전문적으로 설계된 랜섬웨어 스포라, 강력한 오프라인 암호화와 새로운 지불 방법 제시

공격 및 랜섬프리®에 의한 차단 시연

Lucian Constantin | IDG News Service | 2017.1.12

보안 연구원들이 강력한 오프라인 파일 암호화와 혁신적인 몸값 지불 모델을 제시하는 일명 '스포라(Spora)'라고 하는 새로운 랜섬웨어를 발견했다. 지금까지 이 랜섬웨어는 러시아어 사용자들을 대상으로 했는데, 최근 복호화 포털의 영어 버전을 만들어져 조만간 다른 국가에게로 공격을 확장할 것으로 예상된다.

Credit: Peter Sayer

스포라는 C&C(Command-and-Control) 서버에 연결할 필요없이 파일을 암호화할 수 있으며, 무엇보다 모든 피해자가 저마다의 고유한 복호화 키를 가질 수 있다는 점이 차별점이다.

전통적인 랜섬웨어 프로그램들은 AES(Advanced Encryption Standard) 키를 생성한 다음 C&C 서버에 의해 만들어진 RSA 공개키로 해당 키를 암호화한다. RSA 와 같은 공개키 암호화는 공개키와 개인키로 구성된 키 쌍(key pairs)이 필요하며, 파일이 무엇이든 하나의 공개키는 해당 개인키로만 복호화할 수 있다.

대부분의 랜섬웨어는 한 컴퓨터에 설치된 이후 C&C 서버와 연락해 하나의 RSA 키쌍 생성을 요청한다. 공개키는 컴퓨터에 다운로드되지만 개인키는 절대로 이 서버를 떠나지 않고 공격자의 소유로 남아있다. 이는 피해자가 복호화를 위해 대가를 지불하게끔 하는 핵심이다.

랜섬웨어를 설치한 후, 인터넷 상의 서버에 접속하는 문제는 공격자들에게는 약점이다. 예를 들어, 보안 업체들에게 알려진 해당 서버가 방화벽에 의해 차단된다면 암호화 프로세스는 시작하지 않는다.

일부 랜섬웨어는 오프라인 암호화를 이행할 수 있지만, 모든 피해자는 악성코드에 하드코딩된 동일한 RSA 공개키를 사용한다. 이 방식의 단점은 한 피해자에게 제공한 복호화 도구가 동일한 개인키를 공유한 모든 피해자들에게도 적용된다는 점이다.

보안업체인 엠시소프트(Emsisoft) 연구원들은 "소포라 제작자는 이런 문제를 해결했다"며 이 프로그램의 암호화 루틴을 분석한 내용을 발표했다.

이 악성코드는 하드코딩된 RSA 공개키를 포함하지만 모든 피해자가 로컬로 만들어진 고유한 AES 키를 암호화하는데 사용된다. 이 AES 키는 개인키를 암호화하는데 사용된다. 달리 말하면, 스포라 제작자는 지금까지와는 다른 랜섬웨어가 이행해 온 작업에다가 두번째 AES 및 RSA 암호화를 추가했다.

피해자가 몸값을 지불하길 원한다면 공격자 지불 웹사이트에 그들의 암호화된 AES 키를 업로드해야 한다. 그러면 공격자들은 자신의 마스터 RSA 개인키를 사용해 이를 복호화하고 피해자에게 돌려줄 것이다. 복호화 툴은 번들로 제공되는 듯 하다.

이 복호화 툴은 피해자 만의 RSA 개인키를 복호화한 다음, 해당 키를 사용해 파일을 복호화하는데 필요한 파일별 AES 키를 복호화한다. 이런 방법으로 소포라는 C&C 서버 필요없이 운영할 수 있으며 모든 피해자에게 적용될 수 있는 마스터 키가 드러나는 것을 피할 수 있다.

엠시소프트 연구원들은 한 블로그에서 "불행하게도 소포라가 자체 암호화를 이행한 이후에는 악성코드 제작자의 개인키에 액세스하지 않고 암호화된 파일들을 복원할 수 있는 방법이 없다"고 말했다.

피해자에 따라 다른 몸값을 요구하는 모델
또한 소포라는 여타 다른 랜섬웨어 운영과도 차이가 난다. 예를 들어, 제작자는 피해자의 다양한 유형에 따라 다른 몸값을 요구할 수 있는 시스템을 구현했다.

피해자가 지불 웹사이트에 업로드해야 하는 암호화된 키 파일들에는 감염된 컴퓨터에서 악성코드가 수집한 식별 정보들이 들어있다. 이는 공격자가 특히 기업들을 표적으로 소포라 배포 캠페인을 시작하면 그들은 해당 캠페인의 피해자들이 복호화 서비스를 사용하려고 할 때를 알 수 있다는 걸 의미한다

이를 통해 소비자 또는 조직의 수에 따라, 또는 다른 지역의 피해자들에게 자동적으로 몸값을 조정할 수 있다.

또한 파일 복호화 서비스 이외에도 소포라 조직은 별도로 가격을 책정한 다른 서비스를 제공한다. 악성코드가 다시는 해당 컴퓨터를 감염시키지 않도록 보장하는 면제(immunity)라는 서비스와 파일들을 복호화 한 후 이 랜섬웨어를 제거하는 서비스다. 이 모든 서비스를 다함께 구매할 때에는 낮은 가격에 제공하는 풀 패키지 형태도 제공하고 있다.

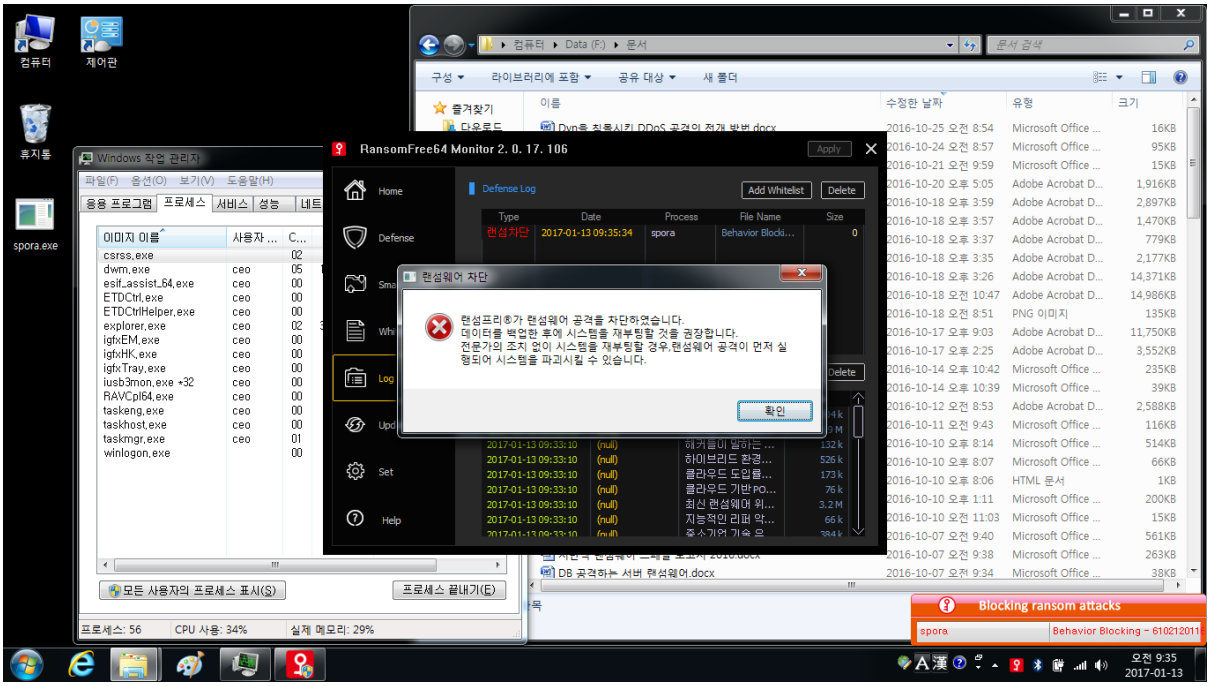
지불 웹 사이트 자체는 아주 잘 디자인되어 있으며, 전문가처럼 보인다. 이는 통합 라이브 채팅과 할인 혜택을 받을 수 있는 기능을 갖고 있다. 엠시소프트 연구원들이 관찰한 바에 따르면, 이 공격자들은 메시지에 즉각적으로 반응한다.
이런 정황들은 소포라가 전문적이고 자금이 풍부한 조직에서 만들어졌다는 걸 의미한다.

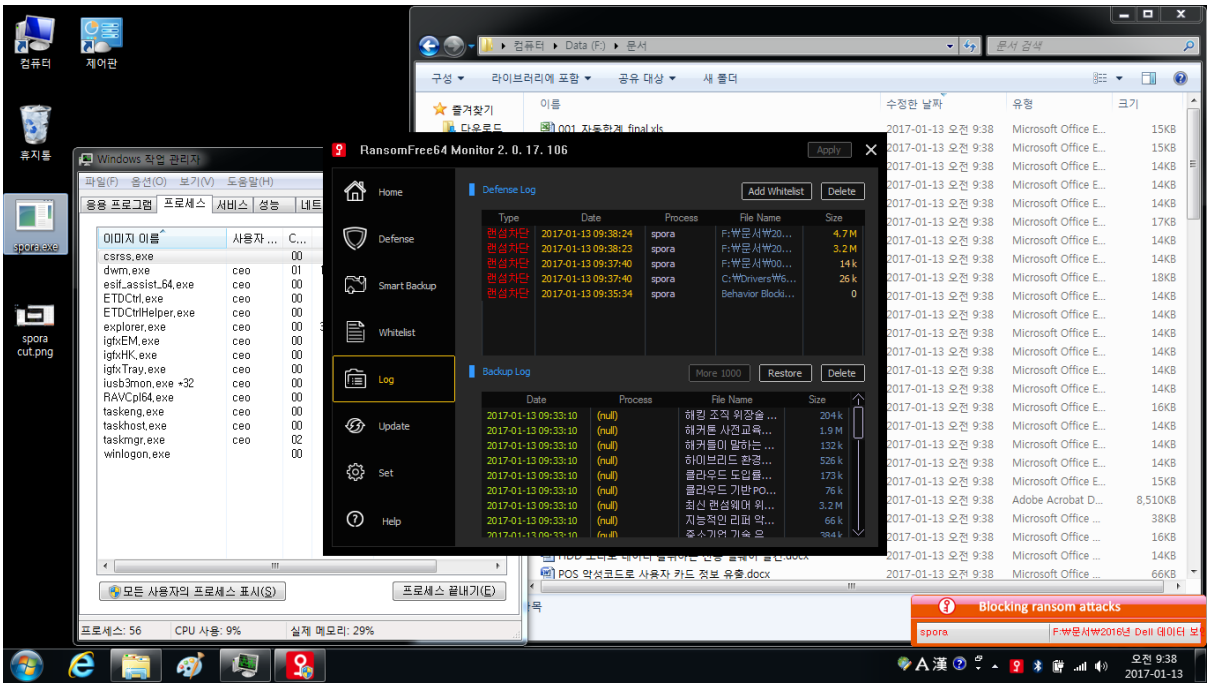
또한 지금까지 관찰된 몸값은 다른 랜섬웨어 조직들이 요구한 액수보다 낮았다. 이는 소포라 배후에 있는

조직은 이 랜섬웨어가 빠르게 정착하길 원하고 있음을 알 수 있다.
소포라는 지금까지 러시아와 다른 러시아 이외 국가 내에서 인기있는 회계 소프트웨어 프로그램의 청구서로 위조된 악의적인 이메일 첨부파일을 통해 배포됐다. 첨부 파일은 악의적인 자바스크립트 코드가 포함된 .HTA(HTML Application) 파일 형식이다. editor@itworld.co.kr

랜섬프리®에 의한 차단 시연

1. 랜섬웨어 실행 파일명 = spora.exe

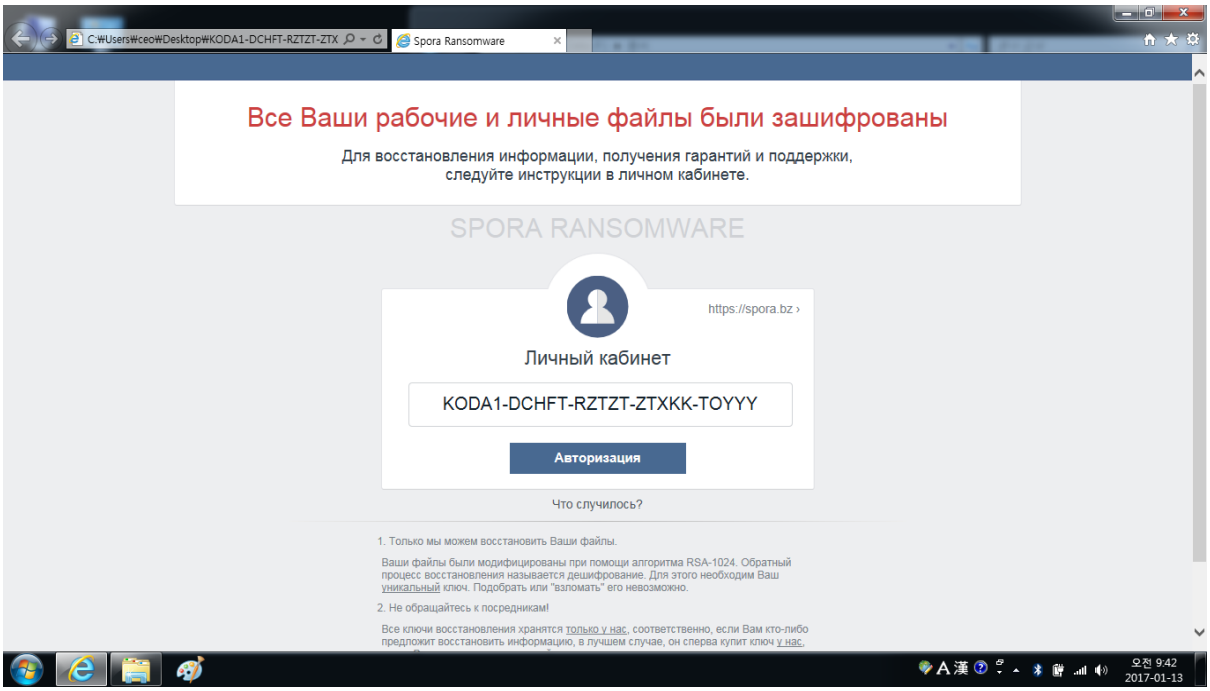




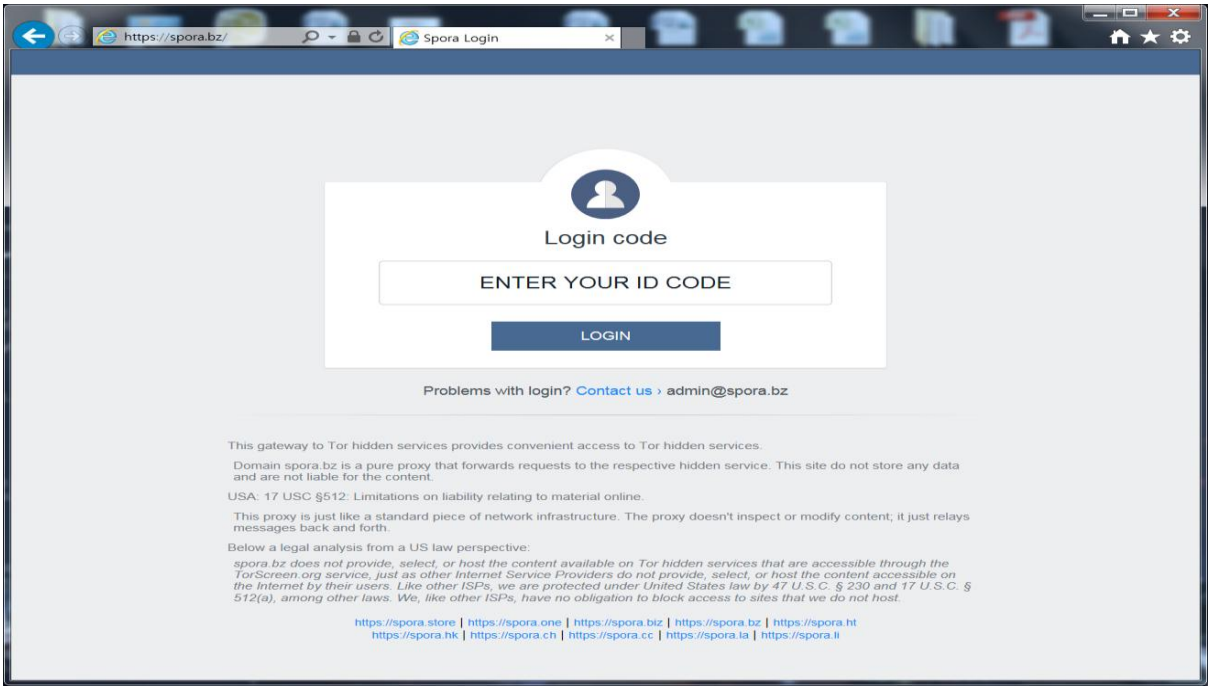
위와 같이 랜섬프리®가 스포라 랜선웨어의 공격을 실시간 차단하는 것을 보실 수 있습니다.

2. 랜섬프리®가 없을 경우

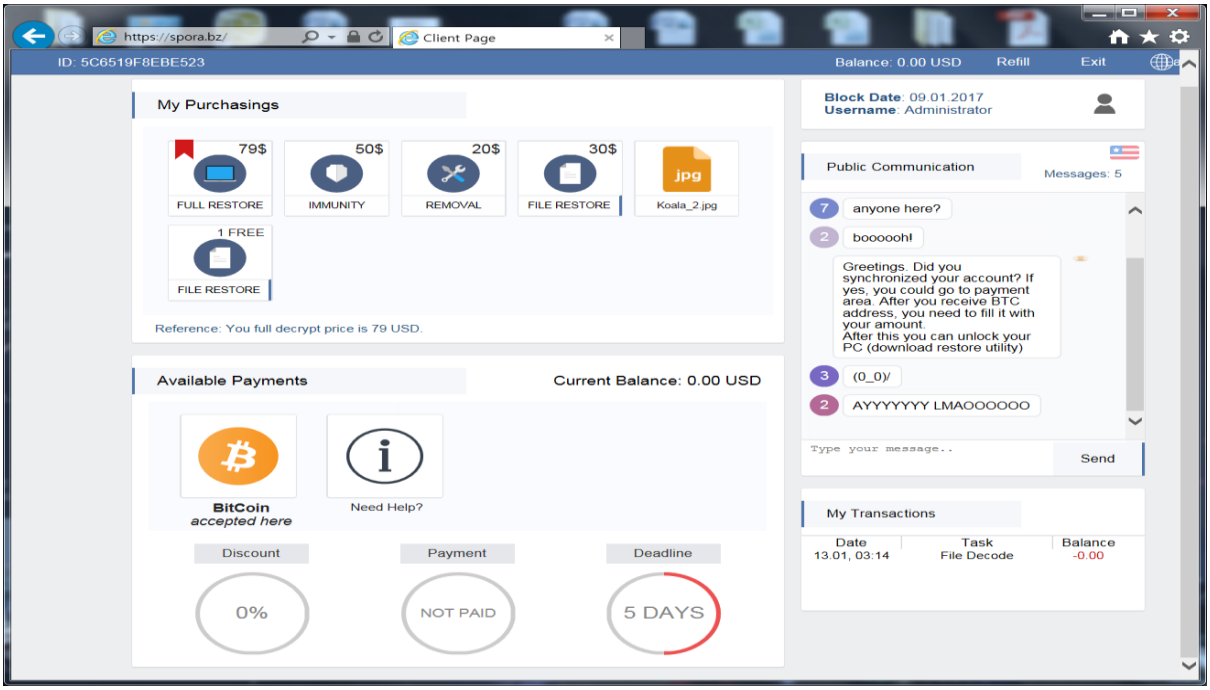
2-1. 스포라 랜섬웨어의 공격을 받으면 아래의 화면이 열려 ID 를 발급하고, 자신들의 홈페이지 (https://spora.bz)에 접속할 것을 안내합니다.



2-2. 홈페이지에 접속하면 아래의 화면이 열립니다.

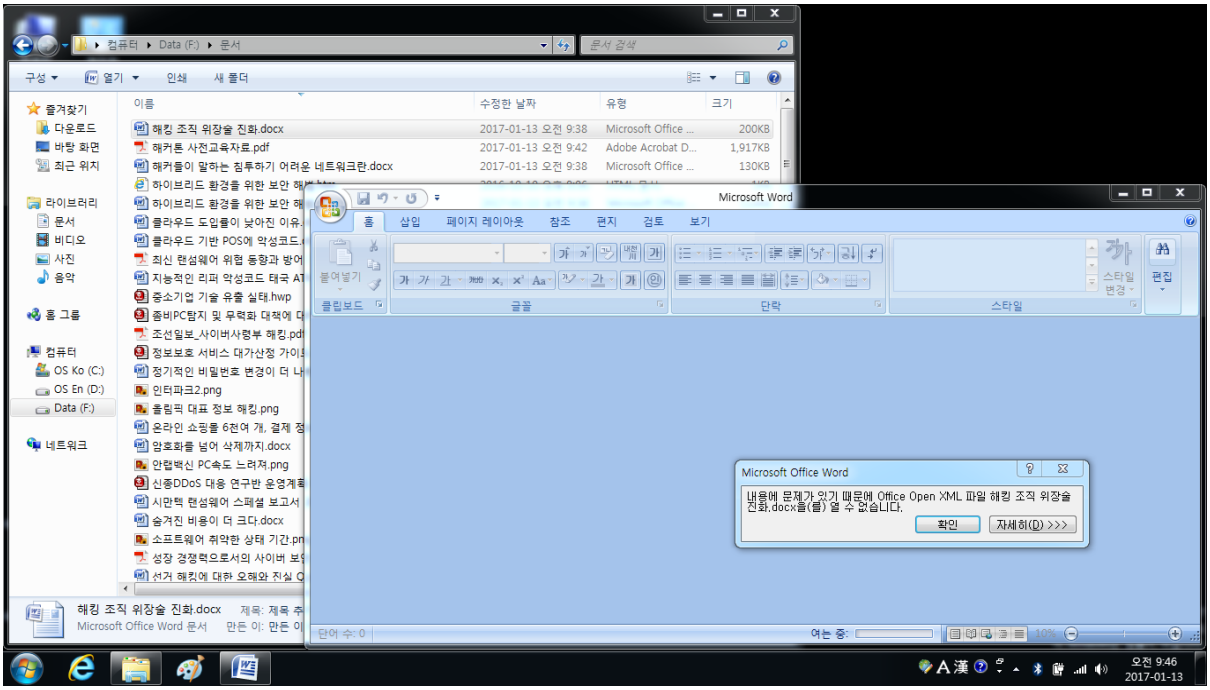


2-3. 앞서 부여 받은 ID 를 입력하고 로그인하면 아래의 화면이 열립니다.



이 화면에서 돈을 지불하도록 유도하고 있으며, 실시간 채팅 기능도 제공되고 있음을 보실 수 있네요.

2-4. 공격을 받은 파일 증상



공격을 당해도 파일이름이나 확장자는 변화가 없습니다만, 열리지는 않습니다.