

03/20/2013

someone posing as me managed to con 38 vendors out of 2 btc each with a fake message about a new silk road posted about cartel formation and not mitigating vendor roundtable leaks.
worked on database error handling in CI

03/21/2013

main server was ddosed and taken offline by host
met with person in tor irc who gave me info on having custom hs guards
buying up servers to turn into hidden service guards

03/22/2013

deployed 2 guards on forum
adjusted check_deposit cron to look further back to catch txns that died with an error

03/23/2013

bought a couple of more servers from new hosts
organized local files
stripped out srsec db naming functions
introduced at least two bugs doing this

03/24/2013

been slowly raising the cost of hedging
organized local files and notes

03/25/2013

server was ddosed, meaning someone knew the real IP. I assumed they obtained it by becoming a guard node. So, I migrated to a new server and set up private guard nodes. There was significant downtime and someone has mentioned that they discovered the IP via a leak from lighttpd.

03/26/2013

private guard nodes are working ok. still buying more servers so I can set up a more modular and redundant server cluster. redid login page.

03/27/2013

set up servers

03/28/2013

being blackmailed with user info. talking with large distributor (hell's angels).

03/29/2013

commissioned hit on blackmailer with angels

04/01/2013

got word that blackmailer was executed
created file upload script
started to fix problem with bond refunds over 3 months old



04/02/2013

got death threat from someone (DeathFromAbove) [REDACTED]
[REDACTED] messaged googleyed about it. goog says he doesn't know. user is prolly friend of [REDACTED] who he confided his plan to.
applied fix to bond refund problem
stopped rounding account balance display

04/03/2013

spam scams have been gaining traction. limited namespace and locked current accounts.
lots of delayed withdrawals. transactions taking a long time to be accepted into blockchain. Wallet was funded with single large transaction, so each subsequent transaction is requiring change to be verified. lesson: wallets must be funded in small chunks.

got pidgin chat working with inigo and mg

04/04/2013

withdrawals all caught up

made a sign error when fixing the bond refund bug, so several vendors had very negative accounts.
switched to direct connect for bitcoin instead of over ssh portforward
received visual confirmation of blackmailers execution

04/05/2013

a distributor of googleyed is publishing buyer info
mapped out the ordering process on the wiki.
gave angels access to chat server

04/06/2013

made sure backup crons are working
gave angels go ahead to find tony76
cleaned up unused libraries on server
added to forbidden username list to cover I <-> l scam

04/07/2013

moved storage wallet to local machine
refactored mm page

04/08/2013

sent payment to angels for hit on tony76 and his 3 associates
began setting up hecho as standby
very high load (300/16), took site offline and refactored main and category pages to be more efficient

04/09/2013

problem with load was that APC was set to only cache up to 32M of data. Changed to 5G and load is down to around 5/16.

ssbd considering joining my staff
transferring standby data to hecho standby server

04/10/2013

some vendors using the hedge in a falling market to profit off of me by buying from themselves. turned off access log pruning so I can investigate later. market crashed today.
being blackmailed again. someone says they have my ID, but hasn't proven it.

04/11/2013

set up tor relays
asked scout to go through all images on site looking for quickbuy scam remnants
cimon told me of a possible ddos attack through tor and how to mitigate against it.
guy blackmailing saying he has my id is bogus

04/12/2013

removed last remnant of quickbuy scam
implemented new error controller

rewrote userpage

04/13/2013

inigo is in the hospital, so I covered his shift today. Zeroed everything and made changes to the site in about 5 hours

04/14/2013

did support. inigo returned.

started rewritting orders->buyer_cancel, been getting error reports about it.

04/15/2013

day off

04/16/2013

rewrote buyer_cancel

04/17/2013

rewrote settings view

04/18/2013

modified PIN reset system

04/19/2013

added blockchain.info as xrate source and modified update_xrate to use both and check for discrepancies and log.
modified PIN reset system

04/20/2013

migrated to different host because current host would not connect to guards. Bandwidth limited and site very slow after migration.

04/21 - 04/30/2013

market and forums under sever DoS attack. Gave 10k btc ransom but attack continued. Gave smed server access. Switched to nginx on web/db server, added nginx reverse proxy running tor hs. reconfigured everything and eventually was able to absorb attack.

05/01/2013

Symm starts working support today. Scout takes over forum support.

05/02/2013

Attack continues. No word from attacker. Site is open, but occasionally tor crashes and has to be restarted.

05/03/2013

helping smed fight off attacker. site is mostly down. I'm sick.

Leaked IP of webserver to public and had to redeploy/shred

promoted gramgreen to mod, now named libertas

05/04/2013

attacker agreed to stop if I give him the first \$100k of revenue and \$50k per week thereafter. He stopped, but there appears to be another DoS attack still persisting.

05/05/2013

Attack is fully stopped. regrouping and prioritizing next actions.

05/06/2013

working with smed to put up more defenses against attack

05/07/2013
paid \$100k to attacker

05/08/2013
reconfigured nginx to not time out. almost all errors have disappeared.

05/10/2013
started buying servers for intro/guard nodes

05/11/2012
still buying servers

05/13/2013
helping catch up support
smed demo'ed multi address scheme for the forum

05/15/2013
more servers

05/22/2013
paid the attacker \$50k

05/26/2013
tried moving forum to multi .onion config, but leaked ip twice. Had to change servers, forum was down for a couple of days.

05/28/2013
finished rewritting silkroad.php controller

05/29/2013
rewrote orders page
paid attacker \$50k weekly ransom
\$2M was stolen from my mtgox account by DEA
added smed to payroll
rewrote cart page

05/30/2013



05/31/2013
\$50k xferred to cimon

06/01/2013
someone claiming to be LE trying to infiltrate forum mods

06/02/2013
loaning \$500k to r&w to start vending on SR.

06/03/2013
put cimon in charge of LE counter intel

06/04/2013

rewrote reso center

06/05/2013 - 09/11/2013

Haven't been logging. [REDACTED]

[REDACTED] did an interview with andy greenberg from forbes where i said i wasn't the original DPR, went over well with community.

[REDACTED] r&w flaked out and disappeared with my 1/2 mil. smed has been working hard to develop a monitoring system for the SR infrastructure, but hasn't produced much in actual results. similarly cimon has been working on the mining and gambling projects, but no results forthcoming. created Anonymous Bitcoin Exchange (ABE) and have been trying to recruit tellers. the vendor "gold" is my best lead at the moment. nod is an H dealer on SR who says he has world class it skills and I am giving him a chance to show his stuff with ABE. did a "ratings and review" overhaul. It hasn't gone over too well with the community, but I am still working on it with them and I think it will get there eventually. tor has been clogged up by a botnet causing accessibility issues.

09/12/2013

Got a tip from oldamsterdam that supertrips has been busted. [REDACTED]

09/13/2013

09/11 - 09/18/2013

could not confirm ST bust. [REDACTED]

[REDACTED] Got covered in poison oak trying to get a piece of trash out of a tree in a park nearby and have been moping. went on a first date with amelia from okc.

09/19/2013

red pinged me and asked for meeting tomorrow.

09/19 - 09/25/2013

red got in a jam and needed \$500k to get out. ultimately he convinced me to give it to him, but I got his ID first and had cimon send harry, his new soldier of fortune, to vancouver to get \$800k in cash to cover it. red has been mainly out of communication, but i haven't lost hope. Atlantis shut down. I was messaged by one of their team who said they shut down because of an FBI doc leaked to them detailing vulnerabilities in Tor.

09/30/2013

[REDACTED]. spoke with inigo for a while about the book club and swapping roles with libertas. Had revelation about the need to eat well, get good sleep, and meditate so I can stay positive and productive.

AccessData FTK Imager 3.0.0.1443

File View Mode Help

Evidence Tree

File List

Name	Size	Type	Date Modified
keys	4 KB	Directory	3/28/2013 6:44:02 AM
to write	4 KB	Directory	5/27/2013 5:13:13 AM
wallets	4 KB	Directory	6/22/2013 8:46:27 PM
collection	4 KB	Directory	8/16/2013 1:01:36 AM
to read	4 KB	Directory	9/13/2013 9:25:55 PM
reference	4 KB	Directory	9/27/2013 7:49:25 PM
project references	4 KB	Directory	10/1/2013 6:42:42 AM
NetWorthCalculator.ods	24 KB	Regular File	12/2/2012 6:01:42 PM
dprid.zip.gpg	4 KB	Regular File	6/19/2013 8:38:00 PM
servers_smed.ods	19 KB	Regular File	6/29/2013 9:20:58 PM
sr_accounting.ods	42 KB	Regular File	7/3/2013 7:25:28 PM
todo_monthly	1 KB	Regular File	9/12/2013 10:00:19 PM
someday.txt	1 KB	Regular File	9/13/2013 1:30:21 AM
emergency	1 KB	Regular File	9/15/2013 4:34:25 AM
projects.txt	1 KB	Regular File	9/22/2013 8:35:12 PM
collection.txt	1 KB	Regular File	9/23/2013 5:48:49 PM
server_config.txt	10 KB	Regular File	9/24/2013 4:08:09 AM
servers.ods	40 KB	Regular File	9/26/2013 2:56:39 AM
todo_weekly	2 KB	Regular File	10/1/2013 1:03:06 AM
designated.txt	1 KB	Regular File	10/1/2013 4:37:55 AM
log.txt	10 KB	Regular File	10/1/2013 5:43:24 AM
todo.txt	1 KB	Regular File	10/1/2013 9:45:29 PM

Properties

General

- Name: log.txt
- File Class: Regular File
- File Size: 9,389
- Physical Size: 12,288
- Start Cluster: 87,648,307
- Date Accessed: 10/2/2013 6:00:07 AM
- Date Created: 10/1/2013 5:43:24 AM
- Date Modified: 10/1/2013 5:43:24 AM
- Actual File: True

UNIX Security Attributes

- Unix Permissions: -rw-rw-r--
- UID: 1,000
- GID: 1,000

Ext2/3/4 Information

- Inode Number: 3,677,791
- Inode Change Time: 10/1/2013 5:43:24 AM

Text Log Content:

```

03/20/2013
someone posing as me managed to con 38 vendors out of 2 btc each with a fake message about a new silk road
posted about cartel formation and not mitigating vendor roundtable leaks.
worked on database error handling in CI

03/21/2013
main server was ddosed and taken offline by host
met with person in tor irc who gave me info on having custom hs guards
buying up servers to turn into hidden service guards

03/22/2013
deployed 2 guards on forum
adjusted check_deposit cron to look further back to catch txns that died with an error

03/23/2013
bought a couple of more servers from new hosts
organized local files
stripped out srsec db naming functions
introduced at least two bugs doing this

03/24/2013
been slowly raising the cost of hedging
organized local files and notes

03/25/2013
server was ddosed, meaning someone knew the real IP. I assumed they obtained it by becoming a guard node. So, I migrated to a new se

03/26/2013
private guard nodes are working ok. still buying more servers so I can set up a more modular and redundant server cluster. redid log

03/27/2013
set up servers

03/28/2013
being blackmailed with user info. talking with large distributor (hell's angels).

```

sda4_crypt.dd/ubucrypt-root [588412MB]/NONAME [ext4]/[root]/home/frosty/backup/log.txt