Trojan+ransomware removal

Date :2023

This isn't that much a project , but rather an real life event , and real time reaction .

Here is the report I sent to the governmental cyber office:

hello ,

I am a computer science student , and very curious (maybe too much)

i am contacting you because I have been targeted by a ransomware I think imported by a Pitou Trojan(according to Malwarebytes)

here are the facts:

my machine : windows 11 xxxxxx , amd ryzen X

- *i downloaded a suspicious exe (greenluma: wanted to see how it works) which is making connection between cracked games and steam clients*
- *scan it with Microsoft defender (didn't detect anything)*
- *ran it*
- *as soon as I ran it I saw that my files extensions began to change to ".gatz" (at the beginning I was thinking it is only ransomware)*
- *I plugged out my computer from the network stop all the weird service and task*
- *Check the shell:startup and startup apps*
- *Check netplwiz (other users) nothing*
- *Reboot in safe mode*
- *I have another computer so I used it to active the oneDrive ransomware restore option (now that the infected is offline)*
- *Hard reset the main computer windows included*
- *Launch different antivirus : avira and avg (nothing)*
- *Began to setup my computer (and nothing got encrypted again)*
- *But then I receive a lot of OTP's notifications for all my accounts I understood that there wasn't only a ransomware*
- *I Install malware bytes*
- *Put it back in safe mode*
- *Then ran malwarebytes the only threats was some PUP in chrome data*
- *Found the rootkit option and ran it again (scan3.txt)*
- *And here is the first time that a got some result Bootkit.Pitou.MBR Hardisk 0*
- *After malwarbytes 's cleaning ran it again and no threat*
- *By security, my father who also learnt computer science send me(by drive we are not together) the desinfec't iso (antivirus ubuntu-based OS from the C'T tech mag) for cleaning the MBR*
- *I flashed it into a USB drive using the other computer then ran it into the main (infected) one*
- *The desinfec't returned a "no threat detected"*

- *Then I carefully reboot my computer in normal mode checking once for startup services*
- *Launch registry cleaner ,malwarebyte and Avast (which I discovered having an mbr scanner) all return "no threat"*
- *Re-plug internet checking scanning again for viruses*
- *During all this time I changed all my passwords using my phone and stored them using Bitwarden*
- *I checked all my social account for devices connected (from all over the world)*
- *Every thing seems to be ok*
- *This morning I finally receive the Ransome mail (900$ in bitcoins cf attachement pictures) I opened the pdf letter with a VirtualBox windows not attached to internet*
- I will attached all information I still have (some are lost because of reset including the virus file src)

- *Here is a possible source of the infected exe file:*
- *Cf BAD_LINKS.txt*
-
- *the file is just an exe file (maybe compressed but just the exe nothing else with it I think it's called "greenluma-2022.exe")*
-
- *These are some external (not mines) emails that was connected :*
- *//suppress the spaces*
- *xxxxxxxx @ yahoo . com → the one who ask ransom*
  xxxxxxxx @ hotmail. com
- *xxxxxxxx @ hotmail. com*
- *xxxxxxxx @ hotmail. com*
-
- *crypto BTC address:*
- *bc1ql944nnvkpw30uxv2hy7pzwc0p2lhwj5ss6gx62*
-
- *the screenshot is :*
- *one I took from the pdf*

This email is what actually happened step by step , it reflect my fast reaction decision making ,my curiosity for learning , and even if this period was one of the most stressful of the year , it is also one of the best because I learnt so much .