

LOCKBIT 3.0



Le rançongiciel Lockbit, connu sous le nom de rançongiciel ABCD à ses débuts, est apparu en septembre 2019. Considéré comme un Raas (Ransomware As A Service), les opérateurs ne cessent de le faire évoluer.

Une deuxième version de Lockbit est apparue en juin 2021 et est devenue très active en ciblant de grandes entreprises et en lançant une grande campagne de recrutement pour de nouveaux affiliés.

Il agit principalement en Amérique du nord et cible plutôt les entreprises financières.

Cette deuxième version du rançongiciel inclut principalement :

- la suppression des shadows copies,
- le bypass du compte utilisateur (UAC),

- le support des version ESXI,
- l'impression des notes de rançons directement sur les imprimantes réseaux détectées.

Depuis mars 2022, le groupe signe son retour avec la version de Lockbit nommée 3.0. Incluant dorénavant le paiement par Zcash ainsi qu'un programme de Bug Bounty et une intimidation plus agressive pour le paiement des rançons, cette nouvelle version fait la une des actualités cyber ces dernières semaines.

A l'heure où la liste des victimes augmentent, nous avons pu nous procurer certaines souches de ce malware afin de les soumettre à notre outil d'analyse GLIMPS Malware. **Il a très rapidement fait apparaitre des fonctions similaires à BlackMatter et Darkside.**

The screenshot displays the Lockbit 3.0 ransomware website interface. At the top, there is a navigation bar with the Lockbit 3.0 logo, a 'LEAKED DATA' banner, and links for 'TWITTER', 'PRESS ABOUT US', 'HOW TO BUY BITCOIN', 'AFFILIATE RULES', 'CONTACT US', and 'MIRRORS'. Below the navigation bar, a grid of 16 cards lists various companies that have been targeted. Each card includes the company name, a ransom note (e.g., '3D 22h 15m 32s'), a ransom amount (e.g., '\$ 1000000'), a brief description of the company, and the date and time the data was updated. The companies listed include lapostemobile.fr, carnbreia.com.au, cabbageinc.com, alpachem.com, axelcium.com, slpcolombus.com, pravocats.fr, lesbureauxdelepargne.com, faacgroup.com, bosco-avocats.com, sigma-alimentos.com, diodes.com, lonseal.com, and metroappliancesandmore.com.

[Analyse Blackmatter]

Ce fichier est identifié par GLIMPS Malware comme exécutable PE32 à destination des machines Windows.

Il comporte 2 sections .data et .ndata qui présentent une forte entropie, signe que le binaire est *packé*.

La technologie DeepEngine intégrée dans notre produit GLIMPS Malware nous indique que ce binaire embarque des fonctions similaires à d'autres souches malveillantes, notamment à une dizaine de variants Blackmatter qui sont eux aussi corrélés au cours de l'analyse Lockbit 3.

The screenshot displays the GLIMPS Malware analysis interface. At the top, navigation tabs include File details, Generated tags (15), GLIMPS Correlate (1), Signatures (3), Perm (2), PEFile (14), File viewer, and Other services. The main section shows a correlation result for 'blackmatter.1' with a threat level of 'Extreme' and 211 function closest samples.

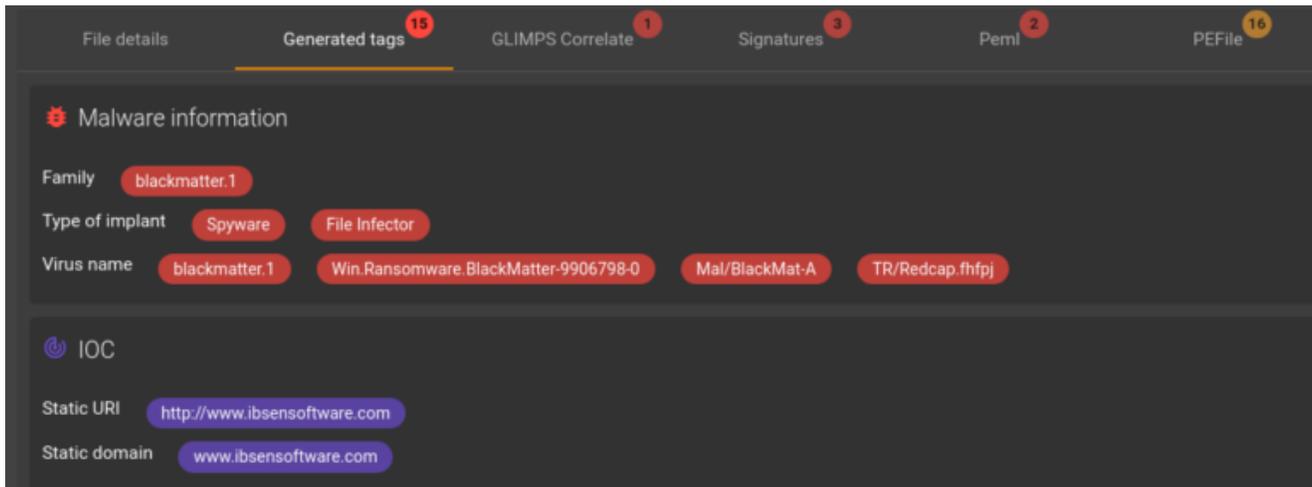
Sample correlated: A list of 10 sample hashes is shown, including '9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58'.

Functions distribution: A pie chart shows the distribution of functions. The legend indicates: No match (grey), Generic code (light grey), Legit (orange), and Malicious (red). A status bar below the chart states '76 malicious functions found'.

Address space distribution: A horizontal bar chart shows the distribution of address space. The legend indicates: No match (blue), Full matches (red), and other colors representing intermediate levels of correlation.

The bottom section shows file details for two sections:

- .data:** Virtual: 0x00015000 (0x00003DFC bytes) - Physical: 0x00012E00 (0x00003600 bytes) - hash: 858a77d63e7e47c3d8e1ccd980804d77 - entropy: 7.962000. A 'High section entropy' tag is present.
- .rsrc:** Virtual: 0x00019000 (0x00000DCA bytes) - Physical: 0x00016400 (0x00000E00 bytes) - hash: d6d3bfb83cd7598e4f7976cb5f557d - entropy: 7.929000. A 'High section entropy' tag is present.

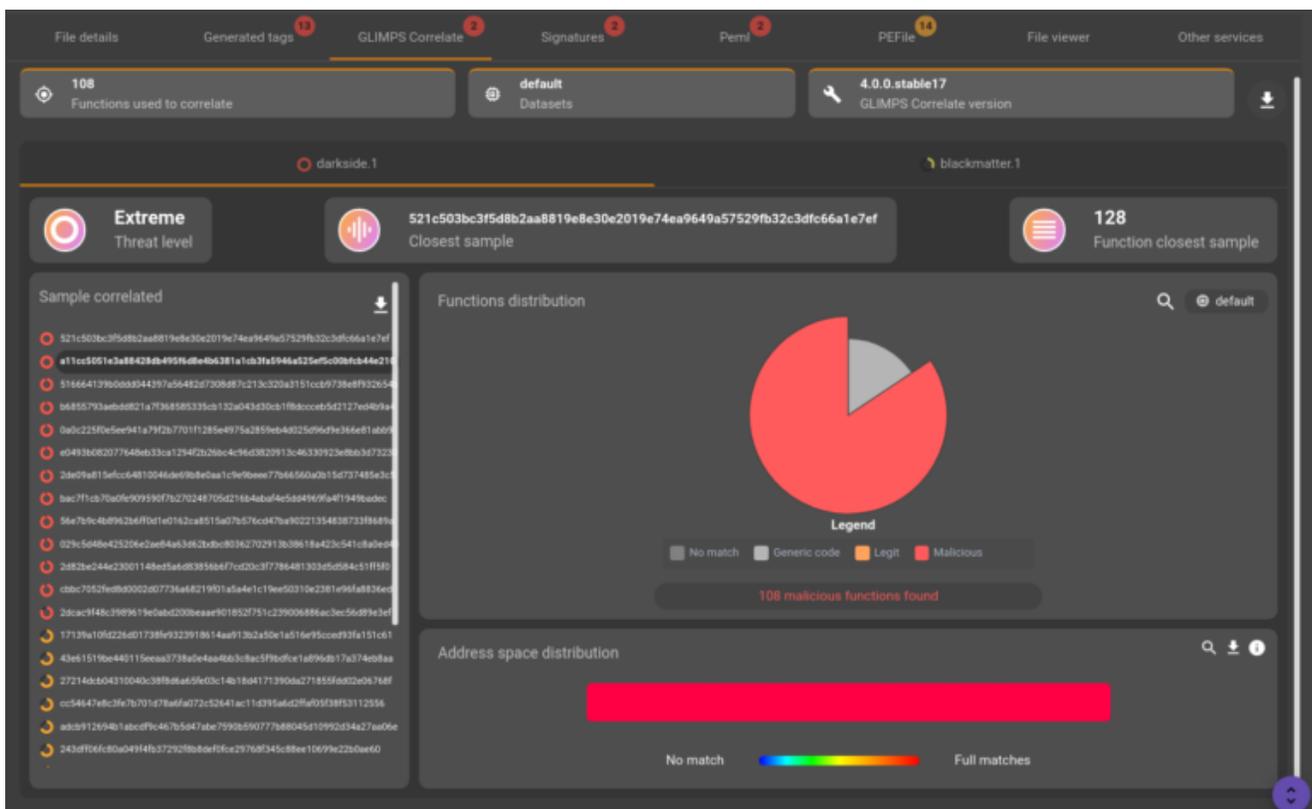


[analyse Darkside]

Une souche d'un malware Darkside a été soumise à GLIMPS Malware. Il est rapidement identifié comme un exécutable au format PE32 à destination de machines Windows.

Il comporte 2 sections .data et .ndata qui présentent une forte entropie, signe que le binaire est *packé*.

La technologie DeepEngine de détection GLIMPS nous indique que ce binaire emporte des fonctions similaires avec d'autres souches malveillantes, notamment une dizaine de variants Blackmatter ainsi que de fortes similarités avec d'autres variants Darkside.



The screenshot displays a software interface for malware analysis. At the top, a navigation bar includes tabs for 'File details', 'Generated tags' (with a red notification bubble '12'), 'GLIMPS Correlate' (with a red notification bubble '2'), 'Signatures' (with a red notification bubble '2'), 'Peml' (with a red notification bubble '2'), 'PEFile' (with a yellow notification bubble '14'), 'File viewer', and 'Other services'. Below this, a 'High section entropy' alert (with a yellow notification bubble '12') and a 'Service version: 4.0.0 stable12' are visible.

The main content area shows two sections:

- .data**: Virtual: 0x0000C000 (0x00003998 bytes) - Physical: 0x00009800 (0x00003000 bytes) - hash: d89a83e336a7b5e94fb29717a66a819a - entropy: 7.717000. A horizontal bar chart below this section shows a high level of entropy, with a 'High section entropy' label at the bottom.
- .ndata**: Virtual: 0x00010000 (0x00000E3A bytes) - Physical: 0x0000C800 (0x00001000 bytes) - hash: 4c4b57bb41c27062dd337b3fb31e3bbd - entropy: 7.544000. A similar horizontal bar chart and 'High section entropy' label are present.

At the bottom, another navigation bar includes 'File details', 'Generated tags' (with a red notification bubble '13'), 'GLIMPS Correlate' (with a red notification bubble '2'), 'Signatures' (with a red notification bubble '2'), 'Peml' (with a red notification bubble '2'), and 'PEFile' (with a yellow notification bubble '14').

The 'Malware information' section is expanded, showing the following details:

- Family: **darkside.1**
- Type of implant: **Spyware**, **Packed**, **Downloader**
- Virus name: **darkside.1**, **Win.Packed.DarkSide-9262656-0**, **TR/Crypt.XPACK.Gen**

[analyse Lockbit 3.0]

Le fichier soumis est un exécutable au format PE32 à destination de machines Windows.

L'analyse de leur sections .data et .pdata indique une forte entropie, ce qui signifie que l'exécutable est *packé*.

La technologie DeepEngine intégrée dans notre produit GLIMPS Malware nous indique que ce binaire embarque des fonctions similaires à d'autres souches malveillantes, notamment 11 exemplaires *Blackmatter* ainsi que 13 exemplaires *Darkside*.

File details | Generated tags ¹¹ | GLIMPS Correlate ² | Signatures ² | Pemi ² | PEFile ¹⁴ | File viewer | Other services



Malicious

Family: **blackmatter.1**
Virus name: **blackmatter.1 Mal/FakeAV-JC TR/Crypt.XPACK.Gen**
Type: **executable/windows/pe32**

4,200
Score

File information Add to whitelist | Download

Heuristics

Malicious

- Malicious file strong signature

Suspicious

- High section entropy
- PEML (LGBM)
- peml_nn_strong

Info

- Extracted from executable
- shortcut malware

MITRE ATT&CK®



File details | Generated tags ¹¹ | GLIMPS Correlate ² | Signatures ² | Pemi ² | PEFile ¹⁴ | File viewer | Other services

🔍

207

Functions used to correlate

📄

default

Datasets

🔧

4.0.0.stable17

GLIMPS Correlate version

blackmatter.1 darkside.1

🔥

Extreme

Threat level

🔊

9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58

Closest sample

☰

211

Function closest sample

Sample correlated

- 9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58
- 730f96240355c786d737bae6662679620c64f5713299ab40106e7625c3d0e4
- 2aa9f5bd4c79bd21c02189f2552d5c9fb216293a251539ea59d4556a01437c
- 8eada5114fbcc73b79648b38423c206367c94de76cb3b395a33ea8859d2952
- 320bd9ed08c648810971bd051184c4a298196742000018d4027bc38fc42e57
- 5d4b42e1b36be04661d278ea523760db09a4f30b7e32b144812ce50c483fa
- 6d4712df42a0982041ef9e2e109ab5718a43830f2966bd9207a7ac3af883db
- b824b0c645f15e213b4c2628f7c083e9e37282059b0396e607d84ea1fed1f
- 22d7967c3bf10b1a37f277ebab261eb4025af0e643794377409e148bcc08d5
- 4e74b473355844ee27e4c568bec821c8e20cc95c96f124999eddbbb932a43e
- 70344eece2a828c46f319b3328125d9ab596902b0eaa24246ee97142eedad9

Functions distribution



101 malicious functions found

Address space distribution



No match █ Full matches

6/8

The screenshot displays the GLIMPS Malware analysis interface. At the top, there are navigation tabs: File details, Generated tags (11), GLIMPS Correlate (2), Signatures (2), Pefile (2), PEFile (15), File viewer, and Other services. Below the tabs, there are two sections for file details:

- .data** - Virtual: 0x0001D000 (0x0000B000 bytes) - Physical: 0x0001AA00 (0x0000A000 bytes) - hash: ad451f79ecc1306c6969af4094c3b6b9 - entropy: 7.986000. A bar chart shows high section entropy.
- .pdata** - Virtual: 0x00028000 (0x00004000 bytes) - Physical: 0x00024A00 (0x00003E00 bytes) - hash: 8dbdc0b2e8a4a892cedac675d0eae9a5 - entropy: 7.976000. A bar chart shows high section entropy.

At the bottom, the **Malware information** section is visible, showing:

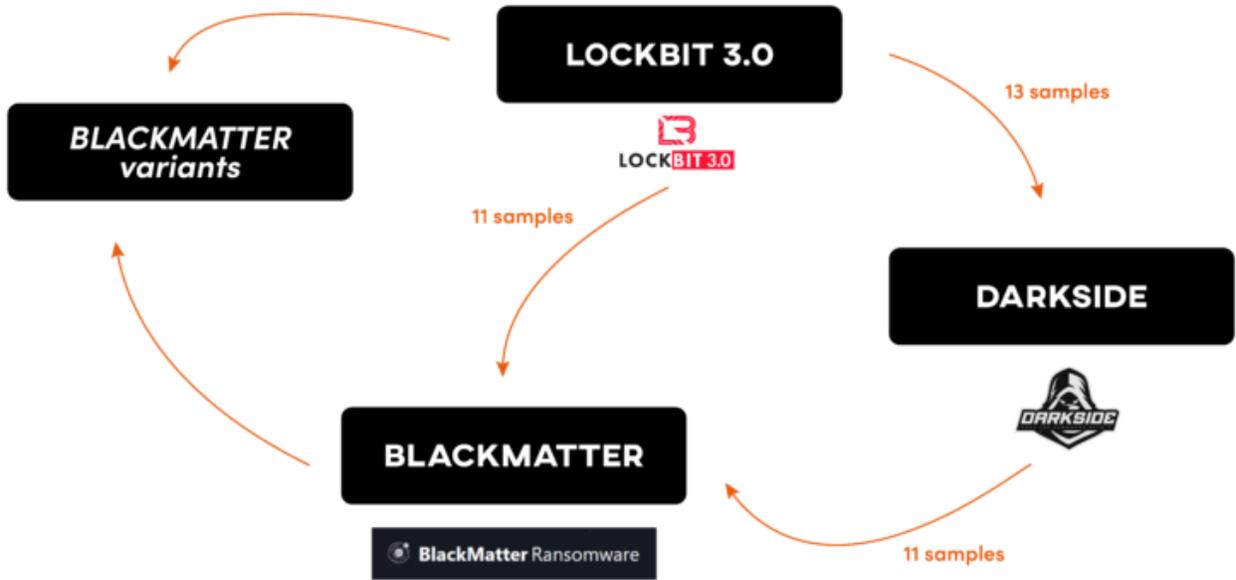
- Family: **blackmatter.1**
- Type of implant: **Packed**, **Downloader**
- Virus name: **blackmatter.1**, **Mal/FakeAV-JC**, **TR/Crypt.XPACK.Gen**

L'apport GLIMPS Malware

En mai 2021, suite à une offensive des forces de l'ordre, les opérateurs du rançongiciel DarkSide décident d'arrêter leur activité. En juillet 2021 apparaît alors le rançongiciel BlackMatter dont une partie du code est similaire à celui de DarkSide, laissant supposer qu'il s'agit soit des mêmes acteurs, soit d'une partie d'entre eux ou alors d'une diffusion du code source. Le 1er Novembre 2021 c'est au tour des opérateurs de BlackMatter de poster un message indiquant l'arrêt de leur activité. Le fait que Lockbit ait des fonctions similaires à DarkSide ainsi que BlackMatter pourrait indiquer, que le code source du rançongiciel DarkSide s'est retrouvé entre plusieurs mains.

Ainsi, les trois analyses qui ont été très rapidement effectuées par GLIMPS Malware nous indiquent que, non seulement, LockBit 3.0 est bien malveillant, mais aussi qu'il présente des concepts codes qui se rapprochent fortement de ceux de BlackMatter ainsi que de Darkside.

L'analyse technique permet de confirmer les informations du volet CTI.



→ corréle avec X samples

Sources :