Cyberwatch Finland

WEEKLY REVIEW
WEEK 9/2024

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

Cyberwatch Finland

KEY TAKEAWAYS

1. Successful operations by the authorities cause harm to large ransomware operators and may affect their future operations.

2. Google and Meta announced measures to combat disinformation ahead of June's European parliament elections. This is partly due to the recently enacted EU Data Services Act DSA.

3. The user's browsing history data is of interest to many different actors. In addition to criminals, marketing companies also seek this data.

1. NEW ERA IN THE WORLD OF CYBERCRIMINALS

Recently, Russian cybercriminal groups BlackCat (ALPHV) and LockBit experienced great difficulties due to successful offensive actions by the authorities. In December, BlackCat suffered significant damage in an attack on the group's servers by the FBI in cooperation with European national police officers. In February, the same fate befell LockBit with a police operation led by Britain's National Crime Agency (NCA). In the case of both BlackCat and LockBit, the authorities gained control of the groups' websites and the servers that run them. In both cases, decryption keys of ransomware used by the groups were also seized and cryptocurrency accounts linked to criminals were frozen. In connection with the shutdown of the BlackCat group in December, LockBit and BlackCat operators announced that they would start cooperating in the ransomware (Ransomware as a Service, RaaS) market. Now, however, both of these RaaS operators, considered to be the largest, have been subjected to momentarily crippling action by the authorities.

Both criminal groups have recently shifted to very immoral and all-consuming offensive activities. In the past, the groups themselves have followed and forced rules on their partners prohibiting the use of the malware they have developed against hospitals, emergency services, school networks or non-profit organisations, for example. BlackCat removed this ethics clause after the December setback, and LockBit also approved an attack on Children's Hospital Chicago in January. Remarkably, just a year ago, LockBit publicly apologized for its subcontractor's ransom attack on Children's Hospital in Toronto, made the decryption keys available to the Children's Hospital, and stopped working with the contractor who carried out the attack.

Behind the activities of both criminal groups are Russian criminals, whom the Russian authorities have urged to wage a fight against the global West while giving approval and protection to criminal activities. This is undoubtedly one of the root reasons why the large-scale multinational police operations we have now seen have combined the activities of the authorities across national borders. In the past, authorities have aimed to weed out financially motivated cybercriminals. Now, a weighty political motive can be seen to have emerged alongside it, because the huge ransom proceeds generated by the cybercriminal groups we are talking about and how cybercriminal groups indirectly benefit the Russian state's economy. The unprecedented scale of operations by Western authorities indicates a desire to prevent large criminal financial flows to Russia in addition to economic sanctions. Another goal of closer cooperation between authorities can be assumed to be to slow down LockBit's continuous application development. As a result of the attack, it was revealed that the group was already preparing a new, more dangerous version of its malware.

In any case, the cyber world is witnessing the beginning of a new era in which large, international coalitions of authorities carry out successful attacks against the largest criminal groups. Traditionally, criminals have always been thought to be one step ahead and the authorities to follow. However, in these operations, police authorities have taken a proactive approach to the fight against cybercrime. Each cybercriminal group has to think about its own actions and be vigilant. It remains to be seen whether the measures taken by the authorities will create a cycle of revenge in which criminal groups will focus more on state actors in the future, leaving the business world in a smaller role. However, it should be remembered that in the case of both LockBit and BlackCat, it is a service provider where attacks are carried out by subcontractors who pay groups to use their applications. With this in mind, criminals will continue to direct their main interest to where it is easiest to get a lot of money at any given time.

2. TECH GIANTS FIGHT DISINFORMATION IN THE EU, DIGITAL SERVICES ACT AFFECTS IN THE BACKGROUND

The anti-disinformation front in Europe received new reinforcements in February when Google and Meta announced that they would launch campaigns to combat disinformation in the context of the European parliament elections in June. In particular, the EU has feared an increase in Russian propaganda and its impact on the upcoming elections. The companies' announcements symbolically coincided around with the start of national application of the European Union's Digital Services Act (DSA), which was on 17th of February. It has been hoped that the DSA will contribute to the fight against disinformation by imposing obligations on online platforms, including on platform moderation, and by obliging platforms to assess and mitigate risks related to democratic and electoral processes. DSA's obligations have already applied to very large online platforms and search engines since 25 August.

In Google's case, the company will launch an advertising campaign between April and May in different platforms, including YouTube and TikTok, in five EU countries: Belgium, France, Germany, Italy and Poland. The advertisements contain information on how to identify misinformation and disinformation and what kind of misinformation is sought to spread. The campaign uses so-called "prebunking" methodology. This means that the aim is to get the target notified of false information earlier than the false information itself reaches the target. When such misinformation reaches the target, he already knows to take it with caution. The reasons given for choosing these countries as the target for advertising included an opportunity to reach a large number of voters in the elections and to make use of the company's own local knowledge. Although the campaign targets the EU's most populous countries, it excludes a significant number of eligible citizens from other member states, which contributes to weakening its effectiveness. However, these measures are undoubtedly appropriate and heading in the right direction.

Meta, meanwhile, is addressing the problem by opening a dedicated Elections Operation Center to identify and counter threats in real time. Tackling misinformation includes fact-checking with 26 partners across the EU in more than 22 languages. In addition, the aim is to tackle coordinated influencing operations and respond to possible misconduct with artificial intelligence, such as deepfakes.

Both companies' decisions are certainly partly influenced by the EU's Digital Services Act, although the announcements do not directly refer to it. According to the European Commission, the main objective of the act is to prevent illegal and harmful activities online and combat the spread of disinformation. However, the DSA has so far received more public attention for its obligations to allow platform users to opt out of personalised marketing, the obligation to create easily understandable terms of use, the obligation to moderate content more openly and the possibility to appeal against the moderation decision. In addition, the DSA unequivocally prohibits targeting advertising at children and targeting advertising at adults on the basis of, for example, ethnic background or sexual orientation. The aim is therefore to increase users' rights and influencing opportunities.

Although the act itself applies to virtually all digital services, it focuses on very large online platforms and search engines. By definition, this includes services whose monthly number of active users exceeds 45 million users in the EU area when examining the average for a six-month period. For these very large operators, an additional obligation is to assess four distinct risk categories, for which measures should also be taken to reduce risks. These include risks related to the dissemination of illegal content, such as the spread of illegal hate speech, democratic processes, civil dialogue and electoral processes. The maximum amount of fines for non-compliance with regulatory obligations can be up to 6% of a company's annual worldwide turnover

EU regulation is often described as bureaucratic and its achievements are doubted. However, it is clear that it also has positive effects. DSA is possibly an example of successful regulation from the citizen's point of view, as it increases the transparency of services and users' choices regarding their own privacy. For wider society, the benefits can be seen precisely in the form of the campaigns described above, which can contribute to reducing the effectiveness of attempts to influence the EU by hostile actors.

3. BROWSING HISTORY DATA IS VALUABLE

Last Thursday, the US Federal Trade Commission (FTC) fined security company Avast $16.5 million. The reason given for the fines was that the company had both collected and sold users' data without their knowledge or approval. In addition to the penalty payment, the FTC also banned Avast from any selling of user data in the future. What makes the situation ironic is that the products through which Avast had collected data had been marketed to users as privacy and anti-tracking services. In practice, it was browser extensions and antivirus software. Sure, they did what Avast promised their customers, but they also collected and stored users' browsing data. According to the FTC's reasoning, Avast had sold this information for various marketing and profiling purposes, thereby violating both the law and the promises it made to its users.

Even though the question is not about any extremely sensitive information, browsing and search history can still reveal a lot about a user. For example, website visits can reveal age, gender, and interests, making the data valuable for targeted advertising companies. At the same time, it can be used to provide indications of, for example, the religious and ideological orientation of users or factors related to their state of health. Based on this information, users can be profiled for targeted marketing purposes. From an individual user's point of view, it may not seem threatening if one's browsing history ends up in the possession of a third party, but their mind may change if the user were given access to a profile compiled by marketing companies based on browsing, search and cookie data obtained from their various sources. For example, it's not uncommon for advertising companies to add information to profiles about pregnancy or changes in health status. This can happen even before the person himself would be ready to share this information with their nearest and dearest.

Preventing tracking is difficult these days. Online behaviour is monitored by parties that have a legitimate right to do so, such as network operators and websites visited, but also unwanted third parties, for example through cookies. Avast's example shows that it can also be difficult to find an operator whose promises of privacy protection can be trusted. Often, instead of actually encrypting one's own data, by using various application solutions, this data is deliberately handed over to one specific actor who promises to take care of it. This is true, for example, with VPNs that promise to encrypt browsing data from third parties, but have also occasionally been caught carelessly handling the data they collect or, at worst, trading it, like Avast. These services are also attractive targets for data breaches, because even if the company itself does not sell the data, the hacker who stole it can do so. The key question is whether and in what form these providers store and log data about their users, and how much the user can or wants to trust its promises. Obtaining certainty about this may be impossible, or at least very difficult. However, with a little background work, it is possible to find out what kind of reputation the service provider promoting privacy has. The price of the service can also serve as a good guide: if a product marketing protection is clearly cheaper than its competitors, the company will most likely make its profits through some other means. In a free service, the user is almost always the product that is sold.

It is also good to remember that browsing data is also collected not only by marketing companies or dishonest security actors, but also by much more malicious parties. Various data-stealing malware, or infostealers, are among the most common types of viruses. In addition to other sensitive information, they also collect browsing and search history from infected devices. This information is also sold and shared, although instead of agreements between consulting firms, these marketplaces are dark web market forums. Cybercriminals may also be interested in users' browsing history, for example, to determine how social engineering might be easiest to approach the victim: whether they gamble, visit adult entertainment or dating sites, for example. All this information can be used to plan crimes and, combined with other information, it can also directly provide criminals with opportunities for pressure or blackmail.

Cyberwatch Finland

HOW TO AVOID UNWANTED TRACKING:

Web browser selection: Different browsers protect users' privacy differently. In comparisons, the most common browsers, such as Chrome and Edge, often receive the worst marks. The best choice among the best-known browsers is considered to be Firefox and LibreWolf, which has been modified from it to take even further protection, and Brave, which is popular in security circles. Often, by choosing a privacy-oriented browser, the user dispenses with some functionalities that improve the user experience, such as browser extensions.

Browser settings: Many browsers, including Chrome and Edge, offer the ability to turn on settings that restrict cookies or other nominally privacy-enhancing features. While they may be useful, in some cases these settings may not significantly change how data is collected. For example, the general option of adding Do Not Track (DNT) requests has been widely found to be completely irrelevant for tracking. On the other hand, incognito or private browsing mode limit tracking quite well.

Opting out of cookies: Although laborious, refusing cookies when browsing websites is a relatively effective way to avoid data ending up for further use. However, in addition to hard-to-find buttons that block all cookies, this may be limited by the fact that the functionality of the website may suffer by refusing cookies. Especially for suspicious or non-HTTPS sites, putting in the extra effort would be extremely important to protect your data. There are also browser extensions or applications that automate this process, but even when using these, you should first make sure that the service provider is reliable so that refusing cookies does not download hidden malware at the same time.

Search engine choice: Like browsers, search engines collect and store browsing data, and there is a lot of variation in these. Google and Bing are again among those collecting the most data. A good and widely used alternative to these is, for example, DuckDuckGo, which can be set by default in many browsers.

Privacy-enhancing applications: Various solutions that protect user data, such as VPN services, are effective solutions for avoiding data collection and protecting your own browsing data. However, when using these, it is good to make sure of the terms and reliability of the service provider, because while protecting your data from third parties, you often hand over all this data to the company providing the VPN service.

REFERENCES

1. New era in the world of cybercriminals

https://www.bleepingcomputer.com/news/security/us-offers-15-million-bounty-for-info-on-lockbit-ransomware-gang/
https://www.bleepingcomputer.com/news/security/police-arrest-lockbit-ransomware-members-release-decryptor-in-global-crackdown/
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
https://www.theregister.com/2024/02/22/lockbit_dismantled_new_variant/
https://www.theregister.com/2024/02/01/lockbit_ransomware_attack_hospital/
https://twitter.com/DailyDarkWeb/status/1609857321315835906
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/
https://cybernews.com/news/lockbit-still-showing-signs-if-life-with-new-attacks-reported-on-friday/
https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant
https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups
https://www.state.gov/first-trilateral-sanctions-against-russian-cyber-actor/
https://therecord.media/alphv-black-cat-ransomware-takedown-fbi

2. Tech giants fight disinformation in the EU, Digital Services Act affects in the background

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fi
https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops
https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms
https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022R2065#d1e2324-1-1
https://faktabaari.fi/nakokulmat/nakokulma-digipalvelusaados-lisaa-avoimuutta-ja-vahvistaa-kayttajien-oikeuksia/
https://prebunking.withgoogle.com/
https://blog.google/around-the-globe/google-europe/supporting-elections-for-european-parliament-2024/
https://about.fb.com/news/2024/02/how-meta-is-preparing-for-the-eus-2024-parliament-elections/

3. Browsing history data is valuable

https://therecord.media/avast-fine-ftc-alleged-browser-data-sales
https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over
https://privacytests.org/
https://www.techradar.com/vpn/avoid-downloading-a-bad-vpn-these-are-the-warning-bells-to-look-out-for
https://brave.com
https://librewolf.net/

Pictures: Pixabay, HilariousGifs.com