Passive Income of Cyber Criminals: Dissecting Bitcoin Multiplier Scam

medium.com/coinmonks/passive-income-of-cyber-criminals-dissecting-bitcoin-multiplier-scam-b9d2b6048372

Rakesh Krishnan January 15, 2021

Rakesh Krishnan

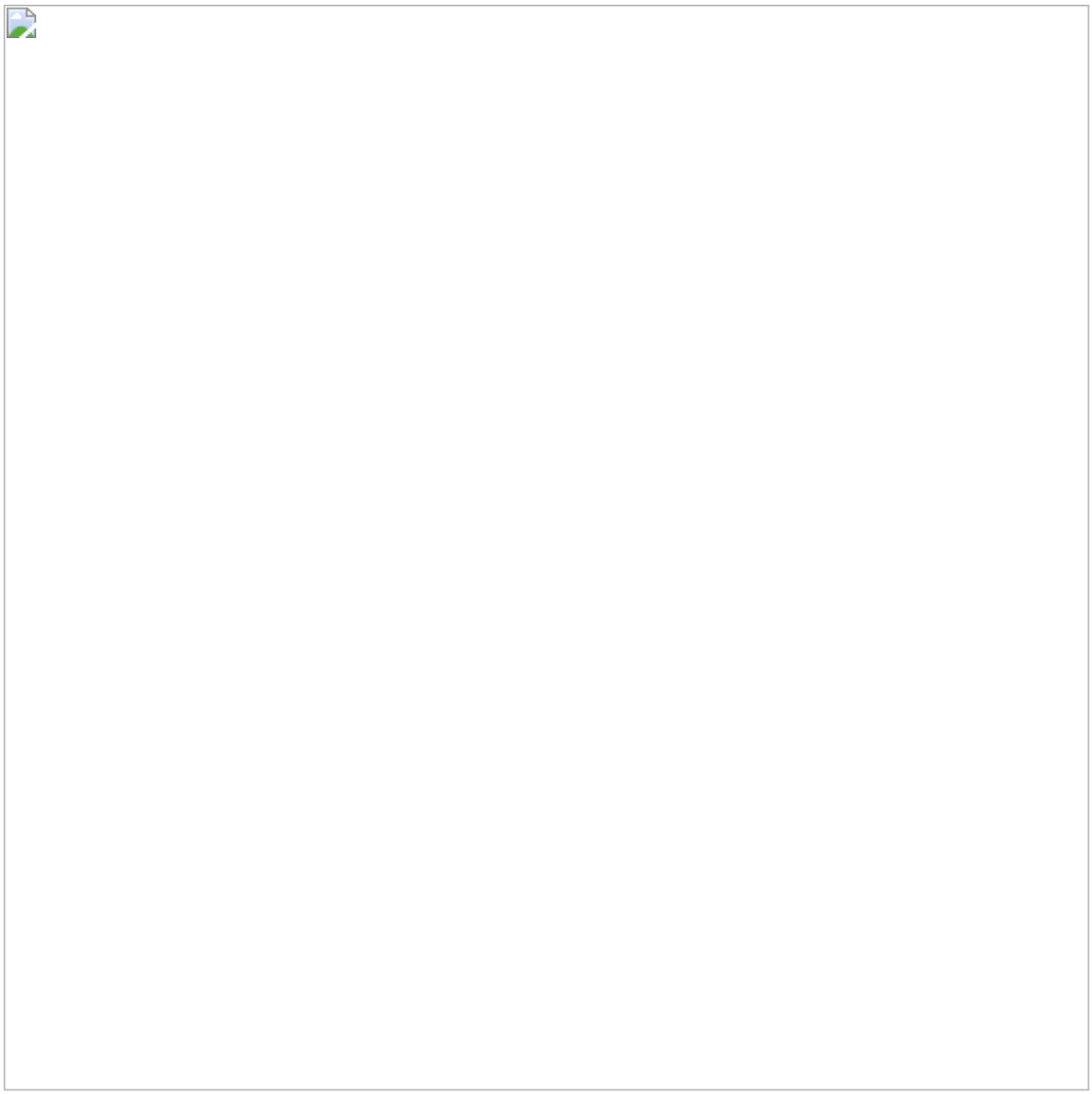
Jan 13, 2021

.

8 min read

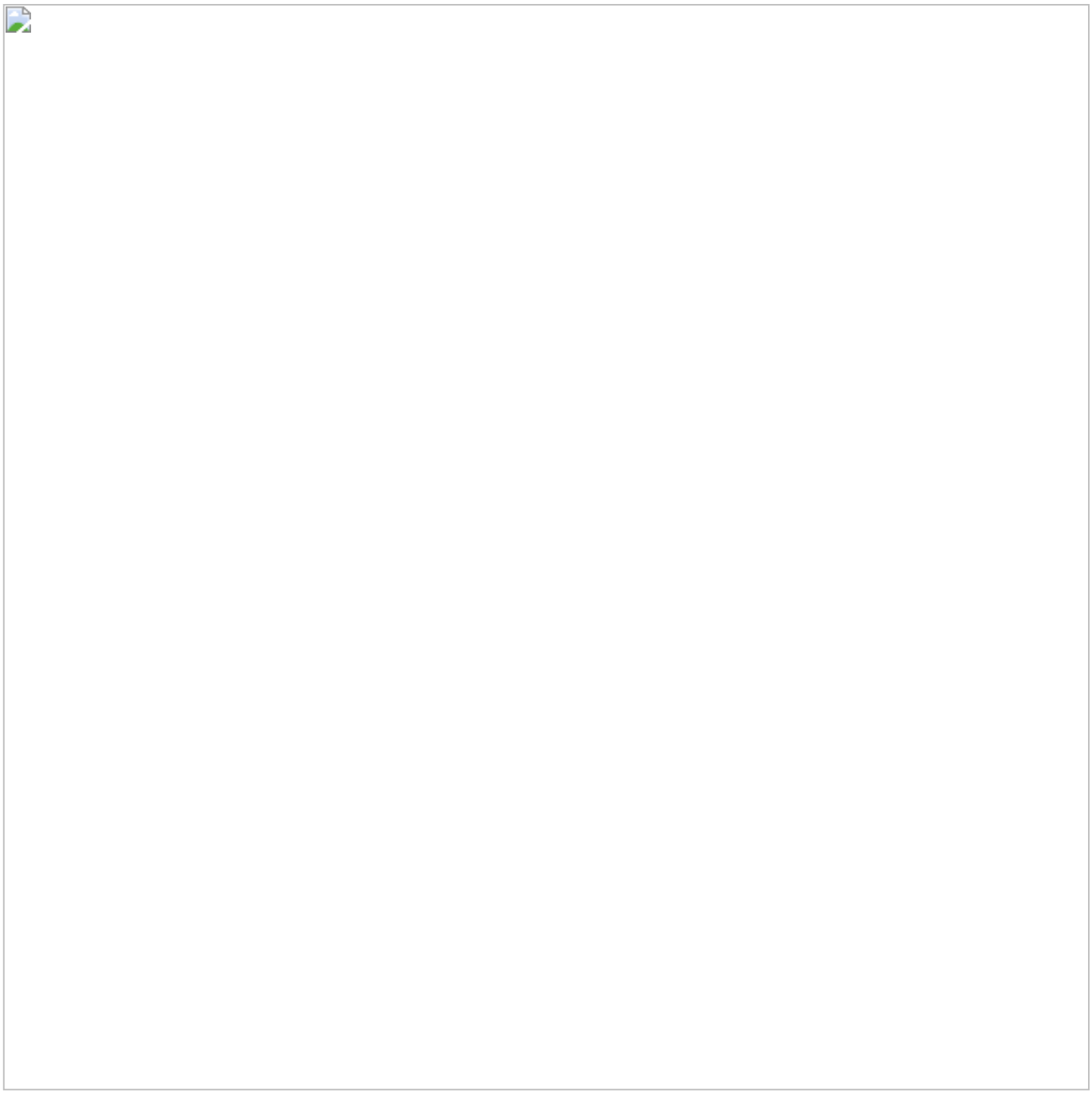
It is a common scenario to come across the various Bitcoin Scams on Dark Web while visiting various services. Some are even advertised on landing pages of popular Dark Web sites, which transports users to the luring page of Bitcoin SCAMS. Inexperienced or Less Tech-Savvy Netizens are stupefied by such posts, falling into the bait; ultimately losing money.

> It is also evident that these kinds of scams are being made operational by infamous Threat Actors such as **Dark Hotel** (Korea) to gain maximized profit to fund their Cyber Operations. One such incident pertaining to **Magniber Ransomware** (which we would be discussing at the end of this article). Hence, this paved the way for a passive income for the cyber criminals without directly infecting the intended targets.



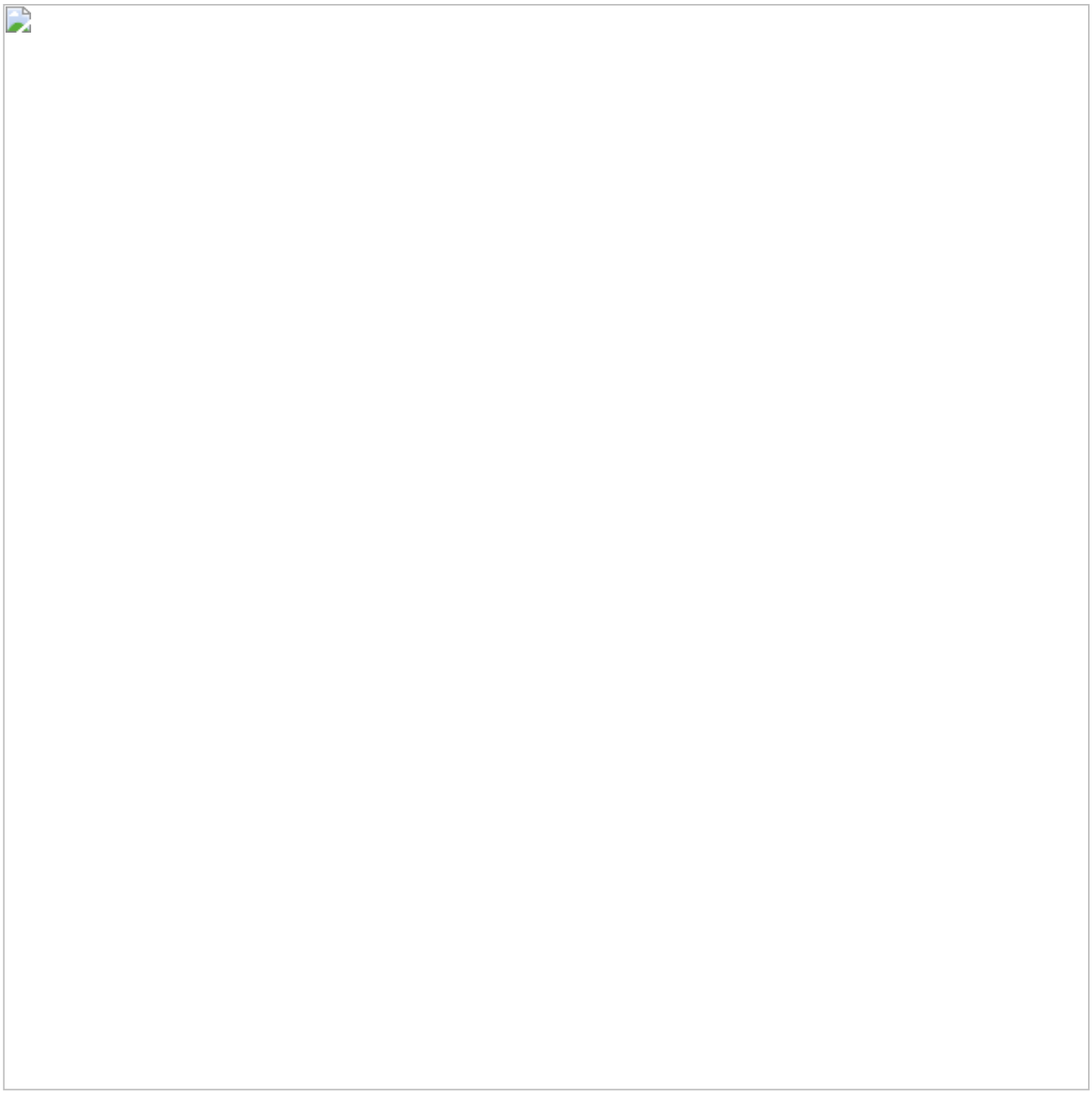
Bitcoin — The Greatest Cryptocurrency is currently witnessing an important stage in its Bull Run, surpassing the Market Value of Facebook (2 days back), to become **$760 Billion** in its Market Value. Moreover, the currency had been legalized in various countries such as the **United States, Australia, Japan, Germany, and South Korea**. It is also notable that more countries are in the pipeline of adopting Bitcoin for Economic Stability. Latin American Countries like **Venezuela (Boliver)** & **Argentina (Peso)** had already started to migrate towards Crypto-Economy, where local currency is getting devalued and spiraling down to hyperinflation.

As the adoption rate has gone astronomical, many more concepts are being added to the Crypto Economic Cultures such as Bitcoin ATMs, KYC-less Exchanges, Paper Wallet, Cold Wallets etc.



This provides a detailed view of Bitcoin ATMs installed over the world.

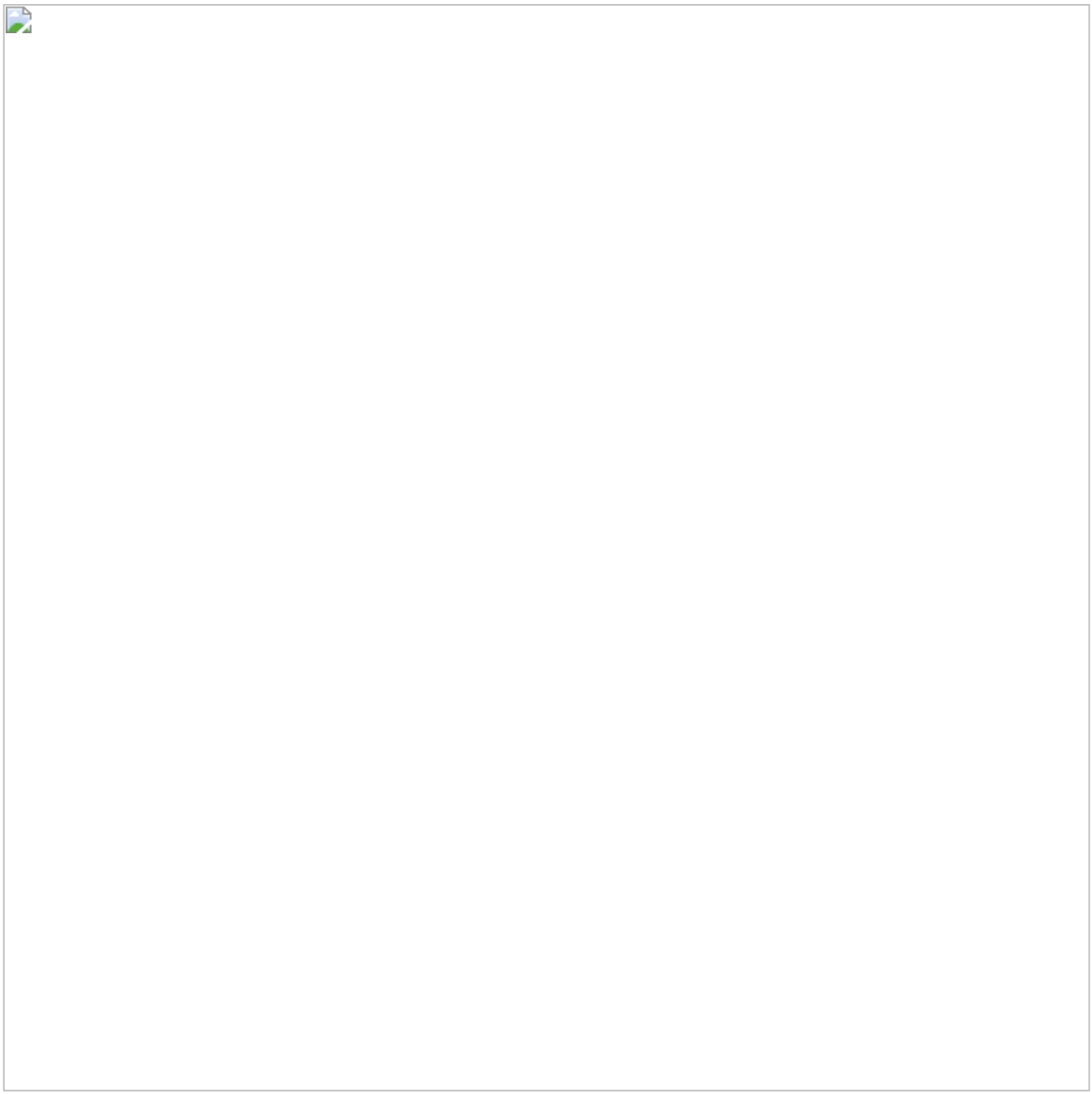
It is also remarkable that Bitcoin forks such as BCH (Bitcoin Cash) are also widely being accepted for day-to-day trading.



As adoption rate gets quadrupled, the SCAMS in this arena is also getting matured; hence defrauding many Bitcoin Enthusiasts. This article explains about 1 such SCAM which are generally known as **Bitcoin Doubling** or

What makes these SCAMS successful are various technical pointers which are implemented in the site to entice the people with partial knowledge and low-maintenance web pages etc. Let’s look into one of the use-case!

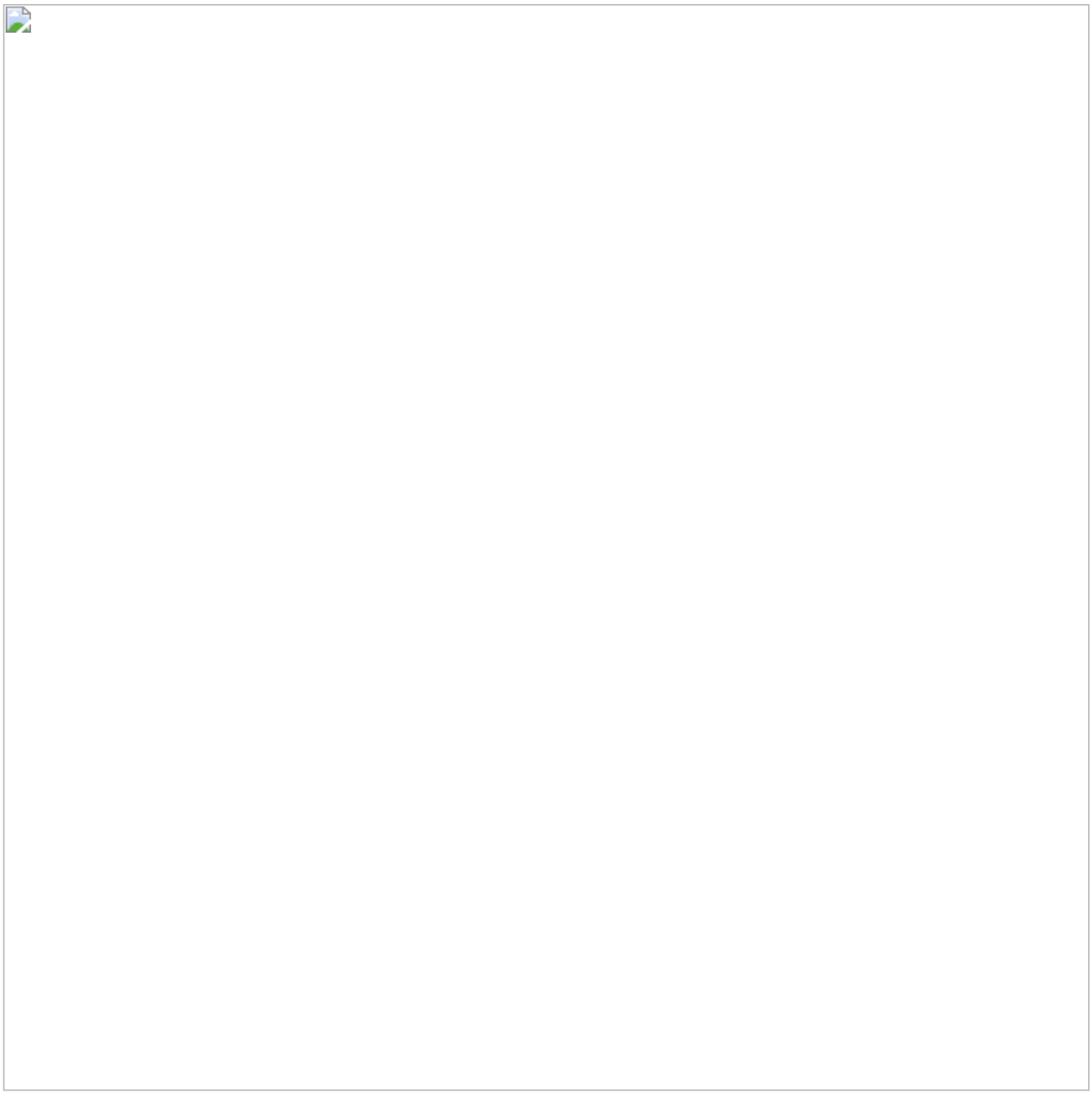
CASE STUDY — REAL TIME



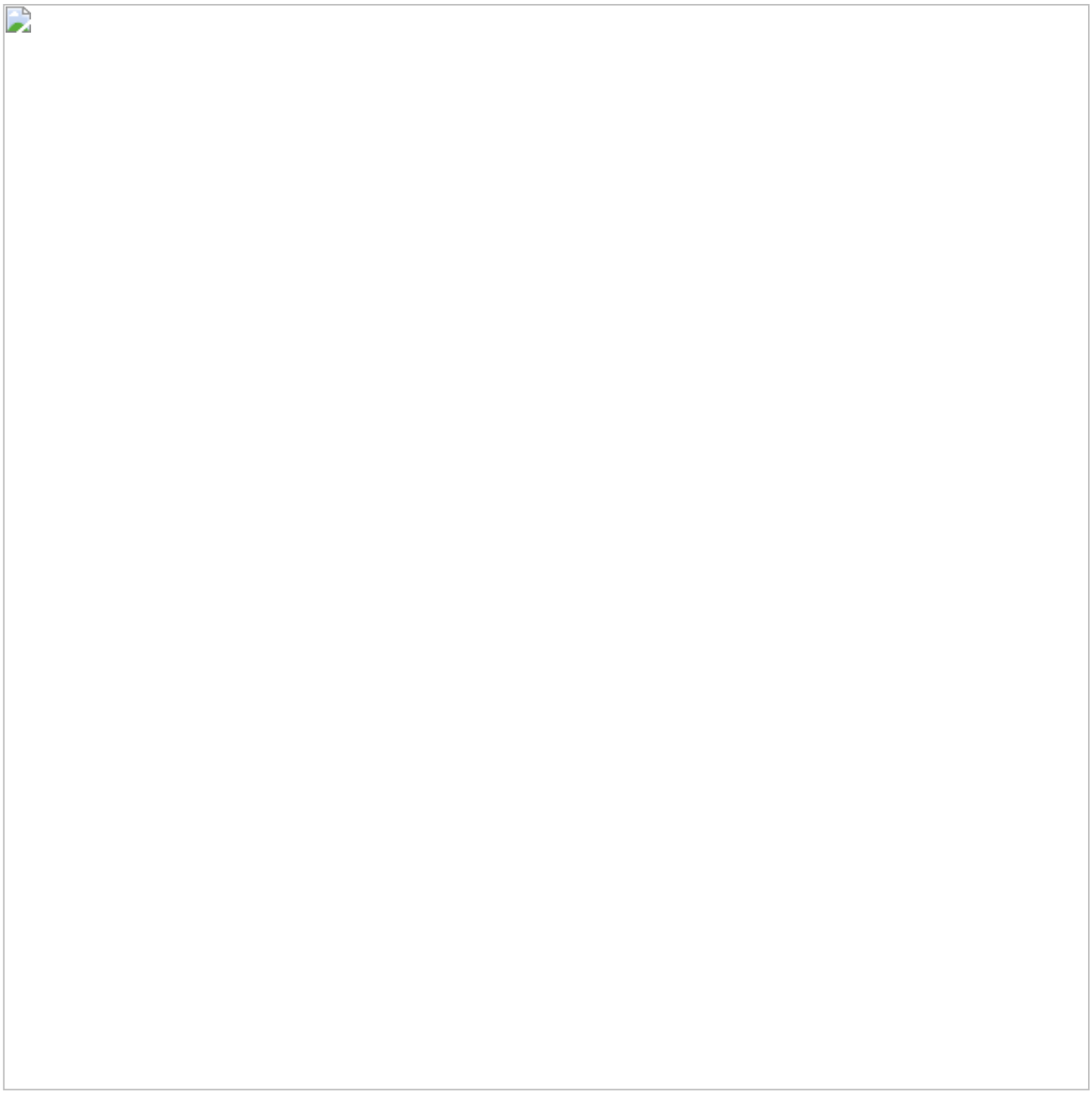
This is one of the common **Introductions** found on such Scams, that instructs the users to feed their **Bitcoin Wallet Address** and **Required Amount** by sliding the Amount Pointer to get it into your account.

There are various factors used in the Website to lure the visitors. Some of them are:-

Live Stats:- This is used as a Trust Factor for newbies. The records are probably pulled from the Live Blockchain Transaction Log, repurposing it as Live Stats to showcase the website activity.

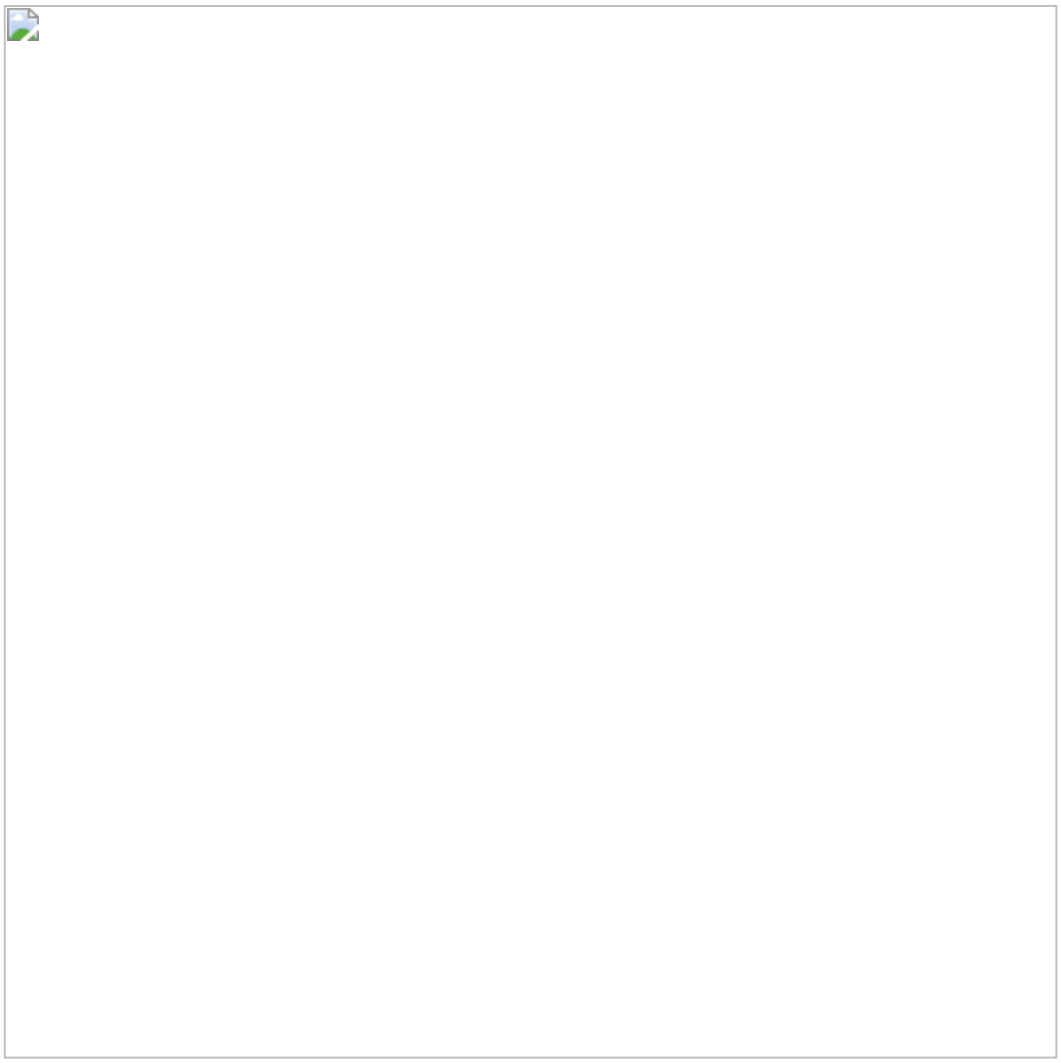


Live Chat Support:- Bragging about the profit made from the site is being dumped in this section. Another bait awaiting inexperienced users.



In order to bust this myth, let’s take a chat conversation and run a plain check:-

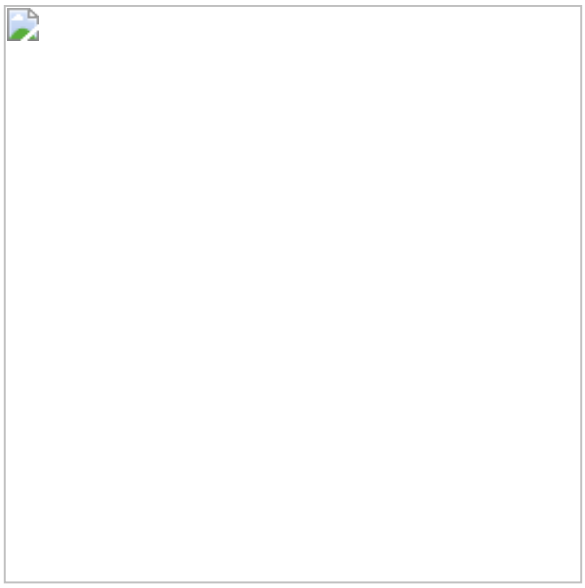
“I thought my friend wanted to fool me with this website link. but you can only get BTC here if you don't mess up with the fee confirmations”



Here, you can see similar Bitcoin Sites where the same chat log was found.

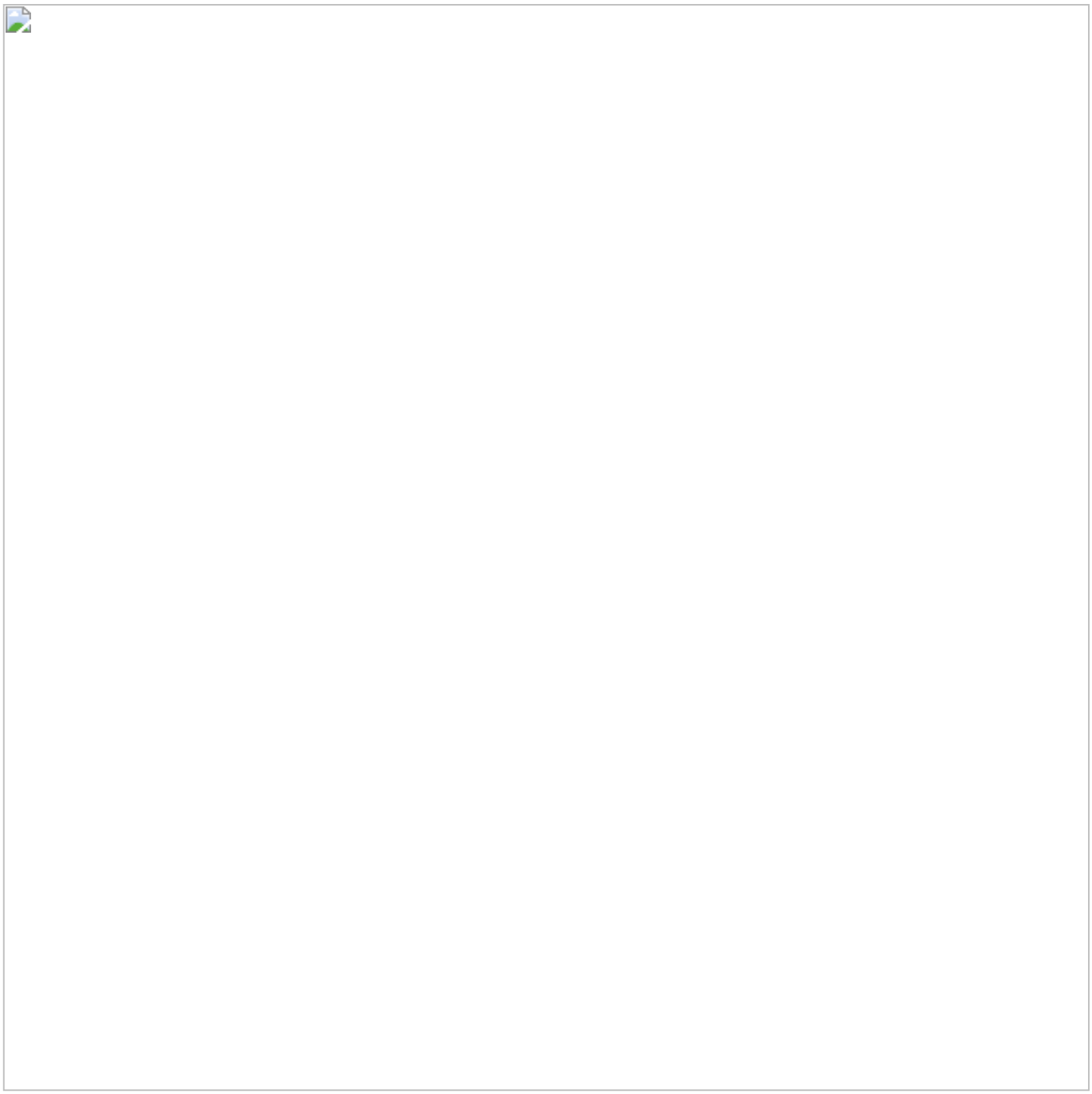
: The best part is- Chat Windows even works without Internet Connection (as my power got disrupted while drafting this), hence proving it to be hard-coded to the website (JS Files).

Receipts: These are tiny pop-ups that appear on the site alerting visitors about its high-activity, claiming to have received funds by various users.



Again, if you are running any of the username checks, you will be thrown many SCAM sites.

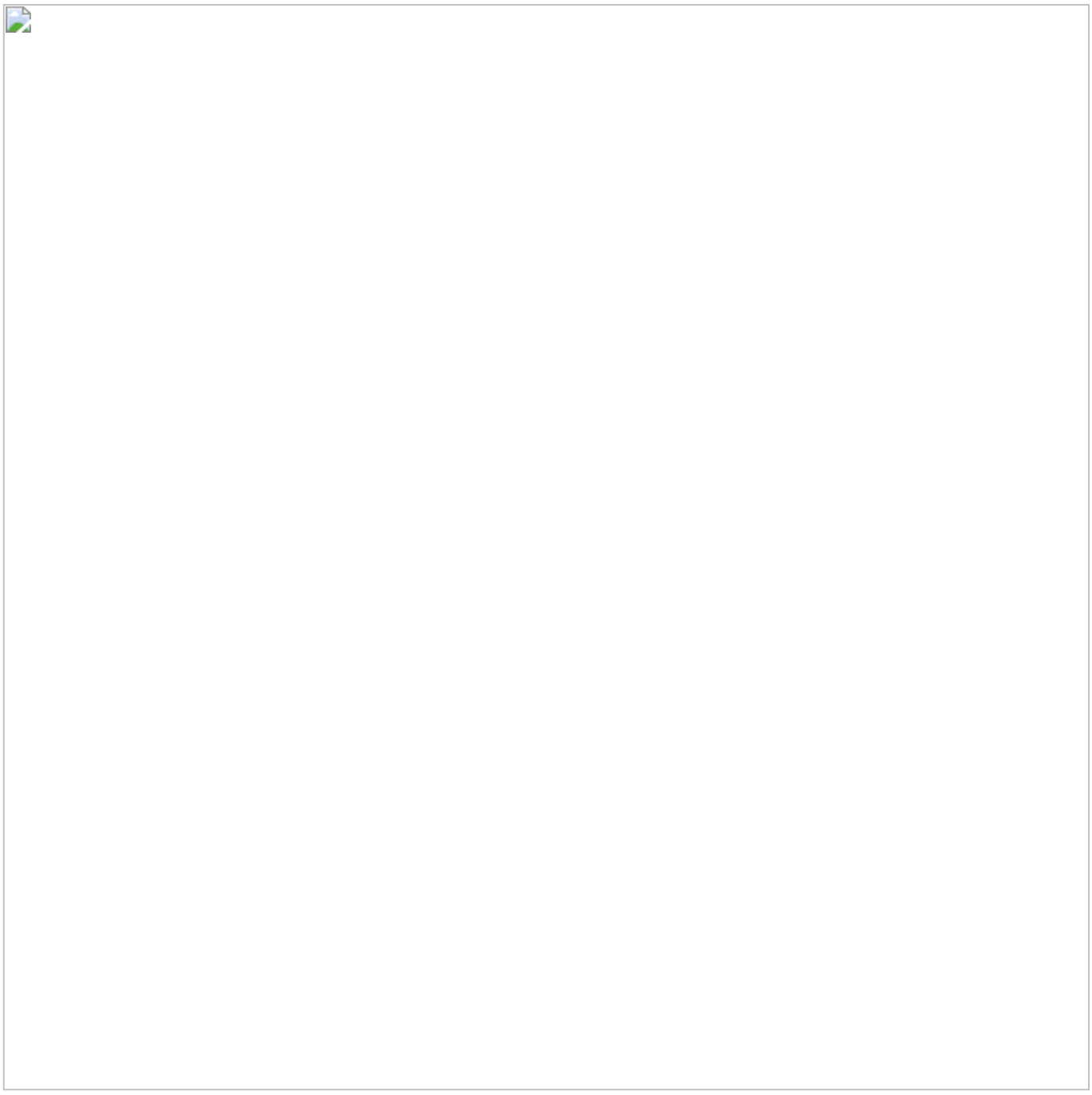
After feeding a BTC Address, it will run a loader to satisfy the eagerness of the visitors. Following Script is being shown:-



```
{ X00Percent: 2, X00Text: 'Starting `injection` process...' },  { X00Percent: 4,
X00Text: 'Connecting and Validating vulnerable BCH node...' },  { X00Percent: 8,
X00Text: 'Spoofing Packets through IPV6 Tunnel...' },  { X00Percent: 10, X00Text:
'Tunnelling via be6e:854229af:c9a::34' },  { X00Percent: 12, X00Text: 'Connecting to
Node Maintenance Channel...' },  { X00Percent: 14, X00Text: 'Establishing connection...'
},  { X00Percent: 16, X00Text: 'Connection successful on port 87118' },  { X00Percent:
18, X00Text: 'Connecting to Node Maintenance Channel...' },  { X00Percent: 18, X00Text:
'Re-spoofing Packets through IPV6 Tunnel...' },  { X00Percent: 32, X00Text: 'Extracting
data bitcoin pools -2 ' },  { X00Percent: 33, X00Text: 'Exploit uploaded... 0%' },  {
X00Percent: 38, X00Text: 'Exploit uploaded... 50%' },  { X00Percent: 42, X00Text:
'Exploit uploaded... 100%' },  { X00Percent: 59, X00Text: 'Success: Spoofing Packets
through IPV6 Tunnel.' },  { X00Percent: 60, X00Text: 'Injecting script...' },  {
X00Percent: 74, X00Text: 'Checking bitcoin pools response...' },  { X00Percent: 74,
X00Text: 'Checking BCH Nodes for Vulnerability (OK).' },  { X00Percent: 74, X00Text:
'79.83.83.61...' },  { X00Percent: 77, X00Text: 'Injecting ....' },  { X00Percent: 79,
X00Text: 'Spoof Successful(OK)' },  { X00Percent: 79, X00Text: 'Checking Again for BCH
Nodes with Vulnerability (OK).' },  { X00Percent: 82, X00Text: 'Vulnerable Node Found at
183.9.25.156' },  { X00Percent: 82, X00Text: 'Reading Blockchain Head...!' },  {
X00Percent: 84, X00Text: 'ea0d7613 f665ce14 4de1a1d5 668088c9 90eadb87\n dda97e16
5c286117 3ade0874 75c559a7 f7b71561\n 39d226e3 30ab7352 21dde7cb 6edd4bd8 b3bad704\n
cf86f763 741569bc 9bda5aaf ee650061 84ab7888\n fc204b9c 5a34d042 4bd08d6 9f0714f2
88b60c25\n bf3adeaa d6144142 e2651076 5eb13ac1 9c2b3db0\n 6b9e46c8 970266fd ca75fae
2bd2aff 31a1e836\n 85efc613 a81994c1 c1e71eb 6788e9d0' },  { X00Percent: 84, X00Text:
'Parsing...' },  { X00Percent: 84, X00Text: 'Writing to Blockchain Head' },  {
X00Percent: 84, X00Text: 'fb7fa163 3b1dcc83 94cd05c2 538ce18b ecb82a6b\n 106837e3
13ffbf3c 4e8bd365 5810def7 e2ede062\n 364e7990 1936ad63 d5a92dbf edda1463 88c0face\n
997c8d02 81efd88 3bb42b9c 1df415ec 838ef3d1\n b63f74e7 228e2427 ae50738b 2c6ae409
5a0b3e4c\n 4793a99a 4dc91ee5 15bf5af4 52fd46b8 842d9af8\n 95123cca e1f15519 72dc61da
fa3d34a9 c0ed34a1 f7009fb8' },  { X00Percent: 84, X00Text: 'Executing request!' },   {
X00Percent: 86, X00Text: 'Waiting for response...' },  { X00Percent: 92, X00Text:
'Reading Blockchain Head.' },  { X00Percent: 93, X00Text: 'Verification...' },  {
X00Percent: 94, X00Text: 'Removing exploit code from blockchain...' },  { X00Percent:
99, X00Text: 'Sending cloned Bitcoin...' },  { X00Percent: 100, X00Text: 'DONE.' },
```

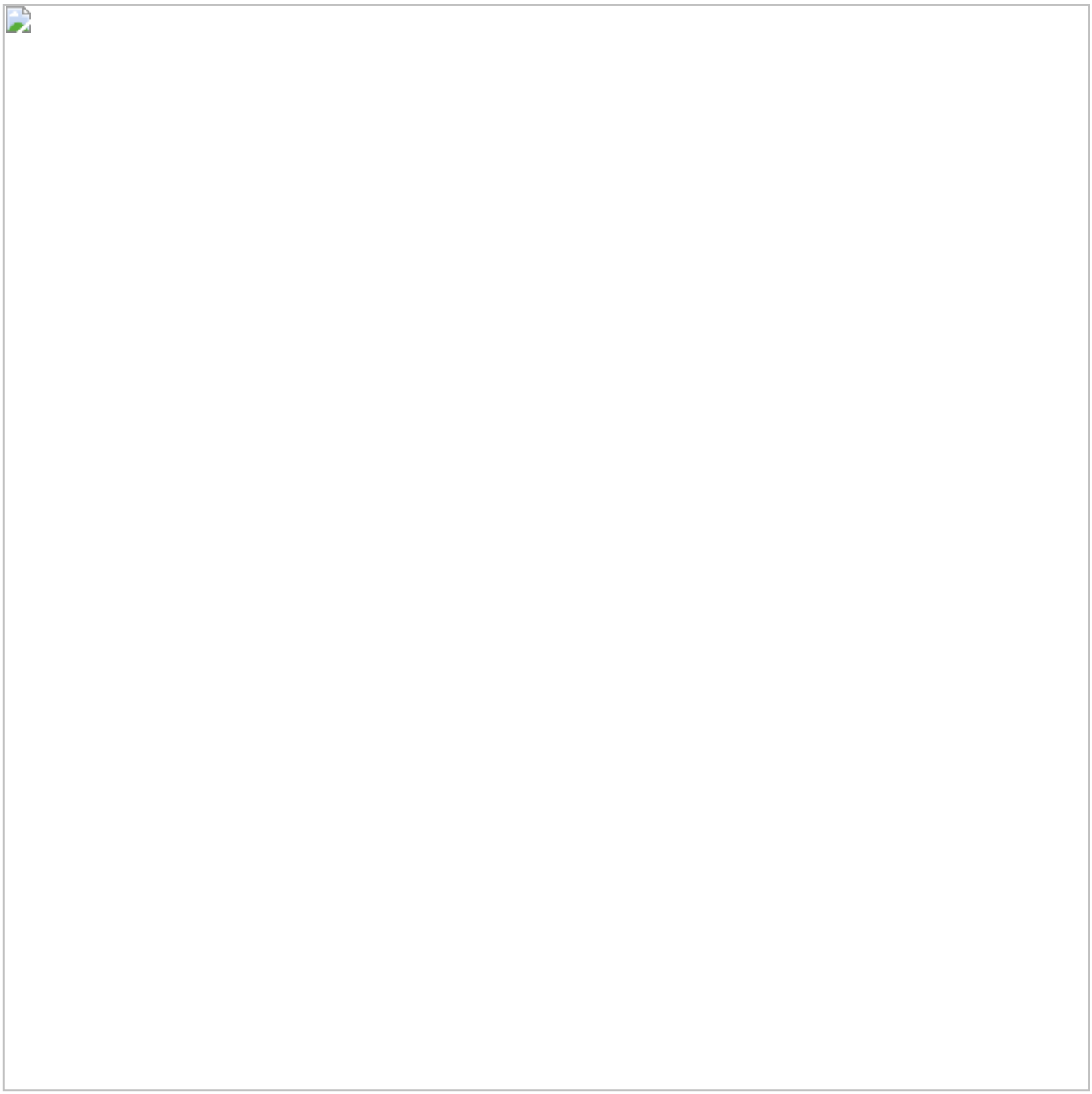
The above listed script is obtained from this , which reported earlier.

Soon after the progress, following screen would appear claiming to have completed the doubling process and funds are ready for transmission:-



Here is the ruse:- Initially you have to deposit $1,300 to Scamster's Bitcoin Address **1EFJNx1zGSgRf5u2L3oyCQunwa8Xro6ihb** receive $3,500 to the user.

By mapping the address, we came to know that this address is active since 4 months and successfully received a sum of ~$310.

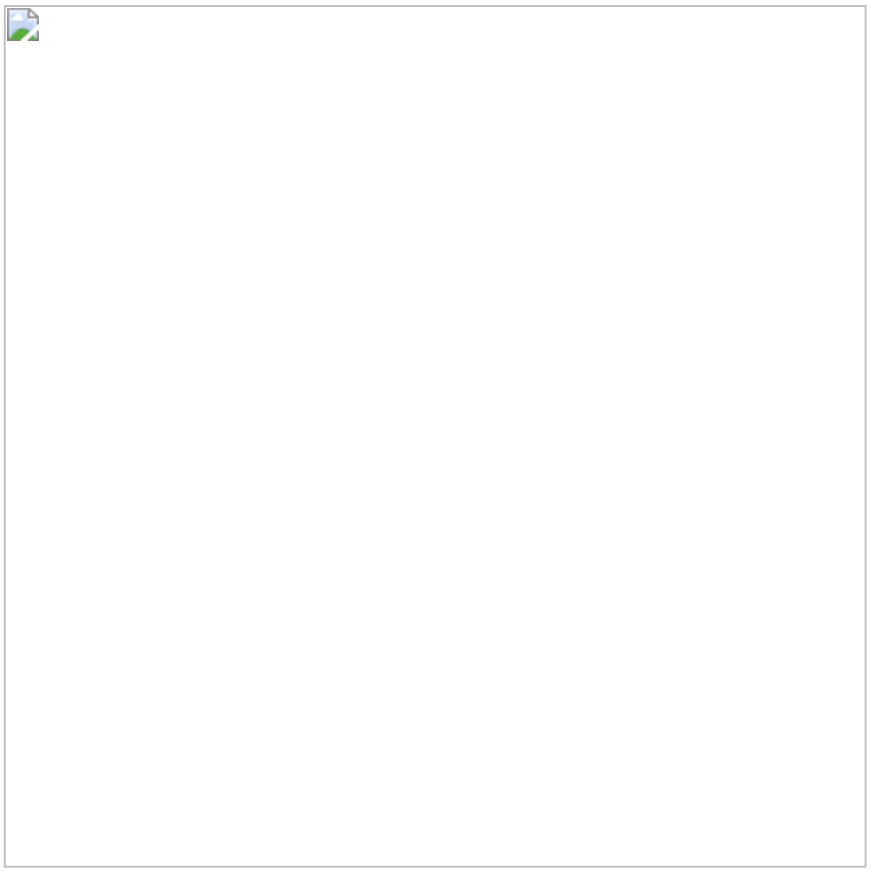


:- As BTC is fluctuating, the amount gets varied. It also depends upon the fees calculated in the Scam site.

This is one of the site that still exists on Dark Web with high activity and it is evident that the last receipt was received a month back (Acc. to Blockchain), proving the scam is not obsolete.

If you think this amount is minuscule, here is another that made around $3,705,769.52 in a span of 7 years (Still goes unflagged), hosted with Hetzner (159.69.62.95) with this Wallet Address: *1F7rkmXCouKbCuXF4DbpCwug9xBcsVvnQ5.*

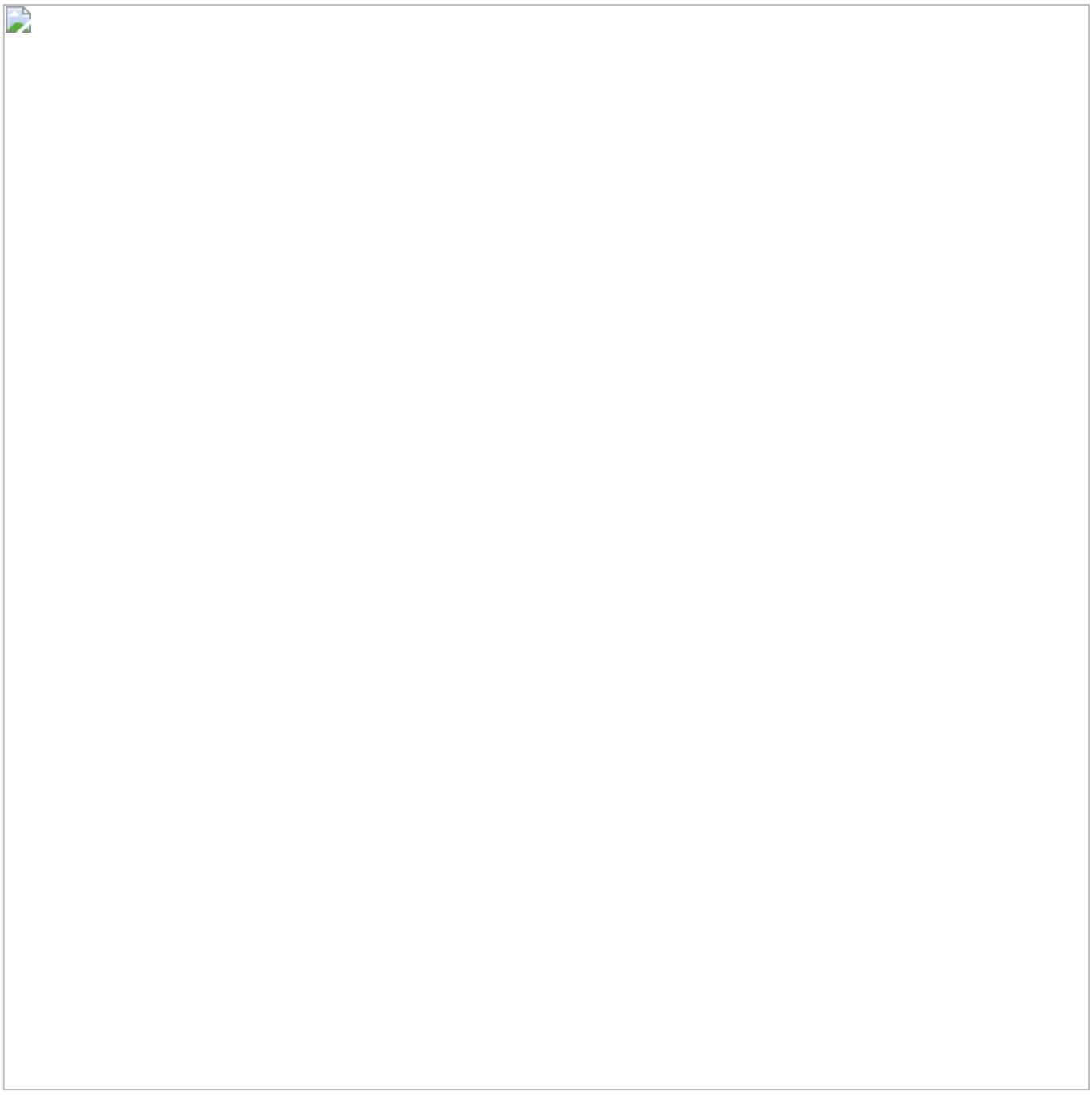
While digging deep, a profile got popped up from Bitcoin Talk Forum named **Giaky** from Italy, whose Wallet Address was mapped to.



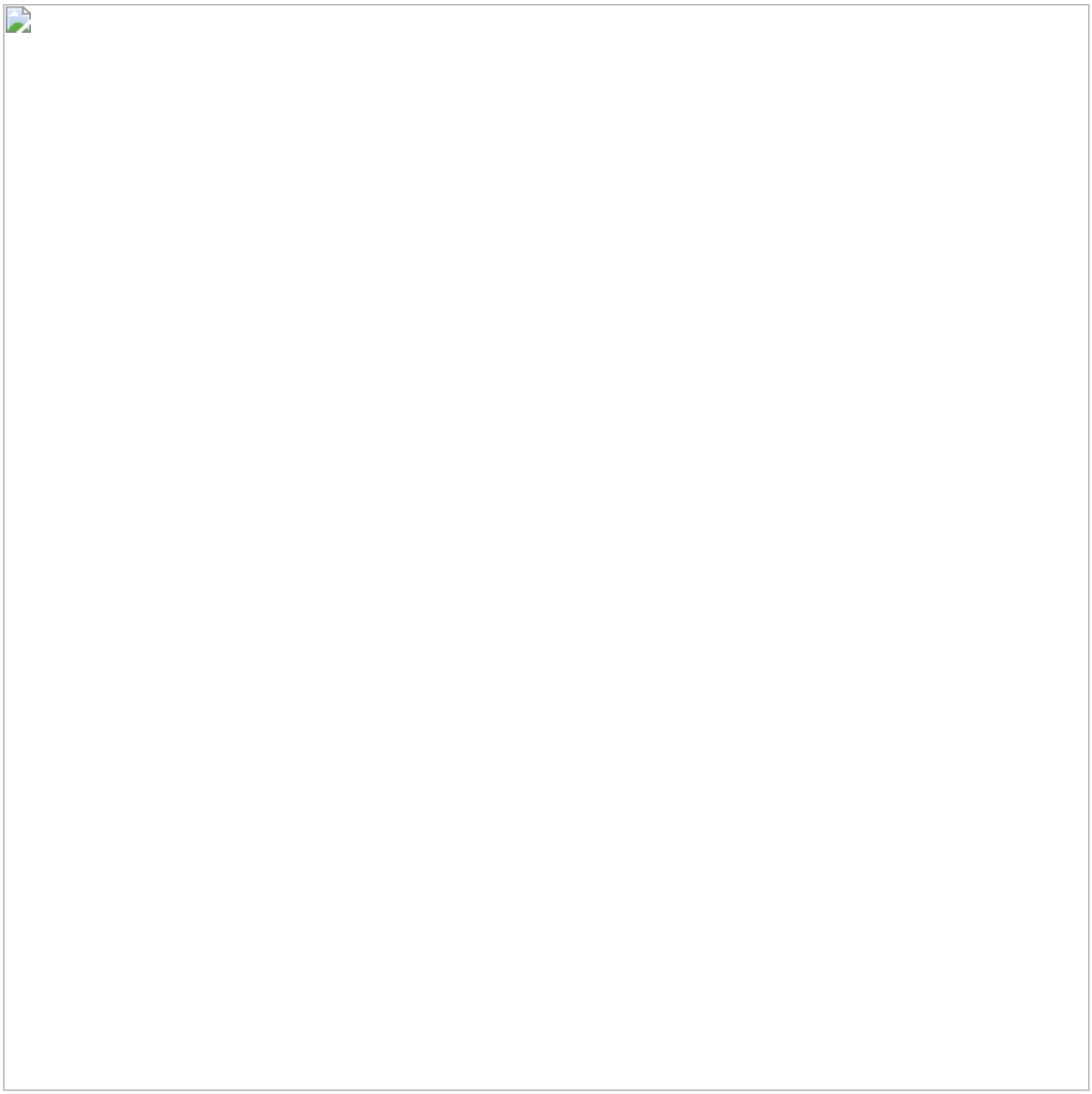
Note: *There is no 100% surety whether the alleged Bitcoin Address belongs to the alleged user, as the data obtained from a Bitcoin Blacklist Comment.*

Similarly, there are a multitude of SCAM Campaign Websites are still operational on both Dark Web and Surface Web, reaping a high cash flow to Scamster's account.

Following are some of the details with reaped profits:-



These are some of the notable websites (that I come across) which are targeting Bitcoin Doubling fanatics. It is also found that there are a large number of mirror sites for the same onion such as:-



According to this Search Engine, there are in-total of **331 Websites** (including Mirrors) exclusively with “BITCOIN DOUBLING” content in it, on Dark Web. Of course, there are more, but not everything can be indexed by a single entity.

Note: This article covers Dark Web Aspect in more detail rather than Surface Web.

MAGNITUDE EK LINKED WITH BITCOIN MULTIPLIER IN THE PAST

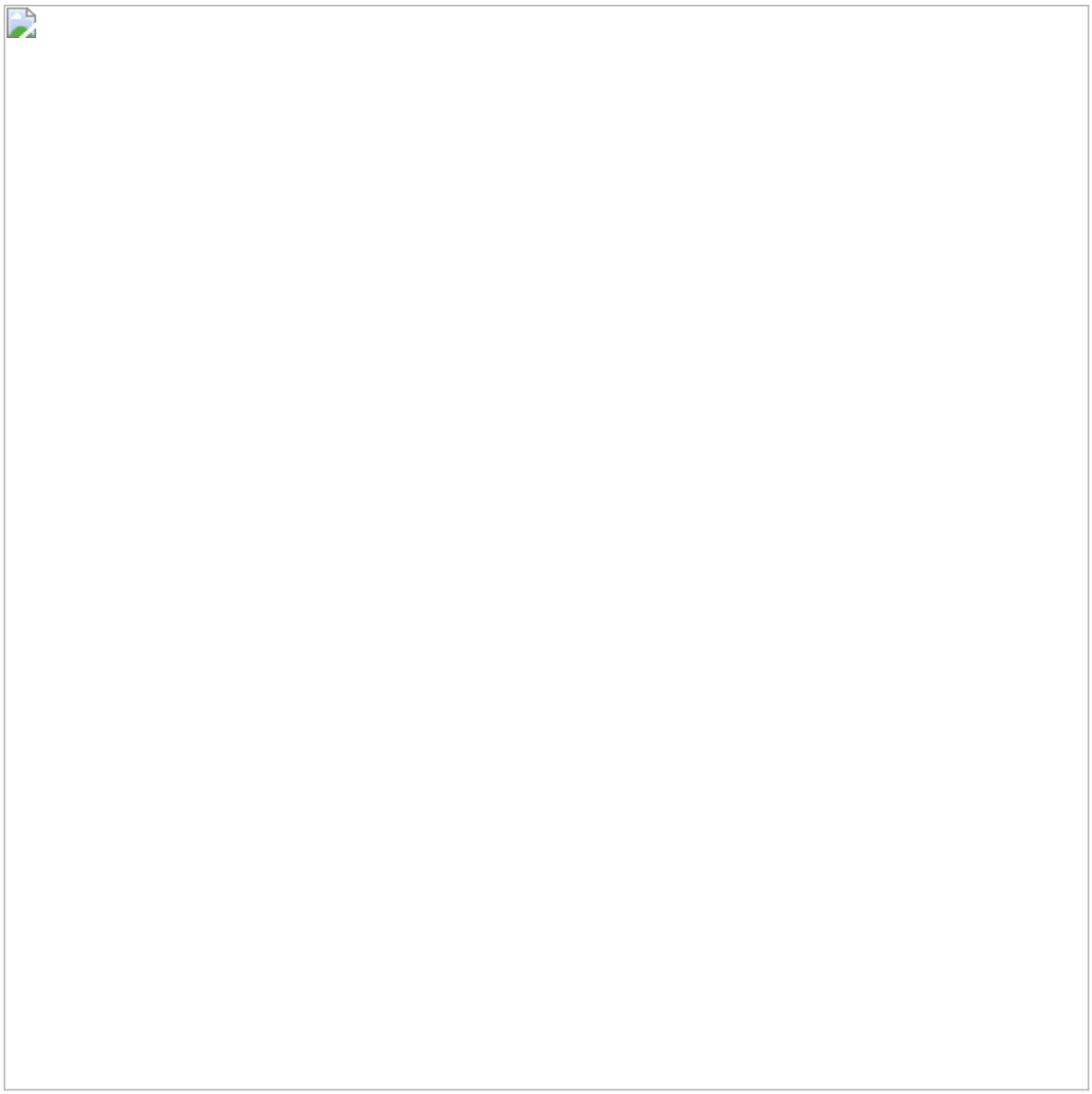
Magnitude is one of the most successful Exploit Kit prevalent on various underground forums over the years. It delivers **Magniber Ransomware** upon infection, affecting APAC Region. The Group (**attributed to infamous South Korean Group DarkHotel**) works by keeping up-to-date

with the recently uncovered security loopholes (CVEs) targeting the intended parties. It is a surprising fact that the **group had also operated various Malwertisements and Bitcoin Scam Websites** as per Malware Bytes Report.

It is evident that the Cyber Criminal Groups are using this means as a passive income in order to fund their cyber attack operations.

KEY TAKEAWAYS

- Never ever fall for the Doubling/Multiplier or any sorts of Scams
- Cyber Criminals can set up such SCAM sites on a large scale, in order to raise large amount without directly infecting anyone with Ransomware
- This is also a form of Passive Income for Cyber Criminals or a long term investment policy without any red flags
- Always check for the Website Reputation before engulfing all the displayed promises
- Check for the Blacklist activities of Bitcoin Address listed on various platforms like BitcoinWhosWho or Bitcoin Abuse
- Be a responsible infosec contributor by flagging malicious Bitcoin Addresses to the said platforms



: Foxman Communications
Follow me on Twitter for interesting DarkWeb/InfoSec Short findings! ;-)

Note:-