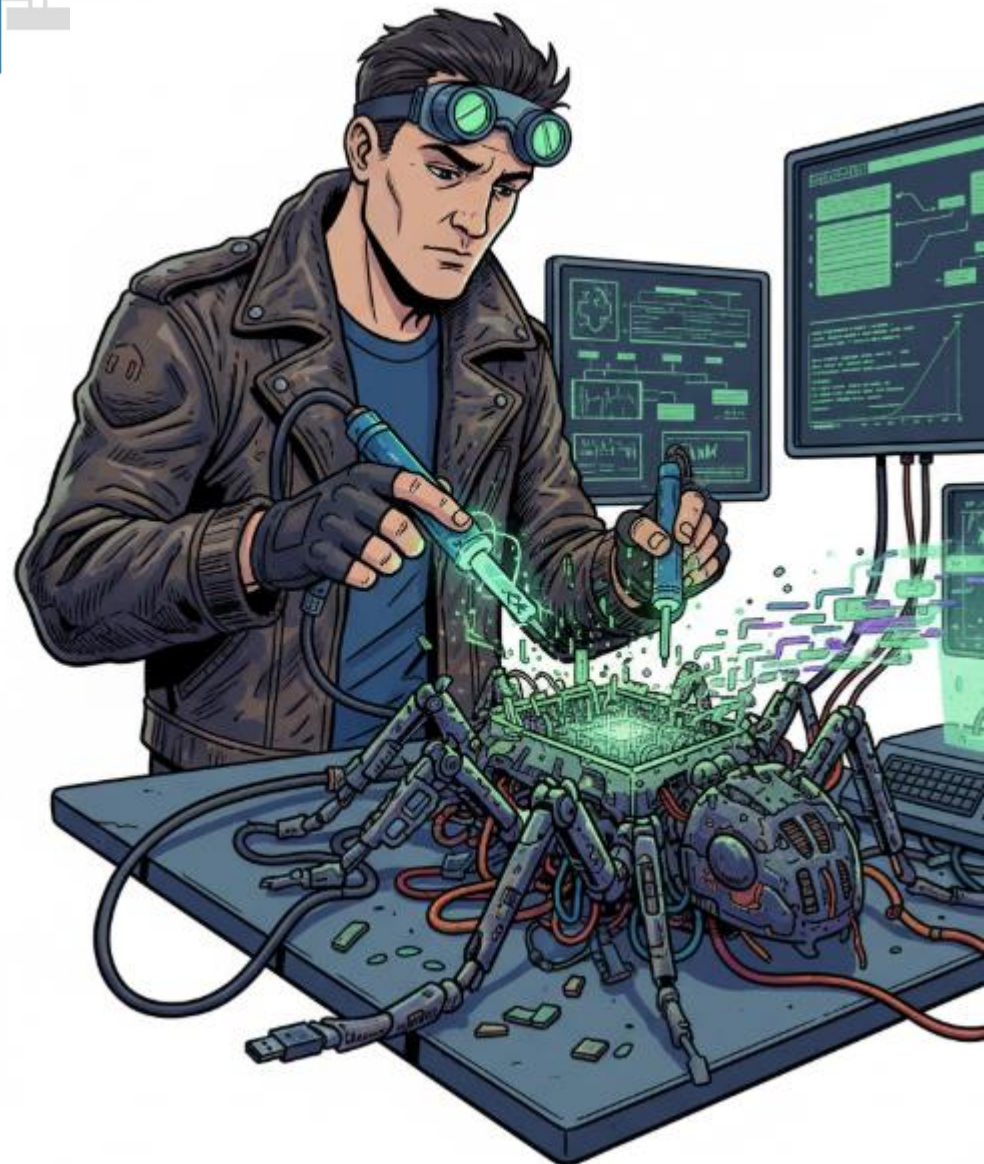
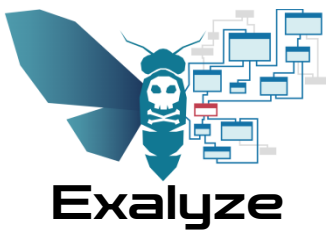


Exalyze



 ExaTrack



Qui sommes nous ?

ExaTrack

- Société créée et faite pour le Threat Hunting
- Mais nous faisons aussi de la Threat Intelligence
- On s'est donc outillés pour analyser et surtout recouper les binaires à large échelle

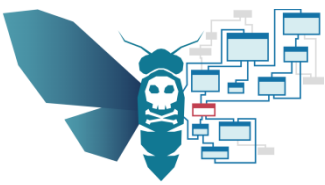
Constat de l'existant

- Le partage c'est un vœu pieux
- Les SOC n'ont pas de reversers (ou peu)
- Les attaquants sont paresseux (et moi aussi)



Ce qu'on avait déjà

- Une plateforme interne de préanalyse et de recoupement de malwares
 - Utilisant Machoc (Algo de comparaison de malware, présenté à SSTIC 2016)
 - Qu'on a mis sous stéroïdes pour comparer à large échelle (Botconf 2025)
 - Identifie des points d'attention dans le binaire
 - Extrais une partie de sa logique
 - Génère des Yara
- On s'est dit qu'on pouvait l'ouvrir à la communauté



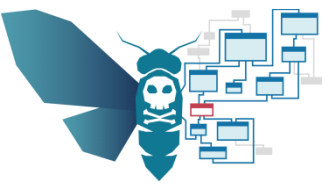
Exalyze

Intérêts : Une analyse statique et **profonde** des binaires

- Pour un SOC : Remplacer 30mn d'un reverser
- Pour un CERT : Entrer en relation avec d'autres victimes et identifier des publications liées au binaire
- Pour un RE/CTI : Rechercher des liens entre binaires, pivoter dans la donnée et gagner du temps pour suivre les attaquants

Ce que l'on fait :

- Comparer un exécutable (son code) avec **plein** d'autres
- Comparer à notre base de signatures interne
- Générer des Yaras rapidement
- Pivoter dans les métadonnées



Exalyze

Le partage ! (*mais pas tout*)



Drag & drop your samples here

or [Select file\(s\)](#) to get started

Sample confidentiality:

Public ▼



Public

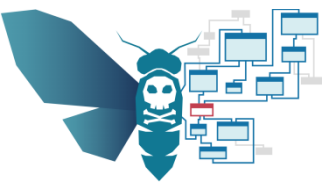
Sensitive

Confidential

Maximum upload size: 25M

ad: 10

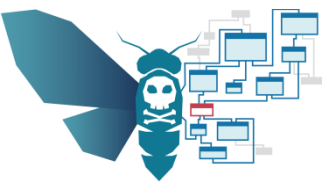
Supported file types: P



Exalyze

3 axes à intégrer/développer :

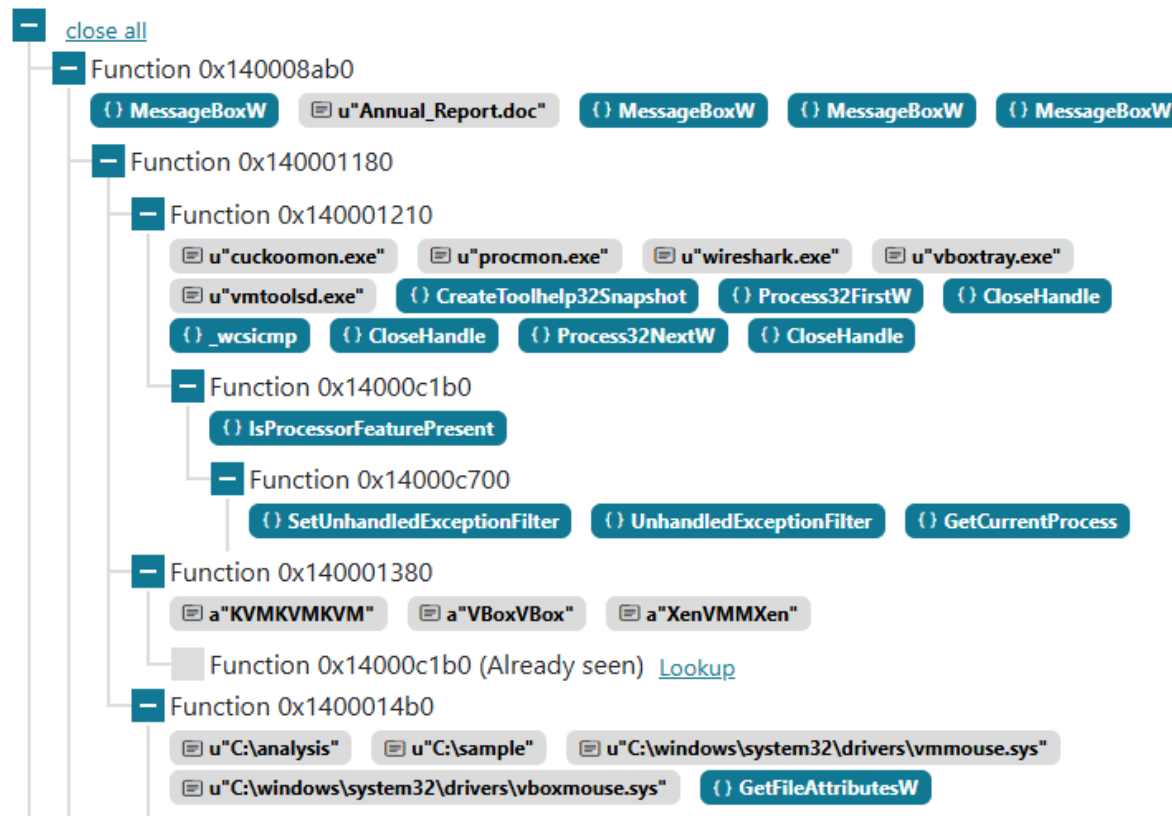
- Avoir une analyse de premier niveau (vue globale/Yara/préanalyse)
- Pouvoir pivoter dans les données
 - Pivots sur la comparaison algorithmique, ce que personne ne fait vraiment
- Avoir une communauté de CERT/SOC/Reverser à faire vivre/alimenter et qui peuvent échanger

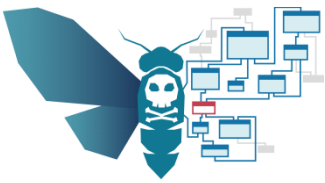


Exalyze

2 technologies uniques (bientôt 3) :

- Le concept et l'extraction de séquences





Exalyze

2 technologies uniques (bientôt 3) :

- La comparaison algorithmique d'un binaire

*< 1sc pour un diff avec
+700k binaire*

Submissions similar_to:"daeb1cd0d1b0796ed6bc3a6c4d5c7f4e11c63f908b5e8b1299184e27821fd2"

Found 4 samples

SHA-256: [f1bff18297acadd37e0b15b1c6cce005eb0c998a47d78ab4c4e7c221025fae1b](#)

First submit filename: malware

64 bits Size: 299.0 kB Last analysis time: 2025-12-03 17:48:55 UTC Control flow graph similarity: 79.0% Entropy similarity: 88% Capabilities



SHA-256: [e32a931de8c88f256f87edcd9a051fa9553d5d6156725718c24a813db2f2b330](#)

First submit filename: malware

64 bits Size: 15.3 MB Last analysis time: 2025-12-03 18:10:56 UTC Control flow graph similarity: 78.0% Entropy similarity: 57% Yara Capabilities



SHA-256: [6c918da3c47f951816b455e43dd161e490e7fedfd1960d605428a16d5bfce88d](#)

First submit filename: malware

64 bits Size: 334.8 kB Last analysis time: 2025-12-04 00:41:31 UTC Control flow graph similarity: 75.0% Entropy similarity: 82% Capabilities

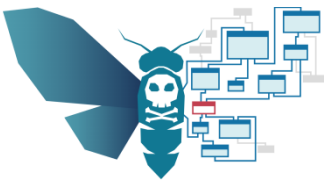


SHA-256: [c65170be2bf4f0bd71b9044592c063eaa82f3d43fcbd8a81e30a959bcaad8ae5](#)

First submit filename: c65170be2bf4f0bd71b9044592c063eaa82f3d43fcbd8a81e30a959bcaad8ae5

64 bits Size: 334.8 kB Last analysis time: 2025-12-04 00:39:42 UTC Control flow graph similarity: 75.0% Entropy similarity: 82% Capabilities Publications



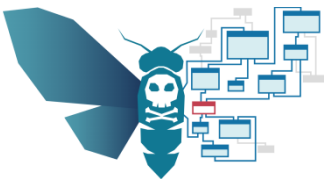


#vis_ma_vie_de_hunter

Exalyze

Faisons un tour sur la plateforme





#vis_ma_vie_de_hunter

Exalyze

Sample report

Public sample

Capabilities

Yara

SHA256: e9b200320fdd7552929bff61dfbd71f47e14b1280cb3658f0c3b651abf0f038b

Reanalyze

Find similar

Generate Yara

Download

View on VirusTotal

Sample information

Capabilities 8

ATT&CK TTPs 7

Network identifiers 1

Yara Matches 1

Publications

File description

Sample type



File size

124.4 kB

MD5

d50c5df5bd2034950733bbc83cb3c6b7

SHA1

41d98c723fb4f8bc195a04e9dd53d7ea7782d486

SHA256

e9b200320fdd7552929bff61dfbd71f47e14b1280cb3658f0c3b651abf0f038b

Architecture

64 bits

Import Hash

[2905cc75aa90851d9c39650750b76d9d](#)

PE Metadata

Rich Hash

[4730a39db3c4dfa11be9302fd3b4cea4](#)

Original Filename

[libssl](#)

Compilation time

2025-11-16 04:26:27 UTC

Company Name

[The OpenSSL Authors](#)

File Description

[OpenSSL library](#)

File Version

[3.4.1.0](#)

Internal name

[libssl](#)

Legal Copyright

[Copyright 1998-2025 The OpenSSL Authors](#)

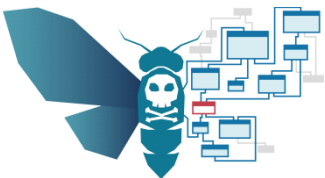
Product Name

[The OpenSSL Toolkit](#)



Entropy map ⓘ

Malware ou pas malware ?



#vis_ma_vie_de_hunter

Exalyze

Sample report

Public sample

Capabilities

Yara

SHA256: e9b200320fdd7552929bfff61dfbd71f47e14b1280cb3658f0c3b651abf0f038b

Reanalyze

Find similar

Generate Yara

Download

View on VirusTotal

Sample information

Capabilities 8

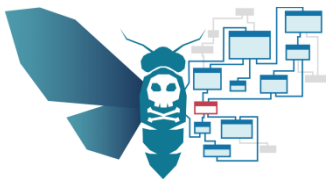
ATT&CK TTPs 7

Network identifiers 1

Yara Matches 1

Publications

Name	Description	Suspiciousness	Actions
inject_code_01	Can inject code in an other process	70 / 100	
delete_log_01	Can clear event logs	60 / 100	
Strings_Rebuild_1	Some strings are generated during the execution	60 / 100	
process_token_change_01	Can rewrite rights of a process	50 / 100	
process_list_01	Can list running processes	40 / 100	
mem_prot_01	Can rewrite memory protections	40 / 100	
Bad_Timestamps_01	Inconsistent timestamps between the PE header and the export table.	40 / 100	
Bad_Checksum_02	The PE checksum is zero	30 / 100	



#vis_ma_vie_de_hunter

Exalyze

Sample information

Capabilities 8

ATT&CK TTPs 7

TA0004 Privilege Escalation

- [T1134](#) Access Token Manipulation
- [T1055](#) Process Injection

TA0005 Defense Evasion

- [T1134](#) Access Token Manipulation
- [T1055](#) Process Injection
- [T1070](#) Indicator Removal
- [T1070.001](#) Clear Windows Event Logs

TA0007 Discovery

- [T1057](#) Process Discovery

Sample information

Capabilities 8

ATT&CK TTPs 7

Network identifiers 1

Yara Matches 1

Publications

Rule

Description

Author

Actions

UNK_Ssinj_01

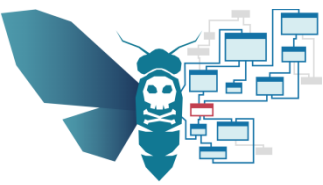
Premium ruleset

2025-11-16 (Modified: 2025-11-16)

Malware found by an ExaTrack threat hunting

Heurs
Exalyze





#vis_ma_vie_de_hunter

Exalyze

Function 0x180002170

{ } UnhookWindowsHookEx { } UnhookWindowsHookEx { } GetCurrentProcess
{ } SetProcessWorkingSetSize { } K32EmptyWorkingSet { } CloseHandle { } CloseHandle
{ } GetConsoleWindow { } ShowWindow { } GetModuleHandleA { } GetModuleFileNameA

Function 0x180001ed0

a"System" a"Security" a"Windows PowerShell" { } OpenEventLogW { } OpenEventLogW
{ } ClearEventLogW { } CloseEventLog { } OpenEventLogW { } ClearEventLogW { } CloseEventLog
{ } Sleep

Function 0x1800027f0

Function 0x180001acc

{ } MultiByteToWideChar { } CreateToolhelp32Snapshot { } Process32FirstW { } _wcsicmp
{ } Process32NextW { } CloseHandle { } OpenProcess { } OpenProcess { } OpenProcess
{ } CloseHandle { } Sleep

Function 0x180001270

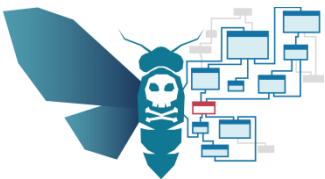
{ } GetCurrentProcess { } OpenProcessToken { } LookupPrivilegeValueA { } AdjustTokenPrivileges
{ } CloseHandle { } GetLastError

Function 0x180002b80 (Already seen) [Lookup](#)

Function 0x180001770

{ } VirtualAlloc { } VirtualAllocEx { } VirtualFree { } LoadLibraryA { } GetProcAddress
{ } VirtualAlloc { } VirtualAllocEx { } VirtualFree { } VirtualFree { } VirtualFreeEx
{ } WriteProcessMemory { } WriteProcessMemory { } WriteProcessMemory { } CreateRemoteThread
{ } VirtualFree { } VirtualFree { } VirtualFreeEx { } WaitForSingleObject { } CloseHandle
{ } VirtualFree { } VirtualFree { } VirtualFreeEx { } ReadProcessMemory


L'analyse des séquences nous permet de voir que OpenSSL utilise powershell et injecte effectivement du code à distance...



#vis_ma_vie_de_hunter

Exalyze

3 détections sur VirusTotal

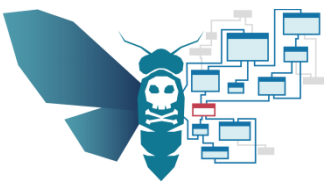
 VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

Bkav Pro	ⓘ W64.AIDetectMalware
Cynet	ⓘ Malicious (score: 100)
Symantec	ⓘ ML.Attribute.HighConfidence
Acronis (Static ML)	✅ Undetected



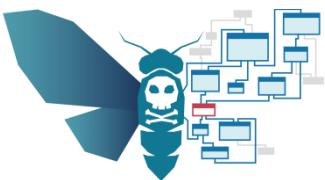
Exalyze

YetAnotherPlatform...

Oui mais **non**.

En gros il existe :

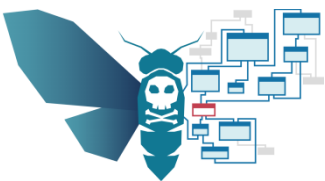
- Des sandboxes (HybridAnalysis, AnyRun, ...)
- Des stockages (Malwarebazaare, ...)
- Des recherches de patterns (VT, UnpackMe, ...)



Exalyze

Différences pour un analyste (reverser)

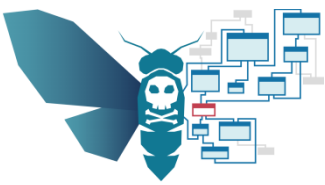
Fonctionnalité	Sandbox (Cuckoo, etc.)	Règle Yara	IDA/Ghidra	Exalyze
Désassemblage	?	?	✓	✓
Comparaison de code	?	?	✓ (unitaire)	✓
Détection d'anomalies	✓ comportement	~ (à écrire)	? manuelle	✓
Lien avec la CTI	?	?	?	✓
Temps d'exécution	3-10 minutes	< 1sc	1-5 minutes	< 5 sc
Temps d'analyse	5-30 minutes	1 sc	30+ minutes	5 minutes



Exalyze

Différences avec les autres plateformes

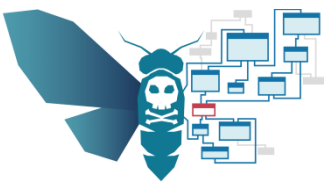
Critère	Exalyze	Any.Run	MalBazaar	VirusTotal	HbAnalysis	Joe Sandbox	Intezer
Type d'analyse	Statique	Dynamique	Statique	Stat+Dyn	Dynamique	Dynamique	Statique
Analyse du code	✓	?	?	?	?	?	✓
Comp. de code	✓	?	?	?	?	?	~
Profilage du bin	✓	✓	?	~	✓	✓	?
Règles Yara	✓	?	✓	~	✓	✓	?
Lien CTI	✓	✓	?	~	?	?	✓
Prix	Free/\$	Free/\$\$	Free	Free/\$\$\$	Free/\$	\$\$\$	\$\$\$



Exalyze

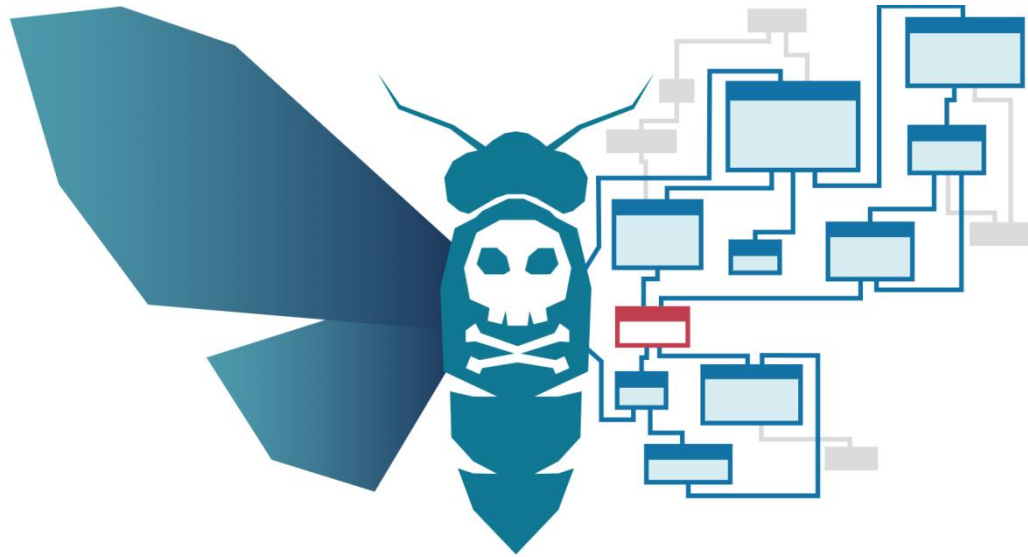
A venir (rapidement) :

- Des pivots supplémentaires
- Un nouvel algo de comparaison (Zubat) capable de retrouver une fonction proche au lieu d'un binaire
- La possibilité d'upload et download des reverse
- Importation du RE d'un sample proche
- Et beaucoup d'autres ;)



Exalyze

Merci pour votre attention
Avez-vous des questions ?



<https://exalyze.io>