IR-4

분야	포렌식
문제 파일 (zip)	https://drive.google.com/file/d/1KhkiZXagtpBXRQ63et2ZCyDtpvAIko87/view?usp=sharing
배포 완료	☐
출제자	이현

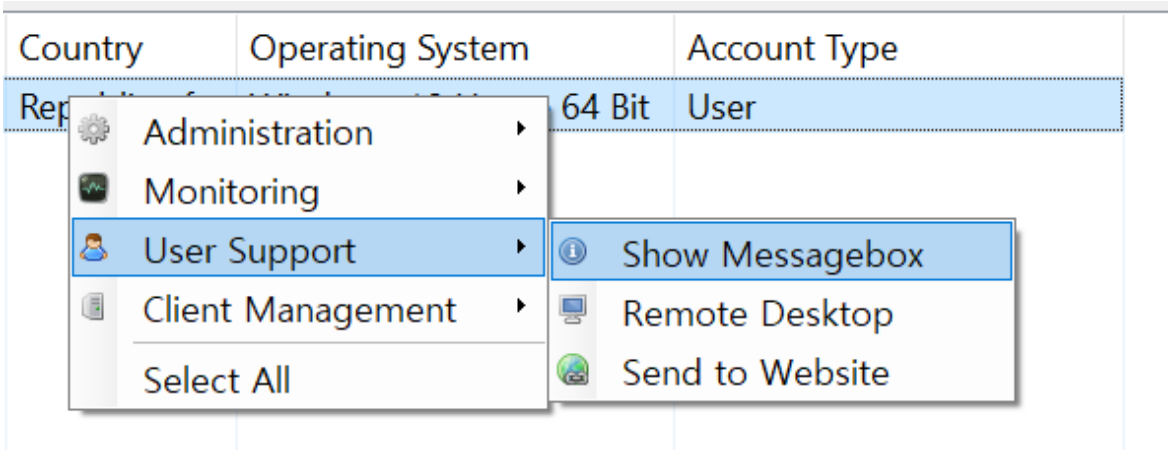
문제

RAT Builder 배포자가 깜짝 메세지를 보냈다고 한다. 메세지를 찾아보자.

답

KEEPER{MessageB0xoxx0xo_0x0xoxxox}

풀이과정



Quasar RAT에서 Show Messagebox 사용

evtx를 보면 MessageBox 뜬 출력 결과를 확인할 수 있다.

254	2024-01-0	7040	Info	Service Control Manager	System	824	7712	DESKTOP-	2	S-1-5-18	Start type of a service has cha	The start type of the Background Intelligent Transf
255	2024-01-0	16	Info	Microsoft-Windows-Kern	System	396	3024	DESKTOP-	2	S-1-5-18		
256	2024-01-0	26	Info	Application Popup	System	2432	3980	DESKTOP-	2	S-1-5-18	Application Error	Caption: KEEPER{MessageB0xoxx0xo_0x0xoxxox}
257	2024-01-0	26	Info	Application Popup	System	2432	2292	DESKTOP-	2	S-1-5-18	Application Error	Caption: KEEPER{MessageB0xoxx0xo_0x0xoxxox}
258	2024-01-0	10016	Warning	Microsoft-Windows-Distr	System	576	2080	DESKTOP-	2	S-1-5-21-266616115-2027809234-2763039858-1001		
259	2024-01-0	16	Info	Microsoft-Windows-Kern	System	7760	4672	DESKTOP-	2	S-1-5-18		