[뉴스스터디] 1주차 랜섬웨어_v.01.01

30기 한아림

[1] 관련 기사

https://securityboulevard.com/2022/03/ransomware-malware-phishing-top-list-of-it-security-concerns/

https://www.helpnetsecurity.com/2022/03/29/ransomware-continues-to-plague-organizations/

"Another full year of remote working demonstrated that navigating security risks is proving a significant challenge for businesses. While the vast majority (79%) of businesses remain concerned about the security risks of an increasingly remote workforce, the study revealed less than half of businesses (48%) have a formal ransomware plan. 55% of IT leaders reported to have implemented multi factor authentication (MFA), a figure unchanged from the previous year.

Nearly a quarter (23%) of enterprises surveyed said hard financial losses from penalties, fines and legal expenses have been or would be the greatest impact from ransomware. Lost productivity, recovery costs and breach notification lagged behind, while softer, long-term costs such as brand reputation and customer loss were even less of a concern."

[2] 내용 요약

위의 두 기사와 이 뉴스는 현재 사이버 세계를 위협하는 공격 기법 중 하나인 랜섬웨어의 심각성에 대해 다루고 있다. 랜섬웨어 공격자가 파일의 대가로 주로 요구하는 가상화폐 가치의 상승으로 랜섬웨어 공격의 빈도가 기하급수적으로 증가하고 있다. 특히 파일을 암호화하는 기존 방식에서 시스템 파괴, 데이터 삭제, 중요 정보 공개 등으로 공격 형태가 점차 과격해지고 있는 추세이다.

알리안츠에서 조사한 바에 의하면 57%의 사업 전문가들이 "가장 염려되는 건 랜섬웨어가 대책없이 증가하고 있다는 것"이라고 밝혔다고 한다. 금융 산업 내 조직들의 경우 70%가 랜섬웨어 공격에 당했고, 범인들이 요구한 돈은 평균 9만 1천 달러인 것으로 조사되었다. 실제로 대부분의 기업들은 랜섬웨어를 이미 '엔데믹'과 같은 존재로 인식한다고 한다. 늘 거대한 지병이나 유행병처럼 우리 주위에 항상 있는 위협이라고 치부하는 것이다.

위의 기사에서 언급하였듯, 1989년 AIDS 플로피 사건을 시작으로, 랜섬웨어 공격은 2022년 현재에 이르러서까지 악질적인 사이버 공격 수법으로 악명을 떨치며 전 세계적으로 피해를 주고 있다.

정보 보안 업체 사이버아크(CyberArk)가 "얻는 것이 투자보다 많다면 랜섬웨어 공격자들은 자신들의 행위를 멈추지 않을 것"이라 말한 것처럼 랜섬웨어는 여태까지, 그리고 앞으로도 회사와 개인의 정보 보호에 큰 걸림돌이 될 것으로 예측된다. 그들은 "현재 랜섬웨어의 ROI는 대단히 높은 편입니다. 그러니 산업 전체가 계속해서 성장하는 것이죠. 이런 상황이라면 앞으로 몇 년 동안은 랜섬웨어가 계속해서 우리를 괴롭힐 것입니다. 전혀 줄어들지 않은 상태로요." 라고 첨언함으로써 랜섬웨어 공격에 대한 심각성을 강조하였다.

[3] 용어 정리

(1) ROI (Return On Investment)

ROI란 'Return On Investment'의 약자로, 한국어로는 투자 이익률을 의미한다. 투자액에 대하여 이익이 얼마만큼이나 올랐는지를 나타내는 지표로, 이 수치가 크면 투자액에 대해 이익이 크다고 할 수 있다. 반대로 이 수치가 작다면 투자를 한 바가 많은 이익으로 이어지지 못했다고 할 수 있다.

ROI는 투자를 한 것에 대한 이익에 초점을 맞춘 개념이기 때문에 투자를 통해 얻어갈 이익의 정도의 지표로써도 이용할 수 있다는 특징이 있다. 투자 효과를 최대화하기 위해서는 이 ROI를 얼마나 높게 유지하는가가 중요한 관건이며, 이러한 측면에서 왜 랜섬웨어가 끊이지 않고 발생하는지를 유추해볼 수 있다.

(2) 공격 벡터 (attack vector)

'해커들이 컴퓨터나 네트워크에 접근하기 위해 사용하는 경로나 방법이자 시스템의 취약점을 공격할 수 있는 수단을 제공하는 것'이라는 의미를 지닌다. 이용 양상으로는 바이러스나 이메일, 첨부 파일, 웹페이지, 팝업윈도, 인스턴스 메시지 및 대화방 등 주로 운용자의 정보 보안 능력이 취약한 프로그래밍에서부터 야기되었다. 이용한다. 이로 인한 피해를 최소화하고자 방화벽이나 안티 바이러스 소프트웨어 등 다양한 방어 기제를 사용하고 있는 현황이지만, 아직까지 모든 공격벡터를 막아낼 수 있는 기제는 존재하지 않는다.

(3) 악성 코드 (malicious software)

악성코드는 악성 소프트웨어(malicious software)의 줄임말이자, "하나의 컴퓨터, 서버 또는 컴퓨터 네트워크에 피해를 입히도록 설계된 모든 소프트웨어"를 지칭하는 개념이다. 위의 모든 것을 통칭하는 악성코드는 그것을 만드는 데 사용된 기술, 기법이 아니라 악성코드를 만든 의도나 용도를 기준으로 분류된다는 특징이 있다.

[4] 랜섬웨어의 정의와 특징

랜섬웨어 (Ransomware)란 몸값을 의미하는 Ransom과 악성코드를 뜻하는 Malware의 합성어이다. 사용자의 동의 없이 피해자의 PC 등에 설치된다는 점에서는 악성코드와 유사하지만, 행위의 목적을 정보의 훼손이나 유출이 아닌 오직 금전의 취득에 두고 있다는 점에서 악성코드와 구별된다.

주된 목적이자 근본적인 목적이 처음부터 피해자에게 암호화시킨 파일이나 레지스토리에 대한 몸값을 요구하여 금전을 취득하는 것이기 때문에 효율적으로 공격을 감행하는 것이 랜섬웨어의 가장 독특한 특징이다. 파일이나 시스템을 파괴하거나 변조, 훼손하기보다는 몸값 요구에 필요한 파일만을 암호화하여 몸값을 극대화하는 것이 랜섬웨어 공격의 핵심 전략이다.

[5] 랜섬웨어의 동작 원리와 순서

[그림 2] 랜섬웨어 동작 순서 (출처 : CSRC Weblog)

랜섬웨어의 기동 원리를 알아보려면 가장 먼저 랜섬웨어 공격이 어디서부터 시작되는지에 초점을 맞추어야 한다. 랜섬웨어 공격이 시작되는 공격 벡터를 살펴보면, 랜섬웨어 공격을 받는 피해자는 자신도 모르게 랜섬웨어에 감염되는 양상을 볼 수 있다. 이때 주된 감염 경로로는 악성 사이트 접속, 출처가 분명하지 않은 메일을 다루는 과정을 통한 감염이 있다. 이 밖에도 출처가 명확하지 않은 소프트웨어를 통해 랜섬웨어에 감염되는 등 랜섬웨어는 다양한 경우의 수를 통해 감염될 수 있다.

피해자가 랜섬웨어에 감염되었다면, 랜섬웨어는 그 상태로 정지해있지 않고 바이러스처럼 증식하여 랜섬웨어를 전파시킨다. 랜섬웨어가 증식하여 감염의 정도를 심화하는 과정에서 랜섬웨어의 특징 중 하나가 드러나는데, 바로 전파 시에 감염된 PC나 전송 프로토콜의 취약점을 이용한다는 것이다. 이때 랜섬웨어는 감염 대상의 복사, 복제 기능을 제것인양 활용하여 감염을 전파하는 등의 지능적인 모습을 보이기도 한다.

랜섬웨어에 의한 피해가 심각한 이유 중 하나는 피해자가 랜섬웨어 감염을 인지하지 못한 상태에서 피해를 당하기 때문이다. 피해자가 랜섬웨어 감염 사실을 알아차리지 못한 채 랜섬웨어를 실행하는 순간 감염되었던 PC의 파일이 암호화되어 사용할 수 없게 된다. 암호화를 수행하는 과정에서 공격자는 모든 파일을 암호화시키기보다는 파일이나 디렉토리 등 주요 요소들을 주로 공략하는 경향이 있다.

랜섬웨어가 필요한 파일을 모두 암호화하고 나면, 피해자로 하여금 자신이 랜섬웨어에 공격당했다는 사실을 인지시킨다. 피해자에게 피해 사실을 알리는 주된 방법으로는 랜섬노트 속 파일의 몸값을 청구하는 내용을 담아 보내는 방법이나 사용할 수 없게 된 파일들을 피해자가 볼 수 있게 바탕화면으로 이동시키는 방법을 사용한다.

[6] 느낀 점

이렇게 체계적인 틀이 짜여져 있는 보안 뉴스를 제작해 보는 것은 처음이라 조금 막막하고 힘들었다. 부족한 경험으로 만든 뉴스이기에 이번 결과물은 글의 완성도나 내용적인 측면에서 여러모로 부실한 점이 많다고 생각한다. 하지만 요즘 전문가들이 주목하는 보안 이슈들에 대한 유용한 정보들을 많이 접할 수 있었고, 뉴스 제작의 방향성을 조금이나마 정할 수 있었기에 뉴스를 만드는데 들인 시간이 아깝지 않았다.

오늘의 주제가 전 세계적으로 이슈가 되고 있는 문제이다 보니 영어나 한국어로 된 자료를 찾는 것은 어렵지 않았다. 하지만 많은 정보들 중 신빙성 있고 유용한 정보를 선별해내는 작업은 꽤 어려웠다. 그래도 여러 언어로 된 문서를 스스로 이해하고 필요한 정보만을 골라내는 연습을 할 수 있었던 좋은 기회였다고 생각한다.

[7] 다음 뉴스 스터디 방향

첫 번째 뉴스에서는 랜섬웨어의 정의와 간단한 기동 원리, 그리고 그 심각성을 다루었다. 다음 뉴스에서의 메인 테마는 크게 두 개인데, 하나는 랜섬웨어의 각 종류별 기동 원리이고, 나머지 하나는 각각의 랜섬웨어가 지닌 고유한 특성들이다.

랜섬웨어의 특이한 기동 방식을 그 랜섬웨어의 고유한 성질의 일종으로 볼 수도 있지만, 그 특이한 기동 방식을 가진 랜섬웨어 중에서도 유사한 것들을 '계'별로 분리해볼 계획이다. 물론 1회차 뉴스에서 랜섬웨어의 작동 원리에 대한 내용을 다루기는 했다. 하지만 오늘 다룬 랜섬웨어의 작동 원리는 그저 대부분의 랜섬웨어가 공통적으로 거쳐가는 간단한 공정에 불과하다는 생각이 들어 이 공정에 대해 더 심층적으로 탐구해보고자 다음 주제의 방향을 위와 같이 설정하였다.

[8] 참고자료

(1) Malwarebytes_All about ransomware attacks

https://www.malwarebytes.com/ransomware

(2) Stop Ransomware_Resources_Ransomware 101

https://www.cisa.gov/stopransomware/ransomware-101

(3) 랜섬웨어의 동향과 서비스형 Conti 동작 원리 살펴보기 (2021)

https://csrc.kaist.ac.kr/blog/2021/03/29/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%EC%9D%98-%EB%8F%99%ED%96%A5%EA%B3%BC-%EC%84%9C%EB%B9%84%EC%8A%A4%ED%98%95-conti-%EB%8F%99%EC%9E%91-%EC%9B%90%EB%A6%AC-%EC%82%B4%ED%8E%B4%EB%B3%B4%EA%B8%B0/

(4) 수익성 높은 랜섬웨어 공격, 아직도 전성기는 오지 않았나 (2022)

https://www.boannews.com/media/view.asp?idx=105242&page=1&kind=1

(5) 악성코드란 무엇인가, 바이러스, 웜, 트로이 목마, 그 이상의 것 이해하기_Josh Fruhlinger | CSO (2018)

https://www.itworld.co.kr/news/110408

(6) Advanced Threat Research Report: Jan. (2022)

https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html

(7) 공격 벡터_Certang (2021)

https://certangsecurity.tistory.com/133

(8) Ransomware explained: How it works and how to remove it (2020)

https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html