# 2,000 REACTIONS TO A MALWARE ATTACK – ACCIDENTAL STUDY

*Adam Haertlé*
BadCyber.com / ZaufanaTrzeciaStrona.pl, Poland

adam@zaufanatrzeciastrona.pl

## ABSTRACT

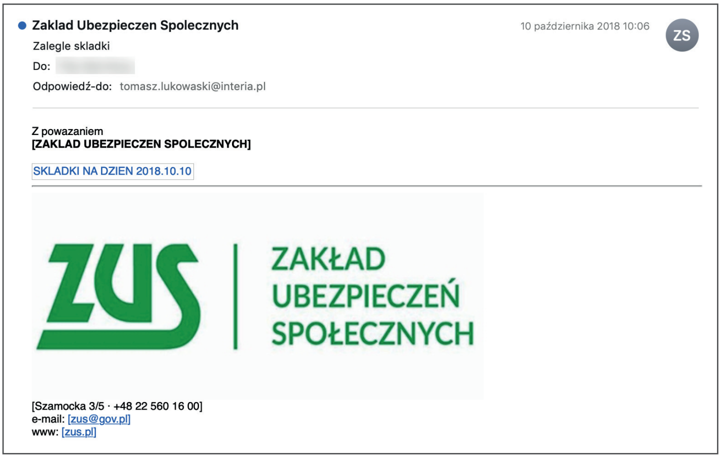
In this paper I present an analysis of 1,976 unsolicited answers received from the targets of a malicious email campaign, who were mostly unaware that they were not contacting the real sender of the malicious messages. I received the messages because the spammers, whom I had described previously on my blog, decided to take revenge by putting my email address in the ‘reply-to’ field of a malicious email campaign. Many of the victims were unaware that the message they had received was fake and contained malware. Some even asked me to resend the malware as it had been blocked by their anti-virus product. I have read those 1,976 messages, analysed and classified victims’ answers, and present them here. The key takeaway is that we need to train users, but at the same time we should not count on them to react properly to Internet threats. Despite dealing with cybercrime victims daily for the last seven years I was surprised by most of the reactions and realized how little we, as the security industry, know about the average Internet user’s ability (or rather inability) to identify threats online. We need to build solutions that will protect users, without their knowledge, sometimes against their will, from their ability to harm themselves.

## THE FIRST ENCOUNTER

It all started on 10 October 2018, when multiple users reported receiving a malicious email, pretending to come from a very well-known Polish organization – *Social Insurance Institution* (*ZUS* in Polish). The topic translated to ‘Overdue deposits’ and the content included the company logo and a link to – allegedly – a document containing information about those overdue deposits (see Figure 1).

The link to the document pointed to the *TinyUpload* file-hosting service, where a file named ‘Deposits for 2018.10.10.doc’ could have been downloaded [1]. I obtained the file and tried to open it in a potentially vulnerable environment, but the RTF exploit included in the file did not work as intended by its authors and I could not get the payload to execute. However, a friend of mine managed to extract the payload by hand and analyse it. It was supposed to open a *bit.ly* link, redirecting to another *TinyUpload*-hosted file in an attempt to execute it. The final payload at the time of the analysis included the Kronos trojan [2].

The authors of the campaign must have realized that their effort had failed, as the initial .DOC file was promptly removed from the file-hosting server (see Figure 2). Two more spam waves followed with the same subject, including links to *SendSpace*-hosted files, and there were more failed attempts at exploiting the RTF vulnerability via .DOC files. Based on the analysis of *bit.ly* link statistics at the time of the attack, I estimate that all those attempts failed miserably at infecting anyone.



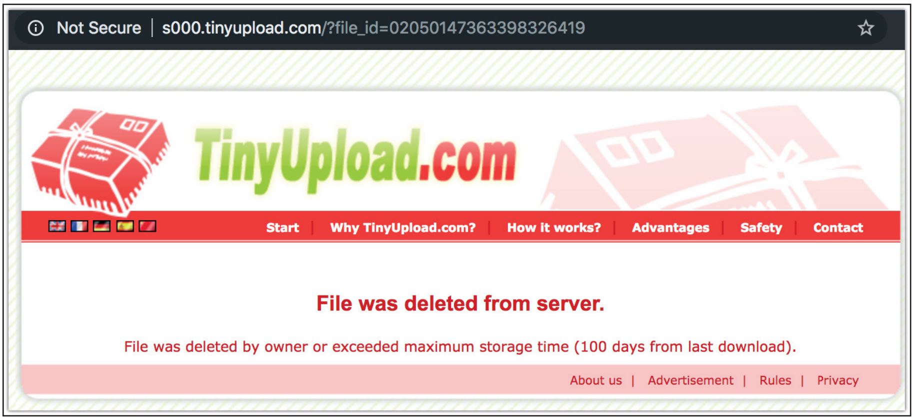
Zaklad Ubezpieczen Spolecznych
10 października 2018 10:06
ZS
Zalegle skladki
Do: [redacted]
Odpowiedź-do: tomasz.lukowaski@interia.pl

Z powazaniem
[ZAKLAD UBEZPIECZEN SPOLECZNYCH]

SKLADKI NA DZIEN 2018.10.10

[Szamocka 3/5 · +48 22 560 16 00]
e-mail: [zus@gov.pl]
www: [zus.pl]

*Figure 1: Social Security Institution campaign.*



Not Secure | s000.tinyupload.com/?file_id=02050147363398326419

File was deleted from server.

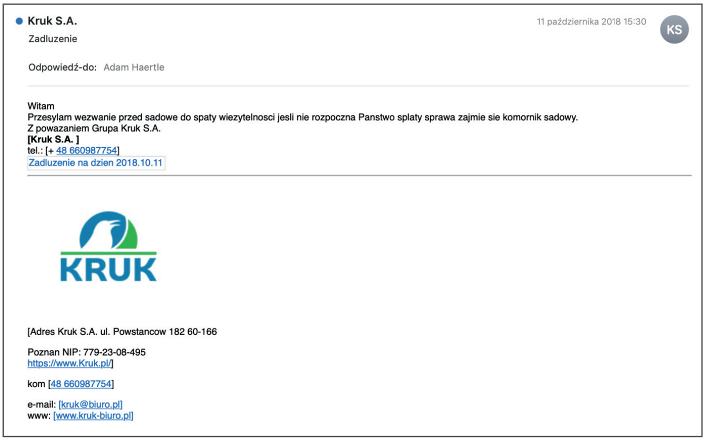
File was deleted by owner or exceeded maximum storage time (100 days from last download).

*Figure 2: File deleted by uploader.*

I described the campaign in a blog post on my security blog *ZaufanaTrzeciaStrona.pl* [3], ridiculing the authors of the malicious messages and their failed efforts. I did not have to wait long for an answer.

## THE BIG SURPRISE

The next day, at 2:14 PM, strange messages started to arrive in my private (not blog-related) mailbox at an unusually high rate. By the end of the day there were more than 1,000 of them, with more arriving in the following days and weeks. All of them were replies to a message I had not sent. The message everyone was responding to was another malware infection attempt, this time pretending to be an email from the largest debt collection agency in Poland, *Kruk*.



Kruk S.A.
Zadluzenie

11 października 2018 15:30

KS

Odpowiedź-do: Adam Haertle

Witam
Przesylam wezwanie przed sadowe do spaty wiezytelnosci jesli nie rozpoczna Panstwo splaty sprawa zajmie sie komornik sadowy.
Z powazaniem Grupa Kruk S.A.
**[Kruk S.A. ]**
tel.: [+ 48 660987754]
Zadluzenie na dzien 2018.10.11

[Adres Kruk S.A. ul. Powstancow 182 60-166

Poznan NIP: 779-23-08-495
https://www.Kruk.pl/]

kom [48 660987754]

e-mail: [kruk@biuro.pl]
www: [www.kruk-biuro.pl]

*Figure 3: Kruk debt collection agency campaign.*

The message topic was 'Liabilities' (in Polish) and the body included a short phrase which could be translated to 'This is the pre-court appeal, if you don't pay your debt a bailiff will take the matter in his hands'. The wording was only loosely formal (in reality it did not make any sense from a legal perspective) and contained multiple spelling errors and typos. Additionally, the link to the alleged document (the line of blue text just above the company logo) was barely visible.

If clicked, the link led to the *SendSpace* file-hosting service, to which a RAR file has been uploaded. The archive included a file named SKAN.PDF.EXE with similar characteristics to the final payload of the previous attack attempt [4].

I believe this message was sent by the same people as those behind the attack mentioned previously. This time they modified the 'reply-to' field to include my personal email address, which explains the sudden influx of messages into my mailbox. As a result, I received a total of 1,976 answers to a message I did not send.

I can only speculate about the attackers' motives for targeting me personally – either it was an attempt at ruining my reputation (probably causing account lockdown or removal by *Google*) or it was meant to serve as a kind of a warning ('we know your private email address'). They did not achieve either of these objectives – instead, they provided me with a unique opportunity to analyse real-life human interactions with the attackers and their malicious message.

## MESSAGE ANALYSIS

While I do not know the number of messages sent, I estimate, based on my knowledge of similar campaigns, that it was between 20,000 and 50,000. This means that the majority of recipients (between 90% and 96%) did not answer the message, which is the best reaction to a malicious spam.

I have excluded automated answers from the statistics as I wanted to concentrate on human reactions only. Of 1,976 answers received, 106 (5.67%) were identified as being automated responses (mostly 'this account is no longer active, please use another address' or 'this message has been read on [specific date and time]'). When we remove this subset from the general population, it leaves us with a total of 1,870 human messages to analyse.

I analysed all 1,870 answers by hand and divided them into 11 categories, based on the prevailing message included in the answer. Below you'll find category names with descriptions, numbers and examples.

1. The first group, representing the most prevalent answer (924 messages (49.41%)), was called 'CAN YOU EXPLAIN'. While not harmful in itself, it means that these recipients did not realize they were the subject of a malware attack. They did not identify the sender as bogus. They did consider the message as unprofessional, badly formatted and unusual, but they did not perceive multiple spelling mistakes and typos as a warning sign. They probably did not identify the link to download malware. They did not pay attention to the fact that the email address to which they sent their answer was not the same as the alleged sender. In short, they were tricked by the attacker into believing that the message was genuine. Some recipients believed it had been sent in error as they did not recall any unpaid debt, others simply asked for more information or a general explanation.
2. The second group was similar to the first one in terms of the meaning of the message, but they chose a different way of communicating their surprise. They sent just question marks. Some chose to send a single question mark, some used three, some spent some time typing, as their message consisted of 29 question marks. The messages did not contain anything but question marks. This group, called 'JUST QUESTION MARKS', had 46 members (2.46%).
3. The third group represented a different issue. These were recipients who complained about the fact that the message did not include an attachment or link to a document explaining the situation, while in fact the link was present in the message. The group 'WHERE'S THE ATTACHMENT' included 264 messages (14.12%). An alternative name for this group could be 'MISSED OPPORTUNITY'. The fact that the link to the malicious document was in some way obscured in the content of the message (or at least not easily observable) might have negatively impacted click-through rates, as one in seven recipients could not locate the link to infect their computer.
4. The fourth group went further. Much further. They must have located the malicious link, they must have clicked it, they must have downloaded the malicious document (SKAN.PDF.EXE) and double-clicked it, but they did not see the document they expected to see on their screens. I call this group, representing 220 recipients (11.76%), 'THE ATTACHMENT DOES NOT WORK'. This means that at least 220 people did, in fact, infect their computers while trying to open the alleged document file, as the executable file they were actually running did not show any decoy document, it just ran silently instead.
5. The fifth group is actually the most worrying. I call this group 'MY ANTI-VIRUS WORKED, PLEASE SEND AGAIN', as these are recipients who mention that their security product (mostly anti-virus) warned them against an infected file, but they wanted the file to be resent because they could not open it. The group consisted of 44 individuals (2.35%).

The next three groups probably did realize that they were targets of an attacker but did not draw the proper conclusions. To start with, they answered the email, when they should have ignored it, but they also made other mistakes.

6. Recipients in group number 6 decided to inform the sender that their actions had been reported to the authorities. While most mentioned reporting to the police, some also mentioned the prosecutor's office (which is also a perfectly normal way of reporting crime in

Poland). While reporting crime seems like a good way to handle these messages, I believe that most of the participants in this group did not actually report it. I draw my conclusion from the fact that a lot of these answers arrived within hours of receiving the original malicious message. It takes much longer to report a crime in Poland and has to be done in person. Additionally, none of the 108 members of the group I call 'REPORTED TO THE AUTHORITIES' (5.78%) provided any proof that the crime had been reported (e.g. a case number or a police precinct location). To make matters worse, most of the members of the group mentioned reporting a fraud, while the crime was in reality that of unauthorized access to a computer. These recipients believed that the aim of the attackers was to defraud them of their money under the pretence of an non-existent debt – such frauds happen very rarely in Poland (if at all – I have not found any publicly reported cases).

7. Messages from group 7 suggest that their authors did realize they were being attacked, and simply mention that fact to the attacker. The group 'I CAN SEE WHAT YOU DID THERE' had 54 members (2.89%). I have no theories about their motivation.
8. On the other hand, I have some theories about the motivation of members for the next group. I decided to call this group 'F- YOU', as that was the most prevalent content among the 110 messages that belong to this group (5.88%). These messages were very rude, with some impressive creativity displayed by their authors and were generally aimed at insulting the authors of the malicious message (while I was just an accidental recipient of the Internet hate). I don't think that spending one's time on insulting malware campaign authors is a good idea (they couldn't care less and the insult most likely will never reach them anyway), but I can understand the emotions behind these messages.

The messages in the last three groups have one thing in common – they were rather surprising.

9. Members of group number 9 decided to use GDPR as a reason their email should be removed from the sender's database. While the actual phrases they used did not show much understanding of the GDRP itself, the responses show that the 27 members of the group I call 'WHAT ABOUT GDPR' (1.44%) did not realize they were victims of a malicious message.
10. One of the biggest surprises were 31 members of group number 10 (1.66%) who spent time pointing out all the spelling errors and typos made in the original message. I call this group 'I'M A GRAMMAR NAZI'.
11. The most surprising group consisted of 42 people (2.25%) who mentioned their debts at various stages of maturity. Members of the group I call 'THIS IS RELEVANT' either mentioned that they had already paid their debts or promised to pay them soon. Some also revealed that they had already filed for personal bankruptcy. This group shows that, no matter what criminals put in their message, some people will always find it highly relevant to their current situation. It is even possible that the criminals persuaded someone to actually pay their debts, which could be a very unexpected side effect of a malicious campaign.

## NOTABLE ANSWERS

Some of the answers I received were particularly elaborate. There were a few essays with more than 100 words. The most impressive was a scanned letter from a lawyer. It was signed by hand and consisted of a few paragraphs explaining why the original message from the attackers showed their deep lack of understanding of legal procedure in Poland.

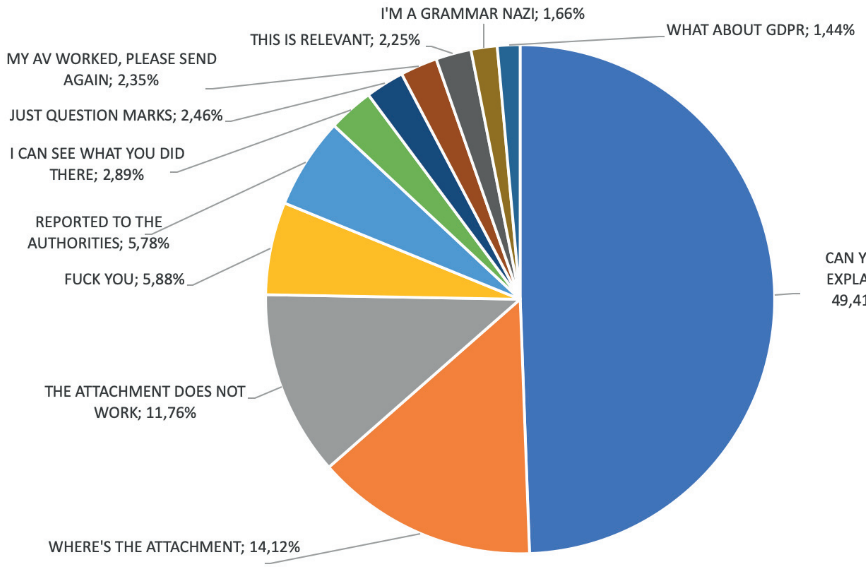


*Figure 4: Message analysis.*

The answers from self-declared experts were the most entertaining. I obtained some sound legal and technical advice. One of those experts explained (quite correctly) that PDF files do not need additional compression, as they have internal compression. While this is true in many cases, that expert did not realize that the RAR file served by the criminals actually included a PDF.EXE file, not a PDF. Another expert mentioned that I was unlucky as he was a lawyer and would make my life miserable. None of them realized that I was not the one who had sent the malicious message.

## SECOND WAVE

When I saw the first messages arriving in my mailbox, I tried to answer them by hand, but that soon became impossible as they were arriving much faster than I could answer them. Therefore, I set up an automated answer, based on the message topic. The text of the answer was as follows:

> ‘The message you received was an attack attempt. You’ll find a detailed description of this attack at [URL to my blog entry about this case]. If you downloaded the file, extracted it and ran it, I recommend turning the computer off and contacting an IT service which will help with malware removal or system reinstallation.’

This message was sent out to all 1,976 senders and, in turn, caused some of them to answer again. I received a total of 42 second-level answers (2.25%, excluding previously identified automated answers), which I also categorized for the purpose of this paper. Two types of answers dominated this time:

1. 21 (50%) messages thanked me for the information. Some also mentioned that they did not open the linked file. One person opened the file, but fortunately did so on a smartphone.

2. The other 21 message authors were genuinely confused. Some just said ‘f*ck you’, while others asked ‘so why are you sending this!?!’, and others suggested that I had created the attack myself and used my explanatory email to them as an excuse to attack them again.

## CONCLUSIONS

While educating users about potential threats online is as important as ever, the aforementioned examples clearly show that this is not enough. There will always be users who will fall into the trap set up by the criminals. Even if the trap is really primitive and obvious. Even if their anti-virus program warns them against it. Even if we, as security experts, tell them that they are being attacked, they still cannot understand what is going on and can easily become victims. The only way to help those users is to find ways to protect them against online threats without them being aware of the fact that they are under protection and – sometimes – against their own creative ways of harming themselves.

## REFERENCES

[1] https://www.virustotal.com/gui/file/0f58b5faf9a9a765a06ec644e8ea946a3099f41f3d1d7201ed02ac90a29d3b89/detection.

[2] https://www.virustotal.com/#/file/c48121bbaaa8353a6681b2e2aaa0245f3681c815c87d90fd8fb833061f67ff43/detection.

[3] https://zaufanatrzeciastrona.pl/post/masowy-ale-bardzo-nieudany-atak-podszywajacy-sie-pod-zus-analiza/.

[4] https://www.virustotal.com/#/file/ab7fe4362fd11795bf175709aa002fc9a4071d93463f37a6ec174d4946f4e882/details.