home

3301

Note: There may be some typos, and you may want to find a solid block of time before reading this article. It's about an internet quest spanning one month and several days…

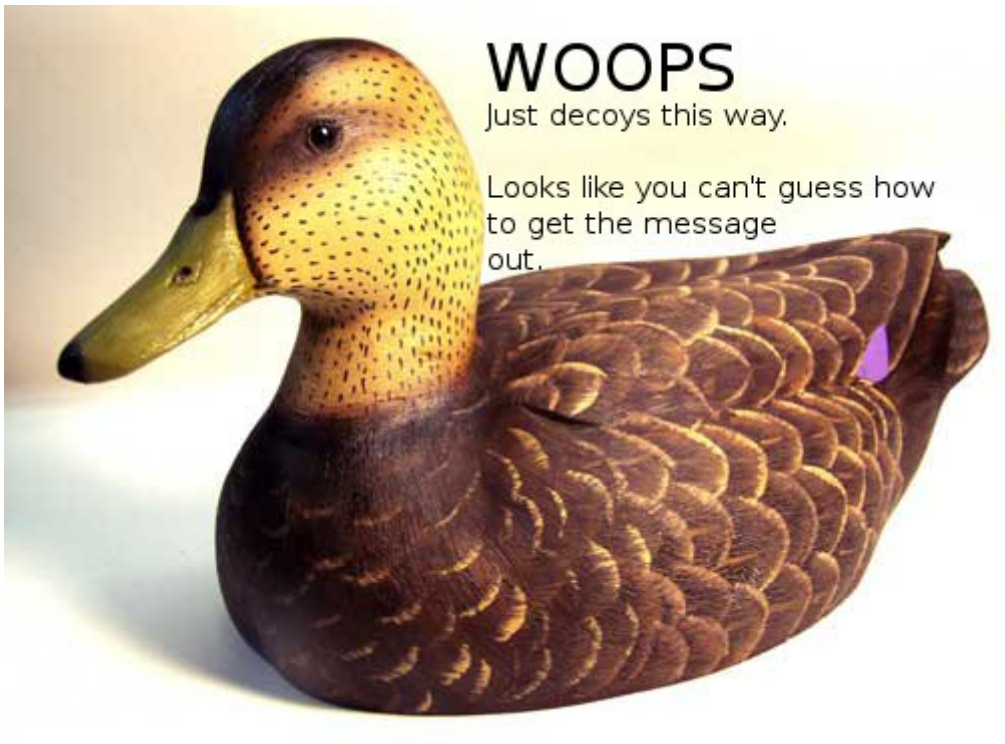
All names in this article have been changed to reflect usernames. Also, I mix points of view ("I", "we") since some parts were collective thinking, and others were individual. Some pieces of this story have been removed to protect the puzzle creators. I note where they are.

It all started when I was sitting in the middle of Advisory at school: my friend *all2well* told me about this puzzle that he'd found on the internet. 4chan's /b/, specifically. A group had posted the following image:

very bottom. It read:

```
TIBERIVS CLAVDIVS CAESAR says "lxxt>33m2mqkyv2gsq3q=w]O2ntk"
```

How odd. I'd never heard of Tiberius Claudius, but upon looking him up, I learned that he was the fourth Caesar. We used a used `rot4` on the string in quotes. Out of that came a URL: http://i.imgur.com/m9sYK.jpg



At this point, I joined an IRC channel on mibbit. From there, I narrowed the groupd down from 30 people to around 10, and we collectively worked on this. This is where `cancer0`, `habitres`, `wakeen`, `manbearpig`, `r`, `math`, and `snogfarth` came into play.

The words "out" and "guess" got us thinking. I was pretty sure that I'd heard of a steganography tool called "outguess". For those of you unfamiliar with steganography, it's the practice of inserting and extracting hidden data into and from carrier files (Wikipedia).

After getting the outguess source from their website (http://www.outguess.org/download.php), I built and compiled it. Man pages were invaluable.

```
outguess -r final.jpg final.txt
```

“Here is a book code. To find the book, and more information, go to http://www.reddit.com/r/a2e7j6ic78h0j/” (missing the 76 lines of book code following — to see the whole thing, visit [this pastebin](#))

Naturally, we followed the link. To our surprise, there were already subreddit subscribers… How odd. Some had even replied to posts in the subreddit. Looking back on that, I realized others were toying with us.

The creator and moderator of the subreddit was `CageThrottleUs`.

In the header of the subreddit, there were some Mayan numerals:

In the sidebar of the subreddit, there was a line that said “Verify: 7A35090F”. This same string also appeared in the title text of the Mayan numerals image.

All of the posts in the subreddit were complete gibberish — not a single was English, or any other discernible language. Evidently, some cipher had been used to mangle the text.

Among the [nonsensical posts](#) was one clear one, entitled “Welcome.” It linked to an image of a doormat:

From then, it was sort of a dead end, until one of us realized that we might as well try `outguess` on the doormat image. Bingo. This text came of it.

Since they announced that they would now always PGP sign messages, we'd know for sure if they posted something.

What is PGP? PGP is an initialism that stands for "Pretty Good Privacy." It's a form of encryption and identity verification, through what's called "public key cryptography." It ensures that no one can read a message except for its intended recipient. Signing is a way to ensure that anyone can read a message, and that it came from a certain recipient.

I promptly ran `gpg --keyserver pgp.mit.edu --recv-key 7A35090F` to download and import their public key. When I examined the key further, I noted that the UID (user ID) field was set to "Cicada 3301 (845145127)". This number, 845145127, was previously unseen. Same deal with Cicada.

From there, we began a full search on Google Books for reference on Mayan numbers, "Cicada 3301", and 845145127.

After hours of very well-timed posts every six hours, a post appeared on the subreddit, titled "Problem?". It had signed outguess text that gave a very vague hint about the location of the key, and a reference to the Holy Grail. One thing was strange about this post: it was posted by a different user, "ImagoOnNib".

At some point later on, however, we realized that ImagoOnNib is an anagram for Mabinogion, the title of King Arthur's story, and CageThrottleUs is an anagram for Charlotte Guest, the first person to translate the Mabinogion to English.

From the Mayan numerals in the header, the subreddit name (a2e7j6ic78h0j7eiejd0120), and the sidebar text, we derived the number sequence:

```
10, 2, 14, 7, 19, 6, 18, 12, 7, 8, 17, 0, 19, 7, 14, 18, 14, 19,
13, 0, 1, 2, 0
```

For example, each character and figure in the sidebar text can be interpreted as a sort of expanded hexadecimal to yield this sequence. We took the gibberish text from the subreddit, in the order posted, and performed a sort of hybrid Caesarr shift. That produced a segment of an Arthurian legend.

Example:

The first word of the garbage text is "Ukbn" — taking the first four numbers in the sequence and applying them in a manner similar to a shift cipher, we get this:

```
U - 10 = K
k - 2 = i
b - 14 = n
n - 7 = g
```

As you can see, we get "King" — the next word is "Arthur", and so on. When we ran out of numbers or started a new line, we started from the beginning of the shift key.

Then, we used the book codes (in the format `line:char`) to get a series of characters from the mass of text.

This was all computed using Python, on ideone.com (so we could easily share code and results).

At first, the text was a tad mangled, so we realized that there must be a formatting error. One of the errors was that Reddit removes excess spaces from posts, so that offeset

Naturally, we called it.

A computer-generated voice answered, and said, “Very good. You have done well. There are three prime numbers associated with the original final.jpg image. 3301 is one of them. You will have the find the other two. Multiply all three of these numbers together and add a .com to find the next step. Good luck.”

Here is a YouTube clip, posted by our very own `habitres`.

Turns out that the other two prime numbers referenced are the width and height of the first image. We multiplied them all together and added a .com to get 845145127.com (now down). On the website, there was a picture of a cicada with a countdown to 9AM PST/12:00 Noon EST/17:00 UTC on Monday.

Naturally, we ran `outguess` on the cicada image, and found this text.

At 17:00 UTC on Monday (expected), the site changed to a list of coordinates and this message: “Find our symbol at the location nearest you.”

The cicada.jpg also changed to contain a signed outguess text with the same list of coordinates.

We rallied people in the IRC channels, and found which were nearest to which coordinates.

One of the coordinates was located in Seattle, at Dr. Charles A. Rohrmann, Jr.’s house. We found his home and cell phone number on his medical profile, and called him.

It went something like this:

```
R: Hello. I am calling because a list of GPS coordinates were
posted online. One of them led to your house. Have you noticed
anything strange outside your house? Maybe suspicious people? New
buildings? People knocking?
Doctor: Where are you calling from?
R: London.
Doctor: How do you know about my house?
R: Like I said, there was a list of GPS coordinates posted
```

```
Doctor: Ive not had anything strange beside this call, no.
R: Nothing at all?
Doctor: No.
R: Well, people may come up in the future. They may ask about the
number 3301 or cicadas. Have you seen anything regarding either
of them.
Doctor: No I have not.
*Hangs up*
```

habitres's brother Bongo went do Sydney, Australia and found two pictures of a QR code. The codes scanned to images on 845145127.com.

manbearpig called the barber shop located at coordinate 4, posing as a student doing a geocaching project. He asked them to take a small look outside, but they saw nothing.

We outguessed some of the images that the codes linked to, and found this text. Another book code.

Another several images had different text.

The second pastebin referred to the poem Agrippa, by William Gibson. Wikipedia explains that, "Its principal notoriety arose from the fact that the poem, stored on a 3.5" floppy disk, was programmed to erase itself after a single use; similarly, the pages of the artist's book were treated with photosensitive chemicals, effecting the gradual fading of the words and images from the book's first exposure to light."

The full text is available here and the code to decode it here.

The book codes did not encode two characters, both of which were 6 - the first two primes (2,3) multiplied.

Decoding the text results in getting a .onion domain, sq6wmgv2zcsrix6t.onion. We all installed Tor and promptly logged on.

We were greeted with this screen:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Congratulations!

Please create a new email address with a public, free, web-based service.
Once you've never used before, and enter it below.  We recommend you do
this while still using Tor, for anonymity.

We will email you a number in the next few days (in the order in which
you've arrived to this page).  Once you've received it, come back to this
site and append a slash and then the number you received to this url.
(For example, if you received "3894894230934209", then you would go to
"http://sq6wmgv2zcsrix6t.onion/3894894230934209")

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJPCikYAAoJEBgfAeV6NQkPtCkQAIEa2HC20SduG8zWtH/0LSJ9
dnQLfjTI/MAPsnp0KXpzcQJ4p2UbNdRb5qtqp3HZQ5qwKK3b/MT+2eB5X+h5q5v/
bVOsPKXN7W+krTi8a2v5KA1fRj8mKcFTXkx9hdq6z6qeePVpeOGXeitU0jgO4uXu
1N9hor4AQFQoXvuELnlqS4YX+/nNgK+Y1Vu1ekvyn9LusidMpSxS/ciiZLD5d3Tl
TJeUOQzdw9TlUmmdeigfBRoqZDnm5UESnS8qS1vd7zg9Ulpw2GfCV8QQl0zWp0lS
KCrArG0Qg4K4shZRQ2BopGM95oFVw2pOnzYr9pp8kpipBWQ6URRF7IEcuG1k5fBt
sfiz7Eb7WWr4Cwk/1Ri625FMyo0Z2KDc1Wo8nkFXZ0/Xle6tyyhhJUZGRbZuHLau
LR5+oQEKKYTRrJFNhqswcXYsCQBBYM2XS+v3nbmTDVKyGNmMpp3/yC/RR91hQ7fr
FqMd5qHKSD0pc5tU5G29J+Ez3CDVN7E60Xy3I1I5ugGE8GP5DmqHn4k/x272lroX
BtiIRTh4f+ghcC6DLdPBc1PRAfLtRbpVR3GVTSCJ/EwBZrH4QJTEGcuXfPQryHbF
0BO795yyXxM61Q9QnU4dkAAQepKLHgcvDlrEJYJzMWo+BOCu7MChoOyo1Zq4eeuI
cPx04KJd4sGtMVWolA3/
=zGQW
-----END PGP SIGNATURE-----
```

Got it, thanks. We'll contact you soon.

Submit

(kudos to `Traveler`, another IRC user), with this HTML.

Everybody in the channel immediately registered tens of email addresses on mailinator. The site went down around Tuesday, January 10, 23:45 UTC, after many users had put in their email addresses.

The next day, `newcandy` discovered that 845145127.com had changed, and was now devoid of image and text. A quick look at the source revealed `<pre>` tags, with a lot of space between them. What was in between? Many tabs and spaces. We figured that this had to be binary, and decrypted it to find this text.

This was the first message not to be signed by `3301`.

About 2-4 afters after I grabbed them, the DNS entry for 845145127.com was changed to 127.0.0.1, and the previous IP (75.119.203.244) stopped responding to pings and TCP SYNs.

At this point, our story takes a darker turn. Our elite IRC group of 8 people deceived the rest, and led them on a wild goose chase. We created a branch off the puzzle, and led them solving unsolvable things. We distracted them so we would progress and they would not. We're sorry to announce that, but it's a necessary part of the story.

For those that missed round one completely: — ends with 3301 sending out emails. From here, a fellow named `n_` (not our `n_`) posted the URL `1853143003544.tk` in a chat room on n0v4, which was the sum of the largest number in each group here. Each group is the larger number, prime factored. The TXT record for that URL said "Go to my largest part". The largest prime factor of 1853143003544 is 33091839349, so we went to 33091839349.tk. This site had no TXT, but contained HTML with a black background and this image:

.

Someone (we still don't know who) found this text. Someone (again, we don't know who) identified the picture to be the bottom half ofthis poem.

I copied the typed version of the text, and formatted it so that it read like the image version. I created this code to read the book code from the text - then we got to cginiziglyaobyph.onion. We all registered multiple emails there. To our knowledge, 3301 began sending out codes at Friday, January 20th, 6:49 UTC, about 3-4 days later. *End round one, alternate.*

Somewhere between January 15th and January 16th the onion site (sq6…) came back up. Our emails came in at around 3:45 on January 15th. We put in our numbers at sq6wmgv2zcsrix6t.onion/NUM, which showed this message.

This message was served only once per number. People who shared their key or message got this by email.

We grabbed our 112 digit numbers (`n`, from the paste) and a server from voxel, and factored using `factmsieve`. It took about 7 hours, and only cost $8.

As of January 16th, putting any number into the onion gave a 500 error:

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, webmaster@cicada and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

.

On January 17th, at around 2:49 UTC, this was fixed, and could ake numbers. When given an RSA-decrypted number, it reported: “Correct. We’ll email you.”

A new email was sent, and told us to go back to the onion/NUM. This led to an updated version, having a poem/song and a PGP message.

The PGP message was a MIDI file.

We developed a procedure for un-puzzling the MIDI:

1. Take the base64-encoded portion of your message with the PGP armour headers around it, remove the “- “ from the beginning and top lines, and feed this into `pgp --decrypt habitres.midi > song.midi`.
2. Download `midiscv`, compile, and run `./midiscv song.midi song.csv`
3. Use this script to produce a message. This script matches the notes in track 3 of the MIDI file with the letter “chorus” at the top of the message with the MIDI in it. This produced a mapping as shown by #INSERT PASTE HERE
4. Using the mapping in reverse from track 2, we produce a message similar to:

```
very good you have proven to be most dedicated to come this far
to attain enlightenment create a gpg key for your email address
and upload it to the mit key servers then encrypt the the
following word list using the cicada three three zero one public
key sign it with your key send the ascii armoured ciphertext to
the gmail address from which you received your numbers your words
are word1 word2 word3 word4 word5 word6
```

the key to a PGP server (like MIT's), with `gpg --keyserver pgp.mit.edu --send-key [KEY_ID]`.

2. Run `gpg --armour --default-key [EMAIL] --sign --encrypt`, type your password, paste in the words you have, hit enter, then Control-D. It will print an ASCII armoured message.

3. Send that file to c99…@gmail.com, the one you've been receiving emails from.

At around Monday, February 6th, 3301 sent the first email. It explained that there would be no more puzzles. It gave directions to log on to a Tor hidden service, with a given username and password.

From there… we'll have to wait for the next one, I guess.

home

I stole some CSS from Better Motherfucking Website.