

ALPHV Targeting

Ransomware & Digital Extortion

TLP: CLEAR

B-2023-12-05a



Key Findings

- ALPHV has been one of the most prominent ransomware and digital extortion (R&DE) threats to the majority of industries globally.
- ALPHV attacks as a proportion of total R&DE activity is on a slight downward trajectory. Likely contributing to this is the host of newer, highly-active threat collectives that have emerged in 2023, which are likely drawing affiliates from prominent, established ransomware-as-a-service (RaaS) offerings.
- The threat from ALPHV will almost certainly remain significant over the next two quarters, as affiliates continue a high attack tempo. Security teams should also monitor for an increasingly diverse spectrum of R&DE operations.

ALPHV Profile



ALPHV (also known as BlackCat and Noberus) is a ransomware strain used to compromise and extort its victims. First observed in 2021, ALPHV operates as a RaaS platform, whereby affiliates frequenting dark web forums subscribe to a subscription-based business model and are able to either purchase or lease malicious software strains. ALPHV is widely reported to have descended from former affiliates of ransomware collectives DarkSide and BlackMatter, which were active during 2020 and 2021 respectively. Its continued presence and prominence in malicious marketplaces is likely contributed to by affiliate payout rates of up to 90 percent, which is significantly higher than many other ransomware services.

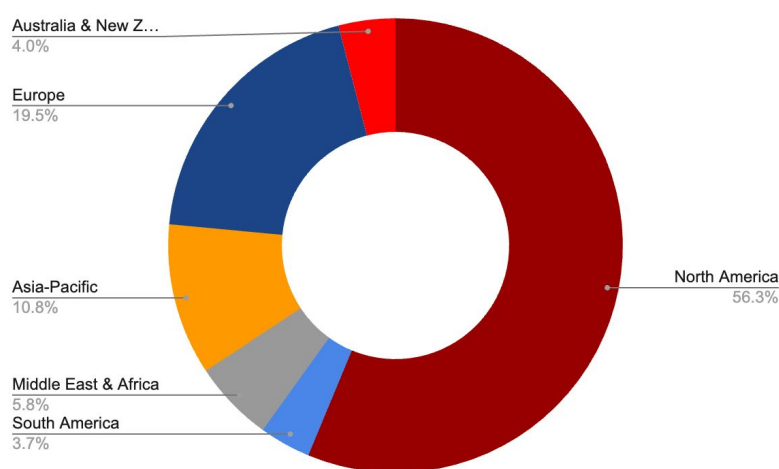
ALPHV is the most prominent and among the first ransomware strains to be written in the Rust programming language (considered more efficient, reliable, and faster than C and C++), creating appeal to threat actors able to leverage these benefits in their malicious software. The strain is known for its flexibility and adaptability, with subscription packages offering different encryption modes, customizable ransom notes, and data exfiltration methods that enable affiliates to fine-tune their attacks. ALPHV was also one of the first collectives to publish stolen credentials to a public data leak site, revealing the results of an attack to victims, other cybercriminals, security researchers, and shareholders. This applies additional pressure on the victim, increasing the chance of eliciting ransom payment.

Disclaimer: All data and analysis included in this report is based on ZeroFox collections only. This does not include data from third parties.

Targeting Overview

ALPHV has been a prominent ransomware strain between January 2022 and October 2023, accounting for approximately 10 percent of all observed R&DE incidents. In the seven quarters analyzed, ALPHV was consistently amongst the top three most frequently deployed ransomware strains.

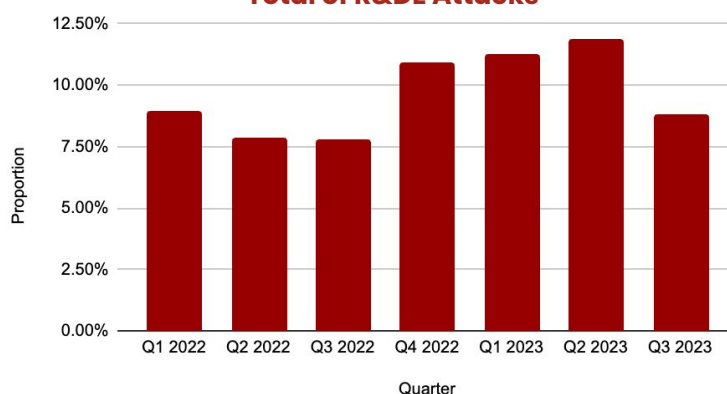
ALPHV Attacks by Region January 2022 - October 2023



Source: ZeroFox Intelligence

Though ALPHV has conducted significantly more attacks so far in 2023 than it did during 2022, attacks have been slightly decreasing overall since Q2—both in the number of total attacks and as a proportion of activity across the threat landscape. This is very likely contributed to by an increase throughout 2023 in new, highly-active threat collectives.

ALPHV Attacks as a Proportion of Total of R&DE Attacks



Source: ZeroFox Intelligence

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 5:00 PM (EST) on December 5, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



Intrusion Vectors

Exploit Internet-Facing Applications

In 2023 alone, affiliates have exploited vulnerabilities in internet-facing systems to deploy ALPHV, including, but not limited to:

- [CVE-2023-28223](#): A Windows domain name service Remote Code Execution vulnerability
- [CVE-2023-5694](#): Affects an unknown function in an internet banking system, leading to remote Cross-Site Scripting exploitation
- [CVE-2023-0669](#): A Remote Code Execution vulnerability in Fortra GoAnywhere Managed File Transfer (MFT)
- [CVE-2023-3690](#): Affects unknown functionality of URL parameters, leading to remote SQL injection

Historically, ALPHV affiliates are also known to have exploited:

- [CVE-2022-23479](#): A Broken Access Control vulnerability leading to Stored Cross-Site Scripting in Traffic Manager plugin
- [CVE-2022-44877](#): Allows remote attackers to execute arbitrary OS commands via shell metacharacters in the login parameter
- [CVE-2021-34523](#): A Microsoft Exchange Server elevation of privilege vulnerability
- [CVE-2021-31207](#): A Microsoft Exchange Server exploitation that bypasses security features
- [CVE-2021-27877](#): A Remote Unauthorized Access and privileged command execution via SHA authentication

Phishing (including Spear Phishing)

Affiliates leverage various social engineering methods to deliver malware, including spear phishing, call-back phishing (vishing), and mass malicious communications. These allow the threat actor to deliver and execute the malware remotely or obtain victim credentials that are used to gain initial system access.

Malware-as-a-Service (MaaS)

ALPHV affiliates have been observed leveraging the MaaS Emotet in order to initiate first-stage system breaches. Emotet has evolved significantly during recent years, offering affiliates the use of banking trojans and malicious botnets that enable the propagation of further malware. Other initial access malware strains have also been used, including Gootloader, SocGholish, Batloader, and Nitrogen.

External Remote Services

ALPHV affiliates are known to exploit Remote Desktop Protocol (RDP) to gain access to victim networks. Threat actors leverage legitimate user credentials obtained via credential harvesting to access external-facing remote working services.

Drive-by Compromise

Threat actors deploying ALPHV have been observed gaining access to a system via a user visiting a website over the normal course of browsing. The user's web browser is typically targeted for exploitation, but adversaries may use malicious domains for Application Access Token acquisition.

Valid Accounts

ALPHV operators are known to obtain credentials of existing accounts to gain initial access. Compromised credentials are used to bypass access controls, establish persistence, escalate privileges, and evade detection.

Initial Access Brokers

ZeroFox has identified ALPHV affiliates that purchase access from Initial Access Brokers on the deep and dark web (DDW), creating established relationships with sellers of access. Sales are increasingly moving towards private, off-forum channels rather than occurring in DDW marketplaces or forums. Established ALPHV affiliates very likely work closely with specific brokers to lower the cost of securing access.

Access sold off-forum is typically cheaper, meaning ALPHV affiliates are likely able to obtain discounts and even be alerted in advance to upcoming accesses that will be listed for sale. This will likely make ALPHV extortion attacks increasingly difficult to intercept in advance by DDW monitoring—and only prevented by a tight security posture, proper training against social engineering and phishing, and good overall company cyber hygiene.

In 2023, there has been an increase in access advertised into third-party vendors of major corporations and government entities. This is due to the potentially weaker security postures of third parties hired by larger organizations and the elevated privileges and accesses that come with being integrated into the larger entity.

Targeting By Region

North America (NA)

Between Q1 2022 and Q3 2023 ALPHV has been continuously leveraged against NA-based organizations and has accounted for approximately 11 percent of all R&DE attacks in the region. This is second only to prominent threat collective LockBit.

In this time period, ALPHV's most frequently-targeted industries NA have been:

1. Manufacturing
2. Healthcare
3. Financial Services
4. Legal & consulting
5. Retail

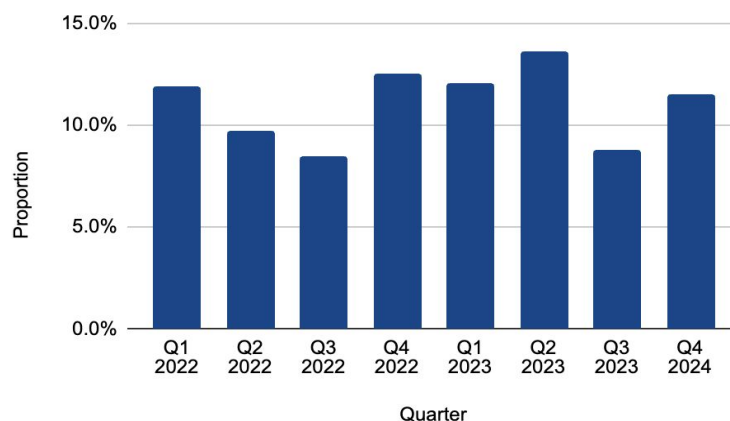
Similar to other R&DE collectives, ALPHV affiliates primarily targets NA-based organizations, with an average of 55 percent of attacks that leverage ALPHV ransomware targeting this region. This percentage has remained relatively similar since Q1 2022, fluctuating between 48.84 and 60.63 percent. However ALPHV has been consistently deployed against NA-based targets at significantly higher proportions of its total activity than the average observed from other threat collectives. There is a roughly even chance that this is contributed to by ALPHV affiliates being based in nations that politically rival NA countries, as well as viewing the region as more lucrative.

There is a roughly even chance that ALPHV's targeting will increase in the next two quarters as ZeroFox has observed an upward trend in the proportion of global R&DE attacks targeting NA. Given ALPHV's already successful and persistent presence in the region, however, there is also a roughly even

chance ALPHV will seek to simply maintain its current targeting patterns.

ALPHV remains one of the most prominent R&DE threats to NA-based organizations, being one of the top three most prolific threat collectives active in the region each quarter since Q1 2022. Notably, the proportion of R&DE activity in NA for which ALPHV ransomware is affiliated had very minimal variation, fluctuating between 8 and 13 percent and averaging at 11 percent. This is a stark contrast to other threat collectives, such as LockBit, for which associated activity fluctuated considerably.

Proportion of R&DE Against NA for Which ALPHV is Responsible



Source: ZeroFox Intelligence

ZeroFox anticipates there is a roughly even chance that ALPHV attacks as a proportion of all R&DE activity will reduce slightly in NA over the next two quarters. This is due primarily to a host of new threat collectives conducting attacks in the region, which are set to alter the threat landscape through developing techniques, tactics and procedures (TTPs). These groups, such as Akira, NoESCAPE, and Lost Trust, are demonstrating proficiency and the ability to conduct sophisticated attacks in shorter time frames than previously observed.

While it is likely that other groups will increasingly target NA organizations, reducing the proportion of attacks that ALPHV accounts for, ALPHV will very likely remain a prominent threat in the region in the next two quarters.

How ALPHV's Targeting of NA Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting NA	% of ALPHV's R&DE Targeting NA
Q1 2022	45.23%	56.90%
Q2 2022	42.52%	53.19%
Q3 2022	45.29%	48.84%
Q4 2022	48.28%	54.69%
Q1 2023	52.45%	56.41%
Q2 2023	52.90%	60.63%
Q3 2023	55.80%	56.00%

Source: ZeroFox Intelligence

Europe

ALPHV is a prominent threat to Europe-based organizations, having been the second-most leveraged ransomware strain deployed in the region since Q1 2022, accounting for approximately 6 percent of all attacks.

Between 2022 and 2023, ALPHV's most frequently-targeted industries in Europe have been:

1. Manufacturing
2. Professional Services
3. Technology
4. Retail
5. Legal Consulting

During 2023 there has been a significant increase in the number of R&DE attacks targeting Europe-based organizations, which is commensurate with the global increase in R&DE. This is despite a reduction in the proportion of attacks targeting the region, which has resumed an upward trajectory but remains lower than early-2022 peaks ALPHV's targeting of Europe-based organizations is not consistent with these trends; since Q1 2022, the proportion of ALPHV attacks targeting the region have been lower than the R&DE average—often by a significant margin. ALPHV's targeting of Europe peaked in Q3 2022 at 27.91 percent of total attacks before dropping as low as 12.6 percent in 2023. While Q3 2023 saw an increase, it remained below global averages.

ALPHV's relatively low levels of European targeting is very likely due primarily to the successful targeting of other lucrative regions. However, there is a roughly even chance that European targets will be increasingly targeted in the next two quarters, in line with the current trend observed across the threat landscape.

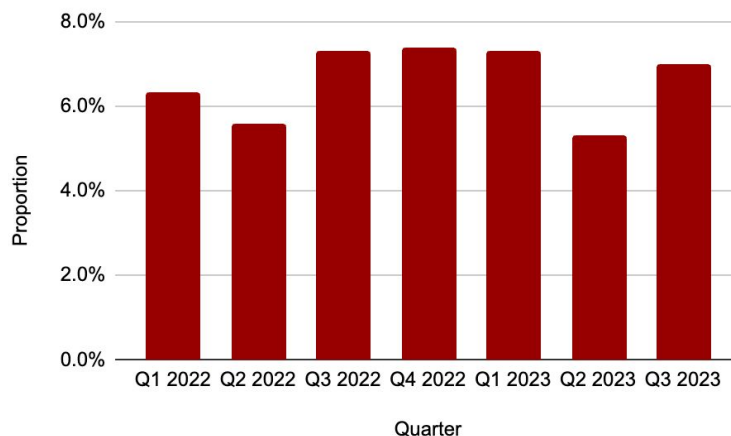
How ALPHV's Targeting of Europe Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting Europe	% of ALPHV's R&DE Targeting Europe
Q1 2022	34.15%	24.14%
Q2 2022	33.50%	23.40%
Q3 2022	29.89%	27.91%
Q4 2022	25.60%	17.19%
Q1 2023	25.50%	16.67%
Q2 2023	26.45%	12.60%
Q3 2023	27.59%	22.00%

Source: ZeroFox Intelligence

Since Q1 2022, the number of attacks targeting European organizations for which ALPHV affiliates were responsible is second only to threat collective Lockbit. Attacks per quarter have fluctuated very little, ranging between 5.6 and 7.2 percent, amounting to 11 and 22 attacks respectively. This relative consistency is similar to that of trends observed by ALPHV affiliates in NA and is in stark contrast to many other threat collectives whose targeting patterns by region fluctuate considerably.

Proportion of R&DE Against Europe for Which ALPHV is Responsible



Source: ZeroFox Intelligence

ZeroFox assesses it is likely that the proportion of R&DE attacks against European targets for which ALPHV affiliates are responsible will remain roughly the same during the next two quarters. Despite a rise between Q2 and Q3 2023, Q4 has so far seen a reduced attack tempo and remains consistently below the R&DE threat landscape average.

There is also a roughly even chance that ALPHV's proportion of attacks will reduce further, given the increased activity in the region stemming from collectives Play, Cactus, NoESCAPE, and Rhysida. This threat landscape diversification is very unlikely to result in ALPHV collectives becoming insignificant, however, and the strain is very likely to remain one of the most prominent threats to organizations in the region in the next two quarters.

Asia Pacific (APAC)

Between Q1 2022 and Q3 2023, ALPHV has been responsible for approximately 12 percent of R&DE attacks targeting organizations in the APAC region, making the strain the second most-prolific threat collective.

Between 2022 and 2023, ALPHV's most frequently-targeted industries in APAC are:

1. Manufacturing
2. Technology
3. Retail
4. Energy
5. Professional Services

The proportion of total R&DE attacks targeting APAC-based organizations has been steadily declining since 2022, from a high of approximately 12 percent down to 6.5 percent in Q3 2023. This is likely due primarily to the increased proportion of attacks leveraged against NA-based targets during the same period. Due to the increased R&DE activity being observed across the threat landscape, however, the total number of attacks in the APAC region are on an upward trajectory.

The targeting of APAC-based organizations by ALPHV affiliates is on an upward trajectory as a proportion of its total activity, in stark contrast to wider trends across the threat landscape. During 2023, they have disproportionately targeted the region by significant margins, after under-targeting in 2022. This is likely a result of the spread of affiliates leveraging ALPHV, with a roughly even chance that they are finding more success in the absence of other threat collectives. ZeroFox anticipates ALPHV affiliates will likely continue over-targeting APAC-based organizations over the next two quarters.

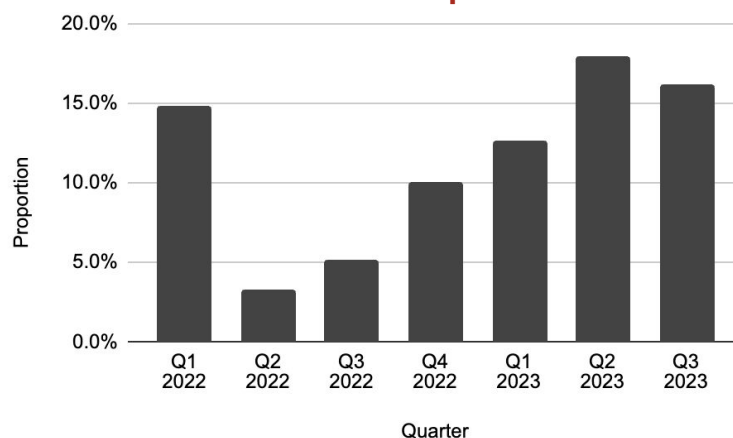
How ALPHV's Targeting of APAC Compares to R&DE as a Whole

Quarter	% of Total R&DE Targeting APAC	% of ALPHV's R&DE Targeting APAC
Q1 2022	8.31%	13.79%
Q2 2022	10.37%	4.26%
Q3 2022	10.69%	6.98%
Q4 2022	12.03%	10.94%
Q1 2023	9.08%	10.26%
Q2 2023	8.32%	12.60%
Q3 2023	6.50%	12.00%

Source: ZeroFox Intelligence

The proportion of R&DE attacks against APAC-based organizations for which ALPHV affiliates are responsible has increased significantly since Q2 2022, from approximately 5 to 17 percent. This has been contributed to by affiliates' increased focus on APAC-based organizations, as well as an overall increase in the leveraging of ALPHV during 2023, consolidating its position as one of the most prolific threat collectives in the region.

Proportion of R&DE Against APAC for Which ALPHV is Responsible



Source: ZeroFox Intelligence

It is likely that ALPHV will continue disproportionately targeting APAC-based organizations, and remain one of the primary R&DE threats to the region in the next two quarters. However, there is a roughly even chance that the overall number of attacks will begin to reduce in line with the broader threat landscape and other collectives that are increasingly active in the region (such as 8Base, Qilin, and NoESCAPE) reducing the proportion of attacks for which ALPHV is leveraged.

Middle East and Africa (MEA)

ALPHV affiliates are responsible for approximately 12 percent of R&DE attacks that occurred in the MEA region between Q1 2022 and Q3 2023. On average, approximately 5.5 percent of ALPHV's attacks target MEA-based organizations.

Between 2022 and 2023, ALPHV's most frequently-targeted industries in MEA are:

1. Manufacturing
2. Technology
3. Financial Services
4. Construction
5. Retail

R&DE attacks against MEA-based organizations have been on an upward trajectory throughout 2023, with the average number of attacks increasing by approximately 100 percent between Q2 2022 and Q3 2023. This still amounts to a relatively low attack tempo in comparison to other regions, however, with an average of 45 attacks per quarter. The proportion of total R&DE attacks that are leveraged against MEA-based organizations has remained relatively consistent since Q1 2022, fluctuating between 3 and 5 percent. As of Q3 2023, the proportion of ALPHV attacks targeting the region is on a slight downward trajectory.

Although slightly higher than average, the proportion of attacks against MEA-based organizations for which ALPHV affiliates are responsible has—alongside the proportion of total attacks—remained relatively consistent, as observed across other regions.

How ALPHV’s Targeting of MEA
Compares to R&DE as a Whole

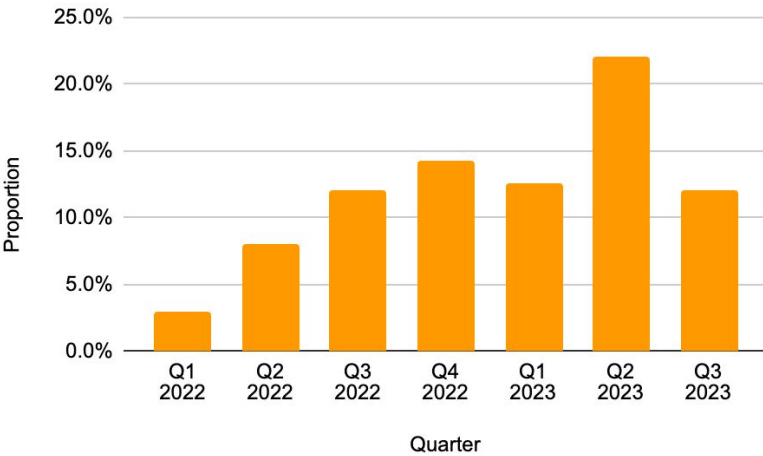
Quarter	% of Total R&DE Targeting MEA	% of ALPHV’s R&DE Targeting MEA
Q1 2022	5.38%	1.72%
Q2 2022	4.25%	4.26%
Q3 2022	4.53%	6.98%
Q4 2022	3.61%	4.69%
Q1 2023	5.76%	6.41%
Q2 2023	4.21%	7.87%
Q3 2023	4.39%	6.00%

Source: ZeroFox Intelligence

The proportion of R&DE attacks in MEA for which ALPHV is responsible has followed similar trends to those observed in NA and APAC. Increases observed during 2023 peaked in Q2 before beginning a steady decline that continues in Q4.

This decline is likely to continue over the next two quarters, both in number of attacks and a proportion of total ALPHV activity. This is very likely due primarily to an increase in Europe-focused activity and increased activity in MEA from threat collectives English, Meow, NoESCAPE, and Hunters International, which together have accounted for over 35 percent of all attacks in Q4 2023 so far.

Proportion of R&DE Against MEA for Which ALPHV is Responsible



Source: ZeroFox Intelligence

South America (SA)

Between Q1 2022 and Q3 2023, ALPHV strains have been leveraged in approximately 5.5 percent of all R&DE attacks in SA. On average, approximately 3.6 percent of all ALPHV attacks are leveraged against organizations in this region. The tempo of R&DE activity targeting SA-based organizations has remained on a relatively steady trajectory since Q1 2022, averaging 37 total attacks per quarter. Within the region, there are significant disparities between the targeting of different countries.

Between Q1 2022 and Q3 2023, ALPHV’s most frequently-targeted industries in SA have been:

- 1. Manufacturing
- 2. Technology
- 3. Critical Infrastructure
- 4. Education
- 5. Financial Services

ALPHV’s targeting of SA-based organizations is significantly more sporadic than that observed in other regions, fluctuating from 0 to 8.5 percent, though following the approximate trajectory of the wider R&DE threat landscape. This similarity is likely indicative of threat collectives across the R&DE landscape opportunistically capitalizing upon lucrative vulnerabilities in the region and is exacerbated by the relatively small number of total attacks. This in turn implies limited ALPHV resources dedicated to the region. Overall, SA was ALPHV’s least-targeted region during this time period, averaging approximately three attacks per quarter.

How ALPHV's Targeting of SA
Compares to R&DE as a Whole

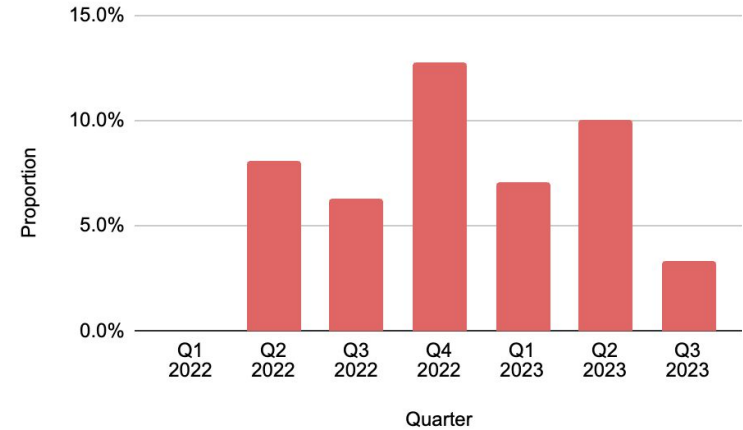
Quarter	% of Total R&DE Targeting SA	% of ALPHV's R&DE Targeting SA
Q1 2022	5.38%	0%
Q2 2022	6.29%	6.38%
Q3 2022	5.62%	4.65%
Q4 2022	6.36%	7.81%
Q1 2023	4.03%	2.56%
Q2 2023	5.61%	4.72%
Q3 2023	2.64%	1%

Source: ZeroFox Intelligence

ZeroFox anticipates the proportion of ALPHV attacks that target SA-based organizations to continue on a downward trajectory over the next two quarters, with continued under-targeting in comparison to the larger R&DE landscape.

Despite SA being ALPHV's least-targeted region, it is the third most prolific threat collective in the region. While LockBit is the most active by a significant margin, a large number of threat collectives conduct low tempo but continuous levels of activity.

Proportion of R&DE Against SA for
Which ALPHV is Responsible



Source: ZeroFox Intelligence

ALPHV will very likely remain one of the most significant threat actors in the region over the next two quarters. The proportion of attacks for which ALPHV is responsible is very likely to remain relatively low, with temporary spikes due to prominent vulnerability exploits that will likely be observed across threat groups.

Targeting By Industry

ALPHV affiliates leverage the ransomware against a large number of industries, targeting organizations of all sizes and statures. Like other R&DE threat collectives, affiliates target networks that offer low-risk, high-payoff opportunities, handle data likely to carry value in malicious marketplaces, or contain exploitable vulnerabilities able to provide initial access.

Between Q1 2022 and Q3 2023, ALPHV was consistently leveraged against the manufacturing industry more than any other, which follows trends set by the majority of the R&DE threat landscape. ZeroFox has also observed a significant rise in the number of ALPHV attacks leveraged against the healthcare industry, which increased by approximately 400 percent between Q1 and Q3 2024 and remains on an upward trajectory.

ALPHV Targeting Trends
Compared with Total R&DE

Industry Vertical	ALPHV Attacks as a Proportion of Total Industry Vertical R&DE 2022-2023	Trajectory of Total R&DE Against Industry Vertical	Trajectory of ALPHV Targeting Against Industry Vertical
Legal / Consulting	17%	↑	→
Financial Services	13%	↑	→
Professional Services	12%	↑	↓
Technology	10%	↑	→
Manufacturing	10%	↑	↑
Retail	10%	→	→
Food & Agriculture	9%	↑	↓
Healthcare	9%	↑	↑
Construction	8%	↑	→
Transport	7%	→	→
Government	7%	→	↓
Education	6%	↑	→

Source: ZeroFox Intelligence

Despite an upward trajectory in the proportion of total R&DE attacks for which ALPHV is responsible—and 2023 reaching an all-time high in the number of observed ransomware attacks—Q3 2023 saw a reduction in activity. There is a likely chance that this is the result of changes occurring within the collective, particularly given the downward trajectory observed in attacks against the food and agriculture and the professional services industries—both of which are increasing across the broader R&DE threat landscape.

There is a roughly even chance that ALPHV is undergoing a period of reduced popularity, resulting in affiliates opting to deploy other RaaS malware strains instead. Since at least Q2 2023, several newly-observed R&DE threat collectives have conducted increasingly frequent attacks. Some of these are likely rebrands of established threat collectives and are able to demonstrate proficiency at a faster pace than previously observed. This is very likely due to the increasing professionalism of malicious marketplaces and the proliferation of the multitude of services that are available. It is likely that some offer competitive services able to draw affiliates from other established strains.

Forward Look

- ALPHV will very likely remain one of the most prominent R&DE threats to the majority of industries across all locations.
- Over the next two quarters, it is almost certain that ALPHV attacks will predominantly target organizations based in Europe and North America, with the former likely to remain on an upward trajectory. It is unlikely that significant changes in targeting trends will be observed across other regions.
- The proportion of total attacks across the R&DE threat landscape for which ALPHV is responsible is likely to reduce slightly over the next two quarters, due in large part to the increased activity observed from new, highly-active threat collectives.
- ALPHV affiliates are likely to target the manufacturing, retail, and professional services sectors more heavily than others, though attacks targeting healthcare organizations are likely to remain on an upward trajectory.
- ALPHV's TTPs are unlikely to change significantly in the next two quarters, though there is a roughly even chance that any significant changes will focus on improving extortion methods, with affiliates demonstrating a history of deploying creative and novel pressure tactics.

Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Implement secure password policies, with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- Leverage cyber threat intelligence to inform detection of relevant cyber threats and associated TTPs.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.
- Deploy a robust External Attack Surface Management solution for ongoing ALPHV-targeted discovery.

How ZeroFox Can Help

Understand the strategic threat faced by your organization by leveraging **ZeroFox On-Demand Investigations** for custom threat intelligence. Understand TTPs used by threat actors—including ALPHV—targeting your organization by obtaining threat actor profiles and updates.

Utilize **ZeroFox Cyber Attack Surface Assessments** for a comprehensive assessment of all perimeter-facing and external digital assets to help mitigate potential exposures.

Employ **ZeroFox Platform's Intelligence Search** capability to help you identify compromised account credentials and vulnerabilities. You can also investigate network and infrastructure Indicators of Compromise (IOCs) of interest, including C2 domains, botnet-infected hosts, domain registrations, and phishing-related email addresses and phone numbers.

Leverage **ZeroFox Advanced Web Search and Dark Ops Curated Intelligence** to alert you to early warnings of threat actor chatter regarding your brand and update you on new extortion targets.

Utilize **ZeroFox's API Threat Intelligence Data Feeds** to correlate alerts in your environment with known threat actor Indicators of Attack/IOCs.

Should your organization be impacted by a data breach, utilize **ZeroFox Incident Response Services** to swiftly deploy **IDX data breach products and services** to mitigate the impact to you and your customers.

ALPHV IOCs

Search for ALPHV IOCs via the ZeroFox Platform Intelligence Search function [here](#).

ALPHV TTPs

Resource Development

Acquire Infrastructure: Virtual Private Server (T1583.003)

- Affiliates are likely to acquire Virtual Private Servers (VPSes) to be used in targeting.

Acquire Infrastructure: Malvertising (T1583.008)

- Affiliates are known to leverage malicious Google ads to lure in victims and mask payloads as legitimate software downloads.

Compromise Accounts (T1586)

- Affiliates compromise accounts for use in targeting.

Initial Access

External Remote Services (T1133)

- Affiliates exploit insecure RDP and VPNs to gain access to victim networks. Actors leverage legitimate user credentials obtained through credential harvesting to access external-facing remote services.

Valid Accounts (T1078)

- Affiliates obtain credentials of existing accounts to gain initial access.

Exploit Public-Facing Application (T1190)

- Affiliates exploit vulnerabilities in internet-facing systems such as ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207).

Phishing (T1566)

- Affiliates leverage phishing and spear phishing to gain access to victims' networks.

Execution

Windows Management Instrumentation (T1047)

- Affiliates leverage wmic[.]exe to delete shadow copies on compromised networks, execute commands, and move across the network.

Scheduled Task/Job (T1053)

- ALPHV exploits group policies to create a scheduled task on each host, which launches the payload.

Command and Scripting Interpreter (T1059)

- Affiliates leverage command and script interpreters (such as PowerShell commands) and batch scripts to stop IIS, delete Volume Shadow Copies, disable recovery, and clear event logs.

Software Deployment Tools (T1072)

- Affiliates leverage third-party software (such as administration, monitoring, and deployment systems) to move laterally.

Native API (T1106)

- ALPHV leverages Native API to execute behaviors.

System Services: Service Execution (T1569.002)

- ALPHV can self-propagate in the local area network using the legitimate PsExec utility, creating a temporary system service.

Persistence

Valid Accounts (T1078)

- Affiliates leverage compromised user accounts to maintain persistence.

Account Manipulation: Device Registration (T1098.005)

- Affiliates likely register devices to an adversary-controlled account.

Server Software Component (T1505)

- Affiliates place web shells on vulnerable servers.

Create or Modify System Process: Windows Service (T1543.003)

- Affiliates likely create or modify system-level Windows processes to execute malicious payloads.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

- Affiliates add a program to a startup folder or reference it with a Registry run key. Affiliates enable automatic logon for persistence.

Hijack Execution Flow: DLL Side-Loading (T1574.002)

- Affiliates side-load DLLs to execute malicious payloads.

Privilege Escalation

Valid Accounts (T1078)

- Affiliates leverage legitimate accounts specified in the configuration data to escalate privileges.

Access Token Manipulation: Create Process with Token (T1134.002)

- Affiliates escalate privileges by leveraging stolen authentication data and the function `CreateProcessWithLogonW`.

Domain Policy Modification: Domain Trust Modification (T1484.002)

- Affiliates add new domain trusts or alter the properties of existing domain trusts.

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)

- Affiliates bypass User Account Control to escalate privileges by using the `ICMLuaUtil` COM interface and the `Masquerade` PEB method.

DLL Side-Loading (T1574.002)

- Affiliates leverage side-load DLLs to escalate privileges and execute malicious payloads.

ALPHV TTPs

Defense Evasion

Obfuscated Files or Information (T1027)

- ALPHV obfuscates files by leveraging software packaging and embedding payloads within other files to conceal malicious content.

Masquerading (T1036)

- Affiliates manipulate features of their artifacts to make them appear legitimate, including renaming the SoftPerfect Network Scanner executable to svchost.exe.

Indicator Removal: Clear Windows Event Logs (T1070.001)

- The executable clears the Windows Event Log files.

Indicator Removal: File Deletion (T1070.004)

- The executable will delete itself from the disk.

Modify Registry (T1112)

- ALPHV uses PsExec to modify the system registry.

Access Token Manipulation (T1134)

- Affiliates modify access tokens and impersonate other users' existing tokens to bypass access controls.

Deobfuscate/Decode Files or Information (T1140)

- ALPHV decrypts configuration data and unpacks the PsExec utility in the payload.

File and Directory Permissions Modification: Windows File and

Directory Permissions Modification (T1222.001)

- ALPHV uses Windows commands to modify file or directory permissions to evade access control lists.

Domain Policy Modification: Group Policy Modification (T1484.001)

- ALPHV modifies Group Policy Objects to circumvent access controls for a domain.

Virtualization/Sandbox Evasion (T1497)

- ALPHV checks the value of the command-line parameter access token.

Disable or Modify Tools (T1562.001)

- ALPHV ends processes and services related to security and antivirus software.

Hide Artifacts: Process Argument Spoofing (T1564.010)

- ALPHV overwrites process memory to hide command-line arguments.

Hijack Execution Flow: Services Registry Permissions Weakness (T1574.011)

- ALPHV hijacks Registry entries used by services to execute its payload.

Reflective Code Loading (T1620)

- ALPHV reflectively loads code into a process to conceal its execution.

Debugger Evasion (T1622)

- ALPHV detects and avoids debuggers.

Credential Access

OS Credential Dumping: LSASS Memory (T1003.001)

- Affiliates dump the LSASS process using legitimate tools.

Multi-Factor Authentication (MFA) Interception (T1111)

- Affiliates intercept MFA mechanisms to obtain access to systems.

Unsecured Credentials (T1552)

- Affiliates obtain insecurely-stored authentication data from the registry and files.

Credentials from Password Stores (T1555)

- Affiliates obtain authentication data from web browsers and other storage spaces.

Discovery

System Service Discovery (T1007)

- ALPHV gathers information about registered local system services, including searching for security services, backups, and databases.

Query Registry (T1012)

- ALPHV can query the Windows Registry to gather system information.

System Network Configuration Discovery (T1016)

- ALPHV searches for network configuration and settings.

Remote System Discovery (T1018)

- ALPHV searches for servers connected to compromised networks.

System Owner/User Discovery (T1033)

- ALPHV attempts to identify system user names and those logged in on a compromised host.

Network Share Discovery (T1135)

- ALPHV searches for network shares on compromised systems.

Network Service Discovery (T1046)

- ALPHV searches for services running on remote hosts and local network infrastructure devices.

Permission Groups Discovery: Domain Groups (T1069.002)

- ALPHV uses the ADRecon tool to determine if a user on a compromised host has domain admin privileges.

System Information Discovery (T1082)

- ALPHV uses wmic to obtain the UUID.

File and Directory Discovery (T1083)

- ALPHV enumerates drives, directories, and files for encryption.

Account Discovery (T1087)

- ALPHV uses the ADRecon tool to obtain information about local and domain accounts.

Lateral Movement

Remote Services: Remote Desktop Protocol (T1021.001)

- Affiliates leverage RDP to move laterally across the network.

Remote Services: SMB/Windows Admin Shares (T1021.002)

- Affiliates leverage the PsExec utility to move laterally across the network.

Remote Services: SSH (T1021.004)

- Affiliates leverage the PuTTY utility to access Linux endpoints.

Lateral Tool Transfer (T1570)

- ALPHV self-propagates in the network by leveraging the PsExec utility.

Collection

Automated collection (T0802)

- Affiliates leverage ExMatter to automate collection.

Data from Local System (T1005)

- Affiliates collect information from the local system for exfiltration.

Data from Network Shared Drive (T1039)

- Affiliates harvest information from network resources for exfiltration.

Data Staged (T1074)

- Prior to exfiltration, affiliates collect data in 7Zip archives.

Data from Information Repositories (T1213)

- Affiliates collect information repositories for exfiltration.

ALPHV TTPs

Command & Control

Ingress Tool Transfer (T1105)

- Affiliates transfer tools from an external system into a compromised environment.

Non-Application Layer Protocol (T1095)

- Affiliates leverage a non-application layer protocol for communication between host and C2 server.

Application Layer Protocol (T1071)

- Affiliates leverage application layer protocols for remote access tools.

Remote Access Software (T1219)

- Affiliates likely leverage TeamViewer and ScreenConnect to establish an interactive C2 channel.

Protocol Tunneling (T1572)

- Affiliates leverage tunnels to automate SSH actions on Windows.

Encrypted Channel (T1573)

- Affiliates leverage asymmetric/symmetric encryption to conceal C2 traffic.

Exfiltration

Automated Exfiltration (T1020)

- Affiliates automatically upload files from target hosts to cloud storage services.

Data Transfer Size Limits (T1030)

- Stolen data is exfiltrated in fixed-size blocks to prevent exceeding data transfer limits.

Exfiltration Over C2 Channel (T1041)

- Affiliates exfiltrate data over existing C2 channels.

Exfiltration Over Alternative Protocol: Exfiltration Over

Asymmetric Encrypted Non-C2 Protocol (T1048.002)

- Affiliates leverage the ExMatter exfiltration tool to send data over an asymmetrically-encrypted network protocol.

Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)

- Affiliates exploit existing communications with cloud services like Google Docs to transmit data directly to cloud storage rather than using a C2 channel.

Impact

Data Destruction (T1485)

- If victims do not cooperate, affiliates delete encryption keys, making file decryption impossible.

Data Encrypted for Impact (T1486)

- Affiliates encrypt Windows devices, Linux devices, and VMWare instances. ALPHV encrypts the contents of files in the local system as well as on available network resources.

Service Stop (T1489)

- Affiliates can stop security, backup, database, email, and other services specified in VM configurations.

Inhibit System Recovery (T1490)

- Affiliates delete Windows Volume Shadow Copies using vssadmin and wmic, which disables recovery, empties Recycle Bin, and prevents backup services.

Defacement: Internal Defacement (T1491.001)

- Affiliates alter the desktop wallpaper on compromised hosts.

Network Denial of Service (T1498)

- If victims do not cooperate, affiliates can carry out DDoS attacks against the victim's infrastructure.

Disk Wipe: Disk Content Wipe (T1561.001)

- Affiliates wipe VM snapshots on compromised networks.

System Shutdown/Reboot (T1529)

- Affiliates shut down or reboot systems to disrupt access or aid the destruction of systems.



APPENDIX A:
ZeroFox Intelligence Probability Scale

All ZeroFox Intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of the occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

APPENDIX B:
Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use TLP: CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP: CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

READY TO SEE FOR YOURSELF?

- Request a Demo:
Sign up on zerofox.com/request-a-demo
- Learn More:
Visit zerofox.com
Contact us at sales@zerofox.com / 855.736.1400