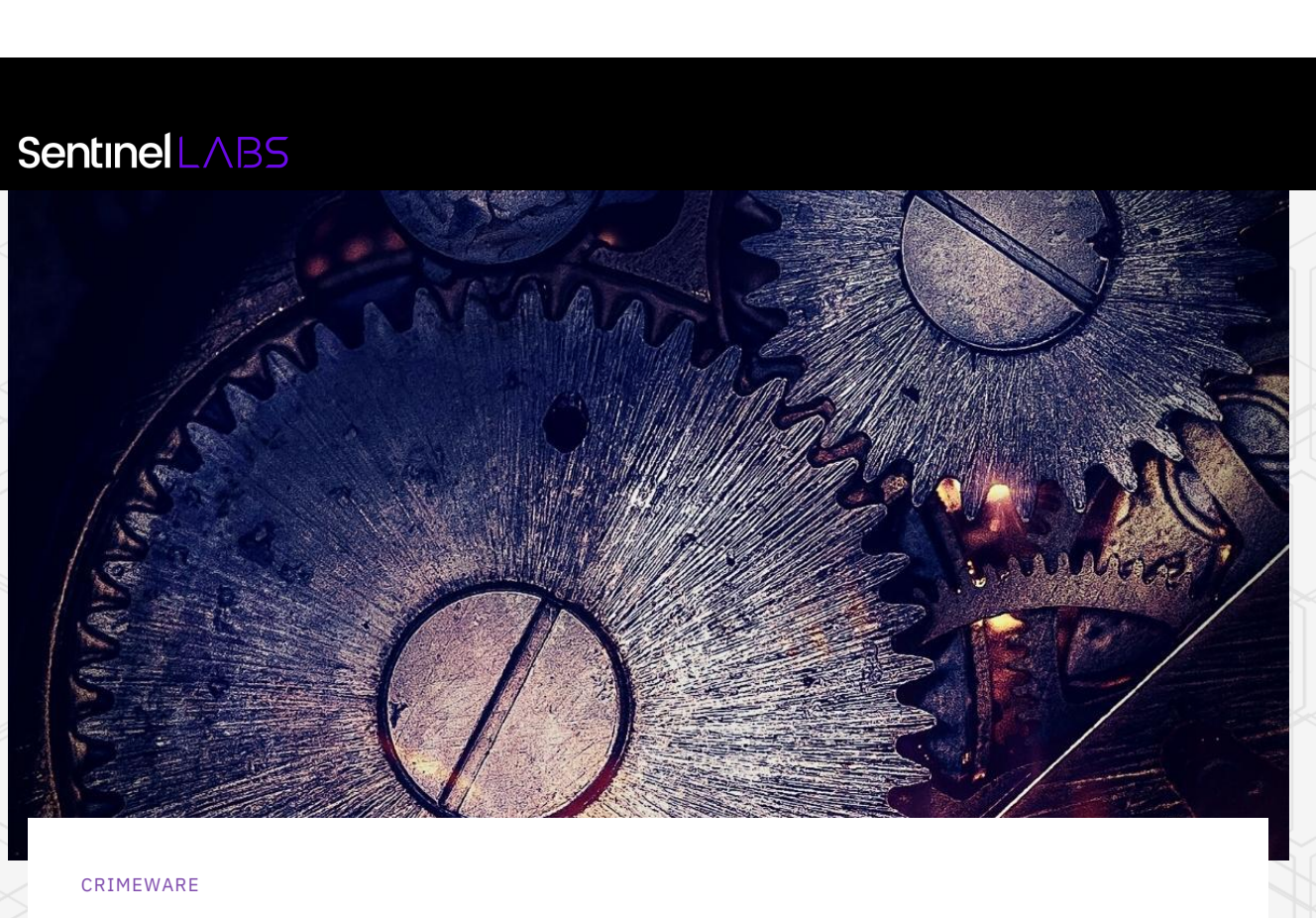


CRIMEWARE

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

ALEKSANDAR MILENKOSKI / SEPTEMBER 8, 2022

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.

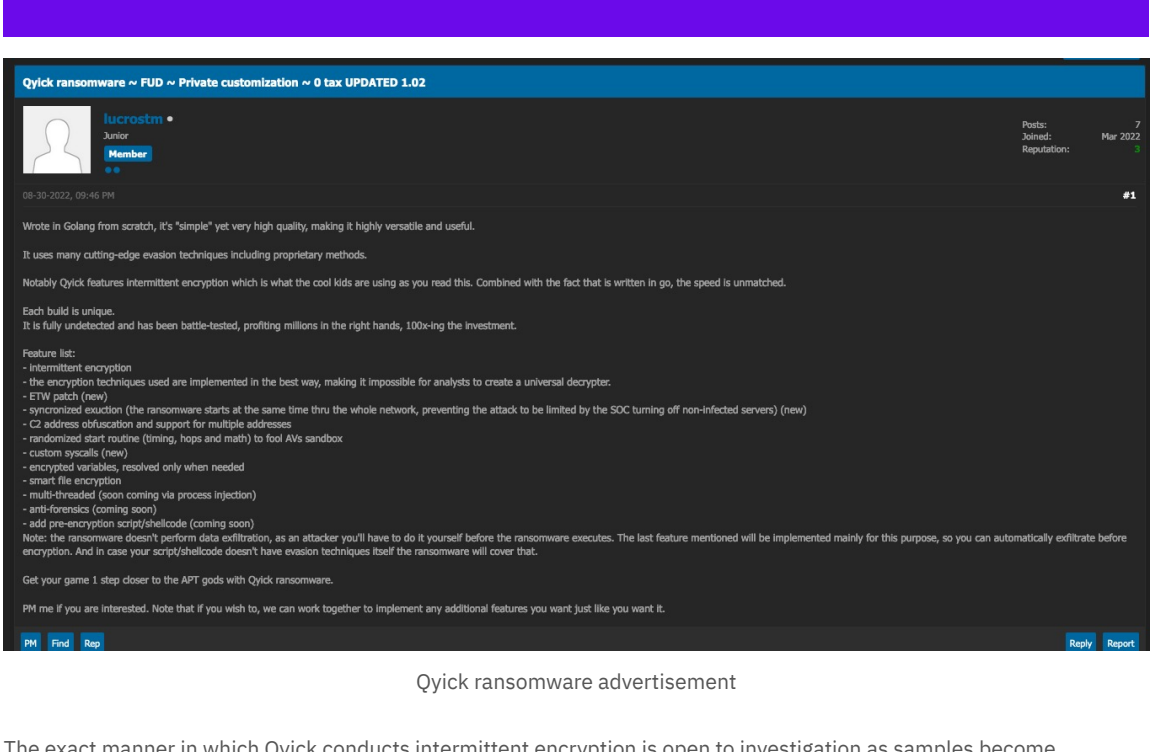
Qyick Ransomware

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 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"
[...]
```

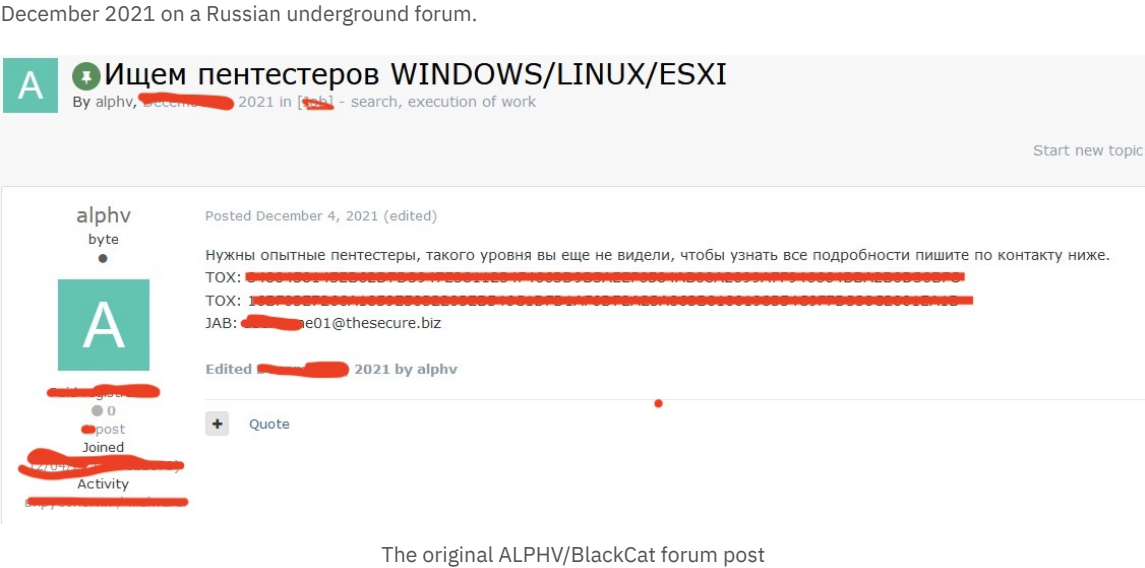
Agenda 'Help' screen, showing the available encryption modes

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

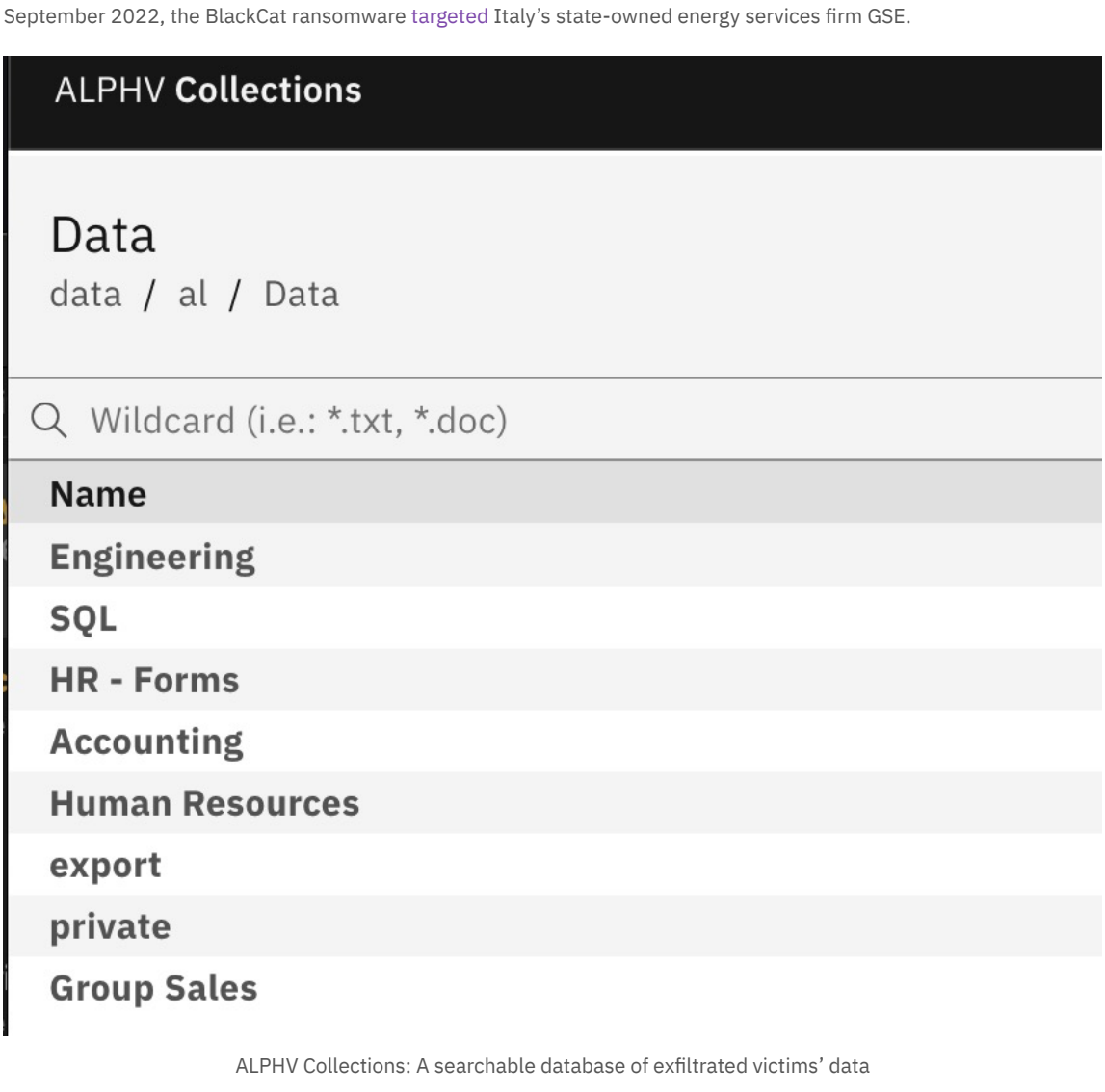
The BlackCat (or ALPHV) ransomware came to prominence in late 2021 and is the first known ransomware to be written in the Rust programming language. The developers behind BlackCat were first spotted advertising its services in early December 2021 on a Russian underground forum.



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: 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 `Full`, `DotPattern` [N,Y], and `AdvancedSmartPattern` [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.

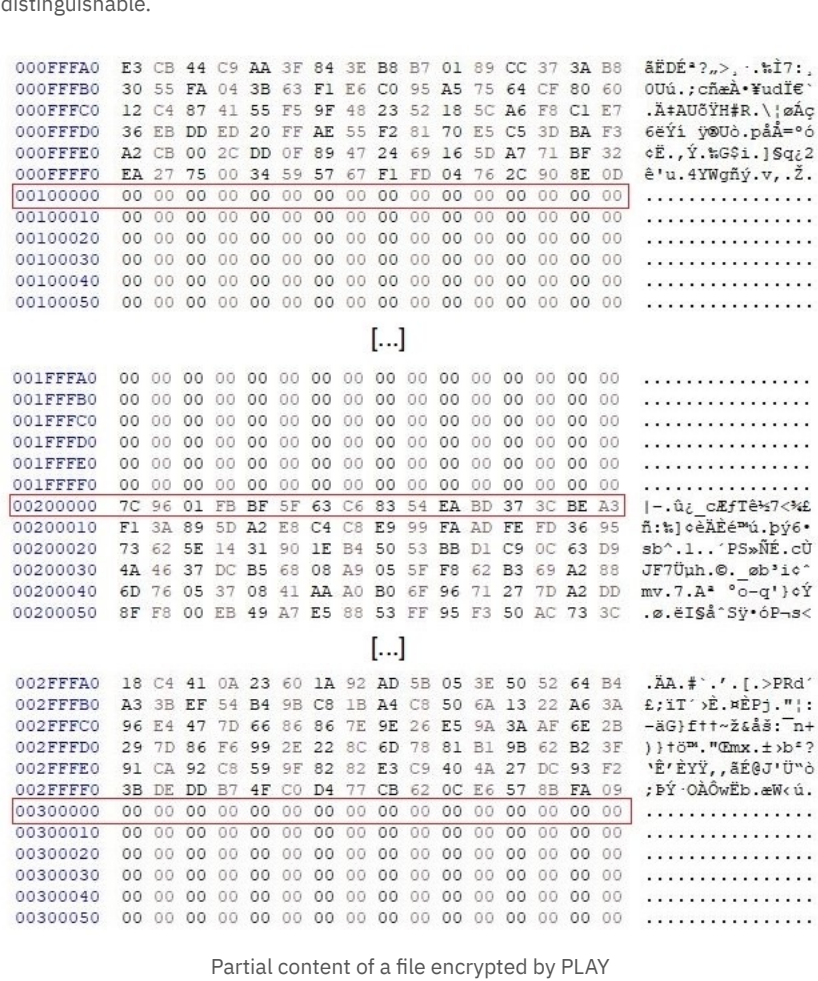
```
PLAY
[illegible]@gmx.com
```

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.

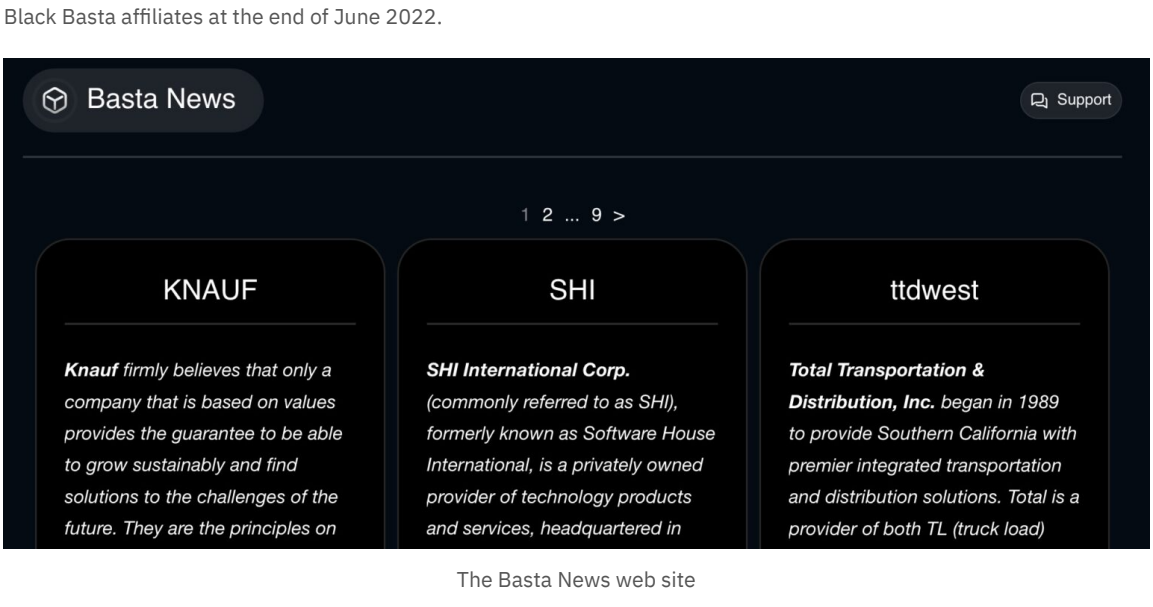


Partial content of a file encrypted by PLAY

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.

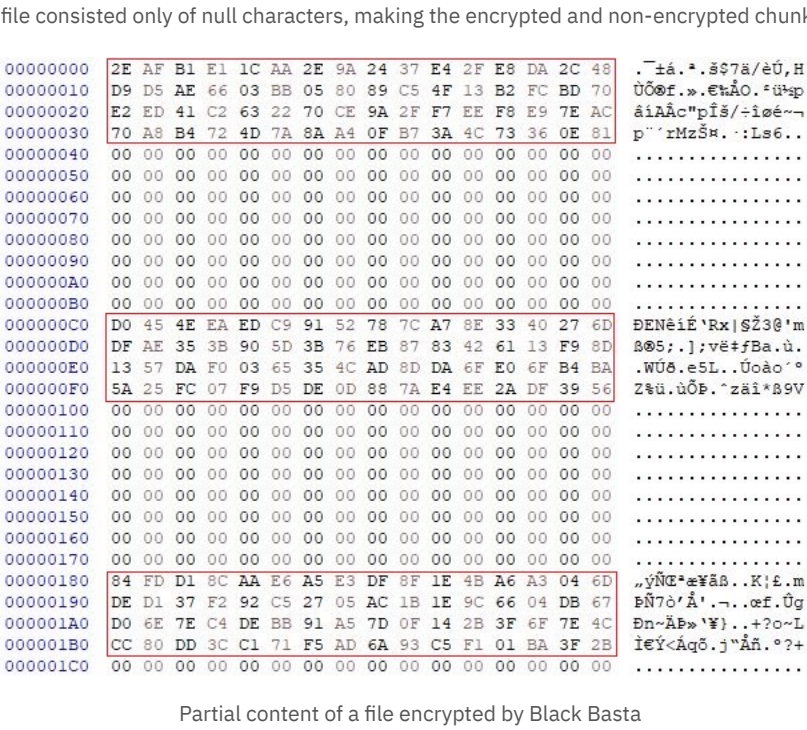


The Basta News web site

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.



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

ENCRYPTION RAAS RANSOMWARE

ALEKSANDAR MILENKOSKI

Aleksandar Milenkoski is a Senior Threat Researcher at SentinelLabs, with expertise in reverse engineering, malware research, and threat actor analysis. Aleksandar has a PhD in system security and is the author of numerous research papers, book chapters, blog posts, and conference talks. His research has won awards from SPEC, the Bavarian Foundation for Science, and the University of Würzburg.