랜섬웨어의 동작 원리와 예방 대책

Operating principle and preventive measures of Ransomware

조 영 주, 김 진 혁*, 오 지 훈**, 소 윤 정***, 선 아 영****
조선대학교 컴퓨터공학과

Cho Young-Ju, Kim Jin-Hyuk*, Oh Ji-Hoon**,
So Youn-Jeong***, Sun A-Young****
Dept of Computer Engineering, Chosun University

요약

발전하는 IoT시대에 컴퓨터의 사용은 현대인들과 밀접한 관계가 되어 있다. 이로 인해, 우리는 다양한 문서들을 직접 종이에 일일이 적는 불편함을 컴퓨터를 통해 편하게 문서화를 할 수 있게 되었다. 그러나 모든 문서가 컴퓨터에 저장이 되어 있다 보니 이를 악용한 바이러스가 바로 랜섬웨어이다. 본 논문에서는 랜섬웨어의 의미와 동작원리에 대해 알아보고, 예방 대책을 제안하고자 한다.

Ⅰ. 서론

현대 사회의 발전으로 인해, 사람들은 쉽고 편하며 질 좋은 삶을 추구하게 되었다. 이러한 사회의 문물 중 가장 큰 것이 바로 컴퓨터라고 할 수 있다. 이러한 컴퓨터의 발전으로 인해, 집에서 게임을 할 수도 있고, 쉽게 영화나 동영상을 시청할 수도 있으며, 무엇보다도 문서 작업을 할 때, 손으로 일일이 작성하지 않고, 컴퓨터를 이용해 쉽게 문서를 작성 및 수정을 할 수 있다. 그러나, 이러한 장점을 악용하려는 다양한 크래커들에 의해 수많은 바이러스들이 발생하였다. 그 중, 랜섬웨어는 몸값을 뜻하는 Ransom과 제품을 뜻하는 Ware의 합성어이며, 사용자의 동의 없이 컴퓨터에 불법으로 설치되어 사용자의 파일을 인질로 잡아 금전적인 요구를 하는 악성프로그램이다. 본 논문에서는 랜섬웨어의 의미와 역사 및 종류와 기법에 대해 알아보고자 한다. 그림1은 랜섬웨어 감염 화면이다.

▶▶ 그림 1. 랜섬웨어 감염 화면[1]

Ⅱ. 본문

1. 랜섬웨어의 의미와 역사

최근 이슈화 되고 있는 랜섬웨어란 납치된 사람에 대한 몸값을 뜻하는 영어 'Ransom'과 'Software'의 합성어이다. 랜섬웨어는 과거 1989년부터 등장하기 시작했고, 처음 '조셉 팝'에 의해 대칭형 암호방식을 사용하는 형태로 만들어졌다가 후에 1996년 '아담 영'과 '모티 융'에 의해 공개키 암호방식을 사용하는 형태로 진화한다. 이 시기까지는 비트코인과 같은 추적 불가능한 가상화폐가 존재하지 않았기 때문에 보통 불법계좌나, 비밀 계좌등으로 해커들이 대금을 지불받아 어느 정도 추적의 가능성이 있었다. 그러나 비트코인이 등장한 이후 2013년 등장한 '크립토락커' 라고 불리우는 랜섬웨어 부터 추적이 불가능한 '비트코인'으로 대금을 지불받고 있어 추적이 더욱 어려워졌다. 체포될 확률이 적어지자 더 많은 랜섬웨어가 생겨났고 암호화 방식도 점점 더 정교하고 복잡해져 사실상 사용자가 기타 방법으로 복구하는 것이 불가능한 수준까지 이르렀다.[2]

2. 랜섬웨어의 특징

사용자의 파일을 인질로 잡아 금전적인 요구를 하는랜섬웨어에는 다음과 같은 특징을 가지고 있다.

2.1 랜섬웨어 유포방식의 다양화

랜섬웨어는 다양한 방법으로 유포되고 있다. 이메일이나 첨부파일 및 메신저를 통한 고전적 기법에 의한 유포에서부터 응용프로그램과 OS 및 웹의 취약점을 통한 사용자 동의 없는 유포 그리고 블로그와 카페 및 토렌트를 이용한 유포까지 그 예를 들 수 있다.

2.2 랜섬웨어 유포파일 형태의 다양화

기존에는 문서파일(.doc, .pdf)등으로 위장하거나 혹은 화면보호기 파일(.scr)등으로 위장하여 유포되었으며, 이는 현재에도 계속 진행중이다. 그러나 이 파일들을 직접적으로 탐지하여 이를 미리 예방해 버리자, 최근에는 자

바 스크립트(.js)를 첨부파일에 포함시켜 해당 파일이 실행이 될 때 백그라운드 프로세서에서 랜섬웨어가 다운로드 되는 변종도 발생하였다.

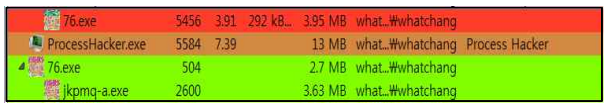
2.3 랜섬웨어의 불법적인 서비스화

랜섬웨어를 제작 배포하려는 사람들을 대행해 랜섬웨어를 제작해주는 "RaaS(Ransomware as a service)"가 등장했다. 이 제작자들은 랜섬웨어의 전파, 감염 현황에 대한 정보를 '고객'에게 제공하며, 감염자들을 대상으로 현재 상황 및 입금 방법을 상담하는 'LiveChat' 서비스를 탑재하여, 피해자들이 랜섬웨어에 대한 피해 구제 서비스를 제공받는 것처럼 착각하게 만드는 사용자를 기망하는 불법적인 서비스가 생겨났다.

3. 랜섬웨어의 동작 원리

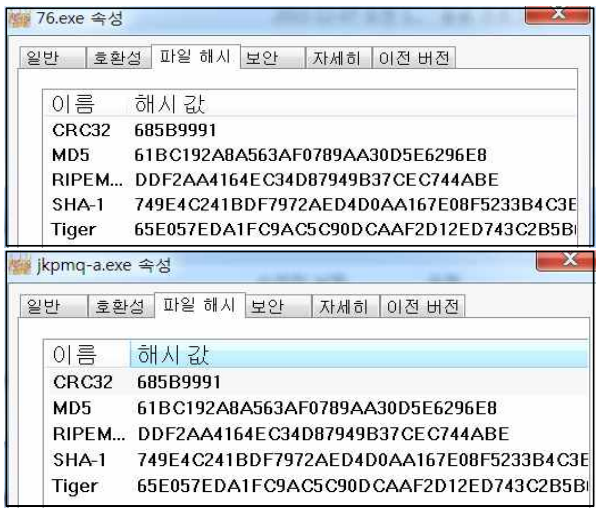
해당 랜섬웨어를 가지고 직접 76.exe라는 파일을 가지고 분석한 결과를 바탕으로 설명하고자 한다.

파일을 실행시킬 경우에, 그림 2와 같이 76.exe밑에 새로운 exe파일이 생성된 것을 볼 수 있다.



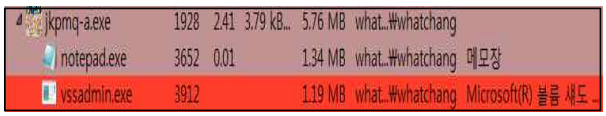
▶▶ 그림 2. 프로세서 상의 생성된 파일목록

이를 바탕으로 파일의 생성위치를 가서 해시값을 확인해 본 결과, 그림 3과 같이 jkpmq-a.exe파일의 해시값이 76.exe파일과 일치한 것을 알 수 있다. 이를 통해, 76.exe파일 밑에 생성된 exe파일이 76.exe파일과 동일파일임을 확인할 수 있었다.



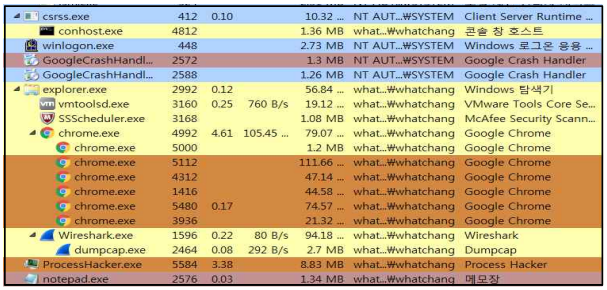
▶▶ 그림 3. 76.exe파일과 새로 생성된 exe파일의 해시값

그 후, 그림 4와 같이 Vssamin.exe라는 파일이 실행이 되는데, 이는 볼륨 쉐도우를 삭제하여, 복구가 불가능하게 한다. 사용자가 랜섬웨어에 걸렸을 때 이를 복구로 풀어버리는 불상사를 방지하기 위해서 랜섬웨어 제작자 입장에서 만든 안전장치이다. 또한, notepad와 html등이 실행되는데 이는 파일을 암호화시키고, 이를 사용자에게 알리기 위해서 실행된다.



▶▶ 그림 4. 악성코드에 의해 실행되는 notepad와 html

그리고, 암호화와 경고 작업 등이 끝나면, 악성 프로그램은 분석되는 것을 방지하기 위해 스스로 종료되며, 해당 프로그램이 저장되어 있던 폴더를 제거해 버린다.



▶▶ 그림 5. 자동 종료된 악성프로그램

이를 process hacker로 볼 경우, 해당 악성코드에 동작 순서는 악성 프로그램과 동일한 파일을 다른 이름으로 다른 폴더에 저장을 하고, 76.exe라는 파일을 삭제 한 후, 특정 확장명을 가지고 있는 몇몇 파일들을 암호화시킨다. 이후 vssadmin을 이용하여 볼륨 쉐도우를 조작하여 복구가 불가능하게 만들고, 이후 사용자에게 파일이 암호화되었다는 사실을 알려서 현금을 요구하는 과정까지를 랜섬웨어의 동작원리라 한다.

Ⅲ. 결론

지금까지 본 논문에서는 랜섬웨어의 의미와 역사 및 특징에 대해 알아보았고 랜섬웨어의 동작원리를 직접 구현 해 보았다. 이러한 랜섬웨어는 더욱 다양한 방법으로 사용자에게 피해를 주고 있다. 랜섬웨어에 감염된 경우에는 해커에게 비용을 지불하더라도, 해커가 이를 완벽하게 복구해 준다는 보장도 없을뿐더러 일시적으로 복호화 해 준 이후, 다시 암호화를 통해 비용을 추가적으로 요구하는 사례 또한 빈번하게 발생한다.

이처럼 랜섬웨어에 감염된 후에는 완치가 힘들기 때문에 이를 미연에 예방하는 것이 중요하다.

랜섬웨어를 예방하는 방법으로 첫째, 백신을 설치하여 감염되기 전에 악성코드를 차단시키도록 한다.

둘째, 중요 파일들은 따로 백업 해 놓거나, 사본을 문서화해서 따로 보관해 둔다.

셋째, 의심되거나 위험한 사이트는 가급적 접속하지 않으며, 확인되지 않은 프로그램 또는 파일은 다운로드 하지 않는다.

이 세 가지 방법의 실천만으로도 중요한 문서 및 컴퓨터를 랜섬웨어로부터 지킬 수 있다.

▌참 고 문 헌▐

[1] http://www.imgrum.org/media/1494347376696904360_3270298813
[2] http://blog.naver.com/kfpaedu/220971849618₩%