

Cerbro Journal

"They did not know it was impossible so they did it." – Mark Twain

ISSUE NR. 4

CERBERO LABS

JANUARY 8, 2024

Since the last issue of our journal, there have been significant developments: the release of Cerbero Suite 7, accompanied by many new packages.

In this issue, we explore the major new features and improvements introduced by this major release and the extensive array of new packages now available for download on Cerbero Store.

Furthermore, this issue marks a first for us, being available exclusively as early access to our customers before its general public release.

CERBERO SUITE 7

With the release of version 7 we have simplified our offering by unifying the editions of Cerbero Suite, thereby removing the distinction between the Standard and Advanced editions. Streamlining our software into a single edition represents our commitment to clarity and user-centric design. Multiple editions can often lead to confusion, making it challenging for users to discern the best fit for their needs. By offering just one, unified edition, we ensure that our users can navigate our platform with ease, fully understanding the breadth of features and tools available without the clutter of overlapping options. This simplicity not only enhances user experience but also fosters trust and transparency.

We have also introduced a more straightforward and customerfriendly licensing model. Every license purchased will now be valid for a full year from the date of purchase, regardless of when the acquisition is made. This one-year license also includes updates to any major new versions that are released within that year-long period.

In the first part of this issue, we delve into the exciting updates introduced in this major version. Highlights include significant UI enhancements, the introduction of the new Fast Text View, File Info View, and File System View, along with improvements to the Python Workspace.

ALL THINGS PYTHON

Need to reverse engineer Python bytecode? No problem, we got you covered! [read more]

		format					
 C/Pythachi's (Kiprgl., pycada) 	Londrics.cppton 75 pp; SPh.	PR					
tools .	IN GAME (Real						
are toble.cp/tos39.pp	Honizie - Dyne Cole - Giffs Cole - Type Instance - B D constants - Type Instance C - Type North - Giffs C - Type North - Giffs C - Type North - Giffs C - Dyne Nort	<pre>net (all - Haw (alla) dises (all - Haw (alla) mple - offset(is)(- m Tect (alla) - Hist (mat) et (alla) - Hist (all - m tes (alla) - Hist (all - m ant (alla) - Haw (all is)(all - Haw (all - m))</pre>	Talan seedalor - Talan kitalaina lat 6007 - Valat - Talan States - Talan States Lat - Talan (1 - Tyl	OF ALL FALLES	ristustarustarusti usti 11 - Milasti Okila - Ol 00 to stor bov to seo t arabiti - Oliman Oaki	California (Marcaldo) and per (MARC - Yadret) Lis anderso, Safet The L - Alexa (Marc) Aris	12.1
	A - Tiper Inverselfts 5 - Tiper HoritARCII 4 - Tiper HoritARCII	- MINEL COME - MINE - MINEL COME - MINE - MINEL COME - MINE	- Miller (m) - Miller 94 - Yicold 317 1 93 - Yicold 31 1				
Interior Desails	- Mil 1 - Dyper Dode - 668	sets Califi - Jiars Dalli -	Palant Deckelence				
Infort Description Pracy Prease Prease	Collever (Pister (Pister Vortypoletyriter) Ener Vortypoletyriter Elever Vortypoletyriter Eleveretyr Eleveretyr Colleve	attp://cooff.as.gy/		0 00 00 00 00 0 00 00 00 0 00 00 00 0 00 0		5	

MORE ARCHIVES

Many new packages covering a vast number of additional archive formats: RAR, XAR, AR & RPM. [read more]

WINDOWS REGISTRY HIVES

Should you require the capability to delve into raw Windows Registry hives, a specialized package is now available! [read more]



PCAP & PCAPNG

Our goal was to eliminate the need to always switch to Wireshark for analyzing PCAP files. [read more]

, fash								Contraction			
• 725 ALA	is and										
CLIMPIN PR	-										
heady d a	Anna	Manual									
in the second	the sea	bac M	3 7.0 E	Packets							
hilpanap	Mather	OTTAL	11.00	_	Tel a	Annual and a second	Destination	Fundament.	Taxable .		
		0000005.8	100000-W	2014-10-13		20.314.201.317	49,204,128,120	252	0 1	072 -> 81 08	IN AVAILABLE OF
		00000048	1000004K	2014-10-12	20-22-08-222104	41.201.331.313	143,114,140,107	102	12 1	0 -> 30'Q DE	TREND PROVIDENT
		00000084	1000004K	2004-00-02		HLIN.MLIN	48.004.008.000	102	14 2	072 -> 81 38	A DHUILDING WALL
	4	00000048.	10000225	2014-00-03		NUMBER OF STREET	41.004.004.000	MITP.	100 1	All Advantional	Anal STRULL Inter
			0000004K				141.014.140.007	909	14 1	a -+ 3370 (H	A HOLDERAM (III)
		00000048	00000KAA	2004-00-03	10-17-01-1010	41.301.311.311	141.014.140.007	919	Labe I	a 2272 (w	A HEREBRIEFER
(mm) **			100000ec			101.014.001.011		110	64 3	079 in 86 (w	(ii) septimizes a
0.04											
statigence indenderation	LOWING		1.000.000		a allan				4411		
				country a	1 000000000				D.8N		
	122	NUMBER OF T			0000001		10 04 10 13 H. FE.				
					00000041		17 45 18 20 DF 04		3.3.00		
					00000034	GF 41 44 2E 48 TK 8	10 KC 20 KB 54 54		and dring 2		
G hains					CONTRACTOR OF	60 72 60 61 60 26 6	C 17 10 10 16 11		manal com-	See.	
						41 47 48 4E TA 5A 2	10 43 HF 16 43 41		Append A Man		
	2				00000545	11 40 46 48 47 17 1	10 20 MK RM 20 35	26 10 10 21	Minkow All		
					cocceded	41 48 20 18 15 18 2 41 41 48 47 18 18 18	10 10 16 16 16 26		and the owners		
						63 63 63 70 Te La 2	10 TK KE 76 76 2F		0.00011-000	n.tani,	
		H-04195	10000						application	n/ani,	
						fer in 16 An Ar ir 1	a al. Do Da Le als		institutes	fermil s	
	-										

MACOS .DS_STORE

Exploring .DS_Store files for digital forensic purposes. [read more]

0.600						1 COOK
a rite kink	fer	-				
CITCHERE IN						
teasty.		"LANNET	1000			
Note		1000445		7204	File Sale	Value
- U-26,9are		000025A3	Loop	Made	andex14	kynnemy (Phyliosid ani
 Sybin 		0000DCLA	witers	Long	Bedro 24	
O (heg) Alers		00000238	010	2005	CALIBOARD	TALM
All front Alarma			ine	Made	0004	kynwerne inflej Landoland set Fuel Fuel Fuel Fuel Fuel Fuel Fuel Fuel
Sit David Andread		00000048	4043	here i	DCDM	Talas
EP (hrP) Antoold			395.8	000	DCDR	2430331147
O (hep) Android		00002272	1,000	3345	0008	hypering in high and set out out out out and an and a first and a first and and a set. As
ea parti pcw		00005513	Large	Market 1	DCDM	kyseering (c%plined) tell tell tell tell tell tell tell tel
CO INVICTION			8000	0000	DCDR	2022-01-04018.000.40
68 (bene) Occurrents			note	4450	0008	2022-01-04718/01/40
		00003044	1044		DCDM	2430534400
Q farmary		11012142	3703	1400	DCDR	1
Privary						
I MATERIAL		CEEnet				B C D E F BRCCC
			12.3		C 42 TO 42 48 73 TK 3	30 00 01 02 03
			10.1	1 33 7	4 45 14 75 73 42 45 1	18 13 48 47 17 unFinishing They
	_		54.4	14.6	1 42 41 72 58 53 48 6	23 54 68 68 62 Euclidee(StorWool)
() Family				6 63 6	44466 641	13 48 dF 77 53 finnaiseritural
() course			83.0		1 41 12 10 17 18 48 4	RF 17 42 RF 15 LBRHAMMIN
			56.5		T 17 10 40 44 40 42 4	TO OF US AN ON CONCERNMENT.
					TR TR 23 32 34 30 2	

CERBERO STORE

For those not yet familiar with it, Cerbero Store is a simple way to install and update optional packages for Cerbero Suite and Cerbero Engine.

Updating specific parts of an application through Cerbero Store is notably more efficient than updating the entire application. This method also prevents users from having to install functionality they are not interested in.

Furthermore, our software operates across multiple platforms, meaning each update traditionally required the creation of multiple software packages. Cerbero Store addresses this issue effectively, as all platforms use the same package code, simplifying the update process and ensuring consistency across different operating systems.

Since the release of Cerbero Suite 7, Cerbero Store has

expanded significantly, adding a variety of new packages. We will delve into these additions in the subsequent pages.

It is worth mentioning, that we have moved some tools and formats to the store to reduce the overall size of the main binary package. All decompilers, for example, have been transitioned to individual packages within Cerbero Store. This move aims to facilitate installations based on necessity.

When trying to decompile code without the required decompiler, Cerbero Suite will ask you if you wish to install

INI	DEX
11 11	

CERBERO STORE	2
UI ENHANCEMENTS	3
FAST TEXT VIEW	4
CHALLENGE: PAYLOAD URL	4
FILE INFO VIEW	5
THREATPULSE	6
FILE SYSTEM VIEW	7
PYTHON WORKSPACE	7
ENGINE INTERMEZZO	8
ALL THINGS PYTHON	9
MORE ARCHIVES	11
WINDOWS REGISTRY HIVES	12
MACOS .DS_STORE	12
PCAP & PCAPNG	13
TIPS & TRICKS	14

the decompiler.

0x00401289 88 0x00401	Cerbero Sui	ite 7.0	11 510	× 14	
0x00401 0x00401 0x00401	To decompile the code th package must be installed	ie "x86 Decor d. Install it no	npiler" w?	·	
0x00401 0x00401 0x00401	[Yes	No		402

After installing the required decompiler package, Cerbero Suite will then move forward with the code decompilation process.

	Cer	bero Store - Cerbero Suite 7.1		_ 🗆 🗙
Category	Filter	🖄 Instal A	All	1 Index option 30 pt - Coloro Set 7.1 - C
All (46)	JavaScript Beautifier	Installed	^	Chan Dan Dan Dan Dan Dan Dan Dan Dan Dan D
Installed (46)	Microsoft Authenticode	Installed		Restary # Special System # Rate P Roda - Type: Data - Office: Roll > 100 in Roll >
Featured (3)	Native Ghidra UI	Installed		# 1 - page start - offense helds - start and - maker Patendri a angle mention to shor her to un this make. Note the - # 1 - page 100 - effective 1000 - start of 000 - Note 1 + 000 # 1 - page 100 - start of 000 - start of 000 - Note 1 + 000 # 1 - page 100 - start of 000 - Note 100 - 1000 -
Cloud (3)	OneNote Format	Installed		
Cryptography (3)	PCAP Format	Installed		Option Columnities Option
Debug (2)	Rlist Format	Installed		Weinstein Ministration Ministratiniterancindeaddddddddddddddddddddddddddddddddddd
Decompilers (3)		Installed		Carponet Construction Const
Development (1)	PYC Format	Installed		19 minayun 1988
File Formats (20)	PowerShell Beautifier	Installed		
Forensics (1)	Py2Exe Extractor	Installed		Version: 1.0.1
Malware (13)	PyInstaller Extractor	Installed		Author: Cerbero Labs
Online (4)	Python Snippets	Installed	5	Size: 60.74 KBs
Reversing (12)	RAR Format	Installed		
Security (1)	RPM Format	Installed		Homepage: https://cerbero.io/packages/pycformat/
Inemes (2)	RegHive Format	Installed	ſ	Description: Support for Python compiled bytecode files. The package facilitates the integration of an external decompiler through the settings.
onpackers (5)	Sample Downloader	Installed		Categories: File Formats
	ShellcodeToExecutable	Installed		
	Silicon Shellcode Emulator	Installed		
	Simple Batch Emulator	Installed		
	SolarizedDark Theme	Installed		
	String Decrypter	Installed	~	

COMMERCIAL-ONLY PACKAGES

Holders of the Personal license for Cerbero Suite have access to a wide range of packages on Cerbero Store. Nevertheless, certain packages, like the Silicon Shellcode Emulator package, are exclusively reserved for commercial licenses. We make a conscious effort to limit the number of packages restricted to commercial licenses, focusing on those that we believe are primarily used for commercial activities.

UI ENHANCEMENTS

As the array of tools in Cerbero Suite continues to expand, we recognized the need for a more intuitive and accessible interface. Hence, we've revamped the main window to feature a scrollable interface, enabling easier navigation. For added convenience, tools can also be filtered by name, ensuring a smoother user experience.

4	Cerbero Suite 7.0 🗕 🗆 🗙
	Cerbero Suite 🚮
	Analysis
Start	Perform a full dsk or custom scan. The report window can be opened once all the fles have been scanned
System Scan	Perform a score on a file or open a project. Dropping a file on this window has the same effect. V Perform a score on a file detectory on this window has the same effect.
Store	Debug
Update	🔓 JavaScript Debugger: Safely debug JavaScript code 👔 Sikon Shekode Emulator
Series	Editor
About	ÛX Hex Editor ▼ 🍡 Python Editor ▼
	Memory
	Reform a scan on a raw memory image
	Online
	B Download a malware sample matching the specified hash from the supported intelligence providers
	Filter

We've introduced a top bar menu in the analysis workspace. This new feature offers a clearer overview of available global shortcuts, streamlining navigation and bolstering overall intuitiveness.

			[PatchTest.exe]	Cerbero Suite 7.0		_ 🗆 🗙
File Navigation Actions Views Tor	ols Help	3				
8-88 / 52 24	New Ce	rbero Instance Ctrl+Al	-N K 📽 🗟 📉 🗉 🗉	# 6 9% 944-256	 703624CAESE3467881A59C48678FC280811880E8A49347C16 	£8543953 🔍 •
C Roots					a × C: Orpet	
a file 0	Layouts				carbon: analysis finished in 0.0 second	da
1 C) IBstchTest ave Dis	Inspect	or				
#	Manage	e Headers				
<u> </u>	Open G	lobal Bookmarks Ctrl+Al	-5			
Nerarchy	Open 5	lookmarka Ctri+Sh	ft+5			• ×
Name	Add Bo	olmark Chief	83 C8 01	02 083	8, 1	^
PatchTest.exe			Lon 401058:	1 00	DDE 20027: 0x00401051	
4 🚞 Documents 🔍	Open G	Hobal Notes Ctrl+Sh	ft+N 85 c0	test eax	x, eax	
🖹 Confinention File 1 (🦎	Open N	lotes Ctrl+N	75 07	jze loc	c_401063	
<	New Di	mumbly CMAA	+C 70 05	ten loc	402108 ; "right paintord)(i"	_
🖓 Summary 🚬	10,000	FRCCRIPPT	11972			
Online		PatchTest:.text:Dx004	01063 loc_401063:	: 00	008 XREF: 0x0040105A	
Intelligence: MalwareBazaar		PatchTest:.text:OxiO4	01063 68 10 21 60 00	push 0x4	40211C : "wrong password\n"	
Inteligence: HybridAnalysis		PatchTest:.text:CulO4	01068 los 401069;	; 00	ODE XXEF: 0x00401061	
Intrinsic threats		PatchTest:.text:0x004	01068 FF 15 90 20 40 00	call dwo	ord ptr [0x402090] -> printf	
W Native Code: x16		PatchTest:.text:0x104	DIDGE OB 40 PC	107 ecx	x, dword ptr [ebp - 4]	
Privacy	_					
L Debug Data		Address: 0x0040005C + Dane				
wannings	Ŷ	Contraction (Native Code: x8)				
(i) Format) while (uVarl !=	0);			^
Fill Dos Header	~	lon 401058:				
El Rich Signature		1f (uVar3 == 0) (
 III Nt Headers 		uVar6 = "righ	password!\n*;			
II File Header						
4 🔠 Optional Header		UVARS = "WEOR	password\n";			
Data Directories)				
II Section Headers		(*_printf) (uVar6)				
Import Directory		return;				
Resource Directory						
Relocation Directory	~	Line: 34 - Column: 8				
Inter Bathon code here (form		(Trlabita 1				
Illance channe come mere from						

In addition, we've made the list of context-specific actions readily accessible through the new top bar menu, ensuring all pertinent tools are just a click away.

No.				(PatchTi	est.exe] - Cerbero Suite 7.0)	
B: • D E F mode Adm Code • E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E = 0 & E & E & E & E & E & E & E & E & E &	file Nevigation Ar	ctions Views Tools Help					
Description Calculation Calculation Calculation Implicit Calculation Implici	R-88 /	Execute Action .	Ctrl+R	4 + 🗙 🚖 🛬 🗞 🗞	EE # 6 % SS	+256 * 703624CAESE3467881A59C48678FC280	81188068A49347C1668543953 🕾 •
Charlow market for the first set of	E Roots	Esecute Script.	Ctrl+Alt+R			a × C: Oxpet	
1 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.	# HQ	Open New Python Editor	CHI+AR+P			carbon: analysis finis	hed in 0.0 seconds
Andrey Marting • Decide Table State S	1 CiL\Patch	pc.					
Weak Onto Instructions Instructions <td< th=""><td>-</td><td>TaxaScript</td><td></td><td>Address Converser</td><td></td><td></td><td></td></td<>	-	TaxaScript		Address Converser			
With the second secon	Of Manager	Online		Display Calcol Kallyes			
Image: Second	CTRUE OF	Pathoo		Loop to Estar Baint	AF	nav. 1	
A Decision in the second	Name	Paversing		and to they rom			
Description Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>	PatchTest.	Unnerker	. 60	0x00401058 log_401058:		; CODE XMEF: 0w00401051	
Image: Control Image:	- Docum	Mean		0x10401058 35 60	test	eax, eax	
Cancer In the start is the instantion in a log in a start is the start is the instantion in a log in a start is the start is the instantion in a log in a start is the start is the instantion in a start is the start is the instantion in a start is the start is the start is the instantion in a start is the start is t	<	, ,	PACCATORC: Coat:	0x00401050 60 00 21 40	co push	0x402100 ; "right password!\n"	
Other Other <th< th=""><td>O Summer</td><td>• ×</td><td>PatchTest:.text:</td><td>0x00401051 XB 05</td><td>310</td><td>loc_401068</td><td></td></th<>	O Summer	• ×	PatchTest:.text:	0x00401051 XB 05	310	loc_401068	
subject to bise the set of t		allen o	PatchTest:.text:	De00401053			
Image: registration registratis registration registration registration registration re	Contractions of Male	wareflaraw.	FatchTest:.text:	0x00401043 48 10 21 40	do push	0x40211C ; "wrong password\n"	
Instruction	a Intelligence: Hybe	ridanalysis	ratchrest:.text:	0x00401058			
Websics Balance State Stat	Intrins	sic threats	PatchTest:.text:	0x00401058 loc_401069:		: CODE 288F: 0x00401061	
Nony Adds:::500/01/20 Adds:::500/01/20 Control (Low of Contro) (Low of Control (Low of Control (Low of Control (Low	Native Code: x84	6	PatchTest:.text:	Control Contro	nov	ecx. dword ptr [ebp - 4]	
Loto pick Name, Settoric for W Image: Settoric for Settoric	P	rivacy					~
Winning Oscience (pace data in) I Version Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source (pace data in) Image: Source	L Debug Data		Address: 0x0040005C -	Dane			
1 0.00000000000000000000000000000000000	Wa	arnings	(F) Decomplex (Network)	oder offici			. ×
If if is constant Vorg = 0 If is constant Vorg = 0 If is constant If is constant	A	- 61 - 17) while OWe	r1 (m.0).			
III is include: Image: Section of the sec	Gromat	• ×	uVar3 = 0;				
1 0 Stylene 1 Write = 0 () 1 0 Stylene 1 () () 1 0 Stylene 1 () () () 1 0 Stylene 1 ()	II Dos Header	^	loc_401058:				
If the case If the ca	III Rich Signatur	*	if tuvar3 -	O) (
1 Optimizer Control Co	 Ell NEHeaders)	anger paratora in .			
U Bouchowsee Units' * New parameters': Botch Newsee ************************************	El He Heade	er	else (
B constrained and Checky by the set of the	* 18 Optional I	neader	uVar6 =	"wrong password\n";			
and Dentry and	El Contine Mand	brectories	(* printf) (v	Var6):			
Because Checkey Check	imoort Direct	tory	aub_401081()				
Addition Decidy V Less M- Charte 8 Tonter Python code hares [froms with Curi-Mate-1]	Besource Dire	ectory	return;				
Dobust Newstore ' V Dec 34 - Dikence 8 Enter Python code here [focus with Ctrl+Alt+.]	Relocation Di	inectory	1				~
Enter Python code here [focus with Ctrl+Alt+.]	Dohna Direct	v	Line: 34 - Column: 8				
		ode here [focus with					

Cerbero Store has undergone a transformation, enhancing its interface for better user navigation and more streamlined package installations. Notably, the revamped interface now

showcases thumbnails for each package, offers direct web URLs to dedicated package pages, and introduces name-based filtering.

x	Cerbero S	ore - Cerbero Suite 7.1 -	
Category	Filter	Instal Al	
ali (46)	JavaScript Beautifier	Installed ^	
installed (46)	Microsoft Authenticode	Installed	
Featured (3)	Native Ghidra UI	Installed	
Cloud (3)	Contribute Format	Installed	
Cryptography (3)	DCAD Format	Installed Installed	
Debug (2)	PC/P rolling	installed and installed in the second	
Decompilers (3)	PList Format	Installed	
Development (1)	PVC Format	Installed	
File Formats (20)	PowerShell Beautifier	Installed	
Forensics (1)	Py2Exe Extractor	Installed Version 1.0.1	
Malware (13)	Pyinstaller Extractor	Installed Authors Cerbero Labs	
Coline (4)	Python Snippets	Installed Size: 60.74 KBs	
Reversing (12)	BAB Format	Date: Wed Dirc 6 2023	
Security (1)	PDM Format	Homepager https://cerben.io/padsages/pycformat/	
Themes (2)	The second second	Description: Support for Python compled bytecode flex. The particular	kage
Unpackers (3)	Regrive rolling	Inside the integration of an external decompart through the set	inga.
	Sample Downloader	Installed Categories: Fie Formats	
	ShellcodeToExecutable	Installed	
	Silicon Shelicode Emulator	Installed	
	Simple Batch Emulator	Installed	
	SolarizedDark Theme	installed	
	String Decrypter	Installed v	

Moreover, users now have the convenience of installing all packages displayed in the current list with a single click.

	Cerbero Store -	Cerbero Suite 7.0
Category	na	🕲 🖄 Instal Al
All (34)	DotNET BinaryFormatter Decoder	Installed
Updates (1)	HybridAnalysis Intelligence	Installed
Installed (30)	Native Ghidra UI	Installed
Featured (4)	Windows Memory Analysis	Installed
Cloud (3)	windows weriory rindigsis	motalica
Cryptography (3)		
Debug (2)		

The user interface for filters has been refined, now allowing users to conveniently search and filter the filters by name.

	[PatchTest.exe] - Cerbero Suite 7.0	_ = = ×
file Nevigation Actions Views Tools Help		
RIDDIFASIONE	1 4 2 2 4 4 4 4 4 4 2 3 5 5 5 5 4 4 6 10 5 5 5 5 5 10 5 5 5 5 5 5 5 5 5 5 5 5	678FC280811880F8M9347C16F8543953
Party and a second s		
- 01 and 0		ala disistad in 0.0 seconda
# FIRE ROSK FI	mat Chatter, many	the reserved in 0.0 percents
1 Cit., Patchestere 0% Pe		
N Herardy A X	🔍 Analysis (PatchTest.core) 🛛 🗡 Ref 🖬	
Name	No Property Value	
PatchTest.exe	A minis	
Documents	Z had	
Confouration Rie 1 Jann 10331 *	A convet Nits a	
< >	/ from base64 englightness bits	
😡 Summary 🔗 🛪	2 to base64 radix 26	
Online ^	value cc	
Intelligence: MalwareBazaar	Condition (optional)	
Intelligence: HybridAnalysis	check sere	
intrinsic threats	cvalue	
W Native Code: x26	+ Add St Remove + Move Up + Move Down Skatgt	
Privacy	offset -1	
L Debug Data	size -1	
wanings	trim ea	
() Format # X		Denim
III Dos Header ^		
II Rich Signature		6 J ABCII
▲ Ⅲ Nt Headers		20 00 13
I File Header	00000010 B8 00 00 00 00 00 00 00	00 00 t
4 🔠 Optional Header	0000018 40 00 00 00 00 00 00 00 00 00 00 00 00	ac ac
Data Directories		20 00
II Section Headers	00100030 00 00 00 00 00 00 00 00 00 00 00 0	00 00
Import Directory	00000038 00 00 00 00 P0 00 00 00 00000038 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00
Resource Directory	00000040 0E 1F BA OE 00 B4 09 CD	25 01
Relocation Directory		
In Dohum Direction		

Similarly to the filters view, actions can now too be filtered by their name.

We've given a fresh facelift to the dialog for loading internally stored scripts. Now, it offers a preview, allowing users to conveniently glimpse the available scripts before selection.

Name	^	1 from Pro.Core import *
gift index longeoid media metalennesspel metalennesspel metalennesspel parte gehens parte gehens	Ţ	<pre>[fmpro.Hc.import 4 def disassembledWillectoof(fame):</pre>

These enhancements represent the minor improvements. In the following pages, we will explore the key additions introduced in Cerbero Suite 7.

4

FAST TEXT VIEW

One of the standout features of Cerbero Suite 7 is the addition of a fast text view designed for previewing sizable files. Not only does this view support syntax highlighting, but its integration is seamlessly woven throughout the entirety of Cerbero Suite, enhancing functionality across the board.



The new fast text view.

Leveraging cutting-edge technology, the view intelligently Additionally, from within the fast text view, pressing auto-detects the codec of input data. Moreover, it offers automatic syntax highlighting tailored to the specific file extension.

You can simply press Ctrl+Shift+T while in a hex view, and you'll instantly activate the fast text view, presenting the selected bytes in a readable text format.



	•							-	-
Ct	rl+Shift+E	will	launch	а	text	editor,	allowing	you	to
se	amlessly ed	it the	text.						
	-								
			[ghidra_9.2_PU	BLIC 202	01113.zip] - Cerbe	ro Suite 7.0		_ 🗆 🗙	

# File Risk 1 C11ghidra_9-2_PUHLIC_20201113.zip 100% (f) Z	www.at ascii - offset: dwd6
N Merarchy	× C, Analysis (ap/constant-values.html)
The second and second	<pre>interview me. the interview me.</pre>

Naturally, the fast text view isn't just for end-users; plugin developers can fully harness its capabilities too.

CHALLENGE: PAYLOAD URL

This challenge is very easy and can be tackled by beginners.

Download the following malware sample and debug or deobfuscate the JavaScript to extract the payload URL.

SHA256: 8FD31EC311D7AED033E8405EE5D6EBD562B 363B8BB18B4E4C04D1F86D7DE81B7

Payload: c2NyaXB0OmhUdFA6Ly9qcGFqdy5qb3VybmV5 ZWRnZS5teS5pZC8/MS8=

FILE INFO VIEW

This versatile view provides you with a detailed list of a file's properties and an array of other valuable information.

File Actions Views Help PatchTest.exe Path Overview Name PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Size 6.5 KBs (6656 bytes) ii Hashes File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Users - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Write Execute Delete Users - Permissions: Read Execute Authenticated Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-11 Double click here to calculate the hash SHA-256 Double click here to calculat			File Info - Cerbero Suite 7.1	-	
Image: Control of the second secon	File Actions Vie	ews Help			
▼ [PatchTest.exe] Name Value Name PatchTest.exe Value Name PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Text Size 6.5 KBs (6656 bytes) File Image: Hashes File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Owner h Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-12 Double click here to calculate the hash SHA-256 Double click here to calculate the hash	🗲 🍺 🛃 🛅	III 🖸 🛄 4			
Name Value Name PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Size 6.5 KBs (6656 bytes) File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Owner h Permissions Addministrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash	[PatchTest.exe]				e ×
Name PatchTest.exe Path C:\tmp\webinar\PatchTest.exe Size 6.5 KBs (6656 bytes) File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Vorter Owner h Permissions: Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash	11 Overview	Name	Value		
Path C:\tmp\webinar\PatchTest.exe Size 6.5 KBs (6656 bytes) File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Owner Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash	0x Hex	Name	PatchTest.exe		
Size 6.5 KBs (6656 bytes) File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Owner Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash	Toxt	Path	C:\tmp\webinar\PatchTest.exe		
File Type exe File Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes Owner Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash		Size	6.5 KBs (6656 bytes)		
Detected Format PE Created lun apr 10 12:26:32 2023 Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes	Hashes	File Type	exe File		
Createdlun apr 10 12:26:32 2023Modifiedsab giu 1 18:42:45 2019Accessedlun apr 10 12:26:32 2023AttributesOwnerhPermissionsAdministrators - Permissions: Read Write Execute DeleteSYSTEM - Permissions: Read Write Execute DeleteUsers - Permissions: Read Write Execute DeleteAuthenticated Users - Permissions: Read Write Execute DeleteMD5Double click here to calculate the hashSHA-1Double click here to calculate the hashSHA-256Double click here to calculate the hash		Detected Format	PE		
Modified sab giu 1 18:42:45 2019 Accessed lun apr 10 12:26:32 2023 Attributes		Created	lun apr 10 12:26:32 2023		
Accessed lun apr 10 12:26:32 2023 Attributes Owner Owner h Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Authenticated Users - Permissions: Read Write Execute Delete Authenticated Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 SHA-256 Double click here to calculate the hash		Modified	sab giu 1 18:42:45 2019		
Attributes Owner h Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Execute Authenticated Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash		Accessed	lun apr 10 12:26:32 2023		
Owner h Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash		Attributes			
Permissions Administrators - Permissions: Read Write Execute Delete SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Execute Authenticated Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash		Owner	h		
SYSTEM - Permissions: Read Write Execute Delete Users - Permissions: Read Execute Authenticated Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash		Permissions	Administrators - Permissions: Read Write Execute Delete		
Users - Permissions: Read Execute Authenticated Users - Permissions: Read Write Execute Delete MD5 Double click here to calculate the hash SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash			SYSTEM - Permissions: Read Write Execute Delete		
Authenticated Users - Permissions: Read Write Execute DeleteMD5Double click here to calculate the hashSHA-1Double click here to calculate the hashSHA-256Double click here to calculate the hash			Users - Permissions: Read Execute		
MD5Double click here to calculate the hashSHA-1Double click here to calculate the hashSHA-256Double click here to calculate the hash			Authenticated Users - Permissions: Read Write Execute Delete		
SHA-1 Double click here to calculate the hash SHA-256 Double click here to calculate the hash		MD5	Double click here to calculate the hash		
SHA-256 Double click here to calculate the hash		SHA-1	Double click here to calculate the hash		
		SHA-256	Double click here to calculate the hash		
Analyze Hex Editor				Analyze	Hex Editor
Enter Python code here [focus with Ctrl+Alt+.]	Enter Python	code here [focus	with Ctrl+Alt+.]		

The new file info view.

What makes this particularly useful is the introduction of an Thanks to the fast text view, text previewing is also available, additional workspace in Cerbero Suite. This new workspace leverages the file info view and can be accessed via the shell context menu, giving you immediate access to essential file details and its content.

The overview of the file displays the most common cryptographic hashes. By activating the items via double-click or keyboard, the hash is calculated and shown.

SHA-1	Double click here to calculate the hash
SHA-256	7D3624CAE5E34678B1A59C48678FC28D811BBDE8A49347C16EB543953041BBF7

Beyond hashes, the file info view shows the hex content of the file.

Patch est.exe																			
Ouoniou	Offset	0	1	2	3	4	5	6	7	8	9	A	в	с	D	Е	F	ASCII	a
Overview	00000000	40	6.8	0.0	00	0.2	00	0.0	00	0.4	00	00	00	FF	FF	00	00	M7	
ix Hex	00000010	88	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	8	
	00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
🖢 Text	00000030	00	00	00	00	00	00	00	00	00	00	00	00	FO	00	00	00		
	00000040	0E	1 F	BA	0E	00	B4	0.9	CD	21	BB	01	40	CD	21	54	68	L. T. ITh	
Hashes	00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno	
	00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.	
	00000070	6D	6F	64	65	2E	0D	0D	AO	24	00	00	00	00	00	00	00	mode\$	
	00000080	FD	F9	55	74	B9	98	3B	27	B9	98	3B	27	B9	98	3B	27	Ut;';';'	
	00000090	FF	C9	E6	27	BA	98	3B	27	FF	C9	E4	27	B 8	98	3B	27		
	0A000000	FF	C9	DB	27	AA	98	3B	27	FF	C9	DA	27	BB	98	3B	27	· / / / /	
	000000B0	64	67	F0	27	BB	98	3B	27	B9	98	ЗA	27	9C	98	3B	27	dg.';':';'	
	000000000	B4	CA	DE	27	B8	98	3B	27	B4	CA	E0	27	B8	98	3B	27	and a straight at the	
	000000000	B4	CA	E5	27	B8	98	3B	27	52	69	63	68	B9	98	3B	27	';'Rich;'	
	000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
	000000F0	50	45	00	00	40	01	05	00	15	B9	F2	50	00	00	00	00	PEL\	
	00000100	00	00	00	00	50	00	02	01	08	10	00	00	00	10	00	00		
	00000110	00	20	00	00	00	00	40	00	00	10	00	00	00	02	00	00		
	00000120	06	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00		
	00000140	00	60	00	00	00	04	00	00	00	00	00	00	03	00	40	81		
	00000150	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00		
	00000160	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00		
	00000170	54	22	00	00	3C	00	00	00	00	40	00	00	EÛ	01	00	00	T"<	
	00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

even for large files.

4	File Info - Cerbero Suite 7.1	-		×	
File Actions Views Hel	p				
🗲 🖻 📮 📮					
<pre>[tcache.py]</pre>		-	-	<i>a</i> ×	
II Overview	import socket import struct			^	
0x Hex 3	import binascii				
M Text	def toInput():				
Hashes 7	while True:				
8	rd = s.recv(1)				
9	if not rd:				
10	break				
11	if d andswith (h">"):				
13	break				
14	print(d)				
15	return d				
16					
1/	def sendRec(b):				
18	s.senuall()				

Of course, you can also retrieve less commonly used cryptographic hashes.

		File Info - Cerbero Suite 7.1	-		×
File Actions Vie	ews Help				
1 🖻 🖗 🛅		4			
[tcache.py]				-	8
d Overview	Name	Value			
y Hoy	MD5	Double click here to calculate the hash			
w TIEX	SHA-1	Double click here to calculate the hash			
🖢 Text	SHA-256	CE9B59B8CF323598EB8548A66E6B8F6E2AAC3463EC8DE2BF6EF6EF01B5C92F42			
Hashes	SHA-384	Double click here to calculate the hash			
	SHA-512	Double click here to calculate the hash			
	SHA3-224	Double click here to calculate the hash			
	SHA3-256	Double click here to calculate the hash			
	SHA3-384	Double click here to calculate the hash			
	SHA3-512	Double click here to calculate the hash			
	RIPEMD-128	Double click here to calculate the hash			
	RIPEMD-160	Double click here to calculate the hash			
	WPOOL	Double click here to calculate the hash			

Hovering over a calculated hash shows its humanized form.

... continued from page 5.

SHA-1	Double click here to calculate the hash
SHA-256	7D3624CAE5E34678B1A59C48678FC28D811BBDE8A49347C16EB543953041BBF7
SHA-384	Double click here to calc Humanized: nitrogen-island-low-december
SHA-512	Double click here to calculate the hash

When exploring files on disk, a quick launch panel appears at the bottom, offering a hassle-free way to open the current file with another tool that supports its type.



The file info view is completely exposed to the SDK, and it can

be further extended via plugins using the UI hook extension type via the "fileinfo" category.

To improve performance, we've completely rewritten the file dialogs, but we didn't stop there: when opening a file, an "Info" button is visible.

File name:	PatchTest.exe	Open
Files of type:	Al Fies (*)	- Cancel
Format:	Auto	-
Detected format	(s): PE	
		🖶 Info

When clicked, this button displays a file info view for the currently selected file, so that before opening a file we can inspect its information and content if necessary.

	Sele	ct a file to s	can (Cerbero	Suite 7.1			×		
C:\tmp\webinar						•	• • •			
My Computer h Desktop Documents Downloads	mw.zip are p	Size 18.27 93 KBs 111.5 6.5 KBs 8.66 KBs	Type zip File malwa zip File exe File zip File	Modified 19/08/2020 10:27 07/08/2020 13:01 31/01/2023 11:38 01/06/2019 18:42 25/02/2017 16:42			~			
File name:	PatchTest.exe	hTest.exe								
Format: Auto										
Detected format(s):	PE						— Inf	ō		
III Overview	Name				Value			^		
0x Hex	Name	PatchTest.e	xe							
	Path	C:\tmp\web	inar\Patcl	nTest.exe						
lext	Size	6.5 KBs (665	56 bytes)							
Hashes	File Type	exe File								
	Detected Format	PE								
	Created	lun apr 10 1	2:26:32 2	023						
	Modified	sab giu 1 18	3:42:45 20	19				~		
						Analyze	Hex Edit	or		

A file dialog displaying and embedded file info view.

THREATPULSE

In response to the rapidly changing and sophisticated nature of cyber threats, we have released the ThreatPulse package, a critical tool designed to combat the latest and potentially unforeseen threats.

Recognizing that new threats may not conform to specific file formats or might target formats not yet fully supported, ThreatPulse offers a versatile and timely solution. It serves as a dynamic resource for detecting emerging threats, sometimes providing temporary detection capabilities that can be crucial until the main binaries of Cerbero Suite are updated.

Available to all Cerbero Suite license holders through Cerbero Store, ThreatPulse ensures that users are equipped with the most current tools and strategies, enabling them to address a broad spectrum of threats effectively and promptly, even those that challenge existing detection paradigms.

					[.]	OS_Store] -	Cerbero Suite 7.1			_ 🗆 🗙
File Navigation Actions Views	Tools Hel	P 1⊡ 4-9				8 N I I	E # 6 10	<mark>6</mark> SHA-256 → 43	ASD083DDEF1AAD4E0D3A84E3FD738D504	277988E8E568F8(🕾
💭 Roots									K Dutput	
# File Risk 1 0:\\.05_Store 10%	For DSSTO	wat RE								
N Herarchy	<i>•</i> ×	C, Analysis (P	Netadeta							
Name	^	offset	ID	Type	Tile N	8214			Value	
 OS_Store 		00002985	lsvp	blob	Android		bytearray(b"bpl	Lst00\xd8\x01\x02\	x03\x04\x05\x06\x07\x08\t\n\x0b\x1	dg/w13/nG_/w10/w
 Systems 		00002C1A	v8m	long	Android		1			
[bwsp] Alarms		00002039	dscl	bool	Cardboard		False			
 (BVP) Alarms (BVP) Alarms 	- 12	00002057	twap	blob	DCIM		bytearray(b"bpl:	ist00\md8\x01\x02\	x03\x04\x05\x06\x07\x08\t\t\x0b\t)	(xOb/xOe/xOf/xOb)
[bwsp] Android		00002048	dscl	bool	DCIM		ralse			
(bxP) Android		00002060	1918	comp	DOIM		2431911167			
😡 (hsp) Android		00002070	1svP	blob	DCIM		bytearray(b'bpl:	ist00\xd8\x01\x02\	x03\x04\x05\x06\x07\x00\t\n\x0b\x1	17D/#11/nF_\x10/>
(bwsp) DCIM		00005010	lavp	blob	DCIM		bytearray(b"bpl	Lst00\xd8\x01\x02\	x03\x04\x05\x06\x07\x08\t\n\x0b\x1	LdE\#13\nG_\#10\s
Entry DOM		0000300c	moOD	duto	DOIM		2022-01-14118:0	9:40		
(bysol Documents)	~	00003029	modD	dutc	DOIM		2022-01-14118:0	9:40		
<	>	00003044	ph15	comp	DC1M		2433126400			
Summery	0 ×	00003060	V525	1000	DCIM		1			
Privacy)
I Metadata		offset	0	12	84567	8 9 8	всрвя	ASCII		
			00 0	0 00 D	2 62 70 60 69	73 74 30	00 D0 01 02 03	bplist00		
		00000020	68 7	7 53 7	61 74 75 73	42 61 72	58 53 68 6P 77	owStatusBar(Show		
		00000030	50 6	1 74 6	62 61 72 58 63 69 68 71	53 68 68	77 54 68 68 68 6C	Fathbar (ShowTool		
2 Format		00000050	10 1	4 43 6	65 74 61 69	62 65 72	53 68 6r 77 53	ContainerShow5		
Fill Mercurus		00000080	69 6	4 65 6	1 61 72 50 57	62 61 73	6F 77 42 6F 75	idebar\WindowBou		
		00000030	58.5	3 68 6	77 53 69 64	65 62 63	72 08 08 09 08	[ShowSidebar		
		00000050	09.5	P 10 1	8 78 78 31 37	34 20 20	32 32 33 70 20	(1174,.223),		
Enter Fython code here [fo	cus with	Ctrl+Alt+								

FILE SYSTEM VIEW

We have created a new interface specifically to showcase file system structures.



The new file system view.

The file system view provides a multifaceted display and embeds the previously presented file info view. Coupled with familiar navigation tools and shortcuts, it ensures a smooth and intuitive journey through any file system.

The SDK provides access to the file system interface and its view, saving plugin developers the hassle of crafting their own.

PYTHON WORKSPACE

Our Python editor and workspace have undergone significant enhancements. Now, they not only support the editing of files on disk, but also come equipped with auto-completion.

Python Editor - Cerbero Suite 7.0	- U ×
File Actions Views Help	
script.py*] - Pythan	ð ×
🕒 📷 🔹 🔛 🔹 Climpliscipt.py	ý
1 from Pro.5iliconSpreadsheet import * 2 from Pro.UI import proContext	
4 class EmulatorHelper(SiliconExcelEmulatorHelper): 5	
<pre>6 definit(self): 7 super(EmulatorNelper, self)init() 8</pre>	
<pre>9 def evaluateFunction(self, emu, ctx, opts, depth, e): 10 function_name = c.toString() 11 print(function_name)</pre>	
12 return SiliconExcelBaulatorValue() 13 14	
15 if v.isValid(): 16 view=SiliconSpreadsheetWorkspaceView(v)	
17 helper = EmulatorHelper() 18 emu = view.getExcelEmulator()	
19 ess, se 20 else: other or the set of the view"	
setVerbose	
setWart setWorkspace	
Enter Fython code here [focus with Ctrl+Alt+.]	

In addition to the auto-completion feature the editor now displays tool-tips that appear while inputting function arguments.

10 11 12 13 14 15 16	<pre># load the file as por pdf = PDFODject() if not pdf.Load(c): print("error: invalid file format") # parse all referenced objects objeable = pdf.baildobjectrale(</pre>
17	<pre># detect unreferenced objects.</pre>
18	(corrupted or malicious PB BuldObjectTableAref_offset:int=INVALID_STREAM_OFFSET) >> PDFObjectTable
19	pdf_DetectObjects(objtable) [Creates a PDF object table.
20	# store the object table interTRBITY
21	pdf.setObjectTable(objtable)
22	# process PDF encryption
23	if not pdf.ProcessEncryption():

Auto-completion currently encompasses all built-in Python libraries and those modules in our SDK that have already been documented. As we continually update and expand the documentation, the scope of auto-completion also grows. Since all core modules are thoroughly documented, autocompletion is an invaluable tool for plugin developers.

8

ENGINE INTERMEZZO



In case you're not yet familiar with Cerbero Engine, here is a quick introduction. You can read more on our web page.

WHAT IS CERBERO ENGINE?

Cerbero Engine is our solution for enterprise projects such as cloud or in-house services. It offers the same SDK as Cerbero Suite and has already been used to analyze billions of files.

WHAT CAN IT DO?

The SDK is extensive and features support for dozens of file formats, scanning, disassembly, decompiling, emulation, signature matching, file carving, decompression, decryption and much more.

We make sure Cerbero Engine keeps up with the latest threats and challenges presented by file formats which are difficult to analyze. We offer state-of-the-art support for various file types such as Adobe PDF and Microsoft Office.

HOW SECURE IS IT?

Cerbero Engine has been designed taking into account all types of security issues when analyzing malicious files: buffer overflows, integer overflows, infinite loops, infinite recursion, decompression bombs, denial-of-service etc.

WHAT PLATFORMS DOES IT SUPPORT?

Just like Cerbero Suite, Cerbero Engine is cross-platform. Currently we offer it for both Windows (x86, x64) and Linux (x64). It is also compatible with older versions of Windows and Linux.

CAN IT BE EMBEDDED?

Cerbero Engine is deployed as an embeddable module: a Dynamic-Link Library (DLL) on Windows and a Shared Library on Linux. The engine can be loaded from both C/C++ and Python 3.

Loading the engine from Python is extremely simple.

```
from ProEngine import *
# initialize the engine
proEngineInit()
# from here on the SDK can be accessed
from Pro.Core import *
# ...
# finalize the engine before exiting
proEngineFinal()
```

Loading the engine from C/C++ is also very simple: it only requires including the 'ProEngine' header and specifying the location of the engine on disk.

```
#define PRO_ENGINE_INIT
#include "ProEngine.h"
```

int main()

{

// from here on the SDK can be \hookrightarrow accessed

// finalize the engine before exiting
proEngineFinal();
return 0;

IS IT FAST?

While the SDK is in Python, our engine is written in C++ and is both multi-thread and multi-process. This design decision guarantees maximum speed, while also giving you the capability to write cross-platform code that is compatible across both Cerbero Engine and Cerbero Suite.

Since the SDK is in Python, you don't need to worry about rebuilding your project when the engine is updated. Moreover, we take great care not to introduce breaking changes to the SDK: we don't want you to worry that an update could cause your code to stop working!

HOW DO YOU LICENSE IT?

We license Cerbero Engine on a per-case basis. Licensing depends on the project's scope. If you are interested in a quotation, please contact us.

Purchasing a license of Cerbero Engine comes with discounted lab licenses for Cerbero Suite. By using Cerbero Suite, your engineers can interactively debug parsing issues, analyze edge cases, use the Python editor for development and create graphical applications that work in conjunction with Cerbero Engine.

ALL THINGS PYTHON

We have released three packages designed to assist reverse engineers in unraveling the complexities of Python PYC bytecode files and how they are deployed. These packages are available to all licenses of Cerbero Suite.

The first package adds support for the PYC format.

4			[cookies.cpython-39.pyc] - Cerbero Suite 7.1	_ 🗆 🗙
File Navigation Actions Views Tools I	Help			
		🛃 🕾 🖾 🖕 📥 🍲	🔶 🖕 🐘 📎 📰 📰 🏄 🔎 60% SHA-256 🔹 FE240AE3E9E5E050E723CI	AB72E86164AA60E2EA416850E72D1C87DE
Roots		in nan sel se sel se	a ta i se ce i se ta i regione de la contractione d	# ×
# El-		Di-	te France	-
# File		RIS	sk Format	
1 C:\Python39\Lib\http\pycache\	cookies.	cpython-39.pyc 60%	РҮС	
প্ট Hierarchy 👼 🗙	🔍 Analy	ysis [Byte Code: Disassembled]	JL	ð ×
Name	1019	b'lower',		^
cookies couthon-39 pvc	1020	b'_reserved',		
Concerence of the second secon	1021	b'COOKIEError',		
	1022) update		
	1024	LocalNames: (
	1025	b'self',		
	1026	b'values',		
	1027	b'data',		
< >	1020	b'val'		
P. C	1030)		
Summary	1031	FreeVars: (
Intrinsic threats	1032)		
The second secon	1033)		
Syte Code: Decompiled	1035	FileName: b'C:\\Python3	39\\lib\\http\\cookies.py'	
Privacy	1036	Name: b'update'		
Personal Information	1037	FirstLine: 337		
Information	1038	LineTable: b'\x00\x01\3	x04\x01\x14\x01\x08\x01\n\x01\x0e\x01\n\x01'	
U Version Information	1035	Disassembly:		
	1041	-		
	1042	0 BUILD_MAP	0	
	1043	2 STORE_FAST	2 ; p'data' 0 : b'dict!	
	1045	6 LOAD FAST	1; b'values'	
🛿 Format 🖉 🗶	1046	8 CALL_FUNCTION	1	
Objects	1047	10 LOAD_METHOD	1 ; b'items'	
	1048	12 CALL METHOD	0	
	1049	14 GET_ITER 16 FOR ITER	48 : loc:66	
	1051	18 UNPACK SEQUENCE	E 2	
	1052	20 STORE_FAST	3 ; b'key'	
	1053	22 STORE FAST	4 ; b'val'	×
Enter Python code here [focus wi	th Ctr	l+Alt+.]		
pic				

The disassembled bytecode of a Python PYC file.

PYC files are compiled bytecode versions of Python source code. These compiled files can be deployed in place of the original source code, serving as a bytecode format for execution by the Python interpreter. PYC files are tied to the specific version of Python they were compiled with, necessitating recompilation when different Python versions are used.

The support is designed to be fully compatible with all Python versions, enabling users to delve into the intricacies of the complete PYC file format and its instructions.



The package also allows the integration of an external

decompiler such as Decompyle++ through the settings.

4		Cerbero Suite 7.1	- 🗆 🗙
	Cer	bero Suite 🚮	
1 Start	General Security	Here you can set up the external decompiler for Python compiled bytecode files.	
G System Scan	Limits	Decompler: Decompler executable Arguments: {nfie} -o (outfie}.	Browse
Extensions	Shellcode Filters		
Store	Certificates Python		
Wpdate Update	Theme System		
🔀 Settings	Portable HybridAnalysis Intelligence		
About	Ghidra Sample Downloader PYC Decompiler		

Once the external decompiler is set up, accessing the decompiled source code is achievable with just a single click.

C:\Python39\Lib\M		Note Politice	
	ltp/pycache\cookies.cpythos-33	ayıc 68% PYC	
8 Herardiy	🖉 🗶 🔍 Analysis (Byte Co	de: Decompled)	ð
Vame	104 class Cook	(leSrror(Exception):	
cookies contheo.2	105 pars		
- contractive procession	100	a a stales and i testers i stales distants i fistorial a trut	
	100 Upercaped	Charg = LoralCharg + ' ()/c=>28(1))'	
	109 Translate	ar = (lambda .0: pags) WASHING: Decompyle incomplete	
	110) (set (rang	<pre>ge(256)) - set(map(ord, _UnescapedChars)))</pre>	
	111 Translate	ir.update()	
	112 ord(**		
<	> 114 is legal	<pre>key = re.compile('(%s)+' % re.escape(Legalchars)).fullmatch</pre>	
16 mm ber	115		
	116 def_quote	(str):	
intrinsic three	eats 117 11000	ite a string for use in a cookie neader.	
byte code: Deassento	119 If the	string does not need to be double-guoted, then just return the	
Byte Code: Decompile	ed 120 string	2. Otherwise, surround the string in doublequotes and quote	
Privacy	121 (with	a \\) special characters.	
Personal Information	122		
Informatio	In 123 11 913	: 13 SCOR OF _13 Legal_Key(SCF):	
Version Information	125 return	None + str.translate(Translator) + '"'	
	126		
	127 _OctalPatt	<pre># re.compile('\\\\(0-3)(0-7)(0-7)')</pre>	
	128 _QuotePatt	<pre>: = re.compile('(\\\\1.')</pre>	
	120 (at utati	te (str) :	
§ Format	d × 111 if sta	r is None or len(str) < 2:	
HE Objects	122 12	sturn str	
,	133 if Nor	<pre>xe[0] != ''' or str[-1] != ''':</pre>	
	134 19	iturn str	
	135 517 -	inter (a. "a)	
	137 n = 14	m(str)	
	138 res =	0	

... continued from page 9.

4	[aifc.exe] - Cerbero Suite 7.1	_ 🗆 🗙
File Navigation Actions Views Tools Help		
R - 🗈 😰 🦸 P 🛼 🗁 🖬 🖬 🗆 4 🔍 🖗	🗛 🔶 🔶 🏠 🙀 🙀 📡 📰 🗱 # 🚛 100% ? SHA-256 🔹 B37017F923D74AF469926E2C6EED99B329A8B5BB0	CF14F941E2D9I 🐴 🔻
C Roots	a x 🔁 Output	ð ×
# File Risk Format		
1 C:\\aifc.exe 100% (f) PE		
	G. Analysis [Byte Code: Disassembled]	ē ×
Name	1632 ArgCount: 1	^
PyInstaller/pyiboot01_bootstrap.pyc	1633 Posoniyargoount: 0 1634 KewWordbargoount: 0	
PvInstaller/pvi rth subprocess.pvc	1635 LocalCount: 1	
PvInstaller/pvi rth pkgutil.pvc	1636 StackSize: 1	
Pvinstaller/pvi rth multiprocessing pvc	1637 Flags: 0x43 (CO_OPTIMIZED, CO_NEWLOCALS, CO_NOFREE)	
Pyinstaller/nyi rth inspect nyc	1638 Code: b' \x00j\x00S\x00'	
Pyinstaller/sifc.pyc	1649 Constants: (1640 None	
Pulactallar/DVZ_00 pvz/_futurapvc	1641)	
Pylinstaller/PYZ-00.pyz/_iuturepyc	1642 Names: (
Pyinstaller/Pyz-ou.pyz/_aix_support.pyc •	1643 b'_nframes',	
× ,	1644)	
🖸 Summary 🗗 🗧	1645 LocalNames: (
Intrinsic threats	1040 D'SEIL', 1647)	
😪 Byte Code: Disassembled	1648 FreeVars: (
🗣 Byte Code: Decompiled	1649)	
Privacy	1650 CellVars: (
Personal Information		
Information	1652 FileName: D'allC.py	
Version Information	1655 Name: Digethianes	
Version monitation	1655 LineTable: b'x00\x01'	
	1656	
	1657 Disassembly:	
El Format 5 X	1658	
	1659 0 LOAD_FAST 0; p Self	
B Objects	1661 4 RETURN VALUE	
	1662 —	
	1663 ; END OF 'getnframes' CODE	
	1005 , blaife read getnframes!	
	barte_tead.getHiames,	~
Enter Python code here [focus with Ctrl+Alt+.]		
ar		

Files automatically extracted from a PyInstaller executable.

The second package is called PyInstaller Extractor.

PyInstaller is a tool that packages Python applications into standalone executables, compatible with Windows, Linux, and macOS. It works by analyzing Python scripts to discover every import statement and include the appropriate Python files, binaries, and libraries in the executable. Additionally, PyInstaller converts all Python code into bytecode before packaging, enhancing performance and security.

The extractor supports all versions of PyInstaller, all supported file types and automatically identifies PyInstaller generated binaries. It also supports PyInstaller bytecode decryption.

If a PyInstaller binary is not automatically detected, files can be extracted manually using the dedicated action.

	Execute Action Cerbero Suite 7.1	×
Installed Editor		
Show disabled actions		Configure
Filter		
Open New Python Editor		^
Reversing		
API Solver		
Unpacker		
PyInstaller Extractor		
UPX Unpacker		
Views		
Open New Hex View		
Open New Text View		
L		*
	OK Cancel	

Finally, the third package is called Py2Exe Extractor.

py2exe is a Python package that converts Python scripts into executable Windows programs. The tool packages Python bytecode and the necessary libraries into a single executable file, eliminating the need for a Python interpreter to be installed on the client machine. py2exe works by analyzing the imported modules in the Python script and includes them along with a Python interpreter as a part of the generated executable.

NGT EARLY 7 (Fer Line In States)	I W W W W W W W W W W W W W W W W W W W	1148300011900201800000343467#602
28 pols	# x Output	
PIN KAK TOTKA		
Cil., source.exe 100% PE		
Heady 6	* G, Analysis (Byte Code: Deassembled)	,
lane	828 1	
	829 FileName: b'source.py'	
A Districtions	BAG ALLOS D'ODODIAS'	
Py2EveExtractor/Ebrary.zin	532 lineTable: b'\x05\x01\x05\x01\x05\x04\x04\x04\x05\x01\x05\x01\x05\x04\x04\x05	
4 Managed Executables	x06\x01\x06\x01\x06\x1e\x04\x05\x10\x02\x14\x015\x02\x06\x01'	
Py2ExeExtractor/modules.pvc	833 RM Distantichus	
	BIA DIRASHEDIY:	
	636 0 BUILD LIST 0	
	837 2 LORD_CONST 0 / (1, 2, 3)	
	838 4 LITERTEND 1	
house A	• P40 8 LOAD CONST 1 2 (4, 5, 6)	
Summary .	644 10 LINT EXTEND 1	
Intrinsic threats	942 12 BUILD_LIST 0	
byte Code: Disasembled	643 14 LOAD COMST 2 7 (7, 0, 9)	
byte code: Decompted	545 10 DUILDLIST 3	
intermation	646 20 STORE MARE 0 r b'X'	
Version Information	647 22 BUILD_LIST 0	
	646 24 LOBD CONST 3 / 19, 8, 1)	
	50 28 NULLINT 0	
	851 30 LOAD_CONST 4 7 (6, 5, 4)	
	852 32 LIST_EXTEND 1	
	853 34 BUILD LIST 0	
land a second	v 155 38 LI27 EXTEND 1	
G and a	656 40 BUILD LIST 3	
Fill Oplace	857 42 STORE SAME 1 / b'Y'	
	656 44 BUILD LIST 0	

The extractor supports all versions of py2exe and automatically identifies py2exe generated executables.

Collectively, these packages equip reverse engineers with a versatile and powerful toolkit for tackling the varied challenges posed by Python-based applications and executables, making Cerbero Suite an indispensable resource in the realm of Python reverse engineering.

10

MORE ARCHIVES

Since the launch of Cerbero Suite 7, we have significantly expanded our archive support, adding to the already extensive range of formats that were previously available. These packages are available to all licenses of Cerbero Suite.

We have released the RAR Format package.

Supporting the RAR format is crucial in the security field due to its frequent use in deploying malicious files. RAR, known for its efficient compression and encryption capabilities, is a popular choice among cyber attackers for distributing malware. Its ability to compress files significantly and password-protect them makes it a preferred method for concealing harmful payloads.

-			forma .		a si tercopa		
6942847675403566201017033002547	ile 2F85AA64548230C0F573032	KD917EB38 0% (f)	ZIP				
S Heardy 8 :	Q. Analysis (Headers)						
arre	* Reader Type	Beader Offset	Reader Size	Data Offset	Data Size		
🚨 DHL Express Receipt_AW8#21907328	FAR BLOCK MAIN	000000000000000	00000000000000011	000000000000000000000000000000000000000	0000000000000000		
4 Archives	RAR BLOCK FILE	000000000000000000000000000000000000000	0001001001001048	000000000000000000000000000000000000000	24523100100100100		
4 6942847675a03566201d1703	RAR BLOCK SUB	000000000000000000000000000000000000000	00000000000000013	0000000000088924	00100100100100104		
 Executations A B Dill Exercise Research AW 	FAR BLOCK ENDARC	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000008910	0000000000000000		
Images							
E Icon 1 (lang.0)							
4 🚞 Other							
Prototype.DEACT/reso							
Prototype.Electricity.re	header_crc: 21243715	11	^	Offset 0 1 2	34567 8		A9011
Prototype Heat Water	header_size: 74			31 36 37	7E 45 02 03 00 AE	D1 1B 04 80 E0 1C 20	7V.+E
>	block_flags: 3			0100110 A9 77 5E 0100120 65 73 73	20 52 65 63 65 69	48 4C 20 45 78 70 72 70 74 58 41 57 42 23	ess.Receipt ANN
Summary 6	block_extra_size: 11 add mine: 452782			0000000 32 31 39	30 37 33 32 30 35	30 32 28 65 70 65 GA	21907328982.exe.
Online	compress_size: 45278			0000040 03 02 12	A5 95 38 11 05 DA 27 06 50 35 06 DB	. 01 89 D1 49 45 60 05 5 61 06 61 D1 58 40 A7	DTTV. 25
Intelligence: MalwareBazaar	flags: 32768			0000060 43 30 09	1A A4 09 22 A2 24	A9 06 06 10 23 00 22	CD
Intelligence: HybridAnalysis	file size: 471040			0000010 0C 62 2A	3D 02 28 30 8C 02	22 28 08 28 08 CA 33	.b*=.(0**.*3
	model 32			0000000 3F 3F F9	CE TR RF 3C RT C2	SO CE RA RA RA SE EL	
	CRC: 3177094941	2422		OB BE GA GAEOSCO	7E 31 51 EA EA AA	EA AD 5A 20 5D 5E 60	m-105.]^k
Fornat di	file host os: 0			0000080 57 57 28	0r 88 38 g5 75 82	: 1D 08 20 87 63 7C PD	NWJ.B01.
II Headers	orig_filename: b'16L	Express Receipt_AB	8#2190732998	0000000 25 41 58	15 1A 92 19 10 D0	TD 19 10 20 58 40 C1	3A5.5.Y0(2).
DHL Depress Receipt_AW0+21907328	filename: 'Dil Expre	IN Receipt_AND#2190	7320902.exe'	0000020 78 83 10	82 05 A1 E1 64 64	45 CA 96 86 89 20 62	dxbbx
						- 40 13 30 30 70 40 40	

The support includes encrypted archives and the inspection of the format structures.

The XAR Format package: XAR (eXtensible ARchive format) is an archive file format which is used for software installation routines in macOS as well as browser extensions in Safari.

		[xar-1.5.2.xar] - Cerbere	Suite 7.1		_ 🗆 🗙
File Navigation Actions Views Tools Help					
R-02 / 52 C REC	3499W ++ ***	NN EE# 6	0% 7 SHA 256 · 2	IDB8F73AE13EAEC1CSCD6CFC78E0047515380	180A5309568817838688300
E Rors				# * 0.000	
# File Risk Fi	ormat				
1 C:\\xar-1.5.2.mar 0% (f) XAR					
R Heardsy a >	Q Analysis (sar-15.2.sar)				
Name	🔨 🔍 Hex 👘 Test 📊 file Stats 📑 Day	kee			
4 🎧 xar-1.5.2.xar	A 12 A 42 10 10 10 10 10 10				
 Documents 	* * * 1 (x+13.590				
in ser-1.5.2/bist/data.ist	Name	🖬 Overview	Name		Value
 All - La 2ries of reap Las Other 	h Makefleincin	On Here	Name	X0F.C	
sar-1.5.2/lib/budattr.c	In sar.1	In Text	Path	xar-1.5.2/src/sar.c	
xar-1.5.2/lb/filetree.h	100 Marc		Size Cla Tana	20.86 KBs (21382 bytes)	
sar-1.5.2/hb/stat.c		a nono	Detected formed	e nie	
sar-1.5.2/Bylot2.h			Created	sab dic 29 18:49:57 2007 GMT	
sar-1.5.2/lib/darwinattr.h			Modified	sab dic 29 18/49/57 2007 GMT	
xar-1.5.2/Rb/RoxarJa.in.in	~		Accessed	sab dic 29 18:50:53 2007 GMT	
O Surgeries			Group	bbraun	
Online			User	bbraun	
Intelligence: MalwareBazaar			Mode	0664	
Intelligence: HybridAnalysis			Access	100-10-1	
			GID	500	
	_		MDS	Double click here to calculate the hash	
U Fernat d >	•		SHA-1	Double click here to calculate the hash	
Ell Hoader Ell Tar			SHA-256	Double click here to calculate the hash	
B Re					

The support includes inspecting the format's structures.

		[xar-1.5.2.xar] - Cerbero Suite 7.1		_ 0 <mark>×</mark>
File Navigation Actions Views Too	is Help			
H-02 / 54 C B] 4 2, 2 4x + + 2 + 2 + 2 N E E # 6 057 99426 - 2068F	73AE13EAEC1CSCD6CFC78E004	751538018045309568817838688300
2 Roes	_		# * 0.0.0x	6 ×
# File Risk	Fo	wat		
1 C:\\xar-1.5.2.xar 0% (I)	XAR			
R Heardy	a x	C, Analysis (Hes)		# ×
Name	^	Name	Type	^
4 🎧 xar-1.5.2.xar		mar-1.5.2	directory	
 Documents 		mar-1.5.2/11b	directory	
h xar-1.5.2/best/data.esl		mar-1.5.2/lib/fbedattr.c	file	
In xar-1.5.2/test/heap1.asl		war-1.5.2/lib/filetree.h	file	
var.152/db/budattr.c		war-1.5.2/lib/stat.c	file	
sar-1.5.2/lib/fietree.h		war-1.5.2/Lib/hash.c	file	
sar-1.5.2/Eb/stat.c		mar-1.5.2/lib/emt2.h	file	
xar-1.5.2/lib/hash.c		sar=1.5.2/lib/darwinattr.h	file	v
sar-1.5.2/lib/ext2.h		cfile id="3">	8 9 A 8 C D 8 F	ASCES
sar-1.5.2/10/darwhatten		odata> 01001000 78 DA CC 57 S8 6r DA 48	14 78 08 BF 82 60 2A AD	xW[0.H.v]*.
4113210-008780101	>	coffset>20 coffset> 0000000 20 75 28 80 M4 88 6A 02	AA 06 86 30 92 63 83 86	.uje.c.
C Semmery		cmine>9030c/mine> 01001030 BT 33 36 01 92 96 54 EA	EE 6A F3 00 C3 B3 7C E7	.36
Online		carchived-checksum style="sml" 00000040 38 17 9F 71 08 F7 5A 84	47 80 70 78 58 24 57 07	1q8.0.1-[9W.
Intelligence: MalwareBazaar		>le9be2091e725dff4d7b0d9fc24772401e2d384 01001040 AC 37 67 33 D2 FA 92 0A	55 AA E2 46 45 07 99 83	.7g3
Intelligence: HybridAnalysis		<pre>/extracted-checksum style="5041" 01001070 CA 55 51 52 56 45 32 5D >e53012ch66a01d47a0165ea95c816ad2fafd122</pre>	54 49 95 51 90 45 84 28	.ugevs2ltz.g.s.(
			56 E0 EF TC 51 31 4A 9A	.4.#815"101J.
		Cacls 010010A5 47 49 90 84 01 63 18 14	14 EA EE AA 48 93 AA 52	GIcHR
Li Ferriat	8 ×	group::rv- 01001000 11 CD 68 FC 26 69 70 A8	AS 83 0A 1P 0A 38 83 59 61 AZ 92 51 DB 2P 55 D5	9 ((a 0 /7)
El Header		other::r 01001000 58 38 BF 38 78 40 AD A4	30 58 72 0A F3 08 96 85	[>.8x8<^rr
HI TOC		<pre></pre> <pre>01001080 B2 42 3A 55 01 AS 80 1A </pre> <pre></pre> <pre></pre> <pre></pre> <pre></pre> <pre>01001080 B2 42 3A 55 01 AS 80 1A </pre> <pre></pre>	4C F3 18 56 35 A5 60 10 52 D2 DC 78 DC 83 DA A8	.810LWS.`.
BI HIS		cctime>2007-12-29718:49:575c/ctime> 05000100 D3 DB E4 04 A0 E1 2C 48	52 55 TO DD E0 E5 63 22	,HROpc"
		Construction of the second sec		
Sater Fython code here [focus		(PALC+.)		

The AR Format package: The AR archive format, originally devised for Unix systems, serves as a straightforward file archiving tool, combining multiple files into a single archive without inherent compression. It's primarily used in Unix-like environments for storing static libraries ('.a' files), and is also a key component in the structure of DEB packages for Debian-based Linux distributions. Furthermore, the AR format finds its application in the Windows operating system as well, where it is used for '.lib' files.

a lite										onter	
(1) 100 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		Risk	Format								
Citra Andrewski Citra Ci		0%0(I) A0	•								
Heardy	<i>a</i> ×	Q Analysis (He	oders)								
ame	^	Name	. 01	fset	Size		Date		User ID Group	. Node	
Galilla default-mysql-client_1.1.0_all.deb		debian-bin	ary 010	0 80000	0101040	Mon Jan	16 05:18:3	2023	0 0	100644	
Acchives		control.te	r.xz 010	00048 0	0100314	Mon Jan	16 05:18:3	2023	0 0	100644	
 A Gontrolitariaz 		data.tar.x	z 010	1035C 0	0000708	Mon Jan	16 05:19:3	2023	0 0	100644	
 Arctives Arctives 											
- Decompressed)											
/control											
./md5sums	×										
	>										
Summary	* ×	ļ									_
		Offset	0 1 2 3	4 5	4 1 0.04 8	5 9 X			ASCII		
			80 50 21 0	16 00 0	0 00 0	0 00 00	10 7A 04 06	62 .P			
		00000020	EO 27 FF 0	90 SD 4	0 17 0	B BC 1C	7D 01 95 CC	1D ."			
		00000040	4A JE 79 11	42 60 3	U CF I	T 67 0C	10 34 72 91 17 65 DD 63	A5	(Dkge.b.		
		00000050	52 C8 65 94	04 18 4	13 3D 2	A DA 55	or b0 D1 54	06	1V.		
format		00000060	10 KE 57 C	90 20 4	12 17 7 IC 61 7	0 3C 62 5 00 75	51 6F BC 03	23 . 24	<		
Handerr	-	00000080	74 E7 FF 50	EF OF	15 S6 E	5 49 38	46 97 05 3#	C4 t.			
		00000090	A8 21 DC 54	C2 40 5	d or S	7 08 34	20 CD 88 58	55	8T.N.4^.		
		00000000	82 28 62 4	20 90 1	IC 16 8	6 ED 86	15 78 AA CS	82 .0	·····		
		00000000	88 03 C2 11	O3 85 1	5 34 8	6 EO A1	12 B7 24 B4	43	e42.9.C		
		03000000	NA 10 51 JI 10 R2 69 R4	E1 09 0	19 UD A	D BA 95	ED 60 16 00	65	ж		
		00000070	6A 20 BC 34	50 06 3	4 46 0	D FD RC	FD ED 13 C4	89	:\F		
			BO 6D 42 31	44 FC 2	12 75 8	C TD FE	55 97 95 BT	17 .ml	17D. "a.).U		
		000000110	75 55 57 57	27 26 1	1. 14 6						

The **RPM** Format package: The RPM Package Manager (RPM) format is a package management system used primarily in Red Hat-based Linux distributions, including Fedora and CentOS. It is utilized for managing the installation, update, and removal of software on Linux systems. An RPM file contains the software itself, along with metadata about the software such as its version, dependencies, and instructions for installation. This format streamlines the process of software management, providing a standardized approach to handling packages on Linux platforms.

	[7zip-23.01-1-omv2390.aarch64.rpm] - Cerbero Suite 7.1	- • ×
File Navigation Actions Views Tools Help		
尼 • 🖻 🖻 📝 🐎 🍋 🗔 🖬 🖾	🗌 🥔 🛼 🖗 🗰 🌞 🙀 🙀 🙀 🗽 🐂 🗮 📰 🊝 🏭 🐔 10 <mark>567</mark> (548-256) — DOBELEAZCIEOSOEG	701811C180E00E848A609403847570086887981
C Roots	d × Ciona	
# File	Risk Format	
1 C:\\7zip-23.01-1-omv2390.aarch64.rpm	10% (f) RPN	
≪ Herardiy 4	R C, Analysis (Headers)	
Name	1 2/31 "66016556/0145260/65648330/0216048662922062/636696230161104910//"	
4 🚨 7zip-23.01-1-omv2390.aarch64.rpm	a7bfbbb5f490ec2197702f5a6199e50f82a1551dfe5987802cc9123eadb352d6*	
4 🚞 Executables	4 1	
Just/bin/7zz	5 arch: "aarch64"	
4 🚞 Other	6 archive compression: "zito"	
Just/bin/7z	# basenames: [
Just/bin/7pa	9 *7z*,	
Just/bin/7zr	10 "720",	
/usr/bin/p7zip	11 -7337,	
/usr/share/doc/7zip/7zC.bd	13 "pTzip".	
/usr/share/doc/7zip/Methods.txt	14 "7zip",	
/usr/share/doc/7zip/readme.txt	15 "72C.tat",	
/usr/share/doc/7zip/src-history.txt	16 Methods.tat.	
/usr/share/licenses/7zip/License.txt	10 ATCOMPTING THE	
Just/share/licenses/72ip/copving.tet	19 "771p".	
Ausrichane/man/man1/inTrin 1 ret	20 "License.txt",	
	21 "copying.txt",	
G Summary 6	* 12 "pittp.1.tst"	
Privacy	24 hugurl: "https://issues.openmandriva.org"	
2 Metadata	25 buildhost: "instance-20220713-1556-2.openmandrivs.org"	
	26 buildtime: Thu Jul 27 14:46:37 2023	
	27 classdict: [
() Fornat d	25 Try dd.hir res associable the backed margin 1 (rest) densicable	
Ell Headers	linked interpreter (lin/id-linux-sarchid.co.i.	
1.0	BuildID[shal]=15ala4e62f5a34f99c905bce90204733dc88aa64, for 080/Linux 3.10.0,	
	stripped",	
	20 "POSIX shell script, ASCII text executable",	
	31 "directory", 32 "ASTIT text".	

All these packages are seamlessly integrated into the Python SDK, enabling programmatic file extraction without the need to open the user interface. This allows for streamlined and automated processing, enhancing the versatility and efficiency of your workflow.

12

WINDOWS REGISTRY HIVES

We have released the RegHive Format package for all licenses of Cerbero Suite.

🗟 = 🖹 🖹 🦩	🐚 🛃 i 🛙	🗅 🖬 🖸 🖸 🖨 🧍 🗛 🖢 🐝 🖕 🄶 兪	🚖 🚖 🔌 💽 🃰 # 🚛 0% MD	5 • DEAB78FEA	A869FB703435E	86B864F5F6			
Roots					e × 🗟 C	utput			
# File	Ris	sk Format							
C:\\SOFTWA	RE 0%	REGHIVE							
Hierarchy	đ×	C Analysis [SOFTWARE]							
me		0x Hex 🎼 Text 📊 File Stats 📑 Registry							
SOFTWARE		> windows Media Foundation	Name	Туре				Data	
		Vindows Media Player NSS	AccessControl	REG BINARY	99cabade03	00000002000	00000000000	0000000070000	0001000000
		Windows Messaging Subsystem Windows NT	BackOffDelay	REG_DWORD	0x000000A	(10)			
		Windows Photo Viewer	BackOffDelayedNotificationsLimit	REG_DWORD	0x0000000	(0)			
		Windows Portable Devices	BackOffFlushInterval	REG_DWORD	0x00000000	(0)			
		Windows Script Host	BackOffLowDiskThresholdMB	REG_DWORD	0x00000258	(600)			
	``	A mundows search b applications	BackOffLowMemoryThresholdKB	REG_DWORD	0x00010000	(65536)			
		Capabilities		_					
ummary	ш л	CatalogList				066	0.1.0		10077
		Description of the second s	"owner": "S-1-5-80-956008885-34	18522649-1831038044	-1853292631	Offset	0 1 2	3 4 5 6 7	ASCII
		CrawlScopeManager	"group": "S-1-5-80-956008885-34	L8522649-1831038044	-1853292631	00000008	02 00 00 (
		Databases	"dacl": [00000010	00 00 00 0	0 07 00 00 00	
		FileChangeClientConfigs	"ace type": "ACCESS ALL	OWED".		00000018	01 00 00 0	0 00 00 00 00	
		Gather	"flags": {	,		00000020	00 00 00 0		
		A pplications	"OBJECT_INHERIT_ACE	: false,		00000030	00 00 00 (0 01 00 00 00	
ormat	<i>6</i> ×	A Windows	"CONTAINER_INHERIT I	ACE": false,		0000038	02 00 00 0)0	
🔢 Registry		PluginManagers	"INHERIT ONLY ACE":	false					
		Projects	},						
		Indexer	"access_mask": {						
		InstallDirectory	"DELETE": true, "PEAD CONTROL": true						
		PerformanceCounters	"WRITE DAC": true,	· /					
		PHSearchConnectors	"WRITE_OWNER": true						
		ProtocolHandlers	× .						
		< >	<		>				

The keys and values of a Windows Registry hive.

Windows Registry hives. It enables detailed inspection of keys and values, and importantly, provides additional insights by displaying the last modification date and time for each

This package offers enhanced functionality for exploring key. Moreover, it includes the ability to view security access details for each key, offering a comprehensive overview of the Registry's structure and access controls.

MACOS .DS_STORE

We have released the DSStore Format package for all licenses of Cerbero Suite.

					[.[OS_Store] ·	Cerbero	Suite 7.1			
File Navigation Actions Views	Tools Hel	lp ⊐ □ 4 - \$	1 ik ik	(4)	* * * *	SNI I	#	€ 10	% SHA-256 • 43	ASD88300EF1AAD4E003A84E3F073805	4277988686568FB(· · ·
C Roots										< Cupit	
File Risk 1 C:\\.DS_Store 10%	For DSST0	mat XRE									
N Herarchy	0 ×	C, Analysis (Notadata	3							
Name	^	Offeet	10	туре	File N	8798				Value	
 OS_Store 		010029A5	lavp	blob	Android		bytearra	y(b*bpl	ist00\xd8\x01\x02\	x03\x04\x05\x06\x07\x08\t\n\x0b	sids\s13\ng_\x10\x
 Experimental Systems 		A1020100	vðrn	1009	Android		1				
[bwsp] Alarms		01002C38	dscl	bool	Cardboard		False				
E love Alarms		01002057	beap	blob	DCIN		bytearre	y(b*bpl	ist00\xd8\x01\x02\	x03\x04\x05\x06\x07\x08\t\t\x0b	t\x0b\x0e\x0f\x0b]
[bwsp] Android		01002048	dacl	bool	DCIM		raise				
(bvP) Android		01002060	1918	comp	DCIM		24319111	.67			
(kvp) Android		00002070	1897	blob	DCIN		bytearre	y(b'bpl	ist00\xd0\x01\x02\	x03\x04\x05\x07\x00\t\n\x0b	x17D/x11/nF_/x10/x
@ [bwsp] DCIM		01005010	lavp	blob	DCIM		bytearra	y(b*bpl	ist00\xd8\x01\x02\	x03\x04\x05\x06\x07\x08\z\n\x0b	sids/si3/nG_\si0/s
Citing (www.p.c.m.		01003000	noto	date	DCIM		2022-01-	14718:0	9140		
(bwsp) Documents	~	00003028	nodD	date	DCIN		2022-01-	14710:0	9:40		
	>	00003044	ph15	comp	DCIN		24331264	00			
Summary	e ×	01003060	värn	1002	DCIM		1				
Privacy											,
1 Metadata		offset	0	1 2	3 4 5 6 7	8 9 1	всі	0 8 8	ASCII		
			000	0 00 D 5 06 0	C 62 70 6C 69	09 08 0	1 10 DE 0	52 68	bplist00		
		00000020	68.2	7 53 7	4 61 74 75 73	42 61 7	58 53 6	9 68 77	owStatusBar[Show		
Q Froma		00010030	50 6 62 6	1 74 6	8 62 61 72 58 8 53 68 67 72	53 68 6	56 69 6	r 68 60 5 37 5r	Pathbar (ShowTool bar (ShowTaby) ev		
H Parcede		00000050	10 1	4 43 6	r 68 74 61 69	68 65 7	53 68 6	77 53	ContainerShow5		
G		00000040	62 6	4 65 6	2 61 72 50 57	60 6E 6	57 69 6	2 68 75	idebar\WindowBou		
		00000080	58.5	3 68 6	F 77 53 69 64	65 62 6	72 08 0	8 09 08	[ShowSidebar		
			09.5	£ 10 1	9 7B 7B 31 37	34 20 2	32 32 3	3 70 20			

In Apple macOS, .DS_Store is a file that stores custom attributes of its containing folder, such as folder view options, icon positions, and other visual information. It is created and maintained by the Finder application in every folder and contains information that can be valuable for forensics purposes, such as file names and timestamps.

This makes these files a rich source for reconstructing user activities, understanding file access patterns, and providing chronological context in digital forensic cases. Their analysis can reveal subtle but critical details about how a macOS system was used, contributing significantly to the overall forensic investigation process.

When the PList Format package is installed, embedded binary PList objects are automatically extracted.



PCAP & PCAPNG

We have released the PCAP Format package for all licenses of Cerbero Suite.

					[http.pcap] -	Cerbero Suite 7.1					_ □	×
File Navigation Actions Views	Tools Help											
R - 🗈 😰 🤌 🦻 📄		- 🔍 酔 🙀	++ 💰	🗙 🛸 🚖 🖈 ۲	è 📰 📰 #	SHA-256	25A72BDF10339F2C2	29916920C8B9	501D294923	108DE8F29B1	9ABA7CC001AB60D	3
E Roots							6 ×	🖹 Output				6
# File Risk	Format											
1 C:\\http.pcap 0%	PCAP											
8 Hierarchy	🖶 × 🔍 Analysis	[http.pcap]										6
Name	0x Hex	🍉 Text 🚺	File Stats	Packets								
http.pcap	Number	Offset	Size	D	ate	Source	Destination	Protocol	Lenght			
	1	00000018	0000004E	2004-05-13 10	:17:07.311224	145.254.160.237	65.208.228.223	TCP	62	3372 -> 80	[SYN] Seq=9510579	939
	2	00000066	0000004E	2004-05-13 10	:17:08.222534	65.208.228.223	145.254.160.237	TCP	62	80 -> 3372	[SYN, ACK] Seq=290	02183
	3	00000B4	00000046	2004-05-13 10	:17:08.222534	145.254.160.237	65.208.228.223	TCP	54	3372 -> 80	[ACK] Seq=9510579	940 A
	4	000000FA	00000225	2004-05-13 10	:17:08.222534	145.254.160.237	65.208.228.223	HTTP	533	GET /downl	oad.html HTTP/1.1	\nhc
	5	0000031F	00000046	2004-05-13 10	17:08.783340	65.208.228.223	145.254.160.237	TCP	54	80 -> 3372	[ACK] Seq=2902183	380 A
<	> 6	00000365	000005AA	2004-05-13 10	:17:08.993643	65.208.228.223	145.254.160.237	TCP	1434	80 -> 3372	[ACK] Seq=2902183	380 A
2 Summary	8 × 7	0000090F	00000046	2004-05-13 10	17:09.123830	145.254.160.237	65.208.228.223	TCP	54	3372 -> 80	[ACK] Seq=9510584	419 A
Online	<											>
Intelligence: HybridAnalysis	Ethernet	-(=b'\xfe\xff	\x00\x01	x00', # fe:f	^ Offset	0 1 2 3 4 5	6 7 8 9 A B	C D E F	ASC CK Am-	.11		
	src	=b'\x00\x00	\x01\x00\x	00\x00', # 0	00000010	FE FF 20 00 01 00 0	0 00 01 00 00 00	08 00 45 00	pr.ere	E.		
	dat	e=2048, a=IP(00000020	02 07 OF 45 40 00 8	0 06 90 10 91 FE .	A0 ED 41 D0	E@	A.		
	v	=4,			00000030	E4 DF 0D 2C 00 50 3 25 BC A9 58 00 00 4	7 45 54 20 2F 64	61 8C 50 18 6F 77 6E 6C	*XGE	La.P. T./downl		
	h	1=5,			00000050	6F 61 64 2E 68 74 6	D 6C 20 48 54 54	50 2F 31 2E	oad.html	.HTTP/1.		
# Format	8 ×	en=519.			00000060	31 OD OA 48 6F 73 7	4 3A 20 77 77 77	2E 65 74 68	1Host:	.www.eth		
H Packets	i	d=3909,			00000070	05 /2 05 01 0C 2E 0	3 6F 6D 0D 0A 55 0 4D 6F 7A 69 6C	73 65 72 2D 6C 61 2E 25	ereal.co	mUser-		
	r	f=0,			00000090	2E 30 20 28 57 69 6	E 64 6F 77 73 3B	20 55 3B 20	.0. (Wind	ows;.U;.		
	c	f=1,			0A000000	57 69 6E 64 6F 77 7	3 20 4E 54 20 35	2E 31 3B 20	Windows.	NT.5.1;.		
	п	ffset=0			000000B0	65 6E 2D 55 53 3B 2	0 72 76 3A 31 2E	36 29 20 47	en-US;.r	v:1.6).G		
	t	tl=128,			00000000	65 63 6B 6F 2F 32 3	0 30 34 30 31 31	33 OD OA 41	ecko/200	40113A		
	1	=6, # TCP			0000000000	61 70 70 60 69 62 6	0 /4 00 /8 /4 2E 1 74 60 6E 6E 2E	78 6D 6C 2C	ccept:.t	ext/xml,		
	9	um=36880,	# 0x9010		000000F0	61 70 70 6C 69 63 6	1 74 69 6F 6E 2F	78 68 74 6D	applicat	ion/xhtm		
		rc=b'\x91\x	fe\xa0\xec	* 65 200 220	00000100	6C 2B 78 6D 6C 2C 7	4 65 78 74 2F 68	74 6D 6C 3B	l+xml,te	xt/html;		
	<	SC-D A(XOU)	New YRUL .	# 03.200.220	*							
	11.											

The packets captured in a PCAP file.

The PCAP format is the main capture file format used in TcpDump/WinDump, snort, and many other networking tools and is fully supported by Wireshark/TShark. Our support does not aim to compete against a specialized tool like Wireshark, but it gives the capability to inspect PCAP files without leaving the Cerbero Suite interface. This is especially useful when analyzing malware reports.

For example, the HybridAnalys Intelligence package allows to download sandbox artifacts by clicking on the 'Job ID' in the report.

				[pcap_mw.gz] - Cer	bero Suite 7.1 -	• ×
File Navigation Actions Vie R • D R • D P	ns Tools Help	2 w + + 4 +	* 5	N EE # 6	94-26 · 265265747028644068349676340701606944766667622316066	a A
IF File 1 1 Cit_n1pcap_mw.gz 1009	tisk Fernat 6 62					
N Herarday # *	C, Analysis (Intelligence: Hybrid	Analysia)				
Name	Хау				Value	
* 🚨 pcap_mw.gz	URL	https://www.hybrid-a	nelysis	.com/sample/2b52b547	47fd26caa80e83469efbcb3acfd1b30689a7e696dfc472e31606	
A Documents	700 ID	655011538416e0870708	1504 (5	andbox report files)		
[decompressed]	Submit Name	0c6224c72c45ad8b0c21	5974742	la46d		
	Size	45.5 XDg (87552)				
	Type	doc, office				
	Description	Composite Document F	11e V2	locument, Little End	ian, Os: Windows, Version 6.2, Code page: 949, Autho.	
	Melware Family	VEA.Maldede.4.35AF20	ec.			
< >	Analysis start Time	wed Nov 22 08:53:39	2023 eM			
Summery # *	Verdict	MALICIOUS				
Online	Antivirus Detection	73				
Dualy	Threat Score	100				
Q VBA Code	Threat level	2				
G Foreign Data						
Privacy	Signatures HETRE Attack	s Submissions Hashes	250N			
(il format e x	30	**	î	Name	Value	_
El Header	Creates mutants			Threat Level	INCOMPTIVE	_
Directories	References Windows f	ilepaths for ILLs (Created Mitant	>
 Root Entry 	loads modules at run	time		*\ToneVersel(hische	1777FF80-1321-4734-6671-706046993504*	
El trable	Requested access to	a system service		*Local\300:6310:3	14:Wilstaging_02*	
H WordDocument	Contains embedded VL	A macros (normalize.		*Local\SMD:6310:1	20:WilError_01"	
El \1CompOb)	Drops files marked a	s clean		*Local\DomesLocke	icacheCounterMatex*	
H \SSummaryInfor	Matched Compiler/Pac	ker signature (DIR)		*x64 1000 ACBPIDS	8-1-5-5-0-209073" France 01"	
4 Macros	Contains embedded VL	A mecros	-	*x64 10MU ACB10 5	-1-5-5-0-209073*	
Enter Python code here						

By selecting 'PCap', the associated PCAP data is automatically downloaded and added to the project as a child object.

4	Select an item Cerbero Suite 7.1	×
Dropped files Memory strings PCap		
	OK Cancel	

It is now possible to directly inspect the generated traffic without leaving Cerbero Suite.

					[pcap_mw.gz]	Cerb	ero Suite 7	л.												2
File Navigation Actions Views Too	is Help	- 8, 2 W	++ +	****	NEE#	c 3	9% SHV25	6	• 08	00084	20050	ECOFRO	FFF002	56660	7935	IFA87380	478870	VEB3423A08	49621	
L Roots												(k)	Output							ä
IF File Risk 1 Citalprop.awagz 100%	Format 62																			
t Heardy #	A ANALYSIS	[decompressed]	0																	1
Name	0xHex	It Test	Fie Stats	E Packets																
# 🎧 pcap_mw.gz	Number	Offeet	Size		Date		Seurce				tion	r.	otocol	Le	inght					
 Documents documents 	1791	00038890	00000052	2023-11-22	08:54:29.081040	192.3	65.241.20	6	192.3	41.24	1.24	TCE		66		49709	-> 50	(513) Dog-	-3934165	
4 Archives	1792	4003A882	00010052	2023-11-22	08156129.081507	192.:	69.240.24		192.1	68.24	1.206	TCR		66		80 ->	49709	(838,808)	zeq=319	30
4 🚨 (pcsp)	1793	00033924	00030046	2023-11-22	08:56:29.081598	192.3	69.241.20	6	192.1	41.24	1.24	205		54		49759	-> 80	(ACE) Sequ	-1914005	11
4 🚞 Other	1794	0003A97A	00000085	2023-11-22	08:54:29.081756	192.3	65.241.20	6	192.3	41.24	9.24	3173	2	165		GET /	connect	tept.txt 3	\$777/1.1	N
[decompresse	1795	4003AA27	0001040	2023-11-22	08156129.082107	192.0	69.240.24		192.1	68.24	1.206	102		60		80 ->	49709	(ACS) req-	-3193898	36
	> 1796	0003AA79	000300000	2023-11-22	08:56:29.097478	192.3	69.240.24		192.1	41.24	1.206	205		204		80 ->	49709	(POSE, ACE)) Seq=21	23
karmany *	1797	0003A857	000380A7	2023-11-22	01:54:29.099695	192.3	65.240.24		192.3	41.24	1.206	TCE		151		80 ->	49709	(FIN, FOSH,	ACK) Se	4-
Online	1798	4003A88%	00031046	2023-11-22	08156129.059729	192.0	68.241.20	6	192.1	68.24	9.24	102		- 54		49769	-> 80	(NCR) Red-	+3934165	25
📦 Intelligence: HylaridAnalysis	1799	0003A044	00030046	2023-11-22	08:56:29.099999	192.3	69.241.20	6	192.1	41.24	1.24	205		54		49759	-> 80	[FIN, ACR]	Seq=192	40
	1800	0003AC8A	00000040	2023-11-22	08:54:29.100230	192.3	65.240.24		192.1	41.24	1.206	TCS		60		80 ->	49709	(ACK) Sequ	-3193099	18
	d	sport=4970	s.			^	offset 00000000	0	1 2	3 4	5 6 3F 01	7	8 9 AS 00	A 8	C AS 0	0 6 8 8 0 60 03	16	A9C11		
d forrat		dport=80, Anno393400	\$183.				00000010	00	50 56	91 28	04 08	00	27 81	20 20	08.0	0 45 00	.19.		Σ.,	
Ell Packets		ack=319303	18940,				46003630	20	18 C2	20 40	51 EA	10	60 3r	DE SI	02 5	C 50 18	1.00	P.1'7-8	6	
		flags=24.	+ 708LA	CX.			00000040	00	15 26	A2 00	00 47	45	54 20	20 63	41.6	E 6E 65		.GET./com	36	
		win=2052,				- 64	00000000	31	25 31	00 64	43 67	33	68 65	63 74	49.6	r (E 3)		Connectio	a:	
		urp=0,	• 18004	14			55003570	20	43 60	68 73	65 00	40	\$5 73	65 72	20.4	1 67 65	.clo	eOser-A	ge	
		opto-bytes	reay (b**1				00003590	52	49 GD	CA 48	4P 73	24	38.25	12 11	27.2	\$ 60 73	31	lost:.vwv.	na l	
	Close\r\	ndser-Apent	i Microso	ft NCS3/r/m	ost: www.msftcom	e l	04100031	64	14 63	67 65	65 65	63	74 74	65 72	74.2	E 63 41	ftcor	mecttest.	00	
						× .														
	N					/														

Additionally, the package adds support for the PCAPNG format. The PCAP Next Generation (PCAPNG) format is an enhanced version of the traditional PCAP format, offering features like capturing traffic from multiple interfaces, higher timestamp resolution, support for additional metadata and customizable options, and enriched capture information about the network environment.

TIPS & TRICKS

SINGLE FILE SCAN

To open the main file more quickly when dealing with a file containing numerous embedded files, you can use the "Skip embedded files" option. This allows you to postpone the scanning of the embedded files, speeding up the initial opening process. Although their scanning is delayed, you retain full access to these embedded files in the UI and can initiate their

REGISTRY HIVES VIA PYTHON

Windows Registry hives are fully integrated into Cerbero Suite, offering support both through the user interface and the Python SDK. The latter approach is particularly beneficial for creating versatile plugins for malware scanning and artifact detection. To illustrate, here's a concise example demonstrating how to access keys and values using Python:

```
from Pro.Core import *
from Pkg.RegHive import *
def parseRegHive(fname):
    c = createContainerFromFile(fname)
    if c.isNull():
```

individual scans whenever you choose to explore them.

	Cerbero Suite 7.0											
Scanning	Cancel Skip embedded files											

<pre>return # retrieve the root key key = obj.GetRegKey() print(key.Name()) # enumerate sub-keys for subkey in key.IterateSubKeys(): print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	<pre>return obj = RegHiveObject() if not obj.Load(c) or not obj.Parse():</pre>
<pre># retrieve the root key key = obj.GetRegKey() print(key.Name()) # enumerate sub-keys for subkey in key.IterateSubKeys(): print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	return
<pre>key = obj.GetRegKey() print(key.Name()) # enumerate sub-keys for subkey in key.IterateSubKeys(): print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	# retrieve the root key
<pre>print(key.Name()) # enumerate sub-keys for subkey in key.IterateSubKeys(): print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	key = obj.GetRegKey()
<pre># enumerate sub-keys for subkey in key.IterateSubKeys(): print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	<pre>print(key.Name())</pre>
<pre>for subkey in key.IterateSubKeys(): print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	# enumerate sub-keys
<pre>print(" ", subkey.Name()) # enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	<pre>for subkey in key.IterateSubKeys():</pre>
<pre># enumerate values for each sub-key for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	<pre>print(" ", subkey.Name())</pre>
<pre>for v in subkey.IterateValues(): print(" ", v.name, v.value_type,</pre>	<pre># enumerate values for each sub-key</pre>
<pre>print(" ", v.name, v.value_type,</pre>	<pre>for v in subkey.IterateValues():</pre>
\hookrightarrow v.value)	<pre>print(" ", v.name, v.value_type,</pre>
	\hookrightarrow v.value)

PDF SDK DOCUMENTATION

Navigating the intricacies of PDF manipulation is now easier, thanks to the comprehensive documentation of our PDF module. This provides invaluable help to developers that want to parse PDF documents using either Cerbero Suite or Cerbero Engine.

Pro.Crypto – Crypto API	·
Pro.Carbon — API for disassembling and decompiling native binaries	
Pro.8P — Multi-Processing API	
Pro.SiliconSpreadsheet — Spreadsheet macro emulation API	Pro.PDF -
Pro.Package - API for handling packages	Overview
Pro.CAB — API for parsing Microsoft Cabinet files	The pro.ptr mo
Pro.CertSficates — API for parsing certificates	PDF Parsi
Pro.crat — API for parsing legacy Office documents	The following co
Pro. Class - API for parsing Java Class	document:

+ marker → API for parsing PDF documents
 Pro.PDF → API for parsing PDF documents
 Overview
 The reverse module contains the API for parsing PDF documents.
 PDF Parsing
 The following and
 Proceeding and
 Proc

ARRAY VALUES EXTRACTION

It is often necessary the raw values from a numerical text array, such as: 0x01, 0x02, 0x03, etc.

A Herardy P		a,	Analys	n (shek	ode)		3 8		Ť	noix free			2 2			nter	0	
Name		1 0x66	0x13,	0:24,	ExEC,	OxFC,	0x85,	0324,	0x75,	0:134,	01229.	CXSE,	Ox33,	OxCO,	0x04,	Cochilly	0x40,	
shelicode		2 (x3) 3 0x30 4 0x46 5 0x56 6 0x33 7 (x0)8	0x88, 0x83, 0x89, 0x85, 0x85, 0x69, 0x61,	0x40, 0x74, 0x06, 0x75, 0x49, 0x08,	5x00, 5x33, 5x75, 5x30, 5x41, 5x41,	OxFR, OxFR, OxFR, OxFR, OxFC, OxFC,	OxTO, OxEL, OxET, OxT4, OxAD, OxER,	0x1C, 0x2E, 0x24, 0x35, 0x03, 0x03,	Coc54, Doc15, Coc24, Doc78, Doc78, Doc25, Coc25,	0x10, 0x10, 0x15, 0x15, 0x13, 0x13,	0x76, 0xFF, 0xE4, 0xF5, 0xD0, 0x30,	Decry Decry Decry Decry Decry Decory Decory	0x33, 0x55, 0x51, 0x85, 0x85, 0x85, 0x85,	Ox18, Ox18, Ox19, Ox76, Ox10, Ox10,	0x66, 0x40, 0x89, 0x20, 0x20, 0x20, 0x20,	CocR8, CocR2, CocR2, CocR2, CocR2, CocR2,	0x56, 0x23, 0x21, 0x74, 0x74, 0x56,	
4	>	0 Coc24 9 (co)3 10 Coc20 11 Coc35 12 Coc4A	0x13, 0x10, 0x10, 0x59, 0x40,	0320, 0389, 0370, 0389, 0389, 0365,	5x66, 5x04, 5x0C, 5x98, 5x7F,	Ox88, Ox88, Ox83, Ox89, Ox89, Ox80,	0x0C, 0x03, 0x74, 0xFF, 0x00,	0x40, 0x03, 0x03, 0x07, 0x00,	Dedity Coche, Dedity Coche, Dedity, Dedity,	Ox46, Ox58, Ox88, Ox89, Ox89, Ox83,	CaEC, CaES, CaES, CaES, CaEO,	DecFF, Sect3, Dec53, Sect3, Sect3, Sect3, Sect3,	Cx54, Cx88, Cx88, Cx80, Cx50, Cx50,	0x24, 0x53, 0x08, 0x00, 0x55,	0x00, 0x00, 0x00, 0x00, 0x00,	CocRE, CocRE, CocRE, CocSE, CocSE,	0x10, 0x60, 0x6A, 0x50, 0x15, 0x15,	
Q Summary P	1001	4 CHAT	0454.	darr.	Dot16.	0683.	Gatta.	dans.	facks.	OWER.	01723.	Exc61.	OUTT.	Garry.	darr.	CHEER.	0412.	
Wernings		5 CodEB	Ox72,	0x01,	CodDC,	Coel4,	0x01,	6x00,	Coc00,	OxID,	0x5C,	0x24,	Oxeoc,	0x07,	0x04,	Coc24,	0x72,	
A Possible Shellcode Detected		16 0x65 17 0x2D 18 0x51 19 0x6C 10 0x51 11 0x6A 12 0x03	0x67, 0x73, 0x07, 0x06, 0x6A, 0x6A, 0x60,	0x73, 0x20, 0x44, 0x44, 0x00, 0x53, 0x53,	(9077, 0x53, 0x10, 0x10, 0x10, 0x6A, 0x77, 0x77, 0x02,	0x64, 0x68, 0x00, 0x00, 0x00, 0x56, 0x56,	0x24, 0xF6, 0x77, 0x50, 0x52, 0x54, 0x13,	0x04, 0x00, 0x70, 0x52, 0x57, 0x6A, 0x6A,	0x76, 0x00, 0x62, 0x6A, 0x6A, 0x6A, 0x00, 0x00,	0x72, 0x10, 0x74, 0x74, 0x00, 0x83, 0x83,	0x33, 0xFF, 0xC7, 0xC4, 0xFF, 0xFF, 0xE5, 0xC0,	(932, 0x54, 0x54, 0x30, 0x54, 0900, 0x75,	0x07, 0x0C, 0x1D, 0x14, 0x53, 0x53,	0x44, 0x85, 0x65, 0x85, 0x87, 0x87,	0x24, 0x25, 0x28, 0x10, 0x00, 0x56, 0x56,	(w)#, 0x33, 0x64, 0x04, 0x75, 0x04, 0x75,	0820, Osc59, Os41, Os41, Os43, Os43, Os43, Os43,	
Li Porrat •	×	13 0x75 14 0x3E 15 0x46 16 0x2E 17 0x61	0xEC, 0xEC, 0x19, 0x11, 0x11, 0x1F,	0x6A, 0x90, 0x36, 0x32, 0x40,	0000, 0xFE, 0x1A, 0x31, 0x6F,	Ox68. Ox88. Ox87. Ox28. Ox28. Ox60.	0xFE, 0x0E, 0x70, 0x32, 0x65,	0x09, 0x09, 0x59, 0x33, 0x22,	0x56, 0x8F, 0x74, 0x31, 0x77,	0x88, 0x81, 0x74, 0x2E, 0x2E,	0x20, 0x20, 0x70, 0x31, 0x31,	0x30, 0x33, 0x38, 0x38, 0x58,	0xFE. 0x2R, 0x2F, 0x38, 0x70,	0xFF, 0xEA, 0x2F, 0x2F, 0x2F,	0x50, 0x50, 0x51, 0x54, 0x54,	CochE, CochE, CochE, CochE, CochE, CochE,	0x48. 0x06. 0x19. 0x14. 0x14.	

The "convert/from_array" filter is an incredily useful tool that performs this task for us. It automatically detects separators

and the radix of the values. Additionally, the radix, the size, and the endianness of the values can all be configured.



Knowing how to use this tool can save you a considerable amount of time!



If you have any questions, feel free to contact us at: info@cerbero.io

You can follow us on X to be notified about the latest updates!

CERBERO LABS