Cyberwatch Finland

WEEKLY REVIEW

13/2024

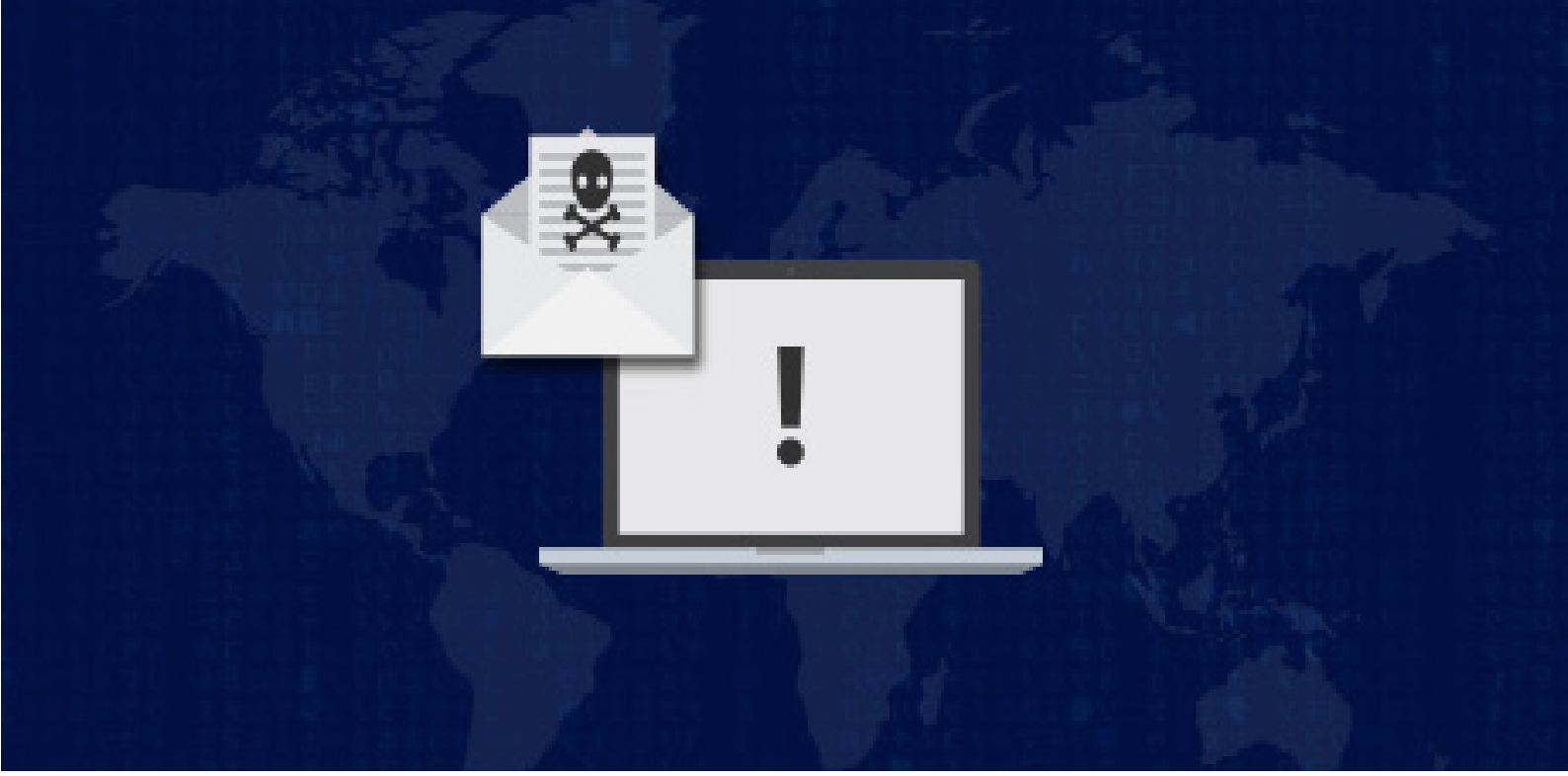
THEME REVIEW

RANSOMWARE

Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

13/2024



THE THREAT POSED BY RANSOMWARE AFFECTS EVERYONE

Ransomware is a common cyber threat that affects both organizations and individuals. Large companies such as technology company Sony, industrial company Boeing and hotel and casino chain MGM Resorts, as well as public sector operators such as universities, li-braries and municipalities around the world have fallen victim to ransomware. Chainanaly-sis, a blockchain analytics company, estimated in a report in February 2024 that up to $1.1 billion of ransomware ended up in the hands of criminals in the previous year. Although estimates of the sums vary slightly, all analyses tell the same story about the growing and increasing phenomenon. The threat is topical and therefore deserves closer scrutiny.

Technically, ransomware works in a fairly simple way: it locks, encrypts, or hijacks a device or the files on it. The device or data can be restored with an encryption key that the crimi-nals promise to give the victim after the ransom in bitcoins or another cryptocurrency has been paid. Ransomware spreads like any other malware — for example, by downloading files from malicious sites or opening a file attached to a phishing email. In the most ad-vanced cases, criminals can also infiltrate the target organization's systems, for example, by exploiting an external vulnerability, and deliver the malware to the target itself. Ransom-ware is mainly used by cybercriminals motivated by financial gain. However, governmental APT groups are also known to have used them in their activities. For APT groups, the motive may be to disguise the actual goal, i.e. to confuse, or simply to consume the target's re-sources and play with time without any intention of returning the stolen data. It is also pos-sible that states exploit financially motivated criminal groups and direct their attacks to desired targets. Disruption or uncertainty caused by extortion attacks may be beneficial for hostile nations interests, and state-sponsored and financially motivated attacks can often be difficult or even impossible to distinguish.

CRIMINAL BUSINESS MODEL RaaS

In recent years, the criminal version of the standard software service model, Ransomware-as-a-service (RaaS), has become more common in financially motivated ransomware opera-tions. In it the developer of ransomware grants access to it to an actor who does not have the ability to create a similar program itself. The license buyer then delivers the malware to a target's systems and performs the actual blackmail. There are several different models of income distribution. The buyer can either pay the agreed part of the ransom received to the RaaS supplier, pay the agreed monthly fee for its use, or redeem a continuous, free license. The price of the service often also includes product support and advice provided by the software provider.

Well-known RaaS vendors include LockBit and AlphV/BlackCat. Both groups are thought to be of Russian origin. For example, LockBit is reported to take a 20% share of every ransom demand paid. RaaS suppliers may also select their buyers, check their backgrounds, set dif-ferent conditions or limit the selection of targets to operators in a particular industry or region. For example, the aforementioned LockBit and BlackCat have previously prohibited service buyers from targeting nonprofit organizations. However, these groups have recently lifted their restrictions. At the moment, the only rule in force seems to be that attacks must not target Russians or pro-Russian entities.

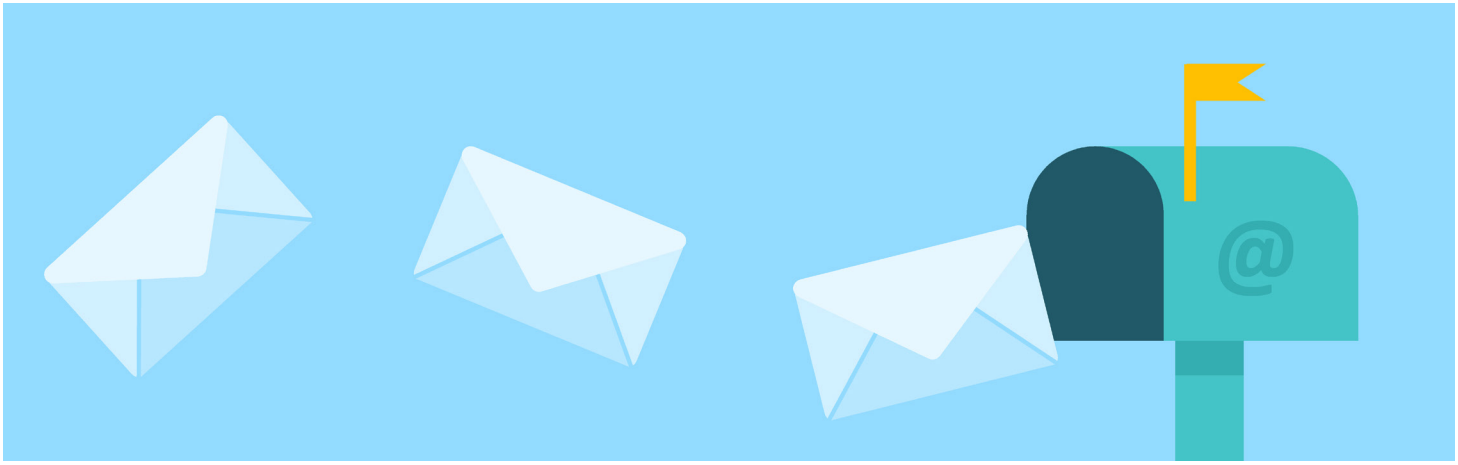
Recently, ransomware has been used to attack critical infrastructure targets, especially hos-pitals. The U.S. Department of Health estimates that the number of attacks on the healthcare sector has increased by as much as 264% over the past year. However, this phe-nomenon is not unique to the United States, as hospitals in Europe have also fallen victim to ransomware. For example, in February 2024, the IT systems of Romanian hospitals were attacked, as a result of which the operations of about a hundred hospitals were thought to have been affected. Another major ransomware attack seen at the beginning of the year targeted the large Nordic IT company Tieto-evry and led to the inoperability of several of its custom-ers' systems and websites. Backups and other valuable data were also lost in the attack. For example, the Swedish Dental and Medical Reimbursement Agency said it had lost all its documents since 2016. At worst, ransomware compromises not only the compa-ny's own data, but also the valuable data of customers and other stakeholders. In addition, a ransomware attack can affect a company's finances in different ways and, for example deteriorate investor confidence in the company.

As with other forms of cyberattacks, ransomware trends live and change. This year, a new family of PikaBot malware has been spotted, which is an example of modern modular ran-somware. It contains several features in the same package that previously had to be done in stages in an attack or required specialized software. The modules include, among other things, intrusion into systems, hiding in them and manipulating access rights. Modular ran-somware can also be updated and modified even after it has reached the target system with features that work just for it. Thus, modular malware is more agile than before and enables more extensive and versatile action for its user.

In extortion itself, various forms of double or triple extortion have increased in popularity. Double extortion generally refers not only to the mere concealment of information, but also threats to make information public. In triple extortion, blackmail can be extended not only to conceal and disclose information, but also to blackmail potential customers or other stakeholders. For example, the blackmailer may contact the organisation's customers di-rectly, state that they have stolen information belong-ing to them, and tell them that the organization that controlled the data is indifferent to negotiations to buy it back. It is also a growing phenomenon that victims of the second stage can be offered their own opportuni-ty to buy back or delete information about themselves. Such a procedure was seen, for ex-ample, in the Vastaamo case, which received a lot of attention in Finland, when the organi-sation itself did not agree to ransom demands.

In addition to cyberattacks directly on the target organization, there is a growing trend of hitting the supply chain. In this way, the attacker may be able to para-lyze the target more easily than by directly attacking what are likely to be the best protected systems. Automat-ed ransomware that uses artificial intelligence to find vulnerabilities is also expected to be-come more common. Criminals also actively monitor vulnerability logs pub-lished by soft-ware companies and try to exploit gaps before they can be patched.

In addition to organizations, ransomware also affects individuals. For example, the StopCrypt Ransomware targets individuals rather than organizations. It is one of the most widely distributed, but significantly less publi-cized, ransomware programs. In these cases, instead of tens or hundreds of thousands of dollars, ransom demands are typically a few thousand.



THREAT ACTORS USE COMMUNICATION TO PUT PRESSURE ON THEIR VICTIMS

Ransomware actors usually actively communicate about the attacks they carry out. This typically happens through the group's own dark web or social media channels. Pages or platforms publish information about the group's victims. In this way, there is public pres-sure on the victim to make the payment.

These sites, which often operate on the dark web, serve many purposes. First, they act as external communi-cation and marketing channels for groups, as the effec-tiveness of a group can be measured, at least indirectly, by the length of the victim list and the type of organi-zations it contains. Secondly, these pages are also where victim organisations are typically directed and lists of other victims can also serve as scare factor for companies ending up on the sites. Thirdly, they also serve as publishing platforms for captured data. When a group reports a new victim, there is often a "sample" of the captured data as evidence of the suc-cess of the attack. Some groups publish these samples at a steady pace until ransom de-mands are met. It is also possible that the captured data will be put up for open sale or auc-tion without an actual ransom demand (Figure1). If an organization does not want the data to end up with a third party, it may have to challenge other parties interested in the data, which are usually other criminal groups, in a bidding war.

Figure 1 Ransomware group Medusa's post about stolen data for sale

Depending on the group, publications can take several different forms, but they often con-tain information on the field and size of the organisation in question. For example, turnover or the number of employees is often mentioned. In some cases, the victim may also be ri-di-culed, or their level of security may be described as lacking. (Figure 2).

Figure 2 INC-Ransomware post

Especially if the ransom is refused, the tone of the posts can become much more aggressive. At worst, these reports may identify staff of the victim organisation, often members of the management team, who are said to be responsible for the poor level of data protection and their contact details may be included in the report (Figure 3).

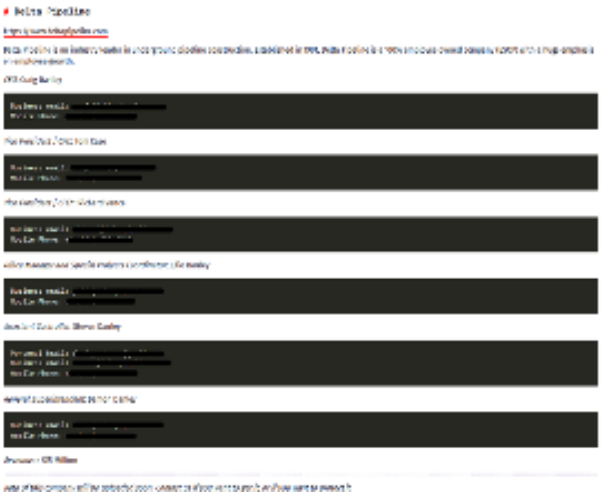


Figure 3 Censored post by LockBit-Ransomware

Humiliating communication is practiced especially in cases of double or triple extortion, in which case the threat actor may also contact other parties affected by the attack, such as the organisation's customers or partners, and direct them to their pages. The goal is for partners to see a sample of their sensitive data and messages from criminals that the victim has not adequately protected this data and does not seem interested in recovering it.

Naturally no organisation hopes to end up on these victim lists. Ending up on one can not only attract more criminal attention, but also significantly increase the reputational dam-age caused by an extortion attack. The problem, however, is that it is practically impossible to prevent listing. It is not in the organization's own hands what and where criminal groups publish them. In addition, contrary to what the groups promise, paying the ransom does not necessarily remove the mention on the site. Even if the public mention is removed, in-formation about victims willing to pay is transmitted through less public channels to other criminal groups. Therefore, the only way to combat the public pressure produced by black-mailers is to communicate objectively and honestly on the subject. If the organization first has time to report the attack itself and what data has been revealed, the criminals' posts will have significantly less sensational value. The importance of correct and timely commu-nication cannot be overemphasized. It can even be a decisive factor in how well an organi-zation survives the event.

The publications of criminal groups may not always be completely honest and may over-state the amount of information obtained or its sensitivity. Some groups are even notori-ous for posting completely false reports of attacks on their sites. On the other hand, many criminal gangs try to maintain a "respectable reputation" and only post about truthful at-tacks on their sites.

It is good to remember that in some cases, criminal communications may be more about a perceived threat of reputational damage than actual damage. When an organisation in cri-sis sees threatening messages, it may forget that most of the publications take place on the dark web, and it is not always certain that they will end up on the surface network or main-stream media. Some of the criminals' publications end up in cybersecurity publica-tions, but especially in minor cases, they are often seen by a relatively small circle that is particularly interested in the phenomenon. However, if it is a larger player, it is more likely that publica-tions will receive more attention outside the dark web.

Analysis of ransomware has always been challenged by the fact that only a small percent-age of all crimes end up in the public domain. Although accurate statistics are difficult to compile, authorities around the world agree that a significant number of cases remain un-reported. From the point of view of criminals, acting under the radar is always desirable, which is why they try to encour-age their victims to pay the ransom and keep quiet about the case.

PREVENTING RANSOMWARE AND MINIMISING ITS EFFECT

- Up-to-date antivirus, firewalls and a fast-patching rate of published vulnerabilities can stop the spread of malicious files.
- Staff training and good cyber hygiene practices are an effective way to prevent the threat.
- In the event of an attack, it is important to isolate the exposed network environment and take measures to investigate the incident.
- Backups play an important role in recovering from the event and the continuity of the organization's operations.
    - However, copies of data alone are not enough, it is also critical to take into ac-count the backup infrastructure, which can be relied on in case of problems.
- Crisis communication and communicating about the incident both internally and to stakeholders are key to minimizing reputational damage and the spread of misin-formation.
- The ransom should not be paid under any circum-stances. Payment does not guaran-tee that the data will be restored or that the data will not be leaked later.

THE ROLE OF CYBER/SECURITY INSURANCE IN RANSOMWARE ATTACKS

- Cyber insurance policies most often cover the costs of a data breach or security breach, such as investigating a data breach, removing malware, and restoring data.
- In insurance contracts, it is precisely agreed what the level of information security of the insured should be.
- Failure to comply with these terms of the contract reduces or even completely elim-inates possible compensation.
- Although the general advice is that the ransom should not be paid, some insurance policies also cover the payment of ransoms for extortion or malware.
- In some cases, however, criminals have been found to be targeting insured organisa-tions in the hope of a more secure ransom payment.

RUSSIAN RANSOMWARE GROUPS BECOME POLITICIZED

- Groups previously known for their financially motivated activities, such as LockBit and BlackCat, have begun carrying out ideological attacks on Western countries with the aim of disrupting and destabilizing "Russia's enemies" in the West.
- In the future, Western countries can expect an increasing number of attacks on criti-cal infrastructure.
- According to estimates, the threats posed by the groups will not increase significant-ly in the near future without strong external support, for example from state actors.

TRUST BETWEEN CRIMINALS IS QUESTIONABLE

- The BlackCat/ALPHV criminal group allegedly disappeared from the dark web after hijacking a ransom of $22 million obtained by an affiliate.
- Questions arise as to whether this is BlackCat's exit scam, a rebranding of the group or the beginning of a cyber cartel
- BlackCat is believed to be the rebranded name of a former hacker group called DarkSide, so the group is familiar with this kind of activity.
- In December 2023, the BlackCat and LockBit criminal groups announced that they would launch a cyber cartel in response to the actions of the authorities.
- This case shows that in a criminal world, partners cannot be trusted.
- This may affect the development of the RaaS service model in the future.

CAN AI HELP FIGHT RANSOMWARE?

- Advances in AI technology have been speculated to be helpful in responding to the ransomware threat.
- AI-based solutions can monitor, analyse and respond to cyber threats in real time or in advance by detecting a threat even before an attack begins.
- AI is particularly good at monitoring and analysing behavioural patterns, detecting unusual activity and limiting unauthorised access to systems.
- When implemented correctly, AI can free up employees' resources and time by au-tomating repetitive tasks.
- AI can also reduce the number of human errors.

REFERENCES:

https://www.malwarebytes.com/blog/business/2024/03/pikabot-malware-on-the-rise-what-organizations-need-to-know

https://blogs.blackberry.com/en/2024/03/ransomware-impacts-healthcare

https://www.bleepingcomputer.com/news/security/stopcrypt-most-widely-distributed-ransomware-evolves-to-evade-detection/

https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups

https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html

https://www.reuters.com/technology/cybersecurity/blackcat-ransomware-site-claims-it-was-seized-uk-law-enforcement-denies-being-2024-03-05/

https://www.itworldcanada.com/article/alphv-blackcat-allegedly-calls-for-ransomware-gang-cartel-to-stand-up-to-police/555578

https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-data-breaches-ransomware-attacks-february-2024

https://www.hawsons.co.uk/2024-ransomware-trends/

https://www.chainalysis.com/blog/ransomware-2024/

https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

https://www.theverge.com/2023/12/12/23998342/insomniac-games-ransomware-attack-sony-rhysida

https://www.malwarebytes.com/blog/business/2024/03/pikabot-malware-on-the-rise-what-organizations-need-to-know

https://www.bleepingcomputer.com/news/security/stopcrypt-most-widely-distributed-ransomware-evolves-to-evade-detection/

https://www.reuters.com/business/aerospace-defense/boeing-investigating-cyber-incident-affecting-parts-business-2023-11-01/

https://www.reuters.com/technology/mgm-says-its-hotels-casinos-operating-normally-after-cyberattack-2023-09-20/

https://www.trendmicro.com/en_no/research/24/b/lockbit-attempts-to-stay-afloat-with-a-new-version.html

Cyberwatch Weekly

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

THE EDITORIAL TEAM
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Pixabay
Shutterstock

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi