NISOS.

THREAT ANALYSIS

Trigona Ransomware Family Explained

May 2023

RESEARCH

Table of Contents

Executive Summary

Although not officially branded as 'Trigona' until October 2022, samples of the ransomware strain have been observed globally prior to the re-branding due to Trigona's unique characteristics. First, Trigona is written in Delphi programming language, enabling the ransomware to leverage password-protected executables in order to obfuscate the malicious content within.[1] Additionally, the ransomware group utilizes an HTML application as a substitute for the typical text-file-based ransomware note.[2] As of February 2023 there have been at least 17 possible Trigona victims identified in the U.S., France, Italy, Germany, Australia and New Zealand.[3] [4] The ransomware operators appear to be primarily targeting marketing and finance organizations but the construction, agriculture, and high technology market segments are also impacted.[5]

Figure 1. Trigona related logo.
Source: BleepingComputer

[1] https://www.zscaler[.]com/blogs/security-research/technical-analysis-trigona-ransomware
[2] https://unit42.paloaltonetworks[.]com/trigona-ransomware-update/
[3] https://gbhackers[.]com/new-trigona-ransomware/
[4] https://izoologic[.]com/2023/03/20/trigona-ransomware-returns-to-hit-europe-australia-and-the-us/
[5] https://gbhackers[.]com/new-trigona-ransomware/

ID Ransomware, a free online service where victims can identify what ransomware encrypted their files by uploading sample encrypted files and ransom notes, has received over 190 Trigona-related submissions since the beginning of 2023.[6] An overview of the submission frequency distribution from the ID Ransomware platform is displayed below (Figure 2).

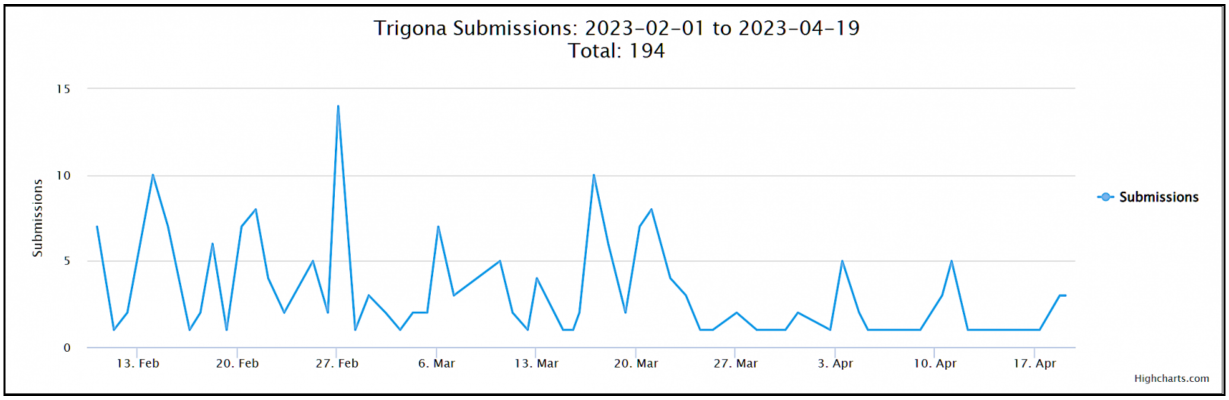


Figure 2. ID Ransomware Trigona Submissions.
Source: BleepingComputer[7]

Etymology and Group Lineage

Trigona shares commonalities with ALPHV/BlackCat and Crylock in terms of actual payload and typical operating norms. Similar to ALPHV/BlackCat, Trigona has been observed exploiting a Zoho ManageEngine ADSelfService Plus vulnerability and follows common living-off-the-land (LotL) tactics by leveraging legitimate tools already present in the victim's environment. More directly, Trigona leverages ALPHV/BlackCat's reputation and data leak site as an additional payment pressuring tactic.[8]

Another functional similarity between the two ransomware families is the presence of a data wiper feature. Trigona released the data wiper feature during an update,[9] confirmed via VirusTotal,[10] around March 12th, 2023 (date identified via SHA hash listed in zscaler wiper-related writeup).[11] Despite this similarity, a key distinction between ALPHV/BlackCat and Trigona is the programming language used for the payloads. Trigona's core payload is built using the Delphi programming language whereas ALPHV/BlackCat's payload is written in Rust.[12]

Trigona also appears to share some characteristics with the CryLock ransomware strain.[13] Both ransomware families deliver ransom notes in HTML format and share common language in the notes themselves which contain specific messaging, such as "the price depends on how soon you will contact

[6] https://id-ransomware.malwarehunterteam[.]com/
[7] https://www.bleepingcomputer[.]com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/
[8] https://areteir[.]com/static/5055b091d5c24a9ed63a06d70f2da20e/Trigona-Report_020224_web.pdf
[9] https://www.zscaler[.]com/blogs/security-research/technical-analysis-trigona-ransomware
[10] https://www.google[.]com/url?q=https://www.virustotal.com/gui/file/8cbe32f31befe7c4169f25614afd1778006e4bda6c6091531bc7b4ff4bf62376/details&sa=D&source=docs&ust=1682986142339875&usg=AOvVaw1xBzTg2LNEkc0cDz1pS4_b
[11] https://www.zscaler[[.]com/blogs/security-research/technical-analysis-trigona-ransomware
[12] https://areteir[.]com/static/5055b091d5c24a9ed63a06d70f2da20e/Trigona-Report_020224_web.pdf
[13] https://unit42.paloaltonetworks[.]com/trigona-ransomware-update/#post-127253-_ka9kzoe4ky9r

us."[14] Additionally, both strains leverage RSA and AES encryption with Trigona choosing 4,112-bit RSA and 256-bit AES encryption in Output Feedback Mode (OFM) specifically.[15]

High Level Attack Overview

Although the means of initial access remain unconfirmed as early reports vary, unpatched system exploitation and email-based social engineering are the prime suspects. Externally-facing, mismanaged MS-SQL Servers are known to be prime targets for brute-forcing in combination with CLR Shell work.[16] Additionally, a specific vulnerability this group exploits is CVE-2021-40539, commonly known as "Zoho ManageEngine ADSelfService Plus authentication bypass", which is associated with the Rest API's and ADSelfServices build 6113 and older.[17] This exploit allows remote code execution without any required user activity.

Once initial access is gained, Trigona operators upload a file, DC2.exe,[18] which will contain the password protected version of the Mimikatz executable. By being password protected, the executable's true purpose is obfuscated from most common detection mechanisms making the credential stealing capability fly in under the radar. Mimikatz is then leveraged to either modify existing account credentials, create new accounts, or change user group associations.[19]

Persistence is established via Registry Run keys with lateraling typically taking place via SMB. Post infection, Trigona-encrypted files get a "._locked" appended to the end of the prior filename. Once file encryption has begun, the group's ransomware note, "how_to_decrypt.hta", gets loaded as an HTML application. The ransom note offers free decryption of three (3) victim files and displays the ransomware price which is cited to increase every hour.

Beyond the novelty of using an HTML application as the ransomware note, Trigona operators embed JavaScript that contains unique computer IDs (CIDs) & victim IDs (VIDs) and ask victims to pay with Monero (XMR), a cryptocurrency known for protecting user anonymity, via a dedicated TOR-based payment portal as seen below (Figure 3):[20]

[14] https://gbhackers[.]com/new-trigona-ransomware/

[15] https://www.zscaler[.]com/blogs/security-research/technical-analysis-trigona-ransomware

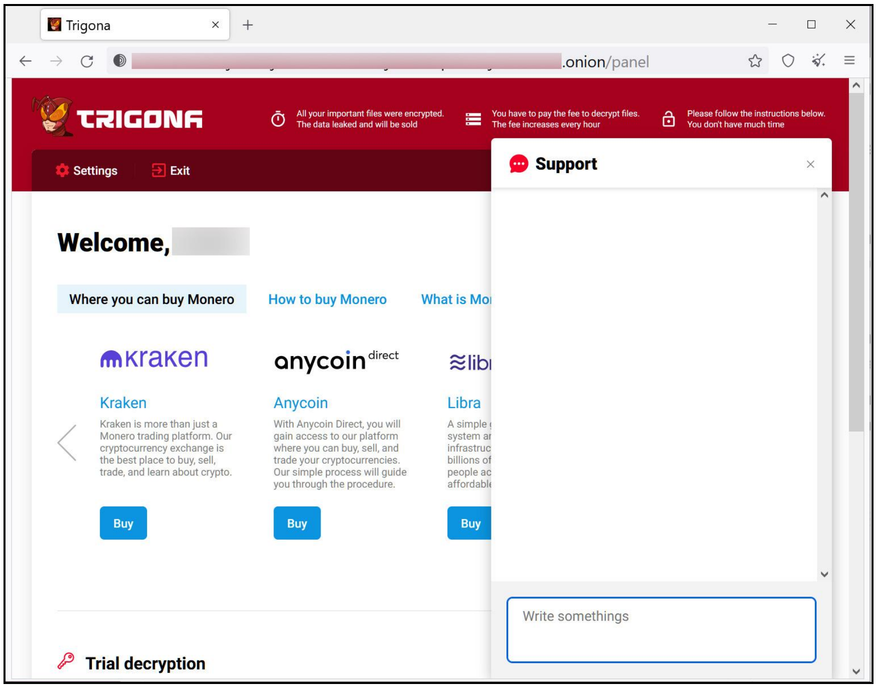
[16] https://www.hivepro[.]com/wp-content/uploads/2023/04/Trigona-Ransomware-Targets-Improperly-Managed-MS-SQL-Servers_TA2023184.pdf

[17] https://areteir[.]com/static/5055b091d5c24a9ed63a06d70f2da20e/Trigona-Report_020224_web.pdf

[18] https://unit42.paloaltonetworks[.]com/trigona-ransomware-update/

[19] https://www.extrahop[.]com/company/blog/2023/trigona-ransomware-uses-password-protected-malware/

[20] https://unit42.paloaltonetworks[.]com/trigona-ransomware-update/



All your important files were encrypted. The data leaked and will be sold

You have to pay the fee to decrypt files. The fee increases every hour

Please follow the instructions below. You don't have much time

Welcome, [redacted]

Kraken

Kraken is more than just a Monero trading platform. Our cryptocurrency exchange is the best place to buy, sell, trade, and learn about crypto.

Anycoin

With Anycoin Direct, you will gain access to our platform where you can buy, sell, and trade your cryptocurrencies. Our simple process will guide you through the procedure.

Libra

A simple
system ar
infrastruc
billions of
people ac
affordable

Figure 3. Trigona Tor negotiation site.
Source: BleepingComputer[21]

Known Infrastructure & Associated Indicators Of Compromise (IOCs):

MD5 hashes:[22]

- 1cece45e368656d322b68467ad1b8c02 - Trigona Dropper (svcservice.exe)
- 1e71a0bb69803a2ca902397e08269302 - Batch Runner (svchost.bat)
- 46b639d59fea86c21e5c4b05b3e29617 -CLR SqlShell
- 530967fb3b7d9427552e4ac181a37b9a - Trigona Ransomware (svchost.exe)
- 5db23a2c723cbceabec8d5e545302dc4 - nt.exe

SHA256 hashes:[23]

- 248e7d2463bbfee6e3141b7e55fa87d73eba50a7daa25bed40a03ee82e93d7db
- 596cf4cc2bbe87d5f19cca11561a93785b6f0e8fa51989bf7db7619582f25864
- 704f1655ce9127d7aab6d82660b48a127b5f00cadd7282acb03c440f21dae5e2
- 859e62c87826a759dbff2594927ead2d23031b37b53233062f68549222311
- 8f8d01131ef7a66fd220dc91388e3c21988d975d54b6e69befd06ad7de9f6079
- 97c79199c2f3f2edf2fdc8c59c8770e1cb8726e7e441da2c4162470a710b35f5
- A86ed15ca8d1da51ca14e55d12b4965fb352b80e75d064df9413954f4e1be0a7
- Accd5bcf57e8f9ef803079396f525955d2cfffbf5fe8279f744ee17a7c7b9aac
- Da32b322268455757a4ef22bdeb009c58eaca9717113f1597675c50e6a36960a
- E7c9ec3048d3ea5b16dce31ec01fd0f1a965f5ae1cbc1276d35e224831d307fc
- E97de28072dd10cde0e778604762aa26ebcb4cef505000d95b4fb95872ad741b
- F29b948905449f330d2e5070d767d0dac4837d0b566eee28282dc78749083684

[21] https://www.bleepingcomputer[.]com/news/security/trigona-ransomware-spotted-in-increasing-attacks-worldwide/
[22] https://asec.ahnlab[.]com/ko/51168/
[23] https://www.fortinet[.]com/blog/threat-research/ransomware-roundup-trigona-ransomware

- Fa6f869798d289ee7b70d00a649145b01a93f425257c05394663ff48c7877b0d
- Fbba6f4fd457dec3e85be2a628e31378dc8d395ae8a927b2dde40880701879f2
- Fd25d5aca273485dec73260bdee67e5ff876eaa687b157250dfa792892f6a1b6

List of IP/URLs associated with the exploit activity listed by Country:

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
157.230.249.23

Onion address of the threat subject:
hxxp://3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion/ [24]

Leak site attributed to Trigona: 45.227.253[.]99[25]

Other Trigona Infrastructure identified: 45.227.253[.]106, 45.227.253[.]98. 45.227.253[.]107[26]

[24] https://www.hivepro[.]com/wp-content/uploads/2023/04/Trigona-Ransomware-Targets-Improperly-Managed-MS-SQL-Servers_TA2023184.pdf

[25] https://twitter[.]com/paul_eubanks/status/1628497550679351303?cxt=HHwWjoCxnZ35ypktAAAA

[26] https://unit42.paloaltonetworks[.]com/trigona-ransomware-update/