Cyberwatch Finland

WEEKLY REVIEW

WEEK 6/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

1. The resilience of Finnish society against denial-of-service attacks has developed.

2. The security risk of push notifications can materialize in the form of information leaking to outsiders.

3. Tracing cryptocurrencies is an area of cybercrime investigation where authorities seem to be evolving.

1. DDOS ATTACKS LOSING IMPACT

In the first days of February, Finland experienced yet another wave of distributed-denial-of-service attacks, perpetrated by the already familiar Russian group NoName057(16). This actor, which considers itself a patriotic Russian hacktivist operator, constantly carries out these attacks on targets around the world. They are often timed to nationally significant days or moments when momentary service interruptions would receive as much attention as possible. In Finland, the attacks coincided with strikes in many sectors and demonstrations against government policies. The hacker group itself also stated that the reason for the attacks was "supporting the Finnish people against the actions of a government that pours money at the criminal government of Ukraine and abandons its own citizens." The attacks lasted for a couple of days until the group, as usual, moved on to the next country. On the third of February, the group's Telegram channel was already full of posts about France's criminal support for Ukraine and how the country's authorities and businesses will tremble under a wave of DDoS attacks.

DDoS attacks are nothing new, and NoName's operations seem to have lost their effectiveness in Finland as well. The primary objective of attacks is to attract attention and increase national uncertainty, but it seems that DDoS attacks are already used to and understood as low-level interference as opposed to dangerous cyberattacks. Of course, the media picked up on the wave of attacks, but the news coverage was not sensational, but rather the style seemed to be to convey information about what is going on and what DDoS attacks mean. This is not only natural, but also important. Media has to highlight such a large wave of attacks, as a result of which the websites of several cities and major companies are simultaneously disrupted. Citizens should be kept aware of denial-of-service attacks, especially coordinated waves of attacks such as this one, even if the actual impact of attacks is both short-term and minor. If this would not happen, the attackers' objective could be much more successful when citizens would find that everyday services are not working without knowing what is really happening. It seems that Finland's national resilience to this threat has increased and denial-of-service attacks will not achieve the effect that the threat actor seems to want from them.

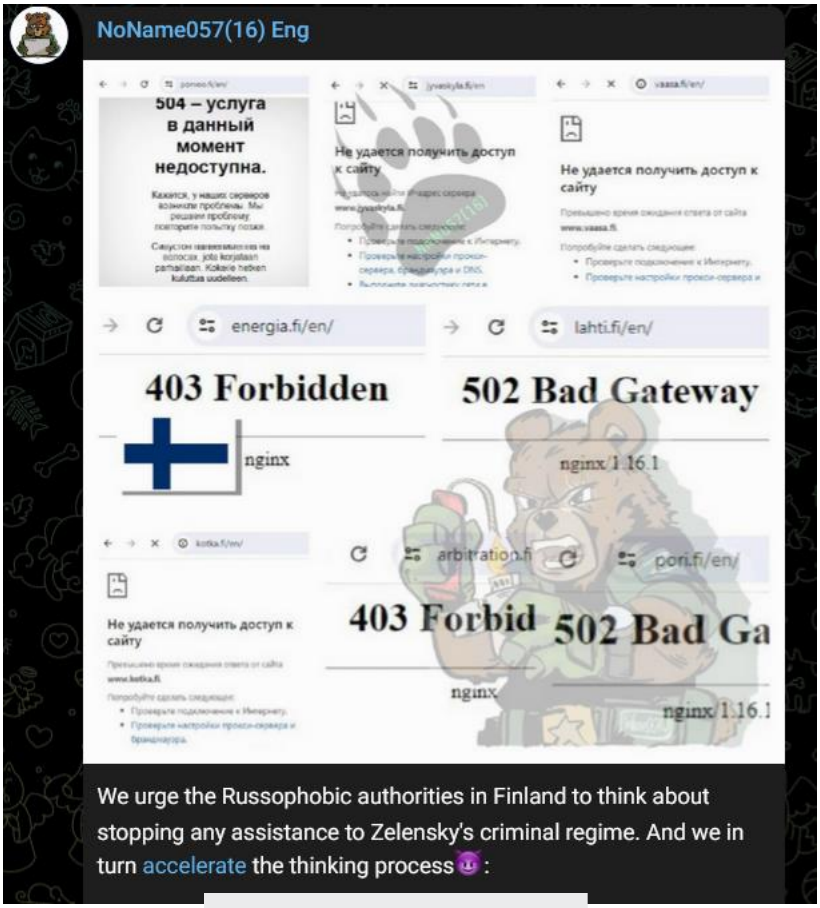
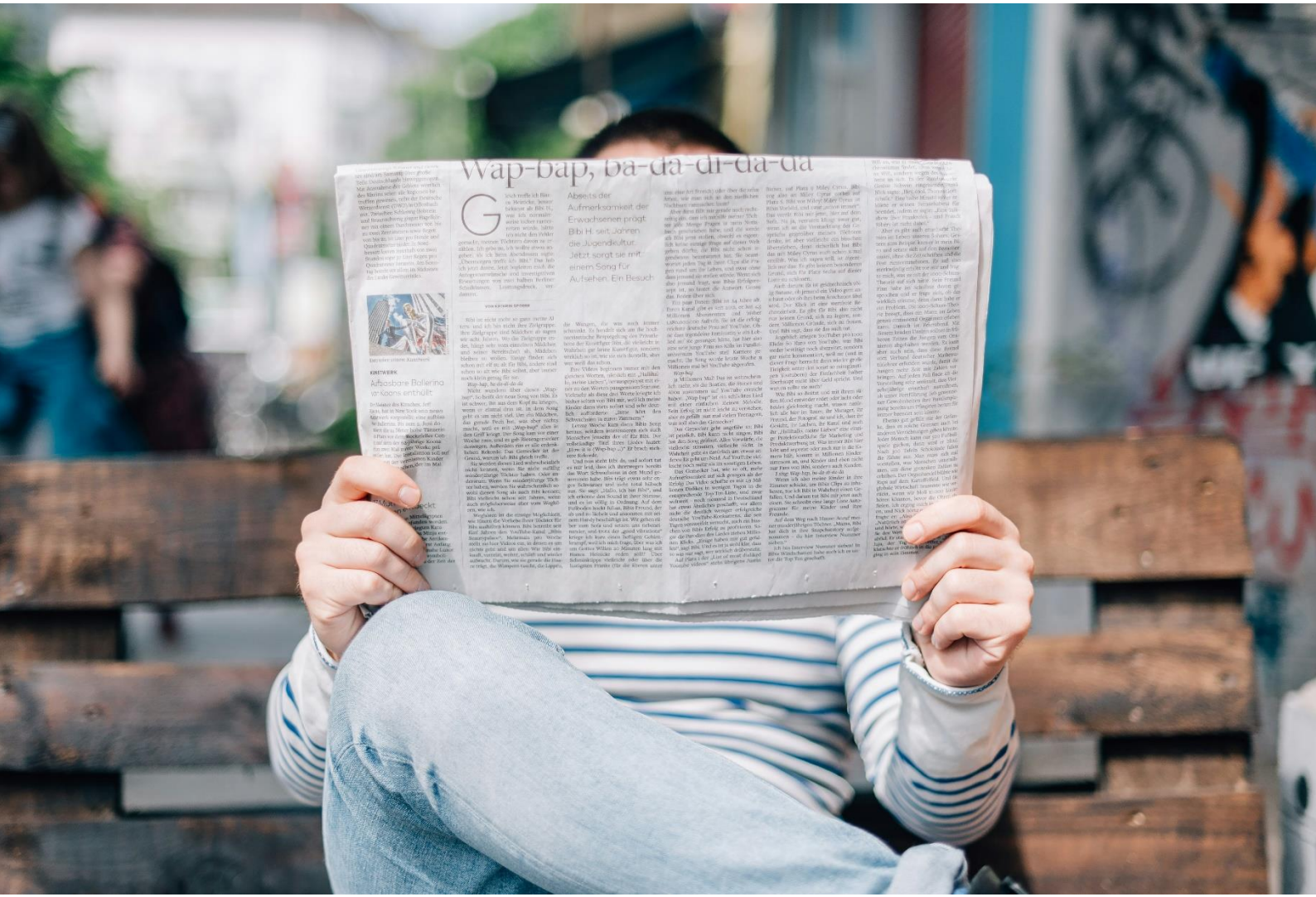


Image taken from Noname057(16)'s Telegram channel 2nd of February.

However, it should be noted that the value of denial-of-service attacks as a tool for influencing information is not only directed at the citizens of the target country. Especially in the case of a group that publicly announces its operations, such as NoName057, communication with those who support the group and its cause and followers of its social media channels is also essential. Pictures of the targeted websites being down are posted rapidly on these channels and posts are full of descriptions of how the lives of the citizens of the target country are made much more difficult due to their actions. This will help maintain the impression that the West is constantly suffering from Russian cyberattacks, and possibly even encourage new hackers to join the patriotic cyber front. NoName057's Telegram channel also posts a lot of borderline false reports of attacks that in reality did not significantly affect the availability of the target service or were not even noticed in the target country. For example, in the last week of January alone, the same group had reported attacks on Finland in three different batches, allegedly targeting the National Cyber Security Centre, the Ministry of Justice and the Helsinki Chamber of Commerce, but these events did not even cross the news threshold in Finland. Admittedly, these most likely have been operations carried out with less intensity. This can also be indicated by the fact that no attempt was made to date them to socially significant moments. Still, the group announced them on their channel with the same boisterous energy as the attacks in early February.

However, DDoS attacks are not entirely harmless. They can also cause real harm if they can be timed at times when access to information about the targeted services would be very critical. For example, DDoS attacks timed to coincide with crises or other exceptional events may be effective in promoting uncertainty, even if we know exactly what they are about. Although in general they do not pose a significant threat, one should not be lulled into an apparent sense of security or the idea that one is completely protected from influence. Attacks should be understood in many different ways as a tool that serves the objectives of information influencing. They are unlikely to disappear from the cyber environment of Finland or Western countries, which is why we must both get used to them and prepare for them. On the positive side, however, the impact of attacks is constantly diminishing as organizations develop their ability to maintain operations when attacked, and citizens become more aware of what attacks are about.



Cyberwatch Finland

2. SECURITY RISKS OF PUSH NOTIFICATIONS

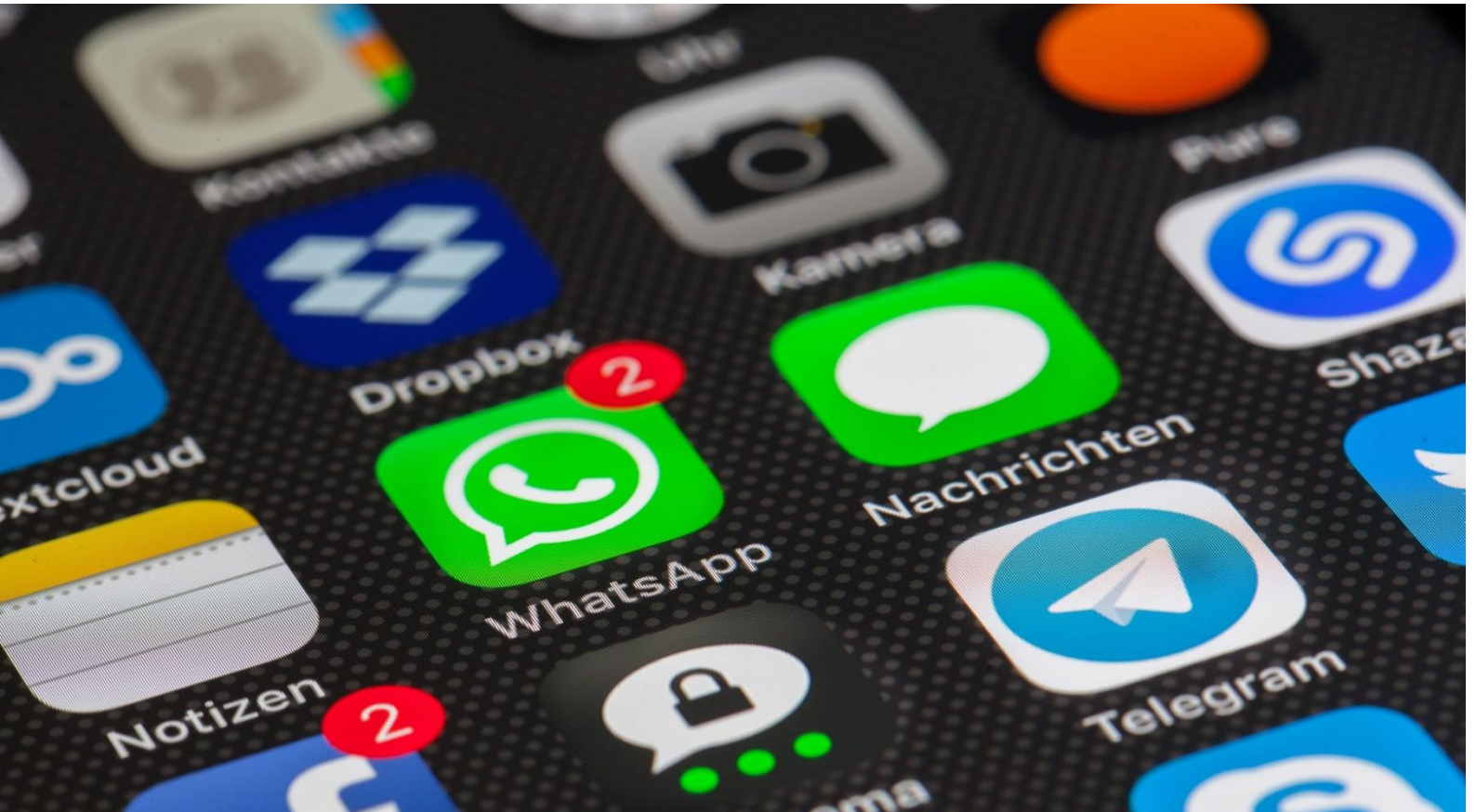
Security of smartphones affects practically everyone. Phones are important to their users in everyday life, as they are used to handle many daily tasks. Therefore, they also contain a lot of information about their user through different applications. Recently, a new threat to smartphone security emerged regarding push notifications. Push notifications are notifications that pop up in your phone's notification center or screen, and in some cases do not depend on whether the application that sends them is running. These notifications are sent by, for example, messaging apps when notifying them of a new message, or news apps depending on the permissions you have given them. However, several cyber risks associated with push notifications have been raised recently.

The first of these dates back to November last year, when US Senator Ron Wyden's letter to the US Senate received widespread attention. Major media outlets such as The Washington Post and Reuters also picked up on the topic. According to Wyden, push notifications provide a way for state actors to spy on phone users. The threat would consist in the fact that information in push notifications, depending on the device and operating system, circulates through Google or Apple servers and is often not end-to-end encrypted. This information could include metadata, such as the time, source and destination of the push notification, and would probably be of interest to security authorities in different countries. This data could be (and have been) requested by security authorities to be disclosed by Apple or Google. This would allow, for example, app users to be linked to specific Apple or Google IDs. The major corporations themselves have commented only sparsely and vaguely on the allegations, and Senator Wyden did not reveal the source of his information either. This makes the actual threat of risk difficult to assess. However, it should be clear that every user would like their data to be as protected and secure as possible from outsiders. For example, The Washington Post reported that it had found several search warrant applications from U.S government actors for push notification data. Apple has since announced that it will only release data in exchange for a court order.

Thus, in the approach proposed by Wyden, a threat manifests when an application sends a notification to an Apple or Google server that a specific user has been notified. Another way in which a threat can be triggered and user data leaked comes from the applications themselves, not the operating systems and their hosts. Last week, security publication Bleeping Computer published news about applications that exploit Apple's iOS system interfaces, where when a user clears a notification, information about the device is sent to the application that sent it. This information may include, for example, information about the last restart of the device, keyboard language, available memory, and a handful of other device specifications. It has been feared that this will enable user profiling and thus more extensive monitoring. According to the source, this kind of data has been collected by popular apps such as TikTok, Facebook and LinkedIn. However, the problem will likely resolve itself, as Apple is reported to be making changes to its API in spring 2024. As a result, apps should accurately disclose what data they are retrieving from the device and for what purpose. If they do not act on this, there would be a risk of completely shutting down applications from Apple's app store.

A third way for the cyber risk of push notifications to materialise is popular with cybercriminals, but requires that the user's credentials have already fallen into the wrong hands. The so-called "push attack" aims to circumvent multi-factor authentication through social engineering. In services using multi-factor authentication, the second stage of authentication is often linked to the user's phone, in which case after entering the username and password, the login must still be approved through a notification on the phone. Threat actors can schedule a login attempt to send a confirmation notification, for example, at a typical start time for work, or try to tire the target person with repeated notifications, one of which they eventually accept, in order to silence the phone.

Protection against the first two risks in particular is challenging for the average user, as the only way to do this at the moment is to block pop-ups completely on the device. This may not be very practical, as notifications are often also necessary and useful. In the first example, the user's risk of being subject to a request for information from government authorities via push notification data is also likely to be small. As for the second risk, Apple's new rules in particular should tackle the problem. When it comes to push attack, the user should stay alert and always be aware of what they are doing with their smartphone. The golden rule of smartphone security is the idea that information you don't want leaked should never be handled on your smartphone. Not all sensitive conversations, documents, or IDs should be accessed or stored on a smartphone. Although these risks do not necessarily materialize through push notifications, the phone may fall into the wrong hands or data security may be compromised through other means. It is always worth emphasizing that smartphones are still at risk for cyber espionage and must be used accordingly.



3. CRYPTOCURRENCY TRACING IS DEVELOPING

At the end of January, the court proceedings concerning the data breach at the Psychotherapy Centre Vastaamo took an internationally noted turn when the Finnish National Bureau of Investigation (Keskusrikospoliisi, KRP) announced that it had succeeded in monitoring the suspected extortionist's financial transactions, which took place using the Monero cryptocurrency. Monero is a popular cryptocurrency among cybercriminals because, unlike for example much better-known Bitcoin, Monero transactions do not store sender and receiver information on an openly available blockchain. In practice, this means that Monero offers its users significantly stronger privacy protections. As a result, currency transactions made with it have been considered impossible to trace. The KRP's claim that Vastaamo has been able to trace currency transactions in connection with the investigation has naturally attracted attention both in the media and in the forums of cryptocurrency enthusiasts. Successful tracking has even been described as a breakthrough in cybercrime investigations, as Monero traffic has so far made it very difficult to establish a link between criminally obtained cryptocurrencies and criminal wallets.

There is no exact information on how the KRP has succeeded in this stunt, which is considered impossible, because in order to safeguard police techniques, precise information has been removed from the published records. However, it is known that a significant part has been played by money transfers in which the suspected blackmailer has converted ransom-paid Bitcoins into Moneros and later back into Bitcoins. It seems likely that instead of decrypting the Monero blockchain, the KRP has managed to connect with a satisfactory probability the bitcoin wallets that have been at different "ends" of Monero transactions. The Monero community has long been aware of the possibility of this kind of tracing, but it has been seen mainly as a theoretical possibility. While detailed information is not available, the achievement should not be underestimated, even if it is not "tracking an untraceable cryptocurrency" in the strict sense of the word.

Tracking cryptocurrency trails is undoubtedly one of the most significant challenges in solving cybercrimes. Therefore, any progress in this area is valuable. Criminals have many different tools at their disposal to make tracking more difficult and to launder cryptocurrencies acquired through criminal activity. Often, it is tracking the traces of money that is the wall that comes up in investigations. Even if criminals are successfully identified, it can be considerably difficult to recover money obtained through extortion, for example. In addition to currencies that are difficult to trace, such as Monero, criminals have other ways of complicating the work of the authorities. For example, the use of various crypto mixers is particularly popular. These specialized services receive transfers from multiple sources, mix currencies, and then distribute them back to new accounts managed by the original users. In practice, therefore, a criminal can transfer currency to himself or his partner through a mixer. Along the way, the money is usually mixed with the coins of thousands of others who make legal or illegal transfers. This washing process can take time and can be carried out several times. Currencies can also move forward in several tranches at random intervals. However, in recent years, techniques have been developed to trace cryptocurrencies through mixers, although there is no information about a method that will definitely work, at least not yet. On the other hand, as in the present case, if such a capacity were to be found on the part of the authorities, it would only be publicly discussed to the extent that is mandatory. If criminals don't know what the police are capable of when it comes to tracking crypto, it creates uncertainty and can raise the threshold for embarking on a criminal path.

Cryptocurrencies have been a very useful tool for criminals practically throughout their existence. A currency that moves quickly and is difficult to trace can even be seen as the lifeblood of the entire financially motivated cybercrime. However, the possibility of privacy-oriented currency transfers is also important outside of cybercrime, as they can be used to add privacy to otherwise publicly available cryptocurrency transactions. This can, for example, circumvent the control of an authoritarian state or receive anonymous donations from abroad to opposition activities. Thus, the use of Monero or crypto mixers is not illegal per se, and the use of the technology is not limited to criminal activity. Simply deactivating these services would not be a viable solution, especially as new ones would most likely emerge immediately to replace them. Advances in tracking cryptocurrencies are extremely significant, as whether it is a new kind of technology or an innovative way of approaching the data in use, success is always a sign that the authorities are gaining the lead of criminals. Cryptocurrencies and related side effects are here to stay.

REFERENCES

1. DDOS attacks losing impact

https://t.me/s/noname05716eng
https://www.hs.fi/talous/art-2000010202403.html
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-jatkuvat-myos-vuonna-2024

2. Security risks of push notifications

https://www.reuters.com/technology/cybersecurity/governments-spying-apple-google-users-through-push-notifications-us-senator-2023-12-06/
https://blog.hypr.com/what-are-push-notification-attacks
https://blog.davidlibeau.fr/push-notifications-are-a-privacy-nightmare/
https://www.bleepingcomputer.com/news/security/iphone-apps-abuse-ios-push-notifications-to-collect-user-data/
https://thehackernews.com/2023/12/governments-may-spy-on-you-by.html
https://www.washingtonpost.com/technology/2023/12/06/push-notifications-surveillance-apple-google/

3. Tracing cryptocurrencies is developing

https://www.bleepingcomputer.com/news/security/vastaamo-hacker-traced-via-untraceable-monero-transactions-police-says/
https://monerofund.org/projects/eae_attack_and_churning
https://medium.com/@nbax/tracing-the-wannacry-2-0-monero-transactions-d8c1e5129dc1
https://www.ledger.com/academy/topics/blockchain/what-is-a-bitcoin-mixer
https://home.treasury.gov/news/press-releases/jy0916
https://www.linkedin.com/pulse/how-cryptocurrency-mixers-enable-money-laundering

Pictures: Pixabay, Pngtree

Cyberwatch Finland