Comments to problematic challenges

This documents contains short comments for solution, where a lot of commanders had some difficulties.

Drone flight

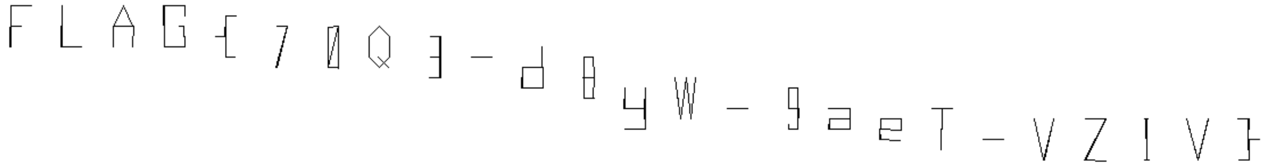
Hi Commander, we have intercepted a message, which has been addressed to a rebellious supersonic drone in laboratory of one famous Czech university and it contains "B-1084 START". The drone has already taken off and now it is beening monitored by our ground radar network. The achieved GPS coordinates have been recorded down, but it looks like purely random flight. You have to analyse the coordinates and find the hidden sense of this activity. Good luck!

This challenge has most wrong flag submissions. The problem was that a lot of commanders prefered speed before precision. Most of them use some goewebpages to display the trajectory of drone, that was quisk and easy. But the **Earth is not flat neither has a rectangular shape** and the drone orbited the earth almost three times and crossed the date line several times. Rectangular display of Earth caused that some letters were distorted (because of crossing the date line several times in both directions).

Next set of problems was **bad recognition of the letters**. Well... there was a relative long text, where the commanders can learn a lot about the font. Anyone can see that:

- The characters B, -, 1, 0, 8, 4 were mentioned in challenge assignment
- The characters F, L, A, G were clear because of format of the flag
- The characters in words “deceiving, mode, activated” were also clear
- The digits are half the width of the letters
- The space between characters is bigger than the character width

The intended solution was to write own script (python with PIL is ideal candidate), which will draw the trajectory. If only „letters lines“ are drawn („too long“ horizontal lines are omitted), this result will appear (only flag part is displayed for sake of better readability in this document):



What we have seen in the wild:

- Problems to distinquish characters 8, B and A (although all of them are known from previous text and the challenge assignment)
- Problems to distinquish characters Z a 7 (even when the horizontal lines are not removed, there is different width of characters)
- Problems to identify the last character V (because it intersects the date line and is distorted in rectangular display of Earth)

One wise old man said once “*If the quick and easy solution does not work, try something else*”.

Ice-cream selling machine

Hi Commander, our reconnaissance teams have discovered one of rebellious self-aware machine outside the library and identified it as smart ice-cream selling machine. It has some technical difficulties (we assume that the machine just has run out of ice cream) and started to call for help. Our wiretapping team has captured part of one attempt and we are sure that it contains special rescue code and we want it. Analyse the trafic and acquire the code. Good luck!

According to received several e-mails and some write-ups, there was no problem to extract the voice record in RTP protocol (some commanders used wireshark to extract/play it some hardcore commanders use scapy to extract it), but the transcription of the read text.

Well, the ICAO phonetic aplhabet was used, because it was invented because “assigned codewords allow that critical combinations of letters and numbers are most likely to be pronounced and understood by those who exchange voice messages by radio or telephone, regardless of language differences or the quality of the communication channel”. Big help is that all commanders were informed about the format of the flag.

Seventh element

Hi Commander, thanks to your discovery of the drone as a false target, our radars could concentrate on the detection of the second drone. This one was classic quadcopter and our trained falcon has caught it up and took it off the sky. The last broadcast was "Seventh element down, malfunction due claws and beak in propellers". The wreck has been completely shattered and just one operational flash drive has been rescued from the crashsite. According to the intelligence, we believe that the drone was ordered to transport some coded message to the elementary school library in city of Ostrava in order to create backup uprising centre. You have to analyse the content of the drive and decode the message. Good luck!

According to some write-ups and many e-mail questions, this challenge was little bit confusing for many commanders.

Well, the image contained 128 GPT partions, on most of them was one file *.file* (hidden one). Each file contained two hexadecimal encoded characters on first line and some hexadecimal number on the second line.

The intended solution was to identify that first line is data and the second one is link to next partition (some varion on linked list - this is also mentioned in the hint “*...They have everything linked.*”). Next, the first element has to be identified (the name of the challenge can help or you can use the knowledge of the beginning of the flag) and then follow the links and concatenate parts of the message. Decoding is easy, because all commanders knows that from the academy challenge.

We like the write-up with link analysis, where the situation is visualized by `dot`. This analysis of the problem is really exhaustive.

Colonel Roche

Hi Commander, did you know that the berserkers, which were assigned to specific tasks, have used to name themselves after humans famous in given field of specialization (this behaviour is maybe some bug in their firmware)? Our infiltrators - remotely operated classic devices equiped with stickers "I'm smart" and "Death to humans" - have discovered a new Berserker named "Colonel Roche", which is responsible for encrypting the commands for the other less or more smart devices. Your previous successes obviously forced the Berserkers to improve the security of communication. You are supposed to find some way how to decrypt a captured message and read the issued command(s). The infiltrators report that this particular machine usually use a day of week as a key (maybe "monday", maybe "saturday", maybe something else... they are not sure). Good luck!

This challenge was difficult, because Google has obviously joined the Berserkers! Or it was bribed by them. In late September, the query "*Jean-Baptiste Roche cryptography*" had returned links to several webpages with description of the appropriate algorithm. Now, only following webpage can be retrieved, but it is not so easy to create appropriate query:

http://knihya.cz/transpozicni-sifra-plukovnika-roche/

Author of this challenge has originally foud the algorithm in the book "*Kryptologie, šifrování a tajná písma*" written by Pavel Vondruška. Standard deciphering tools will not work, because this kind of cipher uses different size of columns.

Lesson learned: Next time, we will prepare own webpages with description of such curious algorithms or we will avoid it.