

Forum:[Hack Forums](#)

Thread: [Spreading silent miner with Rubber Ducky](#)

Buddy89 - March 11, 2023, 1:08 pm

So I bought the rubber ducky and it just recently came in mail. My plan was to have and use it as a learning experience as I am new to this stuff. I was wondering though could you spread silent miner with it and more importantly would it be even worth it? Like near my house there is this Eaport pc gaming place where they have like 20-30 very high end computers where you can go and play versus other people for money or just to play games. Would I be able to spread on the very high end games to silent mine gpu?

{ RadioActive Hack } - March 11, 2023, 2:20 pm

This is defiantly something that is achievable with the rubber ducky. I do not own one personally, so I do not have personal experience or knowledge regarding the device.

So there are two ways I can see that you could use to install the silent miner onto the computers. First, is writing a script to directly install the miner from its internal storage. I would assume this is possible, but I'm not 100% sure.

The second method in case it is not possible to directly pull the miner from the rubber ducky is to host the file online somewhere and write a script that downloads it from the internet and installs it onto the victim's PC. This is completely possible and not too hard to write. I don't know ducky script, but I imagine it would be very simple to achieve. There are surely some folks in the Hak5 community that would be willing to help you out.

Is it worth it? Hmmm probably not, to be honest, I think that miners are quite easy for A/V to detect, although I might be wrong. You would want to configure the miner so that stops mining while games are being played or have it running at a low capacity, so you do not indicate that there is anything nefarious going on by having games noticeable performance issues. Also, when the PC is idle you are still not going to want the miner running at full capacity as the GPUs fans running at full speed during idle is going to catch the attention of the administration staff, especially if you have infected the whole facility.

So if you can avoid A/V detection and raising suspicion among the staff it may be plausible. The only thing on top of that is that you will want to be very cautious of video cameras, it is highly likely that if the miner is discovered they will be able to determine the time that it was installed and check the cameras corresponding with the installation which would point them directly at you if it is visible. That is something you obviously want to avoid. You could possibly write a worm that when put on one PC would use the LAN to infect the others, this would be much hard to spot than you infecting all the computers by hand.

The question is would they think to check the cameras or assume it was downloaded from the internet? Possibly, possibly not.

Will it be profitable? Maybe, given the state of crypto atm and being in-between halvings the value of crypto is pretty low, so It wouldn't surprise me if you don't make much from this. You could hold onto the coin and when the bull market arrives at the next halving, it may turn into a nice chunk of change, but personally, I'm not aware of how much you can expect to earn. I know for me mining is not profitable at the moment and compared to earning about \$5-6 dollars gross a day in 2021 when I test a few days ago, I was only pulling in about \$0.30 a day.

I'm not even sure if the \$5-6 was actually profitable when you include electricity.

DramaKing - March 12, 2023, 4:22 pm

Sure, but it's somewhat of a waste on publicly-accessible computers. It's worth mentioning again that a miner, silent or not, will cause a noticeable impact on gaming performance. And that's if the company doesn't use Deep Freeze to reset any changes made by users, which I would certainly hope to be the case.

DramaKing - March 15, 2023, 1:35 pm

Keeping in mind my earlier advisories, store demo PCs would likely be easier targets than gaming cafes. They'll likely have fewer restrictions on installing software, and while they may not be gaming-focused, they should be barely used. I went to Wal-Mart yesterday, and the recon was promising. You can try the script that I wrote to setup XMRig and tweak it as needed. Just keep in mind that you may need to disable AV, either through normal means, PowerShell, or using a PowerSploit script. It's also possible that the AV trials such computers are set up with have expired. You may also need to do some form of privilege escalation, depending on the store, and how the computers are set up.

mert215 - December 9, 2023, 4:46 am

(Mar 12, 2023 04:22 PM)DramaKing Wrote: [\[CITE\]](#) Sure, but it's somewhat of a waste on publicly-accessible computers. It's worth mentioning again that a miner, silent or not, will cause a noticeable impact on gaming performance. And that's if the company doesn't use Deep Freeze to reset any changes made by users, which I would certainly hope to be the case.

Any idea or method for bypass deepfreeze?

DramaKing - December 9, 2023, 6:55 am

(Dec 9, 2023 05:46 AM)mert215 Wrote: [\[CITE\]](#) Any idea or method for bypass deepfreeze?

Deep Freeze uses a kernel driver. You can't just bypass it, not without breaking the OS certainly. And today companies are generally using Deep Freeze Enterprise, which is centrally managed. Guessing a password won't help.

Kayskop - December 17, 2023, 3:56 pm

It's possible, but I wouldn't recommend it, as spreading online would be easier and more anonymous.

yuulii - January 28, 2024, 8:51 am

Hii guys,

I have my own methods of accessing over 3000+ computers now. If there is anyone with a good hidden script that will not be detected by AV's, we can do a partnership and use my resources. DM me