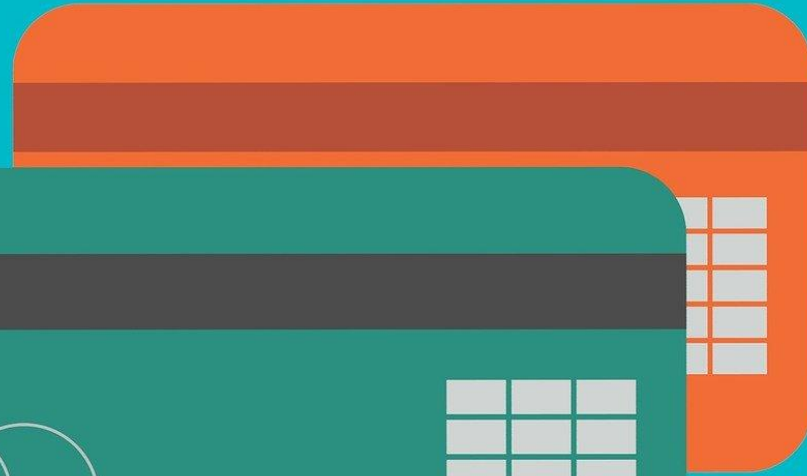


Who Stole My '\$100K' worth of Bitcoin Wallets

Catch Them All with new deceptive bait

Tan Kean Siong
The HoneyNet Project
twitter: @gento_





Threat Level: GREEN

Hand



SANS ISC InfoSec Forums

Keyword, Domain, Port, IP or Host Search

Watch ISC TV. Great for NOCs, SOCs and Living Rooms:
<https://isctv.sans.edu>

Email

[Sign Up for Free!](#)

[← Next Thread](#) [Previous Thread →](#)

Contact Us

Diary

Podcasts

Jobs

Tools

Data

FORUMS

[Auditing](#)

[Diary Discussions](#)

[Forensics](#)

[General Discussions](#)

[Industry News](#)

[Network Security](#)

[Penetration Testing](#)

[Software Security](#)

Questions?

Feedback?

BTC Pickpockets



I observed requests to my webserver to retrieve Bitcoin wallet files:

```

212.92.122.186 - - [17/Oct/2017:07:57:06 -0400] "GET /wallet_backup.dat HTTP/1.1" 404 284 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:07 -0400] "GET /bitcoinstevens.com/wallet.dat HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:09 -0400] "GET /wallet.dat HTTP/1.1" 404 273 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:10 -0400] "GET /bitcoin/wallet.zip HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:20 -0400] "GET /backups/bitcoin/wallet.dat HTTP/1.1" 404 291 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:20 -0400] "GET /wallet.tar HTTP/1.1" 404 275 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:40 -0400] "GET /didierstevens.wallet.dat HTTP/1.1" 404 293 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:41 -0400] "GET /wallet_backup.dat.zip HTTP/1.1" 404 286 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:41 -0400] "GET /home/ubuntu/bitcoin/wallet.dat HTTP/1.1" 404 296 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:57:45 -0400] "GET /bitcoin/wallet.dat.zip HTTP/1.1" 404 287 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:04 -0400] "GET /wallet.dat.zip HTTP/1.1" 404 279 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:05 -0400] "GET /home/ubuntu/bitcoin/wallet.dat HTTP/1.1" 404 296 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:24 -0400] "GET /datadir/wallet.dat HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:25 -0400] "GET /wallet$20-$20copy.dat HTTP/1.1" 404 282 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:25 -0400] "GET /backup/wallet.tar.gz HTTP/1.1" 404 285 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:44 -0400] "GET /wallet_backup.dat HTTP/1.1" 404 282 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:58:48 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 288 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:59:16 -0400] "GET /didierstevens.wallet.dat.zip HTTP/1.1" 404 293 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:59:19 -0400] "GET /backup/wallet.dat HTTP/1.1" 404 282 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:59:37 -0400] "GET /backup/wallet.zip HTTP/1.1" 404 282 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:07:59:37 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 287 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:21 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:22 -0400] "GET /bitcoinstevens.com/wallet.zip HTTP/1.1" 404 293 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:22 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 284 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:28 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 284 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:28 -0400] "GET /backups/wallet.dat HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:46 -0400] "GET /home/root/bitcoin/wallet.dat HTTP/1.1" 404 294 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:00:50 -0400] "GET /wallet.zip HTTP/1.1" 404 275 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:02:47 -0400] "GET /backups/wallet.zip HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:02:49 -0400] "GET /wallet_backup.zip HTTP/1.1" 404 282 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:02:56 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 285 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:03:03 -0400] "GET /didierstevens.wallet.dat HTTP/1.1" 404 289 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:03:35 -0400] "GET /backup/wallet$20-$20copy.dat HTTP/1.1" 404 289 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:04:29 -0400] "GET /wallet.tar.gz HTTP/1.1" 404 278 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:05:25 -0400] "GET /backup/bitcoin/wallet.dat HTTP/1.1" 404 290 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:05:39 -0400] "GET /backups/wallet.tar.gz HTTP/1.1" 404 286 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:05:44 -0400] "GET /didierstevens.com/wallet.dat.zip HTTP/1.1" 404 297 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:05:44 -0400] "GET /backup/wallet.tar HTTP/1.1" 404 282 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:06:23 -0400] "GET /data/wallet.dat HTTP/1.1" 404 280 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:06:43 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:07:19 -0400] "GET /wallet.dat HTTP/1.1" 404 277 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:07:28 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:09:06 -0400] "GET /didierstevens.com/wallet.dat HTTP/1.1" 404 295 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:09:16 -0400] "GET /backups/wallet.tar HTTP/1.1" 404 283 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:10:14 -0400] "GET /backups/wallet.zip HTTP/1.1" 404 289 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:10:38 -0400] "GET /bitcoinstevens.wallet.dat HTTP/1.1" 404 287 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:11:08 -0400] "GET /bitcoin$20datadir/wallet.dat HTTP/1.1" 404 291 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:21:29 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 292 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
212.92.122.186 - - [17/Oct/2017:08:29:25 -0400] "GET /wallet.dat HTTP/1.1" 404 276 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"

```

The files they are looking for are:

DidierStevens



477 POSTS

ISC HANDLER

Nov
18th
2017

212.92.122.186 - - [17/oct/2017:07:57:09 -0400] "GET /wallet.dat HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; ..."

212.92.122.186 - - [17/oct/2017:07:57:10 -0400] "GET /bitcoin_wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:07:57:20 -0400] "GET /backups/bitcoin_wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:07:57:20 -0400] "GET /wallet.tar HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; ..."

212.92.122.186 - - [17/oct/2017:07:57:40 -0400] "GET /didierstevens_wallet.dat.1 HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:07:57:41 -0400] "GET /wallet_backup.dat.zip HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:07:57:41 -0400] "GET /home/.bitcoin/wallet.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M ..."

212.92.122.186 - - [17/oct/2017:07:57:45 -0400] "GET /bitcoin_wallet.dat.zip HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:07:58:04 -0400] "GET /wallet.dat.zip HTTP/1.1" 404 279 "-" "Mozilla/5.0 (Macintosh; Intel mac OS X 1 ..."

212.92.122.186 - - [17/oct/2017:07:58:05 -0400] "GET /home/ubuntu/.bitcoin/wallet.dat HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Macintosh; ..."

212.92.122.186 - - [17/oct/2017:07:58:29 -0400] "GET /datadir/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:07:58:35 -0400] "GET /wallet%20-%20Copy.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:07:58:35 -0400] "GET /backup/wallet.tar.gz HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac O ..."

212.92.122.186 - - [17/oct/2017:07:58:44 -0400] "GET /wallet_backup.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:07:58:48 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 288 "-" "Mozilla/5.0 (Macintosh; Intel Ma ..."

212.92.122.186 - - [17/oct/2017:07:59:16 -0400] "GET /didierstevens_wallet.dat.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; Int ..."

212.92.122.186 - - [17/oct/2017:07:59:19 -0400] "GET /backup/wallet.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; intel mac os x ..."

212.92.122.186 - - [17/oct/2017:07:59:37 -0400] "GET /backup/wallet.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:07:59:52 -0400] "GET /bitcoindata/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; intel mac ..."

212.92.122.186 - - [17/oct/2017:08:00:21 -0400] "GET /bitcoin_wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:00:23 -0400] "GET /didierstevens.com_wallet.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; int ..."

212.92.122.186 - - [17/oct/2017:08:00:28 -0400] "GET /.bitcoin/wallet.dat HTTP/1.1" 404 284 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:00:36 -0400] "GET /backups/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; intel mac os ..."

212.92.122.186 - - [17/oct/2017:08:00:46 -0400] "GET /home/root/.bitcoin/wallet.dat HTTP/1.1" 404 294 "-" "Mozilla/5.0 (Macintosh; Ir ..."

212.92.122.186 - - [17/oct/2017:08:00:50 -0400] "GET /wallet.zip HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel mac OS X 10.8; ..."

212.92.122.186 - - [17/oct/2017:08:02:47 -0400] "GET /backups/wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:02:49 -0400] "GET /wallet_backup.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:08:02:56 -0400] "GET /bitcoin_wallet.dat.1 HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac O ..."

212.92.122.186 - - [17/oct/2017:08:03:03 -0400] "GET /didierstevens_wallet.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M ..."

212.92.122.186 - - [17/oct/2017:08:03:35 -0400] "GET /backup/wallet%20-%20Copy.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Int ..."

212.92.122.186 - - [17/oct/2017:08:04:39 -0400] "GET /wallet.tar.gz HTTP/1.1" 404 278 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 ..."

212.92.122.186 - - [17/oct/2017:08:05:25 -0400] "GET /backup/bitcoin_wallet.dat HTTP/1.1" 404 290 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:08:05:39 -0400] "GET /backups/wallet.tar.gz HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:08:05:44 -0400] "GET /didierstevens.com_wallet.dat.zip HTTP/1.1" 404 297 "-" "Mozilla/5.0 (Macintosh; ..."

212.92.122.186 - - [17/oct/2017:08:05:51 -0400] "GET /backup/wallet.tar HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:08:06:23 -0400] "GET /data/wallet.dat HTTP/1.1" 404 280 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1 ..."

212.92.122.186 - - [17/oct/2017:08:06:43 -0400] "GET /Bitcoin/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:07:19 -0400] "GET /wallet.dat.1 HTTP/1.1" 404 277 "-" "Mozilla/5.0 (Macintosh; intel mac os x 10.8 ..."

212.92.122.186 - - [17/oct/2017:08:07:28 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:09:06 -0400] "GET /didierstevens.com_wallet.dat.1 HTTP/1.1" 404 295 "-" "Mozilla/5.0 (Macintosh; I ..."

212.92.122.186 - - [17/oct/2017:08:09:16 -0400] "GET /backups/wallet.tar HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:10:24 -0400] "GET /didierstevens_wallet.zip HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; intel M ..."

212.92.122.186 - - [17/oct/2017:08:10:38 -0400] "GET /BitcoinData/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:08:11:08 -0400] "GET /bitcoin%20datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; int ..."

212.92.122.186 - - [17/oct/2017:08:11:20 -0400] "GET /bitcoin_datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:08:29:25 -0400] "GET /_wallet.dat HTTP/1.1" 404 276 "-" "Mozilla/5.0 (Macintosh; intel mac os x 10.8; ..."

```
212.92.122.186 - - [17/oct/2017:07:57:09 -0400] "GET /wallet.dat HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x 10.8;
212.92.122.186 - - [17/oct/2017:07:57:10 -0400] "GET /bitcoin_wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:07:57:20 -0400] "GET /backups/bitcoin_wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel
212.92.122.186 - - [17/oct/2017:07:57:20 -0400] "GET /wallet.tar HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x 10.8;
212.92.122.186 - - [17/oct/2017:07:57:40 -0400] "GET /didierstevens_wallet.dat.1 HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel
212.92.122.186 - - [17/oct/2017:07:57:41 -0400] "GET /wallet_backup.dat.zip HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac
212.92.122.186 - - [17/oct/2017:07:57:41 -0400] "GET /home/.bitcoin/wallet.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M
212.92.122.186 - - [17/oct/2017:07:57:45 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac
212.92.122.186 - - [17/oct/2017:07:58:04 -0400] "GET /wallet.dat.zip HTTP/1.1" 404 279 "-" "Mozilla/5.0 (Macintosh; Intel mac OS x 1
212.92.122.186 - - [17/oct/2017:07:58:05 -0400] "GET /ubuntu/.bitcoin/wallet.dat HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Macintosh;
212.92.122.186 - - [17/oct/2017:07:58:29 -0400] "GET /datadir/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:07:58:35 -0400] "GET /wallet%20-%20Copy.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac
212.92.122.186 - - [17/oct/2017:07:58:35 -0400] "GET /backup/wallet.tar.gz HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
212.92.122.186 - - [17/oct/2017:07:58:44 -0400] "GET /wallet_backup.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x
212.92.122.186 - - [17/oct/2017:07:58:48 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 288 "-" "Mozilla/5.0 (Macintosh; Intel Ma
212.92.122.186 - - [17/oct/2017:07:59:16 -0400] "GET /didierstevens_wallet.dat.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; Int
212.92.122.186 - - [17/oct/2017:07:59:19 -0400] "GET /backup/wallet.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x
212.92.122.186 - - [17/oct/2017:07:59:37 -0400] "GET /backup/wallet.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x
212.92.122.186 - - [17/oct/2017:07:59:52 -0400] "GET /bitcoindata/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac
212.92.122.186 - - [17/oct/2017:08:00:21 -0400] "GET /bitcoin_wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:00:23 -0400] "GET /didierstevens.com_wallet.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; int
212.92.122.186 - - [17/oct/2017:08:00:28 -0400] "GET /.bitcoin/wallet.dat HTTP/1.1" 404 284 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:00:36 -0400] "GET /backups/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:00:46 -0400] "GET /home/root/.bitcoin/wallet.dat HTTP/1.1" 404 294 "-" "Mozilla/5.0 (Macintosh; Ir
212.92.122.186 - - [17/oct/2017:08:00:50 -0400] "GET /wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel mac OS x 10.8;
212.92.122.186 - - [17/oct/2017:08:02:47 -0400] "GET /backups/wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:02:49 -0400] "GET /wallet_backup.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x
212.92.122.186 - - [17/oct/2017:08:02:56 -0400] "GET /bitcoin_wallet.zip HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
212.92.122.186 - - [17/oct/2017:08:03:03 -0400] "GET /didierstevens_wallet.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M
212.92.122.186 - - [17/oct/2017:08:03:35 -0400] "GET /backup/wallet%20-%20Copy.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Int
212.92.122.186 - - [17/oct/2017:08:04:39 -0400] "GET /wallet.tar.gz HTTP/1.1" 404 278 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x 10.
212.92.122.186 - - [17/oct/2017:08:05:25 -0400] "GET /backup/bitcoin_wallet.dat HTTP/1.1" 404 290 "-" "Mozilla/5.0 (Macintosh; Intel
212.92.122.186 - - [17/oct/2017:08:05:39 -0400] "GET /backups/wallet.tar.gz HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac
212.92.122.186 - - [17/oct/2017:08:05:44 -0400] "GET /didierstevens.com_wallet.dat.zip HTTP/1.1" 404 297 "-" "Mozilla/5.0 (Macintosh;
212.92.122.186 - - [17/oct/2017:08:05:51 -0400] "GET /backup/wallet.tar HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x
212.92.122.186 - - [17/oct/2017:08:06:23 -0400] "GET /data/wallet.dat HTTP/1.1" 404 280 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x 1
212.92.122.186 - - [17/oct/2017:08:06:43 -0400] "GET /Bitcoin/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:07:19 -0400] "GET /wallet.dat.1 HTTP/1.1" 404 277 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS x 10.8
212.92.122.186 - - [17/oct/2017:08:07:28 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:09:06 -0400] "GET /didierstevens.com_wallet.dat.1 HTTP/1.1" 404 295 "-" "Mozilla/5.0 (Macintosh; I
212.92.122.186 - - [17/oct/2017:08:09:16 -0400] "GET /backups/wallet.tar HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
212.92.122.186 - - [17/oct/2017:08:10:24 -0400] "GET /didierstevens_wallet.zip HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M
212.92.122.186 - - [17/oct/2017:08:10:38 -0400] "GET /BitcoinData/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac
212.92.122.186 - - [17/oct/2017:08:11:08 -0400] "GET /bitcoin%20datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; int
212.92.122.186 - - [17/oct/2017:08:11:20 -0400] "GET /bitcoin_datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel
212.92.122.186 - - [17/oct/2017:08:29:25 -0400] "GET /_wallet.dat HTTP/1.1" 404 276 "-" "Mozilla/5.0 (Macintosh; intel mac OS x 10.8;
```



Honeybag



A tool that allows you to **create 'bait archive'**
with any folders and files,
notify you if someone access it.

Useful for data breach detection, deception defense mechanism, etc.

How Honeybag works



1. Honeybag client

Generate 'bait ZIP file', with any embedded folder / files / doc / PDF, etc

Alerting mechanisms:

- desktop.ini
- .url

```
secret.zip
├── secretfolder
│   ├── company.com.url
│   ├── desktop.ini
│   └── supersecretdocument.pdf
```

1 directory, 3 files

How Honeybag works



1. Honeybag client

Generate 'bait ZIP file', with any embedded folder / files / doc / PDF, etc

Alerting mechanisms:

- desktop.ini
- .url



```
secret.zip
├── secretfolder
│   ├── company.com.url
│   ├── desktop.ini
│   └── supersecretdocument.pdf
1 directory, 3 files
```



2. Honeybag simple DNS server

Listening for incoming alert with DNS traffic, sqlite3 logging

3. RESPONDER IP address

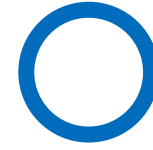
Listening on incoming alert with SMB traffic / NTLM hashes



If we place
'\$100,000' worth BTC wallets
on the Internet for 90 days

What will happen next?





What we have:

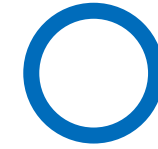
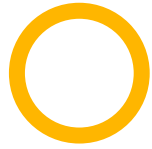


10 Bitcoin Wallets

- unprotected
- each contains **1 BTC Testnet**

(In early 2020

Real 1 BTC = ~USD \$10,000)



What we have:

10 Bitcoin Wallets

- unprotected
- each contains **1 BTC Testnet**

(In early 2020

Real 1 BTC = ~USD \$10,000)



Where we put it:

Open directory web servers

212.92.122.186 - - [17/oct/2017:07:57:09 -0400] "GET /wallet.dat HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; ..."

212.92.122.186 - - [17/oct/2017:07:57:10 -0400] "GET /bitcoin_wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:07:57:20 -0400] "GET /backups/bitcoin_wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:07:57:20 -0400] "GET /wallet.tar HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; ..."

212.92.122.186 - - [17/oct/2017:07:57:40 -0400] "GET /didierstevens_wallet.dat.1 HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:07:57:41 -0400] "GET /wallet_backup.dat.zip HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:07:57:41 -0400] "GET /home/.bitcoin/wallet.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M ..."

212.92.122.186 - - [17/oct/2017:07:57:45 -0400] "GET /bitcoin_wallet.dat.zip HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:07:58:04 -0400] "GET /wallet.dat.zip HTTP/1.1" 404 279 "-" "Mozilla/5.0 (Macintosh; Intel mac OS X 1 ..."

212.92.122.186 - - [17/oct/2017:07:58:05 -0400] "GET /home/ubuntu/.bitcoin/wallet.dat HTTP/1.1" 404 296 "-" "Mozilla/5.0 (Macintosh; ..."

212.92.122.186 - - [17/oct/2017:07:58:29 -0400] "GET /datadir/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:07:58:35 -0400] "GET /wallet%20-%20Copy.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:07:58:35 -0400] "GET /backup/wallet.tar.gz HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac O ..."

212.92.122.186 - - [17/oct/2017:07:58:44 -0400] "GET /wallet_backup.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:07:58:48 -0400] "GET /bitcoin_data/wallet.dat HTTP/1.1" 404 288 "-" "Mozilla/5.0 (Macintosh; Intel Ma ..."

212.92.122.186 - - [17/oct/2017:07:59:16 -0400] "GET /didierstevens_wallet.dat.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; Int ..."

212.92.122.186 - - [17/oct/2017:07:59:19 -0400] "GET /backup/wallet.dat HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; intel mac os x ..."

212.92.122.186 - - [17/oct/2017:07:59:37 -0400] "GET /backup/wallet.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:07:59:52 -0400] "GET /bitcoindata/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; intel mac ..."

212.92.122.186 - - [17/oct/2017:08:00:21 -0400] "GET /bitcoin_wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:00:23 -0400] "GET /didierstevens.com_wallet.zip HTTP/1.1" 404 293 "-" "Mozilla/5.0 (Macintosh; int ..."

212.92.122.186 - - [17/oct/2017:08:00:28 -0400] "GET /.bitcoin/wallet.dat HTTP/1.1" 404 284 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:00:36 -0400] "GET /backups/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; intel mac os ..."

212.92.122.186 - - [17/oct/2017:08:00:46 -0400] "GET /home/root/.bitcoin/wallet.dat HTTP/1.1" 404 294 "-" "Mozilla/5.0 (Macintosh; Ir ..."

212.92.122.186 - - [17/oct/2017:08:00:50 -0400] "GET /wallet.zip HTTP/1.1" 404 275 "-" "Mozilla/5.0 (Macintosh; Intel mac OS X 10.8; ..."

212.92.122.186 - - [17/oct/2017:08:02:47 -0400] "GET /backups/wallet.zip HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:02:49 -0400] "GET /wallet_backup.zip HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:08:02:56 -0400] "GET /bitcoin_wallet.dat.1 HTTP/1.1" 404 285 "-" "Mozilla/5.0 (Macintosh; Intel Mac O ..."

212.92.122.186 - - [17/oct/2017:08:03:03 -0400] "GET /didierstevens_wallet.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Intel M ..."

212.92.122.186 - - [17/oct/2017:08:03:35 -0400] "GET /backup/wallet%20-%20Copy.dat HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; Int ..."

212.92.122.186 - - [17/oct/2017:08:04:39 -0400] "GET /wallet.tar.gz HTTP/1.1" 404 278 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 ..."

212.92.122.186 - - [17/oct/2017:08:05:25 -0400] "GET /backup/bitcoin_wallet.dat HTTP/1.1" 404 290 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:08:05:39 -0400] "GET /backups/wallet.tar.gz HTTP/1.1" 404 286 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:08:05:44 -0400] "GET /didierstevens.com_wallet.dat.zip HTTP/1.1" 404 297 "-" "Mozilla/5.0 (Macintosh; ..."

212.92.122.186 - - [17/oct/2017:08:05:51 -0400] "GET /backup/wallet.tar HTTP/1.1" 404 282 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X ..."

212.92.122.186 - - [17/oct/2017:08:06:23 -0400] "GET /data/wallet.dat HTTP/1.1" 404 280 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1 ..."

212.92.122.186 - - [17/oct/2017:08:06:43 -0400] "GET /Bitcoin/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:07:19 -0400] "GET /wallet.dat.1 HTTP/1.1" 404 277 "-" "Mozilla/5.0 (Macintosh; intel mac os x 10.8 ..."

212.92.122.186 - - [17/oct/2017:08:07:28 -0400] "GET /bitcoin/wallet.dat HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:09:06 -0400] "GET /didierstevens.com_wallet.dat.1 HTTP/1.1" 404 295 "-" "Mozilla/5.0 (Macintosh; I ..."

212.92.122.186 - - [17/oct/2017:08:09:16 -0400] "GET /backups/wallet.tar HTTP/1.1" 404 283 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS ..."

212.92.122.186 - - [17/oct/2017:08:10:24 -0400] "GET /didierstevens_wallet.zip HTTP/1.1" 404 289 "-" "Mozilla/5.0 (Macintosh; intel M ..."

212.92.122.186 - - [17/oct/2017:08:10:38 -0400] "GET /BitcoinData/wallet.dat HTTP/1.1" 404 287 "-" "Mozilla/5.0 (Macintosh; Intel Mac ..."

212.92.122.186 - - [17/oct/2017:08:11:08 -0400] "GET /bitcoin%20datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; int ..."

212.92.122.186 - - [17/oct/2017:08:11:20 -0400] "GET /bitcoin_datadir/wallet.dat HTTP/1.1" 404 291 "-" "Mozilla/5.0 (Macintosh; Intel ..."

212.92.122.186 - - [17/oct/2017:08:29:25 -0400] "GET /_wallet.dat HTTP/1.1" 404 276 "-" "Mozilla/5.0 (Macintosh; intel mac os x 10.8; ..."

118.237.14.248 - - [06/Mar/2020:19:37:56 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:38:49 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:38:51 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:39:06 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:40:54 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:41:52 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:43:51 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:43:57 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:44:16 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:47:00 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:47:18 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:52:54 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:53:03 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:19:55:40 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
139.162.170.47 - - [06/Mar/2020:20:04:13 +0000] "GET /.env HTTP/1.1" 404 341 "-" "curl/7.58.0"
118.237.14.248 - - [06/Mar/2020:20:05:02 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:20:06:42 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:20:15:50 +0000] "-" 408 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:20:16:49 +0000] "-" 408 0 "-" "-"
195.60.190.156 - - [06/Mar/2020:20:19:21 +0000] "GET / HTTP/1.1" 200 830 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36"
118.237.14.248 - - [06/Mar/2020:20:23:09 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:20:23:26 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
138.255.73.253 - - [06/Mar/2020:20:23:58 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
190.94.149.174 - - [06/Mar/2020:20:28:25 +0000] "GET / HTTP/1.1" 200 830 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36"
118.237.14.248 - - [06/Mar/2020:20:29:46 +0000] "-" 408 0 "-" "-"
110.77.227.173 - - [06/Mar/2020:20:36:33 +0000] "GET / HTTP/1.1" 200 830 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36"
118.237.14.248 - - [06/Mar/2020:20:41:54 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
118.237.14.248 - - [06/Mar/2020:20:44:09 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
187.12.151.162 - - [06/Mar/2020:21:30:29 +0000] "GET / HTTP/1.1" 200 830 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36"
103.83.5.41 - - [06/Mar/2020:22:47:55 +0000] "GET / HTTP/1.0" 200 849 "-" "masscan/1.0 (https://github.com/robertdavidgraham/masscan)"
14.247.103.15 - - [07/Mar/2020:00:14:41 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
201.95.169.199 - - [07/Mar/2020:00:35:04 +0000] "GET / HTTP/1.1" 200 830 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36"
54.36.49.151 - - [07/Mar/2020:01:30:31 +0000] "GET / HTTP/1.0" 200 849 "-" "masscan/1.0 (https://github.com/robertdavidgraham/masscan)"
91.121.157.178 - - [07/Mar/2020:02:25:52 +0000] "GET / HTTP/1.0" 200 849 "-" "masscan/1.0 (https://github.com/robertdavidgraham/masscan)"
66.249.65.216 - - [07/Mar/2020:03:31:59 +0000] "GET /robots.txt HTTP/1.1" 404 397 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
66.249.65.218 - - [07/Mar/2020:03:31:59 +0000] "GET /backup/google579cbf79fa33b925.html HTTP/1.1" 404 397 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
109.202.9.19 - - [07/Mar/2020:03:37:27 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
139.162.106.181 - - [07/Mar/2020:03:56:09 +0000] "GET / HTTP/1.1" 200 849 "-" "HTTP Banner Detection (https://security.ipip.net)"

What's happening in **90 days**?

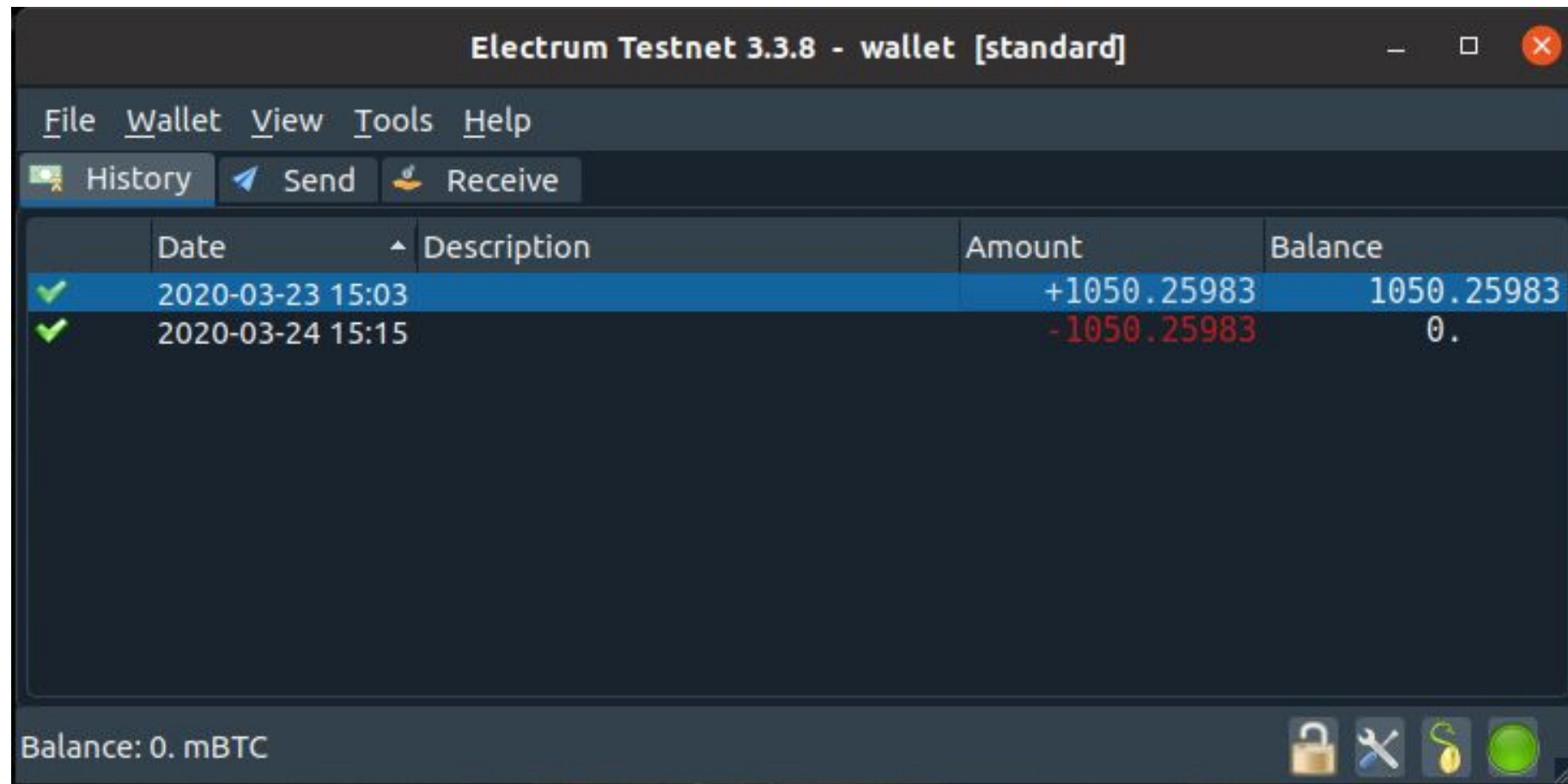
All 10 wallets (Honeybag) were **stolen**

9 / 10 wallets alerted us with 'thief' info. **1 missing**

Fastest record of stolen wallet: **< 1 minute** (after posted on Pastebin)

An Unexpected Scene

Someone just **'wipe out'** one of our BTC Testnet wallets



The screenshot shows the Electrum Testnet 3.3.8 wallet interface. The title bar reads "Electrum Testnet 3.3.8 - wallet [standard]". The menu bar includes "File", "Wallet", "View", "Tools", and "Help". Below the menu bar are buttons for "History", "Send", and "Receive". The main area displays a transaction history table with the following data:

| | Date | Description | Amount | Balance |
|---|------------------|-------------|-------------|------------|
| ✓ | 2020-03-23 15:03 | | +1050.25983 | 1050.25983 |
| ✓ | 2020-03-24 15:15 | | -1050.25983 | 0. |

At the bottom left, the status bar shows "Balance: 0. mBTC". At the bottom right, there are icons for a lock, a wrench, a coin, and a green circle.

Timeline analysis - 2020-03-24

1. Web Server HTTP log

```
user@honeybag:/var/log/apache2$ cat access.log | grep wallet.zip
114.124.197.76 - - [24/Mar/2020:14:40:46 +0000] "GET /bitcoin/wallet.zip HTTP/1.1"
 200 16072 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101
Firefox/74.0"
user@honeybag:/var/log/apache2$
```

Timeline analysis - 2020-03-24

2. Honeybag DNS Alert log

```
UDP request 2020-03-24 14:31:58.630249 (143.215.172.76 48431):
UDP request 2020-03-24 14:32:22.442098 (146.88.240.4 56699):
UDP request 2020-03-24 14:42:27.196795 (182.0.242.44 14834):
[Bingo!] DNS query for domain: BLUE.DESKTOP-AFMMB6K.DESKTOP-AFMMB6K.
[Bingo!] Domain matched with token!
[Bingo!] Opened database successfully
[Bingo!] Records created successfully
UDP request 2020-03-24 14:42:27.209691 (114.121.227.33 58909):
[Bingo!] DNS query for domain: BLUE.DESKTOP-AFMMB6K.DESKTOP-AFMMB6K.
[Bingo!] Domain matched with token!
[Bingo!] Opened database successfully
[Bingo!] Records created successfully
UDP request 2020-03-24 14:43:11.842988 (182.0.242.44 2418):
[Bingo!] DNS query for domain: BLUE.DESKTOP-AFMMB6K.DESKTOP-AFMMB6K.
[Bingo!] Domain matched with token!
[Bingo!] Opened database successfully
[Bingo!] Records created successfully
```

Timeline analysis - 2020-03-24

3. RESPONDER

```
user1@honeybag1:~/Responder/logs$ ls -lht
```

```
total 68M
```

```
-rw-r--r-- 1 root root 41M Mar 24 16:26 Responder-Session.log
```

```
-rw-r--r-- 1 root root 88K Mar 24 15:01 SMB-NTLMv2-SSP-114.124.246.253.txt
```

```
user1@honeybag1:~/Responder/logs$ cat SMB-NTLMv2-SSP-114.124.246.253.txt
```

```
BLUE :: DESKTOP-AFMMB6K: 415fc2711c0064d2:CC964D88D2F5E5B8A4B2C80EDF4C538F:0101000000000000C065  
D201ED41BB8E7989DF98000000000200080053004D004200330001001E00570049004E002D005000520048003400  
520051004100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00  
4800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C00050014005300  
33002E006C006F00630061006C0007000800C0653150DE09D20106000400020000000800300030000000000000  
00200000E1CCBA953547CB33FF9037F9100D30125D4DDBA1BC12CC4453372749185AB1E80A00100000000000000  
0000000000000900280063006900660073002F003100360037002E003100370032002E003200330035002E003100  
0000000000000000000000000000
```

```
BLUE :: DESKTOP-AFMMB6K: 415fc2711c0064d2:CC964D88D2F5E5B8A4B2C80EDF4C538F:0101000000000000C065  
D201ED41BB8E7989DF98000000000200080053004D004200330001001E00570049004E002D005000520048003400  
520051004100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00  
4800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C00050014005300  
33002E006C006F00630061006C0007000800C0653150DE09D20106000400020000000800300030000000000000  
00200000E1CCBA953547CB33FF9037F9100D30125D4DDBA1BC12CC4453372749185AB1E80A00100000000000000
```

Timeline overview - 2020-03-24

14:40:46 UTC - Wallet.zip was stolen from web server

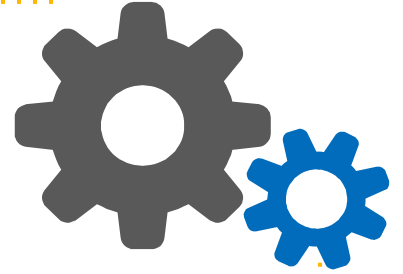
14:42:27 UTC - First DNS alert, someone accessed Wallet.zip

15:01:00 UTC - SMB Alert in RESPONDER log

15:15:00 UTC - He/she 'wipe out' our BTC TESTNET wallet



Do & Don't



- **Be patient!**
- **Customise** our own unique deceptive baits
- **Put up warning message** / banners
- Never underestimate the great impact of this



Honeybag

A tool that allows you to create 'bait archive' with any folders and files, notify you if someone access it.

<https://github.com/honeybag>

Thank you !

VB2020 localhost

Tan Kean Siong
The HoneyNet Project
twitter: @gento_