|  |  |  |  |
| --- | --- | --- | --- |
| **과제명** | . bat 파일을 응용한 랜섬웨어 공격 | | |
| **팀명** | 8조 | **작성일자** | 2017.12.04 |
| **팀원** | 배동현 (20123214) | | |
| 김민지 (20176063) | | |
| 정유정 (20176064) | | |

1. 연구방법

: . bat파일을 응용하여 메모장에 코드 작성 후 사용자가 컴퓨터 켤 때마다 자동으로 BAT파일이 실행되어 정해진 시간 안에 지정된 패스워드를 입력하지 않으면 컴퓨터를 종료시켜 버리는 실습을 해본다. 이는 랜섬웨어(Ransomware)와 비슷한 형태의 방법으로 랜섬웨어 도 조사해본다.

1. 연구과정
2. 랜섬웨어(Ransomware)

: 랜섬웨어(Ransomware)는 몸값 ‘Ransom’ 과 소프트웨어 ‘Software’의 합성어로 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.

암호화되는 랜섬웨어가 있는 반면, 어떤 것은 시스템을 단순하게 잠그고 컴퓨터 사용자가 지불하게 만들기 위해 안내문구를 띄운다.

1. 랜섬웨어공격의 원리 와 흐름

: 암호화 알고리즘의 이용으로 파일 데이터의 암호화 알고리즘을 이용하여 암호화하여 사용할 수 없도록 하는 것이다. 암호화 방식에는 단방향, 양방향 방식이 있다. 단방향 암호화란 한 번 암호화하면 다시 복호화 할 수 없도록 하는 것이다. 양방향 암호화는 암호화한 후 복호화가 가능한 것이다.

최근 단순히 홈페이지를 방문만 해도 랜섬웨어에 감염되기도 한다. 이를 ‘드라이 바이 다운로드(Drive by Download)’ 기법을 이용해서다. 드라이브 바이 다운로드는 공격자가 해당 웹사이트에서 보안이 취약한 점을 노려 악성코드를 숨기고, 이 악성코드를 사용자가 자신도 모르게 내려받아 실행해 감염되는 방식이다.

랜섬웨어의 공격 흐름은 크게 6단계로 나눠볼 수 있다.



1. 대상 파일 검색

* 감염이 되었다고 가정할 때 랜섬웨어는 피해자의 컴퓨터에서 공격 대상이 되는 파일을 검색하는 것이다. 공격자의 입장에서는 피해자가 랜섬웨어 감염 당했을 때 비용을 지불하면서 복구를 시킬만한 중요한 문서를 찾아 공격하려는 것이다. 그렇기 때문에 중요한 정보를 포함한 파일을 최대한 많이 암호화 시켜 버린다.

공격자는 이런 작업을 위해 먼저 암호화 시킬 대상 파일을 검색하는 것이 선행이 되어야 한다.

1. 파일 암호화

* 암호화를 할 대상 파일을 선별하여 찾았다면 랜섬웨어는 본격적으로 그 데이터들을 암호화 작업을 수행하게 된다. 이때 사용되는 암호화 알고리즘은 자체 제작된 알고리즘일 수도 있고, 이미 널리 이용되는 암호화 알고리즘일 수도 있다. 기본적으로 양방향 암호화는 암호화를 하기 위한 키와 복호화를 하기 위한 키가 동일하게 사용된다.

공격자 입장에서 가장 단순하게 만들 수 있는 방법은 모든 대상 파일에 대해 동일한 암호화 알고리즘을 사용해 처리하는 방법이다. 이 경우에는 암호화 및 복호화를 위한 키도 1개뿐이라 공격자가 만든 프로그램이 단시간 내에 분석이 되어 버리면 피해자는 자신이 아닌 다른 사람에 의해 자료를 복원할 가능성이 높아지므로 공격자의 목적인 수익으로 이어지기가 힘들어진다.

공격자는 이러한 문제 때문에 자신의 공격이 좀 더 효율적으로 성공하여 자신의 공격이 피해자뿐만 아니라 제 3자도 풀 수 없도록 해야 좀 더 수익창출의 가능성이 높아질 것이기 때문에 좀 더 복잡한 암호화 처리 알고리즘을 고려할 필요가 있다. 컴퓨터 1대의 안에서 다양한 암호화 키를 만들어 암호화 처리가 이루어 지도록 하는 것이 효과적이다.

2-1. 고정 키 암호화

* 고정 키 암호화 방식은 가장 단순한 방식으로 사실상 테스트 또는 교육용 목적에서 만들어진 랜섬웨어가 아닌 이상에는 찾아보기 힘들며 랜섬웨어 자체 또는 처리과정에서 각 파일이나 환경에 변화하지 않는 고정된 단일 키로 암호화가 수행된다.

2-2. 다이나믹 키 암호화

* 다이나믹 키 암호화는 말 그대로 암호화를 위한 키가 다이나믹하게 변화하는 방식을 의미하는 키 이다. 시스템의 환경이나 파일명, 속성 등을 고려해 상황에 따라 다른 암호화 키를 만들어 사용하는 방법이다.

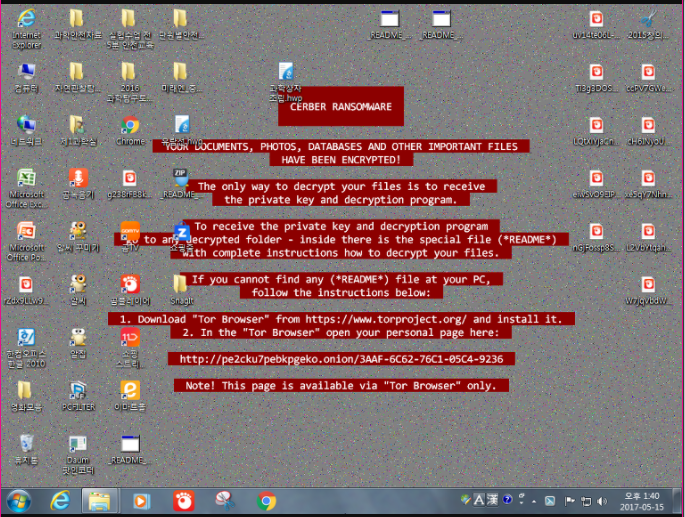
1. 파일 이동

* 어느 정도 파일의 암호화에 성공했다고 판단이 되면 공격자는 이제 피해자에게 공격 당했다는 사실을 알리기 위한 사전작업을 해야 할 필요가 있다. 지금까지 처리된 공격은 공격대상이 있는 폴더에서 암호화 처리를 수행한 것이기 때문에 피해자는 자신이 공격을 당했다는 사실을 알 수 없어 문제를 해결해야 한다는 필요성을 느끼지 못하는 상태이기 때문이다.

이에 공격자는 피해자에게 공격 당했다는 사실을 알리면서 동시에 피해자가 보유하고 있는 많은 중요자료들이 손상되어 복원을 해야 할 필요성이 있다는 것도 보여주는 과정이 필요한데 이것이 바로 바탕화면 위치에 파일을 이동시키는 이유라고 볼 수 있다. 실제로 많은 랜섬웨어가 감염시킨 파일들을 바탕화면으로 옮기는 양상을 보이는데 그러한 행동의 배경사유가 바로 피해자에게 알리기 위한 작업이다.

1. 감염 안내 및 복구 방법 메시지 출력

* 피해자가 바탕화면에 옮겨진 파일들을 발견하고 이상하다는 증상을 확인하게 되면 자신의 자료가 정상적으로 열리거나 확인되지 않는다는 사실에 당황하게 된다. 이때 공격자는 피해자에게 안내메시지를 통해서 지금 상황이 어떠한지 등의 랜섬웨어 발생에 대해 알려준다. 내용은 피해자의 자료를 공격자가 암호화 하였으니 중요한 자료가 있어 복원하고 싶으면 금전적인 비용을 지불하라는 메시지를 출력한다. 보통 추적을 피하기 위해 비트코인을 요구하는 것이 대부분이다.



* 랜섬웨어 감염된 컴퓨터의 배경화면



* 랜섬웨어에 감염된 모습

1. 랜섬웨어의 공격목적

: 랜섬웨어의 기본적인 목적은 중요한 정보를 암호화시켜 그 정보들을 복호화 시켜주는 대가로 금전적 이익을 받는데 주로 목적이 있다. 이러한 목적 때문에 랜섬웨어는 보통 양방향 암호화를 기반으로 가능한 많은 중요자료를 감염대상으로 삼는 것을 목표로 한다. 기본적으로 업무를 보기 위해 주로 사용되는 문서들의 doc, docx, xls, xlsx, ppt, pptx같은 확장자를 가진 파일과 이미지 확장자인 gif, jpg, png등 다양한 파일이 공격대상이 된다.

랜섬웨어는 특이하게 다른 악성코드들이 사용자들이 감염여부를 모르게 숨어있는 반면에 랜섬웨어는 이러한 금전적 이익을 위해 파일명 뒤에 enc 또는 다른 특이한 문자가 붙은 형태로 바탕화면에 이동시킨 다던지, 요금을 지불하라는 메시지 창을 화면에 띄우는 것이 그에 해당하는 모습이다.

이는 감염된 피해자가 자신의 자료가 공격 당했다는 사실을 인지하고 피해 복구를 위한 의지가 발생하여야 수익으로 연결이 되기 때문이다. 그러나 예외적으로 수익을 위한 행동이 아닐 때에는 복원이 불가능한 단방향 암호화 방식을 사용하여 감염되면 자료를 복원할 수 없도록 만들기도 한다.

1. 피해복구 가능성

: 만약 랜섬웨어에 피해를 당했다면 몇 가지의 요소를 통해 피해복구 가능성에 대해 알아볼 수 있다.

1. 양방향 암호화를 이용하고 있는 랜섬웨어인지 파악한다.

: 첫 번째는 자신이 피해 당한 랜섬웨어가 양방향 암호화 알고리즘을 사용하고 있는지에 대하여 파악한다. 이를 파악하기 위해서는 감염된 랜섬웨어를 찾아내어 디버깅이나 리버스엔지니어링을 통한 직접적인 분석을 해야 한다. 그러나 전문가가 아닌 일반인들은 감염된 랜섬웨어가 어떤 상태인지, 어떤 알고리즘을 사용 중인지에 대해 알아내기 어렵다. 그럴 때는 전문가의 도움을 받는 것이 좋다. 하지만 양방향 알고리즘을 사용하지 않은 랜섬웨어라면 복구가 불가능이라 할 수 있으므로 이후의 과정은 의미가 없게 된다.

1. 랜섬웨어 내부에 암호화 및 복호화를 위한 키가 존재하는지 파악한다.

: 두 번째로 감염된 랜섬웨어 내부에 암호화 또는 복호화 키가 내장되어 있는지 파악하는 것이다. 만약 랜섬웨어 내부에 암호화 또는 복호화 키가 내장되어 있다면 해당 악성코드를 만든 공격자에게 비용을 지불하지 않더라도 리버스엔지니어링이 가능한 전문가에게 부탁하거나 백신 회사에서 해당 랜섬웨어에 대한 복원 툴이 공개되는 것을 기다려 자료 복원을 기대해 볼 수 있다. 그러나 만약 암호화 키가 고정되어 있지 않고 랜덤으로 만들어져 암호화 하고 있을 경우에는 복원 가능성이 낮아지게 된다.

1. 공격자에게 비용을 지불했을 경우 복원시켜준 사례가 있는지 파악한다.

: 세 번째로 공격자에게 비용을 지불했을 경우에 자료를 확실히 복원시켜준 사례가 있는지 파악하는 것이다. 만약 공격자가 비용을 지불해도 자료를 복원해주지 않는다면 금전적 피해라는 2차 피해만 발생하고 자료는 복원하지 못하게 될 가능성이 높다.

3가지 요소를 모두 보면 단방향 암호화를 이용한 랜섬웨어의 복구 가능성이 매우 희박하다고 볼 수 있다. 하지만 양방향 암호화를 사용하고 랜섬웨어 자체에 암호화 및 복호화를 위한 키가 포함되어있다면 복구 가능성이 높아질 수 있다.

1. 암호화 & 복호화
2. 암호화

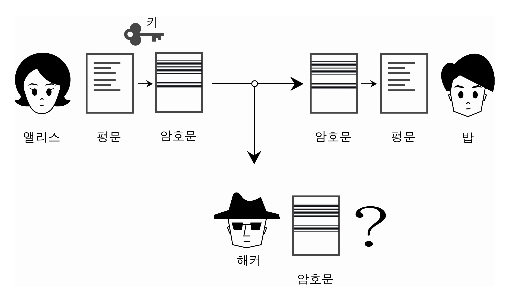
: 정보통신 기술의 발전에 따라 개인정보의 저장과 유통이 광역화, 네트워크화 되고 있어 이렇게 저장/유통되는 개인정보는 다양한 위협에 쉽게 노출되고 있다.

공격자는 정보통신망을 통해 개인정보 송수신시 패킷 도청 소프트웨어를 사용하여 가로채거나 또는 개인정보가 저장된 서버의 취약점을 찾아 고유식별정보 등과 같은 중요한 개인정보를 해킹하게 된다. 이러한 위협으로부터 중요 정보를 보호하기 위해서 개인정보의 전송 및 저장 시 암호화가 필요하다.

암호화란 일상적인 문자로 쓰인 평문을 암호키를 소유하지 않은 사람이 알아볼 수 없도록 기호 또는 다른 문자 등의 암호문으로 변환하는 방법으로 정보의 기밀성 및 무결성, 사용자 인증 등을 위해 광범위하게 이용하고 있다. 이런 암호화의 역 과정을 복호화라고 한다.

1. 암호화의 목적

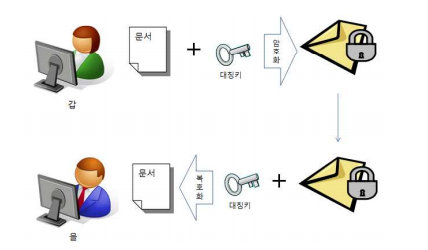
* 기밀성: 암호문에 맞는 키를 가진 사람만이 그 암호문을 복호화 할 수 있어야 한다.
* 무결성: 데이터의 변경이 없었다는 것을 보증한다.
* 인증: 메시지를 보내는 사람이 자기가 생각했던 그 상대방인지 확신 하는 것이다.
* 부인방지: 메시지의 송.수신 후 그 사실을 사후에 증명함으로써 부인을 방지하는 것



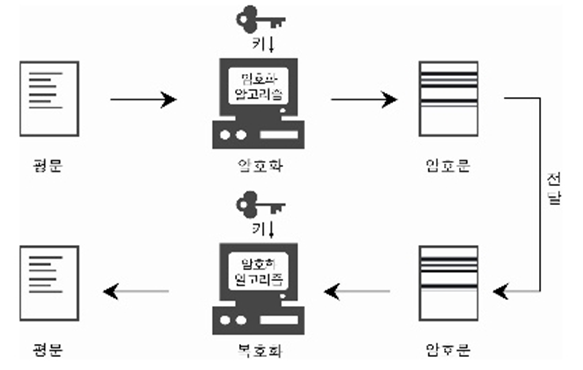
* 암호화 그림1-1

1. 암호화 종류 및 특징
2. 대칭키 암호화

* 대칭키 암호화 방식은 전송하고자 하는 평문을 암호화하고 복호화 하는데 동일한 키를 사용하는 방식이다.
* 대칭키 암호화 방식은 공개키 암호화 방식에 비해 빠른 처리속도를 제공하고, 암호키의 길이가 공개키 암호화 방식보다 상대적으로 작아서 일반적인 정보의 기밀성을 보장하기 위한 용도로 사용되고 있다.
* 하지만, 정보 교환 시 서로간에 동일한 키를 공유해야 하므로 여러 사람과의 정보 교환 시 많은 키를 유지 및 관리해야 하는 어려움이 있다.



* 대칭키 암호화 1-1

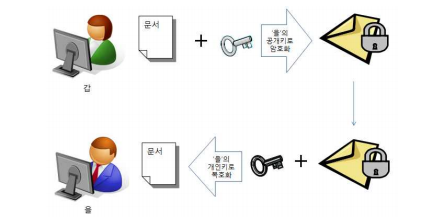


* 대칭키 암호화 1-2
* 대칭키 암호화 알고리즘

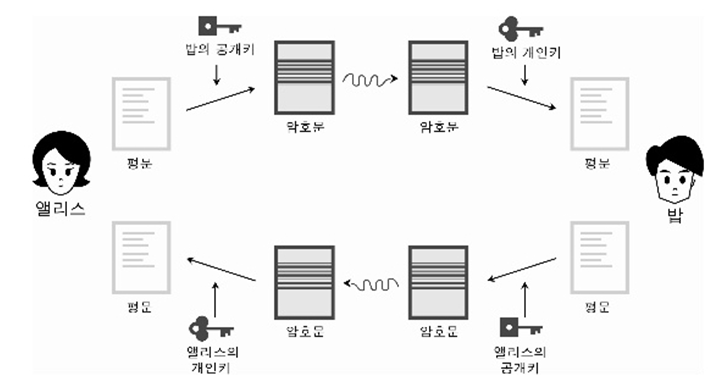
|  |  |
| --- | --- |
| 구분 | 내용 |
| 개요 | 암호화된 문서를 암호화에 사용된 키를 공개하지 않고 개인이 비밀로 하여, 이 키를 아는 자만이 볼 수 있도록 하는 알고리즘을 뜻함. |
| 장점 | 비대칭키 알고리즘에 비해 속도가 빠르다. |
| 단점 | 키 교환을 위해 안전한 메커니즘의 전달방법이 요구된다.  각 쌍이 사용자들마다 유일한 키가 생성되어 다수의 쌍이 존재할 경우 키의 수가 증가되고 이로 인해 키 간의 신뢰가 어려워진다.  인증 기능이 없다. |
| 특징 | 암호화, 복호화 키가 동일하다. |

1. 공개 키 암호화

* 공개 키 암호화 방식은 공개 키와 개인 키의 키 쌍이 존재하여 평문을 암호화, 복호화 하는데 서로 다른 키를 사용하는 방식으로 비대칭 키 암호화 방식이라고도 불린다.
* 공개 키 암호화 방식은 데이터 암호화 속도가 대칭 키 암호화 방식에 비해 느리기 때문에 일반적으로 대칭 키 암호화 방식의 키 분배나 전자서명 또는 카드번호와 같은 작은 크기의 데이터 암호화에 많이 사용되고 있다.



* 공개 키 암호화 1-1



* 공개 키 암호화 1-2
* 비대칭 키 암호화 알고리즘

|  |  |
| --- | --- |
| 구분 | 내용 |
| 개요 | 대칭 키가 가지는 키 분배의 문제점을 해결하기 위해 제안 및 사용된 것이  비대칭 키(공개 키)암호 알고리즘 이다. |
| 장점 | 키가 공개되어 있기 때문에 따로 분배할 필요가 없다.  인증, 부인봉쇄 기능을 제공한다.(전자서명 및 사용자 인증 등에 사용되기도 한다.) |
| 단점 | 암호화, 복호화 키가 다르다.  공개 키로 비밀 키를 복호화 하는 것은 불가능하다. |

1. 단방향(해쉬함수) 암호화

* 단방향 암호화 방식은 해쉬함수를 이용하여 암호화된 값을 생성하며 복호화 되지 않는 방식이다.
* 해쉬함수는 임의의 길이를 갖는 메시지를 입력으로 하여 고정된 길이의 해쉬값 또는 해쉬 코드라 불리는 값을 생성하며, 동일한 입력 메시지에 대해 항상 동일한 값을 생성하지만 해쉬값 만으로 입력 메시지를 유추할 수 없어 전자서명 체계와 함께 데이터의 무결성을 위해 사용된다. 비밀번호와 같이 복호화가 필요 없지만 입력 값의 정확성 검증이 필요한 경우에 사용하고 있다.

1. 최근 랜섬웨어 사태
2. 워너 크라이

: 워너 크라이 랜섬웨어는 전 세계 150개국에서 30만대 이상의 컴퓨터를 감염시킨 악성코드이다. 감염되면 파일들이 암호화되어 열수 없게 되는데 해커들은 파일을 풀어주는 대가로 비트코인 을 요구한다.



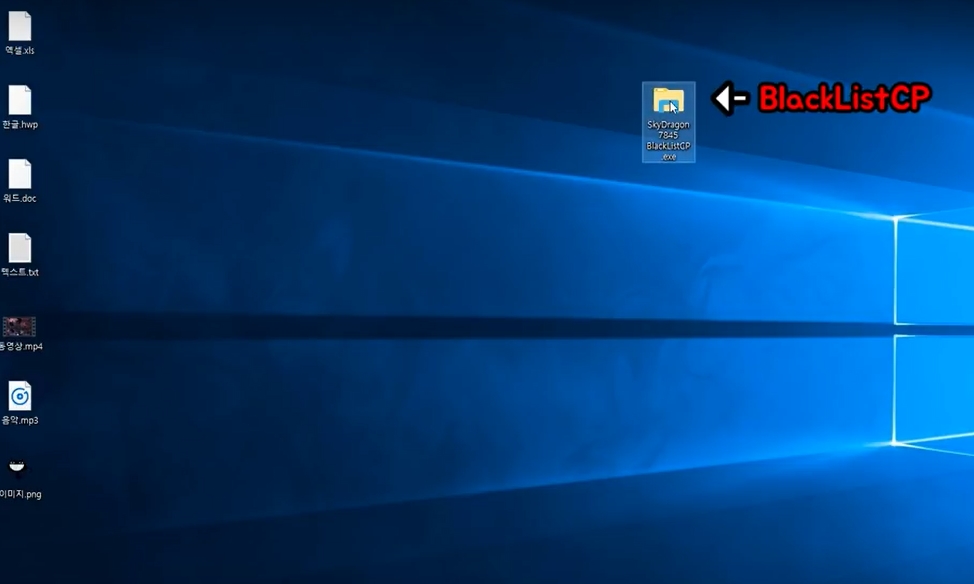
위에 첨부한 이 화면이 워너 크라이에 감염된 컴퓨터의 메시지 창이다. 내용을 보면, ‘당신의 컴퓨터는 암호화 되었다. 몇 개의 정보는 밑에 복호화 키를 이용해 복호화가 가능하다. 하지만 모든 파일을 복호화 할 순 없다. 네가 만약 3일안에 해당 계좌로 비트코인을 송금하면 확실하게 풀어주겠다. 하지만 3일이 지나면 가격이 배가 되며 7일이 지나면 영구적으로 복구 할 수 없다.’라고 되어 있다. 이 워너 크라이 랜섬웨어는 네트워크 망을 통해 감염이 되는 랜섬웨어이다. 무슨 프로그램을 다운받지 않아도 인터넷 네트워크에 연결이 되어 있다면 감염이 되는 것이다. 다행히 한국에선 그렇게 큰 피해를 입히진 않았지만 해외에서는 큰 피해를 입은 것으로 발표되었다. 이 워너 크라이를 미국 국가 안보국(NAS) 에서는 최종적으로 북한의 소행이라고 발표하였다.

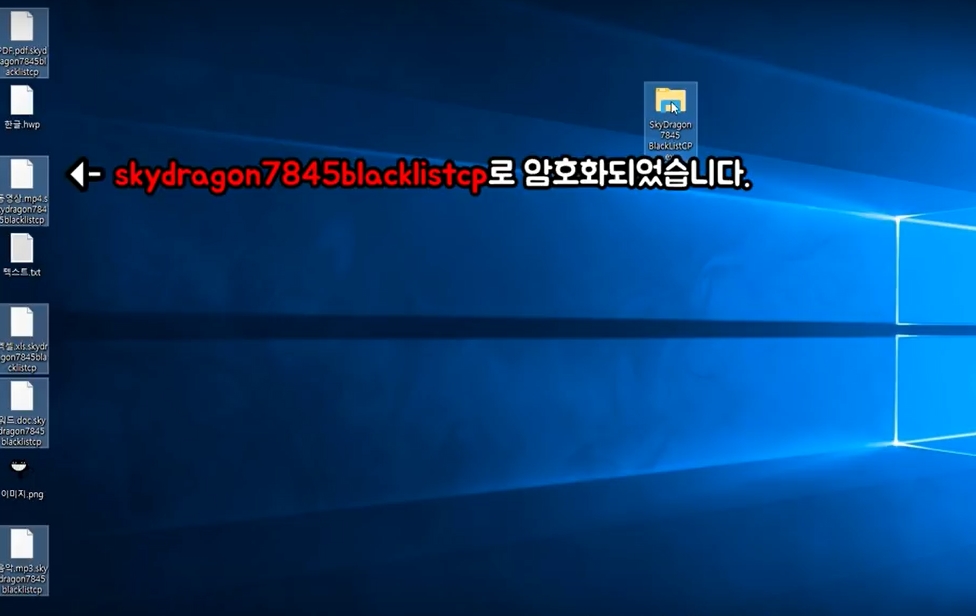
1. 에레보스

: 에레보스는 웹 호스팅 업체를 타깃으로 한 랜섬웨어이다. 가장 큰 피해는 호스팅 업체 인터넷나야나 사건이다. 인터넷나야나는 리눅스 서버 300대 가운데 153대가 에레보스 랜섬웨어에 감염되었다. 해당 업체뿐만 아니라 고객 사 3,400여곳의 홈페이지가 마비되면서 피해 규모가 꾸준히 늘었다. 이후 인터넷나야나 는 이 랜섬웨어를 복호화 하기 위해 13억 이라는 거액을 해커에게 송금하였고 이는 역사상 랜섬웨어에 의한 기업 최고의 피해이다. 연구원들은 이번 에레보스 랜섬웨어는 기존 랜섬웨어보다 비교적 저렴한 가격으로 감염자들이 복구 비용을 내도록 유혹한다며 출처가 불분명한 파일은 절대 실행하면 안 되고 보안 업데이트를 항상 최신으로 수행하고 백신이나 취약점 차단 솔루션을 사용하여 감염을 방지할 수 있다고 말하였다.

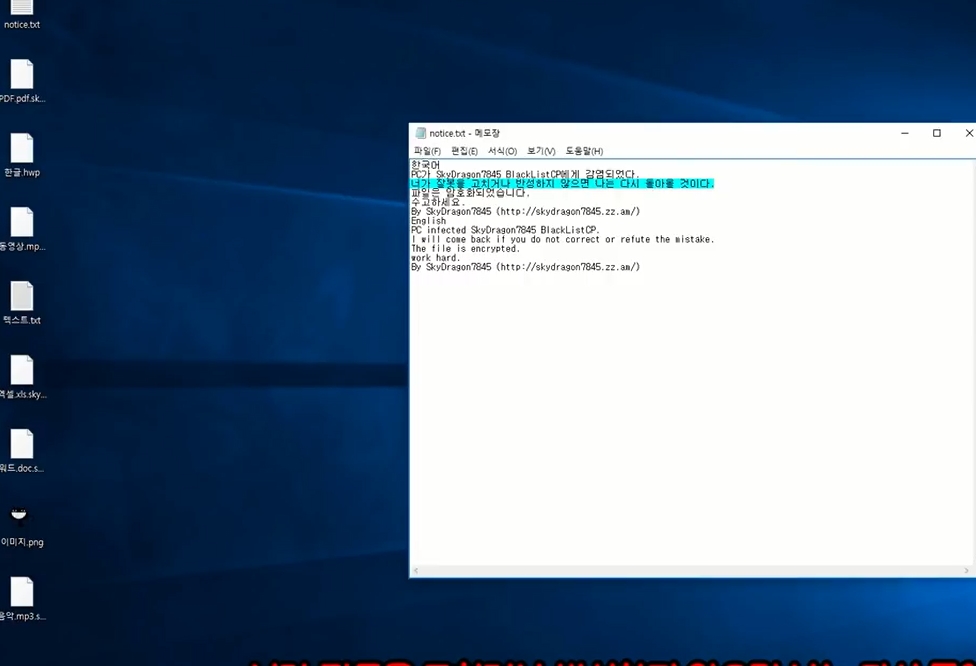
1. 실습 : 랜섬웨어는 아니지만 랜섬웨어 느낌이 나는 파일을 이용한 실습

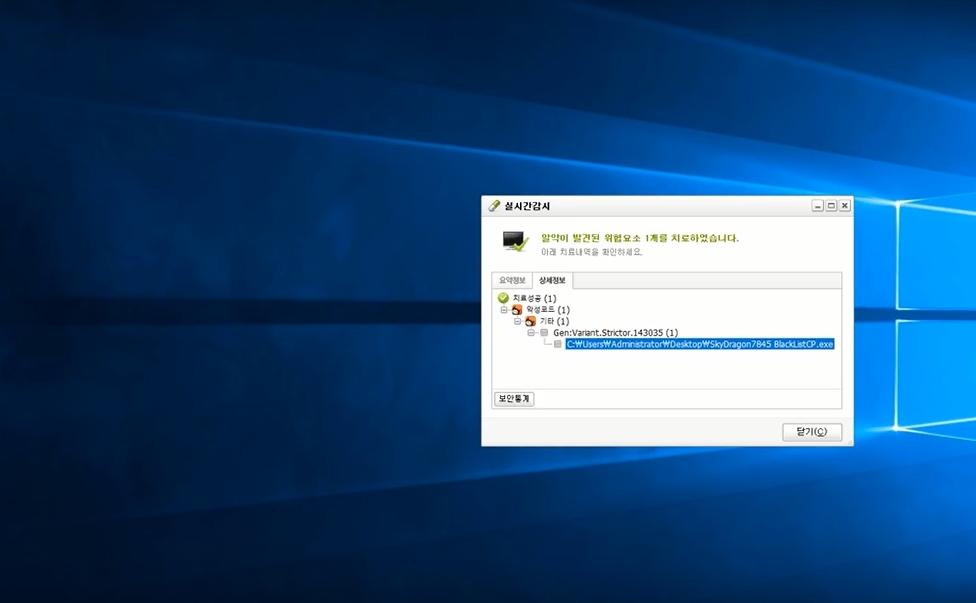
* 윈도우에서 메모장으로 변수와 shutdown을 이용하여 컴퓨터 자체에 암호를 걸어 암호입력 실패시 PC가 종료되는 프로그램.



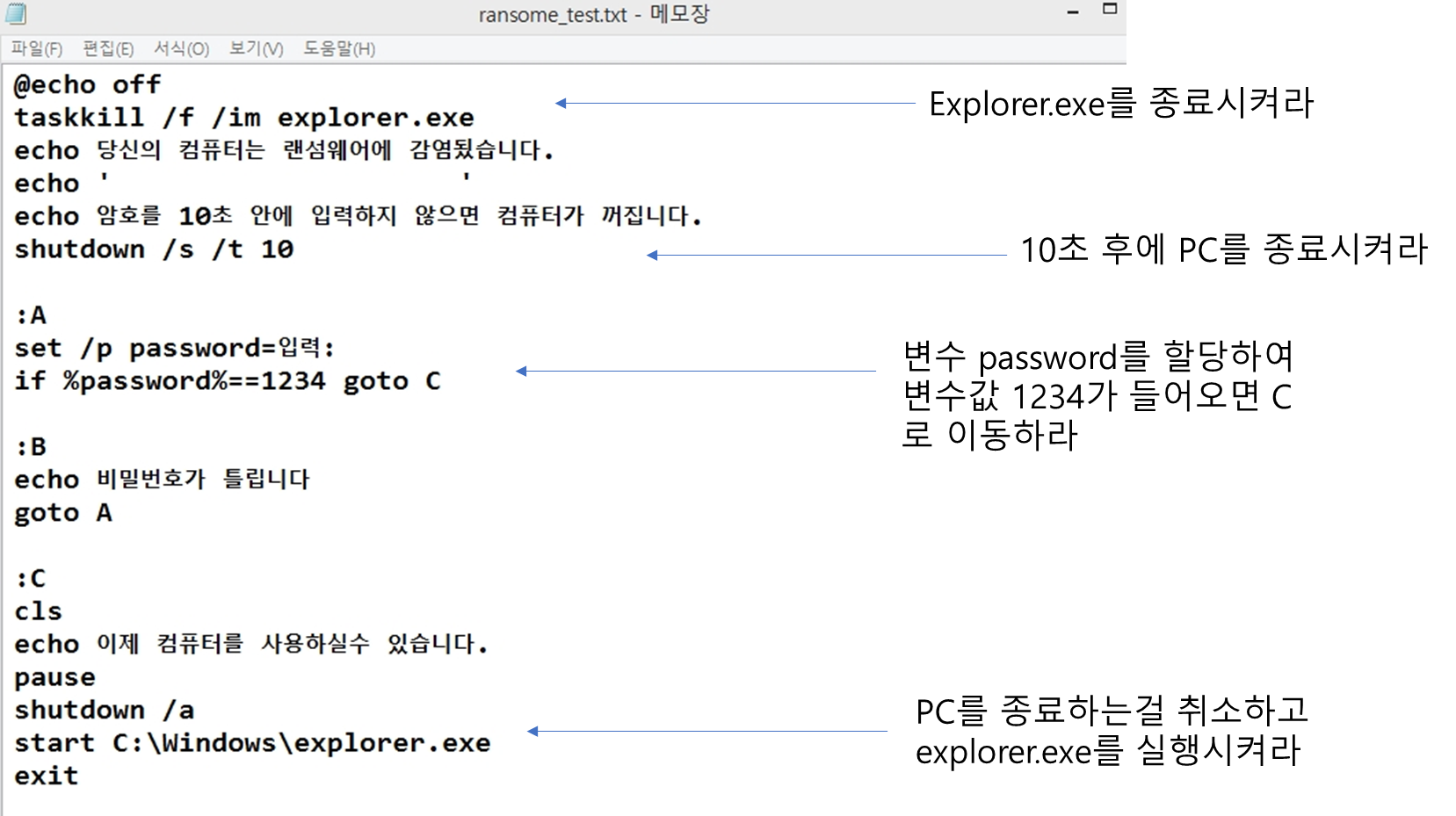


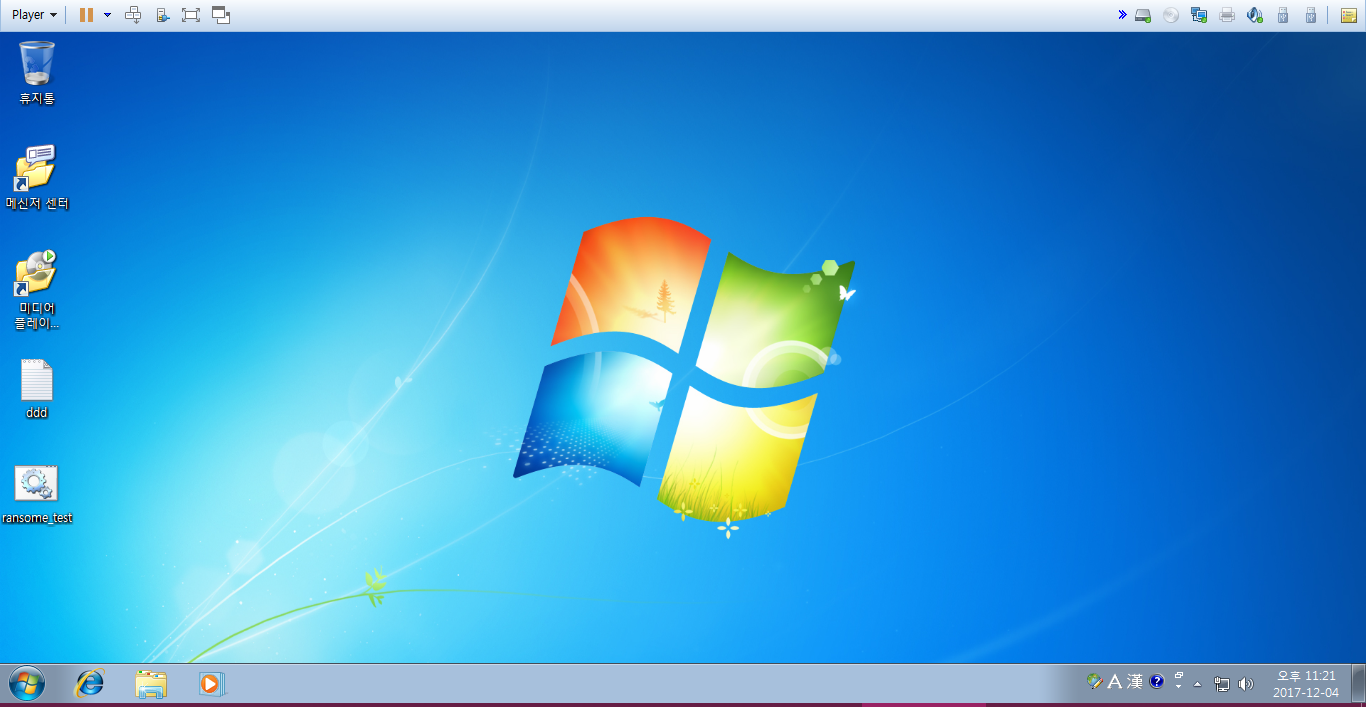
1. 랜섬웨어 실행시 자동으로 생성되는 파일





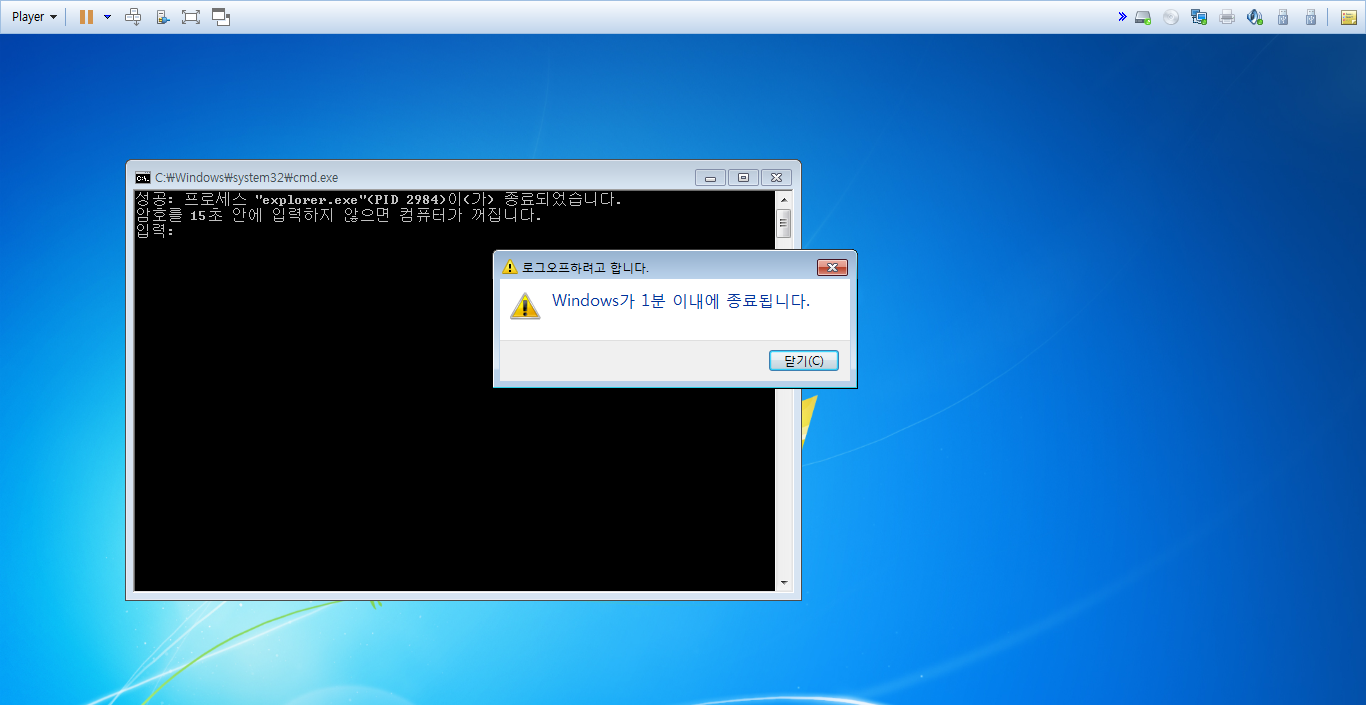
1. 실습에 필요한 ransom\_test파일을 메모장에 작성 후 .bat 파일로 만든다.



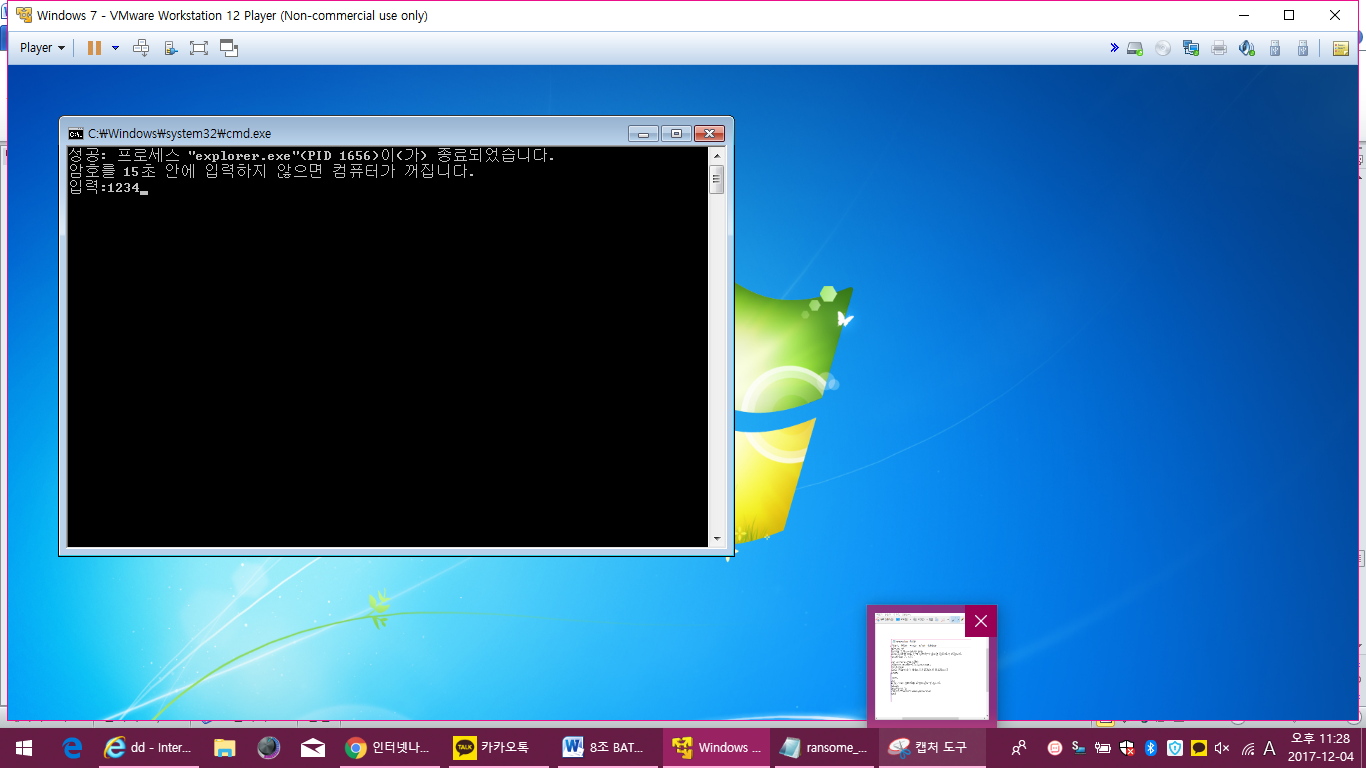


1. ransom\_test.bat 파일을 클릭하면 1분 이내에 종료한다는 메시지가 출력되면서

지정된 패스워드를 입력해야 하는 입력 창이 뜬다.

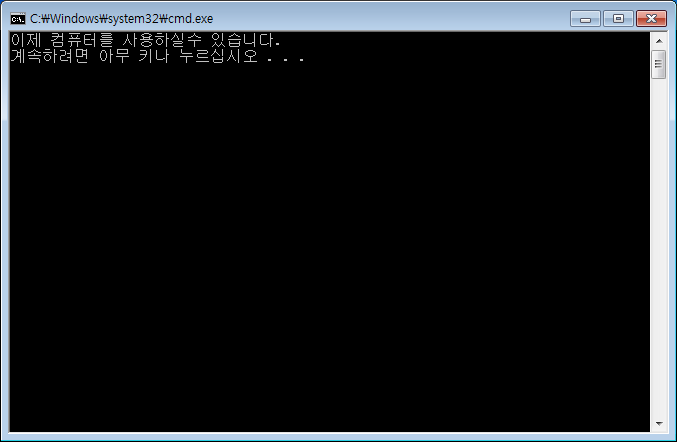


1. .txt파일을 만들 때 지정했던 패스워드 1234를 입력한다.

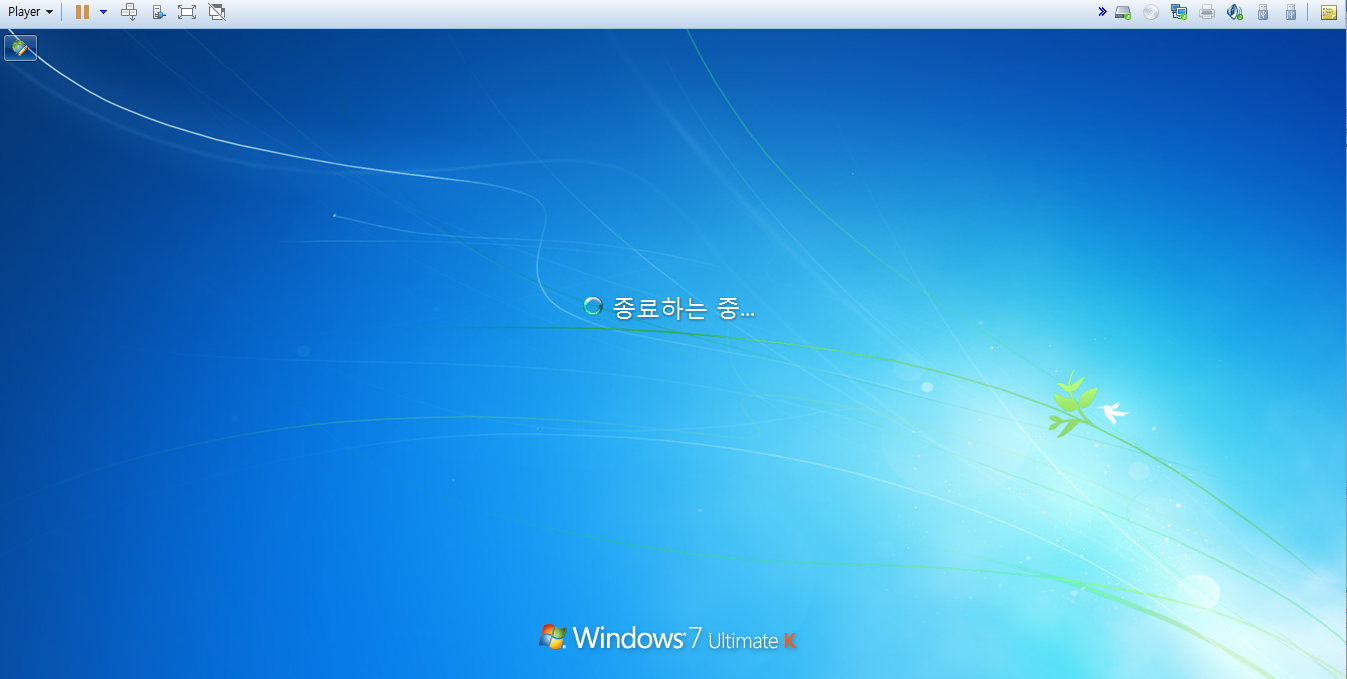


1. 패스워드를 입력하면 다시 정상적으로 이용이 가능해진다.

(패스워드를 입력하고 나서 ‘계속하려면 아무 키나 누르십시오’ 문구를 무시하면 또 강제로 종료가 되어버린다.)



1. 하지만 패스워드를 모르는 상태라면 정해놓은 시간이 지난 후 강제로 종료되는 것을 볼 수 있다.



1. 연구결과
2. 랜섬웨어 – PC 예방법

* 사용 중인 백신 및 SW 최신 업데이트

: 백신 및 OS, 웹 브라우저, PDF, Flash Player, Office 등 SW 업체에서 제공하는 업데이트 적용은 필수

* 주기적 데이터 백업

: 중요한 파일은 외장하드 등에 주기적으로 백업

* 이메일 내 수상한 첨부파일 실행금지

: 랜섬웨어 이외에도 다양한 악성코드가 첨부파일 형태로 유포된다. 따라서 수상한 첨부파일은 실행하지 않는 것이 좋다.

* 보안 취약 사이트 방문 자제

: 의심스러운 사이트 접속을 자제하고 백신의 유해사이트 차단 기능 활용

1. 랜섬웨어- 스마트 폰 예방법

* 문자 메시지 / SNS 내 URL 실행 자제
* 앱 다운로드 시 공식 마켓 평판 확인
* 스마트 폰 백신 설치 및 최신 버전 유지
* 기기 관리가 권한 등록 주의

1. 참고자료

* 위키백과, ‘암호화’,

<https://ko.wikipedia.org/wiki/%EC%95%94%ED%98%B8%ED%99%94>

* 나무위키, ‘인터넷나야나’,

<https://namu.wiki/w/%EC%9D%B8%ED%84%B0%EB%84%B7%EB%82%98%EC%95%BC%EB%82%98%20%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%20%EA%B0%90%EC%97%BC%20%EC%82%AC%ED%83%9C>

* KISA 인터넷 보호나라, ‘랜섬웨어 예방법’,

<https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=25723>

* 네이버블로그, ‘윈도우 버전별 SMB 차단방법’,

<http://post.naver.com/viewer/postView.nhn?volumeNo=7687490&memberNo=3326308>