STRATEGIC REPORT TLP:CLEAR

Ransomware-driven data exfiltration: techniques and implications

Livia Tibirna, Caroline Lewis and TDR team, November 2024

sekoia

Table of Contents

Introduction

This report focuses on the **exfiltration techniques leveraged by ransomware and extortion groups** in lucrative campaigns. It aims to provide a comprehensive analysis of the techniques and tools used during the exfiltration phase and the **impact** on affected organisations. It also includes observations relating to the collection tactic, which we consider essential for a comprehensive understanding of exfiltration campaigns.

First, we will explore the **progressive adoption** of the exfiltration technique by ransomware and extortion groups and the **motivations** behind their campaigns. Second, we will analyse the different **categories of targeted data** during the exfiltration phase.

Next, we will focus on the **tools** leveraged by lucrative intrusion sets to gather valuable data from a victim's environment. Finally, we will provide insights into **detecting** different tools and techniques associated with data exfiltration.

While this report focuses on opportunistic, ransomware-driven intrusion sets and campaigns, it is worth noting that a wide range of **distinct financially motivated intrusion sets** employ exfiltration tactics. This includes operators of infostealers, remote access trojans (RATs), spyware, credit card skimmers, backdoors, and other types of malicious software. Moreover, **state-sponsored actors** also largely leverage the exfiltration tactic in information-gathering campaigns. While we may reference these categories of actors in our analysis, they are not the primary focus of our study.

Our research involves both an analysis of open-source reporting from 2022 to November 2024 and in-house investigations.

Key Takeaways

> **Data exfiltration** became a **critical element** in ransomware campaigns, in line with the widespread adoption of the double extortion technique between 2019 and 2024.

> Attackers **leverage stolen data** to maximise **financial and reputational impact** through public exposure on dedicated leak sites, while also potentially selling the data to other threat actors or using it for additional extortion and subsequent attacks.

> These motivations, along with factors like reduced effort and the circumvention of encryption-related challenges, led some ransomware groups to **focus partially or exclusively on data exfiltration** for extortion, without encrypting files.

> Besides lucrative ransomware and extortion groups, exfiltration is also **leveraged by state-sponsored intrusion sets** during ransomware operations, likely to misdirect attribution, conduct covert intelligence gathering campaigns, and generate revenue.

> Over the past five years, ransomware operators increasingly refined their extortion techniques to **maximise leverage for double extortion**. They adopted a more strategic approach by **pre-qualifying and triaging collected data**. This involves **targeted searches** aimed at extracting high-value, sensitive files, such as financial information, personal and medical records, classified documents, IT-related and network data and other highly sensitive information.

> Ransomware groups use a combination of **custom and publicly available tools** to facilitate data exfiltration. This is according to their specific features and their intended use in exfiltration campaigns: **enumeration**, **compression**, **uploading**, *etc*.

> Advanced intrusion sets increasingly develop and use **custom exfiltration tools** to enhance efficiency, precision, and stealth. Ransomware operators occasionally leverage **commodity malware**, including infostealers and Malware-as-a-Service (MaaS) tools, to streamline the data exfiltration processes. However, their use remains limited compared to publicly available alternatives.

> **Legitimate and publicly available tools** are widely leveraged to facilitate stealthy and cost-effective data exfiltration while blending in with legitimate activities to evade detection.

> To mitigate the impact of data theft and ransomware deployment, companies should prioritise **early detection** of data exfiltration attempts through a **multimethod strategy**, including monitoring suspicious behaviour, file access patterns, and the use of known exfiltration tools, while focusing on critical files and directories to detect potential data movement.

Part one

Pressure and profit: the rise of ransomware-driven exfiltration campaigns

Contextualising the increasing pressure on victims

Data exfiltration is a significant threat in cybersecurity, referring to the **unauthorised transfer of data** from a compromised system or network to an infrastructure controlled or misused by the attacker.

Between 2019 and 2024, significant evolutions were continuously observed regarding the behaviour of ransomware-driven campaigns. One such evolution is the **increasing usage of exfiltration in ransomware campaigns**, leading to the expansion of the double extortion tactics that use data theft for additional leverage.

In late 2019, the intrusion set deploying the **Maze** ransomware became one of the **first major actors to exfiltrate data** in addition to encrypting it. It then leveraged collected data as a secondary method of extortion. To this aim, Maze built a dedicated Data Leak Site (DLS) that publicly listed the names of compromised companies and threatened to publicly release the stolen information if they refused to comply.

The adoption of the double extortion technique was primarily intended to **prompt victims into actually paying the ransom**, because even though victims manage to recover their backups after encryption, the **damage from stolen data persists**. Besides being publicly released and therefore widely accessible, including to competitors, it could be privately sold to other threat actors or leveraged for a second extortion attempt. Faust could be an example of ransomware that makes use of such techniques, as it exfiltrates sensitive information without relying on a dedicated DLS. Moreover, paying the ransom for avoiding above-mentioned risks could still expose victims to legal repercussions, as many countries adopted data protection laws that carry significant fines for non-compliance.

The double extortion technique proved **highly lucrative**, as corroborated by Unit42 data. Indeed, Maze ransom demands in 2020 averaged $4.8 million, a significant increase compared to the average of $847,344 across all ransomware families the same year.

In early 2020, other major ransomware players such as NetWalker and RagnarLocker adopted the double extortion technique and started to claim victim organisations on their respective DLS actively to actively claim victim organisations on their respective DLS. **Data exfiltration became a common tactic** over 2020 and by the end of the year, **at least 16** distinct ransomware families were using leak pages. The rise of DLSs and an increasing number of ransomware variants using these techniques **intensified the pressure on victims**, the average ransom payment rising to $312,493 in 2020 compared to $115,123 in 2019.

By 2023 and 2024, ransomware operations **increasingly incorporated data exfiltration** into their tactics and it became almost a **standard feature** in ransomware campaigns. Moreover, ransomware actors likely became **more efficient in exfiltrating data** from targeted systems; based on Mandiant data, the median time from initial access to ransomware deployment in incidents involving data theft decreased from 9 days in 2022 to 6.11 days in 2023.

In 2023, most ransomware incidents (between 59% and 91% - depending on the source) involved some form of data exfiltration, marking a **significant** rise from earlier years.

Motivations behind the shift to data exfiltration

We observed some ransomware groups shifting to a simpler yet highly profitable extortion approach in recent years, by **focusing partially or exclusively on data exfiltration without encrypting** files.

For example, in 2021 the **TA505** intrusion set started to conduct extortion campaigns based on data exfiltration only, notably in large-scale vulnerability exploitation campaigns. Also, part of the 2022 incidents related to the **Industrial Spy** and **Luna Moth** (aka Silent Ransom) operations only involved data exfiltration.

Another example involves the **BianLian** intrusion set initially employing a double-extortion model that shifted to primarily exfiltration-based extortion in early 2023. Similar findings were later observed in campaigns attributed to the **Hunters International** and the **Akira** intrusion sets.

Reporting in the Q3 2024 also highlights a shift in tactics by the **Meow** ransomware operation, moving from data encryption to selling stolen data on cybercriminal forums and its own DLS. Similarly, **Inc Ransom** pivoted to focus on stealing and extorting sensitive data in the second half of 2024.

Moreover, we monitor a constantly increasing number of intrusion sets **specialised in data-theft extortion**, such as **Karakurt** and **TommyLeaks**.

We assess this for several reasons. First, attackers increasingly prioritise data theft, which became an **equally important lever for extortion** as encryption. This is amplified by the growing ability of corporate victims to manage operational backups and execute plans for rebuilding compromised infrastructure. As a result, the **primary concern shifted** from the impact of encryption to the risks associated with **attackers possessing sensitive data**.

Second, data extortion is **less resource-intensive** regarding human, technical and financial effort, since it bypasses both the development and deployment stages of ransomware, including managing the decryption mechanisms. This aligns with a “low-effort, high-reward" strategy.

This is especially true during **large-scale attack campaigns** such as exploiting the MOVEit vulnerability by TA505, with the intrusion set stealing data and not encrypting it, likely to avoid encryption and/or decryption challenges at scale.

In other cases, data-theft extortion serves as a **temporary alternative** to encryption. For example, **Akira** operators relied on this approach between late 2023 and early 2024. Talos researchers assess this corresponds to the timeframe when Akira actors completed a rewrite of their ransomware code. It is also possible that certain ransomware operators faced unexpected **challenges during the encryption process**, pushing them to pivot towards leveraging data theft as an alternative means of demanding ransom.

Additionally, the **public release of decryption tools** for specific ransomware variants such as for BianLian in early 2023 possibly prompted the attackers to further monetise intrusions through data-theft extortion, rather than investing in the development of a new or updated encryption malware.

Finally, exfiltration is generally **more challenging to detect** than data encryption, as it can be disguised within legitimate network traffic. In contrast, the encryption process has an immediate and noticeable impact on the targeted system, making it more likely to be quickly intercepted by security teams. However, ransomware campaigns involving data exfiltration may **last much longer** compared to incidents without data theft, which puts into perspective the initial stealth advantage that exfiltration provides.

Based on ReliaQuest estimations from Q4 2024, the number of ransomware groups adopting exfiltration-only tactics will increase by at least 25% in the mid-term future.

From lucrative campaigns to intelligence gathering

While most actors mentioned above conduct **opportunistic, lucrative campaigns**, several state-sponsored intrusion sets were also reported **leveraging commodity ransomware** with exfiltration capabilities to **disguise their espionage activities**.

In mid-2024, the FBI and CISA reported on the Iranian state-sponsored **APT33** collaborating directly with **commodity ransomware-as-a-Service** (RaaS), most likely to **steal sensitive information** from the targeted networks. Also, the China-nexus APT **ChamelGang** leveraged the **CatB** ransomware since at least 2022 in campaigns aiming at intelligence collection, as well as Personal Identifiable Information (PII) theft and financial gain.

Similarly, the North Korean state-sponsored group **Andariel** was observed in a campaign related to **Play** ransomware, suggesting involvement in data collection, and possibly data exfiltration activities.

Another valuable observation is certain **double extortion ransomware groups** that used to operate as lucrative and opportunistic **added espionage activities to their arsenal**. Indeed, the intrusion set operating the **RomCom backdoor** which is also associated with **Cuba** ransomware was repeatedly reported to conduct opportunistic ransomware and exfiltration operations, as well as attacks in support of intelligence operations.

We assess with high confidence that **synergies** between **profit-driven** ransomware groups and **state-sponsored** intrusion sets will **continue to grow** in the medium term, driven by objectives such as **attribution misdirection, disguised intelligence gathering, revenue generation**, and enabling **states to benefit from the advanced capabilities** of a few lucrative groups.

Part two

Data as leverage: targeting valuable information

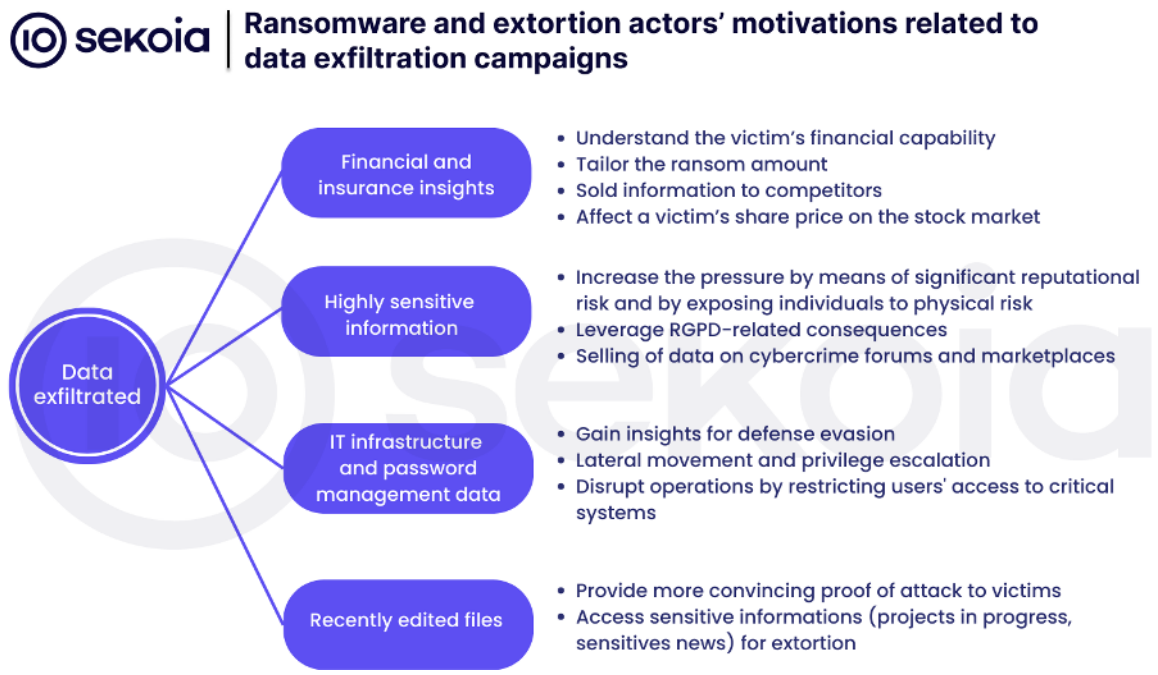
When ransomware operators navigate through a victim's data, their primary goal is to **identify high-value, sensitive information** that could be leveraged for **double extortion**, to maximise the pressure on victims. They also aim to **speed up the exfiltration process** by avoiding downloading too large volumes of generic data.

The groups that include exfiltration in their campaigns commonly target **specific file extensions** that could contain data of interest, which include document files (.doc, .xls, .ppt), text and data files (.txt, .csv), database files (.sql). At the same time, they often avoid exfiltrating backup and snapshot files.

To achieve this, ransomware operators often employ techniques such as **searching for specific keywords** within files and directories, relying on either **manual browsing** or **hardcoded commands**, embedded in the deployed tool or malware.

In certain cases, ransomware operators manage to **preview selected documents** before they collect and exfiltrate them (*e.g.* BlackCat, INC ransomware).

In the paragraphs below, we outline several **categories of data** that ransomware actors particularly target during exfiltration.



Financial and insurance-related data

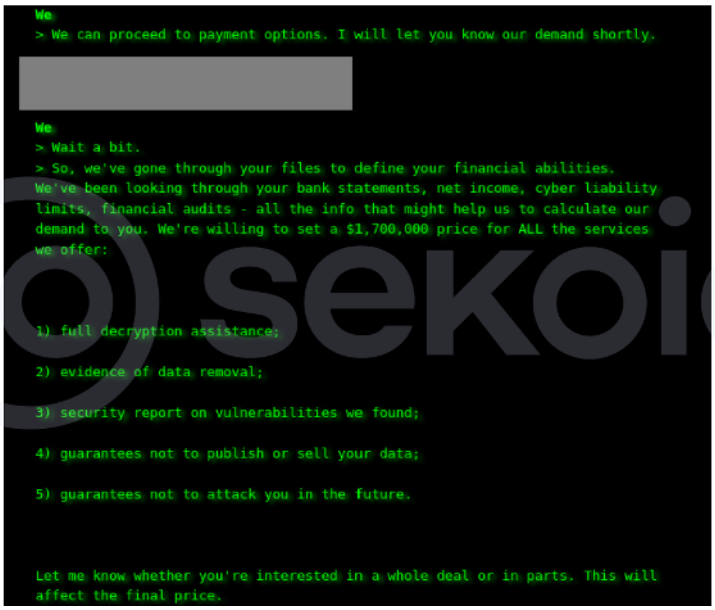
Numerous ransomware operators demonstrate an **interest in financial repositories** during the exfiltration phase. Financial information exfiltrated by ransomware actors typically include accounting and financial transaction data, insights on the insurance coverage, salaries databases, *etc.*

To do so, ransomware actors scan networks prior to exfiltration for **finance-related keywords** included in specific files and directories. For example, **RansomEXX** campaigns were reported to leverage the Pyxie Remote Access Trojan (RAT) for collecting data of interest based on the following keywords: "10-q", "10-sb", "n-csr", "nasdaq", which are terms related to financial regulatory filings and disclosures, and stock exchanges.

The same applies to **Ryuk**, **Pysa** and **Embargo** ransomware variants that contain hardcoded commands to search for "finance" and "Accounting" directories. Also, Mandiant observed the PowerLift tool being leveraged by an unknown ransomware actor in a 2023 campaign to exfiltrate data related to the victim's financial operations and other confidential information.

In the final stages of an attack, ransomware actors can leverage those financial insights to assess a victim's financial capacity and **tailor ransom demands** to increase the likelihood of payment. These demands are often calculated based on the victim's reported revenue or their insurance coverage. For instance, **Akira** ransomware operators explicitly state in their ransom notes: "We will thoroughly examine your financial records, including bank statements, savings, and investments, to present you with a reasonable demand". Moreover, based on Reliaquest observations from Q3 2024, **organisations mentioning cyber insurance** during negotiations were **more likely to pay ransoms** closer to the initial demand compared to those that didn't.

Akira ransomware operators' statement during negotiations on the group's dedicated portal



In cases where the ransom is supposedly not paid, **exposing such information poses significant risks** for impacted organisations. Indeed, ransomware groups were previously reported leveraging significant, time-sensitive financial events like announcements, mergers and acquisitions to **adjust the timeline of the attack** to **increase pressure** on victims during the extortion phase. Former declarations by Revil and DarkSide representatives clearly illustrate this point, as the ransomware operators expressed an interest in **affecting a victim's share price** on the stock market, for example by notifying market traders before publicly claiming the attack.

Such impact was in fact reported in campaigns conducted by **LockBit** affiliates, which **affected the victim's financial position** and its ability to secure additional investment and funding. Furthermore, if the attackers make the data publicly accessible or sell it, **competitors may also gain insights** into a company's financial information and potentially leverage it to engage in anti-competitive practices.

Highly sensitive information

A number of ransomware campaigns we observed over the past years aim to exfi**ltrate highly sensitive data**, *e.g.* confidential documents, government-related data, highly sensitive personal data, medical and legal information, *etc*.

For instance, the **Vice Society** ransomware group was reported using a custom PowerShell to target highly sensitive information within the victim's network, pointing to potential **acts of harm and abuse**. During intrusions, they typically tailor this script to search for directory and file names containing terms like *violence*, *abuse*, *theft*, *stealing*, *humiliation*, *harassment*, and *death*.

Similarly, a custom exfiltration tool leveraged by **Ryuk** ransomware operations targeted a range of high-value entities, including **military operations** and federal agencies. The ransomware used specific keywords to gather sensitive information, particularly focusing on confidential, **classified data** related to military activities and **criminal investigations**. This highly likely aims to identify documents that can cause **significant reputational harm if exposed** and to put greater pressure on victims during negotiations for ransom payment.

Medical records are also highly prized by ransomware actors such as **Akira**. This is due to the sensitive nature of the information they contain (personal identification details, protected health information, biometric data, medical histories), making it a **valuable asset in negotiations** (infrastructures with sensitive information are more likely to pay in this case), but also on cybercrime marketplaces.

In addition to the direct consequences for patient care that ransomware attacks on healthcare facilities can have, like delay in critical operations and disruption in essential healthcare services leading to endangering patients' well-being, **failing to secure stored medical information** could result in **significant fines** and **damage an organisation's reputation**. Indeed, several countries have **strict data security laws** stipulating that sensitive information like medical records must be stored in accordance with regulations such as the General Data Protection Regulation (GDPR).

IT infrastructure and password management data

Many ransomware operations are interested in accessing **IT-related information**, particularly resources containing **password management data**. For example, **Phobos** ransomware operators target technical documents (including network architecture) and databases for password management software during the exfiltration phase. A **Nokoyawa** operator was also observed browsing file shares, looking at password related documents, as well as a **Dagon Locker** actor that accessed files related to the IT department and containing corporate passwords prior to exfiltration.

In incidents related to **BlackCat**, a **custom tool** named "confucius_cpp" was leveraged to search for the "**security_reports**" keyword on shared folders. Moreover, BlackCat operators were also observed collecting **domain information** and data related to computers, trust information and devices connectivity. The **ExMatter** exfiltration tool was also reported targeting specific files pertaining to web and application source code, Remote Desktop shortcuts, Computer-aided design (CAD) and Geographic Information Systems (GIS) files. The same applies to **Cuba** ransomware, exfiltrating **source code** data if the victim is a software developer.

Collecting IT-related data could be used to **access sensitive information**, gain **remote access**, or resold it to other malicious actors. Gathering insights about a company's network infrastructure also enables ransomware operators to perform **lateral movement** and **privilege escalation** after an intrusion. **Vulnerabilities found in the source code** could also be exploited for future attacks.

They can further **disrupt operations** by restricting legitimate users' access to critical systems through password changes or tampering with access controls. The obtained accesses could also be sold for other intrusion sets to use. However, the value of such data may be limited, as users often change passwords once they are aware of a breach.

Recently edited files

Multiple ransomware actors specifically target recently edited files for exfiltration. This tactic was notably observed during **DarkSide**-related operations in 2021, and in campaigns leveraging the **ExMatter** tool throughout 2021 and 2022. These campaigns prioritised **files created within the past year** or those **most recently modified**. In the second half of 2024, Arctic Wolf also documented **Akira** and **Fog** ransomware intrusions that only exfiltrated up to **six months' worth of data**, and expanded it up to 30 months for the folders containing potentially more sensitive information.

By focusing on recent files, attackers can better understand the victim's current activities, allowing them to gather **sensitive information in use** at the time of the intrusion, such as ongoing confidential projects, strategic developments, or undisclosed business transactions.

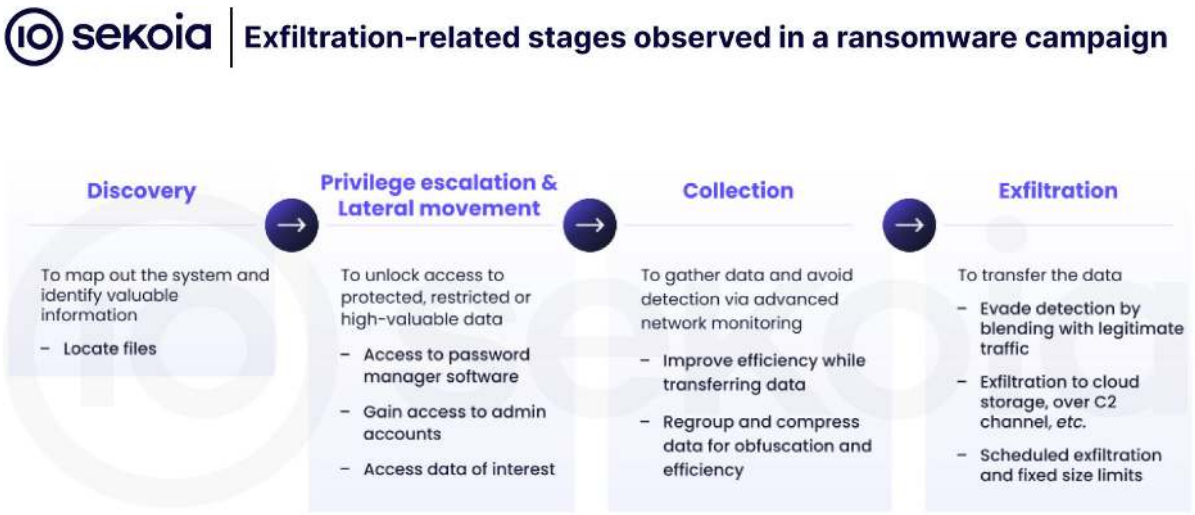
This **up-to-date** and potentially valuable data provides **critical proof of the attack**. The threat of leaking sensitive, often non-public information stands as an additional method to pressure victims into paying the ransom, as its disclosure could damage the victim's reputation, disrupt ongoing projects, or impact future business deals.

Part three

Understanding the exfiltration process: the role of custom, commodity and publicly available tools

In this section, we will detail the **exfiltration process** and introduce the **custom, commodity and publicly available tools and malware** used by ransomware and extortion groups to **facilitate data exfiltration**.

We will break this down according to their intended use in exfiltration campaigns. Many of these groups use a combination of both custom and publicly available tools for different purposes such as **enumeration**, **compression** and **uploading** in accordance with their specific features.



Data exfiltration in ransomware attacks can rely on **manual or automated actions**, involving several stages that progressively lead to the theft and transfer of valuable information.

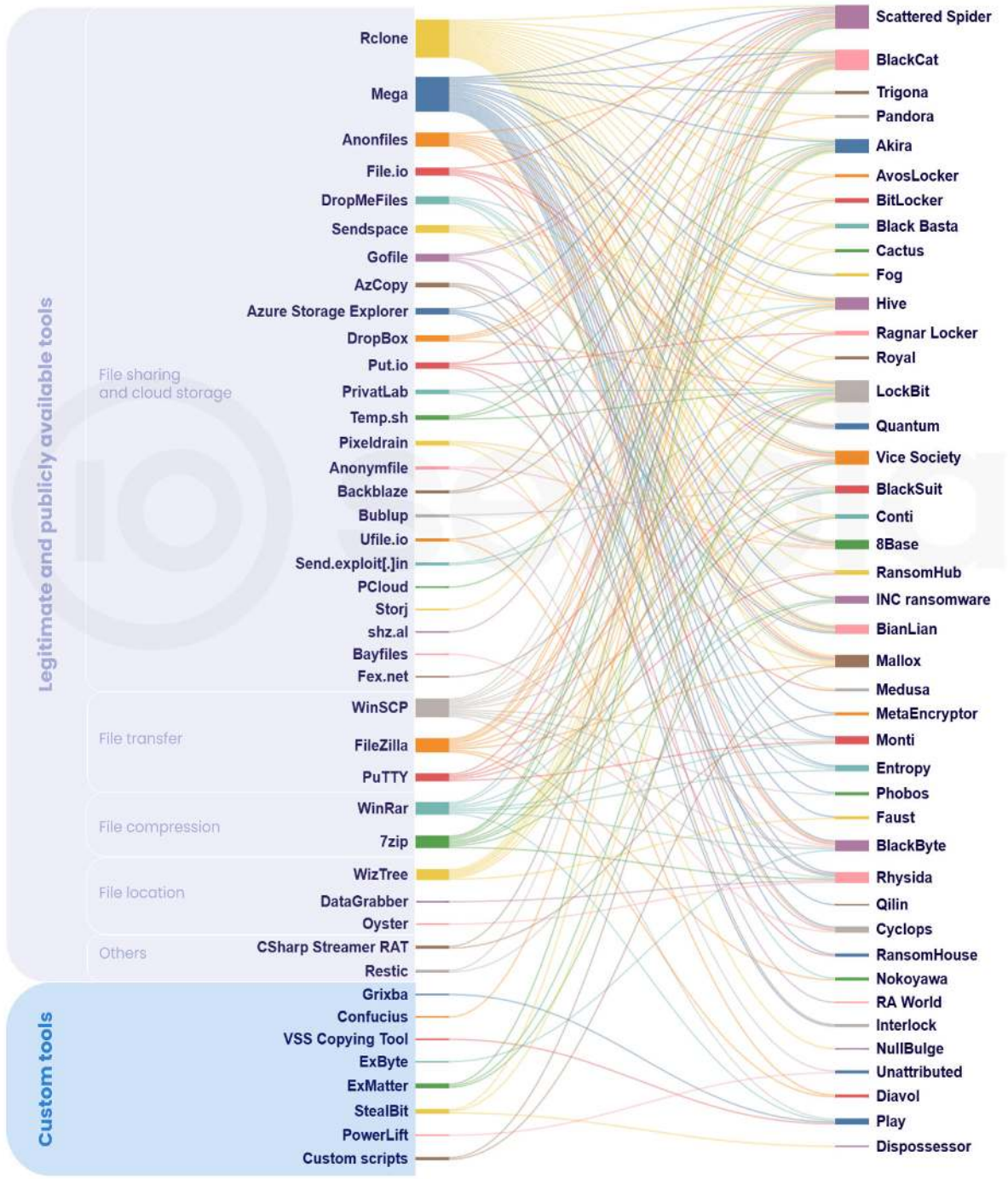
Following initial compromise, the data exfiltration process is designed to **identify**, **extract**, and **transfer** sensitive information from a victim's network to an infrastructure controlled or misused by the attacker. The graph above illustrates the different exfiltration-related stages that can be observed in a ransomware-driven campaign.

Reconnaissance represents the first step during which the attackers identify information of interest for later exfiltration. Then **privilege escalation** could lead to **lateral movement** where the attackers could gain access to new accounts with higher privileges and access to high-valuable information. **Data compression**, which is part of the collection phase, is an optional step before the **transfer of collected data**, in which the files' size is reduced to enhance stealth and evade detection.

In most double extortion campaigns, **data exfiltration** occurs **prior to data encryption**. However, there are isolated cases where exfiltration took place after completed encryption, likely to track victim's incident response and recovery efforts.

During all these stages, ransomware actors rely on a **wide range of tools** to facilitate data exfiltration, which we will detail in the following sections of this report.

Tools most used by main ransomware operations to facilitate exfiltration in lucrative campaigns, from 2022 to November 2024, based on open-source reporting



Custom tools and malware

A certain number of ransomware actors develop and leverage their own tools and malware to facilitate data exfiltration. Custom tools can vary from a **simple script** to a **fully operational tool** with different commands. They could also be sold to other threat actors, which could then mislead attribution.

Using custom tools possesses certain advantages over publicly available tools, providing attackers with **greater control** over functionalities and data targeting, and therefore improved efficiency. Indeed, attackers are able to continuously **tailor specific elements** to avoid detection, especially if their infrastructure was already observed in previous attacks. This in turn requires **greater investment** of resources by malicious actors.

Further, custom tools can be **more precise in the type of collected data**, such as enabling the search for specific keywords. Moreover, by maintaining greater control over the exfiltration process and automating key tasks, attackers can minimise the time required for exfiltration and therefore the dwell time[1] of a ransomware attack. This also reduces the risk of detection, as extended campaigns are more likely to be spotted due to a greater number of artefacts left behind in the logs.

From our observations, custom exfiltration tools are developed by **relatively advanced groups** in terms of malware development and maintenance. However, we observe that the use of custom tools to facilitate exfiltration is still limited to a relatively small number of intrusion sets. Moreover, Mandiant assesses that custom data exfiltration tools were used in a smaller number of cases compared to publicly available tools, based on their observations over 2023.

Scripts

As for some examples of custom exfiltration tools, there are **custom scripts** where intrusion sets can add their own elements with different objectives, like automated exfiltration with the C2 of the actor directly in the script, or to install other tools used for collection and exfiltration.

Vice Society performs automated exfiltration with a custom script that connects to the intrusion set's web server via an HTTP request. **Mallox** has a custom shell script to deliver and execute the payload, and also to exfiltrate the victim's information to two servers. This allows attackers to have a backup of the data.

[1] The time between the initial intrusion and completion of encryption

Enumeration tools

Another type of custom tools observed in data exfiltration campaigns are **enumeration tools**, which are useful in the discovery and collection phases of an attack. The **Play** ransomware group is particularly known for developing such tools. This group is behind the custom tool **Grixba**. It is designed to list all users and computers within a domain, and to enumerate software and services using legitimate applications such as Windows Management Instrumentation (WMI) and Windows Remote Management (WinRM). The tool also gathers information on security solutions and backup software, regrouping it into a ZIP file before exfiltration. The second custom tool attributed to Play is the **VSS Copying Tool**, which is used to enumerate files and folders in VSS snapshot and copy the files to a chosen destination, before their encryption.

Uploading files

The following custom tools are leveraged by ransomware actors during the exfiltration stage, typically by transferring the data to a server controlled or misused by the threat actor.

ExByte is a custom data exfiltration tool developed and deployed by the **BlackByte** group since late 2022. While ExByte is also capable of enumerating files during the collection phase, it is notably used for uploading selected files to the cloud storage platform **Mega**. BlackByte actors operate **a dedicated Mega account** accessing it through API authentication with **credentials hardcoded** directly into ExByte. While incidents involving ExByte were still reported over 2023, its use likely declined, with fewer, sometimes unconfirmed, cases reported in 2024. As of October 2024, ExByte remains **exclusively associated with the BlackByte group**.

Another example is the **BlackMatter** intrusion set observed using **ExMatter**, a custom tool which can select specific files and send them to a server before loading the ransomware. This custom tool can **destroy itself** if it is deployed on a virtual environment or a sandbox for example. It can also corrupt exfiltrated files and create a report for them. These abilities make this custom tool advantageous for threat actors as opposed to more open-source tools. Of note, variants of this tool have been reported being **leveraged by other RaaS groups** such as LockBit and Conti. We assess with medium confidence that ExMatter is either sold to other ransomware groups or actively shared among former BlackMatter affiliates.

StealBit is an exfiltration tool developed by the **LockBit** intrusion set. Unlike other tools that rely on third-party cloud-sharing services, StealBit directly sends data to the LockBit Data Leak Site. According to LockBit developers, the tool offers a better bandwidth for data exfiltration compared to other ransomware. Of note, StealBit was reported being **used to deliver other ransomware** than LockBit, such as Dispossessor, and was also leveraged by the intrusion set DEV-0504 to deploy multiple ransomware over time. We could also mention **PowerLift**, a custom exfiltration tool reported being used in 2023 by an unidentified ransomware actor. As of October 2024, there is no further information available concerning this tool.

Commodity malware

Beyond their custom tooling, ransomware groups also occasionally employ **commodity malware** to facilitate data exfiltration. Taking advantage of readily available tools simplifies and accelerates the collection and transfer of sensitive information, making the whole process more cost-effective.

In the collection phase, intrusion sets deploy **commodity infostealer** malware (*e.g.* Scattered Spider using Meduza, Lumma, *etc.*) to gather databases, documents, passwords and other sensitive information from victims.

Other groups like BlackCat and MetaEncryptor were observed using **CSharp Streamer RAT** for exfiltration purposes. Notably, it was used by BlackCat to access the file and backup servers with an RDP connection created by CSharp Streamer. Based on the distinctive malware patterns observed over successive campaigns and its modular structure, researchers at HiSolutions assess that CSharp Streamer might be a **MaaS**.

Legitimate and publicly available tools

On the other hand, multiple ransomware groups use **legitimate and publicly available tools** to facilitate exfiltration during attack campaigns. The **variety** and **accessibility** of off-the-shelf exfiltration-related tools provide attackers with numerous options to conduct their exfiltration campaigns more effectively.

Although these tools offer **limited customisation options** for attackers, they are often free and highly accessible. However, they are also usually more well-known by security teams, making them easier to detect - unless they can be legitimately employed for non-malicious purposes. Consequently, detecting malicious activity becomes more challenging when it involves the use of legitimate tools.

File location

Ransomware actors typically use publicly available file location tools to navigate the victim's environment and **identify valuable data** for exfiltration, while blending in with legitimate actions to avoid detection.

An example of a tool leveraged for locating files within the compromised system is **WizTree**, which could be used to qualify files according to their size by analysing the disk. Indeed, the intrusion set behind **Faust** ransomware, a variant of **Phobos**, was reported to use WizTree to get a detailed list of files before exfiltration. While the exact activities Faust performed with this tool are not known, we assess that ransomware groups can leverage WizTree to rapidly identify large files to avoid exfiltrating them, for **time optimisation** and **detection evasion**.

File compression

Before transferring the collected data from the victim's environment, ransomware groups commonly leverage **compression tools** to **avoid detection** of large data transfers. Most often, attackers use legitimate tools to **reduce the data size** without raising suspicion, thus enhancing stealthiness and furtiveness.

WinRAR is an example of one such tool, often used for **creating archives** in exfiltration campaigns attributed to ransomware such as INC, Akira, Play and others. **7-Zip** is another tool typically used to compress files and create archives with an additional protection layer to the collected data by **adding a password**. This is most probably done to **block the victim's access** to the content of collected and exfiltrated data.

File sharing and cloud storage solutions

Some publicly available exfiltration tools, often designed as solutions for enhanced data protection, such as cloud file-sharing solutions, can be exploited by ransomware groups for malicious purposes.

Mega is such a cloud platform used for sharing files. Ransomware groups can use it to host exfiltrated data without being detected, especially if the victim already leverages it for its own needs. Most ransomware actors use the Mega platform by default when transferring files, often in association with **MEGAsync** and **Rclone**.

Rclone is an open-source tool used to manage and upload files to cloud solutions, notably aiming to automise the exfiltration process. It is extensively used by ransomware operators, being **the tool most widely used in data exfiltration** since at least 2021 and up to 2023. In 2023, it was leveraged in 30% of intrusions observed by Mandiant.

Some operators were reported **embedding their Mega credentials in Rclone**, yet this was also seen in link with other exfiltration tools (*e.g.* BlackByte when deploying ExByte).

As creating an account is mandatory when using Mega, the proactive monitoring of observed accounts can be useful to the attribution of a campaign or to the understanding of connections between ransomware operators and affiliates.

For example, the ACS CTI team reported on **Trigona** and **BlackCat** ransomware groups using **Rclone** to transfer exfiltrated files to the **same Mega account** in two different incident response cases. This is highly likely indicative of overlaps among the Trigona and BlackCat operators and/or affiliates.

Another prominent duo **increasingly used** to exfiltrate the victim's data to an attacker-controlled cloud storage solution is **Azure Storage Explorer** leveraging the utility **AZCopy**. Rhysida, BianLian and Interlock intrusion sets were already reported using them in the second half of 2024. We assess that **Microsoft Azure tools will be increasingly leveraged** in ransomware attacks for exfiltration purposes, notably due to their scalability, their efficiency when uploading large data via multiple instances and their ability to disguise as a trusted corporate service.

Another way to exfiltrate data involves file-sharing solutions like **Dropbox**, a legitimate tool widely used to share files between users. For instance, **Pandora** was seen using it in association with the exfiltration tool **Rclone**.

Similarly, **OnionShare Service** is an open-source tool that allows sharing files anonymously. By **using the Tor network**, attackers can hide by masking the IP address of their server which makes identifying their infrastructure more complex. For example, the intrusion set deploying **Alpha** uses OnionShare to host the compromised data. From a defender's perspective, the use of the Tor network can be an indicator of suspicious activity if it is uncommon in a given environment.

WinSCP is a tool designed to copy files from a local computer to a remote one. It is often used as an alternative to the transfer of files via the attacker's C2 server. The data transferred is protected with cryptographic methods. For instance, **Akira** was observed using WinSCP along with **FileZilla** to exfiltrate archives.

FileZilla is an open-source tool that uses the File Transfer Protocol to move files between computers. The protocol in itself is not malicious, it is the use of it by a ransomware group to exfiltrate data which detection teams should look out for. As an example, we can see it with **Nokoyawa** using FileZilla before deploying ransomware, as did **Diavol**, which installed the tool directly onto infected systems before exfiltrating large databases. In fact, the installation of **FileZilla** followed by large data transfer via this tool could be an indicator to detect suspicious usages.

Open-source tools are legitimately used making malicious use challenging to detect amidst regular traffic. This could lead to lots of false positives. However, it is essential to monitor these tools to ensure protection on all the different techniques used by attackers as these tools can be diverted from their legitimate use.

Part four

Detecting ransomware-related exfiltration attempts

Since exfiltration is, for most ransomware-related intrusions, a precursor of the encryption phase, it is essential for companies to protect themselves by **detecting exfiltration attempts at their earliest** to minimise the impact of a potential ransomware deployment. They can also focus on earlier stages such as initial access, privilege escalation as well as reconnaissance and lateral movement to be more efficient.

To be more effective in the investigation and the detection of an exfiltration attempt, a multimethod approach strategy should be set up to identify suspicious behaviour. **Sigma correlation** and **anomaly rules** are a must-have to detect suspicious actions, especially those performed via legitimate tools. Indeed, an attacker can use a variety of tools for reconnaissance, data collection and finally exfiltration. A correlation rule can help to identify these activities, such as detecting the use of a compression tool followed by the exfiltration of the compressed files, indicating a potential malicious behaviour. Meanwhile, anomaly rules focus on suspicious actions based on the specific environment.

Detecting access followed by suspicious file movement

A potential indicator of an exfiltration attempt could be **unusual access** to an **abnormal number of sensitive data**, followed by its **subsequent movement**. Suspicious activity often includes a high number of downloads or external sharing attempts, which should raise suspicion.

It is essential to focus on monitoring critical files and directories which are more likely to be targeted by attackers due to the valuable and sensitive information they contain, which can increase leverage over victims. To mitigate risks, security teams should implement rules related to the access to these specific files and directories. For example, monitoring should focus on the discovery and collection of files within an "admin" directory or similar high-risk locations. The data transfer from an internal network to unknown hosts or suspicious ports could also be a lead for detection rules, as it could indicate an exfiltration to an external network.

Detecting known indicators of compromise

Another way to detect unauthorised transfer of files is by detecting the presence of **indicators** known to be **related to exfiltration** like C2 IP addresses or domain names. A focus should be placed on domains associated with **cloud storage** sites as well as common **file-sharing** sites used by attackers.

During a typical double extortion campaign, attackers can also regroup the data before exfiltration. For instance, the intrusion set deploying **Play** uses its custom tool **Grixba** to add all the stolen data into a single CSV file before exfiltration. By doing so, attackers can create new files or leave indicators of data moved and/or copied.

Detecting those indicators, or else the attackers' attempts to remove these traces, can aid in detection of exfiltration attempts, and also in early detection of ransomware activity.

> Since 2023, the Sekoia Threat & Detection (TDR) team monitors a **LockBit ransomware affiliate**'s operations, including its use of the **ExMatter** exfiltration tool. The proactive monitoring of implemented servers allowed us to collect over 80 IP addresses of exfiltration servers, as of November 2024.

Detecting tool usage

Exfiltration attempts can also be detected by identifying specific tools used in the process. Nevertheless, many open-source exfiltration tools are legitimate, which makes detecting malicious usage challenging. To mitigate this, it is useful to implement rules targeting **suspicious behaviour** associated with the tools known to facilitate data exfiltration.

First, it is essential to monitor exfiltration attempts observing **processes with names related to common open-source tools**. In the same way, ransomware operators often deploy various tools and scripts with names directly linked to the ransomware, before encryption or exfiltration begins. Second, we can monitor the command lines and look out for **tool-specific commands** as an intrusion set can change processes' and tools' names to evade detection.

Focus on detecting multiple tools with different techniques allows having a better visibility on the attack surface and extending the detection radius.

> Based on a Sekoia investigation following an exfiltration attempt from the ransomware **DragonForce**, we managed to retrace the different events prior to the ransomware deployment. First of all, threats were detected on multiple assets after some suspicious brute force and login from an unknown account. Then focusing on this account, we discovered several suspicious commands to impair defences and to gain access to databases. In this attack, the intrusion set used **Rclone** and **Mega** for the exfiltration phase.

Conclusion

Ransomware groups continue to evolve, leveraging data exfiltration as a primary or secondary technique to **generate revenue**. Exfiltration of sensitive information **primarily supports their double extortion campaigns**, threatening victims with public exposure of stolen data.

We assess with high confidence that ransomware intrusion sets will **increasingly rely on data exfiltration** as a means of extortion. Additionally, it is likely that a greater number of today's ransomware actors will focus exclusively on exfiltration without encryption in their extortion campaigns. This approach requires less effort, allowing attackers to remain undetected within the system for a longer period, while still exerting pressure on the victim.

With data in attackers' possession victims face **continued risk** - even after paying a ransom - of data exposure, repeated attacks or even legal repercussions following the breach. Additionally, the victims' ability to pay may prompt other malicious actors to conduct further attacks for financial gain.

To support their exfiltration campaigns, ransomware and extortion groups leverage a wide range of **custom-built**, **commodity** and **publicly available tools** and **malware**. **Advanced groups** often invest more resources into developing **proprietary tools**, enabling customisation to suit specific attack objectives. These custom tools may be shared among all the affiliates in the case of a RaaS operation, or even **adopted by other intrusion sets**. This practice is indicative of the continuously interconnected and collaborative nature of the ransomware cybercrime ecosystem. Nevertheless, from our observations over the past years, **intrusion sets most often used publicly available tools** and utilities to exfiltrate data from victim environments.

The **rapid adoption** and deployment of customised or publicly available tools is further challenging for detection and attribution, highlighting the need for **close monitoring of exfiltration techniques** rather than solely focusing on specific tools. For greater value, detection efforts should prioritise identifying techniques and activities in the pre-exfiltration phase to provide more effective protection and prevent damage. Focusing on the **discovery and collection phases**, instead of doing this only on the actual transfer of stolen files, is essential for effective detection.

While monitoring the use of the tools known to facilitate exfiltration can serve as a starting point for creating detection rules, they can also be disguised by attackers to prevent straightforward detection strategies. To counter this, detection teams should prioritise **anomaly-driven** detection engines and **correlation rules** to identify a wide range of exfiltration methods.

In the case of double extortion campaigns, **early detection** represents a pivotal step for security teams to detect an intrusion before encryption impacts the targeted system. Given that ransomware groups continually adapt their tactics to evade detection and bypass defences, detection rules must be regularly updated and reviewed to strengthen the defence.

List of references

"Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up" - *KrebsOnSecurity*, December 2019

"A case of the FAUST Ransomware" - *Truesec*, 01 December 2023

"Highlights from the 2021 Unit 42 Ransomware Threat Report" - *Global Security Mag*, March 2021

"Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools" - *Google Cloud*, 03 June 2024

"How Data Exfiltration is Changing the Ransomware Landscape" - *Blackfog*, 19 February 2024

"#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability" - *CISA*, 07 June 2023

"Technical Analysis of Industrial Spy Ransomware" - *Zscaler*, 01 August 2022

"Threat Assessment: Luna Moth Callback Phishing Campaign" - *Unit 42 Palo Alto*, 21 November 2022

"#StopRansomware: BianLian Ransomware Group" - *CISA*, 16 May 2023

"Hive Ransomware's Offspring: Hunters International Takes the Stage" - *BitDefender*, 09 November 2023

"Akira, again: The ransomware that keeps on taking" - *Sophos*, 21 December 2023

"Ransomware and Cyber Extortion in Q3 2024" - *Reliaquest*, 15 October 2024

"Akira ransomware continues to evolve" - *Talos*, 21 October 2024

"Decrypted: BianLian Ransomware" - *Decoded Avast.io*, 16 January 2023

"Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations" - *CISA*, 28 August 2024

"ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware" - *SentinelOne*, 26 June 2024

"Nameless and shameless: Ransomware Encryption via BitLocker" - *NCC Group*, 08 November 2024

"IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment" - *the DFIR report*, 10 June 2024

"Investigating New INC Ransom Group Activity" - *Huntress*, 11 August 2023

"Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims" - *IC3*, 01 November 2021

"Possible Ryuk-Based FTP Stealer/Uploader" - *Vitali Kremez on Twitter*, 11 September 2019

"Mespinoza Ransomware Gang Calls Victims "Partners," Attacks with Gasket, "MagicSocks" Tools" - *Unit 42 Palo Alto*, 15 July 2021

"The Rust Revolution: New Embargo Ransomware Steps In" - *Cyble*, 24 May 2024

"Inside Akira Ransomware Negotiations" - *Lab539*, 06 August 2024

"Sodinokibi Ransomware May Tip NASDAQ on Attacks to Hurt Stock Prices" - *BleepingComputer*, 26 February 2020

"UK logistics firm blames ransomware attack for insolvency, 730 redundancies" - *The Record*, 26 September 2023

"CrowdStrike, 2023 Global Threat Report" - *CrowdStrike*, 2023

"Information-Stealing Malware with Connections to Ryuk Targets Government, Military, and Financial Files" - *Trend Micro*, 16 September 2019

"Watchtower 2023" - *SentinelOne*, January 2024

"#StopRansomware: Phobos Ransomware" - *CISA*, 29 February 2024

"From OneNote to RansomNote: An Ice Cold Intrusion" - *The DFIR Report*, 01 April 2024

"From IcedID to Dagon Locker Ransomware in 29 Days" - *The DFIR Report*, 29 April 2024

"The many lives of BlackCat ransomware" - *Microsoft*, 13 June 2022

"Analyzing Exmatter: A Ransomware Data Exfiltration Tool" - *Kroll*, 22 Mars 2022

"From Caribbean shores to your devices: analyzing Cuba ransomware" - *Securelist by Kaspersky*, 11 September 2023

"Inc Ransom Attack Analysis" - *Reliaquest*, 06 August 2024

"Newly Discovered Function in DarkSide Ransomware Variant Targets Disk Partitions" - *Fortinet*, 17 May 2021

"BlackMatter: New Data Exfiltration Tool Used in Attacks" - *Symantec*, 01 November 2021

"Arctic Wolf Labs Observes Increased Fog and Akira Ransomware Activity Linked to SonicWall SSL VPN" - *Artic Wolf*, 24 October 2024

"Vice Society: A Tale of Victim Data Exfiltration via PowerShell, aka Stealing off the Land" - *Unit 42 Palo Alto*, 13 April 2023

"TargetCompany's Linux Variant Targets ESXi Environments" - *Trend Micro*, 05 June 2024

"Play Ransomware Group Using New Custom Data-Gathering Tools" - *Symantec*, 19 April 2023

"FLINT 2023-028 - Unveiling a LockBit ransomware affiliate's operations" - *Sekoia.io*, 17 May 2023

"A BlackByte Ransomware intrusion case study" - *Microsoft*, 19 May 2024

"Exbyte: BlackByte Ransomware Attackers Deploy New Exfiltration Tool" - *Symantec*, 21 October 2022

"The five-day job: A BlackByte ransomware intrusion case study" - *Microsoft*, 06 July 2023

"BlackByte blends tried-and-true tradecraft with newly disclosed vulnerabilities to support ongoing attacks" - *Talos*, 28 August 2024

"HC3: Analyst Note" - *Health Sector Cybersecurity Coordination Center*, 12 December 2022

"THREAT ANALYSIS REPORT: Inside the LockBit Arsenal - The StealBit Exfiltration Tool" - *Cybereason*, 2021

"Dark Web Profile: Dispossessor Ransomware" - *SOCRadar* , 17 May 2024

"Inside Intelligence Center: LUNAR SPIDER Enabling Ransomware Attacks on Financial Sector with Brute Ratel C4 and Latrodectus" - *EclecticIQ*, 30 October 2024

"How to detect the modular RAT CSHARP-STREAMER" - *HISOLUTIONS*, 25 June 2024

"The Active Adversary Playbook 2022" - *Sophos*, 07 June 2022

"The 2024 Ransomware Threat Landscape" - *Symantec*, 2024

"BlackCat & Trigona Ransomware Connection" - *Alex Necula on LinkedIn*, 2024

"Highway Blobbery: Data Theft using Azure Storage Explorer" - *modePUSH*, 14 September 2024

"Unwrapping the emerging Interlock ransomware attack" - *Talos*, 07 November 2024

"Ransomware gangs now abuse Microsoft Azure tool for data theft" - *BleepingComputer*, 17 September 2024

"Log4Shell Vulnerability in VMware Leads to Data Exfiltration and Ransomware" - *Trend Micro*, 28 June 2022

"ALPHA Ransomware launched DLS" - *Rakesh Krishnan on Medium*, 26 January 2024

"Aki-RATs – Command and Control Party" - *Intrinsec*, 28 November 2023

"Diavol Ransomware" - *The DFIR Report*, 13 December 2021

About Sekoia.io TDR team

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform. TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

sekoia

About Sekoia.io

Sekoia.io is the European cybertech, leading provider of Extended Detection and Response (XDR) solutions based on Cyber Threat Intelligence (CTI). Its mission is to provide businesses and public organizations with the best protection technologies against cyber attacks.

By combining threat anticipation through knowledge of attackers (Sekoia Intelligence) with automation of detection and response, the Sekoia SOC platform (Sekoia Defend – XDR) provides security teams a unified view and total control over their information systems. Its interoperability with third-party solutions and compliance with international technical standards enable organizations to take full advantage of their existing technologies.

Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

Find more publications on blog.sekoia.io

Please don't hesitate to provide your feedback on our publications by clicking here.
You can also contact us at tdr@sekoia.io for further discussions.