[뉴스스터디] 2주차 랜섬웨어_v.01.02

30기 한아림

[1] 관련 기사

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/recent-ransomware-attacks/

According to Checkpoint Research, the number of organizations impacted by ransomware globally has more than doubled in the first half of 2021 compared with 2020, and the healthcare and utilities sectors are the most targeted sectors since the beginning of April 2021.

The success of double extortion in 2020 has been evident, particularly since the outbreak of the Covid-19 pandemic. While not all instances – and their outcomes – are reported and publicized, statistics collected between 2020 and 2021 illustrate the assault vector's importance. The average ransom price has risen by 171% in the last year, to almost $310,000.

Ransomware attacks that have taken place at the end of 2020 and the beginning of 2021 point toward a new attack chain – essentially an enlargement to the double extortion ransomware approach, incorporating an extra, unique threat to the process – A Triple Extortion attack.

Famous attacks in 2021- Microsoft Exchange hack, Colonial Pipeline network, City of Tulsa, JBS Meat Company, Fujifilm

[2] 저번 주, 이번 주 뉴스 스터디 요약

저번 뉴스 스터디에서는 랜섬웨어의 정의와 파일이나 중요한 정보를 인질로 삼아 몸값을 요구하는 공통적인 성격을 언급하며 랜섬웨어에 대한 탐구를 진행하였다. 또 랜섬웨어들의 파일 암호화나 공격 벡터 단계 등 간단하며 공통적인 기동 원리와 동작순서에 대한 내용을 다루었다. 이어, 랜섬웨어로 인한 물질적, 인적 피해 사례 또한 언급하며 랜섬웨어 공격의 심각성도 다룬 바 있다.

이번 주 뉴스 스터디에서는 이전에 다룬 내용에서 조금 더 심도있는 내용을 다룬다. 이번 뉴스에서는 다양한 계열의 랜섬웨어 중에서도 Crypt 계열의 랜섬웨어인 크립토락커(CryptoLocker)와 크립토월(Cryptowall)의 특징과 사용 기제에 대해 알아보았다. 위의 두 랜섬웨어가 어떤 방식으로 사용자의 기기를 감염시키는지, 대략적인 파일의 몸값은 얼마인지와 각각 사회에 언제부터 나타나 얼마나 큰 피해를 입혔는지 등을 다루었다.

[3] 용어 정리

(1) 리다이렉션(Redirection)

'리다이렉션(Redirection)'은 서버나 사이트에 방문하는 방문자가 방문 초기에 요청한 URL이 아닌 다른 URL을 제공하는 행위이다. 본래 URL을 리디렉션하는 행위는 서버, 사이트 방문자의 편의를 위해 진행되는 경우가 많다. 예를 들어 사이트가 새 주소로 이동했음에도 방문자가 옛 사이트 주소를 방문했을 때 이 사용자를 새 사이트의 주소로 옮기기 위해 사용하기도 하고, 여러 페이지를 하나의 페이지로 통합하는 작업을 수행할 때 사용하기도 한다.

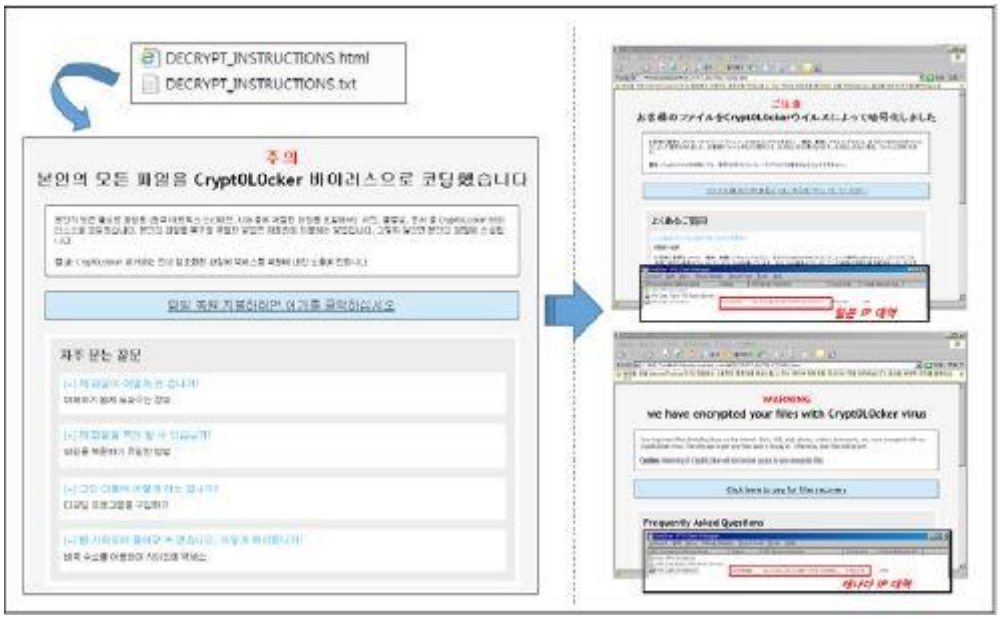
그러나 일부 리디렉션은 검색엔진을 속이거나 크롤러에 제공하는 것과 다른 콘텐츠를 사용자에게 표시함으로써 사용자를 속이며 범죄에 이용되기도 한다. 그 대표적인 예로는 아래에 나오는 랜섬웨어 공격을 위한 기반을 만드는 작업을 수행하는 경우인데, 악성코드를 사용자가 다운받게 끔 하기 위해 사용자를 보안이 안정화된 서버나 사이트에서 보안이 취약한 곳으로 리다이렉션(Redirection)시키는 것 등이 있다.

(2) Angler Exploit Kit (EK)

2013년에 처음 발견된 피싱 공격 도구의 일종으로 여러 기능을 지닌 툴이다. 제로데이의 취약점을 이용하는 코드, 백신과 VM 테스트 코드 등을 탑재한 고기능 피싱 공격 도구로써, 보안연구원들이 이 Angler Exploit Kit (EK)를 세계에서 현존하는 EK 중 가장 선진화된 것이라고 평가한 바 있다. 이 뿐만 아니라 Angler Exploit Kit (EK)는 높은 난독화 기술, IDS, IPS 우회 기능, Fileless infections 기능 등 다양한 기능도 포함하고 있어 랜섬웨어나 APT 공격 등에 자주 쓰이는 추세이다.

[4] Crypt 계열 랜섬웨어의 종류와 특징

(1) 크립토락커(CryptoLocker)



[그림 1] 크립토락커(CryptoLocker) 감염 화면 (출처 : AhnLab)

2013년 9월에 처음 발견된 랜섬웨어로, 이전까지 국내에서 발견된 많은 랜섬웨어와는 달리 이루어진 언어가 한글이라는 점이 특징이다. 크립토락커(CryptoLocker)에 감염되면 위와 같은 화면이 나타나며, 피해자들에게 파일의 몸값을 받아내기 위해 결제 방법을 창을 통해 상세히 설명해 준다는 특징이 있다. 비트코인의 주가가 상승함에 따라 기승을 부리고 있는 랜섬웨어 중 하나이

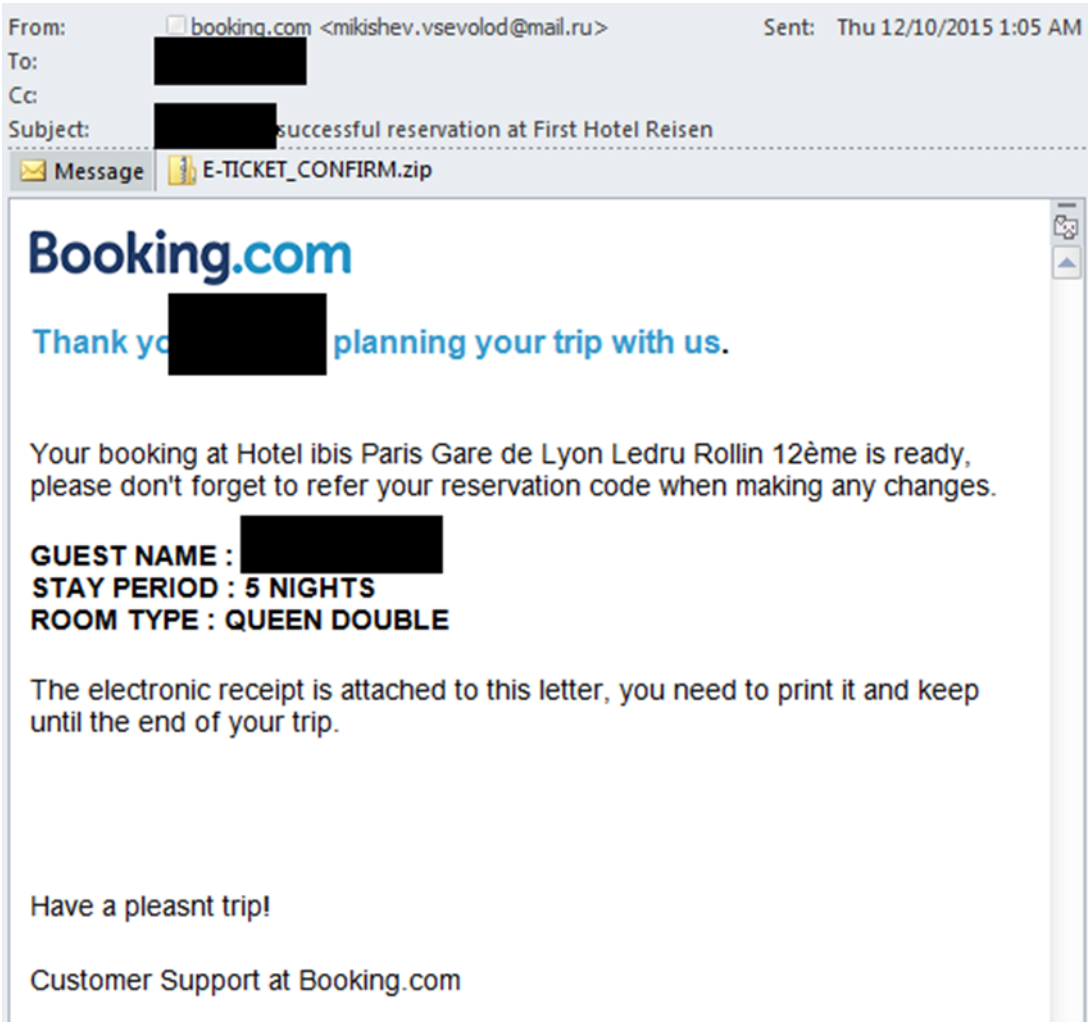
며, 암호화된 파일들을 복원하는 대가로 평균적으로 한화 약 438,900원의 비트코인을 요구한다.

우리나라에 유포된 바 있던 크립토락커(CryptoLocker)는 사용자가 사용하고 있는 시스템의 취약점을 이용한 전형적인 웹을 기반으로 한 DBD(Drive-By-Download) 방식을 통해 감염이 이루어졌다고 확인된 바 있다. 국내에서 많은 사용자들을 보유하고 있는 사이트에 공격 피해 대상자가 접속하면 보안에 취약한 사이트로 '리다이렉션(Redirection)' 되면서 시스템의 특정 취약점에 의해 랜섬웨어 악성코드가 다운로드되고 실행시키는 방식을 통해 감염이 진행되는 경향이 있다.

[그림 2] 크립토락커(CryptoLocker) 감염 경로 (출처 : AhnLab)

(2) 크립토월(Cryptowall)

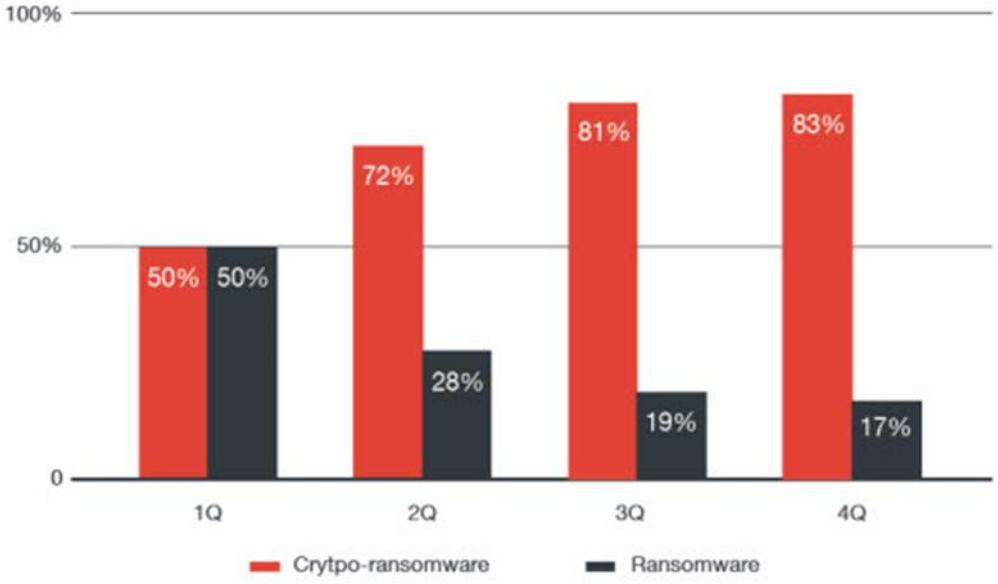
- 2009년 초반부터 피해를 입히기 시작한 랜섬웨어로, 기존의 랜섬웨어를 방어하기 위해 사용하였던 안티바이러스를 회피하는 기제를 가지고 있는 독특한 랜섬웨어이다. 크립토월(Cryptowall)을 만든 사람들은 대중이나 회사, 단체 등의 이메일 주소를 지속적으로 수집해왔고, 이 데이터를 통해 피싱메일을 전송하여 랜섬웨어 공격을 위한 토대 형성에 이용하였다.



[그림 1]Booking.com 이메일 (출처 : https://softmate.tistory.com/88)

위의 사진과 같이 booking.com 등의 이메일로 위장하여 전송되었기에 피해자들이 이상함을 느끼기 어려웠으며, 피해자들이 인지하지 못한 상태로 랜섬웨어의 링크와 첨부물을 통해 암호화 과정이 진행되며 공격이 시작된다. 이 뿐만 아니라 크립토월(Cryptowall)은 C&C서버나 스팸 메시지, 스파이웨어, 그리고 보안이 취약해진 감염된 웹사이트 등을 이용하여 사용자들에게 랜섬웨어를

감염시키기도 한다. 이후에 새로운 버전인 크립토월 4.0이 발표되고 난 이후에는 'Angler Exploit Kit (EK)'를 이용해 사용자가 특정 사이트에 접속하는 것만으로도 감염이 진행되는 드라이브 바이 다운로드(DBD, Drive-By Download) 방식으로 확산된 바 있다.



[그림 1] 2015년말까지 크립토 랜섬웨어 수 증가로 랜섬웨어 추월 (자료제공: 트렌드마이크로)

이 뿐만 아니라 크립토월(Cryptowall)은 다른 랜섬웨어들보다 개수 증가의 폭과 새로운 버전이 나오는 속도가 매우 넓고 빠르다는 특징이 있다. 위의 사진에서 알아볼 수 있듯, 2015년 말까지 크립토월(Cryptowall)은 매우 가파른 속도로 증가했으며 버전 3.0, 4.0을 연이어 발표하면서 2015년 가장 악명높은 랜섬웨어로 지목되기도 하였다.

[5] 느낀 점

이번 뉴스 스터디를 진행하며 내가 생각해왔던 것보다 더 많은 종류의 랜섬웨어가 존재한다는 사실을 깨닫게 되었다. 이번 뉴스를 위한 조사를 하기 전까지 나는 같은 계열의 랜섬웨어는 반드시 같은 기제의 공격 기법을 사용한다고 생각하고 있었으나, 이번 뉴스 제작을 위한 공부를 하며 내가 생각하였던 바가 틀렸음을 알 수 있었다.

아무래도 정의에서 각 종류로 넘어가는 섹션이 존재하다 보니 이전에 작성하였던 뉴스 스터디의 내용보다 더 심도 깊은 내용을 다루려고 노력하였으나 아무래도 분량의 문제 때문에 자잘한 디테일이 부족한 것 같아 아쉽다고 생각한다. 다음 뉴스 스터디에서는 내용의 질은 유지하되 작고 세심한 부분까지 보완할 수 있도록 노력해야겠다는 생각이 들었다.

[6] 다음 뉴스 스터디 방향

다음 뉴스스터디에서는 랜섬웨어 중 상당히 높은 몸값을 요구하는 특징을 가진 케르베르(Cerber~) 계열의 랜섬웨어에 대한 내용을 다룰 예정이다. 오늘의 내용 구성과 마찬가지로, 세상에 모습을 보인 시기와 자주 사용하는 공격 기법, 주로 사용하는 감염 방식이나 그 피해의 정도 등을 다루어 볼 생각이다. 이 뿐만 아니라 각 랜섬웨어의 파일 복구 비용으로 얼마가 소요되는지에 대해서도 다루어 볼 생각이다.

마지막으로, 위 랜섬웨어들의 정리와 설명을 보면 랜섬웨어의 해결방안이나 대처방법이 기술되어 있지 않다. 랜섬웨어가 비슷한 특징을 지니고 있더라도 해결 방안이 굉장히 제각각인지라 분량을 조절하기 위하여 이는 모든 랜섬웨어의 종류(계)를 살펴보고 난 후에 별도의 뉴스스터디의 주제로 선정하여 단독으로 다룰 예정이다.

[7] 참고자료

(1)Crowdstrike_Types of Ransomware (2021)

https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/

(2) AhnLab_한국을 강타한 랜섬웨어 '크립토락커' 어떻게 공격했나 (2015)

https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&curPage=&seq=23630

(3) Search Security(Shaun Nichols)_REvil ransomware attacks resume, but operators are unknown (2022)

https://www.techtarget.com/searchsecurity/news/252516434/REvil-ransomware-attacks-resume-but-operators-are-unknown

(4) 보안뉴스 김경애_크립토월, 앵글러 업고 가장 악명높은 랜섬웨어 1위 등극 (2016)

https://www.boannews.com/media/view.asp?idx=50060

(5) Check Point_Recent Ransomware Attacks (2021)

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/recent-ransomware-attacks/

(6) TREND MICRO _ Ransomware (2021)

https://www.trendmicro.com/vinfo/us/security/definition/ransomware