3. Акименко, К.В. Основы таможенного права: учебно-методическое пособие / К.В. Акименко, А.Ю. Жевлакова, Н.Н. Панкова. – Минск: “Право и экономика”, 2021. – 221с.

BLACK MINING. HOW TO PROTECT COMPUTERSFROM CRYPTOVIRUSES
ЧЕРНЫЙ МАЙНИНГ. КАК ЗАЩИТИТЬ КОМПЬЮТЕРЫ ОТ КРИПТОВИРУСОВ

Чепикова Д.А.
Научный руководитель: ст. преподаватель Кажемская Л.Л.
Белорусский национальный технический университет

Today, the concept of "mining" has already managed to light up on the pages of narrow-profile economic or IT publications. Mining (from the English "mining of minerals") - the activity of creating new structures to ensure the functioning of cryptocurrency platforms [1].

Wherever there are rules, there are those who want to circumvent them or break them. The world of cryptocurrencies is no exception, because modern miners have already developed methods that will allow you to receive digital currency through computers owned by other people. So, there is black mining-illegal mining of cryptocurrency.

There are two types of black mining that involve other people's PCs: browser mining and virus mining.

Browser mining works if your PC enter the cryptocurrency mining network. Let's say it is a website that decided to mine cryptocurrency on the resources of visitors. The site begins to use the power of the user's video cards, while they, unsuspectingly, continue to use the site. Although the output of such mining is not particularly large, the attackers take the number of visitors. The first to catch such an "experiment" was the Piratebay torrent tracker. The site users themselves noticed something wrong – when visiting the torrent, the load on the processors increased to almost one hundred percent.

Unlike classic viruses, which simply steal and forward information from a computer, mining viruses use its technical power. A malicious program can get into a computer in two ways: together with various installation files (when the virus program disguises itself as secure program components or various activation keys), or as a result of an attack on the server. Viruses can do more damage to the PC than browser mining, but browser attacks are exposed to much more computers. With daily use, the computer runs at 20-30% of its power, and with black mining, the machine accelerates to 80-100% [2].

The miner program loads the user's PC and its graphics card to the maximum. There is another minor feature of the virus miners - the additional service of the virus. The service ensures that the main pirated program is fixed in the computer system, its autorun when the computer is turned on, and also monitors security. Such an additional service is often responsible for ensuring that the computer activity monitoring program does not detect a pirate miner, so it suspends it work in time. In particular, the suspension of the virus can occur at the time of launching the utility, for example, to check the loading of the video card. In addition, the same service checks for the presence of the miner on the hard drive, prevent it from being deleted and restore it after deletion [3].

As a rule, the fact that your PC was attacked by black miners, indicates its slow operation. When the computer starts to slow down when visiting a particular resource, then, most likely, black miners used your browser. You should pay attention to how the technology works on those sites that provide for a long pastime: torrent trackers, online games, and movie sites. Similarly, black mining inevitably leads to an increase in electricity consumption.

How to protect yourself from browser mining? To date, there are a number of effective measures that will help protect your PC from virus attacks through the browser. Among them are the following: editing a file called "hosts" if the addresses of malicious sites are known; installing the "Anti-WebMiner" utility and the "NoCoin" browser extension; to disable JavaScript in the browser and apply "NoScript"; adding anti-mining protection to "AdBlock", as well as "uBlock".

How not to catch a miner virus? There are a number of rules that will protect you from the activities of black miners:

1. Never download unlicensed programs or applications to your computer. Also, avoid entering activation keys from questionable sources and never use unverified links;

2. If you are the owner of a PC that was made by Apple, you should set the option in the settings, which implies downloading only software products from the "App Store";

3. If you prefer the OS "Windows", you need to create an account and boot the computer only through it;

4. In the event that the PC has become very slow, use the "Task Manager" (you may be able to detect the very utilities that take up 80-90% of the processor power), contact the service [4].

As you can see, black mining has become a serious problem with the development of digital technologies that is why this problem is common in all countries with a developed IT sphere. In order to overcome this problem, it needs to be fought not only by ordinary users and antivirus programs, but also at the state level with the help of laws.

Литература

1. Википедия. Свободная энциклопедия. Майнинг. – [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Майнинг. – Дата доступа: 31.03.2021.
2. Чёрный майнинг: как зарабатывают деньги через чужие компьютеры. – [Электронный ресурс]. – Режим доступа: https://lifehacker.ru/chernyj-majning/. – Дата доступа: 28.03.2021
3. Черный майнинг: с миру по монетке. – [Электронный ресурс]. – Режим доступа: https://sputnikabkhazia.ru/world/20171025/1022226065/Chernyj-majning-s-miru-po-monetke.html. – Дата доступа: 25.03.2021.
4. Черный майнинг: как защитить свой компьютер и не стать жертвой мошенников. – [Электронный ресурс]. – Режим доступа: https://ria.ru/20170907/1502026690.html. – Дата доступа: 21.03.2021.

LES CENTRALES NUCLEAIRES
АТОМНЫЕ ЭЛЕКТРОСТАНЦИИ

Беганская В., Абметко Н.
Научный руководитель: ст. преподаватель Ходосок Е.В.
Белорусский национальный технический университет

Dispositions générales. Des centrales nucléaires – il s'agit essentiellement des centrales thermiques qui utilisent l'énergie thermique des réactions nucléaires.

L'occasion de l'utilisation du combustible nucléaire, principalement de l'uranium 235U, en tant que source de chaleur est liée à la réaction en chaîne de la fission de la substance et de la sélection lors de cette énorme quantité d'énergie. Auto et réglable réaction en chaîne de la fission nucléaire de l'uranium est assurée dans un réacteur nucléaire. En raison de l'efficacité de la fission des noyaux d'uranium 235U lors du bombardement de leur lents neutrons thermiques jusqu'à dominé réacteurs sur la lenteur des neutrons thermiques. En tant que combustible nucléaire utilisent généralement un isotope de l'uranium 235U, dont le contenu dans l'uranium naturel est 0,714 %; la masse principale de l'uranium en isotope 238U(99,28%). Le combustible nucléaire utilisent généralement sous forme solide. Le concluent dans le shell. Ce genre d'éléments combustibles appelé lit de boulets, ils sont placés dans le travail dans les canaux de la zone active du recteur. L'énergie thermique émis lors de la réaction de fission, est évacuée de la zone active du réacteur à l'aide de liquide de refroidissement, qui est pompé sous pression à travers chaque canal de travail ou de la zone active. La plus courante caloporteur est de l'eau, qui est soigneusement nettoyé.