#Encryption as protection against Malware

##What happens when an attacker gets control of your computer?

When an attacker gets control of your computer, they have access to your sensitive data. They can destroy anything they can get their hands on. For others, it’s a bump in the road. Encryption makes losing control of your computer a lot less of a threat. Don’t mistake what’s being said. It’s still a bad scenario, but at least the access to the files on the computer has a level of protection that antivirus software can’t guarantee.

There is a downside to this, “encrypted traffic of any sort cannot be scanned by firewalls, anti-virus software, mobile scanning software, or anything designed to act as a virtual border guard for data traffic.”[^1] This is one downside to encrypted traffic because it’s made to look harmless by design. The same goes for encrypted malware, persisting because it seems like regular ordinary data.

The lesson is that if you forget the key or lose it, you will be unable to access that data. Encryption is a double-edged sword, but it is a necessary evil from an enterprise perspective, and the benefits outweigh the costs. Disclaimer: That does not mean you should encrypt everything.

Only encrypt what is necessary, and leave the rest to the wolves.

##How to encrypt your hard drive

How do we encrypt our hard drives? It’s simple. Find a program, paid or free, and encrypt it. How do you know what program to use? There are hundreds of programs on the internet, and many of them seem sketchy. The best resource in this situation is the court of public opinion. Find trusted ones with a good history and plenty of users to tear its weaknesses to pieces in front of a live audience. Later on, in the lesson, I will go over some examples, and there are others that you can use, so don’t take my word for it. Try and test some of your own.

I’ll break down the process in some easy steps to give you an idea of what to expect:

* First, you’re going to select the drive/folder/file you want to encrypt.
  + Be sure that you encrypt files that work in tandem. That way, you don’t need to permit them to work with one another.
* Second, generate a password or do some action that creates a randomly generated key.
* Third, the program will use that key and a public key to encrypt the hard drive.
* Fourth, you will then be prompted to enter the key any time you want to access that file on the computer.
  + Some programs may have the ability to store the key on an external USB. This method prevents keyloggers from figuring out the password quickly. Other programs will keep the key encrypted on the computer and use it to verify your identity when you enter the password associated with it.

You can also find a video below going into a little more detail about the process of encryption![^2]

(Encryption and public keys)[https://www.youtube.com/watch?v=6-JjHa-qLPk]

##Programs that help with hard drive encryption

So then, what programs should you look for? They come in two general categories, paid and free. You might be thinking, “Ah, well, it’s free, which must mean that it's bad.” Not necessarily. Many encryptions are handled through the random generation of large prime numbers. This is so that when the private key is crafted, the resulting merger between private and public keys is hard to crack. This large prime leads to solid encryption that can be stupidly difficult and expensive to break.

Because of the nature of encryption, plenty of open-source software created has viability for encryption. It’s just a matter of permutations and combinations. Remember, when it comes to passwords, the more options there are, the better. Most passwords operate off a value where m[^n] is some exponentially large number that would take time to go through the possibilities.

Sometimes the best thing to do is to use encryption in communication. In that instance, “all you need is a digital certificate, which Outlook will automatically help you find” [^3].” Programs built into the everyday lives of corporations, big and small, will allow you to encrypt your emails and protect your information.

###Free Programs vs Paid

Paid programs have their benefits, namely features and reputation. With features, you can have the option to have more devices encrypted, ultimately lowering the cost and improving your security. Often, this is the solution that large companies are attracted to. They also have a reputation, which means that they have recognizability, and that reputation backs up these means of encryption as a choice. Another thing that they have going for them because their profit means that they have a bigger team and more technology to work with. The downside is that a corporation will have to work especially hard to ensure that what it is they’re encrypting turns enough profit to pay for the service.

A company can use free programs and as many of them as you want, but there’s no connection between the encrypted devices unless the company using it builds one. The only reputation that it can rely on to tout its success is its encryption algorithm's computational difficulty. The second that they break the free encryption is the moment that a company is forced to move on to a different solution. Another issue is that the programmer may not guarantee upkeep and continued development. If a person programming encryption software decides to move on to another project, there could be no disclosure of that to a company which means that they are now left with old, outdated encryption software.

Below is an example of a free program you can find because asking you to purchase a program to try out seems unacceptable.

##Free Example

###What is (VeraCrypt)[<https://veracrypt.fr/en/Home.html>]?

VeraCrypt is free software that enterprises can use to encrypt. VeraCrypt is self-reported software claiming to be brute force proof. The Fraunhofer Institute for Security Information investigation performed a year-long analysis of the program for the Federal Office for Information Security[^4]. To summarize, this is what they used to analyze the program:

* CPPCheck: A tool for static analysis of C/C++ code.
* TScan Code: A tool for static analysis of C/++/# and Lua code.
* Clang: I’m sure you can guess by now.
* Clang-Tidy
* VisualCodeGrepper
* Cpplint

These programs are run on static versions of the code. This term means nothing is running, so you don’t get a view of it in run time. Nothing changes when the institute performs Dynamic code analysis where the program is running. Below I’ll list the programs they used for dynamic analysis. Why am I listing all these programs? Find a program you like and try running them. You may be surprised at the vulnerabilities or syntax errors you find.

* Dr. Memory
* Valgrind

Ultimately, for the syntactically incorrect program that it is, VeraCrypt passes the Fraunhofer Institutes’ tests. It remains a working program that fixes some of the issues of its predecessor. By no means is VeraCrypt perfect, it still has several persistent problems present in TrueCrypt, but ultimately, it still functions as a reliable program for encryption.

#Works Cited

[^1]Kerstetter, J. (1999). IT’s cryptography conundrum. *PC Week*, *16*(28), 10.

[^2]Kahn Academy. (2019). *Encryption and public keys*. *YouTube*. Retrieved April 16, 2022, from https://www.youtube.com/watch?v=6-JjHa-qLPk.

[^3]Krause, J. (2005). D-I-Y Security. *ABA Journal*, *91*(2), 56–57.

[^4]Evkan, H., Lahr, N., Niederhagen, R., Petri, R., Poller, A., Roskosch, P., & Tröger, M. (2021, January 30). *Security evaluation of veracrypt*. Federal Office for Information Security. Retrieved April 16, 2022, from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Veracrypt/Veracrypt.html