

Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection

 sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

Aleksandar Milenkoski



By Aleksandar Milenkoski & Jim Walter

We observe a new trend on the ransomware scene – intermittent encryption, or partial encryption of victims’ files. This encryption method helps ransomware operators to evade detection systems and encrypt victims’ files faster. We observe that ransomware developers are increasingly adopting the feature and intensively advertising intermittent encryption to attract buyers or affiliates.

Intermittent encryption is important to ransomware operators from two perspectives:

- **Speed:** Encryption can be a time-intensive process and time is crucial to ransomware operators – the faster they encrypt the victims’ files, the less likely they are to be detected and stopped in the process. Intermittent encryption does irretrievable damage in a very short time frame.

- **Evasion:** Ransomware detection systems may use statistical analysis to detect ransomware operation. Such an analysis may evaluate the intensity of file IO operations or the similarity between a known version of a file, which has not been affected by ransomware, and a suspected modified, encrypted version of the file. In contrast to full encryption, intermittent encryption helps to evade such analyses by exhibiting a significantly lower intensity of file IO operations and much higher similarity between non-encrypted and encrypted versions of a given file.

In mid-2021, the LockFile ransomware was one of the first major ransomware families to use intermittent encryption for evading detection mechanisms, encrypting every other 16 bytes of a file. Since then an increasing number of ransomware operations have joined the trend.

In this post, we review several recent ransomware families that feature intermittent encryption in an attempt to evade detection and prevention: Qyick, Agenda, BlackCat (ALPHV), PLAY, and Black Basta.

Qyick Ransomware


At the end of August 2022, we observed a user named *lucrostm* advertising a new commercial ransomware called Qyick in a popular TOR-based crime forum. We track the same user as an established vendor of other malicious tools including remote access tools and malware loaders.

The Qyick ransomware offering is a one-time purchase, as opposed to the more common subscription model. The price ranges from .2 BTC to approximately 1.5 BTC, depending on the level of customization the buyer requires. The buyer receives a compiled executable with a guarantee: if the ransomware is detected by security software within 6 months of purchase, the author will provide a new sample with a discount between 60% and 80% of the original price.

Qyick is written in Go and features intermittent encryption. *lucrostm* claims the apparent speed of the Qyick ransomware is achieved through the use of intermittent encryption and the ransomware's implementation in Go, hinting at the current trend of intermittent encryption in the ransomware threat scene.

“Notably Qyick features intermittent encryption which is what the cool kids are using as you read this. Combined with the fact that is written in go, the speed is unmatched.”

Qyick ransomware ~ FUD ~ Private customization ~ 0 tax UPDATED 1.02

 **lucrostm**
Junior Member

Posts: 7
Joined: Mar 2022
Reputation: 3

08-30-2022, 09:46 PM #1

Wrote in Golang from scratch, it's "simple" yet very high quality, making it highly versatile and useful.

It uses many cutting-edge evasion techniques including proprietary methods.

Notably Qyick features intermittent encryption which is what the cool kids are using as you read this. Combined with the fact that is written in go, the speed is unmatched.

Each build is unique.
It is fully undetected and has been battle-tested, profiting millions in the right hands, 100x-ing the investment.

Feature list:

- intermittent encryption
- the encryption techniques used are implemented in the best way, making it impossible for analysts to create a universal decrypter.
- ETW patch (new)
- synchronized exuction (the ransomware starts at the same time thru the whole network, preventing the attack to be limited by the SOC turning off non-infected servers) (new)
- C2 address obfuscation and support for multiple addresses
- randomized start routine (timing, hops and math) to fool AVs sandbox
- custom syscalls (new)
- encrypted variables, resolved only when needed
- smart file encryption
- multi-threaded (soon coming via process injection)
- anti-forensics (coming soon)
- add pre-encryption script/shellcode (coming soon)

Note: the ransomware doesn't perform data exfiltration, as an attacker you'll have to do it yourself before the ransomware executes. The last feature mentioned will be implemented mainly for this purpose, so you can automatically exfiltrate before encryption. And in case your script/shellcode doesn't have evasion techniques itself the ransomware will cover that.

Get your game 1 step closer to the APT gods with Qyick ransomware.

PM me if you are interested. Note that if you wish to, we can work together to implement any additional features you want just like you want it.

PM Find Rep Reply Report

Qyick ransomware advertisement

The exact manner in which Qyick conducts intermittent encryption is open to investigation as samples become available.

The current version of Qyick does not have data exfiltration capabilities. However, *lucrostm* has announced that future versions will feature execution of arbitrary executable code, meant primarily for the execution of data exfiltration capabilities.

Agenda Ransomware

Agenda ransomware, first spotted in August 2022, is written in Go and has been used primarily to target healthcare and education organizations in Africa and Asia. The ransomware has some customization options, which include changing the filename extensions of encrypted files and the list of processes and services to terminate.

Agenda ransomware supports several encryption modes that the ransomware operator can configure through the encryption setting. The 'help' screen displays the different encryption modes available: `skip-step`, `percent`, and `fast`.

[...]

`-encryption value`

Flag allow you to redefine embed encryptor config to your custom.

Format Requirements:

generic format: `./binary.exe "mode ; param1:val1 ; param2:val2 ; ... ; paramN:valN"`.

generic format: `./binary.exe -encryption mode:param1:val2;param2:val2;...;paramN:valN`

'val' represents megabytes.

All 'val' must be integers.

If you want whitespaces inside flag - use double quotes (look at 1st generic format).

Allowed mode and params combinations:

Mode: 'skip-step'. Params 'step' and 'skip'

Mode: 'fast'. Params 'f'

Mode: 'percent'. Params 'n' and 'p' (p must between 1 and 99)

example:

```
./binary.exe -encryption "skip-step ; skip:10 ; step:20"
```

```
./binary.exe -encryption skip-step;skip:10;step:20
```

```
./binary.exe -encryption "percent ; n:10 ; p:30"
```

```
./binary.exe -encryption "fast;f:10"
```

[...]

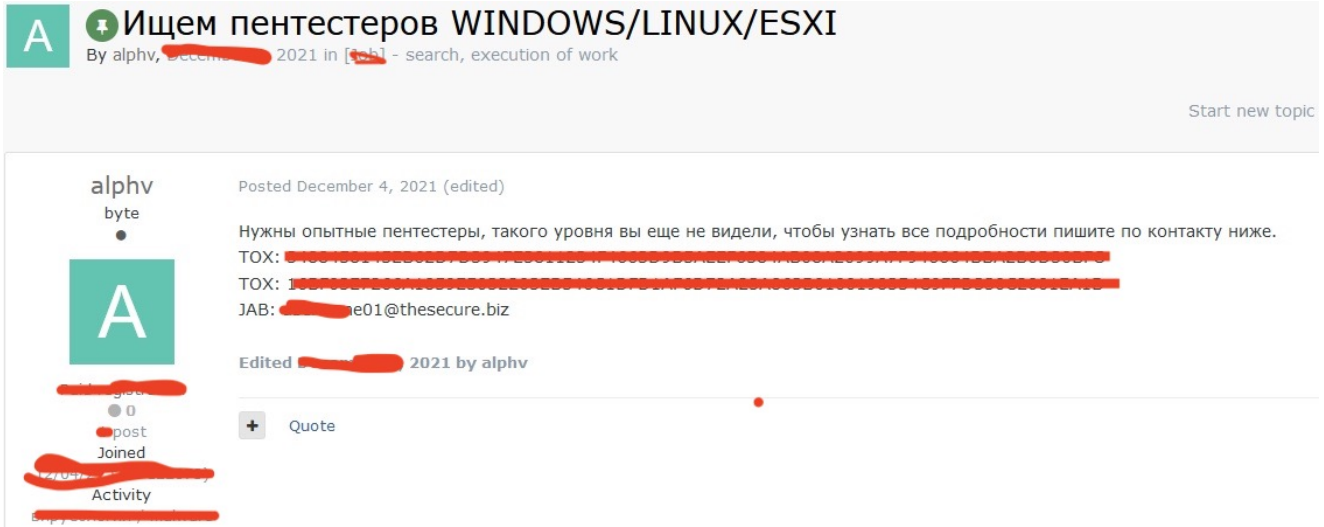
Agenda 'Help' screen, showing the available encryption modes

Our analysis of Agenda revealed the following information about each mode.

| Encryption mode | Description |
|------------------------------|--|
| skip-step [skip: N, step: Y] | Encrypt every Y MB of the file, skipping N MB. |
| fast [f: N] | Encrypt the first N MB of the file. |
| percent [n: N; p:P] | Encrypt every N MB of the file, skipping P MB, where P equals P% of the total file size. |

BlackCat (ALPHV), the First Rust Ransomware-As-A-Service

The BlackCat (or ALPHV) ransomware came to prominence in late 2021 and is the first known ransomware to be written in the Rust programming language. The developers behind BlackCat were first spotted advertising its services in early December 2021 on a Russian underground forum.



The original ALPHV/BlackCat forum post

The ALPHV threat group runs a ransomware-as-a-service (RaaS) program and shares ransom payments with affiliates. ALPHV uses bulletproof hosting to host their web sites and a Bitcoin mixer to anonymize transactions.

The ALPHV threat group is an early adopter of extortion schemes such as threatening victims with DDoS attacks, leaking exfiltrated data online as well as intimidating employees and customers of victim organizations should they not pay ransom. Major organizations and businesses have been the target of the BlackCat ransomware globally. For example, in September 2022, the BlackCat ransomware targeted Italy's state-owned energy services firm GSE.

ALPHV Collections

Data

data / al / Data

🔍 Wildcard (i.e.: *.txt, *.doc)

Name

Engineering

SQL

HR - Forms

Accounting

Human Resources

export

private

Group Sales

ALPHV Collections: A searchable database of exfiltrated victims' data
SentinelLabs researcher [Aleksandar Milenkoski](#) has reverse-engineered BlackCat ransomware samples and [outlined](#) the different encryption modes that BlackCat supports, the majority of which implement intermittent encryption. The table below lists these encryption modes.

| Encryption mode | Description |
|--------------------|---|
| Full | Encrypt all file content. |
| HeadOnly [N] | Encrypt the first N bytes of the file. |
| DotPattern [N,Y] | Encrypt every N bytes of the file with a step of Y bytes. |
| SmartPattern [N,P] | Encrypt the first N bytes of the file. BlackCat divides the rest of the file into equal-sized blocks, such that each block is 10% of the rest of the file in size. BlackCat encrypts P% of the bytes of each block. |

| | |
|------------------------------|--|
| AdvancedSmartPattern [N,P,B] | Encrypt the first N bytes of the file. BlackCat divides the rest of the file into B equal-sized blocks. BlackCat encrypts P% of the bytes of each block. |
| Auto | Combinatory file encryption mode. Encrypt the content of the file according to one of the file encryption modes <code>Full</code> , <code>DotPattern</code> [N,Y], and <code>AdvancedSmartPattern</code> [N,P,B]. BlackCat selects and parametrizes a file encryption mode based on the filename extension and the size of the file. |

An evaluation [study](#) subjecting files of varying sizes (50 MB, 500 MB, 5 GB, and 50 GB) to the BlackCat ransomware revealed that using intermittent encryption can be of significant benefit to threat actors. For example, in contrast to full encryption, encrypting files using the `Auto` file encryption mode resulted in noticeably reduced wallclock processing time starting at 5 GB file size (8.65 seconds) and a maximum reduction in wallclock processing time of 1.95 minutes at 50 GB file size. Wallclock processing time is the total wallclock time (in seconds) that the ransomware spends on processing a file, which includes reading, encrypting, and writing file content. The full results of this study will be presented at the [VirusBulletin Conference 2022](#).

We also note that BlackCat includes some internal logic for maximizing encryption speed. The ransomware encrypts files using the Advanced Encryption Standard (AES) encryption algorithm if the victim's platform implements AES hardware acceleration. If not, the ransomware falls back to the ChaCha20 algorithm that is fully implemented in software.

PLAY Ransomware

PLAY ransomware is a new entrant in the ransomware scene and was [first spotted](#) at the end of June 2022. The ransomware has recently victimized high profile targets, such as the [Court of Córdoba](#) in Argentina in August 2022. PLAY's ransom note consists of a single word – PLAY – and a contact email address.

PLAY

@gmx.com

A PLAY ransomware ransom note

In contrast to Agenda and BlackCat, PLAY ransomware does not feature encryption modes that can be configured by the operator. PLAY orchestrates intermittent encryption based on the size of the file under encryption, encrypting chunks (file portions) of **0x100000** bytes. For example, [previous research](#) states that under certain conditions, the PLAY ransomware encrypts:

- 2 chunks, if the file size is less than or equal to 0x3fffffff bytes;
- 3 chunks, if the file size is less than or equal to 0x27fffffff bytes;
- 5 chunks, if the file size is greater than 0x280000000 bytes.

In our analysis, we observed that a sample encrypted every other **0x100000** byte chunk until the end of the file. The file consisted only of null characters, which effectively makes the encrypted and non-encrypted chunks visually distinguishable.

```

000FFFA0 E3 CB 44 C9 AA 3F 84 3E B8 B7 01 89 CC 37 3A B8 äĒĒÉ?„> , .%İ7:,
000FFFB0 30 55 FA 04 3B 63 F1 E6 C0 95 A5 75 64 CF 80 60 0Uú.;cñæÄ•¥udİĒ`
000FFFC0 12 C4 87 41 55 F5 9F 48 23 52 18 5C A6 F8 C1 E7 .Ä+AUöYH#R.\!øÁç
000FFFD0 36 EB DD ED 20 FF AE 55 F2 81 70 E5 C5 3D BA F3 6ëYi y@Uò.páÄ=°ó
000FFFE0 A2 CB 00 2C DD 0F 89 47 24 69 16 5D A7 71 BF 32 cĒ.,Ý.%G§i.]$qç2
000FFFF0 EA 27 75 00 34 59 57 67 F1 FD 04 76 2C 90 8E 0D è'u.4YWgñý.v,.Ž.
00100000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00100010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00100020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00100030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00100040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00100050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

[...]

```

001FFFA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001FFFB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001FFFC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001FFFD0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001FFFE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001FFFF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00200000 7C 96 01 FB BF 5F 63 C6 83 54 EA BD 37 3C BE A3 |-.ûç_cĒfTĒs7<¾Ē
00200010 F1 3A 89 5D A2 E8 C4 C8 E9 99 FA AD FE FD 36 95 ř:;%çĒĒĒĒú.pý6•
00200020 73 62 5E 14 31 90 1E B4 50 53 BB D1 C9 0C 63 D9 sb^.1...`PS»ŃĒ.cŪ
00200030 4A 46 37 DC B5 68 08 A9 05 5F F8 62 B3 69 A2 88 JF7Ūuh.©._øb'iç^
00200040 6D 76 05 37 08 41 AA A0 B0 6F 96 71 27 7D A2 DD mv.7.A* °o-q'}çÝ
00200050 8F F8 00 EB 49 A7 E5 88 53 FF 95 F3 50 AC 73 3C .ø.ĒİŠĒ^Sý•óP-s<

```

[...]

```

002FFFA0 18 C4 41 0A 23 60 1A 92 AD 5B 05 3E 50 52 64 B4 .ĒĒ.#`.'.[.>PRd`
002FFFB0 A3 3B EF 54 B4 9B C8 1B A4 C8 50 6A 13 22 A6 3A Ē;iT`>Ē.ĒĒPj."!;
002FFFC0 96 E4 47 7D 66 86 86 7E 9E 26 E5 9A 3A AF 6E 2B -ăG)ftt~ž&ăš:~n+
002FFFD0 29 7D 86 F6 99 2E 22 8C 6D 78 81 B1 9B 62 B2 3F )}tö™."Ēmx.±>b²?
002FFFE0 91 CA 92 C8 59 9F 82 82 E3 C9 40 4A 27 DC 93 F2 `Ē'ĒYŸ,,ăĒ@J'Ū"ò
002FFFF0 3B DE DD B7 4F C0 D4 77 CB 62 0C E6 57 8B FA 09 ;Bý·OÀŌwĒb.æW<ú.
00300000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00300010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00300020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00300030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00300040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00300050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

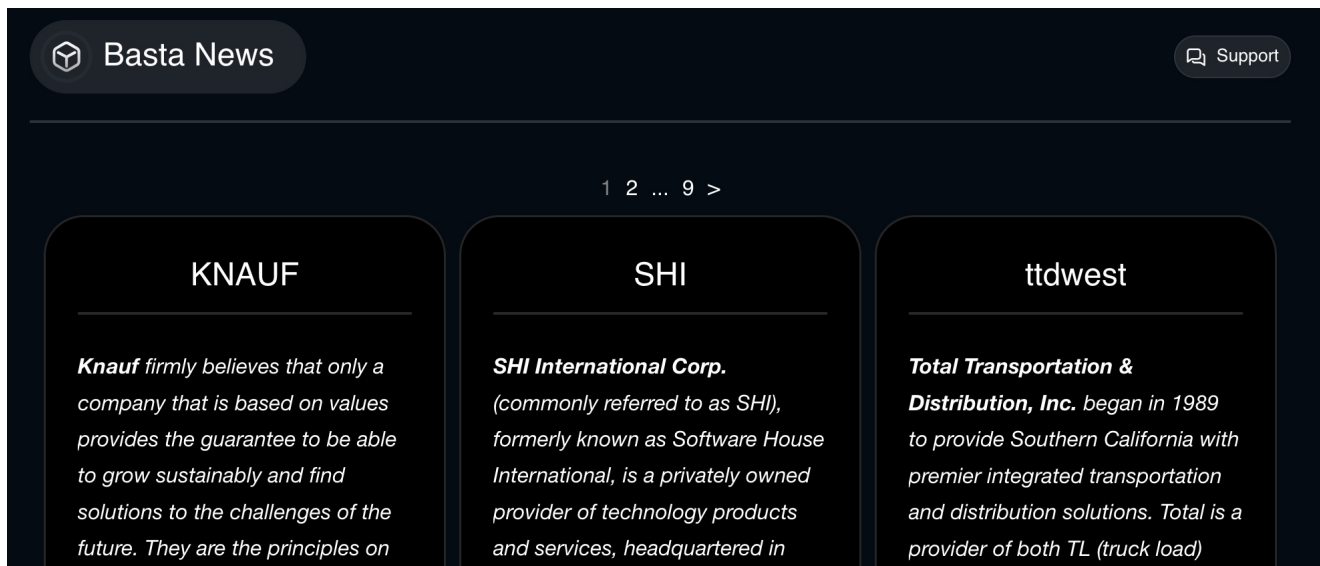
Partial content of a file encrypted by PLAY

Black Basta Ransomware

Black Basta is a RaaS program that emerged in April 2022 with ransomware samples dating back to February 2022. Current intelligence indicates that Black Basta emerged from the crumbled ashes of the Conti operation. The ransomware is written in the C++ programming

language and supports Windows and Linux operating systems. Black Basta operators use the double extortion scheme threatening victim organizations with leaking exfiltrated data on the threat group's TOR-based web site Basta News should the victims not pay ransom.

Black Basta is rapidly gaining ground on the ransomware scene and targets major organizations globally – the ransomware operation reported more than 20 victim organizations on Basta News within the first two weeks of its existence. Targeting, especially early on, was primarily focused on utilities, technology, financial, and manufacturing industries. For example, the major German building materials manufacturer [Knauf](#) suffered an attack conducted by Black Basta affiliates at the end of June 2022.



The Basta News web site

Like PLAY ransomware, Black Basta does not feature encryption modes that can be configured by the ransomware operator, but orchestrates intermittent encryption based on the size of the file under encryption. Black Basta encrypts:

- all file content, if the file size is less than 704 bytes;
- every 64 bytes, starting from the beginning of the file, skipping 192 bytes, if the file size is less than 4 KB;
- every 64 bytes, starting from the beginning of the file, skipping 128 bytes, if the file size is greater than 4 KB.

Our analysis showed that for a file with a size greater than 4 KB, the Black Basta ransomware encrypted 64 byte portions with an interval of 128 bytes between each, until the end of the file. In similar fashion to PLAY ransomware, the file consisted only of null characters, making the encrypted and non-encrypted chunks visually distinguishable.

```

00000000 2E AF B1 E1 1C AA 2E 9A 24 37 E4 2F E8 DA 2C 48 .-±á.*.šš7ä/èÚ,H
00000010 D9 D5 AE 66 03 BB 05 80 89 C5 4F 13 B2 FC BD 70 ÛÕ@f.».€%ÅO.°üþp
00000020 E2 ED 41 C2 63 22 70 CE 9A 2F F7 EE F8 E9 7E AC áíAÂc"pîš/÷îøé~¬
00000030 70 A8 B4 72 4D 7A 8A A4 0F B7 3A 4C 73 36 0E 81 p``rMzŠš. .:Ls6..
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000C0 D0 45 4E EA ED C9 91 52 78 7C A7 8E 33 40 27 6D ĐENéíÉ`Rx|šŽ3@'m
000000D0 DF AE 35 3B 90 5D 3B 76 EB 87 83 42 61 13 F9 8D Š@5;.];vëþfBa.ù.
000000E0 13 57 DA F0 03 65 35 4C AD 8D DA 6F E0 6F B4 BA .WÚš.e5L..Úoào`°
000000F0 5A 25 FC 07 F9 D5 DE 0D 88 7A E4 EE 2A DF 39 56 Zšü.ùÕš.ˆzāi*š9V
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000180 84 FD D1 8C AA E6 A5 E3 DF 8F 1E 4B A6 A3 04 6D „ýŇŇ€*æŷãš..K|š.m
00000190 DE D1 37 F2 92 C5 27 05 AC 1B 1E 9C 66 04 DB 67 ÞŇ7ò'Á'.¬..œf.Ūg
000001A0 D0 6E 7E C4 DE BB 91 A5 7D 0F 14 2B 3F 6F 7E 4C Đn~ÄÞ»'ŷ}...+?o~L
000001B0 CC 80 DD 3C C1 71 F5 AD 6A 93 C5 F1 01 BA 3F 2B İ€Ý<Áqõ.j"Ăñ.°?+
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Partial content of a file encrypted by Black Basta

Conclusion

Intermittent encryption is a very useful tool to ransomware operators. This encryption method helps to evade some ransomware detection mechanisms and encrypt victims' files faster. Given the significant benefits to threat actors while also being practical to implement, we estimate that intermittent encryption will continue to be adopted by more ransomware families.

SentinelOne Singularity fully detects these ransomware samples.

Ransomware Samples

| Family | SHA1 |
|----------|--|
| Agenda | 5f99214d68883e91f586e85d8db96deda5ca54af |
| BlackCat | 8917af3878fa49fe4ec930230b881ff0ae8d19c9 |
| PLAY | 14177730443c70aefeeda3162b324fdedf9cf9e0 |

Black Basta a996ccd0d58125bf299e89f4c03ff37afdab33fc