Frédéric GRELOT

Cofounder,
Scientist Lead

#Botconf2023, Lightning talk session

GLIMPS

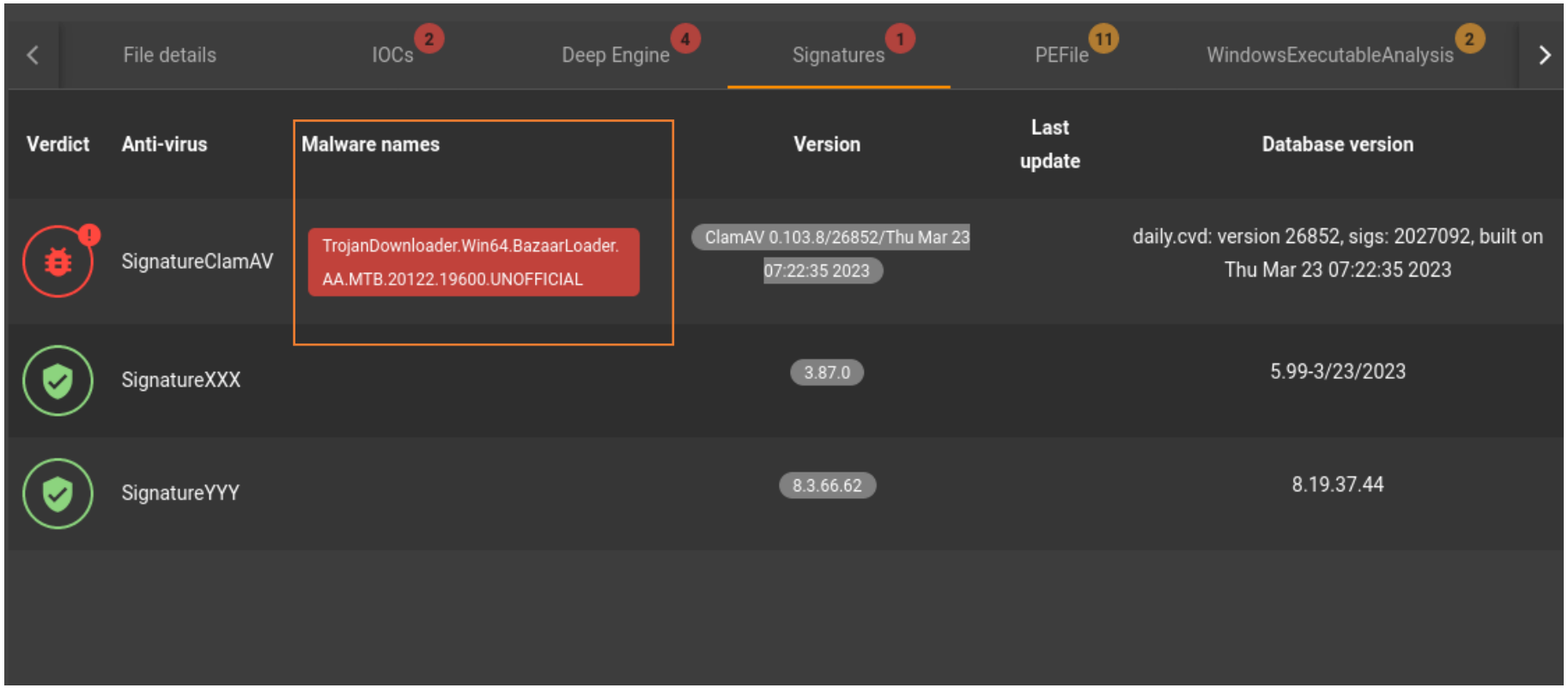
Daniel Plohmann explicitely asked for that?

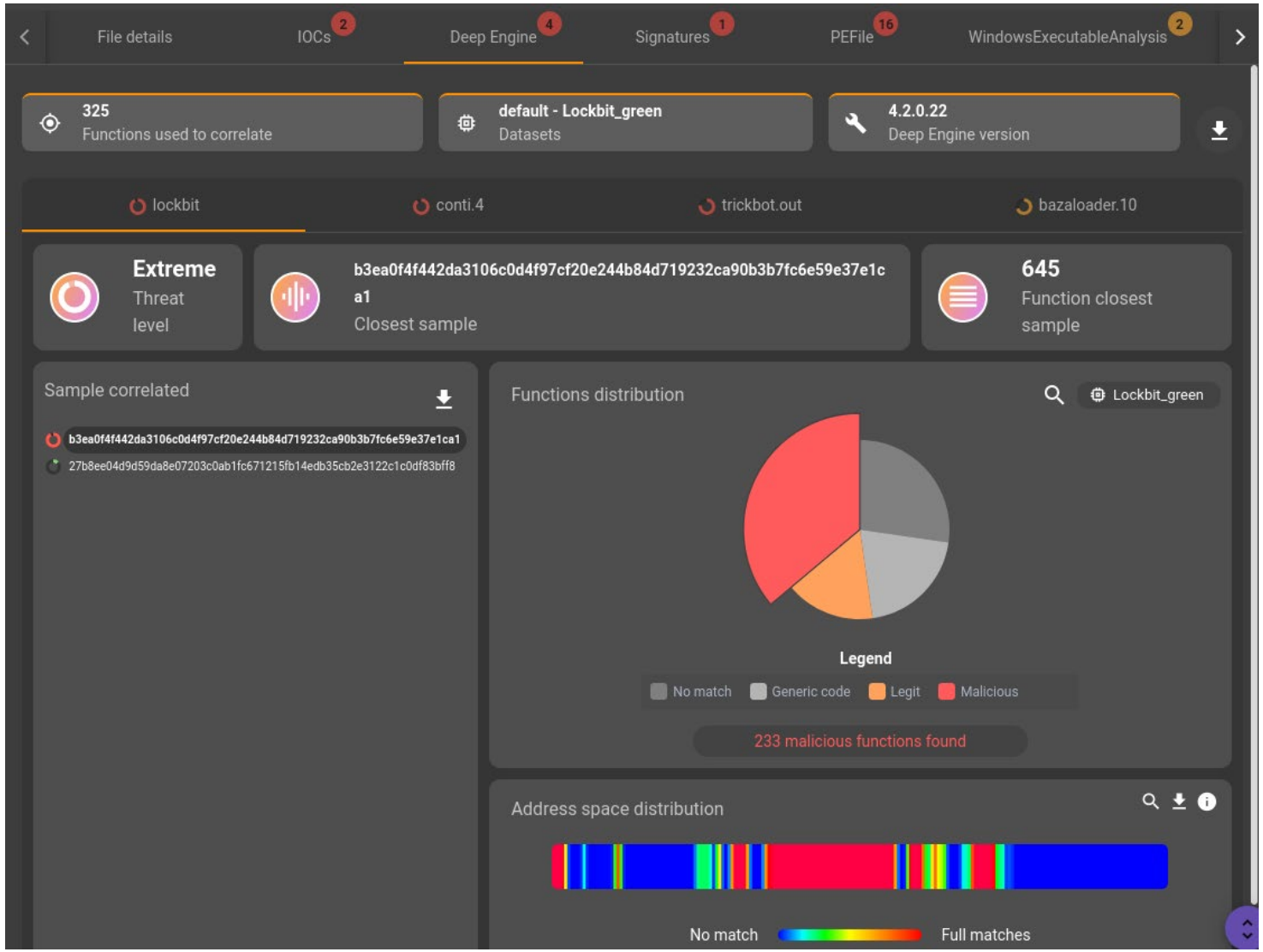
Fraunhofer FKIE

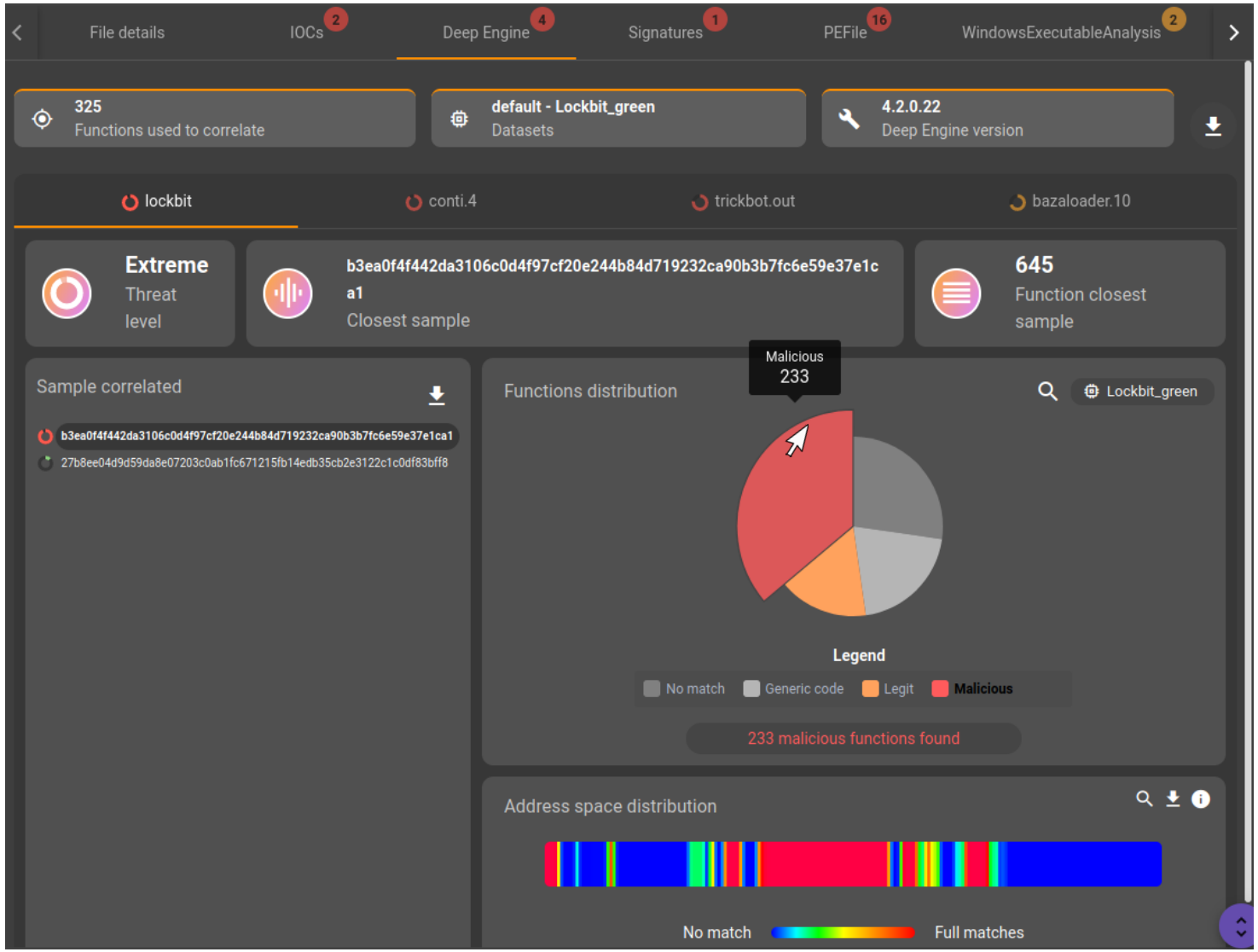
Our CTI teams worked on a Lockbit Green sample 2 weeks ago

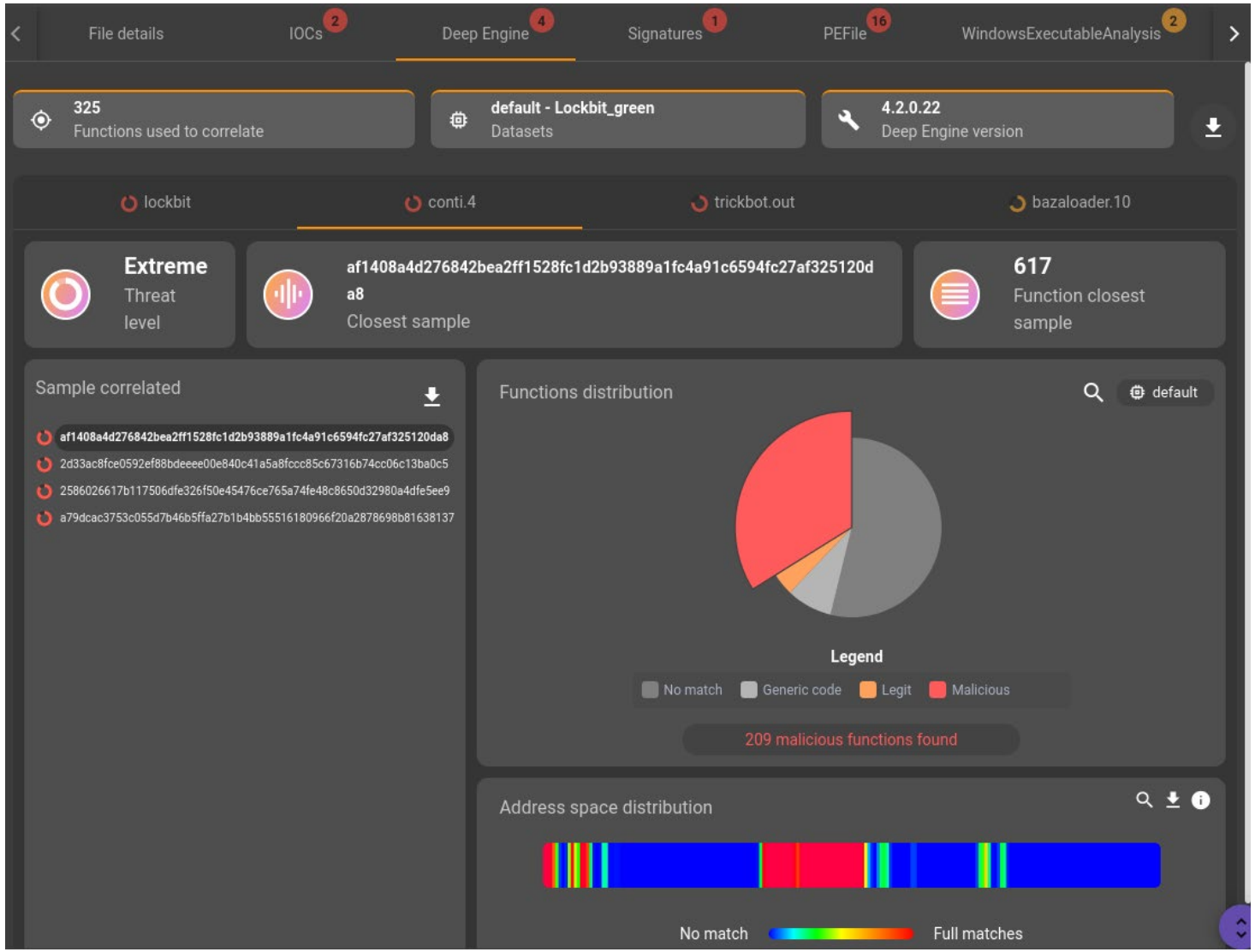
All binaries analyzed here come from Malwarebazaar (I think)

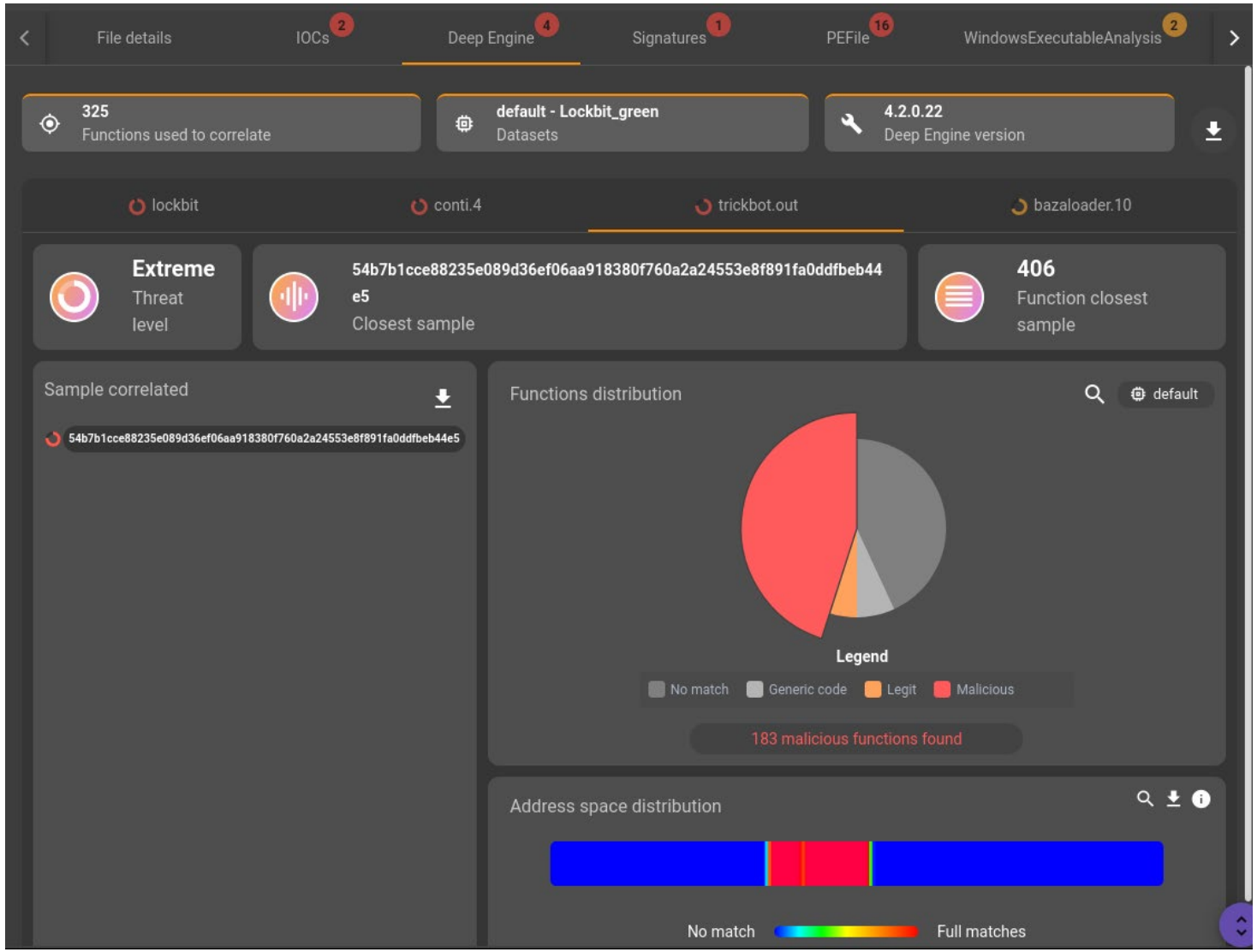
- `fb49b940570cfd241dea27ae768ac420e863d9f26c5d64f0d10aea4dd0bf0ce3`
- `b3ea0f4f442da3106c0d4f97cf20e244b84d719232ca90b3b7fc6e59e37e1ca1`

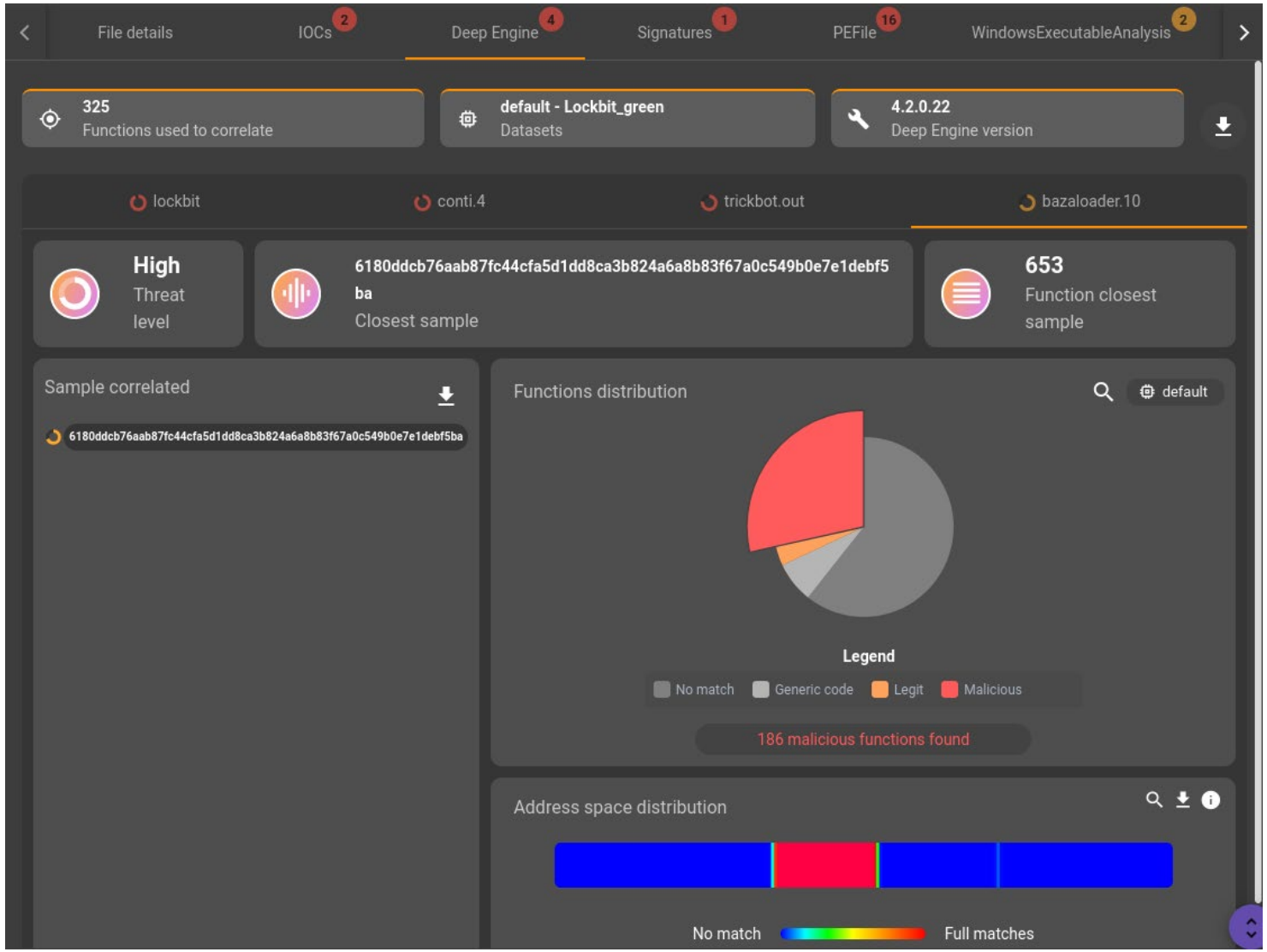

File details
IOCs 2
Deep Engine 4
Signatures 1
PEFile 11
WindowsExecutableAnalysis 2
Verdict
Anti-virus
Malware names
Version
Last update
Database version
SignatureClamAV
TrojanDownloader.Win64.BazaarLoader.AA.MTB.20122.19600.UNOFFICIAL
ClamAV 0.103.8/26852/Thu Mar 23 07:22:35 2023
daily.cvd: version 26852, sigs: 2027092, built on Thu Mar 23 07:22:35 2023
SignatureXXX
3.87.0
5.99-3/23/2023
SignatureYYY
8.3.66.62
8.19.37.44

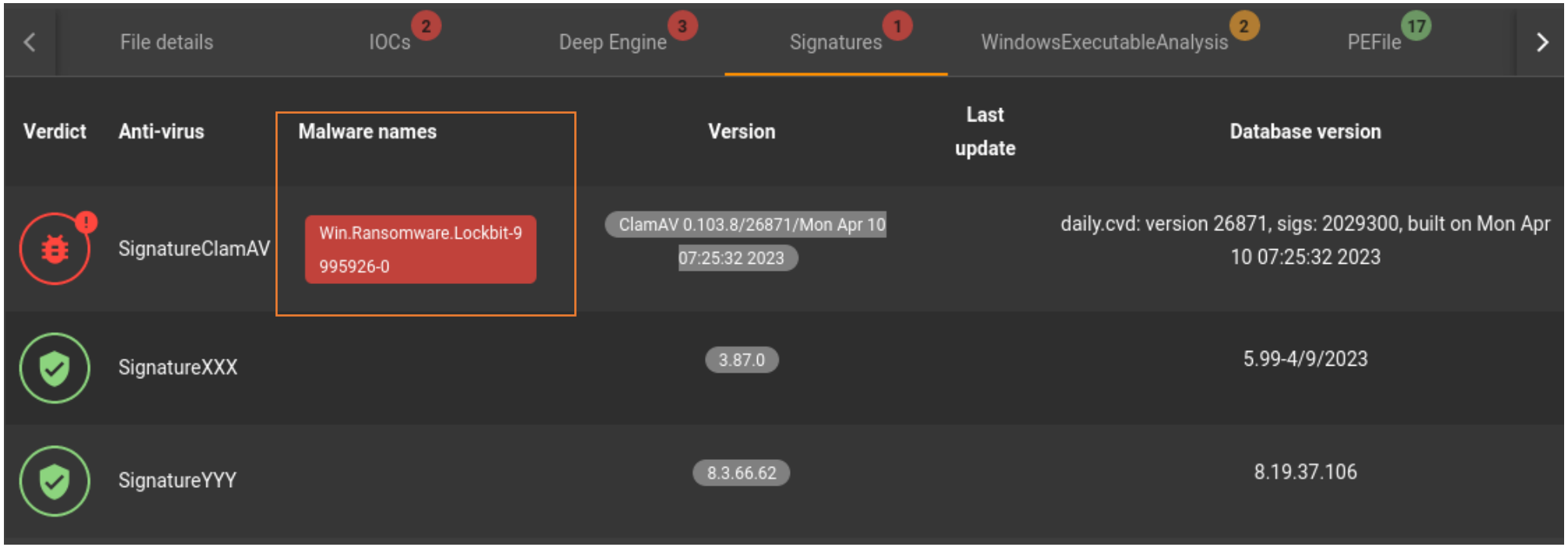

File details
IOCs 2
Deep Engine 4
Signatures 1
PEFile 16
WindowsExecutableAnalysis 2
325
Functions used to correlate
default - Lockbit_green
Datasets
4.2.0.22
Deep Engine version
lockbit
conti.4
trickbot.out
bazaloader.10
Extreme
Threat level
b3ea0f4f442da3106c0d4f97cf20e244b84d719232ca90b3b7fc6e59e37e1ca1
Closest sample
645
Function closest sample
Sample correlated
b3ea0f4f442da3106c0d4f97cf20e244b84d719232ca90b3b7fc6e59e37e1ca1
27b8ee04d9d59da8e07203c0ab1fc671215fb14edb35cb2e3122c1c0df83bff8
Functions distribution
Lockbit_green
Legend
No match
Generic code
Legit
Malicious
233 malicious functions found
Address space distribution
No match
Full matches


File details
IOCs 2
Deep Engine 4
Signatures 1
PEFile 16
WindowsExecutableAnalysis 2
325
Functions used to correlate
default - Lockbit_green
Datasets
4.2.0.22
Deep Engine version
lockbit
conti.4
trickbot.out
bazaloader.10
Extreme
Threat level
b3ea0f4f442da3106c0d4f97cf20e244b84d719232ca90b3b7fc6e59e37e1ca1
Closest sample
645
Function closest sample
Sample correlated
b3ea0f4f442da3106c0d4f97cf20e244b84d719232ca90b3b7fc6e59e37e1ca1
27b8ee04d9d59da8e07203c0ab1fc671215fb14edb35cb2e3122c1c0df83bff8
Functions distribution
Lockbit_green
Malicious
233
Legend
No match
Generic code
Legit
Malicious
233 malicious functions found
Address space distribution
No match
Full matches


File details
IOCs 2
Deep Engine 4
Signatures 1
PEFile 16
WindowsExecutableAnalysis 2
325
Functions used to correlate
default - Lockbit_green
Datasets
4.2.0.22
Deep Engine version
lockbit
conti.4
trickbot.out
bazaloader.10
Extreme
Threat level
af1408a4d276842bea2ff1528fc1d2b93889a1fc4a91c6594fc27af325120da8
Closest sample
617
Function closest sample
Sample correlated
af1408a4d276842bea2ff1528fc1d2b93889a1fc4a91c6594fc27af325120da8
2d33ac8fce0592ef88bdeeee00e840c41a5a8fccc85c67316b74cc06c13ba0c5
2586026617b117506dfe326f50e45476ce765a74fe48c8650d32980a4dfe5ee9
a79dcac3753c055d7b46b5ffa27b1b4bb55516180966f20a2878698b81638137
Functions distribution
default
Legend
No match
Generic code
Legit
Malicious
209 malicious functions found
Address space distribution
No match
Full matches


File details
IOCs 2
Deep Engine 4
Signatures 1
PEFile 16
WindowsExecutableAnalysis 2
325
Functions used to correlate
default - Lockbit_green
Datasets
4.2.0.22
Deep Engine version
lockbit
conti.4
trickbot.out
bazaloader.10
Extreme
Threat level
54b7b1cce88235e089d36ef06aa918380f760a2a24553e8f891fa0ddfbeb44e5
Closest sample
406
Function closest sample
Sample correlated
54b7b1cce88235e089d36ef06aa918380f760a2a24553e8f891fa0ddfbeb44e5
Functions distribution
default
Legend
No match
Generic code
Legit
Malicious
183 malicious functions found
Address space distribution
No match
Full matches


File details
IOCs 2
Deep Engine 4
Signatures 1
PEFile 16
WindowsExecutableAnalysis 2
325
Functions used to correlate
default - Lockbit_green
Datasets
4.2.0.22
Deep Engine version
lockbit
conti.4
trickbot.out
bazaloader.10
High
Threat level
6180ddcb76aab87fc44cfa5d1dd8ca3b824a6a8b83f67a0c549b0e7e1debf5ba
Closest sample
653
Function closest sample
Sample correlated
6180ddcb76aab87fc44cfa5d1dd8ca3b824a6a8b83f67a0c549b0e7e1debf5ba
Functions distribution
default
Legend
No match
Generic code
Legit
Malicious
186 malicious functions found
Address space distribution
No match
Full matches


File details
IOCs 2
Deep Engine 3
Signatures 1
WindowsExecutableAnalysis 2
PEFile 17
Verdict
Anti-virus
Malware names
Version
Last update
Database version
SignatureClamAV
Win.Ransomware.Lockbit-9995926-0
ClamAV 0.103.8/26871/Mon Apr 10 07:25:32 2023
daily.cvd: version 26871, sigs: 2029300, built on Mon Apr 10 07:25:32 2023
SignatureXXX
3.87.0
5.99-4/9/2023
SignatureYYY
8.3.66.62
8.19.37.106

Frédéric GRELOT

Cofounder, Scientist Lead : federic.grelot@glimps.re

https://www.linkedin.com/in/frédéric-grelot-3243052a/

Blog post coming soon...