Case 2023-01-23 12-43-50 Table of Contents

OSForensics
by PassMark Software

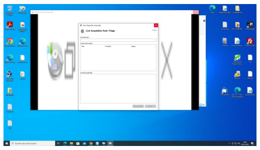
Case Report: '2023-01-23 12-43-50'

Case Name:	2023-01-23 12-43-50
Report Date:	23/01/2023, 12:52:32, GMT +1:00 Central European Time

CASE SUMMARY

This report was automatically generated by Auto Triage

Attachments

Case Item ID	Title	Filename	Preview	Date Added (GMT +1:00)	Additional Details
3	Screen Capture	2023-01-23 11-46-57 Fullscreen.png		23/01/2023, 12:46:57	**Notes:** Auto-generated by Auto Triage
10	File Listing	2023-01-23 11-46-53 FileListing.csv		23/01/2023, 12:51:49	**Notes:** Auto-generated by Auto Triage

Case Activity Log

Date	Level	Module	Investigator	Description
23/01/2023, 12:51:39	Minor	Create Signature		Signature creation completed
23/01/2023, 12:50:58	Minor	User Activity		User Activity Scan completed (MRU: 1047 - Chat: 0 - Event: 33996 - USB: 261 - WLAN: 0 - Cryptocurrency: 0 - BAM: 88 - AntiForensics: 0 - Cookie: 0 - Download: 201 - URL: 2963 - SearchTerm: 483 - Login: 9 - Bookmark: 5 - Custom Dictionary: 0 - Install: 708 - AutoRun: 16 - Mounted: 4 - UserAssist: 261 - JumpList: 1511 - Prefetch: 0 - Clipboard: 0 - WinSearch: 0 - ShellBag: 546 - MobileBackup: 0 - P2P: 0 - Timeline: 1605 - RecycleBin: 15 - ShimCache: 0)
23/01/2023, 12:50:19	Minor	Deleted Files		Deleted File Search completed on "Drive-C: [Logical Drive (Forensics Mode)]" (28736 deleted files found)
23/01/2023, 12:47:23	Minor	Password Recovery		Failed to retrieve Windows password hashes on "local machine": No previous security permissions have been saved.
23/01/2023, 12:47:22	Minor	System Information		System Information collection on "live system" complete
23/01/2023, 12:46:58	Minor	Password Recovery		Retrieving Windows password hashes on "local machine"
23/01/2023, 12:46:58	Minor	Create Signature		Signature creation started
23/01/2023, 12:46:58	Minor	Deleted Files		Deleted File Search started on "Drive-C: [Logical Drive (Forensics Mode)]"
23/01/2023, 12:46:56	Minor	System Information		System Information collection started on "live system"
23/01/2023, 12:46:52	Minor	User Activity		User Activity Scan started on live machine
23/01/2023, 12:46:52	Minor	Password Recovery		Retrieving browser passwords on "local machine"

Date	Level	Module	Investigator	Description
23/01/2023, 12:43:55	Major	Case Manager		New Case "2023-01-23 12-43-50" saved to "C:\Users\Mañana\Documents\PassMark\OSForensics\Cases\2023-01-23 12-43-50\"

System Information

Case Item ID	Title	Date Added (GMT +1:00)	Additional Details
2	Detect BitLocker	23/01/2023, 12:46:56	**Filename:** SI 2023-01-23 11-46-53.bitlocker.html **Notes:** Auto-generated by Auto Triage
5	System Information	23/01/2023, 12:47:22	**Filename:** SI 2023-01-23 11-47-22.html **Notes:** Auto-generated by Auto Triage

User Activity

Case Item ID	Title	Date Added (GMT +1:00)	Additional Details
9	User Activity Scan	23/01/2023, 12:50:59	**Filename:** UA 2023-01-23 11-46-50.csv **Notes:** Auto-generated by Auto Triage

Deleted File Search

Case Item ID	Title	Date Added (GMT +1:00)	Additional Details
8	List of Deleted Files	23/01/2023, 12:50:19	**Filename:** DF Drive-C 2023-01-23 11-46-53.csv **Notes:** Auto-generated by Auto Triage

Login/Passwords

Case Item ID	Title	Date Added (GMT +1:00)	Additional Details
6	Password/Login Scan	23/01/2023, 12:48:06	**Filename:** PR 2023-01-23 11-48-05.csv **Notes:** Auto-generated by Auto Triage
7	Windows Login - Local Users	23/01/2023, 12:48:06	**Filename:** PR 2023-01-23 11-48-06.local.csv **Notes:** Auto-generated by Auto Triage

Process Snapshots

Case Item ID	Title	Date Added (GMT +1:00)	Additional Details
4	Process List	23/01/2023, 12:47:16	**Filename:** MV 2023-01-23 11-47-16.csv **Notes:** `Auto-generated by Auto Triage`

Memory Dumps

Case Item ID	Title	Date Added (GMT +1:00)	Additional Details
1	Physical Memory Dump	23/01/2023, 12:46:50	`Auto-generated by Auto Triage` **Filename:** PhysMem.0.2023-01-23 11-43-55.memdump.bin

OSForensics Information

Application Name:	OSForensics
Major Version:	10
Minor Version:	0
Build:	1006

Certificate Information

Digital Signature is OK.

Name:	OSForensics (by passmark.com)
Link:	http://www.passmark.com
Issued By:	Sectigo Public Code Signing CA R36
Issued To:	PassMark Software Pty Ltd
Date Signed:	28/Nov/2022 04:18
Serial Number:	3a40f3370808bda1520827090bfa0541
Hashing Algorithm:	SHA 1