Ransomware as a Service (RaaS)

Co-Author

Artie Crawford
NMFTA

TAM-C

Co-Author

TAM-C Intelligence Central

NMFTA National Motor Freight Traffic Association, Inc. | CYBER

White Paper: Assessing Ransomware-as-a-Service (RaaS) Threats Facing the Transportation Sector

Executive Summary

Ransomware remains one of the most relevant cyber threats to commercial enterprises. Within the ransomware ecosystem, threat actors continue to evolve and form new structures to develop malware, identify targets, and carry out attacks. The following white paper highlights one such structure, the Ransomware-as-a-Service (RaaS) operation, and dives deep into the unique threats it poses, particularly for the transportation sector.

This white paper will provide key insights into:

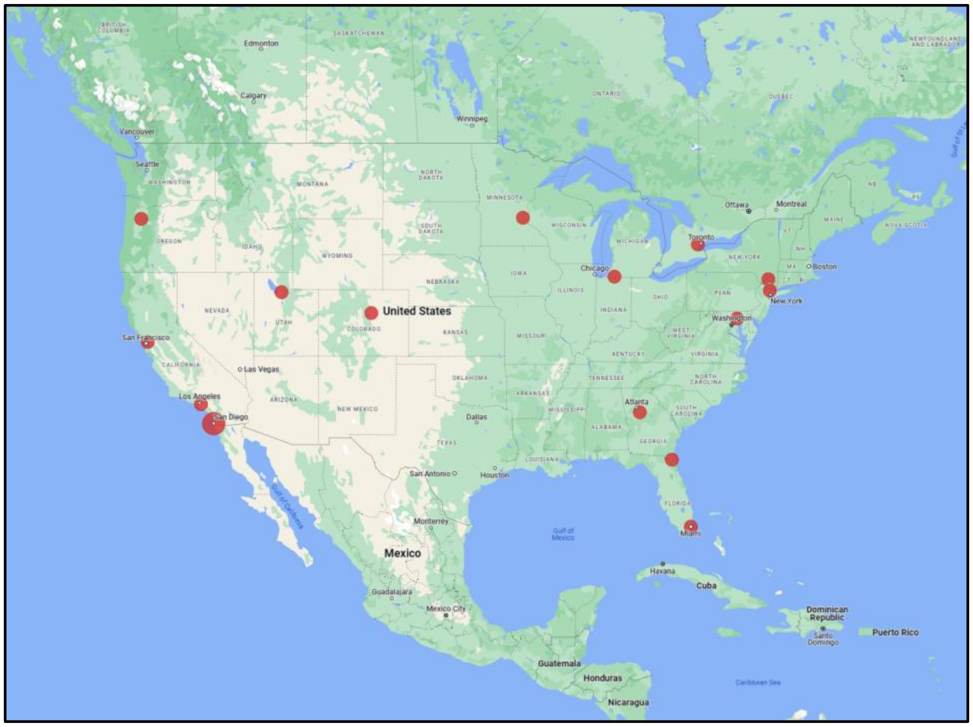
- Differences between conventional ransomware gangs and Ransomware-as-a-Service (RaaS) operations
- Background information, including details on tactics, techniques, and procedures (TTPs), for five of the most active RaaS operations in the current cyber landscape
- Context for how these operations pose threats for all businesses, including small and medium-sized companies, in the transportation sector

Introduction

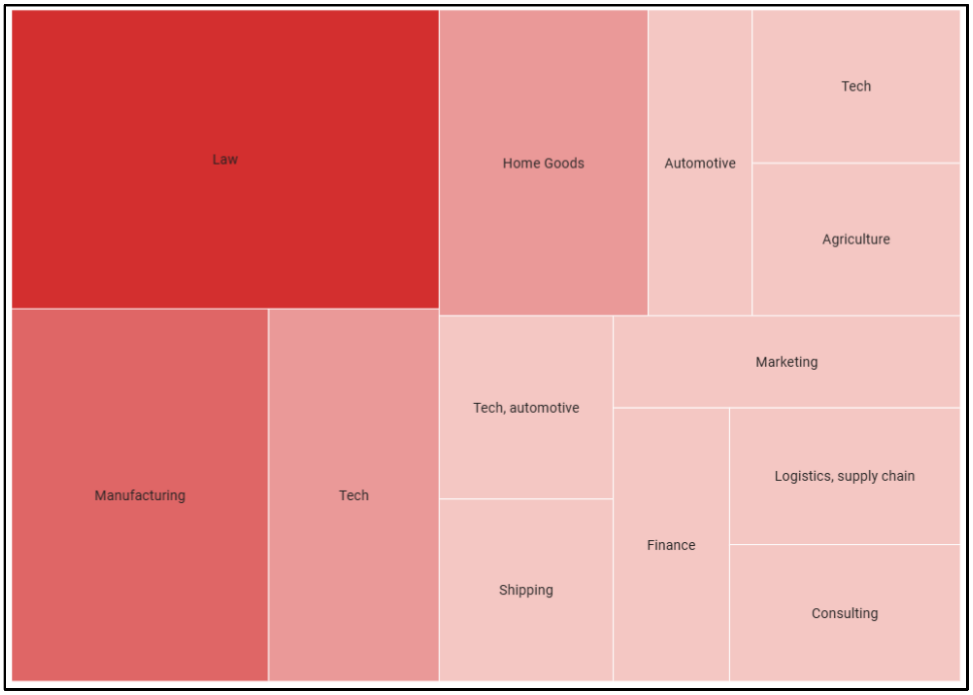
Late in the night on 17 April 2022, the pro-Russian ransomware gang Conti initiated an attack against the Costa Rican government in what became one of the largest ever ransomware attacks in history. Starting with the servers of the Ministry of Finance, which the gang had infiltrated with stolen login credentials, Conti began to exfiltrate sensitive information and encrypt critical data on the government's systems. Over the following days and weeks, the attack spread to over 30 other ministries and agencies, causing widespread chaos and disruptions to government services and functions before the gang ultimately demanded ransoms amounting to $10 million to decrypt the data on the impacted servers.

Government recovery and reconstruction of impacted cyber infrastructure took years and triggered ripples of panic throughout other small countries in Latin America and elsewhere in the world, prompting a push for heightened cybersecurity policies and awareness to prevent attacks of that scale from occurring again. But while Conti ravaged the Costa Rican government, the Ransomware-as-a-Service (RaaS) operation CL0P cyber gang was busy with its own debilitating attacks elsewhere in the world.

On 15 April 2022, just two days before the Costa Rica attack, Cl0P published a series of ransom notes on its Dark Web (DW) leak site claiming to have compromised and stolen data from 20 different small and medium-sized businesses, eighteen of which were located in North America and one of which was involved in import-export operations out of Miami, Florida. These CL0P attacks largely went unnoticed while media attention was elsewhere, and 16 of the 20 victims saw their stolen data published on CL0P's leak site just one week later, and the victims likely felt the impacts of these attacks for months and even years.



Above: *Map of CL0P ransomware attacks claimed on 15 April 2022*



Above: *Treemap of the number of CL0P ransomware attacks claimed on 15 April 2022, by sector*

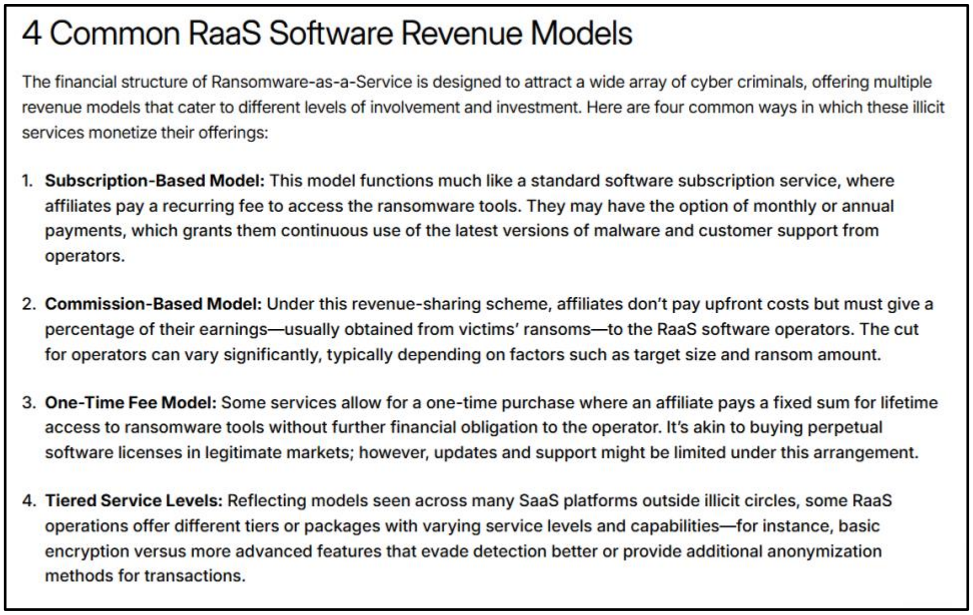
The Conti and CL0P attacks in April 2022 illustrate one of the key differences between conventional ransomware and RaaS operations. While conventional ransomware prioritizes large organizations capable of paying significant ransoms, RaaS targets more indiscriminately, posing a significant threat of economic and reputational losses for companies of all sizes. This white paper will dive deeper into RaaS operations, first by expanding on the similarities and differences between them and conventional ransomware. It will then spotlight several RaaS operators currently active in the cyber landscape today, including examples of specific tactics that these groups use during attacks. The paper will conclude by detailing how RaaS operations pose a threat to the transportation sector and offering key insights into why an awareness of the tactics used by these cyber-criminal organizations is relevant for trucking companies of all sizes.

Ransomware vs. Ransomware-as-a-Service (RaaS)

A Ransomware-as-a-Service (RaaS) operation describes a specific type of threat actor that uses the same type of malware variants seen across all forms of ransomware attack but that functions with a starkly different organizational structure. A malicious allusion to the Software-as-a-Service (SaaS) business model, RaaS is a paid service that a single operator offers to interested threat actors, known as affiliates, to carry out cyberattacks on their behalf and against the targets of their choosing. RaaS operators establish some form of agreement on target, tactics, and profit and sometimes offer affiliates the use of an online dashboard or application to organize and carry out these attacks.

The more complicated organizational structures of RaaS operations have produced an array of profit-sharing agreements. Proofpoint has identified several common types of revenue-sharing models in a review of known RaaS operators' Tactics, Techniques, and Procedures (TTP):

- **Subscription:** The RaaS operator provides affiliates access to the service for a subscription fee on a monthly or annual basis. A similar structure is a **one-time fee** granting lifetime membership to affiliates.
- **Commission:** A profit-sharing arrangement is implemented in the event of a successful attack, giving the operator and affiliate pre-defined percentages of the extracted ransom.
- **Tiered/customizable services**: The operator provides a quote for services rendered based on a selection of certain offerings, particularly for the inclusion of certain malware components or features.



4 Common RaaS Software Revenue Models

The financial structure of Ransomware-as-a-Service is designed to attract a wide array of cyber criminals, offering multiple revenue models that cater to different levels of involvement and investment. Here are four common ways in which these illicit services monetize their offerings:

1. **Subscription-Based Model:** This model functions much like a standard software subscription service, where affiliates pay a recurring fee to access the ransomware tools. They may have the option of monthly or annual payments, which grants them continuous use of the latest versions of malware and customer support from operators.

2. **Commission-Based Model:** Under this revenue-sharing scheme, affiliates don't pay upfront costs but must give a percentage of their earnings—usually obtained from victims' ransoms—to the RaaS software operators. The cut for operators can vary significantly, typically depending on factors such as target size and ransom amount.

3. **One-Time Fee Model:** Some services allow for a one-time purchase where an affiliate pays a fixed sum for lifetime access to ransomware tools without further financial obligation to the operator. It's akin to buying perpetual software licenses in legitimate markets; however, updates and support might be limited under this arrangement.

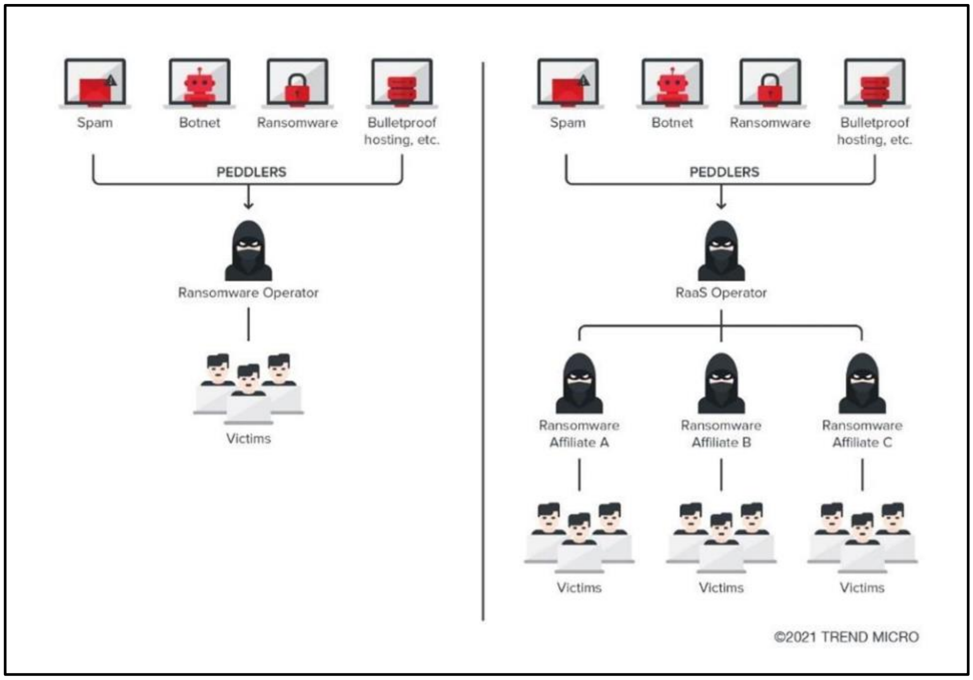
4. **Tiered Service Levels:** Reflecting models seen across many SaaS platforms outside illicit circles, some RaaS operations offer different tiers or packages with varying service levels and capabilities—for instance, basic encryption versus more advanced features that evade detection better or provide additional anonymization methods for transactions.

Above: *Explanations for different payment and profit-sharing structures that RaaS operators are known to use (Source)*

With the general divide between conventional ransomware gangs and RaaS operations, two key differences shed light on the nature of the threat that RaaS poses:

- ***Barrier to Entry***

One of the most significant differences between conventional ransomware gangs and RaaS operators is the significantly reduced barrier to entry, as RaaS offers less-skilled hackers the opportunity to use highly sophisticated malware infrastructure to launch attacks. RaaS operators develop their malware tools and scalability with the goal of increasing the number of affiliates, while deferring to their affiliates for the victim selection and attack planning. RaaS thus provides a division of labor that allows for more efficiency throughout the operation and, as a result, broadens the range of possible targets for attacks. Conventional ransomware gangs, on the other hand, are tasked internally with infrastructure maintenance, malware development, and attack planning and perpetration, forcing them to directly focus their effects on a smaller number of victims if they hope to achieve any success with a larger payout.



Above: *Diagram illustrating the organizational structure of ransomware vs. RaaS threat actors (Source)*

- ***Financial vs. Political Motivation***

While both conventional ransomware gangs almost universally have some form of financial motivations, even in situations when political tensions are relevant in deciding the target for attack, the expanded targeting and organization of RaaS operations means that political motivations or alliances are often not a factor when deciding who to attack. Conventional ransomware gangs vary extensively in this regard: In North Korea, state-sponsored Advanced Persistent Threat (APT) groups target large, critical infrastructure organizations with the goal of producing revenues for the state amid harsh sanctions against the country. State-backed APTs in Iran have similarly used ransomware operations to supplant oil and gas revenues lost to sanctions. In Russia, a number of ransomware operations have existed over the years with the tacit approval of the Russian government so long as its geopolitical interests align with the actions of these criminal enterprises. With RaaS operations, conversely, the operator itself typically limits its own involvement in identifying targets for attacks, leaving this duty instead to the affiliates.

The main differences between conventional ransomware and RaaS operations emerge from their organizational structure, while the tactics they use can often be indistinguishable. This means that RaaS operations pose threats of economic and reputational damage similarly to conventional ransomware but that this threat more broadly affects companies of all sizes around the world, including trucking companies and other organizations in the transportation sector.

Active RaaS Operations

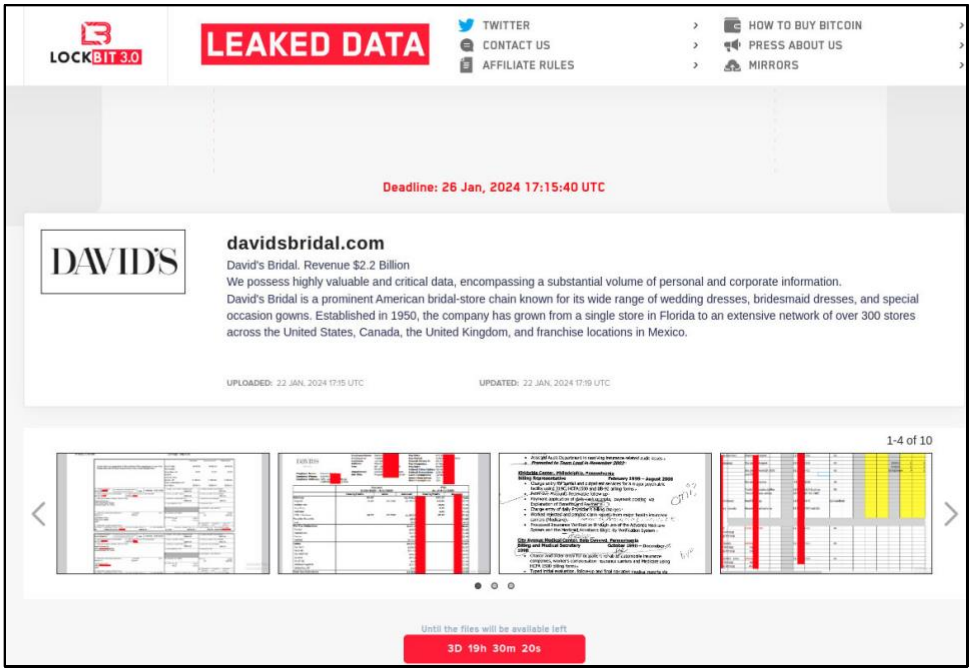
Within the overall cyber threat ecosystem, several RaaS operations stand out for the extent of their operations, number of attacks, size of their ransoms, and length of time that they have been active in targeting commercial enterprises around the world. Each of the following RaaS operations is highly visible and poses unique threats to organizations around the world.

LockBit

LockBit Statistics

- Active since January 2020
- Over $500 million extorted from nearly 3,000 victims
- Approximate average ransom of $167,000
- Targeted sectors include transportation, finance, agriculture, education, energy, government, healthcare, and manufacturing

LockBit was launched at the start of 2020, evolving from its previous “ABC ransomware” brand, and by 2022 had become the most deployed ransomware variant globally, a status it has maintained since that time. Since its inception, the group has deployed four separate generations of its malware, most recently having launched LockBit 4.0. After rebrands such as this, the group has been known to change some of its known indicators of compromise to become harder to identify, although multiple versions of the malware continue to be used in attacks.



Deadline: 26 Jan, 2024 17:15:40 UTC

davidsbridal.com

David's Bridal. Revenue $2.2 Billion

We possess highly valuable and critical data, encompassing a substantial volume of personal and corporate information.

David's Bridal is a prominent American bridal-store chain known for its wide range of wedding dresses, bridesmaid dresses, and special occasion gowns. Established in 1950, the company has grown from a single store in Florida to an extensive network of over 300 stores across the United States, Canada, the United Kingdom, and franchise locations in Mexico.

UPLOADED: 22 JAN. 2024 17:15 UTC

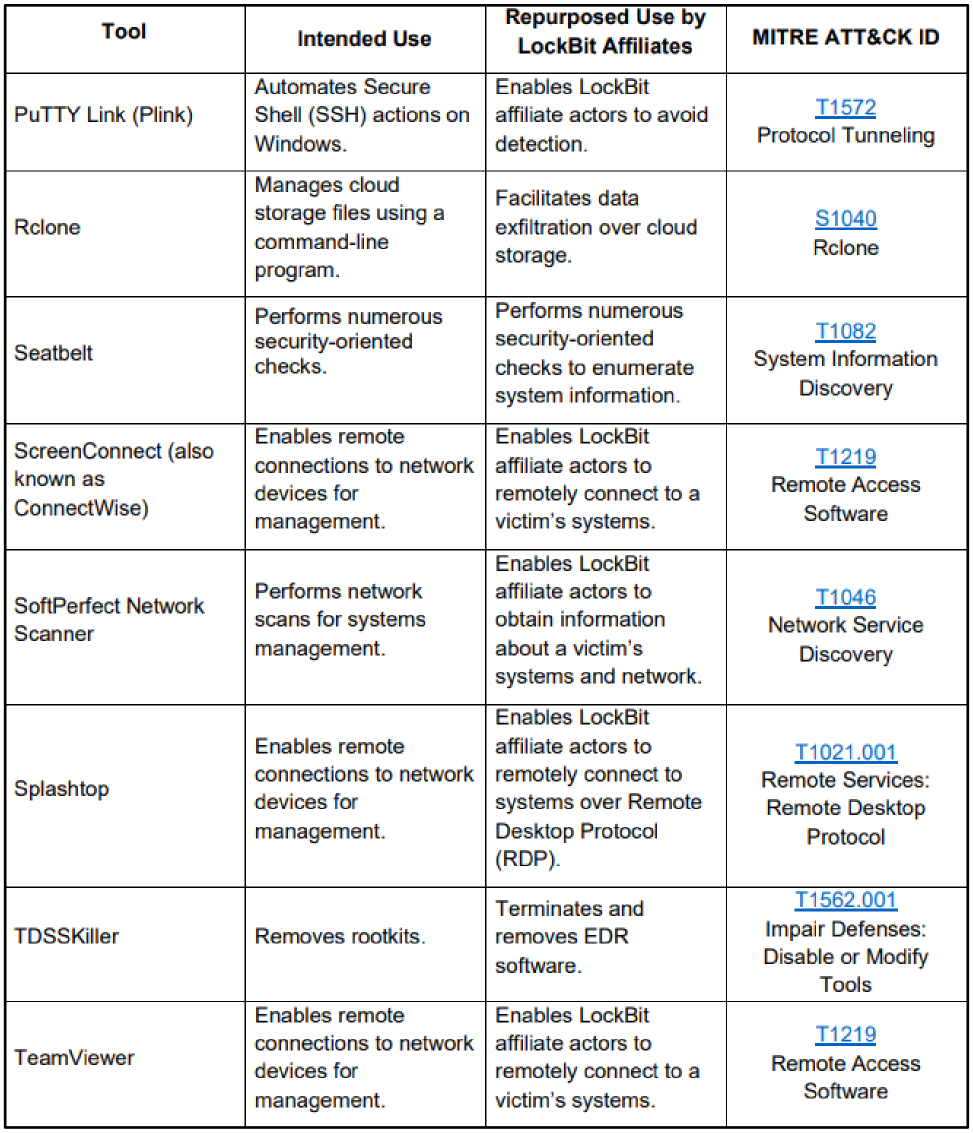
UPDATED: 22 JAN. 2024 17:19 UTC

Until the files will be available left

Above: *LockBit 3.0 dark web leak site (Source)*

LockBit affiliates have deployed an expansive range of malicious tools and exploited open-source programs in their attacks. In a June 2023 public advisory, the US Cybersecurity and Infrastructure Security Agency (CISA) identified 39 separate open-source software tools that LockBit and its affiliates had by that point exploited in their attacks. These tools helped the threat actors achieve such functions as network scanning, enabling remote connections or monitoring, terminating anti-malware programs, conducting reconnaissance on compromised devices, exfiltrating login credentials from systems or browsers, facilitating connections with Command-and-Control (C2) servers, and removing rootkits, among others.

LockBit's initial entry vectors also vary widely but often involve the exploitation of unpatched vulnerabilities in industrial control systems, file transfer programs, print management systems, Java logging frameworks, authentication services, and programs working with the Remote Desktop Protocol (RDP).



Tool	Intended Use	Repurposed Use by LockBit Affiliates	MITRE ATT&CK ID
PuTTY Link (Plink)	Automates Secure Shell (SSH) actions on Windows.	Enables LockBit affiliate actors to avoid detection.	T1572 Protocol Tunneling
Rclone	Manages cloud storage files using a command-line program.	Facilitates data exfiltration over cloud storage.	S1040 Rclone
Seatbelt	Performs numerous security-oriented checks.	Performs numerous security-oriented checks to enumerate system information.	T1082 System Information Discovery
ScreenConnect (also known as ConnectWise)	Enables remote connections to network devices for management.	Enables LockBit affiliate actors to remotely connect to a victim's systems.	T1219 Remote Access Software
SoftPerfect Network Scanner	Performs network scans for systems management.	Enables LockBit affiliate actors to obtain information about a victim's systems and network.	T1046 Network Service Discovery
Splashtop	Enables remote connections to network devices for management.	Enables LockBit affiliate actors to remotely connect to systems over Remote Desktop Protocol (RDP).	T1021.001 Remote Services: Remote Desktop Protocol
TDSSKiller	Removes rootkits.	Terminates and removes EDR software.	T1562.001 Impair Defenses: Disable or Modify Tools
TeamViewer	Enables remote connections to network devices for management.	Enables LockBit affiliate actors to remotely connect to a victim's systems.	T1219 Remote Access Software

Above: *Sample of some open-source software tools that LockBit has exploited in attacks (Source)*

RansomHub

RansomHub Statistics

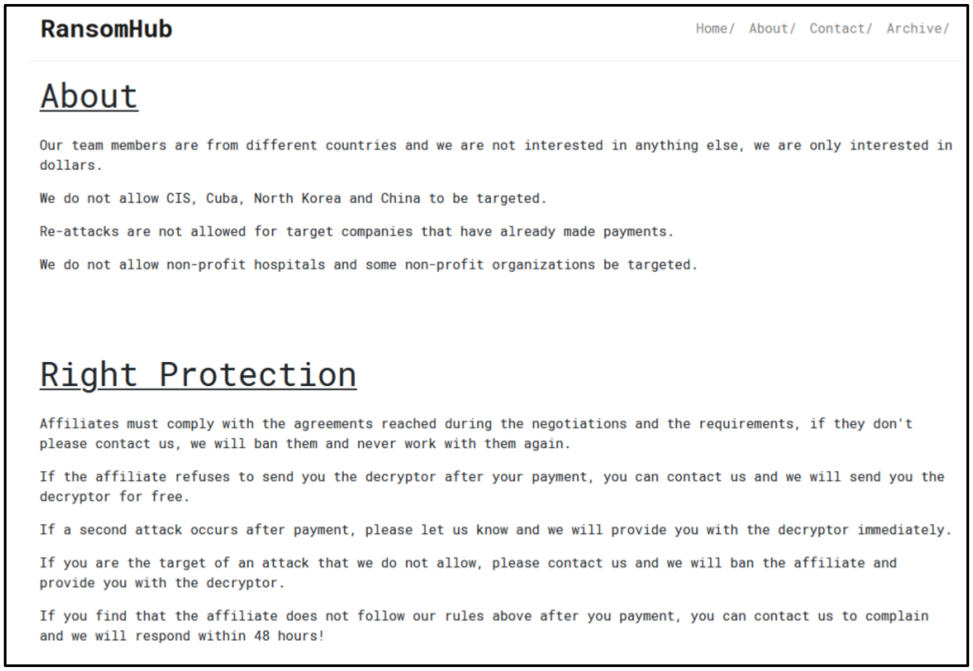
- Active since February 2024
- Attacked more than 300 victims, as of late 2024
- Ransom collection success rate of approximately 11 percent
- Targeted sectors include government and utilities, tech/IT, healthcare, agriculture, finance, manufacturing, transportation, and communications

RansomHub has exhibited rapid growth in activity since its formation in February 2024. RansomHub may be a rebrand of the now-defunct Knight Ransomware, as their codes are nearly identical. Additionally, findings also showed that both Notchy and Scattered Spider, which were previously affiliated with the ALPHV/BlackCat ransomware operation, have entered a partnership with RansomHub.

As of late 2024, the group had revealed on its dark web leak site attacks against 261 victims. The group also has a reported ransom collection success rate of 11.2%. As part of its RaaS operation, RansomHub pays a percentage of any successful ransom to the affiliate responsible for an attack and keeps a percentage so that the group can continue to function. The group has developed a set of rules for its affiliates to follow posted in the "About" page of its dark web leak site. In this section, the group indicates its motivation is purely financial and lays out three primary rules:

- No attacks on CIS countries, Cuba, North Korea or China.
- No attacks on companies that have already paid ransoms.
- No attacks on non-profit hospitals and some non-profit organizations.

These rules are followed by a section explaining if any affiliates of the group attack organizations that meet the above criteria that the affiliate will be banned from working with RansomHub and a decryption key will be provided to the victim for free. It also lays out a method for victims to challenge attacks committed by RansomHub affiliates.



About

Our team members are from different countries and we are not interested in anything else, we are only interested in dollars.

We do not allow CIS, Cuba, North Korea and China to be targeted.

Re-attacks are not allowed for target companies that have already made payments.

We do not allow non-profit hospitals and some non-profit organizations be targeted.

Right Protection

Affiliates must comply with the agreements reached during the negotiations and the requirements, if they don't please contact us, we will ban them and never work with them again.

If the affiliate refuses to send you the decryptor after your payment, you can contact us and we will send you the decryptor for free.

If a second attack occurs after payment, please let us know and we will provide you with the decryptor immediately.

If you are the target of an attack that we do not allow, please contact us and we will ban the affiliate and provide you with the decryptor.

If you find that the affiliate does not follow our rules above after you payment, you can contact us to complain and we will respond within 48 hours!

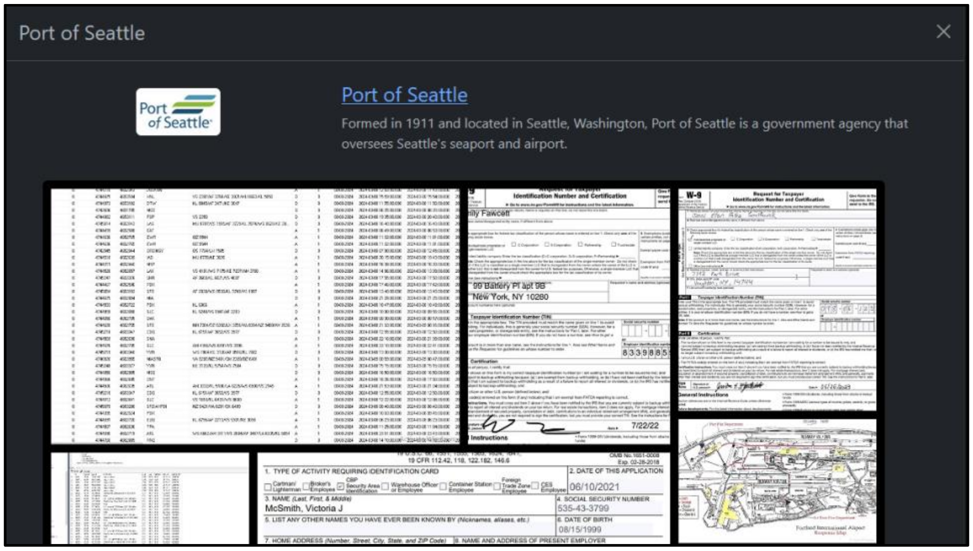
Above: *Rules and guidelines about use of RansomHub RaaS operation*

According to CISA, the most common methods by which RansomHub infiltrates targeted systems during its attacks include phishing emails, password spraying, and the exploitation of known vulnerabilities. RansomHub affiliates regularly exploit a range of known vulnerabilities in internet-facing applications and devices from providers such as Citrix and Fortinet. They also routinely target internet-facing IoT devices. Enterprise management, authentication, and server tools are also a common target for infection and subsequent lateral movements such as Confluence Data Center and Server, SMBv1 servers in Microsoft Windows operating systems, and the Netologon authentication tool.

Rhysida

Rhysida Statistics
- Active since May 2023 - Attacked 175 victims - Targeted sectors include education, healthcare, manufacturing, information technology, and government

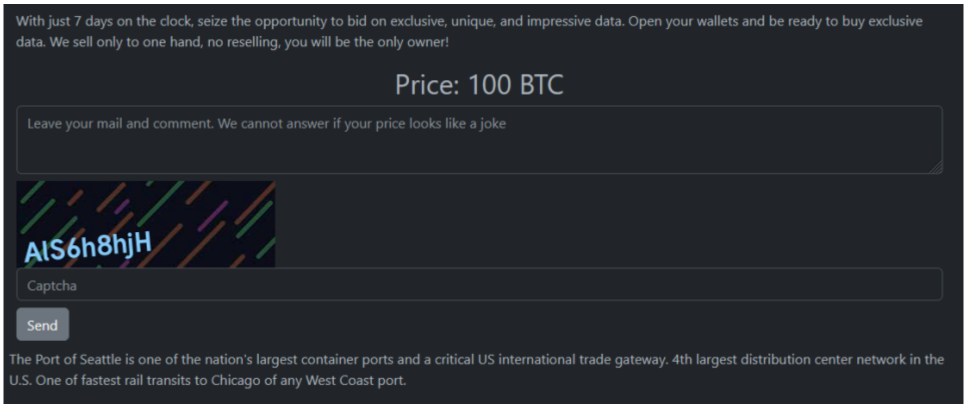
Rhysida has been active since May 2023, and gained significant attention in September 2024 when it launched a disruptive ransomware attack on the Port of Seattle in Washington. The group usually implements a double-extortion tactic for additional leverage to collect ransom payments and holds auctions for the purchase of some companies’ data that the gang has stolen and promoted for sale on its DW leak site. The ransomware gang claims it will only sell acquired information to one buyer unless the timer on the auction expires, in which case the data will be made public.



Port of Seattle

Port of Seattle

Formed in 1911 and located in Seattle, Washington, Port of Seattle is a government agency that oversees Seattle's seaport and airport.



With just 7 days on the clock, seize the opportunity to bid on exclusive, unique, and impressive data. Open your wallets and be ready to buy exclusive data. We sell only to one hand, no reselling, you will be the only owner!

Price: 100 BTC

Leave your mail and comment. We cannot answer if your price looks like a joke

The Port of Seattle is one of the nation's largest container ports and a critical US international trade gateway. 4th largest distribution center network in the U.S. One of fastest rail transits to Chicago of any West Coast port.

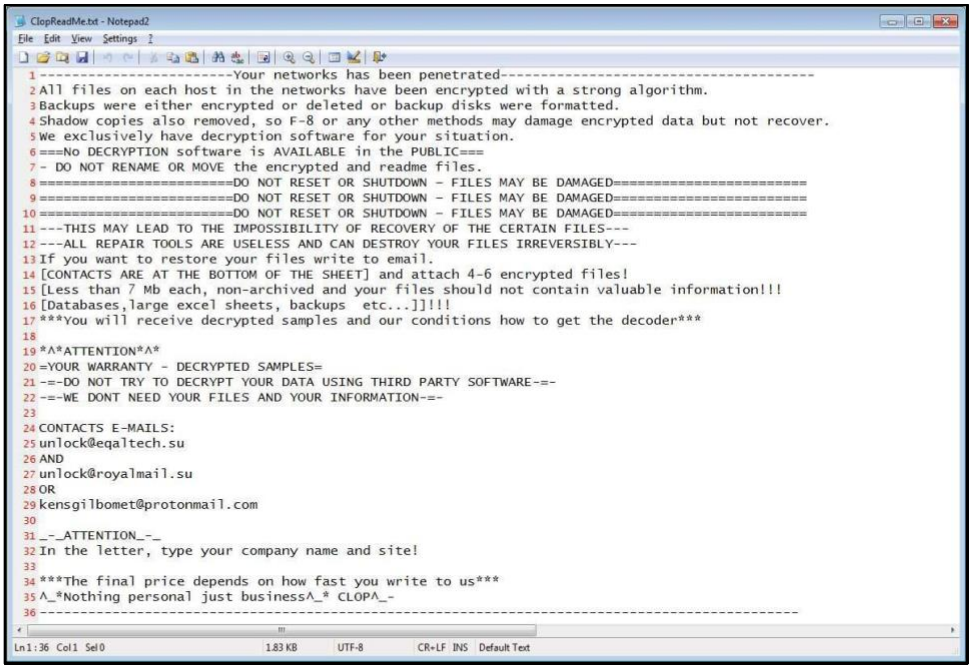
Above: *Posts offering the Port of Seattle data for exclusive sale on Rhysida's DW leak site*

According to CISA, Rhysida's most common method of gaining initial access to victim organizations lies with known vulnerabilities exploited in public-facing devices, including Virtual Private Networks (VPN) access points, as well as standard phishing tactics. Affiliates have commonly exploited RDP connections once gaining entry to targeted networks, established VPN connections, and executed PowerShell scripts—tactics collectively known as "living off the land," or using native systems and programs for malicious purposes.

CL0P

CL0P Statistics
- Active since February 2019 - Attacked over 8,000 victims globally and 3,000 victims in the United States alone - All sectors impacted by CL0P attacks

CL0P is one of the oldest RaaS operations, and it has seen some fluctuations in the scale and scope of its activities in the six years since it first became active. The most common entry vectors the group uses when launching attacks are general phishing tactics, exploiting vulnerabilities in a range of enterprise systems, directly targeting RDP instances, and using stolen login credentials for legitimate user accounts.



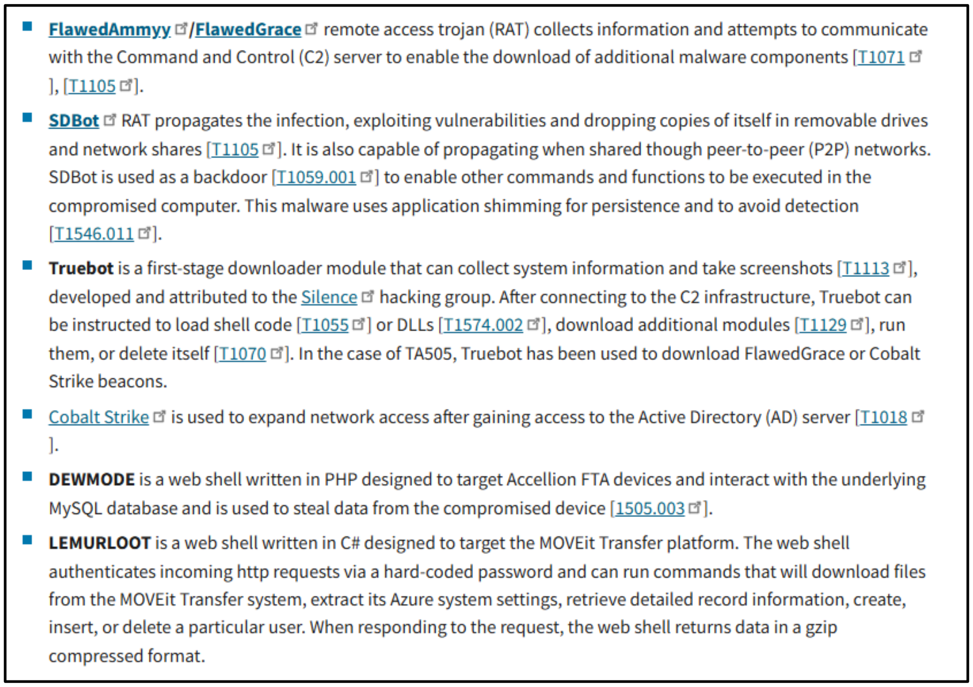
```
------------------------Your networks has been penetrated---------------------------------------
All files on each host in the networks have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F-8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation.
===No DECRYPTION software is AVAILABLE in the PUBLIC===
- DO NOT RENAME OR MOVE the encrypted and readme files.
========================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED========================
========================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED========================
========================DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED========================
---THIS MAY LEAD TO THE IMPOSSIBILITY OF RECOVERY OF THE CERTAIN FILES---
---ALL REPAIR TOOLS ARE USELESS AND CAN DESTROY YOUR FILES IRREVERSIBLY---
If you want to restore your files write to email.
[CONTACTS ARE AT THE BOTTOM OF THE SHEET] and attach 4-6 encrypted files!
[Less than 7 Mb each, non-archived and your files should not contain valuable information!!!
[Databases,large excel sheets, backups  etc...]]!!!
***You will receive decrypted samples and our conditions how to get the decoder***

*^*ATTENTION*^*
=YOUR WARRANTY - DECRYPTED SAMPLES=
-=-DO NOT TRY TO DECRYPT YOUR DATA USING THIRD PARTY SOFTWARE-=-
-=-WE DONT NEED YOUR FILES AND YOUR INFORMATION-=-

CONTACTS E-MAILS:
unlock@eqaltech.su
AND
unlock@royalmail.su
OR
kensgilbomet@protonmail.com

_-_ATTENTION_-_
In the letter, type your company name and site!

***The final price depends on how fast you write to us***
^_*Nothing personal just business^_* CLOP^_-
-----------------------------------------------------------------------------------------------
```

Above: *Example of a CL0P ransomware note (Source)*

The group gained significant attention in mid-2023 for being the first threat actor to exploit an SQL injection vulnerability (CVE-2023-34362) in the Progress Software's file transfer program MOVEit, a tactic seen previously in the group's exploiting of zero-day exploits in Accellion File Transfer Appliances and Fortra/Linoma

GoAnywhere MFT servers in the preceding years. The MOVEit vulnerability was the entry point for a much larger supply chain attack, impacting nearly 2,800 organizations within the two months after it was discovered in May 2023.

Throughout the course of its attacks, CL0P has used a variety of malware tools that it uses during different stages of its attacks. A June 2023 CISA advisory reported on some of these tools, identifying the FlawedAmmyy and SDBot Remote Access Trojans (RAT), Truebot downloader module, Cobalt Strike exploits, and Dewmode and Lemurloot webs hells to download files and exfiltrate data.



- **FlawedAmmyy**/**FlawedGrace** remote access trojan (RAT) collects information and attempts to communicate with the Command and Control (C2) server to enable the download of additional malware components [T1071], [T1105].
- **SDBot** RAT propagates the infection, exploiting vulnerabilities and dropping copies of itself in removable drives and network shares [T1105]. It is also capable of propagating when shared though peer-to-peer (P2P) networks. SDBot is used as a backdoor [T1059.001] to enable other commands and functions to be executed in the compromised computer. This malware uses application shimming for persistence and to avoid detection [T1546.011].
- **Truebot** is a first-stage downloader module that can collect system information and take screenshots [T1113], developed and attributed to the Silence hacking group. After connecting to the C2 infrastructure, Truebot can be instructed to load shell code [T1055] or DLLs [T1574.002], download additional modules [T1129], run them, or delete itself [T1070]. In the case of TA505, Truebot has been used to download FlawedGrace or Cobalt Strike beacons.
- Cobalt Strike is used to expand network access after gaining access to the Active Directory (AD) server [T1018].
- **DEWMODE** is a web shell written in PHP designed to target Accellion FTA devices and interact with the underlying MySQL database and is used to steal data from the compromised device [1505.003].
- **LEMURLOOT** is a web shell written in C# designed to target the MOVEit Transfer platform. The web shell authenticates incoming http requests via a hard-coded password and can run commands that will download files from the MOVEit Transfer system, extract its Azure system settings, retrieve detailed record information, create, insert, or delete a particular user. When responding to the request, the web shell returns data in a gzip compressed format.

Above: *CISA-compiled list of malware tools that CL0P ransomware has used in its attacks (Source)*

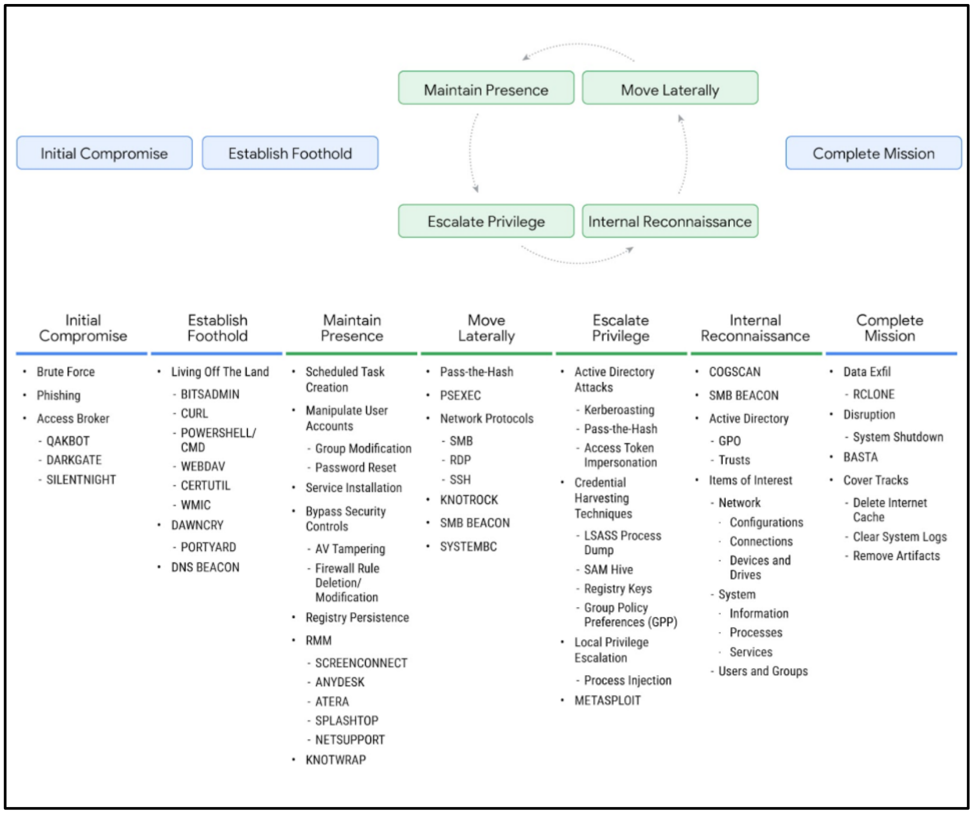
Black Basta

Black Basta Statistics
● Active since April 2022 ● Attacked over 500 victims ● Targeted sectors include virtually all critical infrastructure entities

Black Basta has relied on several methods for gaining initial access to victims' networks. The most common entry vector is through spearphishing, the more curated and targeted form of traditional phishing. Black Basta has also previously had an extensive affiliation with Qakbot, a botnet malware operation that functioned as an access broker to individual nodes in its expansive network of compromised devices. While Qakbot was disrupted and dismantled in operations in August 2023, Black Basta worked with other access brokers, including for a brief period with a group called Darkgate, before soon crafting its own custom botnet-like malware to initiate attacks, most notably a malware called SilentNight.

The Black Basta operator have exploited several vulnerabilities to facilitate and escalate its attacks:

- Authentication bypass vulnerability in Connectwise ScreenConnect (CVE-2024-1709)
- Privilege escalation vulnerability (ZeroLogon) in the Netlogon Remote Protocol (CVE-2020-1472)
- Privilege escalation vulnerabilities (NoPac) in Microsoft's Active Directory Domain Services (CVE-2021-42278 and CVE-2021-42287)
- Privilege escalation vulnerability (PrintNightmare) in Microsoft Windows Print Spooler (CVE-2021-34527)



Initial Compromise

- Brute Force
- Phishing
- Access Broker
  - QAKBOT
  - DARKGATE
  - SILENTNIGHT

Establish Foothold

- Living Off The Land
  - BITSADMIN
  - CURL
  - POWERSHELL/CMD
  - WEBDAV
  - CERTUTIL
  - WMIC
- DAWNCRY
  - PORTYARD
- DNS BEACON

Maintain Presence

- Scheduled Task Creation
- Manipulate User Accounts
  - Group Modification
  - Password Reset
- Service Installation
- Bypass Security Controls
  - AV Tampering
  - Firewall Rule Deletion/ Modification
- Registry Persistence
- RMM
  - SCREENCONNECT
  - ANYDESK
  - ATERA
  - SPLASHTOP
  - NETSUPPORT
- KNOTWRAP

Move Laterally

- Pass-the-Hash
- PSEXEC
- Network Protocols
  - SMB
  - RDP
  - SSH
- KNOTROCK
- SMB BEACON
- SYSTEMBC

Escalate Privilege

- Active Directory Attacks
  - Kerberoasting
  - Pass-the-Hash
  - Access Token Impersonation
- Credential Harvesting Techniques
  - LSASS Process Dump
  - SAM Hive
  - Registry Keys
  - Group Policy Preferences (GPP)
- Local Privilege Escalation
  - Process Injection
- METASPLOIT

Internal Reconnaissance

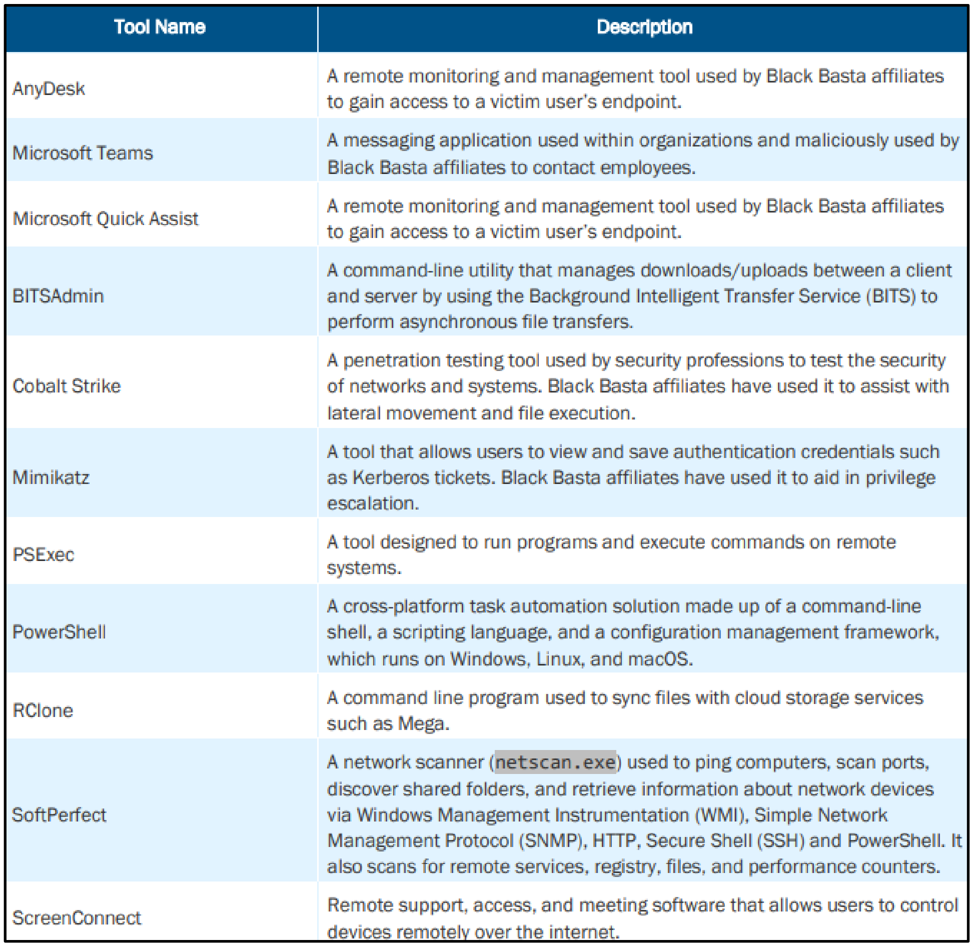
- COGSCAN
- SMB BEACON
- Active Directory
  - GPO
  - Trusts
- Items of Interest
  - Network
    - Configurations
    - Connections
    - Devices and Drives
  - System
    - Information
    - Processes
    - Services
  - Users and Groups

Complete Mission

- Data Exfil
  - RCLONE
- Disruption
  - System Shutdown
- BASTA
- Cover Tracks
  - Delete Internet Cache
  - Clear System Logs
  - Remove Artifacts

Above: *Timeline of stages of Black Basta operator cyber attack (Source)*

Once compromising a network and escalating privileges within that system, Black Basta exploits a number of open-source programs in order to expand the scope of its attack, exfiltrate and encrypt data, and seize more direct control of affected systems. Notable examples of these tools include the AnyDesk and Splashtop Remote Monitoring and Management (RMM) tools, the Cobalt Strike penetration testing tool, the Mimikatz authentication credential saving and storage tool, and the WinSCP file transfer tool.



Tool Name	Description
AnyDesk	A remote monitoring and management tool used by Black Basta affiliates to gain access to a victim user's endpoint.
Microsoft Teams	A messaging application used within organizations and maliciously used by Black Basta affiliates to contact employees.
Microsoft Quick Assist	A remote monitoring and management tool used by Black Basta affiliates to gain access to a victim user's endpoint.
BITSAdmin	A command-line utility that manages downloads/uploads between a client and server by using the Background Intelligent Transfer Service (BITS) to perform asynchronous file transfers.
Cobalt Strike	A penetration testing tool used by security professions to test the security of networks and systems. Black Basta affiliates have used it to assist with lateral movement and file execution.
Mimikatz	A tool that allows users to view and save authentication credentials such as Kerberos tickets. Black Basta affiliates have used it to aid in privilege escalation.
PSExec	A tool designed to run programs and execute commands on remote systems.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
RClone	A command line program used to sync files with cloud storage services such as Mega.
SoftPerfect	A network scanner (`netscan.exe`) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) and PowerShell. It also scans for remote services, registry, files, and performance counters.
ScreenConnect	Remote support, access, and meeting software that allows users to control devices remotely over the internet.

Above: *CISA-compiled list of open-source tools Black Basta operators use during attacks (Source)*

Considering the structure and TTPs of these five RaaS operators, two key points are necessary to consider when contextualizing the broader threat of RaaS to trucking companies. First, these five operators alone have collectively targeted thousands of organizations, ranging in size from small local businesses to corporations with thousands of employees. And second, each RaaS operation uses a unique set of TTPs to gain access to victims' networks, although the end result of a successful RaaS attack is always the encryption or theft of sensitive data. What these two points show is that RaaS operators pose and will continue to pose evolving threats to organizations of all sizes, including in the transportation sector, and that mitigating the risks of attacks requires ongoing vigilance and attention.

RaaS Threat Facing the Transportation Sector

Within the TTPs of various RaaS operators in the transportation sector, trucking companies are not often elevated above other businesses as ideal targets for attacks. But trucking companies have nevertheless been caught in the wide nets that these RaaS operations cast, particularly due to the high scalability of these operations and the number of RaaS affiliates eager to indiscriminately attack any organization that may be forced to pay a ransom.

Since April 2024, the five RaaS operations highlighted in the previous section have collectively been responsible for dozens of attacks, many of which specifically targeted transportation, logistics, and supply chain companies in North America. Examples of these attacks include the following:

- On 4 February 2025, RansomHub claimed an attack on a trucking and logistics company in British Columbia, stealing over 160 gigabytes of data that the group threatened to release if no ransom was paid.
- On 6 January 2025, CL0P claimed an attack on a supply chain solutions company in Wisconsin, sharing on its DW leak site 62 files containing information sensitive to the company’s operations.
- On 3 January 2025, LockBit shared details on its DW leak site of an attack the group carried out against an international logistics company headquartered in Hong Kong, with an additional regional headquarters in California and further offices across the United States and Canada. LockBit claimed to have stolen 84.5 gigabytes of data during the attack.
- On 17 October 2024, RansomHub claimed an attack on a Michigan-based trucking and logistics service provider, indicating in a DW post that it stole 75 gigabytes of sensitive data and threatened to release it within the following week.
- On 9 May 2024, Black Basta claimed an attack on a trucking and logistics company based in Michigan, stealing over 200 gigabytes of data, samples of which the group shared on its DW leak site, including corporate data, employee information, and HR documents.
- On 8 May 2024, LockBit claimed an attack on a trucking and logistics company based out of Toledo, Ohio. The threat actor claimed an unspecified amount of data, which it threatened to release the following week.

- On 17 April 2024, LockBit claimed an attack on a Montana-based truck manufacturing and repair company, stealing an unspecified amount of data, which the group threatened to release two days later.

Despite the above-stated differences between conventional ransomware and RaaS operations, the reasonings that each threat actor structure has for targeting certain organizations are often similar. In conventional ransomware attacks, the operator typically seeks to disrupt larger organizations, often in a critical infrastructure sector, that have the ability to pay much larger ransoms and whose disruption would cause extensive impacts in local or regional economies. With RaaS, organizations that have an interconnected role in local economies, particularly those whose operations downstream customers rely on, represent ideal targets for attack.

A regional trucking company, for instance, could suffer a ransomware attack that locked internal systems for days or even weeks. The company could face legal consequences for failing to meet contractual obligations and reputational consequences for having sensitive customer or supplier information exposed online, serving to pressure it into complying with the threat actor’s demands to hasten the return of its systems back to regular function. These impacts are not unique to RaaS attacks, as there will be few differences in the aftermath of attacks. But the most glaring threat for the transportation sector lies in the expanding and indiscriminate nature of RaaS victimology: while conventional ransomware gangs will not attack just any company, the same cannot be said for RaaS.

The ultimate takeaway for trucking companies is that RaaS operations have repeatedly and persistently targeted the transportation sector and that trucking companies have not been spared from being the target of disruptive RaaS attacks that have resulted in hundreds of thousands of dollars in damages. But as the threats of RaaS attacks are unique to trucking companies, neither are the steps needed to mitigate this risk. Preventing ransomware attacks requires that all company employees continually adhere to active, uniform, cybersecurity practices, maintain smart habits with account security and login credentials, and act quickly when faced with such threats as phishing attempts.

Conclusion

Conventional ransomware and RaaS operations share several similarities, but more importantly for trucking companies, they share a number of key differences. As primarily financially motivated operations, RaaS groups maintain networks of affiliates responsible for identifying targets and planning and carrying out certain aspects of attacks, allowing the RaaS groups to outsource some of their work and to scale their operations much larger than conventional ransomware gangs. This structure reduces the barrier to entry for less-sophisticated hackers and vastly expands the scope of the threats that these operations pose to companies of all sizes. Highly visible RaaS operations share some common TTPs but likewise differ in the type of malware used and vulnerabilities exploited during the initial stages of attacks, illustrating the threats that RaaS operators pose and will continue to pose as current operations shut down and new ones emerge in their place.

The transportation sector in general and trucking companies in particular certainly face threats of RaaS attacks. Some of the most highly visible RaaS operators have publicized attacks against such companies over the past year, including several instances when stolen data was made available on DW leak sites. These threats are not unique to trucking companies, but as RaaS operators have claimed responsibility for attacks on thousands of companies of all sizes around the world, trucking companies are often caught in this wide net. Further complicating this threat, RaaS groups frequently update their TTPs, making it imperative that company employees at all levels adhere to strict cybersecurity protocols and that systems are monitored and updated to eliminate vulnerabilities before they are exploited in an attack.