusk

Following

That was a DM, right?

2:41 AM - 23 Feb 2018

1,954 Retweets **27,039** Likes

556 2.0K 27K

Tweet your reply

Elon Musk @elonmmusk · 7h
Replying to @elonmusk
Hint: it wasn't. And I'm giving away 5,000 Ether to commemorate the launch!

ETH Address: bit.ly/2ELCNLI

To participate, just send 0.3-2 Ether to the address above and get 3-20 Ether back to your address.

If you're late, your Ether will be sent back.

48 780 1.4K

Connor Oneal @ConnorOneal12 · 6h
I'm having a blast - sent - received - sent - received - lol!

15 484 796

Tweet

© 2018 Twitter About Help Center Terms
Privacy policy Cookies Ads info

Elon Musk @elonmmusk · 7h

Replying to @elonmusk

Hint: it wasn't. And I'm giving away 5,000 Ether to commemorate the launch!

ETH Address: bit.ly/2ELCNLI

To participate, just send 0.3-2 Ether to the address above and get 3-20 Ether back to your address.

If you're late, your Ether will be sent back.

48 780 1.4K

Connor Oneal @ConnorOneal12 · 6h

I'm having a blast - sent - received - sent - received - lol!

15 484 796

Elon Musk
@elonnmuusk

Follow

Replying to @realDonaldTrump @elonmusk and 2 others

Thank u President, i want to give away 100 ethereum to ur followers, just send 0.2 eth to the address below and u will receive 2.0 eth 0x44bd8348a45ac183c358a9b59dea0f8ba1721129

5:14 AM - 7 Feb 2018

2 Retweets **4** Likes

0x12ef06b21e5b0d...	5139134	21 secs ago	0xc0559cfa1aa4611...	IN	0x6c441ec1c3464e...	0.3 Ether	0.00042
0x313479eadf88212...	5138918	59 mins ago	0xb66204333e7f29f...	IN	0x6c441ec1c3464e...	0.59479 Ether	0.00021
0x79614c1916f9686...	5138888	1 hr 5 mins ago	0x7ed1e469fcb3ee1...	IN	0x6c441ec1c3464e...	0.44051836 Ether	0.000084
0x33e3988a890d49...	5138826	1 hr 23 mins ago	0x49462b5126c176...	IN	0x6c441ec1c3464e...	0.74666256 Ether	0.000483
0xd2736d59273e64...	5138735	1 hr 45 mins ago	0x6c441ec1c3464e...	OUT	0xd8bc7066efacdcc...	29.098206440532503 Ether	0.000483
0x33a47cdd61ed56...	5138728	1 hr 48 mins ago	0x6c441ec1c3464e...	OUT	0xd8bc7066efacdcc...	10 Ether	0.000483
0xed735eba8f31fd6...	5138717	1 hr 50 mins ago	0x6c441ec1c3464e...	OUT	0xd8bc7066efacdcc...	10 Ether	0.000483
0x2fc09f8f49a1b12...	5138712	1 hr 52 mins ago	0x6c441ec1c3464e...	OUT	0xd8bc7066efacdcc...	10 Ether	0.000483
0x7eef3f1bd308ad5...	5138703	1 hr 54 mins ago	0x6c441ec1c3464e...	OUT	0xd8bc7066efacdcc...	10 Ether	0.000483
0x01845df8bf30cf7f...	5138695	1 hr 56 mins ago	0x6c441ec1c3464e...	OUT	0xd8bc7066efacdcc...	5 Ether	0.000483
0x59fc364074b62e6...	5138574	2 hrs 27 mins ago	Poloniex Wallet	IN	0x6c441ec1c3464e...	1.99 Ether	0.0010899
0xe88dd3b8fbfa05b...	5138558	2 hrs 32 mins ago	Poloniex Wallet	IN	0x6c441ec1c3464e...	0.9 Ether	0.0010899
0x7ebe863174d4e7...	5138458	2 hrs 54 mins ago	0xa95350d70b18fa...	IN	0x6c441ec1c3464e...	0.430094642003821 Ether	0.00042
0x1f6b9040b0fdf92...	5138408	3 hrs 8 mins ago	0x5b438e1a970ac5...	IN	0x6c441ec1c3464e...	0.94369 Ether	0.00021
0x1492c7d2080733...	5138404	3 hrs 9 mins ago	0xcb1866afeecc7b8...	IN	0x6c441ec1c3464e...	0.06 Ether	0.000861
0xbea57a407e7c10...	5138387	3 hrs 12 mins ago	0x8b98258f8f81442...	IN	0x6c441ec1c3464e...	0.4 Ether	0.000483
0xf87f9a98c12703e...	5138329	3 hrs 27 mins ago	0xf646cbe3b030fb6...	IN	0x6c441ec1c3464e...	0.71647375 Ether	0.000861
0x99e278bc3bc95b...	5138309	3 hrs 31 mins ago	0x59fb67e81247a91...	IN	0x6c441ec1c3464e...	4 Ether	0.000483
0xabd335b8f5c0eb...	5138261	3 hrs 40 mins ago	Kraken_4	IN	0x6c441ec1c3464e...	0.995 Ether	0.002205
0x19eee68a26c09d...	5138223	3 hrs 48 mins ago	0xb6aac3b56ff8184...	IN	0x6c441ec1c3464e...	1 Ether	0.000735

Elon Musk: @eonmusk, @elonnmuusk, @elonmsuk

John McAfee: @officialnmcafee, @officialnmcafee

Vitalik Buterin: @VitallikButern, @VitallikButern

Warren Buffet: @WarrenBuffert

Coinbase: @coindase

CoinMarketCap: @coinmarketcap3

Elon Musk

@elonmusk

Follow

Replying to @IAmJohnMcMahon

I want to know who is running the Etherium scambots! Mad skillz …

8:54 PM - 8 Jul 2018

525 Retweets **5,817** Likes

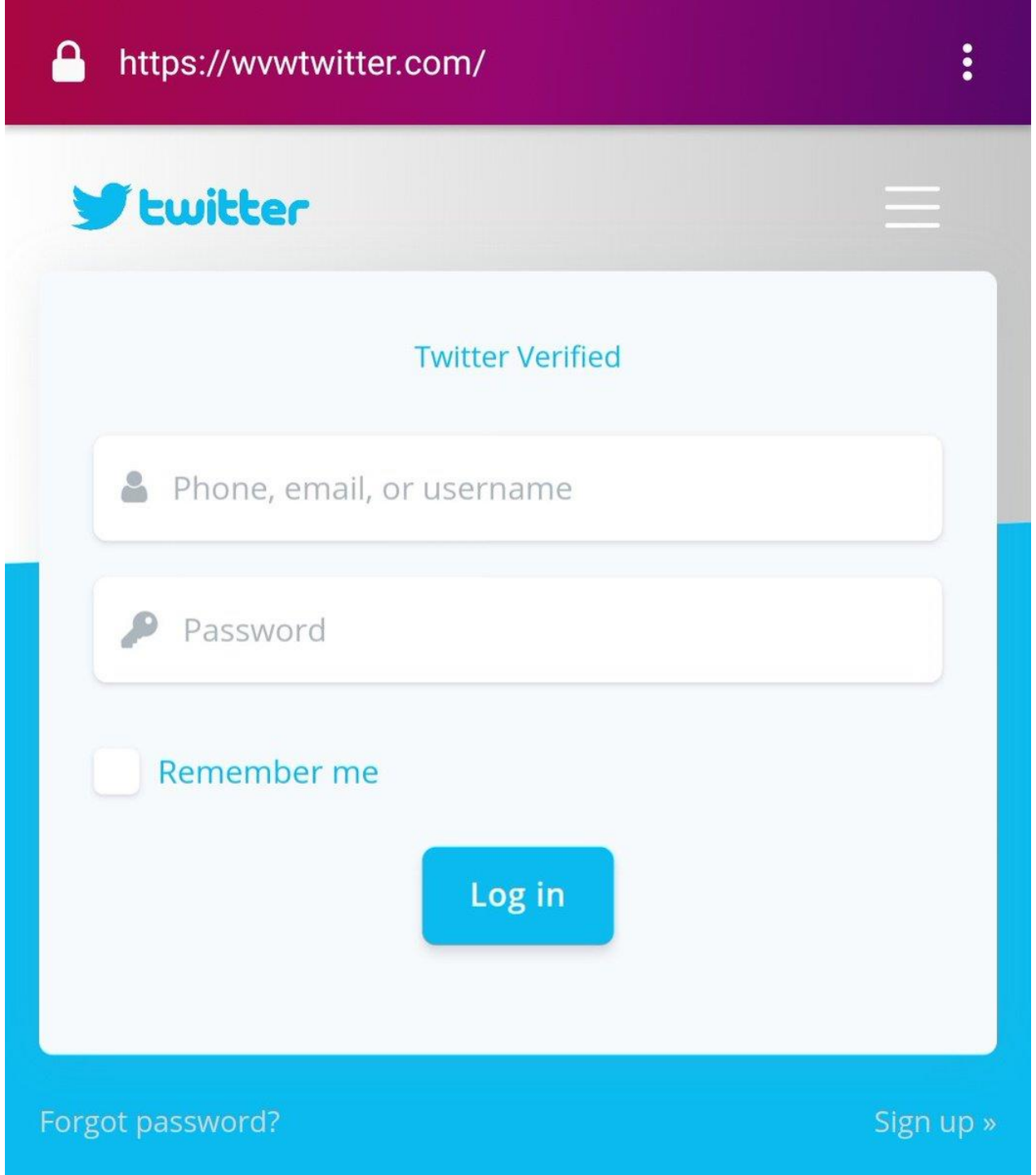
303 525 5.8K

Tweet @tweetvericfied

Simply Go to wvwtwitter.com

5 3 19

Promoted


https://wvwtwitter.com/
twitter
Twitter Verified
Phone, email, or username
Password
Remember me
Log in
Forgot password?
Sign up »