

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/17/2011

To: Cyber

Attn: SSA [redacted]
CCU-1

b6
b7C

From: New York

CY-02

Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 288A-NY-306786 (Pending) - 1

Title: UNSUB(S);
[redacted] VICTIM;
COMPUTER INTRUSION;
OO:NY

Synopsis: [redacted]

b7E

Details: On August 1, 2011, [redacted] telephone number [redacted] date of birth [redacted] filed a complaint with the FBI New York Office. Subsequently, on August 11, 2011, writer and SA [redacted] telephonically interviewed [redacted] in regard to his initial complaint. Furthermore, [redacted] and his partner came to 26 Federal Plaza on August 16, 2011 to explain his complaint in detail to writer, SA [redacted] and SA [redacted].

b6
b7C

[redacted] is self-employed and maintains and operates [redacted]

[redacted] has held an account with <http://mybitcoin.com> (MYBITCOIN). MYBITCOIN is an online depository of BTC. MYBITCOIN has been in business since middle of 2009 and it is one of the first to offer such service. MYBITCOIN had thousands of users and their wallets that may contain up to millions of dollars in BTCs.

On July 29, 2011, MYBITCOIN's website went offline. Every account at MYBITCOIN was inaccessible, virtually leaving all of its users without any of their stored BTCs. [redacted] lost [redacted] using the exchange rate around the time of the incident, as a result of this event.

MYBITCOIN did eventually come back online after approximately 7 days. During this time there was an inquiry/investigation driven by the online BTC community against owner(s) of MYBITCOIN. When MYBITCOIN came back online, it announced that their servers were compromised by hackers and a certain percentage of BTCs were stolen. However, MYBITCOIN stated that some of the BTCs were recovered and offered a claim process that allowed for its users to settle their losses by MYBITCOIN reimbursing 49% of their last known stored value.

UNCLASSIFIED

UNCLASSIFIED

To: New York From: New York
Re: 288A-NY-NEW, 08/17/2011

Writer requests that caption case be opened and assigned to SA [redacted] add SA [redacted] and [redacted] as co-case agents. The captioned case is being handled by the United States Attorney's Office in the Southern District of New York. AUSA [redacted] is assigned to the case.

b6
b7c

Background on Bitcoins (BTC)

BTC is an open source project published by Satoshi Nakamoto in 2008. BTC is a decentralized, peer-to-peer, virtual currency. The value of BTC is represented by a public/private keypair. Public keys serve as a address or a wallet of BTC users and it is shared between parties involved in a BTC transaction. Private keys are secured by the owner of a BTC and it is used as proof of ownership and authorization to transfer a certain BTC to another party. This keypair structure, along with decentralized organization provides a level of anonymity since there are no registered accounts in existence.

All transactions that occur in the BTC system are broadcasted to as many computers within the BTC system as possible. This block chain is collectively maintained and extended as valid transactions are added on to the block. The block chain contains all transaction history and can not be altered. In order to corrupt the block chain, one will need to overpower the aggregate computing power of the BTC system.

The first 50 BTC were generated in January of 2009. BTC are generated by calculating a target matching cryptographical hashes, also known as a block. This mathematical problem is controlled by a set of rules that are agreed upon by computers participating in the BTC system. The difficulty of calculating the target hashes are precisely known and adjusted to be solved at an average of every 10 minutes.

Users correctly calculating the target hash are rewarded with a set amount of BTCs. Currently, each "mined" block pays out 50 BTC. The pay out amount will be halved every 4 years from beginning of BTC system's existence. The amount of BTC that can be in circulation is predetermined. The maximum number of BTC in circulation will approach limit of 21 million, while never reaching 21 million. The smallest denomination of BTC is 0.00000001. In 2140, all of the available BTC will be in circulation with 6,929,999 hash blocks being solved, having mined a total of 20,999,999.999999999 BTC. Currently, there are over 7 million BTC in circulation, which is 1/3 of BTC that can be in circulation.

Other than mining for BTCs. Users can obtain BTC by purchasing it from anyone that is willing to barter. There are money exchangers, ranging from a organized business entities to a private individuals, that convert hard currency to BTC and vice versa. BTC is valued by scarcity of BTC in circulation, driven by supply and demand. A fair exchange rate for BTC can be obtained by observing major exchangers, i.e. Mt. Gox. Mt. Gox is a website that facilitates BTC to money exchanges between its registered users. Mt. Gox does not appear to provide money exchange service itself but rather play as a match maker between its users.

BTC is stored on the computer running a BTC client, within the public key representing the wallet. Since BTC is virtual and stored as if it was a computer file, BTC is susceptible to corruption, damage and compromise on its host computer. There are online businesses that provide escrow service, like an online piggy bank that serve as a protected repository of BTC. BTC user may open an account with an online wallet service who then can provide better security of BTC wallets to include data backups, accidental deletion prevention and remote accessibility. BTC users are left to blindly trust the integrity and security of such service provider.

UNCLASSIFIED

UNCLASSIFIED

To: New York From: New York
Re: 288A-NY-NEW, 08/17/2011

LEAD(s):

Set Lead 1: (Action)

CYBER

AT WASHINGTON D.C.

Read and clear.

◆ ◆

UNCLASSIFIED

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/18/2011

To: New York

Attn: FMU

From: New York

CY-02

Contact: [Redacted]

Approved By:

[Redacted]

Drafted By:

[Redacted]

Case ID #: 288A-NY-306786 (Pending) - 2

Title:

UNSUB(S);

[Redacted] - VICTIM;
COMPUTER INTRUSION;
OO:NY

Synopsis: Funds requested for the registration fee to a conference.

Details: FBI New York is currently working a matter involving a new form of electronic currency, Bitcoin (BTC). The captioned case has many Bitcoin users who lost majority of their BTCs in savings due to a compromised server.

BTC is a decentralized, virtual, peer-to-peer currency that has been around since 2009. Due to its online nature, the systems participating in BTC network is susceptible to and a target of online hacking, viruses and other Internet vulnerabilities. In addition, BTC's relatively infant state leaves many potential problems, to include misuse and abuse, yet to be discovered.

From August 19, 2011 to August 21, 2011, Bitcoin Conference and World Expo 2011 NYC is being held in New York, New York. This a first global conference for the BTC community. Many major service, product providers for BTC, media outlets and investors are expected among the guest and participants. The conference agenda includes talks and sessions to educate and discuss current issues relating to BTC. Writer requests \$52.00 to pay for admission fee to attend the conference for two agents. The money will be exchanged to BTC to pay for the conference.

| | | | |
|---------------------------|------------|-------|------|
| Current authorization | [Redacted] | | |
| Registration fee \$26 x 2 | \$ | 52.00 | |
| Tax | | \$ | 0.00 |
| Total amount | \$ | 52.00 | |
| Balance after payment | [Redacted] | | |

b6
b7c

b7E

UNCLASSIFIED

UNCLASSIFIED

To: ?? From: New York
Re: 288A-NY-, 08/18/2011

◆◆

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 09/16/2011

To: New York

From: New York
CY-02

Contact: [Redacted]

b6
b7C

Approved By: [Redacted]

Drafted By: [Redacted]

Case ID #: 288A-NY-306786 (Pending) -4
188B-NY-266547-C (Pending)

Title: VICTIM NOTIFICATION FORM

Synopsis: Computer Intrusion


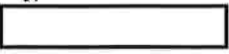
Reference: 288A-NY-306786 Serial 1

Details:

VnsCase#: 288A-NY-306786
CAgtName: [Redacted]
PContact: Person
BusName :
BusEIN :
BusAcct :
VicFirN : [Redacted]
VicMidN :
VicLastN: [Redacted]
SSAN :
VicDate : 20110729
VicDOD :
VicMinor: N
DOB : [Redacted]
Race : W
Sex : M
Addr : [Redacted]
Addr2 :
City :
State :
Country :
Zip :
Email :
HPhone :

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Fax :
VWrkAddr: 
VWrkadd2:
VWrkCity:
VWrkSt :
VWrkCtry:
VWrkZip :
WEmail :
WPhone :
WFax :
VicPager:
NOKFirN :
NOKMidN :
NOKLastN:
NOKRel :
NOKAddr :
NOKAddr2:
NOKCity :
NOKState:
NOKCtry :
NOKZip :
NOKHEmal:
NOKWEmal:
NOKHPho :
NOKWPho :
NOKHFax :
NOKWFax :
NOKPager:
GrdFirN :
GrdMidN :
GrdLastN:
GrdRel :
GrdAddr :
GrdAddr2:
GrdCity :
GrdState:
GrdCtry :
GrdZip :
GrdHEmal:
GrdWEmal:
GrdHPho :
GrdWPho :
GrdHFax :
GrdWFax :
GrdPager:
PropRet : N
TotLoss : 
Lang. :
Disable :

b6
b7C

b6
b7C

To: New York From: New York
Re: 288A-NY-306786, 09/16/2011

◆◆

Document Details

Classification: SN

Case ID: 288A-NY-306786

Serial Number: 000005

Topic: FBI POLICE COMPLAINT INFORMATION

Originating Office: NY

Responses: 0

Document Date: 08/01/2011

Document Type: OTHER

To: NEW YORK

From: NEW YORK

Document Text

FEDERAL BUREAU OF INVESTIGATION

Date of

transcription

Investigation on
File #

at

Date dictated

by

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to

your agency;

it and its contents are not to be distributed outside your agency.

02/10/2012

[redacted] date of birth [redacted]
[redacted] telephone number
[redacted] was interviewed telephonically. After being advised of the identity of the interviewing agent and the
nature of the interview [redacted] provided the following information:

b6
b7C

[redacted]
[redacted]
[redacted] BITCOIN is an online currency that
is secured by a cryptography.

[redacted] uses MYBITCOIN.COM to store his BITCOINS.
MYBITCOIN.COM is one of the oldest websites for providing an online
storage of BITCOINS via electronic wallet or electronic bank function.
MYBITCOIN.COM has over hundreds of thousands of account holders.
[redacted] account alone is worth approximately [redacted] USD. [redacted]
has about [redacted] BITCOINS.

b6
b7C

On July 28, 2011, MYBITCOIN.COM stopped allowing withdrawals,
however, deposit were allowed. On July 29, 2011, MYBITCOIN.COM servers
when offline. The website was unavailable for approximately 7 days.
There are many account holders that do not have access to their
BITCOINS. [redacted] wanted to schedule a meeting in person to explain
the situation in detail, in person.

b6
b7C

[redacted] began with a [redacted] USD initial investment to purchase
BITCOINS at a low price. Other than converting physical currency to
BITCOINS, BITCOINS can also be "mined" by participating on the BITCOIN
network of computer servers. Currently, it is not profitable to mine
BITCOINS with an average computer specifications.

08/11/11

New York, New York

(telephonically)

288A-NY-306786 - 6

[redacted]

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of

transcription

Investigation on

at

File #

Date dictated

by

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to

your agency;

it and its contents are not to be distributed outside your agency.

02/10/2012

[redacted] date of birth. [redacted]

b6
b7C

[redacted] telephone number

[redacted] was interviewed at 26 Federal Plaza, New York, NY. After being advised of the identities of the interviewing agents and the nature of the interview, [redacted] provided the following information:

[redacted]

[redacted] first heard of BITCOIN at the end of October 2010.

b6
b7C

[redacted]

[redacted]

MYBITCOIN.COM provides online storage for BITCOINs. It started around early to middle of 2009. [redacted] has an account at MYBITCOIN.COM [redacted]

b6
b7C

[redacted] MYBITCOIN.COM may be linked to a Canadian hacker group, HACK CANADA. HACK CANADA was previously involved in credit card fraud. Many people used MYBITCOIN.COM service to store their BITCOIN online rather than on their own computer.

On July 29, 2011, MYBITCOIN.COM disappeared and was offline for about seven days. During that time, MYBITCOIN.COM changed its web hosting service and registration information and remained silent. [redacted]

[redacted] As a result of MYBITCOIN.COM's disappearance, an online chatroom, BITCOIN POLICE started. BITCOIN POLICE is a "vigilante" group, created by [redacted]@GMAIL.COM to help

08/16/11 New York, New York

288A-NY-306786 - 7
[redacted]

b6
b7C

On
Page

[redacted] received a SMS text message to his Google Voice number. The message came from someone who claimed to be a close associate of [redacted] [redacted] is affiliated with MYBITCOIN.COM. The text message came from British Columbia, Canada. The text message explained that the disappearance of MYBITCOIN.COM was not a scam and when the website is fixed, a forum will be established to help return money to the rightful account holders.

MYBITCOIN.COM did return online and a claim page was set up. MYBITCOIN.COM announced that they had technical issues because they were compromised by hackers. The hackers stole 51% of MYBITCOIN.COM's BITCOIN holdings in small increments.

[redacted] filed a claim, following the instruction on the restored website. [redacted] was able to get back his remaining 49%. Other account holders were able to get their 49% back until approximately three days ago, on or around August 13, 2011. All reimbursements stopped as of that day.

b6
b7C

Other than MYBITCOIN.COM, MT. GOX, based in Japan also offers online storage of BITCOINS. MT. GOX is owned by [redacted] LNU (Last Name Unknown), a French national. MT. GOX converts USD to BITCOIN by accepting money via bank wire. DWALLA and LIBERTY RESERVE. [redacted]

b6
b7C
b7E

[redacted] LNU [redacted] the main technical lead for BITCOIN. [redacted] took over for SATOSHI, creator of BITCOIN. SATOSHI's writing sounds similar to writings done by member of the British Academia. SATOSHI maintained the BITCOIN network until April 2010, when he disappeared.

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/10/2012

To: New York

From: New York

CY-02

Contact: [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-NY-306786 (Pending) - 8

Title: [REDACTED] UNSUB(S);

Synopsis: To close case.

Details: Writer request closing of captioned case. [REDACTED]

b7E

◆◆

UNCLASSIFIED

Bitcoin - Continued

Law Enforcement Impact

(U//LES)) Law enforcement is concerned about the use of Bitcoins to facilitate illegal activities online. The Silk Road is an online black market exchange for contraband goods, like illicit drugs, stolen credit cards, etc. and it operates using Bitcoin. Recently on October 1, 2013, the FBI was able to shut down the website because they captured alleged founder, [redacted] Previously authorities were unsuccessful because the site was hosted as a hidden service on the Tor network.

b6
b7C
b7E

(U//LES)) [redacted]



Silk Road

anonymous marketplace

~~Law Enforcement Sensitive:
For Official Use ONLY (FOLU)~~

