

Timestamp	Host	User	PID	Task
06/28/2021 16:57:32	DESKTOP-9H6TMKP	Tyler	7176	New Callback of type apollo with description:
Created by mythic_adr	min at 06/28/2021 16:33:03 U	UTC		
06/28/2021 16:57:32	DESKTOP-9H6TMKP	SYSTEM	5044	New Callback of type apollo with description:
Created by mythic_adr	min at 06/28/2021 16:33:03 I	UTC		
06/28/2021 16:57:33	DESKTOP-9H6TMKP	SYSTEM	4692	New Callback of type apollo with description:
ų ų	min at 06/28/2021 16:33:03 I	JTC		
06/28/2021 16:58:32	DESKTOP-9H6TMKP	Tyler	5708	New Callback of type apollo with description:
• • –	min at 06/28/2021 16:33:03 I	UTC		
06/28/2021 16:58:36	DESKTOP-9H6TMKP	Tyler	8612	New Callback of type apollo with description:
ų ų	min at 06/28/2021 16:33:03 I			
06/28/2021 16:58:36	DESKTOP-9H6TMKP	Tyler	3644	New Callback of type apollo with description:
	nin at 06/28/2021 16:33:03 l			
06/28/2021 19:14:55	DESKTOP-9H6TMKP	Tyler	7176	exit
06/28/2021 19:14:54	DESKTOP-9H6TMKP	SYSTEM	4692	exit
06/28/2021 19:14:55	DESKTOP-9H6TMKP	SYSTEM	5044	exit
06/28/2021 19:14:54	DESKTOP-9H6TMKP	Tyler	5708	exit
06/28/2021 19:14:54	DESKTOP-9H6TMKP	Tyler	8612	exit
06/28/2021 19:14:55	DESKTOP-9H6TMKP	Tyler	3644	exit
06/28/2021 19:28:22	DESKTOP-9H6TMKP	Tyler	7756	New Callback of type apollo with description:
• • –	nin at 06/28/2021 19:07:15 U			
06/28/2021 19:28:38	DESKTOP-9H6TMKP	Tyler	7756	exit
06/28/2021 19:38:25	WORKSTATION5	SYSTEM	3176	New Callback of type apollo with description:
• •	min at 06/28/2021 19:07:15 U		22.40	N. C.III. 1. C II. 'd. I. 'd'
06/28/2021 19:38:35	WORKSTATION5	SYSTEM	3240	New Callback of type apollo with description:
• •	nin at 06/28/2021 19:07:15 U		2240	C-11
06/28/2021 19:39:34 T1106: Native API	WORKSTATION5	SYSTEM	3240	ps_full
06/28/2021 19:38:59	WORKSTATION5	SYSTEM	3028	New Callback of type apollo with description:
Created by mythic_adı	min at 06/28/2021 19:07:15 V	UTC		71 1
Created by mythic_adr 06/28/2021 19:40:13	min at 06/28/2021 19:07:15 WORKSTATION5	UTC SYSTEM	7900	New Callback of type apollo with description:
06/28/2021 19:40:13		SYSTEM		
06/28/2021 19:40:13	WORKSTATION5	SYSTEM		
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17	WORKSTATION5 nin at 06/28/2021 19:07:15 U	SYSTEM UTC SYSTEM	7900	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17	WORKSTATION5 nin at 06/28/2021 19:07:15 WORKSTATION5	SYSTEM UTC SYSTEM	7900	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr	WORKSTATION5 nin at 06/28/2021 19:07:15 WORKSTATION5 nin at 06/28/2021 19:07:15 WORKSTATION5 nin at 06/28/2021 19:07:15 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC	7900 7656 7584	New Callback of type apollo with description: New Callback of type apollo with description: New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20	WORKSTATION5 min at 06/28/2021 19:07:15 WORKSTATION5 min at 06/28/2021 19:07:15 WORKSTATION5 min at 06/28/2021 19:07:15 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber	7900 7656	New Callback of type apollo with description: New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr	WORKSTATION5 min at 06/28/2021 19:07:15 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC	7900 7656 7584 1396	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37	WORKSTATION5 min at 06/28/2021 19:07:15 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM	7900 7656 7584	New Callback of type apollo with description: New Callback of type apollo with description: New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr	WORKSTATION5 min at 06/28/2021 19:07:15 0	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC	7900 7656 7584 1396 5812	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:41:12	WORKSTATION5 min at 06/28/2021 19:07:15 0 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC SYSTEM UTC AllCyber	7900 7656 7584 1396	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:20 Created by mythic_adn 06/28/2021 19:40:37 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn	WORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber	7900 7656 7584 1396 5812 8280	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:41:12 Created by mythic_adr 06/28/2021 19:41:42	WORKSTATION5 min at 06/28/2021 19:07:15 0 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC SYSTEM UTC AllCyber	7900 7656 7584 1396 5812	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:20 Created by mythic_adn 06/28/2021 19:40:37 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:44:49 T1106: Native API	WORKSTATION5 min at 06/28/2021 19:07:15 0 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber UTC SYSTEM UTC SYSTEM	7900 7656 7584 1396 5812 8280 3240	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:41:12 Created by mythic_adr 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33	WORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber	7900 7656 7584 1396 5812 8280	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:41:12 Created by mythic_adr 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API	WORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber UTC AllCyber UTC AllCyber	7900 7656 7584 1396 5812 8280 3240	New Callback of type apollo with description: Pew Callback of type apollo with description: ps_full ps_full
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:41:12 Created by mythic_adr 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API 06/28/2021 19:49:37	WORKSTATION5 min at 06/28/2021 19:07:15 0 WORKSTATION5 MORKSTATION5 WORKSTATION5 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber UTC SYSTEM UTC SYSTEM	7900 7656 7584 1396 5812 8280 3240	New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:20 Created by mythic_adn 06/28/2021 19:40:37 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API 06/28/2021 19:49:37 T1113: Screen Capture	WORKSTATION5 min at 06/28/2021 19:07:15 0 WORKSTATION5 MORKSTATION5 WORKSTATION5 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber UTC AllCyber UTC SYSTEM AllCyber	7900 7656 7584 1396 5812 8280 3240 8280	New Callback of type apollo with description: ps_full ps_full screenshot {"Architecture":"x64","PID":492}
06/28/2021 19:40:13 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:17 Created by mythic_adr 06/28/2021 19:40:20 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:40:37 Created by mythic_adr 06/28/2021 19:41:12 Created by mythic_adr 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API 06/28/2021 19:49:37 T1113: Screen Capture 06/28/2021 19:46:06	WORKSTATION5 min at 06/28/2021 19:07:15 0 WORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber UTC AllCyber AllCyber AllCyber AllCyber	7900 7656 7584 1396 5812 8280 3240	New Callback of type apollo with description: Pew Callback of type apollo with description: ps_full ps_full
06/28/2021 19:40:13 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:20 Created by mythic_adn 06/28/2021 19:40:37 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API 06/28/2021 19:49:37 T1113: Screen Capture 06/28/2021 19:46:06 Created by mythic_adn	WORKSTATION5 min at 06/28/2021 19:07:15 10 WORKSTATION5 MORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC SYSTEM AllCyber AllCyber AllCyber	7900 7656 7584 1396 5812 8280 3240 8280 8280	New Callback of type apollo with description: ps_full ps_full screenshot {"Architecture":"x64","PID":492} New Callback of type apollo with description:
06/28/2021 19:40:13 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:20 Created by mythic_adn 06/28/2021 19:40:37 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API 06/28/2021 19:49:37 T1113: Screen Capture 06/28/2021 19:46:06 Created by mythic_adn 06/28/2021 19:46:06	WORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5 wORKSTATION5 wORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 wORKSTATION5 wORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC AllCyber UTC AllCyber AllCyber AllCyber AllCyber	7900 7656 7584 1396 5812 8280 3240 8280	New Callback of type apollo with description: ps_full ps_full screenshot {"Architecture":"x64","PID":492}
06/28/2021 19:40:13 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:17 Created by mythic_adn 06/28/2021 19:40:20 Created by mythic_adn 06/28/2021 19:40:37 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:41:12 Created by mythic_adn 06/28/2021 19:44:49 T1106: Native API 06/28/2021 19:45:33 T1106: Native API 06/28/2021 19:49:37 T1113: Screen Capture 06/28/2021 19:46:06 Created by mythic_adn	WORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5 wORKSTATION5 wORKSTATION5 WORKSTATION5 WORKSTATION5 WORKSTATION5 wORKSTATION5 wORKSTATION5 min at 06/28/2021 19:07:15 to WORKSTATION5	SYSTEM UTC SYSTEM UTC SYSTEM UTC AllCyber UTC SYSTEM UTC AllCyber UTC SYSTEM AllCyber AllCyber AllCyber	7900 7656 7584 1396 5812 8280 3240 8280 8280	New Callback of type apollo with description: ps_full ps_full screenshot {"Architecture":"x64","PID":492} New Callback of type apollo with description:



Mythic - Timeline

T1083: File and Directory Discovery

T1106: Native API

06/28/2021 19:48:21 WORKSTATION5 AllCyber 8280 download {"File":"C:\\\Users\\\\AllCyber\\\\

Documents\\\AllCyber\\\CoachMacPassword.txt","Host":""}

T1020: Automated Exfiltration T1030: Data Transfer Size Limits T1041: Exfiltration Over C2 Channel