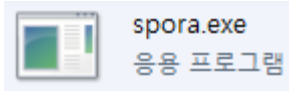


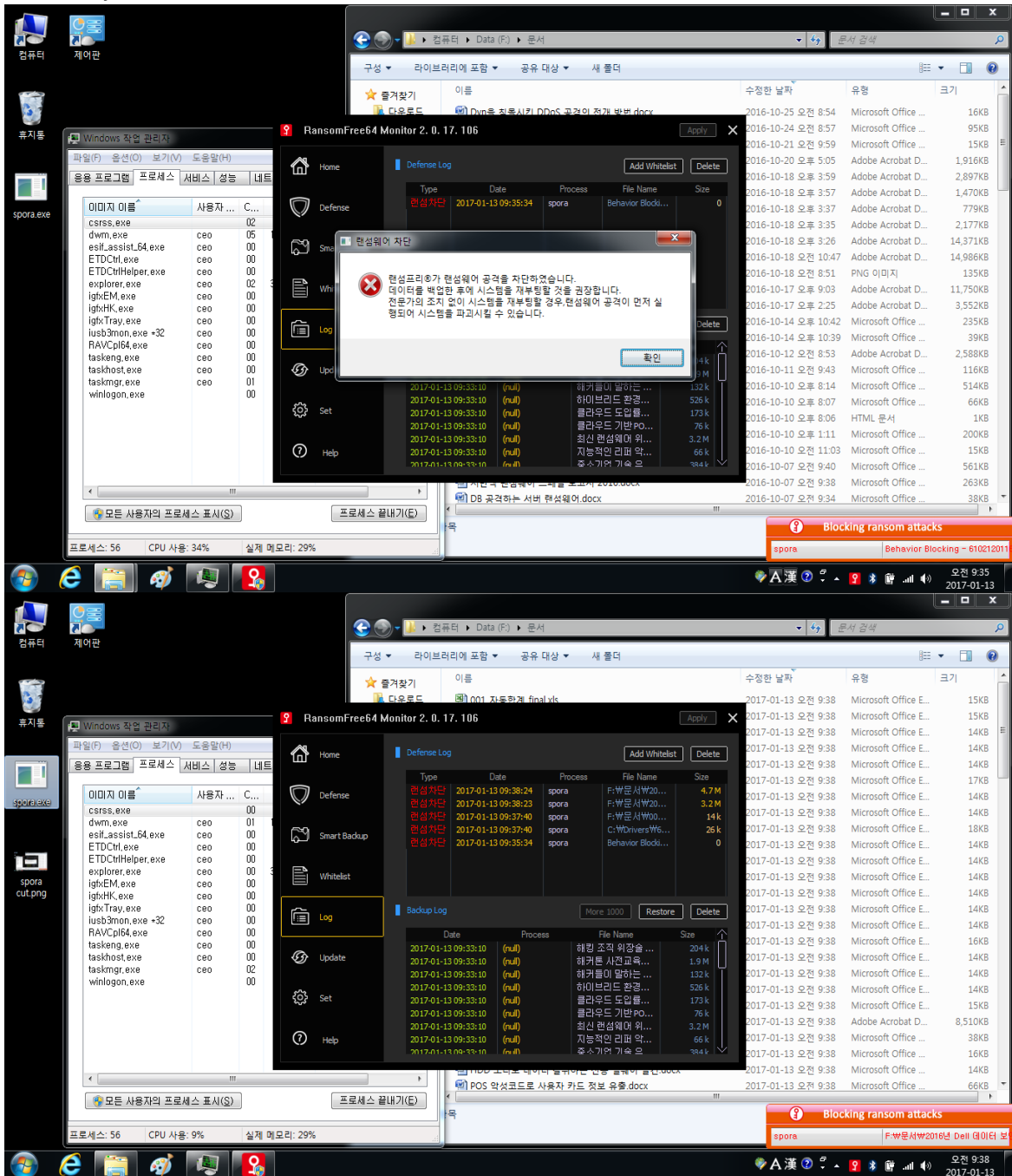
Today's Ransomware - spora

Jan. 13, 2017

1. Filename : spora.exe



2. Blocked by RansomFree®

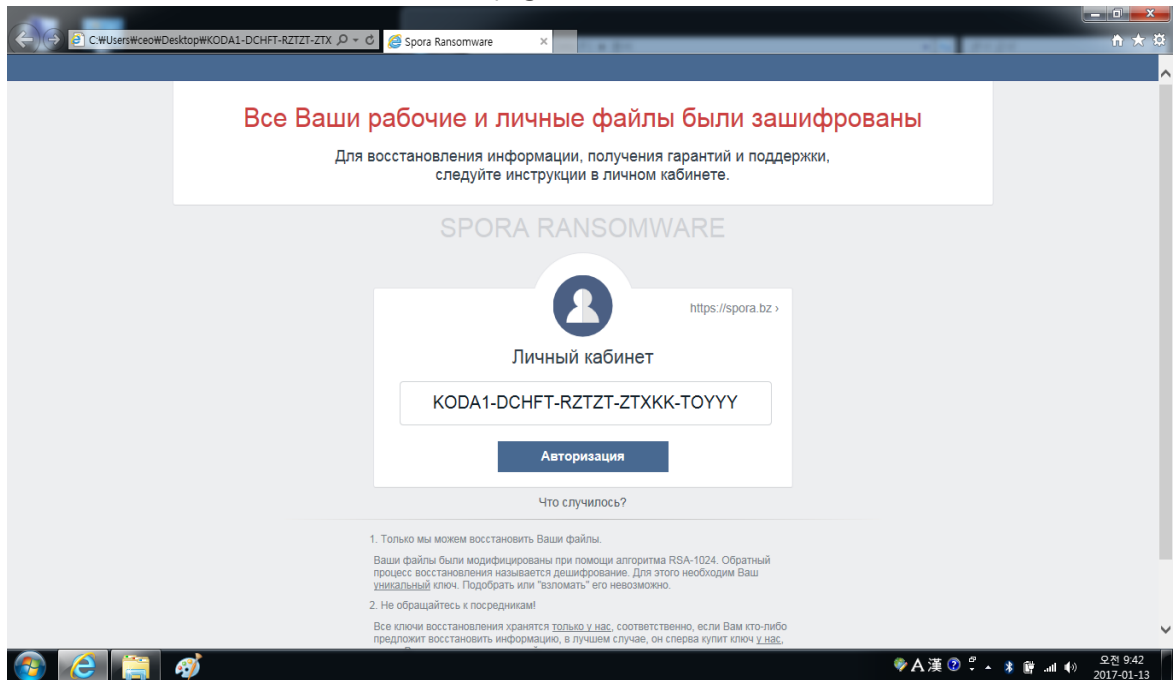


The screenshot displays the RansomFree64 Monitor 2.0.17.106 interface. The 'Defense Log' shows several entries for 'ransom' and 'spora' processes. A dialog box is open, stating: '랜섬웨어가 랜섬웨어 공격을 차단하였습니다. 데이터를 백업한 후에 시스템을 재부팅할 것을 권장합니다. 전문가의 조치 없이 시스템을 재부팅할 경우 랜섬웨어 공격이 먼저 실행되어 시스템을 파괴시킬 수 있습니다.' (Ransomware has blocked ransomware attack. It is recommended to back up data and then restart the system. Restarting the system without professional assistance may cause ransomware attack to occur first, which can destroy the system.) The background shows a task manager window with a list of processes including csrss.exe, dwm.exe, and spora.exe.

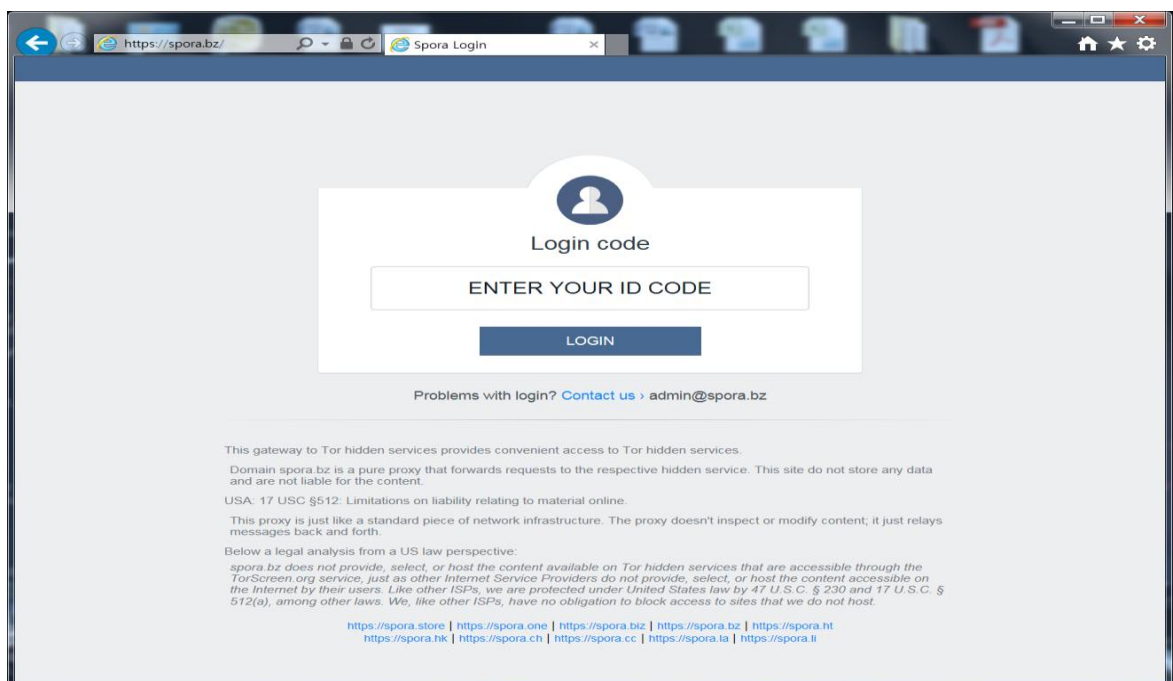
Type	Date	Process	File Name	Size
랜섬차단	2017-01-13 09:35:34	spora	Behavior Block...	0
랜섬차단	2017-01-13 09:38:24	spora	F:\부문서W20...	4.7 M
랜섬차단	2017-01-13 09:38:23	spora	F:\부문서W20...	3.2 M
랜섬차단	2017-01-13 09:37:40	spora	F:\부문서W00...	14 k
랜섬차단	2017-01-13 09:37:40	spora	C:\Drivers\W6...	26 k
랜섬차단	2017-01-13 09:35:34	spora	Behavior Block...	0

3. Victim in case RansomFree® was not installed.

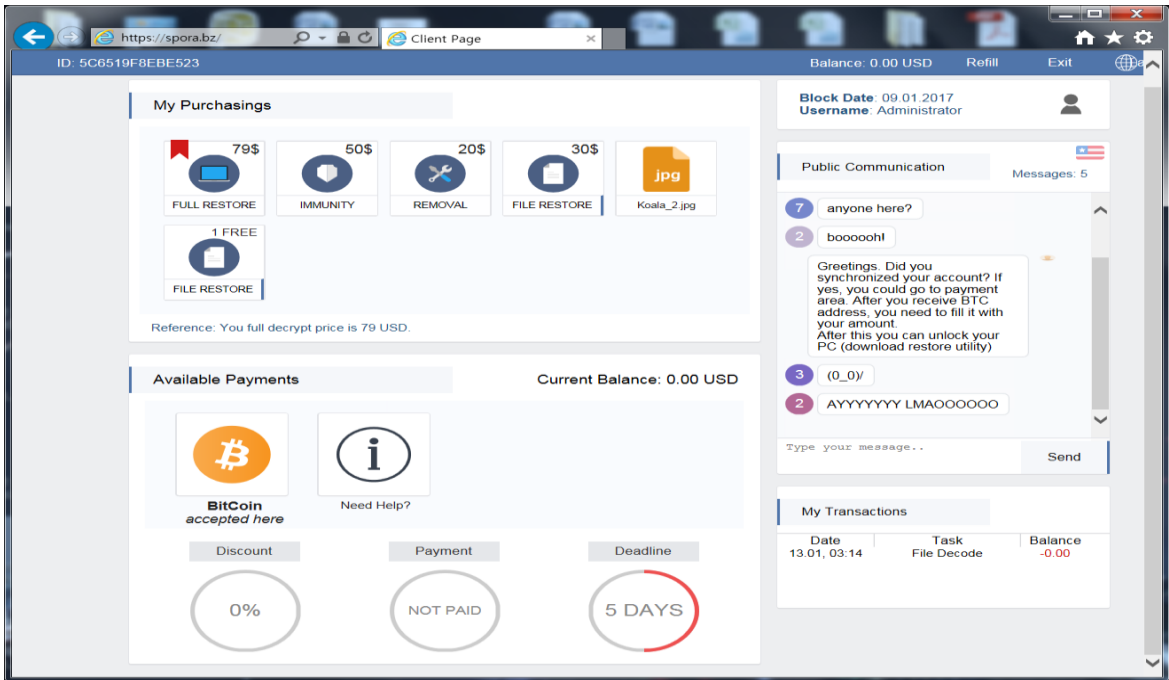
3-1. Issue an ID and drive to their homepage.



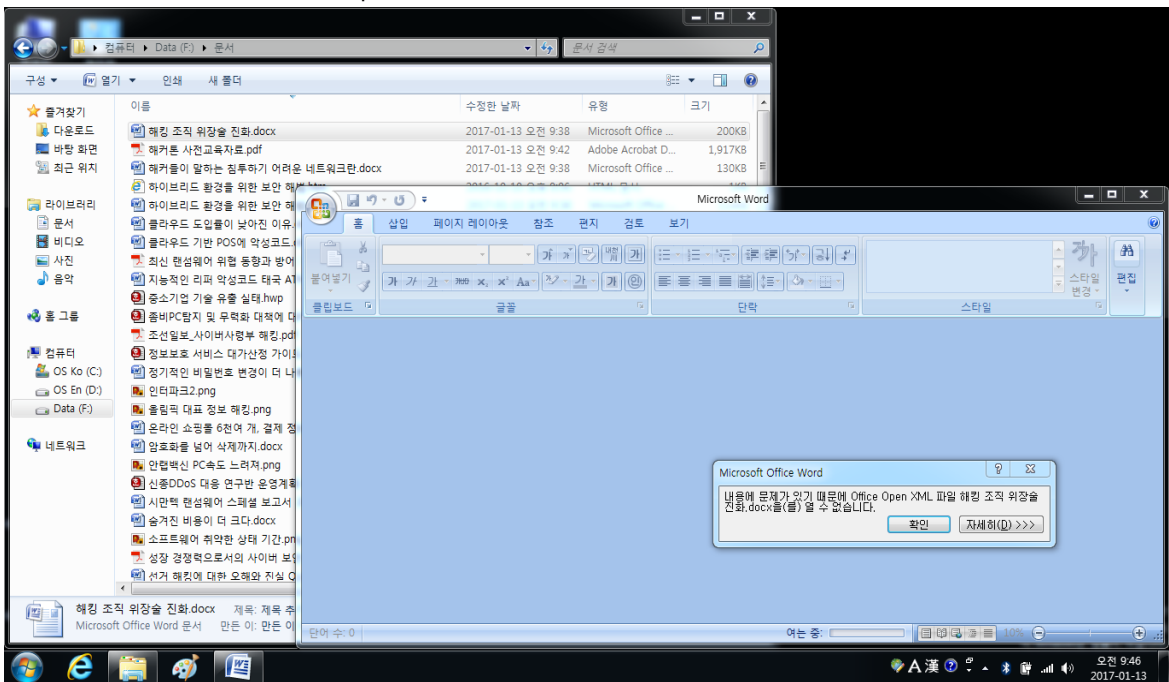
3-2. Enter an ID.



3-3. A payment window opens to induce payment.



3-3. Attacked files were not opened.



The file name and extension does not changed.