Lockbit 3.0 | GLIMPS

Published: 2022-07-11 · Archived: 2026-04-05 19:10:45 UTC

Temps de lecture : 6 min

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,

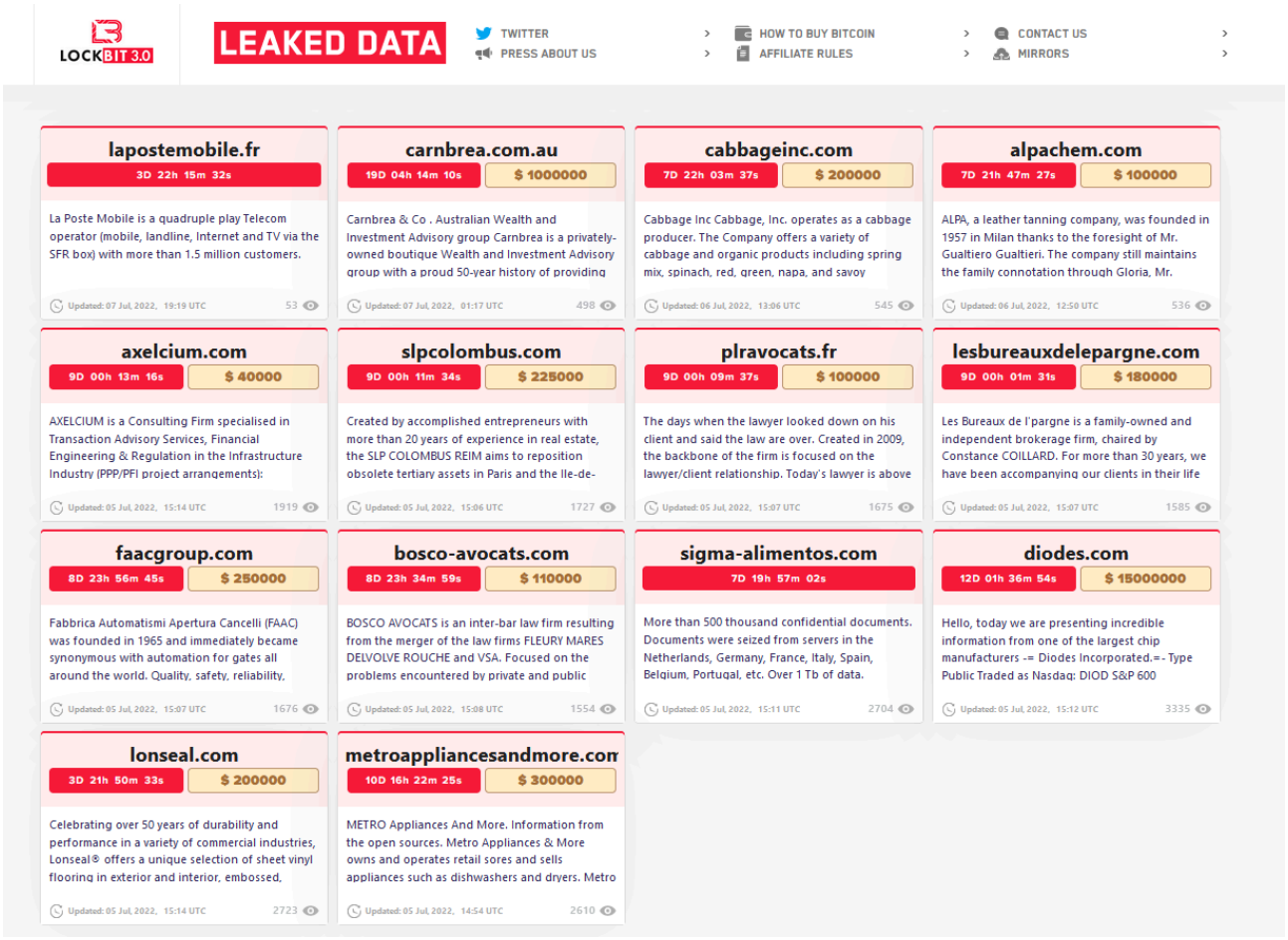
• le bypass du compte utilisateur (UAC),

• 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.**



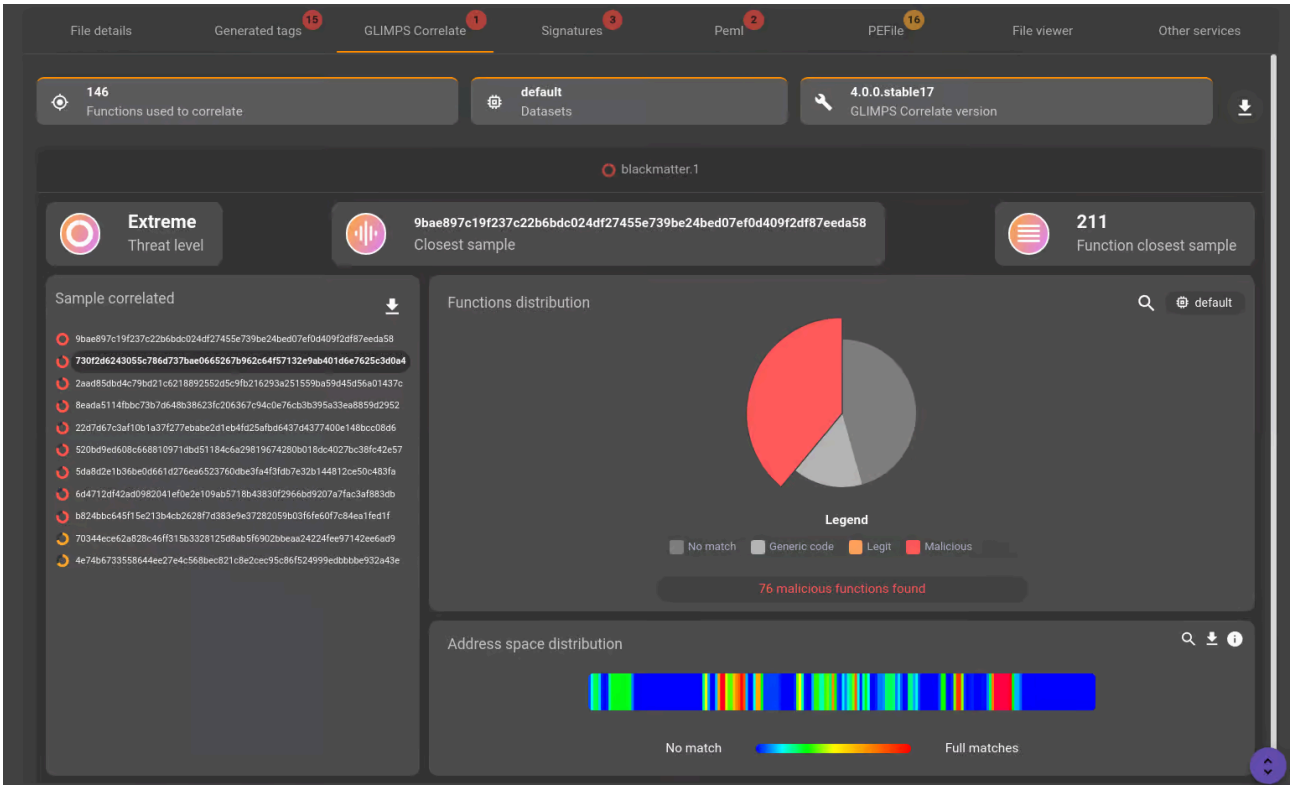
Consulter la fiche d'identité CTI LockBit

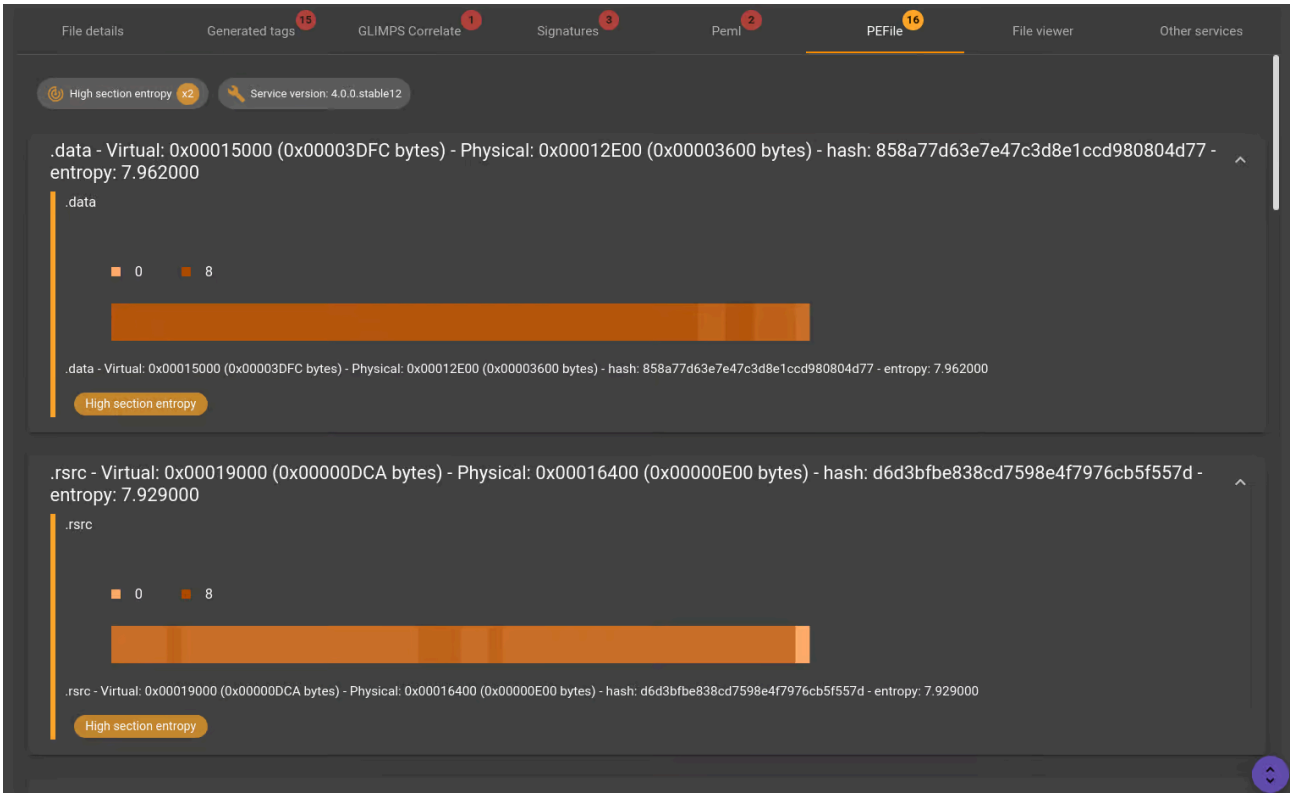
Analyse Blackmatter

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.


File details
Generated tags 15
GLIMPS Correlate 1
Signatures 3
Peml 2
PEFile 16
File viewer
Other services
146
Functions used to correlate
default
Datasets
4.0.0.stable17
GLIMPS Correlate version
blackmatter.1
Extreme
Threat level
9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58
Closest sample
211
Function closest sample
Sample correlated
9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58
730f2d6243055c786d737bae0665267b962c64f57132e9ab401d6e7625c3d0a4
2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c
8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952
22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6
520bd9ed608c668810971dbd51184c6a29819674280b018dc4027bc38fc42e57
5da8d2e1b36be0d661d276ea6523760dbe3fa4f3fdb7e32b144812ce50c483fa
6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db
b824bbc645f15e213b4cb2628f7d383e9e37282059b03f6fe60f7c84ea1fed1f
70344ece62a828c46ff315b33281258d8ab5f6902bbeaa24224fee97142ee6ad9
4e74b6733558644ee27e4c568bec821c8e2cec95c86f524999edbbbbe932a43e
Functions distribution
default
Legend
No match
Generic code
Legit
Malicious
76 malicious functions found
Address space distribution
No match
Full matches

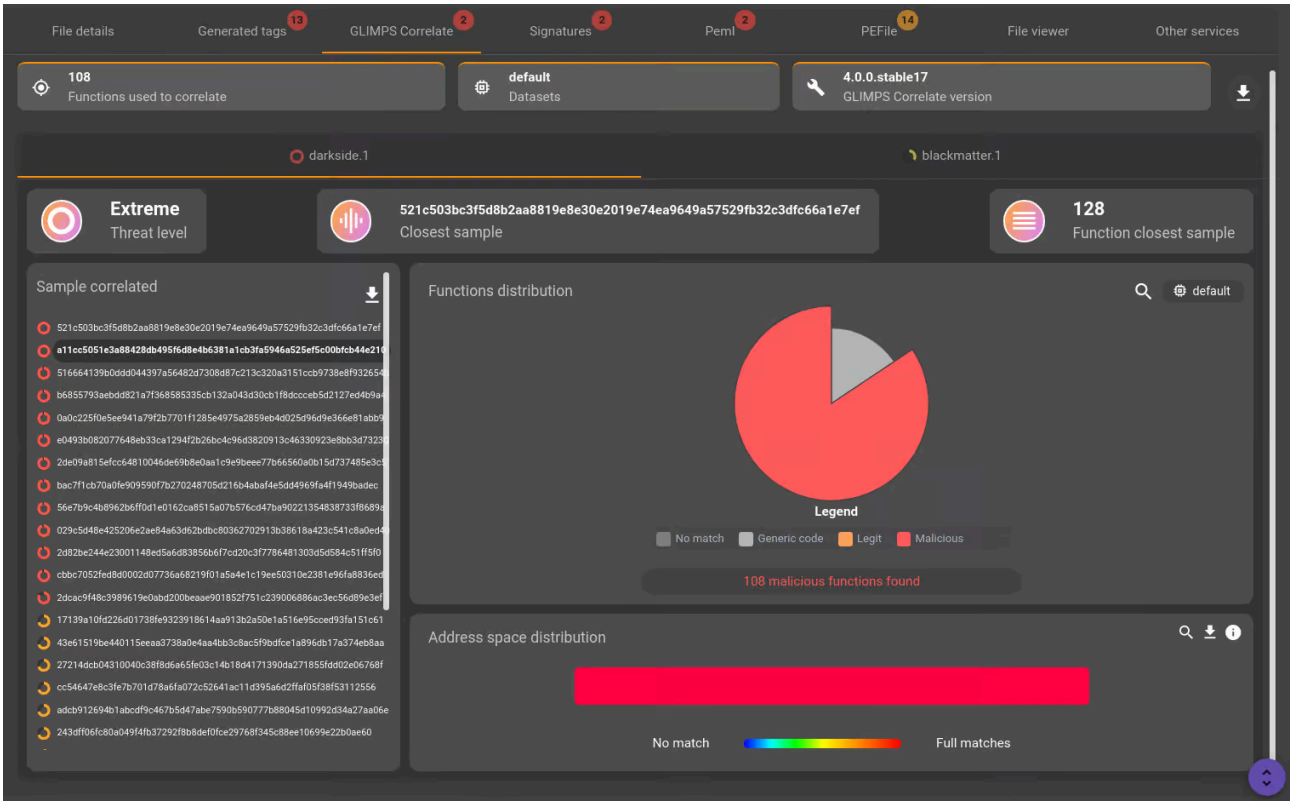

File details
Generated tags 15
GLIMPS Correlate 1
Signatures 3
Peml 2
PEFile 16
File viewer
Other services
High section entropy x2
Service version: 4.0.0.stable12
.data - Virtual: 0x00015000 (0x00003DFC bytes) - Physical: 0x00012E00 (0x00003600 bytes) - hash: 858a77d63e7e47c3d8e1ccd980804d77 - entropy: 7.962000
.data
0
8
.data - Virtual: 0x00015000 (0x00003DFC bytes) - Physical: 0x00012E00 (0x00003600 bytes) - hash: 858a77d63e7e47c3d8e1ccd980804d77 - entropy: 7.962000
High section entropy
.rsrc - Virtual: 0x00019000 (0x00000DCA bytes) - Physical: 0x00016400 (0x00000E00 bytes) - hash: d6d3bfbe838cd7598e4f7976cb5f557d - entropy: 7.929000
.rsrc
0
8
.rsrc - Virtual: 0x00019000 (0x00000DCA bytes) - Physical: 0x00016400 (0x00000E00 bytes) - hash: d6d3bfbe838cd7598e4f7976cb5f557d - entropy: 7.929000
High section entropy

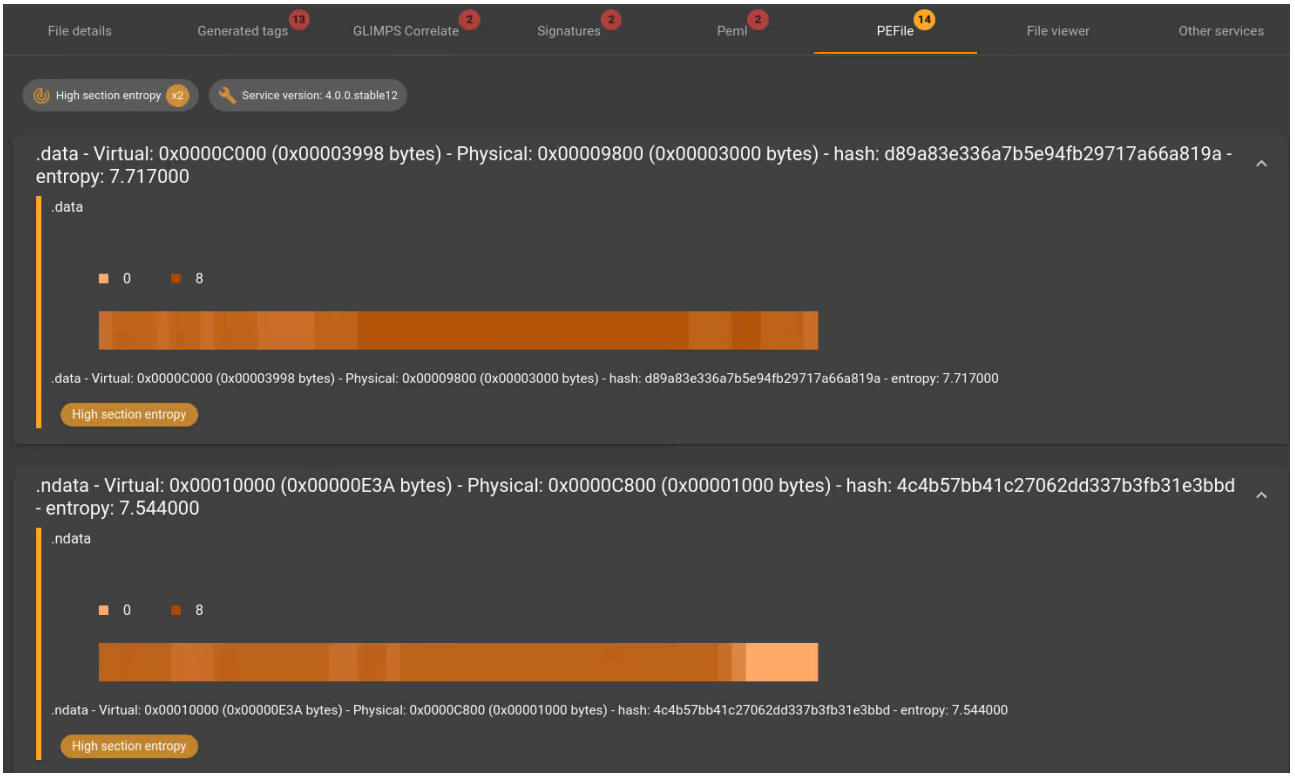
Analyse Darkside

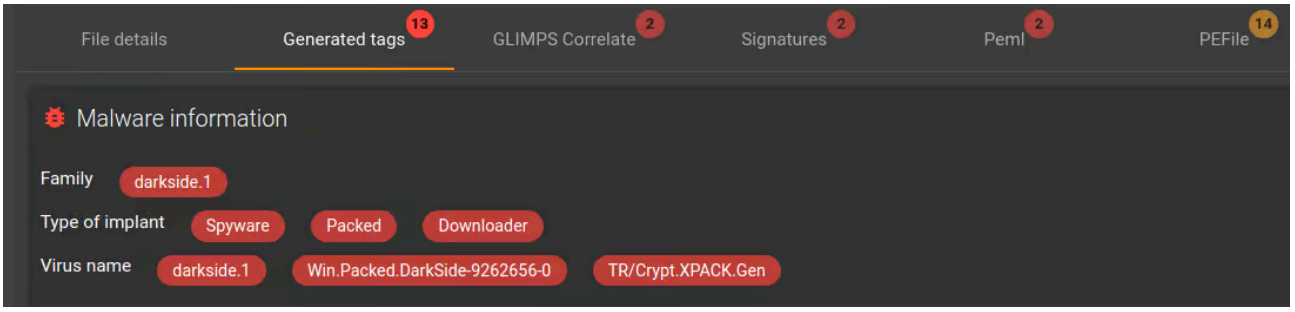
Une souche d'un malware Darkside a été soumis à GLIMPS Malware. Il est rapidement identifié comme un exécutable au format PE32 à destination de machines Windows.

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.





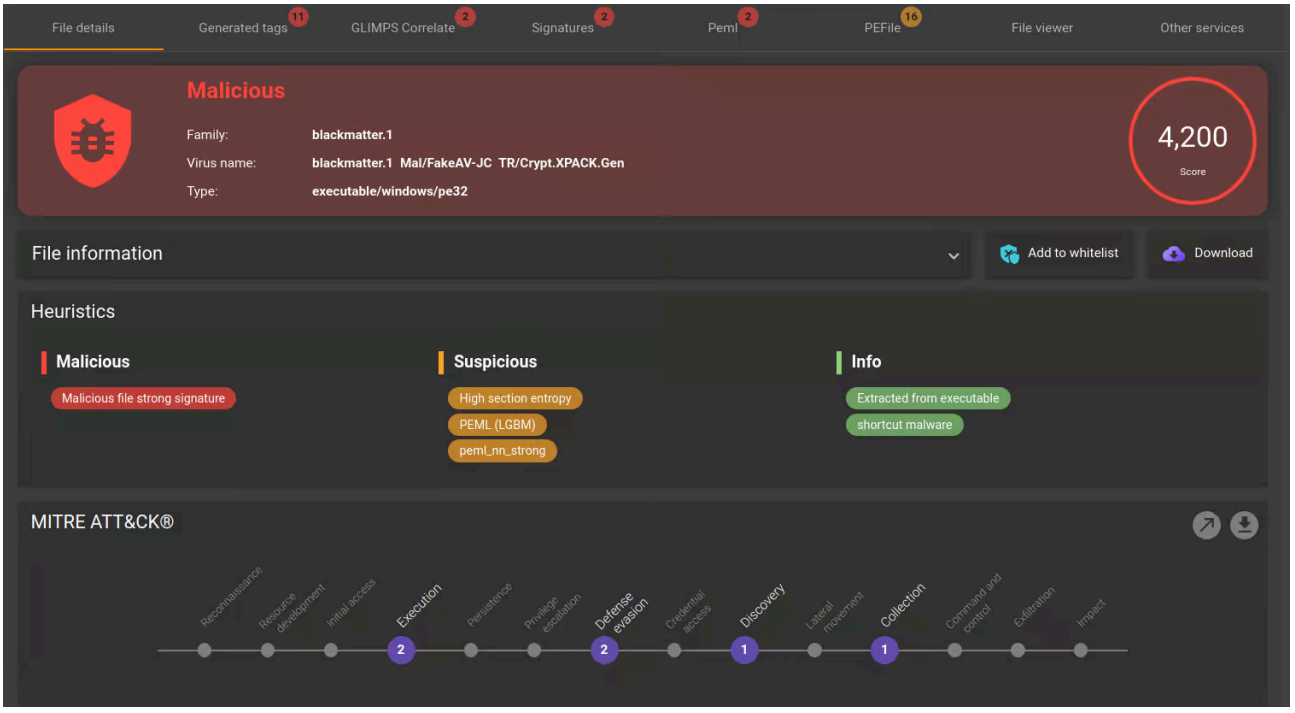


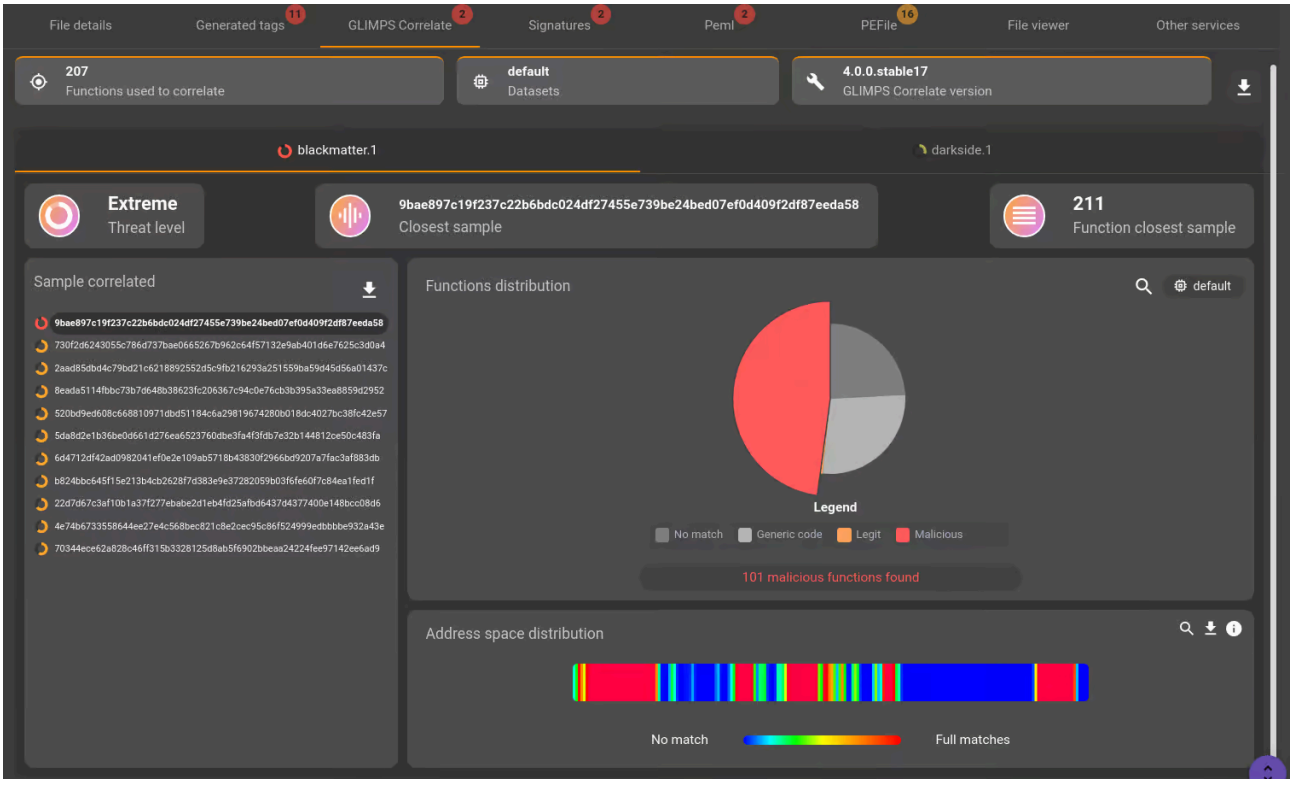
Analyse Lockbit 3.0

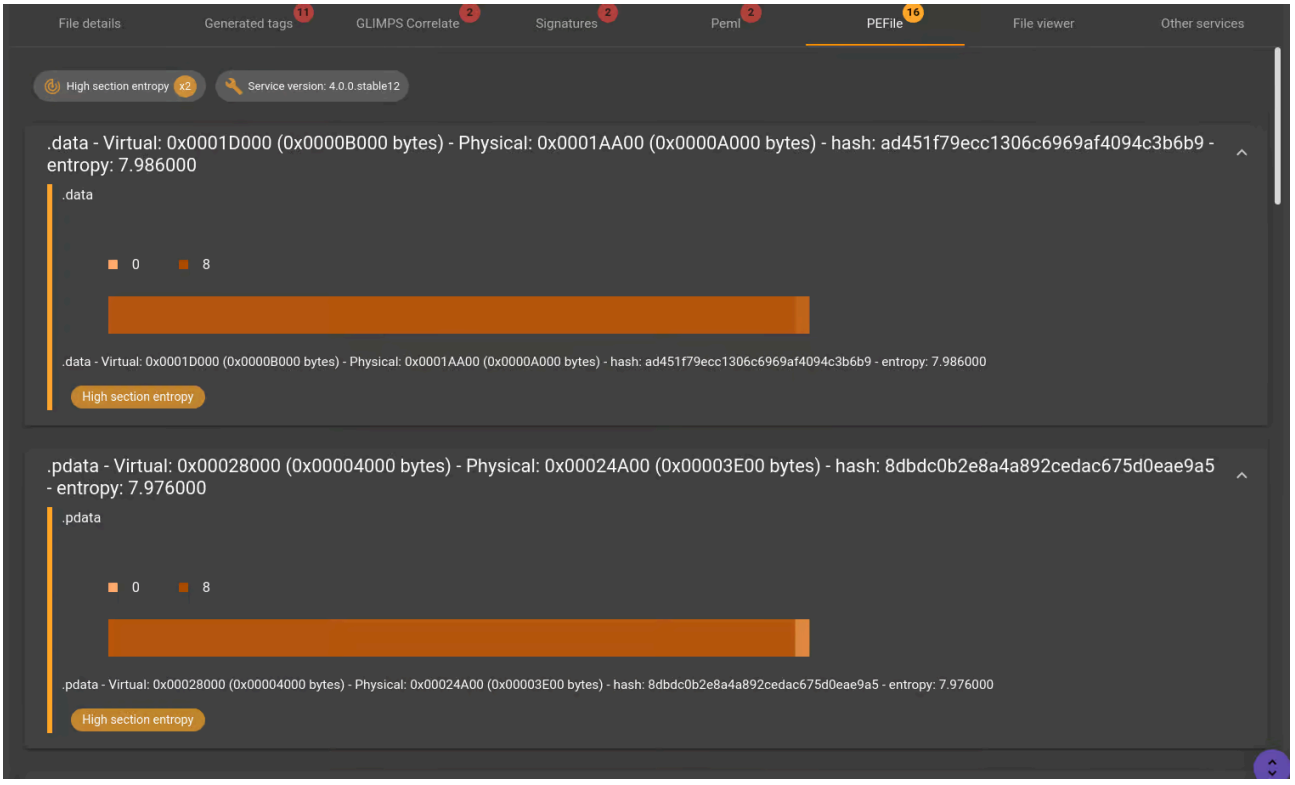
Le fichier soumis est un exécutable au format PE32 à destination de machines Windows.

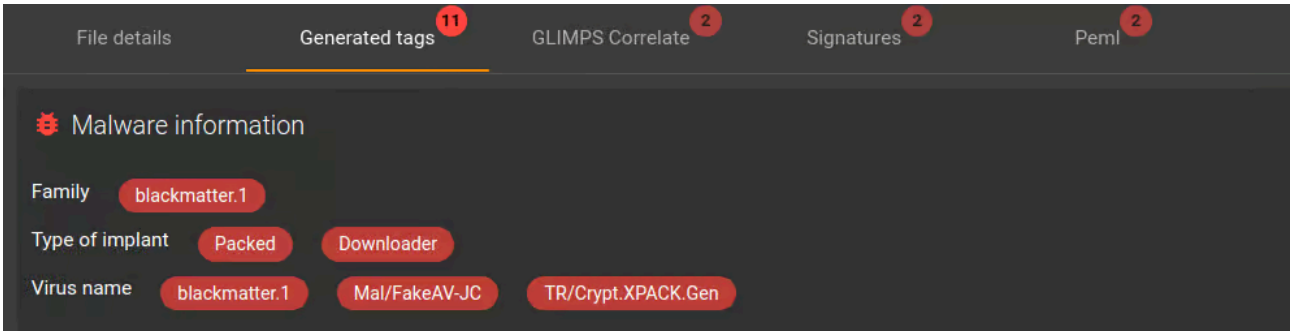
L'analyse de leur sections .data et .pdata indique une forte entropie, ce qui signifie que l'exécutable est *packé.*

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
Peml 2
PEFile 16
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®
Reconnaissance
Resource development
Initial access
Execution
Persistence
Privilege escalation
Defense evasion
Credential access
Discovery
Lateral movement
Collection
Command and control
Exfiltration
Impact
2
2
1
1


File details
Generated tags 11
GLIMPS Correlate 2
Signatures 2
Peml 2
PEFile 16
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
730f2d6243055c786d737bae0665267b962c64f57132e9ab401d6e7625c3d0a4
2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c
8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952
520bd9ed608c668810971dbd51184c6a29819674280b018dc4027bc38fc42e57
5da8d2e1b36be0d661d276ea6523760dbe3fa4f3fdb7e32b144812ce50c483fa
6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db
b824bbc645f15e213b4cb2628f7d383e9e37282059b03f6fe60f7c84ea1fed1f
22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6
4e74b6733558644ee27e4c568bec821c8e2cec95c86f524999edbbbbe932a43e
70344ece62a828c46ff315b3328125d8ab5f6902bbeaa24224fee97142ee6ad9
Functions distribution
default
Legend
No match
Generic code
Legit
Malicious
101 malicious functions found
Address space distribution
No match
Full matches





L’apport GLIMPS Malware

En mai 2021, suite à une offensive des forces de l’ordres, 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 a 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.

Prêts à aller plus loin ?

Plus d'articles

Source: https://www.glimps.fr/lockbit3-0/