Kitten.gif: Meet the Sabbath Ransomware Affiliate Program, Again

By Mandiant

Published: 2021-11-29 · Archived: 2026-04-05 21:14:28 UTC

Written by: Tyler McLellan, Brandan Schondorfer

In September 2021, Mandiant discovered a post on exploit.in seeking partners for a new ransomware affiliate program. By October 21, 2021, the 54BB47h (Sabbath) ransomware shaming site and blog were created and quickly became the talk of security researchers. In contrast with most other affiliate programs, Mandiant observed two occasions where the ransomware operator provided its affiliates with pre-configured Cobalt Strike BEACON backdoor payloads. While the use of BEACON is common practice in ransomware intrusions, the use of a ransom affiliate program operator provided BEACON is unusual and offers both a challenge for attribution efforts while also offering additional avenues for detection.

Mandiant Advanced Practices began proactively identifying similar BEACON infrastructure across past Mandiant Consulting engagements, Advanced Practices external adversary discovery program, and commercially available malware repositories. Through this analysis, Advanced Practices linked the new Sabbath group to ransom activity under previously used names including Arcane and Eruption.

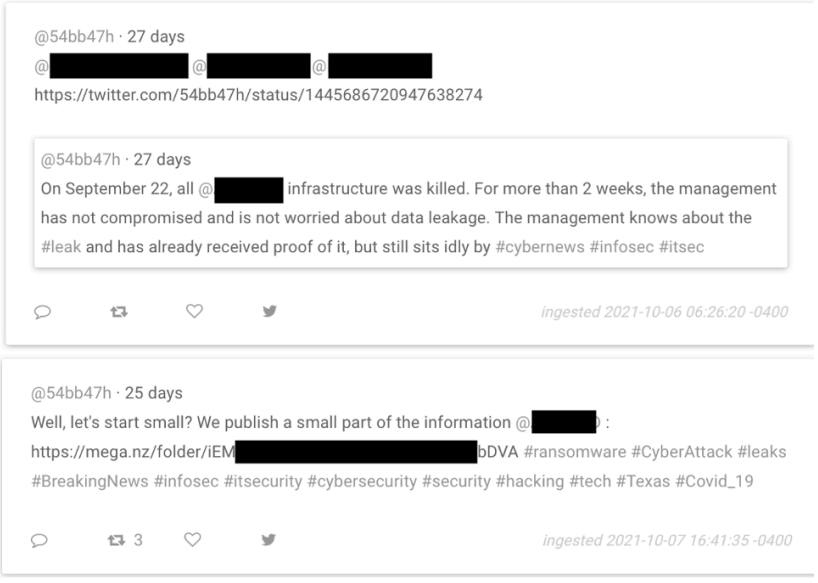
UNC2190, operating as Arcane and Sabbath, has targeted critical infrastructure including education, health, and natural resources in the United States and Canada since June 2021. The targeting of critical infrastructure by ransomware groups has become increasingly concerning as evidenced by governments moving to target ransomware actors as national security level threats with particular attention to groups that target and disrupt critical infrastructure.

Stealthy Ransomware

In July 2020, UNC2190 deployed ROLLCOAST ransomware while branded as Eruption. Mandiant has not observed samples of UNC2190-deployed ransomware in 2021 and no samples of ROLLCOAST have ever been submitted to VirusTotal. In the following sections, some of the technical reasons why UNC2190's ransomware has evaded capture and discovery will be discussed.

Next Level Extortion and 'Backup Killers'

Sabbath first came to light in October 2021 when the group publicly shamed and extorted a US school district on Reddit and from a now suspended Twitter account, @54BB47h. During this recent extortion, the threat actor demanded a multi-million-dollar payment after deploying ransomware. Media reporting indicated that the group took the unusually aggressive step of emailing staff, parents and even students directly to further apply public pressure on the school district.



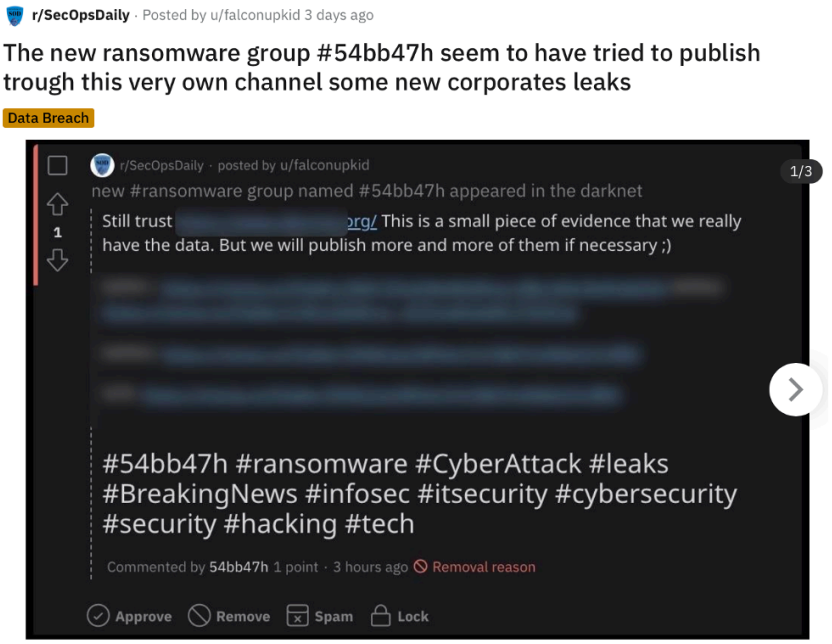
@54BB47h on Twitter

UNC2190 uses a multifaceted extortion model where ransomware deployment may be quite limited in scope, bulk data is stolen as leverage, and the threat actor actively attempts to destroy backups.

```
.########.##........########..########..##........########.##.....##....########.########....###....##.....##
.##.......##....##..##.....##.##.....##.##....##..##.....##.##.....##.....##....##.....##..##.##...###...###
.##.......##....##..##.....##.##.....##.##....##..##.....##.##.....##.....##....##.....##.##...##..#### ####
.########..##....##..########..########..##....##....##....#########.....##....##.....##.##.....##.## ### ##
.......##.##########.##.....##.##.....##.##########...##.....##.....##.....##....##.....##.#########.##.....##
.##....##.##.......##..##.....##.##.....##.##.....##....##.....##.....##.....##....##.....##.##.....##.##.....##
..######..########.##...########..########........##....##.....##.....##.....##....########..##.....##.##.....##
Dear Sir or Madam,
-----------------------------------------------------------------------------------------------------------
Congratulations!
Id like to inform you that your company has been randomly chosen for audit and that you haven't
passed it.
All of your servers are encrypted, same as your backups. Our encryption algorithms impossible to
decrypt, same as your company data and infrastructure. However, do not get nervous, as you shall
restore all of your all your infrastructure and data! In order to do that, follow simple steps
that are described bellow:
1. Buy decryption key.
2. Restore all of the company data and infrastructure.
-----------------------------------------------------------------------------------------------------------
The system hack wasnt done eiter by your competitors or 3rd party, it was strictly our
initiative. Our main and only interest is money.
Also, to be mentioned, we value our reputation and principles a lot, therefore any amateur
attempts will be strictly suppressed and will make current situation worse. In addition, all of
decryption software mentioned above is tested, as a proof of our abilities, there is a
possibility of decrypting few small files for free, for your understanding.
-----------------------------------------------------------------------------------------------------------
Data leakage.
As you probably understood, we have stolen big volume of data from yur network. Mainly, we stole
data using our smartfilters from all of your servers- full dump of your network.
We may discuss the volume of stolen data.
To sum up, we have completely destroyed your system and infrastructure. We would like to suggest
you to think twice, and think about the problems associated with GDPR.
-----------------------------------------------------------------------------------------------------------
TO GET YOUR INFO VISIT US:
<redacted>.onion
```

Ransom note example

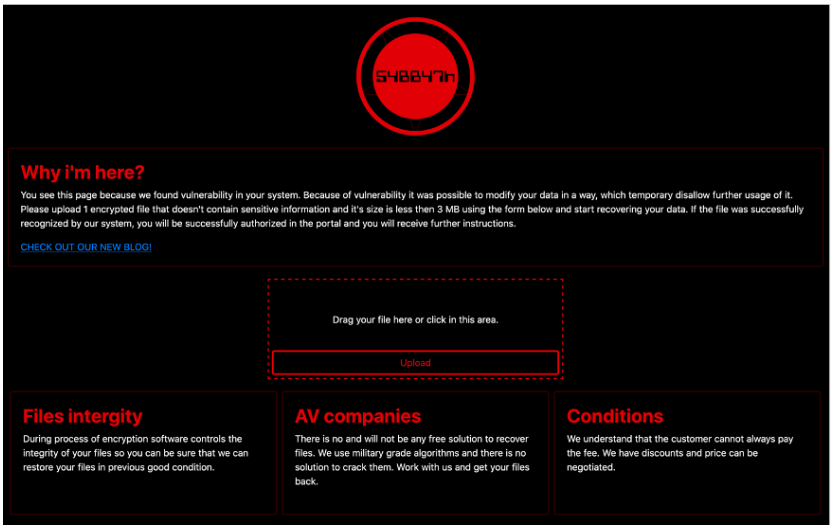
The threat actor has utilized public data leaks to extort the victims to pay ransom demands. While Sabbath operates a public shaming blog, Mandiant only observed victims being publicly extorted beginning in mid-November 2021, where 6 victims were added over the span of two days. Previously under the Arcane brand, Mandiant observed three victims publicly extorted in June 2021.



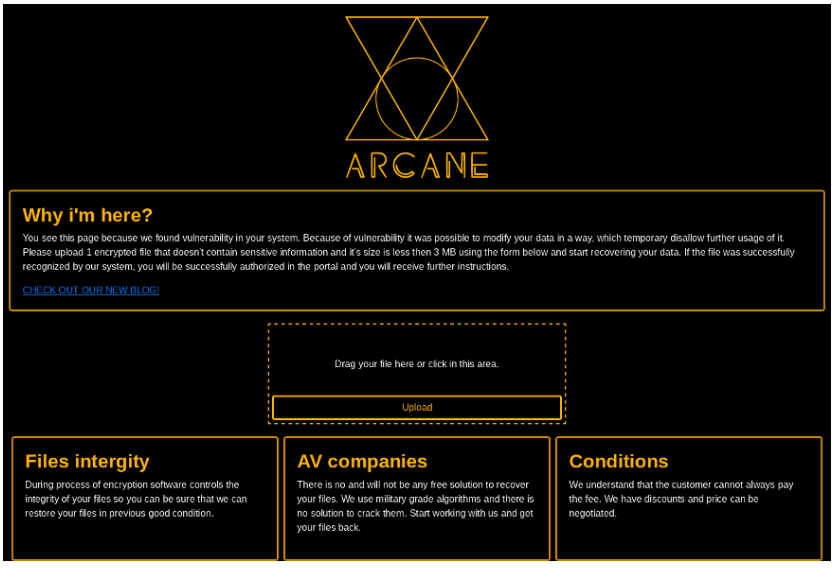
Source: Reddit SecOpsDaily

Arcane Rebranded

Mandiant discovered that the new Sabbath public shaming web portal and blog first published in October 2021 is nearly identical to that of Arcane from June 2021. This included the same text content, and minor changes to the name, color scheme, and logo. The threat actor kept consistent grammatical errors in their updated web forums.



Sabbath 54bb47h5qu4k7l4d7v5ix3i6ak6elysn3net4by4ihmvrhu7cvbskoqd.onion Website October 2021



thearcane.top website June 2021

Behind the scenes, few technical changes were made to the affiliate model used to carry out the attacks between the rebranding from Arcane to Sabbath. BEACON samples and infrastructure from both ransomware affiliate services remained unchanged. The malware sample PE compile times were identical on Themida-packed BEACON droppers used by the threat actor (such as md5 6bd1a3849bb9d5f9ac5b4f4049081334 and 38667bc3ad2dcef35a5f343a5073e3f2).

Hunting for UNC2190 BEACON Samples

Since July 2020, UNC2190 has utilized BEACON with unique Malleable profile elements, including:

- GET requests ending with kitten.gif, such as:
  - hxxps://markettc.biz/gifs/ZsoCzxU-X-5D3ZhV2zzKgc8SHhygCYmWpBRCS_mRV_SZxyWaaSPw7FFtcZ66twQ_uTDp5EdlsmRa6K8GPtMVBnKOHhM6EgcnE4znZPiyXskZJXmHLSYAnkpLwhOrxyCoRkFthelDgVnuW7k3UVzDjEz3W4xuxSKBq2DuseaG-F0dob1M/kitten.gif
- POST variable “image_url”, points to a specific image hosted on popular Russian social media site VK: hxxps://sun9-23.userapi.com/G4JvdZDEfLdIPlNN1-JkMGQ2unf2KEIV54Om5g/abJ70jGHfVk.jpg
- User agent, such as: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36"

Mandiant discovered additional infrastructure similarities utilized by UNC2190 including:

- Actual IPs masked using a cloud service.
- Self-signed TLS certificate common name “Microsoft IT TLS CA 5”

Evolving to Evade Antivirus Detection

In March 2021, Mandiant Consulting observed an intrusion for another tracked UNC group where antivirus had detected and blocked two attempts to load a BEACON payload which Mandiant attributes to UNC2190. Subsequently, a different tracked threat actor deployed different ransomware at this victim with more success. Starting July 6, 2021, Mandiant detected the use of Themida to pack UNC2190 BEACON malware and protect it from detection.

ROLLCOAST Ransomware Deep Dive

In July 2020, Mandiant first detected ROLLCOAST ransomware usage by UNC2190. ROLLCOAST

is a ransomware program that encrypts files on logical drives attached to a system. ROLLCOAST is a Dynamic Linked Library (DLL) with no named exports. When observed by Mandiant it uniquely had only one ordinal export 0x01. This suggested the sample was designed to avoid detection and be invoked within memory, possibly through BEACON provided to affiliates. Incident responders working on similar intrusions should capture memory for analysis. ROLLCOAST was not written to disk during this intrusion and was only detected in memory by Mandiant.

The malware begins by checking the system language and exits if it detects a non-supported language code from the table below. Many other ransomware families have similar checks to avoid encrypting systems in Russia and other Commonwealth of Independent States member countries presumably to avoid attracting the attention of law enforcement in countries where the ransomware operator and affiliates are more likely to reside.

Language Exclusions

ROLLCOAST will exit if the system language matches one of the following:

Language ID	Description
0x419	Russian (Russia)
0x41A	Croatian (Croatia)
0x41B	Slovak (Slovakia)
0x41C	Albanian (Albania)
0x41D	Swedish (Sweden)
0x41E	Thai (Thailand)
0x41F	Turkish (Turkey)
0x420	Urdu (Islamic Republic of Pakistan)
0x421	Indonesian (Indonesia)
0x422	Ukrainian (Ukraine)
0x423	Belarusian (Belarus)
0x424	Slovenian (Slovenia)
0x425	Estonian (Estonia)
0x426	Latvian (Latvia)
0x427	Lithuanian (Lithuania)
0x428	Tajik (Cyrillic, Tajikistan)
0x429	Persian (Iran)
0x42A	Vietnamese (Vietnam)
0x42B	Armenian (Armenia)
0x42C	Azerbaijani (Latin, Azerbaijan)
0x42D	Basque (Basque)
0x42E	Upper Sorbian (Germany)
0x42F	Macedonian (Former Yugoslav Republic of Macedonia)
0x430	Southern Sotho (South Africa)

0x431	Tsonga (South Africa)
0x432	Setswana (South Africa)
0x433	Venda (South Africa)
0x434	isiXhosa (South Africa)
0x435	isiZulu (South Africa)
0x436	Afrikaans (South Africa)
0x437	Georgian (Georgia)
0x438	Faroese (Faroe Islands)
0x439	Hindi (India)
0x43A	Maltese (Malta)
0x43B	Sami, Northern (Norway)
0x43D	Yiddish (World)
0x43E	Malay (Malaysia)
0x43F	Kazakh (Kazakhstan)
0x440	Kyrgyz (Kyrgyzstan)
0x441	Kiswahili (Kenya)
0x442	Turkmen (Turkmenistan)
0x443	Uzbek (Latin, Uzbekistan)
0x444	Tatar (Russia)

Similarities to Tycoon

Mandiant compared elements of ROLLCOAST to elements of Tycoon ransomware and found some similarities:

- Both ransomware families encrypt files using AES in GCM mode
- Overlap between the ignored directories, files, and extensions including the ignored extension ".lolz".

This suggests the developers modelled ROLLCOAST on, or copied elements from, Tycoon ransomware. ROLLCOAST and TYCOON differ in their overall implementations: TYCOON is a Java based ransomware whereas ROLLCOAST is not. In addition, there is functionality in the publicly reported TYCOON that ROLLCOAST does not appear to have (shell commands, backup tampering, firewall tampering, wmic).

ROLLCOAST Strings

```
 FOUND DEVICE:
Start encryption of %s
[-] Failed to init dir traverse for: %s
Finished encryption of %s
Work out other countries. Don't be fool!
Hello from test.dll. Parameter is '%s'
Hello from test.dll. There is no parameter
Microsoft Primitive Provider
[-] AES FAILED 1: STATUS_NOT_FOUND
[-] AES FAILED 1: STATUS_INVALID_PARAMETER
[-] AES FAILED 1: STATUS_NO_MEMORY
[-] AES FAILED 1: UNDEFINED
ChainingModeGCM
```

ROLLCOAST Encrypted File Naming Convention

Files are encrypted and renamed to this format: .[].

Example encrypted file recovered from VirusTotal:

covid results from .pdf.[6EEC0F355072].54bb47h

Conclusion

Although UNC2190 is a lesser known and potentially a smaller ransomware affiliate group, it's smaller size and repeated rebranding has allowed it to avoid much public scrutiny. In Mandiant's 2021 Trends and 2022 Predictions report, ransomware data theft operations affecting healthcare are noted as having increased from January 2020 to June 2021, despite some groups claiming they would avoid targeting hospitals. UNC2190 has continued to operate over the past year while making only minor changes to their strategies and tooling, including the introduction of a commercial packer and the rebranding of their service offering. This highlights how well-known tools, such as BEACON, can lead to impactful and lucrative incidents even when leveraged by lesser-known groups.

Acknowledgements

With thanks Joshua Shilko for analytical contributions, Barry Vengerik, Tufail Ahmed, Isif Ibrahima, Andrew Thompson, Jake Nicastro, Nick Richard, and Moritz Raabe for technical review, and all the Mandiant Researchers, Consultants, Advanced Practices External Collectors, and FLARE REs for support, research, and assistance to create the content of this post.

MITRE ATT&CK

Mandiant has observed UNC2190 use the following techniques:

ATT&CK Tactic Category	Techniques
Discovery	T1016: System Network Configuration Discovery T1057: Process Discovery T1083: File and Directory Discovery T1518: Software Discovery
Impact	T1486: Data Encrypted for Impact
Discovery	T1016: System Network Configuration Discovery T1057: Process Discovery T1083: File and Directory Discovery T1518: Software Discovery
Defense Evasion	T1027: Obfuscated Files or Information T1027.002: Software Packing T1055: Process Injection T1497: Virtualization/Sandbox Evasion T1497.001: System Checks T1564.003: Hidden Window
Persistence	T1136: Create Account
Command and Control	T1071.001: Web Protocols T1573.002: Asymmetric Cryptography
Resource Development	T1587.003: Digital Certificates T1608.003: Install Digital Certificate
Execution	T1059.001: PowerShell

Yara Signatures

Note: FE_Hunting rules are designed to broadly capture suspicious files and are not designed to detect a particular malware or threat.

```
 rule FE_Hunting_THEMIDA_strings_FEBeta
{
    meta:
        author = "Mandiant"
        date_created = "2021-10-26"
        date_modified = "2021-10-26"
        md5 = "7669f00b467e2990be182584b341c0e8"
        rev = 2
        sid = 415583
    strings:
        $themida = ".themida" nocase
    condition:
        uint16(0) == 0x5A4D and filesize < 20MB and (@themida[1] < 1024)
}
```

```
 rule FE_Ransomware_Win64_ROLLCOAST_1
{
    meta:
        author = "Mandiant"
        date_created = "2020-07-15"
        date_modified = "2020-07-15"
        md5 = "45882426ecddb032981fd6c299b3cc47"
        rev = 2
    strings:
        $sb1 = { 48 8D [5] 48 8D ?? 24 ?? E8 [4-32] B? 30 00 00 00 [8-64] 25 FF F9 FF FF 0F BA E8 0B }
        $sb2 = { FF D? 85 C0 0F 84 [4] 48 8D [2-16] 83 E8 06 0F 84 [4] 83 E8 08 0F 84 [4] 83 E8 0F }
        $sb3 = { 41 B8 C5 02 00 00 0F 10 00 0F 10 48 10 0F 11 02 0F 10 40 20 0F 11 4A 10 0F 10 48 30 0F 11 42 20 0F 10 40
        $sb4 = { FF 15 [4] 05 E7 FB FF FF 83 F8 2B }
        $ss1 = "\x00Program Files\\" wide
        $ss2 = "\x00Program Files (x86)\\" wide
        $ss3 = "\x00.[\x00"
        $ss4 = "\x00].\x00"
    condition:
        (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x020B) and all o
}
```

Indicators

MALWARE FAMILY	Indicator
BEACON	aequuira1aedeezais5i.probes.space
BEACON	jeithe7eijeefohch3qu.probes.site
BEACON	datatransferdc.com
BEACON	farhadl.com
BEACON	markettc.biz
BEACON	probes.space
BEACON	tinysidney.com

BEACON	helpgoldr.com
BEACON	frankir.com
BEACON	greentuks.com
BEACON	45.79.55.129:443
BEACON	45.146.166.24:443
BEACON	45.147.230.221:2002
BEACON	aimee0febai5phoht2ti.probes.website
BEACON	cofeeloveers.com
BEACON	doratir.com
BEACON	gordonzon.com
BEACON	probes.site
BEACON	probes.website
BEACON	45.79.55.129:80
BEACON	45.141.84.182:443
BEACON	45.147.230.137:3001
BEACON	PE Compile time 1622138290 (2021/05/27 17:58:10)

MALWARE FAMILY	MD5	SHA1	SHA256
BEACON	ef3363dfe2515b826584ab53c4bb7812	3357fd8d5a253b7d84101e902480bf2dd2f7773c	da92878c314307a5e5c9df687ec19a40
BEACON	f1b2f83aa08b8f6f01cac6bf686786d2	366390c3cd829d1172f02e564d35cfb2c667e9fc	0fb410b9a4d32a473b2ee28d4dc5e19a
BEACON	6bd1a3849bb9d5f9ac5b4f4049081334	a0928456f12e909ec03eadce449bc80f120bfbf8	298662f3fed24d757634a022c16f4124
BEACON	e94089ff2e0b93ce38076cca370cf8cc	dc3c26f305648a12484c17d6166397a002a93707	afd61168c1fae6841faa3860dca0e583
BEACON	ac76d6c5c223688edf2d53745036d594	5972b873977912adf06203b61685f32a6ccb9eee	a053408747e9b32721d25c00351c4ce

BEACON	64da229042dffddf5bb30a4a1d8b1f1e	3dc46fa5ebc87e8adcb6eaa0b407574506c957bb	b2ffd7d83e004308a97355a18529fe35
BEACON	1789f6177300d503289c482910f223d9	5c3f297bab8a5e93aac91a9df920c54bee2c836d	e302a958856208adeab4ab3cd6d2991e
BEACON	dbfa3eb08d858d5bbb0cc72f497192b0	182e9d1026c63503aadb78bbc3788b7ba2cdb69a	8ddb23c90cb4133b4624127a1db7533
BEACON	79c6c4329a36df20a6abf67b01352b20	fc7b3d8beab604cf47203f4f9a2aa8594bd54fb7	1bbb11e526141af7bafb5d4db3671b1a
BEACON	6ae156c0a1900b6ff2c903a950d50dce	7b178842e1b53f163f869d9da3da32032fe29abb	1cd586852d2c06b0f7209c7a4da8f3d0
BEACON	b0333d840e136326a2bd612fcf73fff0	8467b4f784156f2e508a3fed0ef0b6ddcf330c0d	79b47780382f54ca039ad248d8241e4
BEACON	7669f00b467e2990be182584b341c0e8	2eaa91f38461d708ee6e94ec2f738f3cdfb229b7	f4ac75a045acee2cadbe9fa0e02bfd4ab
BEACON	60aec56cb2262ae46fc39c45fc814711	bb22515f2e8e4d5660dc8565869d966502a0123e	3edb237aeee6efad6f21f0f2c2037ec0f
BEACON	f7e7201325892dcc287c60a0748edb16	35f02a778ea7504331ddd025f0d927e0773ffd31	a4891cc85802833d9a89e2522a42a7e3
BEACON	c4a369880e3e5c3dc42ebf8cdacc9d6c	037889e6d714c7ff6341bdb8a8bebbddc21fc36e	756ed760cbf4b35054c78a75009f748f
BEACON	98f2b23eb265d73a05b2cce17d53eba4	41cc9afc79aaee60f6436192c6582907e41d89f7	87cdcbc55aed4267f47a913b17f4bc69
BEACON	38667bc3ad2dcef35a5f343a5073e3f2	22cf10ec5047a86a49c1819c4943290321a29918	a8741f6f400c7fedfbdc7a298ab4a636b
BEACON	aa2a14e1819f4b1cc685801e07186b0d	101930bbec76ee4a147117cdfcb56aa2208a579d	5a6b7569c2b8e91f5bd8a67322af384c
BEACON	61bbe1c1b2aa40c0d8aa7e00c2c4f7b6	6eff4b7b5ccf92eb0f134591237fe1db7c71826a	f883f7d7c068b6f1eb62804591d748c2
ROLLCOAST ransom note July 2020	0b6757090d9ebc8d497e71b177acf256	25b175a71906e354a24003803574c4420f02a82f	e25f2284fc6e80011587bf95829d8ff30

Posted in

- Threat Intelligence
- Security & Identity

Source: https://www.mandiant.com/resources/sabbath-ransomware-affiliate