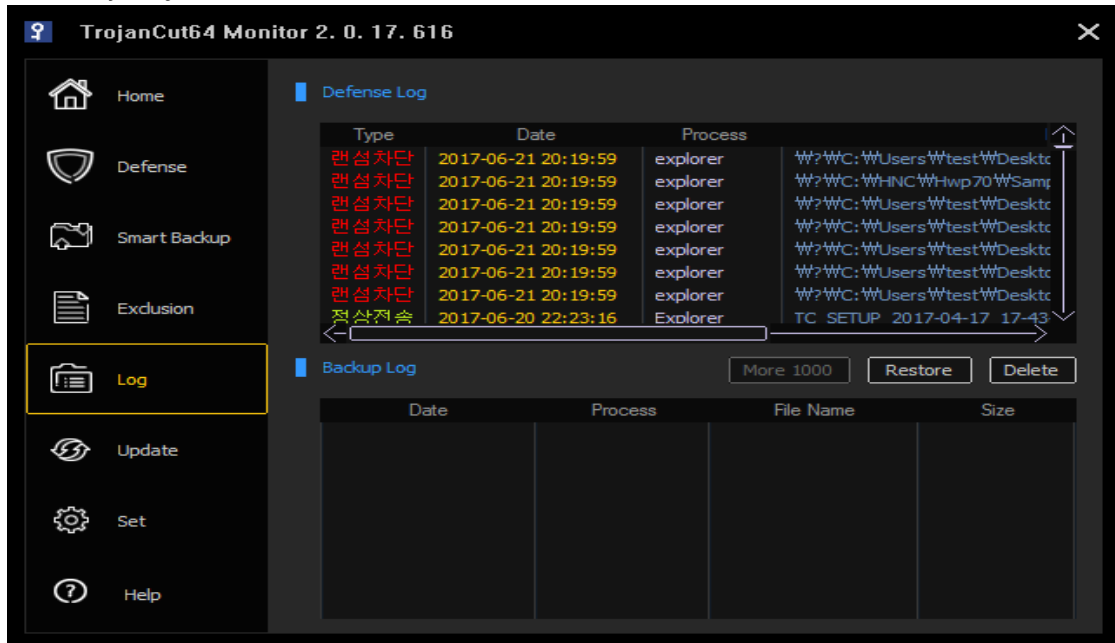


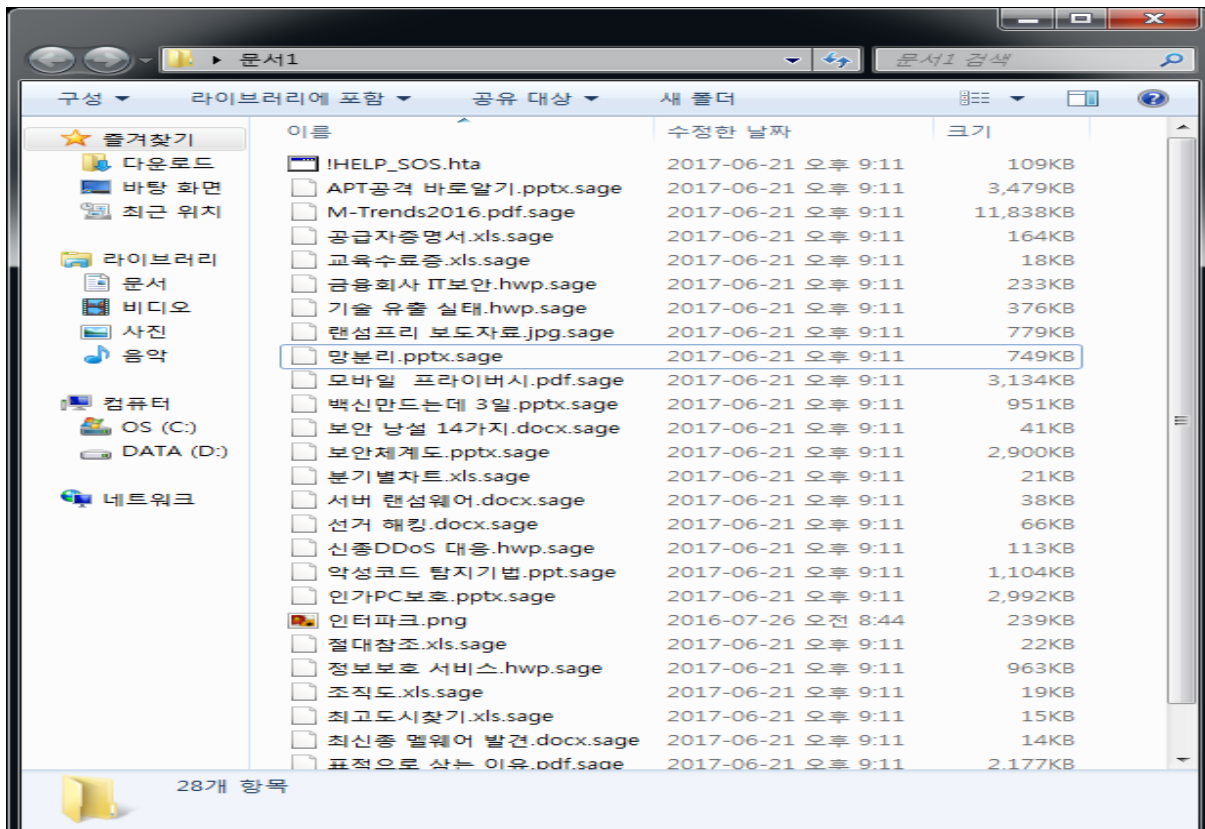
# Today's Ransomware - SAGE 2.2

Jun. 21, 2017

## 1. Blocked by TrojanCut®



## 2. Victim in case TrojanCut® was not installed - All file name's extensions were changed to sage.



### 3. Screen of Victim

The image shows a computer screen with a ransomware message. The top part is a window titled "Decryption Instructions" with a menu of languages: English, Deutsch, Italiano, Français, Español, Norsk, Português, Nederlands, 한국어, Bahasa Melayu, 中文, Türkçe, Tiếng Việt, हिन्दी, Basa Jawa, العربية, and فارسی. The main text in Korean reads: "파일 복구 지침", "파일을 열 수 없으며 일부 소프트웨어가 올바르게 작동하지 않는 것으로 나타났습니다.", "예상대로입니다. 파일 내용은 그대로 있지만 'SAGE 2.2 Ransomware'가 암호화했습니다.", "파일을 잃어 버리지 않으며 해독하여 정상 상태로 되돌릴 수 있습니다.", "당신이 할 수 있는 유일한 방법은 'SAGE Decrypter' 소프트웨어와 개인 복호화 키를 가져 오는 것입니다.", "파일을 복원 할 수 있다고 주장하는 다른 소프트웨어를 사용하면 파일이 손상되거나 파괴 될 수 있습니다.", "SAGE Decrypter 소프트웨어 및 암호 해독 키는 개인 페이지에서 다음을 통해 액세스 할 수 있습니다:", and a URL: <http://7gie6ffnrjykggd.2igu316.com/>.

The bottom part shows a desktop with a ransomware message in green text: "ATTENTION! ALL YOUR FILES WERE ENCRYPTED! PLEASE READ THIS MESSAGE CAREFULLY". It states: "All your important and critical files, databases, images and videos were encrypted by 'SAGE Ransomware'. It uses military grade elliptic curve cryptography, so you have no chances restoring your files without our help! But if you follow our instructions we guarantee that you can restore all your files quickly and safely! We created files with instructions named !HELP\_SOS in every folder with encrypted files. Please be sure to copy instruction text and links to your notepad to avoid losing it". It provides two links: <http://7gie6ffnrjykggd.2igu316.com/> and <http://7gie6ffnrjykggd.17b3o.net/>. A personal key is listed: "Your personal key: AWXYZ7wKwh9w6AHzm\_6UPqRYh9KHZzB3LuHQ8yRF UVZH3PZi\_J8KTWPZX3sglmFjY3VyYWN5liA6IDMw LCAibG9jYXRpb24iDogeyAibGF0iA6IDM3LjUx MTE1MjcsICJsbmciDogMTI3LjAxOTYwMzEgSwg lnN0YXR1cyIlgOiAiT0silH0g". It also mentions "If can't open any of those, you can use 'TOR Browser'" and provides the website <https://www.torproject.org/> and instructions to use TOR Browser to access <http://7gie6ffnrjykggd.onion/>. The desktop taskbar shows icons for a computer, control panel, Oracle VM VirtualBox, folders, recycle bin, WannaCry 2.0.zip.sage, spora.zip.sage, cerber6.zip.sage, sage V2.2.zip.sage, and !HELP\_SOS files. The system tray shows the date and time: "오전 9:26 2017-06-22".