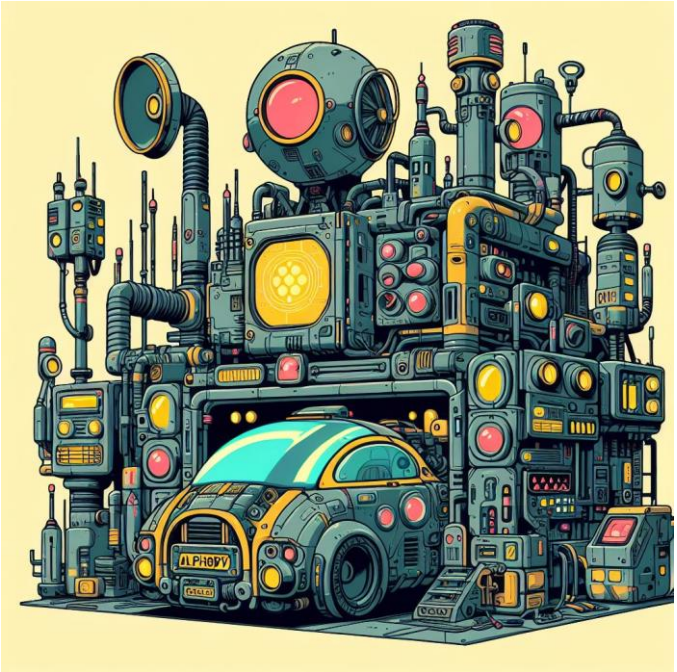

Abstract – This document presents a analysis of the Alpha ransomware site, associated with the ransomware group also known as BlackCat. The analysis covers the ransomware technical details, including its encryption mechanisms, initial access vectors, lateral movement techniques, and data exfiltration methods.

The insights gained from this analysis are important for cybersecurity practitioners, IT professionals, and policymakers. Understanding the intricacies of AlphV/BlackCat ransomware enables the development of more effective defense mechanisms, enhances incident response strategies.

I. Introduction

The AlphV ransomware site, associated with the ransomware group also known as BlackCat, experienced a series of disruptions and takedowns by the FBI, followed by attempts by the group to regain control. On December 19, 2023, the FBI, in a coordinated effort with international law enforcement, seized the group's website and shared a seizure notice on the leak site. This action was part of a disruption campaign against the BlackCat ransomware group, which has targeted the computer networks of over 1,000 victims worldwide, including those supporting U.S. critical infrastructure.

The FBI also developed a decryption tool that was provided to hundreds of ransomware victims globally, enabling businesses, schools, healthcare, and emergency services to recover and come back online. However, AlphV officials quickly responded by regaining temporary control of their site and posting a new notice stating, "This website has been unseized." They downplayed the significance of the FBI's action and announced that 'VIP' affiliates would receive a private program on separate isolated data centers.

Despite the initial success of the FBI's seizure, the AlphV site came back online, stripped of all references to victims previously published as part of their extortion strategy. The group also claimed that the FBI only had decryption keys for about 400 companies, leaving more than 3,000 victims with encrypted data. In retaliation, AlphV lifted its self-imposed ban on attacking critical infrastructure sectors, including healthcare and nuclear facilities.

The back-and-forth between the FBI and AlphV led to multiple instances of the website being seized and then "unseized," showcasing a tug-of-war over control of the site. Despite these events, the FBI and its partners continue to investigate and pursue the individuals behind BlackCat, with the goal of bringing them to justice.

II. AlphV ransomware

The ALPHV ransomware operates by running with an access token consisting of a 32-byte value. It comes with an encrypted configuration that contains a list of services/processes to a list of whitelisted directories/files/file extensions, and a list of stolen credentials from the victim environment. The ransomware scans the volumes on the local machine, mounts all unmounted volumes, and starts encrypting files. It also deletes all Volume Shadow Copies, making it harder for victims to recover their data.

Ransomware has evolved to include more complex arguments, making it harder to detect. Its configuration data is not JSON formatted, but raw structures, and it contains junk code and thousands of encrypted strings which hinder static analysis.

ALPHV ransomware has been observed to exploit vulnerabilities in exposed services or weak credentials for initial access. It also uses tools like ExMatter to steal sensitive data before deploying ransomware.

III. AlphV Tactics

The ALPHV ransomware employs several distribution tactics to compromise systems:

- **Phishing Emails**: These deceptive messages are crafted to lure victims into opening malicious content, often disguised as legitimate communications
- **Malvertising**: This involves the use of malicious advertisements to distribute malware. The ALPHV ransomware group has been known to manipulate Google Ads to lead unsuspecting users to malicious sites
- **Infected Software Installers**: The group often uses infected software installers to deliver the ransomware. This includes cloned webpages of legitimate organizations, which are used to distribute malware via infected links or files
- **Exploitation of Software Vulnerabilities**: The group exploits vulnerabilities in Windows operating systems, exchange servers, and Secure Mobile Access products to gain access to victims' networks
- **Triple Extortion Method**: This emerging threat involves stealing data from local machines and cloud servers, executing ransomware, and then introducing additional pressure on the victim via DDoS attacks or data leaks

IV. ALPHV ENTRY POINTS

The ALPHV ransomware has been identified as one of the most prolific ransomware-as-a-service variants in the world, affecting various sectors including Manufacturing, Technology, Retail & Wholesale, Finance, Healthcare and Public Health, Government and Energy, and Professional Services.

The initial entry points of ALPHV ransomware into victim networks are primarily through compromised user credentials and exploiting software vulnerabilities. For instance, ALPHV affiliates have been observed targeting publicly exposed Veritas Backup Exec installations, which were vulnerable to specific CVEs, for initial access to victim environments.

In the healthcare sector, ransomware attacks often exploit multiple possible entry points, including phishing emails, software vulnerabilities, Remote Desktop Protocol attacks, and drive-by downloads from malicious websites. The ALPHV ransomware has been a significant threat to the Healthcare and Public Health (HPH) sector.

In the financial sector, ALPHV ransomware attacks have underscored the need for enhanced incident detection capabilities and robust, timely reporting in the face of evolving cyber threats.

In the technology sector, the ALPHV ransomware gang has been known to compromise digital lending technology vendors, as seen in the attack on MeridianLink.

In the government sector, the disruptions caused by the ransomware variant have affected U.S. critical infrastructure, including government facilities.

In the energy sector, the ALPHV ransomware has been observed to target networks that support U.S. critical infrastructure.

In the professional services sector, the ALPHV ransomware has been known to target legal, IT, industrial, and financial services.

In addition to these methods, ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise. It's also worth noting that some ALPHV affiliates exfiltrate data and extort victims without ever deploying ransomware.

V. ENCRYPTION AND PAYMENTS METHODS

ALPHV ransomware employs sophisticated encryption methods to lock victims' data. The ransomware uses a combination of symmetric and asymmetric encryption, although specific details about these algorithms are not publicly disclosed. More specifically, ALPHV ransomware uses either AES or ChaCha20 encryption, depending on its configuration. The ransomware generates a random AES key for each file, which is then encrypted using an RSA public key stored in the BlackCat configuration. The file is then encrypted using AES.

As for payment methods, ALPHV ransomware affiliates typically request ransom payments in cryptocurrencies, specifically Bitcoin and Monero. These cryptocurrencies are favored due to their decentralized nature and the anonymity they provide to the recipients. The ransom amounts demanded by ALPHV are often exorbitant, ranging from five to six digits in USD. However, it's worth noting that the threat actors have been known to negotiate and accept payments below the initial ransom demand

VI. ALPHV TARGETS

The ALPHV ransomware has been found to target organizations of various sizes. According to data from ransom leak sites, the most victims come from companies with 51-200 employees, accounting for 20.57% of the total. This is followed by companies with less than 50 employees, which make up 16.91% of the victims:

- Companies with 501-1,000 employees: 7.12%
- Companies with 1,000-5,000 employees: 9.92%
- Companies with 5,000-10,000 employees: 2.38%
- Companies with 10,000+ employees: 4.46%

However, it's important to note that there is a category labeled "unknown," accounting for 27.87% of the total, indicating that the company size of some victims is not know.

In the fourth quarter of 2022, BlackCat's successful attacks primarily targeted small businesses, making up 38.9% of the total, followed by midsize companies at 28.6%.

ALPHV ransomware targets a wide range of organizations across multiple sectors:

- **Healthcare Organizations**: ALPHV has been linked to attacks on healthcare organizations, including the leaking of sensitive images of breast cancer patients. Norton Healthcare was also a victim of an ALPHV attack
- **Financial Institutions**: Fidelity National Financial was targeted by ALPHV. The ransomware group also claimed a breach in the systems of accounting software vendor Tipalti, with plans to extort the vendor's clients
- **Oil Companies**: Two German oil companies were targeted by the BlackCat ransomware group
- **Hospitality and Entertainment**: High-profile attacks have been linked to ALPHV, including those on MGM Resorts and Caesars Entertainment
- **Manufacturing and Warehousing**: ALPHV has targeted a manufacturer and a warehouse provider
- **Government Facilities and Emergency Services**: The DOJ connected the ALPHV ransomware variant to attacks against U.S. critical infrastructure, including government facilities and emergency services
- **Schools**: Schools have also been targeted by ALPHV
- **Defense Industrial Base Companies**: These companies have been targeted by ALPHV as part of its attacks on U.S. critical infrastructure

A. Healthcare Organizations industry

This ransomware variant has been involved in numerous incidents, affecting healthcare organizations by encrypting sensitive data, including patient information, and demanding ransom for decryption keys. The attacks have not only led to financial losses but also posed serious risks to patient care and safety. The aggressive enforcement actions by law enforcement agencies, including the development of decryption tools, have provided some relief to victims.

Notable Attacks and Impacts

- **McLaren HealthCare Ransomware Attack**: A significant ransomware attack on McLaren HealthCare, a large Michigan healthcare provider, highlighted the vulnerability of healthcare systems to cyber threats.
- **Targeting of Hospitals and Healthcare Networks**: The ALPHV/BlackCat ransomware group has attacked numerous hospitals, exposing sensitive patient data and placing patient care and lives at risk. These attacks have been part of a broader pattern of targeting networks that support U.S. critical infrastructure
- **Impact on Patient Care and Data Security**: The ransomware attacks on healthcare organizations have had devastating effects, including the disruption of healthcare services, exposure of sensitive health information, and financial losses.

Law Enforcement Response

- **DOJ Disruption Campaign**: The Department of Justice (DOJ), in collaboration with the FBI and international partners, launched a disruption campaign against the ALPHV/BlackCat ransomware group. This campaign aimed to mitigate the threat posed by the ransomware to critical infrastructure, including the healthcare sector
- **FBI Decryption Tool**: As part of the disruption efforts, the FBI developed a decryption tool that was provided to victims of the ALPHV ransomware, including healthcare organizations. This tool helped save victims from ransom demands totaling approximately $68 million, enabling affected businesses and healthcare facilities to recover and resume operations

B. Financial Institutions industry

The ALPHV has posed a significant threat to the financial institutions industry, leveraging sophisticated tactics to target banks, insurance companies, and other financial service providers. This ransomware variant is known for its stealthy operations, aiming to encrypt files, steal sensitive data, and demand ransom, often employing double-extortion tactics.

Notable Attacks and Impacts

- **Fidelity National Financial Attack**: One of the most high-profile incidents involved Fidelity National Financial, a Fortune 500 provider of title insurance. The ALPHV/Black Cat group claimed responsibility for this cyberattack, which led to disruptions in title insurance, escrow, and other related services.
- **Increased Ransomware Threats**: The financial industry has seen a surge in ransomware attacks, with a notable increase in both the frequency and sophistication of these incidents. Financial organizations are attractive targets due to the vast amounts of sensitive customer and partner data they hold, making them ideal for double-extortion attacks. The Clop, LockBit, and ALPHV/BlackCat ransomware groups have been particularly active in targeting this sector
- **Impact on Financial Operations**: Attacks on financial institutions can have severe consequences, including the disruption of critical financial services and trading activities. For instance, a suspected ransomware attack against the U.S. trading arm of the Industrial and Commercial Bank of China disrupted trading in the U.S. Treasury market, underscoring the potential for ransomware to impact financial stability

Law Enforcement Response and Industry Recommendations

- **Infrastructure Takedown** Efforts: Law enforcement agencies, including the FBI, have taken action against the infrastructure of the ALPHV ransomware group. These efforts aim to disrupt the group's operations and mitigate the threat they pose to critical sectors, including financial institutions
- **Cybersecurity Measures**: Financial institutions are advised to enhance their cybersecurity defenses to protect against ransomware threats. This includes investing in skilled personnel, advanced tools, and fostering a culture of proactive defense. Regular training, continuous monitoring, and collaboration within the cybersecurity community are essential strategies to combat sophisticated ransomware groups like ALPHV/BlackCat.

C. Oil Companies industry

The group operates under a ransomware-as-a-service (RaaS) model and has targeted organizations worldwide, including many in the United States

Notable Attacks and Impacts

ALPHV ransomware, also known as BlackCat, has targeted the oil industry with significant attacks. Notably, the group exposed 400 GB of data claimed to be stolen from Encino Energy, Ohio's primary oil producer. Despite this, Encino Energy reported no impact on their operations from the attack. In Europe, ALPHV was implicated in an attack on German oil companies Mabanaft and Oiltanking, which disrupted their loading and unloading systems and forced energy giant Shell to reroute supplies. These attacks demonstrate ALPHV's capability to target and disrupt critical energy infrastructure.

Law Enforcement Response

Law enforcement agencies, including the FBI, have taken action against the infrastructure of the ALPHV ransomware group. The FBI and international law enforcement agencies infiltrated and shut down the group's infrastructure, which had targeted more than 1,000 victims over 18 months. While no arrests were announced as part of the takedown, the operation

represents a significant effort to disrupt the activities of ransomware groups targeting critical sectors like the oil industry.

D. Hospitality and Entertainment industry

Alphv has targeted the hospitality and entertainment industry with several high-profile attacks. The group's operations are characterized by the theft of sensitive data, including customer personal and financial information, followed by demands for ransom. The sophisticated tactics employed by the group include the use of social engineering and malvertising.

Notable Attacks and Impacts

- **LBA Hospitality Attack**: ALPHV targeted LBA Hospitality, which manages hotels under major chains like Marriott and Hilton. The group claimed to have compromised around 200GB of "highly confidential" internal company data, including client and employee personal details, financial reports, credit card information, and more
- **MGM Resorts International Attack**: ALPHV was responsible for a cyberattack on MGM Resorts, causing significant operational disruptions. The attack disabled online reservation systems, digital room keys, slot machines, and websites. The group used social engineering tactics to gain access to MGM's systems and deployed ransomware to more than 100 ESXi hypervisors within MGM's network
- **Caesars Entertainment Attack**: Caesars Entertainment was another victim of ALPHV, which resulted in at least $100 million in damages and a reported ransom payment of $15 million
- **Westmont Hospitality Group Breach**: ALPHV/BlackCat ransomware gang claimed to have breached Westmont Hospitality Group, one of the world's largest privately-held hospitality businesses
- **Motel One Data Breach**: The group attacked the hotel chain Motel One and threatened to leak 6 TB of stolen data, including customer contact details, internal documents, and credit card data

Tactics and Techniques

The group has been known to abuse Google search ads to spread ransomware, using major brands as lures to direct users to malicious sites. They also employ social engineering tactics, such as spear-phishing and calling help desks to gain access to networks.

E. Manufacturing and Warehousing industry

The Alphv has been linked to a series of high-profile attacks on various sectors, including manufacturing and warehousing. The group has targeted more than 1,000 victims over the past 18 months, making it the second-most prolific ransomware-as-a-service group in the world.

Notable Attacks and Impacts

One of the most significant attacks attributed to the previously mentioned ALPHV/BlackCat group was on MGM Resorts International. The ALPHV/BlackCat ransomware group has also been observed using Google Ads to distribute malware, targeting businesses including a manufacturer and a warehouse provider. ALPHV/BlackCat affiliates often pose as company IT and/or helpdesk staff and use phone calls or SMS messages to obtain access to systems.

Another notable attack was on Clarion, a global manufacturer of audio and video equipment for cars and other vehicles. The group claimed to have leaked confidential data about their business and their partners, including the engineering information of the company's customers.

Organizations should also be aware that the group targets both Windows and Linux devices, as well as network-attached storage (NAS) devices, which are often used to store backups and sensitive data.

F. Government Facilities and Emergency Services industry

The Alpvh has significantly impacted the government facilities and emergency services industry. This ransomware variant, recognized for its sophisticated tactics and global reach, has targeted critical infrastructure, including government facilities and emergency services, causing disruptions and posing threats to national security and public safety.

Notable Attacks and Impacts

- **Disruption to Critical Infrastructure**: The ALPHV ransomware variant has been connected to attacks against U.S. critical infrastructure, encompassing government facilities and emergency services.
- **Global Scale of Operations**: ALPHV/BlackCat has emerged as the second most prolific ransomware-as-a-service variant globally. Its activities have led to significant global repercussions, with the group compromising over 1,000 entities worldwide.
- **Financial Impact and Ransom Payments**: The group has demanded over USD 500 million in ransoms and received nearly USD 300 million in payments. This financial impact highlights the lucrative nature of ransomware operations targeting critical sectors, including government facilities and emergency services

Law Enforcement Response

- **DOJ Disruption Campaign**: The Department of Justice, in collaboration with the FBI and international partners, launched a disruption campaign against the ALPHV/BlackCat ransomware group. This campaign aimed to mitigate the threat posed by the ransomware to critical infrastructure, including government facilities and emergency services
- **FBI Decryption Tool**: As part of the disruption efforts, the FBI developed a decryption tool provided to victims of the ALPHV ransomware, including those in the government facilities and emergency services industry. This tool helped save victims from ransom demands totaling approximately USD 68 million, enabling affected entities to recover and resume operations

G. Schools industry

ALPHV ransomware has targeted the education sector, including K-12 schools, universities, and other educational institutions. These attacks have disrupted educational processes and compromised sensitive student and staff data. The sector's susceptibility to cyber threats, due to often limited resources

and a large number of potential adversaries, necessitates a proactive approach to cybersecurity, including regular updates, employee training, and the implementation of strong security protocols.

Notable Attacks and Impacts

- **Increased Ransomware Attacks**: There has been a sharp increase in ransomware attacks on schools, with a 17 percent rise in such incidents. The attacks have involved the encryption of files and threats to leak stolen data if ransoms are not paid
- **High-Profile School Districts Affected**: School districts such as Dallas Public Schools and Minneapolis have been among the high-profile victims of ransomware attacks.
- **Global Reach**: The attacks on schools have not been limited to the United States; educational institutions in the United Kingdom, Australia, Germany, France, and Brazil have also encountered ransomware attacks
- **Impact on Educational Operations**: Ransomware attacks on schools can lead to significant operational disruptions, including the interruption of the application process, operations, and classes. In some cases, the attacks have been severe enough to contribute to the closure of schools

Tactics and Techniques

- **Double Extortion**: ALPHV ransomware operators often employ double extortion tactics, where they encrypt files and also threaten to leak stolen data. This approach puts additional pressure on the victims to pay the ransom
- **Exploitation of Vulnerabilities**: The leading cause of ransomware attacks in the education sector has been the exploitation of vulnerabilities in devices. Schools often lack the resources for robust cybersecurity measures, making them susceptible to such attacks

H. Defense Industrial Base Companies industry

The Alpvh has targeted a wide array of sectors, including the defense industrial base companies. This focus on critical infrastructure sectors underscores the strategic approach of the group to compromise entities that are vital to national security and economic stability.

Notable Attacks and Impacts

- **Targeting Critical Infrastructure**: The Department of Justice (DOJ) has identified the defense industrial base companies as one of the critical infrastructure sectors targeted by the ALPHV ransomware variant.
- **Financial and Operational Impact**: The global losses attributed to ALPHV, which employs multiple-extortion attack models, are substantial. The group's activities have resulted in significant financial demands and have underscored the potential for operational disruptions within the defense sector