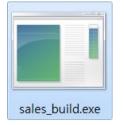
## Today's Ransomware - locked

Dec. 01, 2016

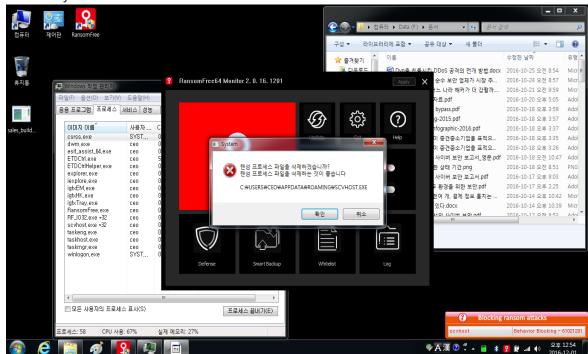
1. Filename : sales\_build.exe



2. Processor name : scvhost.exe

파일단	등 Windows 작업 관리자								
이미지 이름   사용자   C   메모리(   설명     csrss.exe   00   1,784 KB   데스크톱 참 관리자     dwm.exe   ceo   00   12,952 KB   데스크톱 참 관리자     esif_assist_64,exe   ceo   00   6,584 KB   ETD Control Center     ETDCtrl.exe   ceo   00   3,496 KB   ETD Control Center Helper     explorer.exe   ceo   00   3,496 KB   ETD Control Center Helper     igfxEM.exe   ceo   00   3,496 KB   BigfxEM Module     igfxHK,exe   ceo   00   3,808 KB   igfxEM Module     igfxTray,exe   ceo   00   3,956 KB   igfxHK Module     igfxTray,exe   ceo   00   12,414 KB   RansomFree     RasomFree,exe   ceo   00   4,576 KB   Realtek HD 오디오 관리자     RF_IO32,exe +32   ceo   00   768 KB   RansomFree     isskeng,exe   ceo   00   3,024 KB   Scvhost,exe     taskhost,exe   ceo   00   3,024 KB   Yet 스케롤러 엔진     taskhost,exe   ceo   03   4,468 KB   Windows 작업 관리 진자	파일(E) 옵션(Q) 보기(V) 도움말(H)								
csrss,exe     00     1,784 KB       dwm,exe     ceo     00     12,952 KB     데스크톱 참 관리자       esif_assist_64,exe     ceo     00     2,272 KB     데스크톱 참 관리자       ETDCtrl,exe     ceo     00     3,496 KB     ETD Control Center       ETDCtrl,exe     ceo     00     3,496 KB     ETD Control Center       explorer,exe     ceo     00     3,496 KB     ETD Control Center       igfxEM,exe     ceo     00     3,496 KB     Windows 탈색기       igfxEM,exe     ceo     00     3,808 KB     igfxEM Module       igfxTray,exe     ceo     00     3,956 KB     igfxTray,exe       iusb3mon,exe +32     ceo     00     12,444 KB     RansomFree       RAVCpl64,exe     ceo     00     4,576 KB     Realtek HD 오디오 관리자       RF_IO32,exe +32     ceo     00     3,024 KB     Scvhost,exe       taskeng,exe     ceo     00     3,024 KB     Yel 스케롤러 엔진       taskeng,exe     ceo     00     3,024 KB     Yel 스케롤러 엔진       taskeng,exe <td colspan="8">응용 프로그램 프로세스 서비스 성능 네트워킹 사용자</td>	응용 프로그램 프로세스 서비스 성능 네트워킹 사용자								
csrss.exe dwm.exe001,784 KB 12,952 KB데스크톱 참 관리자esif_assist_64.execeo002,952 KB데스크톱 참 관리자esif_assist_64.execeo006,584 KBETD Control CenterETDCtrl.execeo003,496 KBETD Control Center Helperexplorer.execeo0029,108 KBWindows 탑색기igfxEM.execeo003,808 KBigfxEM ModuleigfxTray.execeo003,956 KBigfxTray.exeiusb3mon.exe +32ceo002,216 KBiusb3monRansomFree.execeo001,784 KBRansomFreeRAVCpl64.execeo003,026 KBRansomFreeRF_IO32.exe +32ceo109,824 KBsc/host.exetasknost.execeo003,024 KBsc/host.exetasknost.execeo003,024 KBsc/host.exetasknost.execeo034,468 KBWindows 작업 을 위한 호스트 프로	이미지 이름^	사용자	с	메모리(	설명				
esif_assist_64,exe ceo 00 2,272 KB ETDCtrl,exe ceo 00 6,584 KB ETD Control Center ETDCtrl,exe ceo 00 3,496 KB ETD Control Center Helper explorer,exe ceo 00 29,108 KB Windows 탐색기 igfxEM,exe ceo 00 4,440 KB igfxEM Module igfxTray,exe ceo 00 3,956 KB igfxHK Module igfxTray,exe ceo 00 3,956 KB igfxHK Module igfxTray,exe ceo 00 3,956 KB igfxTray,exe iusb3mon,exe *32 ceo 00 2,216 KB iusb3mon RansomFree,exe ceo 00 12,444 KB RansomFree RAVCpI64,exe ceo 00 4,576 KB Realtek HD 오디오 관리자 RF_IO32,exe *32 ceo 00 768 KB RansomFree Monitor Scyhost exe *32 ceo 00 3,024 KB Scyhost exe taskeng,exe ceo 00 3,024 KB 작업 스케울러 엔진 tasknost,exe ceo 03 4,468 KB Windows 작업 울위한 호스트 프로			00	1,784 KB					
ETDCtrl, exe   ceo   00   6,584 KB   ETD Control Center     ETDCtrlHelper, exe   ceo   00   3,496 KB   ETD Control Center Helper     explorer, exe   ceo   00   2,496 KB   ETD Control Center Helper     igfxEM, exe   ceo   00   4,440 KB   igfxEM Module     igfxHK, exe   ceo   00   3,956 KB   igfxTray, exe     iusb3mon, exe +32   ceo   00   2,216 KB   iusb3mon     RansomFree, exe   ceo   00   4,576 KB   Realtek HD SELS Pela     RAVCpl64, exe   ceo   00   7,88 KB   RansomFree     RAVCpl64, exe   ceo   00   3,024 KB   Realtek HD SELS Pela     raskeng, exe   ceo   00   3,024 KB   scvhost, exe     taskhost, exe   ceo   00   3,024 KB   scvhost, exe     taskhost, exe   ceo   00   3,024 KB   Scvhost, exe     taskhost, exe   ceo   00   3,024 KB   Windows 작업 a 위한 호스트 프 i		ceo	00	12,952 KB	데스크톱 창 관리자				
ETDCtrlHelper,exe   ceo   00   3,496 KB   ETD Control Center Helper     explorer,exe   ceo   00   29,108 KB   Windows 탈색기     igfxEM,exe   ceo   00   3,808 KB   igfxEM Module     igfxTray,exe   ceo   00   3,808 KB   igfxHK Module     igfxTray,exe   ceo   00   3,956 KB   igfxTray,exe     iusb3mon,exe *32   ceo   00   2,216 KB   iusb3mon     RansomFree,exe   ceo   00   12,444 KB   RansomFree     RAVCpl64,exe   ceo   00   4,576 KB   Realtek HD 오디오 관리자     RFL032,exe *32   ceo   00   768 KB   RansomFree   Monitor     scvhost exe   ceo   00   3,024 KB   Scvhost exe   taskeng.exe     tasknost,exe   ceo   00   5,564 KB   Windows 작업 관리자	esif_assist_64,exe	ceo	00	2,272 KB					
explorer, exe ceo 00 29,108 KB Windows 탐색기 igfxEM, exe ceo 00 4,440 KB igfxEM Module igfxHK, exe ceo 00 3,808 KB igfxHK Module igfxTray, exe ceo 00 3,956 KB igfxTray, exe iusb3mon, exe *32 ceo 00 2,216 KB iusb3mon RansomFree, exe ceo 00 12,444 KB RansomFree RAVCp164, exe ceo 00 4,576 KB Realtek HD 오디오 관리자 RF_IO32, exe *32 ceo 00 7,58 KB RansomFree Monitor scvhost, exe *32 ceo 10 9,824 KB scvhost, exe taskeng, exe ceo 00 3,024 KB 작업 스케롤러 엔진 taskhost, exe ceo 03 4,468 KB Windows 작업 관리자	ETDCtrl,exe	ceo		6,584 KB	ETD Control Center				
igfxEM.exe ceo 00 4.440 KB igfxEM Module igfxHK.exe ceo 00 3.808 KB igfxHK Module igfxTray.exe ceo 00 3.956 KB igfxTray.exe iusb3mon.exe *32 ceo 00 2.216 KB iusb3mon RansomFree.exe ceo 00 12.444 KB RansomFree RAVCpI64.exe ceo 00 4.576 KB Realtek HD 오디오 관리자 RF_IO32.exe *32 ceo 00 758 KB RansomFree Monitor <u>scyhost.exe *32 ceo 10 9.824 KB scyhost.exe</u> taskeng.exe ceo 00 3.024 KB 작업 스케롤러 엔진 taskhost.exe ceo 03 4.458 KB Windows 작업을 위한 호스트 프로	ETDCtrlHelper,exe	ceo							
igfxHK,exe ceo 00 3,808 KB igfxHK Module igfxTray,exe ceo 00 2,216 KB igfxTray,exe iusb3mon,exe *32 ceo 00 2,216 KB iusb3mon BansomFree,exe ceo 00 12,444 KB BansomFree RAVCpl64,exe ceo 00 12,444 KB BansomFree RAVCpl64,exe ceo 00 7.68 KB BansomFree Monitor scvhost,exe *32 ceo 10 9,824 KB scvhost,exe taskeng,exe ceo 00 3,024 KB 작업 스케롤러 엔진 taskhost,exe ceo 00 5,564 KB Windows 작업 관리자		ceo							
igfxTray.exe ceo 00 3,956 KB igfxTray.exe iusb3mon.exe ★32 ceo 00 2,216 KB iusb3mon RansomFree.exe ceo 00 12,444 KB RansomFree RAVCp164.exe ceo 00 4,576 KB Realtek HD 오디오 관리자 RF_IO32.exe ★32 ceo 00 768 KB RansomFree Monitor scvhost.exe ★32 ceo 10 9,824 KB scvhost.exe taskeng.exe ceo 00 3,024 KB 작업 스케롤러 엔진 taskhost.exe ceo 00 5,564 KB Windows 작업 관리자		ceo							
iusb3mon.exe +32     ceo     00     2,216 KB     iusb3mon       RansomFree,exe     ceo     00     12,444 KB     RansomFree       RAVCpl64,exe     ceo     00     4,576 KB     Realtek HD 오디오 관리자       RFL032,exe +32     ceo     00     768 KB     RansomFree Monitor       scvhost.exe     ceo     00     3,024 KB     scvhost.exe       taskeng.exe     ceo     00     5,564 KB     Windows 작업 관리자       taskmgr.exe     ceo     03     4,468 KB     Windows 작업 관리자	igfxHK,exe	ceo			igfxHK Module				
BansomFree,exe ceo 00 12,444 KB BansomFree   RAVCp164,exe ceo 00 4,576 KB Realtek HD 오디오 관리자   RFL032,exe +32 ceo 00 768 KB BansomFree Monitor   scvhost exe +32 ceo 10 9.824 KB scvhost exe   taskeng,exe ceo 00 3,024 KB 작업 스케롤러 엔진   tasknost,exe ceo 00 5,564 KB Windows 작업 관리자		ceo							
RAVCp164,exe     ceo     00     4.576 KB     Realtek HD 오디오 관리자       RF_IO32,exe + 32     ceo     00     768 KB     RansomFree Monitor       scvhost,exe + 32     ceo     10     9.824 KB     scvhost,exe       taskeng,exe     ceo     00     3.024 KB     작업 스케롤러 엔진       tasknost,exe     ceo     00     5.564 KB     Windows 작업 관리자									
RF_IO32,exe +32     ceo     00     768 KB     RansomFree Monitor       scvhost,exe +32     ceo     10     9,824 KB     scvhost,exe       taskeng,exe     ceo     00     3,024 KB     작업 스케즐러 엔진       taskeng,exe     ceo     00     5,554 KB     Windows 작업을 위한 호스트 프로       taskmgr,exe     ceo     03     4,468 KB     Windows 작업 관리자									
Scvhost exe     +32     Ceo     10     9.824 KB     Scvhost exe       taskeng,exe     ceo     00     3.024 KB     작업 스케 플러 엔진       taskhost,exe     ceo     00     5.564 KB     Windows 작업을 위한 호스트 프로       taskmgr,exe     ceo     03     4.468 KB     Windows 작업 관리자		ceo							
taskeng.exe ceo 00 3,024 KB 작업 스케플러 엔진 taskhost.exe ceo 00 5,564 KB Windows 작업을 위한 호스트 프로 taskmgr.exe ceo 03 4,468 KB Windows 작업 관리자									
taskhost,exe ceo UU 5,564 KB Windows 작업을 위한 호스트 프로 taskmgr,exe ceo 03 4,468 KB Windows 작업 관리자				9,824 KB	scvhost, exe				
taskmgr,exe ceo 03 4,468 KB Windows 작업 관리자				3,024 KB	작업 스케 술러 엔진				
winlogon,exe UU 2,380 KB		ceo			Windows 작업 관리자				
	winlogon, exe		υu	2,380 KB					
중 모든 사용자의 프로세스 표시( <u>S</u> ) 프로세스 끝내기( <u>E</u> )									
프로세스: 59 CPU 사용: 23% 실제 메모리: 29%									

3. Blocked by RansomFree®



4. Victim in case RansomFree® was not installed

1.0				×
G 🔾 - 📕 🕴	1퓨터 ▶ Data (F:) ▶ 문서 🗸 🗸	☞ 문서 검색	_	Q
구성 ▼ 라이브	[러리에 포함 ▼ 공유 대상 ▼ 새 풀더		iii <b>→</b> 🗍	0
☆ 즐겨찾기	이름	수정한 날짜	유형	-
🚺 다운로드	F0400A20AC0498E347AB6C5180E6CF08BF682209779CA7112FD87BF4DDA51AD7DCA940543A1C9A67E3421B77BAD95BC7337C5DE02E61792Alocked	2016-11-28 오후 2:58	LOCKED 파일	
🌉 바탕 화면	F0400A20AC0498E347AB6C518026CF08BFAB2209779CA7D12FD87BF41DA51AD7DCA940943A1C9AA7E3421B77BAD95BC7337C5DE02E61.locked	2016-11-28 오후 2:58	LOCKED 파일	
🗓 최근 위치	F0400A20AC0498E347AB6C518026CF08BFAB2209779CA7112FD87BF41DA51AD7DCA94094.locked	2016-11-28 오후 2:58	LOCKED 파일	
	6400A20AC0498E347AB6C518026CF08BFA82209779CA7112FD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7337C5DE02E61792A78258C88942F0971	2016-11-28 오후 2:58	LOCKED 파일	Ξ
詞 라이브러리	F0400A20AC0498E347AB6C5180260FCB8FAB2209779CA711EFD878F41DA51AD7DCA9.locked	2016-11-28 오후 2:58	LOCKED 파일	
📑 문서	0400A20AC04982347AB6C9180260FCBBFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477.locked	2016-11-28 오후 2:58	LOCKED 파일	
🛃 비디오	6400A20AC04982347AB6C9180260FCB8FAB2209779CA711EFD87BF41DA51AD7.locked	2016-11-28 오후 2:58	LOCKED 파일	
🔛 사진	6400AE0AC0498E347AB6C5180E6CF0BBFAB2209779CA711EFD87BF41DA51AD7DC6940943A1C9AA7E342A477.locked	2016-11-28 오후 2:58	LOCKED 파일	
👌 음악	6400AE0AC0498E347AB6C5180E60FC8BFAB2209779CA711EF187BF41DA51AD7DCA940943A1C9AA7E342.locked	2016-11-28 오후 2:58	LOCKED 파일	
	D F0400AE0AC0498E347AB6C518026CF08.locked	2016-11-28 오후 2:58	LOCKED 파일	
💌 컴퓨터	0 F0400AE0AC0498E347AB6C518026CF0B8FAB.locked	2016-11-28 오후 2:58	LOCKED 파일	
🌉 OS Ko (C:)	D F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF4DDA51AD7DCA940943A1C9AA7E3421B77BAD95BC7337C5DE02E61792A78258C88942F.locked	2016-11-28 오후 2:58	LOCKED 파일	
👝 OS En (D:)	0 F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA9.locked	2016-11-28 오후 2:58	LOCKED 파일	
👝 Data (F:)	D F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA94094.locked	2016-11-28 오후 2:58	LOCKED 파일	
	6400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940543A1C9AA7E342A477BAD95BC7337C5DE0.locked	2016-11-28 오후 2:58	LOCKED 파일	
👊 네트워크	F0400AE0AC0498E347AB6C518026CF0BBFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C.locked	2016-11-28 오후 2:58	LOCKED 파일	
	6400AE0AC0498E347AB6C518026CF0BBFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7.locked	2016-11-28 오후 2:58	LOCKED 파일	
	D F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342.locked	2016-11-28 오후 2:58	LOCKED 파일	
	6400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7.locked	2016-11-28 오후 2:58	LOCKED 파일	
	F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7337C.locked	2016-11-28 오후 2:58	LOCKED 파일	
	6400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7337C5DE0.locked	2016-11-28 오후 2:58	LOCKED 파일	
	F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD878F41DA51AD7DCA940943A1C9AA7E342A477BAD958C7337C5DE02E61.locked	2016-11-28 오후 2:58	LOCKED 파일	
	D F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7337C5DE02E61792A.locked	2016-11-28 오후 2:58	LOCKED 파일	
	D F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7337C5DE02E61792A78258C8B.locked	2016-11-28 오후 2:58	LOCKED 파일	
	D F0400AE0AC0498E347AB6C518026CF08BFAB2209779CA7D1EFD87BF41DA51AD7DCA940943A1C9AA7E342A477BAD95BC7337C5DE02E61792A78258C8B942F.locked	2016-11-28 오후 2:58	LOCKED 파일	
		<u>2016 11 20 0 ≈ 2.50</u>		+
7871 9				

## All your files have been encrypted.

All your files have been encrypted!	*				
All your documents (databases, texts, images, videos, musics etc.) we that is now on our servers.	ere encrypted. The encryption was done using a secret key				
To decrypt your files you will need to buy the secret key from us. We a	are the only on the world who can provide this for you.				
Note that every 6 hours, a random file is permanently deleted. The faster you are, the less files you will lose.					
Also, in 96 hours, the key will be permanently deleted and there will be no way of recovering your files.					
What can I do?					
Contact us by email telling your ID (below) and wait for us to send the	instructions.				
Contact us by: successl@sigaint.org					
As a proof, you can send one encrypted file, so we will send it back de	ecrypted. Use it as a guarantee that we can decrypt your files. $\mbox{\boldmath $\nabla$}$				
Next Russian Roulette file 5 hours, 58 minutes and 37 seconds Last (0) file deleted:	Time until total 3 days, 23 hours, 58 minutes and 37 seconds				
Your ID: 1.FEAA3310 Got the					
Coboo	See the files I'll get back if I'm a good boy				

The file extension of the attacked files were changed to "locked".