RANSOMWARE ACTOR PROFILING

THOROUGH INSIGHTS ON THE BIGGEST PLAYERS

CybelAngel®

CONTENTS

INTRODUCTION

> Ransomware, once a containable nuisance, has metastasized into a multi billion dollar industry. It is a pervasive and sophisticated ecosystem of cybercrime that **relentlessly evolves.**

SO, HOW EXACTLY HAVE THE RULES OF RANSOMWARE CHANGED?

The Ransomware as a Service (RaaS) age is here, a fully mature market where powerful malicious tools are packaged and sold, enabling a wider net of threat actors to launch devastating campaigns.

Groups like **RansomHub** have surged into this market, quickly overtaking established names like **LockBit** by recruiting experienced affiliates and refining their extortion models. They operate with the efficiency of a startup, targeting critical infrastructure and leaving a trail of encrypted data across at least **210 victims** in a single year. We are consistently reminded that the barrier to entry for sophisticated cyberattacks has been dangerously lowered.

One word to describe these changes lately? **Relentless.**

We are past simple data encryption strategies now. Instead the preferred playbook, mastered by groups such as **Cl0p**, embraces a quadruple extortion model. It begins with data theft, escalates to public leaks on Tor hosted sites, intensifies with DDoS attacks that cripple services, and culminates in the targeted harassment of executives, employees, and even occasionally media to amplify pressure. Considering the mentality behind recent ransomware communications, it can be considered psychological warfare as much as it is a technical assault.

The sheer variety of these ransomware gangs requires a nuanced understanding of their individual tactics. **Akira**, for instance, stands out with its retro, command line interface and its deep ties to the infamous **Conti group**. It favors a double extortion model and has shown a particular focus on the United States, becoming the most detected variant in the third quarter of 2024. Meanwhile, the Lynx

ransomware group presents a facade of "ethical" hacking, claiming to avoid hospitals and non profits, yet its attacks on critical infrastructure like electricity providers tell a different story. It leverages a RaaS panel that makes deployment unnervingly simple for its affiliates, offering them a staggering **80% of the profits.**

And we cannot ignore the resilience of older, more established actors. **Ryuk, first seen in 2018**, remains a formidable force, known for its ability to delete shadow copies and encrypt entire network drives, making recovery without backups nearly impossible. It often employs a slow, methodical approach, moving laterally through systems to maximize damage before demanding enormous ransoms. Then there is **Black Basta**, a group that burst onto the scene in **2022** and quickly targeted over **500 organizations globally**. Despite a recent law enforcement takedown, its highly skilled members, believed to be remnants of the **Conti and FIN7 syndicates**, are simply regrouping under new banners, proving that dismantling the brand does not eliminate the threat.

This complex ecosystem represents an unprecedented challenge so we know that you will find this analysis helpful.

ACTOR PROFILES

GROUP	VICTIMS (2025)	TARGETED SECTORS	KEY PATTERNS IN ATTACKS
Black Basta	450+ (2022–early 2025); operations ceased Q1 2025	Healthcare, Manufacturing, Finance, Critical Infrastructure	Phishing, RDP/VPN brute-force (including automated tools like BRUTED), double extortion, social engineering.
Lynx	96+ (publicly listed); 42 attacks Jan; 10 observed Q1 2025	Manufacturing, Retail, Finance, Public Sector	Double extortion, RaaS, high-value targets, advanced encryption, customizable via CLI, deletes backups
Ryuk	Not specified	Large Enterprises, Critical Assets	Rapid encryption, Big Game Hunting.
Akira	213 victims Q1 2025; 72 attacks Jan	Business, Construction, Infrastructure, Tech	Double extortion, rapid data theft, exploits VPN/perimeter devices, absorbs affiliates from other groups.
Cl0p	392 victims Q1 2025; 60 attacks Jan	Consumer Goods, North America	Mass exploitation of zero-days (e.g., Cleo MFT), encryption-less extortion, supply chain attacks.
RansomHub	84 victims March 2025; 14% Q1 market share; 43 attacks Jan	Healthcare, Various	Consistent posting, re-extortion, absorbs affiliates, data leak threats, prolific RaaS by victim volume.
Dragonforce	120+ victims past year; 23 in April peak	Manufacturing, Construction, Tech, Healthcare, Retail, Public	Phishing, RDP/VPN brute-force, vulnerability exploits (e.g., CVE-2024-21887), double extortion, RaaS, affiliate absorption.

ACTOR 1

BLACK BASTA

BLACK BASTA

STEALTHY LAYERED PROWESS

Black Basta first appeared in April 2022, launching with a flurry of activity. Within two weeks, its leak portal "**Basta News**" listed more than 20 victims. Since then, the group has targeted over 500 organizations worldwide, with a focus on healthcare, manufacturing, and construction across the United States, United Kingdom, Canada, Australia, and the European Union.

Believed to be a rebrand or offshoot of the infamous Conti gang, Black Basta operates independently but shares infrastructure and tactics with other Russian-speaking cybercriminal groups such as **FIN7** and **BlackMatter**. Unlike public facing RaaS outfits, Black Basta works behind closed doors to quietly deploy tailored attacks, by utilising a trusted circle of affiliates.

WHAT MAKES THEM DIFFERENT?

The group's most dangerous tactic is its use of **layered social engineering**. Affiliates flood targets with spam emails, then pose as IT support via phone or Microsoft Teams to offer fake help. This process tricks victims into downloading remote access tools like **AnyDesk** or **Quick Assist**. This calculated strategy reveals an in-house development effort far beyond copy-paste ransomware kits.

Black Basta has also developed automated tools to breach network devices with weak credentials, giving it more options for infiltration beyond phishing.

WHAT'S THE OPERATIONAL IMPACT?

Their attack blends technical skill and psychological expertise.
Once initial access is gained, affiliates use tools like SoftPerfect NetScanner, disguised under benign file names, to map the network. They move laterally with Cobalt Strike, PsExec, ScreenConnect, and Splashtop. To escalate privileges, they deploy Mimikatz and exploit known flaws like ZeroLogon and PrintNightmare.

Before any encryption takes place, data is exfiltrated using RClone or WinSCP. Files are then encrypted using ChaCha20 with RSA-4096 keys, and volume shadow copies are deleted to block recovery efforts. A ransom note named "readme.txt" appears across the network, directing victims to a Tor site and providing a unique identifier. No ransom amount is stated; victims typically have 10 to 12 days to respond before their data is published.

WHAT TO KEEP IN MIND?

Black Basta thrives on low visibility and operational control. Its avoidance of open recruitment, combined with the use of advanced social engineering and network reconnaissance, results in precise and damaging attacks. The February 2025 leak of their internal chat logs confirmed the group's structured hierarchy and disciplined affiliate coordination.

Their focus on critical infrastructure sectors, combined with the use of legitimate IT tools and aggressive privilege escalation, makes Black Basta particularly difficult to stop once inside. For CISOs, this means focusing defenses not just on endpoints, but also on identity management, communication protocols, and employee trust channels.

BLACK BASTA IN NUMBERS

500+

VICTIM ORGANIZATIONS TARGETED GLOBALLY

20+

INITIAL VICTIMS LISTED WITHIN THE FIRST TWO WEEKS

10 TO 12 DAYS:

DEADLINE GIVEN BEFORE PUBLIC DATA RELEASE

6+

COUNTRIES IMPACTED, INCLUDING THE U.S. AND EU NATIONS

1 MAJOR INTERNAL LEAK:

FEBRUARY 2025 CHAT LOG DISCLOSURE

ACTOR 2

RANSOMHUB

RANSOMHUB

A CALCULATED DISRUPTOR

First appearing on the RaaS scene in February 2024, RansomHub has already claimed over **210 victims** across a wide swath of critical infrastructure—from water utilities and financial services to healthcare and manufacturing.

Initially dismissed as a LockBit copycat, RansomHub's strategy quickly proved more ambitious. By Q3 2024, it had eclipsed LockBit in successful attack claims. What's more, its user-friendly affiliate model with enforced codes of conduct, curated targets, and a generous revenue split, has made it the ransomware operation of choice for experienced cybercriminals left displaced after the takedown of groups like **AlphV and LockBit**.

WHAT MAKES THEM DIFFERENT?

Unlike traditional ransomware groups that operate in shadows and silos, RansomHub functions like a well-oiled service platform. It offers affiliates everything they need. Like encryption tools, data leak portals, support, and imposing guardrails: **no attacks on nonprofits, no double targeting, no tolerance for broken decryption promises.** Victims even have a contact line for complaint escalation if an affiliate fails to deliver a decryption key.

WHAT'S THE OPERATIONAL IMPACT?

Victims are typically given 3 to 90 days to respond before their data is posted publicly. Each attack starts with a precise infiltration via known vulnerabilities (like **CVE-2020-1472**), followed by stealthy lateral movement and advanced evasion techniques. Data is exfiltrated, encrypted, and leveraged in a double extortion play that leaves CISOs with a painful choice—pay, or watch sensitive information go public.

This is not cybercrime as usual. RansomHub is organized, opportunistic, and rising fast. It's no longer enough to prepare for ransomware in general, instead CISOs must study RaaS as the criminal enterprise that it is.

WHAT TO KEEP IN MIND?

RansomHub affiliates use renamed binaries like windows.exe, exploit common vulnerabilities like CVE-2020-1472, and evade endpoint detection. They exfiltrate data using PuTTY, Cobalt Strike, and S3 buckets.

RANSOMHUB IN NUMBERS

$1.1B

GLOBAL RANSOMWARE REVENUE IN 2023—UP 140% YOY.

2ND PLACE

RANSOMHUB'S RANK AMONG U.S. RANSOMWARE VARIANTS IN Q3 2024.

<1% GAP

BETWEEN RANSOMHUB AND THE TOP RANSOMWARE VARIANT IN THE U.S.

$2.6M

BETWEEN RANSOMHUB AND THE TOP RANSOMWARE VARIANT IN THE U.S.

$1.82M

AVERAGE COST OF RECOVERY, EVEN IF YOU DO NOT PAY.

ACTOR 3

RYUK

RYUK

PRECISE & DEADLY TARGETING

Known for its precision targeting and devastating impact, Ryuk has earned a reputation as one of the most formidable ransomware families. Ryuk ransomware was one of the first ransomware variants capable of identifying and encrypting network drives and resources, as well as deleting shadow copies on victim endpoints, making data recovery nearly impossible without external backups. First appearing in 2018, Ryuk ransomware quickly made headlines for targeting large, enterprise Microsoft OS.

WHAT MAKES THEM DIFFERENT?

Ryuk's uniqueness is down to its ability to identify and encrypt network drives and resources, while deleting shadow copies on the victim endpoint. Ryuk is a variant of the Hermes 2.1 ransomware, first sold on the dark web in 2017 by the cryptocriminal gang CryptoTech. In 2021, it was discovered that the new Ryuk variant had self-spreading, worm-like capabilities to cause damage without human intervention. Initially thought to be linked to North Korean actors, Ryuk ransomware was later discovered to be associated with a Russian cybercriminal organization, Wizard Spider, specifically a smaller cell named Grim Spider. The ransomware group's name is unique—Ryuk originally comes from the name of a character from the popular manga and anime series Death Note.

WHAT'S THE OPERATIONAL IMPACT?

Ryuk ransomware attacks perform their initial compromise through TrickBot, a recognized banking Trojan malware, or backdoor vulnerabilities distributed by phishing emails. Microsoft categorizes Ryuk as a human-operated ransomware operation. Threat actors move laterally through systems to perform reconnaissance, steal sensitive information, and exfiltrate data. When a user clicks on a malicious link or attachment, ransomware is installed onto a victim's device.

Ryuk's ransomware encrypts files on the victim's device using a strong encryption algorithm—a combination of RSA-2048 and AES-256. Ryuk's encryption also avoids any processes or disk locations that may slow down or interfere with the encryption. From this vulnerability, the ransomware can spread through internal systems and networks.

Ryuk functions as a late-stage payload, delivered by widely used frameworks like **Cobalt Strike**, **Emotet**, **GrimAgent**, or **TrickBot**. The ransomware payload is spread across the target environment to extort maximum funds from the business. Volume Shadow copies (VSS) are also deleted to inhibit full system

WHAT TO KEEP IN MIND?

Ryuk's ability to evade detection can be attributed to a relaxed cybersecurity posture within organizations, including a lack of firewall protection, weak password security, no multifactor authentication (MFA), and non-randomized local admin passwords. The prevailing belief that robust security measures compromise performance often leaves organizations exposed. Given the resilience of the new Ryuk variant, proactive prevention is more effective than mitigation after an attack.

RYUK IN NUMBERS

YEAR OF EMERGENCE: 2018

Primary targets: Large organizations e.g. businesses, hospitals, government institutions, and city services

$150 MILLION

Ransom amount extorted (average)

TARGETED GEOGRAPHY: PRIMARILY **USA** AND **CANADA**, WITH **75%** OF ATTACKS GOING TOWARDS THE **AMERICAN HEALTHCARE SECTOR**.

RANSOM DEMANDS:

Ranging from $100,000 to $500,000, with one FBI reported case amounting to $5 million worth of Bitcoin.

ENCRYPTION SPEED:

Encrypted 100,000 files (53GB) in 14 minutes and 30 seconds in one test.

ACTOR 4

AKIRA

AKIRA

A RETRO-STYLED MENACE

Akira is a RaaS gang that emerged in **March 2023**. Anyone can use Akira's malware to steal and encrypt sensitive data, such as by phishing, only returning it after receiving a ransom payment, with sums ranging from **$200,000 to millions**. Akira stands out most for its retro style.

WHAT MAKES THEM DIFFERENT?

Akira is one of the top RaaS gangs, ranking alongside players such as LockBit and RansomHub. A recent blockchain analysis suggests that Akira originated from the **Russian backed Conti ransomware group**, which dissolved in 2022. Its Tor-based site is styled upon 1980's "green screen" consoles, controlled by typing certain commands (leaks, news, contact, help, clear). Attacks from this gang tend to focus on the business sector, but it's also been active in construction, critical infrastructure, education, manufacturing, retail, and technology.

WHAT'S THE OPERATIONAL IMPACT?

Akira ransomware attacks typically involve several technical stages. Initial access is gained by exploiting vulnerabilities in VPNs without multifactor authentication (e.g., **Cisco CVE-2020-3259** and **CVE-2023-20269**), spear phishing emails, abusing Remote Desktop Protocol (RDP), or using stolen credentials. Tools like **Anydesk** are also used for remote access. For persistence and discovery, Akira maintains access and enables privilege escalation with fake domain accounts or administrative accounts (e.g., **itadm**). It steals credentials from the Local Security Authority Subsystem Service (LSASS) or with tools like **Mimikatz** and **LaZagne**, and identifies network devices with tools like Advanced IP Scanner. To evade detection, Akira deploys multiple ransomware variants, such as "**Megazord**" and "**Akira_v2**," and disables security processes with services such as PowerTool to facilitate lateral movement. Data exfiltration occurs using tools and algorithms like **FileZilla**, **RClone**, **WinSCP**, or **WinRAR** to move stolen data to external servers or cloud storage.

For data encryption, Akira uses a hybrid encryption strategy, with its latest version specifically targeting virtual machines. It also deletes volume shadow copies to block system recovery efforts, with its encryptor (**w.exe**) using PowerShell commands.

Akira utilizes a double extortion model (encrypting and stealing data), demands Bitcoin payments, and applies pressure by threatening to publish stolen data and even calling victims. They have been known to lower ransom demands and wipe backups to hinder system recovery efforts.

WHAT TO KEEP IN MIND?

To safeguard against the spread of an Akira virus, organizations should follow the “3-2-1 rule” for back-ups (3 copies, 2 media types, 1 offline/offsite copy) to facilitate data protection and system recovery.

Disabling command-line and scripting activities and permissions can block threat actors from using company software, and disabling hyperlinks in emails can prevent malicious clicks. Finally, organizations must have a well-defined incident response plan that is regularly tested and updated.

AKIRA IN NUMBERS

MAJOR TAREGT:

France accounted for 53.1% of detected Akira attacks.

VICITIM COUNT

Claims **6-30+** victims per month, reaching an all-time high of 73 victims in November 2024.

MARKET SHARE:

Responsible for 21% of ransomware attacks in Q1 2024.

DATA EXFILTRATION SPEED:

Can run “lightning-fast data exfiltration” from Veeam servers in around 2 hours.

RANSOM PAYMENTS

Generated $42 million between March 2023 and April 2024. U.S. ranking: Was the most-detected ransomware variant in the US by market share in Q3 2024 (13%).

ACTOR 5

CLOP

CL0P

REACHING NEW HEIGHTS VIA QUADRUPLE EXTORTION

The Cl0p ransomware group has taken extortion to a new level (a quadruple level, to be precise), shifting from encryption-based tactics to outright data theft to stunning success. First observed in 2019 as a variant of the CryptoMix ransomware family, Cl0p, "Clop" or TA505, quickly became a forcible, well regarded threat. They are widely understood to be a Russian gang with their name supposedly taken from the Russian word "klop", meaning bed bug.

WHAT MAKES THEM DIFFERENT?

Unlike traditional ransomware groups that rely solely on encrypting files to demand ransom, Cl0p has evolved to use a combination of data theft and a quadruple extortion model. This means victims who refuse to pay risk having their stolen data leaked publicly on their Tor hosted data leak site, known as '**CL0P^_-LEAKS**'. Quadruple extortion adds two additional layers of coercion beyond initial encryption and data publication: **DDoS attacks** to render services inoperable, and targeted harassment of stakeholders (employees, customers, media) to amplify reputational damage. In recent years, Cl0p has moved away from traditional encryption based ransomware to "encryption-less" attacks, simply stealing data and threatening to leak it.

This shift allows them to bypass certain security measures and increase their ransom demands. Like many other Russian speaking threat groups, Cl0p cannot function on devices within the CIS.

WHAT'S THE OPERATIONAL IMPACT?

The Cl0p gang is another RaaS model advocate, where affiliates distribute the malware, and the core operators manage ransom negotiations and infrastructure. The gang's cyberattacks primarily target large corporations, surmising they are more willing and able to pay large ransoms. Cl0p has frequently taken advantage of zero-day vulnerabilities, unknown security flaws exploited before protection can be implemented.

Some infamous examples include the **MOVEit Transfer attack** in 2023, where a hidden flaw (**CVE-2023-34362**) was exploited to steal data from hundreds of organizations, and attacks on **Accellion FTA** and **Cleo enterprise** software. The quadruple extortion model exploits both technical and psychological weaknesses.

WHAT TO KEEP IN MIND?

Given Cl0p's sophisticated techniques, organizations must adopt a proactive cybersecurity approach. Regularly applying security patches and updates, especially for file transfer software like MOVEit, Go-Anywhere MFT, and Accellion FTA, is crucial, along with regular vulnerability assessments.

Since Cl0p targets file transfer systems, it is strongly recommended to encrypt sensitive data both in transit and at rest, regularly back up critical files to offline or immutable storage, and restrict access to file transfer tools. Preparation is key, requiring developed and tested incident response playbooks, tabletop exercises, and a clear policy on negotiating with ransomware actors.

CLOP IN NUMBERS

RANSOM PAYMENTS EXTORTED:

More than **$500 million.**

ORGANIZATIONS COMPROMISED (GOANYWHERE MFT 2023):

Over 130 organizations.

EARNINGS FROM MOVEIT TRANSFER CAMPAIGN (2023): $75-100 MILLION.

ACTIVITY RANKING (Q4 2024):

Emerged as the most active group, overtaking RansomHub and Akira.

RANSOMWARE MARKET GROWTH (2024):

A 42% increase in reported attacks, plus a 125% increase in active groups.

ACTOR 6

LYNX

LYNX

ETHICALLY CHALLENGED

Lynx ransomware, with its many worldwide cybercriminals, utilizes TTPs such as terminating processes, deleting backup files, and encrypting network shares, making their attacks especially devastating. While a sophisticated group, they are also a newer player, targeting widely between SMEs and enterprises to extort funds.

The group deploys a RaaS model to create and disseminate their attacks across industries such as finance, architecture, and manufacturing sectors.

WHAT MAKES THEM DIFFERENT?

The cybercriminals behind the Lynx ransomware claim to follow an "**ethica**l" approach when choosing targets to minimize harm done to society, stating they do not target governmental institutions, health-care, or non-profit organizations. To recruit more threat actors, Lynx uses affiliate marketing techniques to good effect. The structured RaaS panel is divided into multiple sections (e.g. "**News**," "**Companies**," "**Chats**," "**Stuffers**," and "**Leaks**") to make their activities easier to deploy. **Lynx affiliates also receive a generous 80% share** of ransom proceeds, handle all negotiations, and maintain control over the ransom wallet. Lynx also offers additional services, such as a call center to harass victims and advanced storage solutions for the more performant affiliates. Most businesses today use Windows as their preferred operating system, and for this reason, Lynx malware runs only on Microsoft Windows OS to disrupt operations.

WHAT'S THE OPERATIONAL IMPACT?

The IoCs used by the Lynx group include phishing emails and social engineering, where emails are sent to targets to download and install the Lynx malware. Once executed, the Lynx malware encrypts files and appends the **.lynx extension** to the file name and deletes backup files like shadow copies to hinder recovery. The group typically employs double extortion tactics to pressure victims into paying the ransom, where stolen data is simultaneously sold on leak sites and to the highest bidder.

Lynx ransomware relies on several cyberattack vectors to gain access to the victim's data, including malicious downloads of ransomware and hacking forums where information can be exchanged. Lynx ransomware uses the **Restart Manager API RstrtMgr** to enhance its encryption capabilities and maximize its impact. It also utilizes specific commands such as **executables (.exe), installers (.msi), and libraries (.dll)** to execute the ransomware, and executes privilege escalation exploits to gain elevated system access and bypass security restrictions. Lynx ransomware actively terminates system processes, including anti-virus software, to bypass security defenses.

The group uses external cloud storage providers to avoid the detection of exfiltration. Lynx ransomware modifies the desktop background of the infected system, replacing it with a ransom note in a **ReadMe. Txt file**. It encrypts networks by appending the file **extension .lynx** to erase backup files, including shadow copies, and encrypts network shares with the **Advanced Encryption Standard (AES)**. TOR is also used to maintain anonymity and communicate with victims.

WHAT TO KEEP IN MIND?

Lynx operates with discipline, often delaying payload execution to avoid immediate detection. It selects its victims carefully, favoring mid-sized financial and logistics firms with under-resourced SOCs. The group's tactics reflect a growing trend of stealth-first ransomware operations, prioritizing persistence and lateral movement over rapid disruption. Unlike many RaaS affiliates, Lynx operators display centralized coordination and evidence of reconnaissance tailored to each victim. This is not opportunistic malware—it's methodical sabotage that aligns with business cycles and infrastructure dependencies. Its encryption routines are modular, enabling targeted disruption while preserving leverage for negotiation. For CISOs, the presence of Lynx signals a shift toward adversaries who blend espionage-level patience with extortion-driven endgames.

LYNX IN NUMBERS

YEAR OF EMERGENCE: JULY 2024

GEOGRAPHIC REACH:

Affected more than 20 countries globally, including the United States, the United Kingdom, Germany, Canada, France, Spain, and South Korea.

VICTIM COUNT (JANUARY 2025):

Data leak site lists 96 victims, but suspected amount is higher.

U.S. VICTIM SHARE: 60% OF VICTIMS LOCATED WITHIN THE UNITED STATES.

MOST TARGETED INDUSTRY:

Manufacturing industry (over 20% attack rate).

CODE SIMILARITY:

48% overall code similarity with INC ransomware and 70.8% similarity in specific functions, suggesting repurposed source code.

ACTOR 7

DRAGONFORCE

DRAGONFORCE

A NEW ARRIVAL MAKING A BIG SPLASH

Who claims to take over a rival ransomware group and then brags about it online? DragonForce is an actor keen to make some noise in a saturated rebel market.

Once an irrelevant hacktivist group, the DragonForce gang has evolved into a professional ransomware operation with some notable victims (most recently behind the Marks & Spencer attack). In a nutshell they run a RaaS program, build custom payloads, and leak stolen data on their terms. Consider them worth paying attention to.

Their ransomware variant emerged around August 2023, but its roots trace back further. Originally known as DragonForce Malaysia, the group began as a pro Palestine hacktivist group, targeting organizations across the Asia-Pacific and the US. Over time, though, its focus shifted from political attacks to more profit driven ransomware campaigns.

WHAT MAKES THEM DIFFERENT?

By early 2023, the DragonForce ransomware group had fully pivoted into ransomware. In March 2024, the group expanded its RaaS offering, launching a model akin to a franchise. Affiliates could now run their own ransomware brands, supported by DragonForce's infrastructure, with everything from client panels and data hosting to 24/7 backend support with anti-DDoS protection. Technically, DragonForce started with a **LockBit 3.0** based variant, then introduced a second strain, a fork of **ContiV3**, tailored for double extortion attacks. Their malware was designed for broad impact, targeting ESXi, NAS, BSD, and Microsoft Windows systems, with constant upgrades to its encryption engine and features. Unlike groups that operate in bursts, DragonForce maintains steady pressure. One of their standout moves is its claim to have taken over the infrastructure of RansomHub, which was the largest ransomware group over the past year. This announcement appeared both on the **RAMP forum** and DragonForce's Tor-based leak site, signaling a bold attempt by the cybercriminals to absorb or replace a major competitor.

WHAT'S THE OPERATIONAL IMPACT?

DragonForce typically starts with phishing emails or other social engineering scams, tricking users into opening malicious attachments or clicking harmful links. Once inside, they often exploit vulnerabilities in **Remote Desktop Protocol** (RDP) and **VPN solutions**. After gaining a foothold, DragonForce deploys tools like Cobalt Strike and SystemBC to move laterally and harvest credentials. They use network scanners, such as SoftPerfect Network Scanner, to identify additional targets.

A key tactic is "**Bring Your Own Vulnerable Driver**" (BYOVD), which allows them to disable security software by exploiting known vulnerable drivers. DragonForce's RaaS program is highly customizable. Affiliates can adjust encryption settings, disable security features, and personalize ransom notes. The business model is hugely motivating itself as it lets affiliates **keep 80% of any ransom collected**.

Even if backups are available, victims still face the risk of a damaging data breach. The ransomware payload is designed to be flexible and robust, targeting various systems, including **ESXi**, **NAS**, **BSD**, and Windows environments. The gang relies on a dedicated DragonForce leak site on the dark web to pressure victims. If the ransom payment isn't received, stolen data is publicly posted, adding reputational and regulatory risk.

WHAT TO KEEP IN MIND?

DragonForce may not innovate, but its precision and operational maturity make it a persistent threat. It favors exposed remote access points like RDP and VPNs, often combining them with fast weaponization of known vulnerabilities. Their payloads are customized, often delivered with commercially available red-teaming tools to mask intent. Attack patterns suggest a focus on sectors with high uptime sensitivity and delayed patching practices. Recent activity shows increasing use of BYOD techniques to bypass endpoint defenses. Their infrastructure is resilient and adapted for long haul extortion, not smash and grab hits. For CISOs, DragonForce represents the industrialization of ransomware, well funded, patient, and business aware.

DRAGONFORCE IN NUMBERS

YEAR OF EMERGENCE: AUGUST 2023 (AS RANSOMWARE VARIANT)

VICTIM COUNT:

Claimed 82 victims between August 2023 and August 2024.

AFFILIATE REVENUE SPLIT:

Affiliates keep 80% of any ransom collected.

TARGETED SYSTEMS:

ESXi, NAS, BSD, and Microsoft Windows.

GEOGRAPHIC CONCENTRATION:

Heavy concentration in the US, UK, and Australia.

NOTABLE VICTIMS:

Ohio Lottery (600 GB data stolen), Yakult Australia (nearly 100 GB data exfiltrated), Saudi Arabian real estate/construction company (over 6 TB data stolen), Marks & Spencer, Co-op.

RANSOMWARE RESOURCES

1	#StopRansomware Guide by CISA, FBI, NSA, and MS-ISAC
2	NIST Ransomware Risk Management (Special Publication 1800-26)
3	The No More Ransom Project
4	CISA's Ransomware Webpage
5	FBI Ransomware Resources
6	U.S. Secret Service Ransomware Advisory
7	FinCEN Advisory on Ransomware (FIN-2021-A004)
8	U.S. Department of Health and Human Services (HHS) Ransomware Guidance
9	U.S. Treasury Department's OFAC Advisory on Ransomware Payments
10	Australian Cyber Security Centre (ACSC) Ransomware Guidance
11	UK National Cyber Security Centre (NCSC) Ransomware Guidance
12	ENISA (European Union Agency for Cybersecurity) Ransomware Resources
13	Multi-State Information Sharing and Analysis Center (MS-ISAC) Ransomware Guide
14	Institute for Security and Technology (IST) - Ransomware Task Force
15	INTERPOL's Global Cybercrime Programme Resources
16	Ransomware Task Force (RTF) Report
17	Europol's European Cybercrime Centre (EC3) Public Awareness Materials

WRAPPING UP

One core question pops up again and again, In the face of such a relentless and evolving ecosystem, can organizations truly stay primed on the defensive?

In short, the answer is **yes**.

You need to dedicate proper attention, resources, and strategic manpower to reviewing your cyber strategy.

CISOs, with the right security measures in place, can absolutely navigate the myriad of vulnerabilities that ransomware groups exploit. The preceding profiles have shown that while the threat is complex, it is not insurmountable. From Black Basta's calculated social engineering to Cl0p's mass exploitation of zero days and RansomHub's franchise like RaaS platform, understanding the adversary's playbook is the first step toward defeating it.

Overall, you need not only shields against data encryption and theft but also ensures adherence to stringent regulatory standards and protects your organization from the operational, financial, and reputational damage that defines modern quadruple extortion tactics. The most critical aspect to consider is that proactive, external facing intelligence solutions are essential for safeguarding your brand's integrity. These tools mitigate security threats and help to bolster the confidence of your customers and partners.

Adding to this, the dynamic landscape of cyber threats where groups rebrand after takedowns and new actors constantly emerge underscores the urgency for businesses to constantly refine and update their security protocols. It is clear that to offset the risk of cyberattacks like these, a static approach to security will no longer suffice.

In short, you should zone in on these four core areas:

- **Creating a security first mindset culture across your organization**, with robust training to identify the sophisticated phishing and social engineering tactics that are common initial access vectors.

- **Proactive identification of potential vulnerabilities** by patching exposed systems like **VPNs** and **RDPs** and investing in external attack surface management.

- I**mplementation of cutting edge security measures and tools**, including MFA, network segmentation, and a "3-2-1" data protection strategy for secure, offline backups.

- **Evolving your cybersecurity outlook from a reactive to a proactive approach** by developing, testing, and regularly updating a well-defined incident response plan.

Detect, Anticipate, Control, External Threats

Secure your digital activities with CybelAngel, the only comprehensive threat Intelligence provider.

START NOW