Custom Sample README

Welcome to the first custom malware sample in Zero2Automated! This first sample is fairly basic, and contains features covered in the past few chapters, with some additional functionality that requires a deeper dive into the binary. Your goal is to reverse engineer the sample(s), and figure out how they work! Automation is a huge aspect of malware reverse engineering, so maybe take a look and see if there's anything that can be automated? Such as automating the unpacking routine, extraction of any configs/IoCs, or emulation of the communications!
For those of you looking at the sample before the 15th of July, your goal is the same, however in order to compete in the blog post/writeup competition, you need to write up your analysis of the malware, including whatever automation tool/scripts you have written to speed up analysis. Points are awarded based on how in depth your analysis goes, and extra points will be given for automation and possibly some interesting approaches to analyzing the sample!
If you are looking at the sample after the 15th, you can still write up your analysis and send it over to us, or upload it online and we can take a look and give any pointers if necessary!
As you may have guessed, this is less of a CTF, and more of a real life situation - there isn't a flag in the binary that you're searching for, your goal is to document the functionality of the binary. This puts you in a real life situation, without the 6,000 functions to sort through to find a specific routine (such as malware families like Dridex or ZLoader), so hopefully it will be a good learning experience!
Anyway, enough of the backstory - let's get into the "story"...

Hi there,

During an ongoing investigation, one of our IR team members managed to locate an unknown sample on an infected machine belonging to one of our clients. We cannot pass that sample onto you currently as we are still analyzing it to determine what data was exfilatrated. However, one of our backend analysts developed a YARA rule based on the malware packer, and we were able to locate a similar binary that seemed to be an earlier version of the sample we're dealing with. Would you be able to take a look at it? We're all hands on deck here, dealing with this situation, and so we are unable to take a look at it ourselves.
We're not too sure how much the binary has changed, though developing some automation tools might be a good idea, in case the threat actors behind it start utilizing something like Cutwail to push their samples.
I have uploaded the sample alongside this email.

Thanks, and Good Luck!