Spring 2023 Report

최신 웹보안 동향 보고서

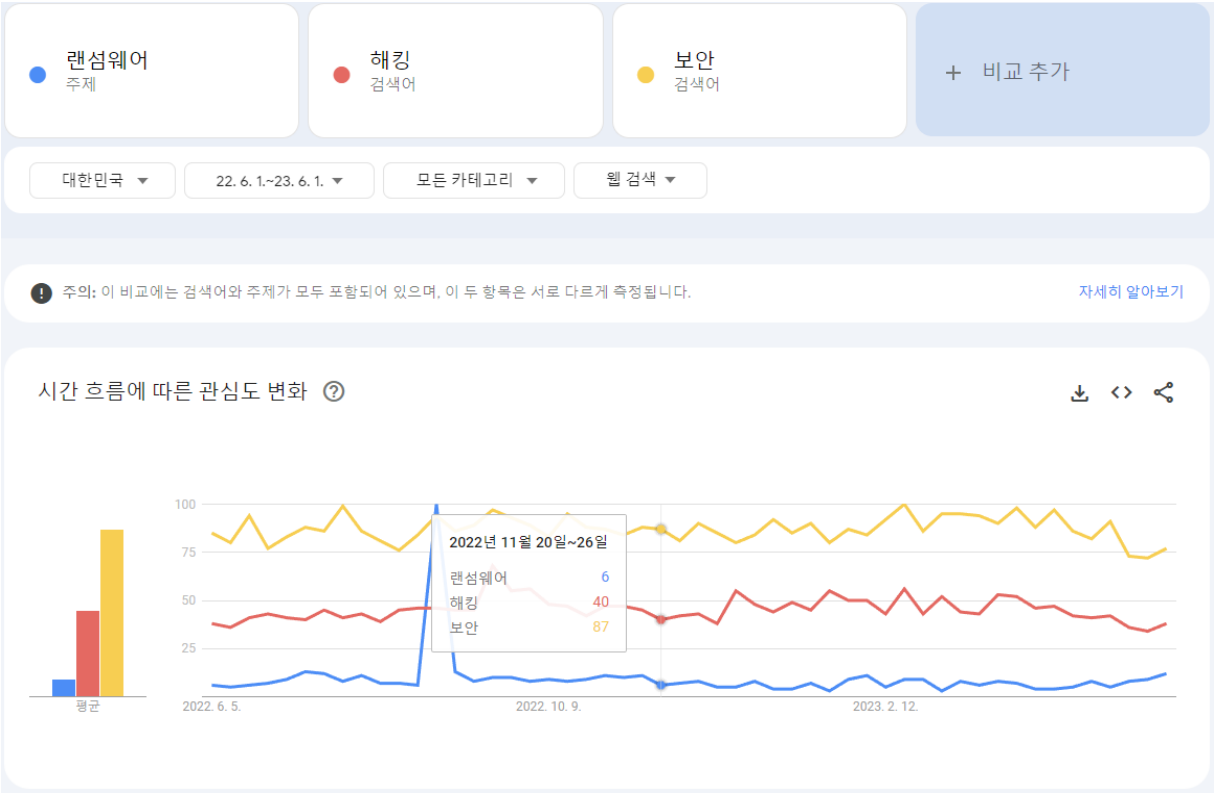
WEBSE

contents

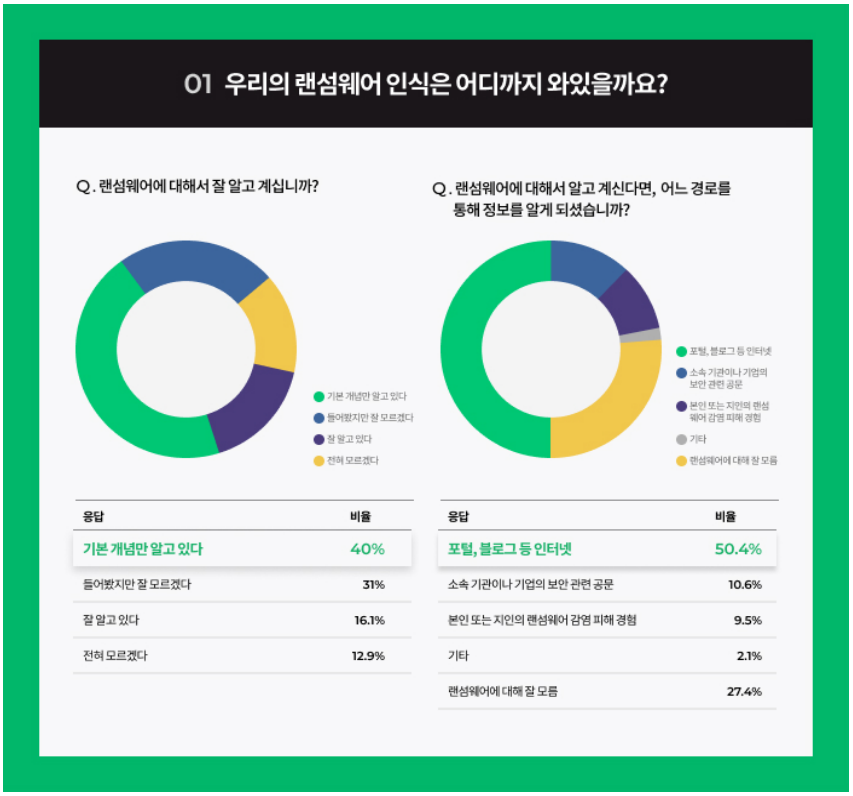
01| 개요

통계로 보는 랜섬웨어

국내에서 1년동안 랜섬웨어에 대한 관심도는 2022월 8월 30일 발생한 알약 랜섬웨어 오진 사태를 제외하면 한자리에 머물 정도로 낮은 관심을 보입니다.

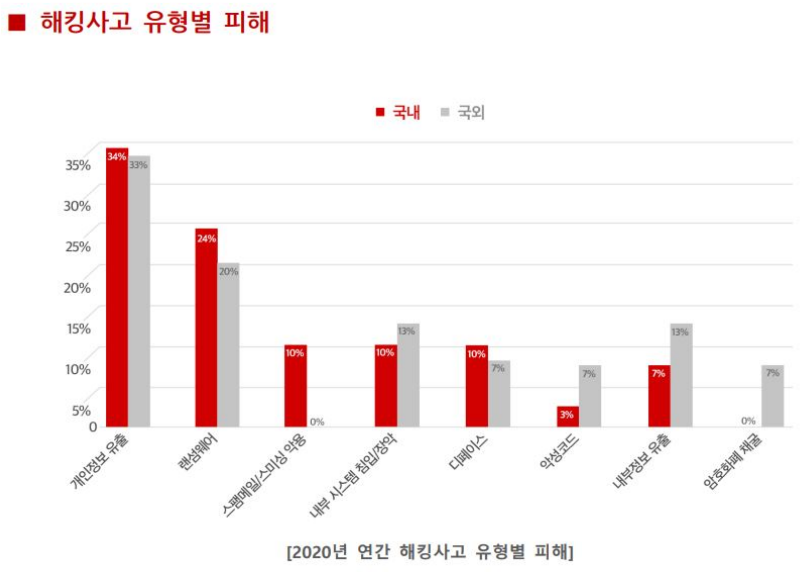


다른 내용인 해킹이나 보안 키워드와 비교해봤을 때 랜섬웨어라는 주제는 상대적으로 낮은 관심을 보이는 것을 알 수 있습니다.



이스트 시큐리티의 2022년 7월 설문조사에서도 랜섬웨어가 무엇인지 잘 알고있는 비중은 17%에 불과하다. 또한 약 13프로의 사람들은 랜섬웨어가 무엇인지 전혀 모르겠다 라고 답변하여 랜섬웨어에 대한 일반 사용자의 수준이 아직은 부족하다는 것으로 나타났습니다.

해킹사고 유형별 피해



[2020년 연간 해킹사고 유형별 피해]

그러나 2022년 해킹사고 유형별 피해에서는 랜섬웨어 피해가 개인정보 유출 피해 다음으로 24%의 비중을 담당하는 것으로 알려졌습니다. 전체 사이버 범죄 중 약 67%가 사이버 사기범죄에 해당하는 점에서 본다면 해킹사고 중 랜섬웨어 공격은 더욱 높은 비중을 차지하는 것을 짐작할 수 있습니다.

02| 최신 취약점 트랜드

2.1 최신 사이버공격 피해

국내 랜섬웨어 피해는 매년 급증하고 있다. 21년 기준 피해액은 약 2조 5천억에 이를거라는 조사가 그 결과이다. 한국 랜섬웨어 침해 대응센터의 조사에 따르면 2015년부터 7년간 피해액을 모두 합치면 6억 8천 6백억에 달할 것으로 조사되었다. 랜섬웨어 피해를 당한곳은 중소기업이 (43%), 소상공인 (25%), 개인 (22%)이 대부분을 차지했다. 반면 공공기관(2%)와 대기업(1%)은 상대적으로 피해를 적게 입은것으로 파악되었다.

국내 랜섬웨어 침해 현황

구분	2015	2016	2017	2018	2019	2020	2021 (추정)	합계
접수 건수	2,678	3,255	4,475	4,652	2,223	2,060	2,000	21,343건
	전화신고 포함				전화신고 제외			
총 피해 금액	1,090 억 원	3,000 억 원	7,000 억 원	1조 2,500 억원	1조 8,000 억원	2조 원	2조 5,000 억원	6조 8,590억 원

KBS 자료 한국랜섬웨어침해대응센터

[그림1] 국내 랜섬웨어 침해 현황

2.2 랜섬웨어 동향

랜섬웨어 공격은 그전적 이익을 얻을 수 있는 기업들을 주요 타겟으로 삼고 있으며 지능화된 공격으로 발전하고 있다. 2021년 러시아 보안기업 GROUP-IP의 랜섬웨어 분석 보고서에 의하면 전체 랜섬웨어 피해 대비 서비형형 랜섬웨어 (Ransomware as a Service, RaaS)에 대한 피해가 64%로 조사되었다. RaaS를 활용하면 배경지식이 많지 않은 사람도 손쉽게 랜섬웨어 공격을 감행할 수 있다. 따라서 앞으로 RaaS 공격 비율은 앞으로도 더욱 증가할

것으로 예상된다.

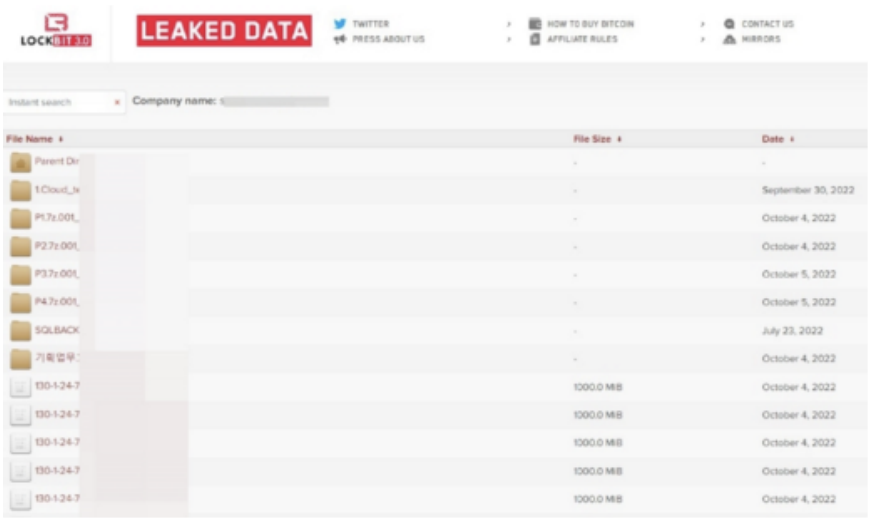
또한 APT 공격도 다시금 주목받고 있다. APT 공격 방식을 결합한 랜섬웨어는 워터링홀,드라이브 바이 다운로드와 같은 사회공학기법을 이용해 사용자 계정을 탈취하거나 알려진 취약점을 이용해 침투한다. 코로나-19로 인해 원격 근무가 많아지면서 공격 표면이 확대돼 공격자가 취약점에 접근하는게 더욱 쉬워졌다. 팔로알토 네트웍스가 조사한 지난 21년 랜섬웨어 유출 사이트에 공개된 피해 건수는 2566개로 전년대비 85% 증가한 것이다. 이 중 유명한 콘티에 대한 피해 사례는 511건, 록빗 2.0에 의한 것은 406건이었다.

록빗 랜섬웨어 피해 사례

록빗은 서비스형 랜섬웨어로 이는 개발자가 랜섬웨어를 제작해 판매하고 공격자는 이를 구매해 유표하는 형태로 공격에 성공할 경우 수익을 나눠가지는 랜섬웨어를 말한다. 또한 랜섬웨어의 버전 업데이트와 버그바운티를 통해 계속해서 발전하고 있기에 각별한 주의가 필요한 랜섬웨어 중 하나이다.

피해 사례로는 가장 최근 lockbit이 대한민국 국세청을 해킹했다고 주장하며, 탈취한 파일을 공개해 포스팅 하는 사건이 있었다.

이외에도 지난 22년 8월 29일 록빗 3.0 이 s사의 해킹사실을 공지하며 입증할 샘플 사진을 올린 사건이 있다. 기업은 록빗으로부터 2TB이 달하는 자료를 정보를 탈취했으며 첫 공격을 성공한 지난 7월 345 비트코인을 요구했으나 기업은 이를 지불하지 않았으며 이에 대해 탈취한 자료를 모두 업로드 한것으로 나타났다.



[그림2] 록빗에서 공개한 S사의 해킹 자료

royal mail의 록빗 감염 사례

지난 1월 영국의 한 우편 업체인 Royal Mail에서도 록빗 랜섬웨어에 감염되는 사건이 있었다. 이로인해 한달 넘게 국제 수출 서비스가 중단되는 피해가 생겼다. 현재는 모든 서비스를 복구했으며 lockbit 랜섬웨어 갱단이 탈취한 데이터를 유출하며 몸값을 요구했지만 후에 복호화 도구를 제공하며 데이터 공개를 중단한 것으로 협상했다고 나왔다. Royal Mail이 몸값을 지불했는지는 확실하게 나타나지 않은것으로 보인다.

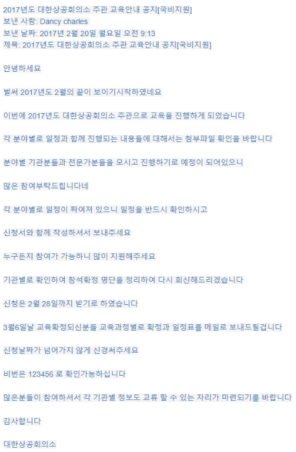
https://techcrunch.com/2023/02/23/royal-mail-restores-global-shipping-weeks-after-lockbit-ransomware-attack/

Venus Locker 랜섬웨어

venus locker랜섬웨어는 메일의 첨부파일, p2p를 이용한 다운로드나 인터넷 홈페이지를 통해서 감염될 수 있는 랜섬웨어이다.

랜섬웨어에 걸리게 될 경우 컴퓨터는 일시적으로 느려진다는 특징이 있다. 이후 바탕화면의 이미지가 바뀌고 pc에서 접근할 수 있는 모든 저장소의 파일들이 암호화되어 파일을 열어볼 수 없게된다. 또한 venusLocker파일의 확장자가 venusp 혹은 venusf로 변경된다. venusLocker 랜섬웨어는 피해자에게 1btc의 금액을 요구하는 특징이 있으며 피해 사례에서도 회사내에 감염된 pc 2대에 대해 한화 약 1,210,000원에 달하는 가상화폐를 요구한것을 확인할 수 있었다.

이외의 피해 사례에서도 이메일 첨부파일을 실행한 교내 사용자 2명이 700GB이상의 첨부 파일을 실행하며 venusLocker 랜섬웨어에 감염되었고 이후 공격자로부터 3btc의 가상화폐를 요구받은것을 볼 수 있었다.


2017년도 대한상공회의소 주관 교육안내 공지[국비지원]
보낸 사람: Dancy charles
보낸 날짜: 2017년 2월 20일 월요일 오전 9:13
제목: 2017년도 대한상공회의소 주관 교육안내 공지[국비지원]

안녕하세요

봄버 2017년도 2월의 끝이 보이기시작하였네요

이번에 2017년도 대한상공회의소 주관으로 교육을 진행하게 되었습니다

각 분야별로 일정과 함께 진행되는 내용들에 대해서는 첨부파일 확인을 바랍니다

분야별 기관분들과 전문가분들을 모시고 진행하기로 예정이 되어있으니

많은 참여부탁드립니다네

각 분야별로 일정이 짜여져 있으니 일정을 반드시 확인하시고

신청서와 함께 작성하셔서 보내주세요

누구든지 참여가 가능하니 많이 지원해주세요

기관별로 확인하여 참석확정 명단을 정리하여 다시 회신해드리겠습니다

신청은 2월 28일까지 받기로 하였습니다

3월6일날 교육확정되신분들 교육과정별로 확정과 일정표를 메일로 보내드릴겁니다

신청날짜가 넘어가지 않게 신경써주세요

비번은 123456 로 확인가능하십니다

많은분들이 참여하셔서 각 기관별 정보도 교류 할 수 있는 자리가 마련되기를 바랍니다

감사합니다

대한상공회의소

[그림3] venus 랜섬웨어 메일

venusLocker 랜섬웨어는 한글로 되어 있다는 특징이 있으며, 첨부파일을 여는 순간 감염이 된다. 따라서 소상공인들이 당하기 쉬운 랜섬웨어이다.

귀신 랜섬웨어

https://www.soft2000.com/29855

https://www.inews24.com/view/1514240

귀신 랜섬웨어는 한국형 랜섬웨어로 국내 여러 기업, 기관들을 공격해왔다.

귀신(Gwisin) 랜섬웨어는 매그니베르(Magniber) 랜섬웨어와 동일하게 MSI 설치 파일 형태로 동작하지만, 불특정 다수를 대상으로 유포되는 매그니베르와 달리 특정 기업을 타겟으로 제작되어 유포되고 있다. 참고로, MSI 파일이란 윈도우 인스톨러 패키지 파일을 뜻한다.

귀신 랜섬웨어는 파일 실행만으로는 악성 행위가 발현되지 않으며, 특별한 실행 인자 값이 필요하다. 이 때문에, 샌드박스 기반 보안 제품에서 파일을 실행하는 것만으로는 악성 행위가 발생하지 않아 탐지가 어려울 수 있다.

피해 사례로는 국내 콜택시 배차관리 사업자인 오토피온이 랜섬웨어 공격을 받아 대전, 부산, 인천, 춘천 등 국내 30여 지역의 콜택시 운영이 중단된 사건, 광주·전남 지역의 골프장이 랜섬웨어에 감염돼 홈페이지와 예약시스템이 중단된 사례가 주요 사례로 꼽힌다.

콘티 랜섬웨어

콘티 랜섬웨어는 클라우드 컴퓨팅과 결합한 RaaS 기법을 이용한 공격 랜섬웨어이다. 콘티는 2021년만 2억 달러에 가까운 금액을 피해자들로 부터 갈취한 것으로 나타났다.

<parker Hannifin>

미국의 대형 제조업체 parker hannifin이 conti랜섬웨어 공격으로 인해 직원 정보가 유출되었다고 발표했다. 이로인해 개인 정보가 손상될 가능성이 있는 직원에게 알리는 절차를 시작했다. parker는 연 매출이 140억 달러 이상이며 직원은 57,000에 달하는 큰 회사인 만큼 이 사건을 심각하게 받아들이고 있다. 이 파일에는 현재 및 이전 직원, 그들의 부양 가족 및 Parker의 그룹 건강 플랜 구성원과 관련된 정보가 포함될 수 있다. Parker는 영향을 받는 직원에게 신원 보호 지원을 제공할 예정입라 했다. 또한 Conti는 공격에 대한 책임을 주장하고 Parker의 데이터를 강탈한 것으로 추정됩니다.

https://www.secureworld.io/industry-news/parker-manufacturing-conti-ransomware

<독일 풍력 터빈 제조 업체 **nordx** 피해 사례>

세계 최대의 제조업체 중 하나인 Nordex Groupdl 지난 22년 4월 콘티 랜섬웨어로 부터 공격을 받았다. 공격의 영향으로 업체는 랜섬웨어에 감염되었을 수 있는 시스템들을 모두 종료했다. conti는 데이터를 유출하지 않고 있기에 회사와 몸값을 협상하고 있을것으로 나타났다.

이 사건은 세계에서 가장 큰 재생 에너지 회사 중 하나를 사이버 공격 했다는 점에서 재생가능 에너지에 대한 의존도를 높이려는 전 세계의 성장 동력에 막대한 타격을 주었다.

https://www.hackread.com/conti-ransomware-german-wind-turbine-giant-nordex/

2.3 DBD & Watering hole 기반 공격 사례

dbd 이용한 랜섬웨어 피해사례

17년 5월 wannaCry 랜섬웨어 공격이 있다. 이 공격은 악성 코드가 포함된 이메일을 통해 전파되었으며, 이메일 수신자가 링크를 클릭하면 악성 코드가 다운로드되고 실행되어 전체 네트워크를 감염시키는 방식으로 작동했다.

이외에 kaseya 랜섬웨어 공격이 있다. 이 공격은 kaseya의 소프트웨어 업데이트 서버에 악성 코드가 심어져 이를 다운로드한 사용자들의 컴퓨터를 감염시켰다. 이 공격으로 수천개의 it 서비스 제공업체를 포함한 수백만대의 컴퓨터를 감염시켰으며, 수천개의 회사와 기관이 데이터와 시스템을 잃게 되었다.

http://m.boannews.com/html/detail.html?idx=106772

<health Service Executive 랜섬웨어 공격, 워터링 홀 사용>

지난 21년 5월 14일 아일랜드의 hse가 워터링 홀 공격을 당해 랜섬웨어에 감염되었던 사건이다. 이 공격은 hse의 웹사이트에 악성 코드가 삽입되어 해당 웹 사이트를 방문한 사용자들의 컴퓨터에 랜섬웨어를 설치하는 형태로 이루어졌다. 이 공격으로 hse의 모든 시스템과 서버는 마비가 되어 더이상 의료 서비스를 제공할 수 없는 상황이 되었다.

공격자들은 이후 서비스 복구를 위해 hse에 2천만 달러를 요구했으나 정부는 돈을 지불하지 않겠다고 말했다. 이 공격으로 아일랜드 병원의 서비스가 중단되었으며 이로인해 hse의 전국 및 지역 네트워크가 거의 폐쇄되어 많은 왜래 진료소와 의료 서비스가 취소되었다.

https://abcnews.go.com/International/irelands-health-service-hit-significant-ransomware-attack/story?id=77685241

https://cyberlaw.ccdcoe.org/wiki/Ireland's_Health_Service_Executive_ransomware_attack_(2021)

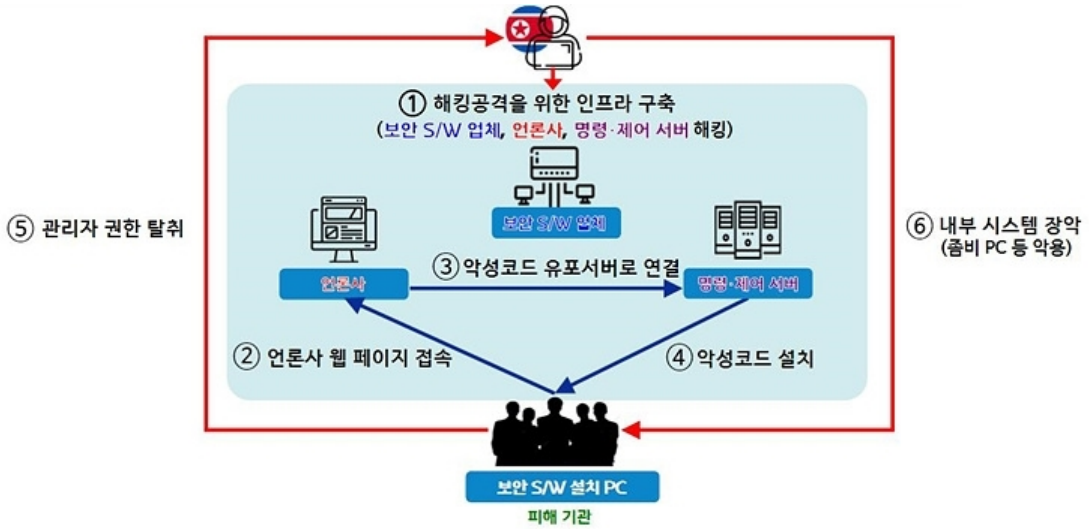
워터링홀을 이용한 랜섬웨어 피해 사례

20년 2월, 미국 경제 발전 연구소의 웹사이트가 워터링 홀에 당해 랜섬웨어에 감염되는 사례가 있다. 공격을 받은 eda는 모든 서버와 데이터가 랜섬웨어로 암호화되어 사용이 불가능해졌으며 이로인해 일정시간 동안 업무를 중단하게 되었다.

<북한 워터링홀을 이용한 악성코드 배포 사건>

지난 23년 4월 북한의 해킹 그룹 라자루스가 워터링 홀 기법을 활용해 랜섬웨어를 배포한 사건이 있었다. 해킹 정황을 살펴보면 국내 유용 금융보안인증 업체를 해킹한 후, 소프트웨어 취약점을 악용해 공격에 활용할 웹 서버와 명령,제어 경유지 등 공격 인프라를 장기간 치밀하게 준비하였다. 또한

특정 언론사 사이트에 접속할 경우 자동으로 악성코드가 설치되는 워터링 홀 수법을 이용하였으며 이를 통해 국내 61개 기관이 해킹되는 등의 대규모 피해가 발생한 걸 확인 할 수 있었다.



[그림4] Watering hole 공격과정

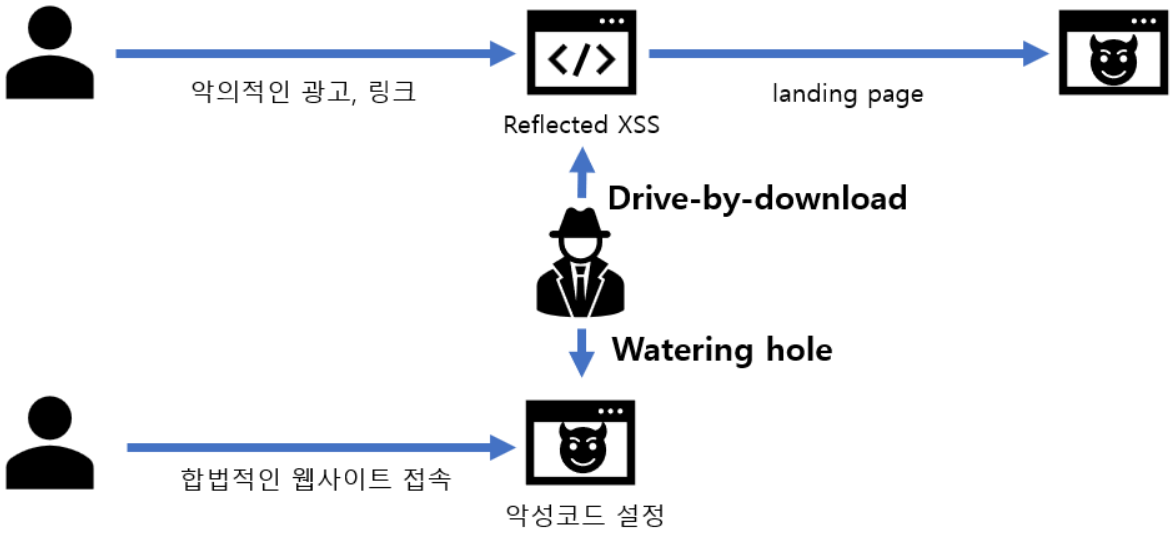
참고 자료:https://www.boannews.com/media/view.asp?idx=117224

03| 랜섬웨어 가상 시나리오

3.0 Introduction

최근 발생하는 랜섬웨어 공격은 중소기업이나 소상공인 그리고 개인을 대상으로 발생 빈도가 늘어나는 것을 알 수 있다. 이러한 현상은 자주 대상이 이용하는 웹에서 랜섬웨어가 감염되어 발생했을 가능성이 매우 높다고 볼 수 있다. 이를 통해 우리는 몇가지 웹기반 랜섬웨어 시나리오를 제공한다.

3.1 시나리오 개요



[그림5] 랜섬웨어 감염 시나리오

웹에서 랜섬웨어가 감염되는 대표적인 경로는 다음과 같다.

1) 광고나 링크를 통해 랜딩 페이지로 유도 후 **Drive-by download** 공격

2) 사전에 공격대상이 자주 이용하는 페이지에 **Watering hole** 공격을 수행

1) Drive-by-download

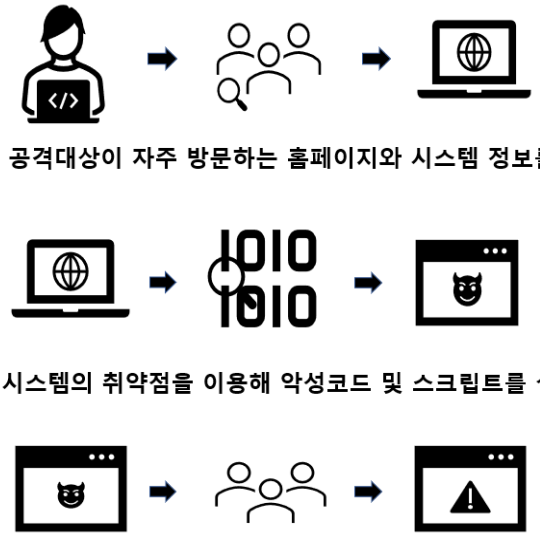
사용자 모르게 다운로드 되어 실행되는 악성 프로그램으로 웹 브라우저나 웹 어플리케이션의 취약점을 이용하여 사이트 방문시 자동으로 악성코드를 다운로드해서 감염되게 하는 공격유형을 의미

[그림6] Drive-by-download 공격

2) Watering hole

타겟이 자주 들어가는 홈페이지를 파악했다가, 그 홈페이지의 취약점을 통해 악성코드를 심어 사용자가 모르게 해당 악성코드를 다운로드 받게 하고, 다운로드 된 악성코드를 통해 공격을 하는 유형.

대표적으로 브라우저에서 동작하는 Flash, Javascript, VBScript, ActiveX, XSS, HTML, Image 취약점 등을 공격에 사용한다.



[그림7] Watering hole 공격

3.1 시나리오 분석

본 시나리오를 보다 체계적으로 대응하기 위해 사이버 킬체인으로 시나리오를 단계적으로 분류한다. 이를 통해 시나리오에서 각 단계별 대응책을 마련할 수 있으며, 해당 시나리오가 충분히 실현가능한 공격이란 점을 다시 확인할 수 있다.

사이버 킬체인**(Cyber Kill Chain)**이란**?**

사이버킬체인이란 군사용어 킬체인에서 비롯되어 생성된 용어로, 사이버 공격을 방어하기 위한 적극적인 방어 전략이며 여러 공격 단계들 중 일부를 무력화 또는 지연시켜 공격의 효율성을 낮추고 피해를 최소화하는데 그 목적이 있다.

프로세스상에 따른 대응이기 때문에 공격자가 지속적으로 특정 대상을 노리는 APT(지능형 지속 공격)를 설명하는데 자주 언급되는 전략 중 하나이기도 하다. 다양한 사이버 공격 중 APT공격을 분석해보면 일반적으로 아래의 5가지 단계를 거치게 된다. 따라서 사이버 공격을 각 단계별로 분석해 각 단계에서 발생하는 위협 요소를 파악하고 대응한다면 모든 공격을 막을 수는 없지만 피해를 최소화 할 수 있다. 한 마디로 발생하는 모든 사이버 공격을 100% 막아내는 것은 어렵기 때문에 공격자의 입장에 서서 공격의 절차를 파악 및 분석하여 위협요소를 단계별로 제거해나가 피해를 최소화하는 일련의 활동인 것이다.

앞서 언급했던 것과 같이 사이버킬체인은 크게 5단계로 구성된다.

- 정찰(Reconnaissance)
- 무기화 및 전달(Weaponization and Delivery)
- 익스플로잇/설치(Exploit and Installation)
- 명령 및 제어(Command and Control)
- 행동 및 탈출(Action and exfiltration)

이 5단계는 방어자의 입장에서 공격 전(before)과 공격 후(after)로 나눌 수 있으며 공격 전(before)단계에서 체인을 끊어내는 게 이 전략의 목표라고 할 수 있다.

1단계	정찰(Reconnaissance)	공격대상 인프라에 침투해 거점을 확보하고 오랫동안 정찰 수행
2단계	무기화 및 전달 (Weaponization and Delivery)	공격 목표를 달성하기 위해 정보를 수집하고 권한을 획득
3단계	익스플로잇/설치 (Exploit and Installation)	공격용 악성코드를 만들어 설치
4단계	명령 및 제어 (Command and Control)	원격에서 명령 실행
5단계	행동 및 탈출 (Action and exfiltration)	정보유출 혹은 시스템 파괴 후 증거 삭제

[표1] 사이버킬체인 단계

1) Drive-by-download Cyber kill chain

첫 시나리오를 사이버 킬체인에 따라 나누면 다음과 같다.

정찰(Reconnaissance)	스캐닝 도구를 활용해 공격대상 취약점 탐색
무기화 및 전달(Weaponization and Delivery)	악의적인 광고나 링크로 대상 유도
익스플로잇/설치(Exploit and Installation)	Drive-by-download로 악성코드 설치
명령 및 제어(Command and Control)	C2서버와 통신하며 악성코드 확산
행동 및 탈출(Action and exfiltration)	대상 내부의 데이터 암호화

[표2] Drive-by-download 시나리오 사이버킬체인

2) Watering hole Cyber kill chain

두번째 Watering hole 공격을 사이버 킬체인에 따라 나누면 다음과 같다.

정찰(Reconnaissance)	공격대상이 자주 접속하는 사이트 탐색
무기화 및 전달 (Weaponization and Delivery)	웹사이트 설정 및 해당 사이트 취약점 분석
익스플로잇/설치 (Exploit and Installation)	Watering hole로 악성코드 삽입 및 설치
명령 및 제어(Command and Control)	C2서버와 통신하며 악성코드 확산
행동 및 탈출(Action and exfiltration)	대상 내부의 데이터 암호화

[표3] Watering hole 시나리오 사이버킬체인

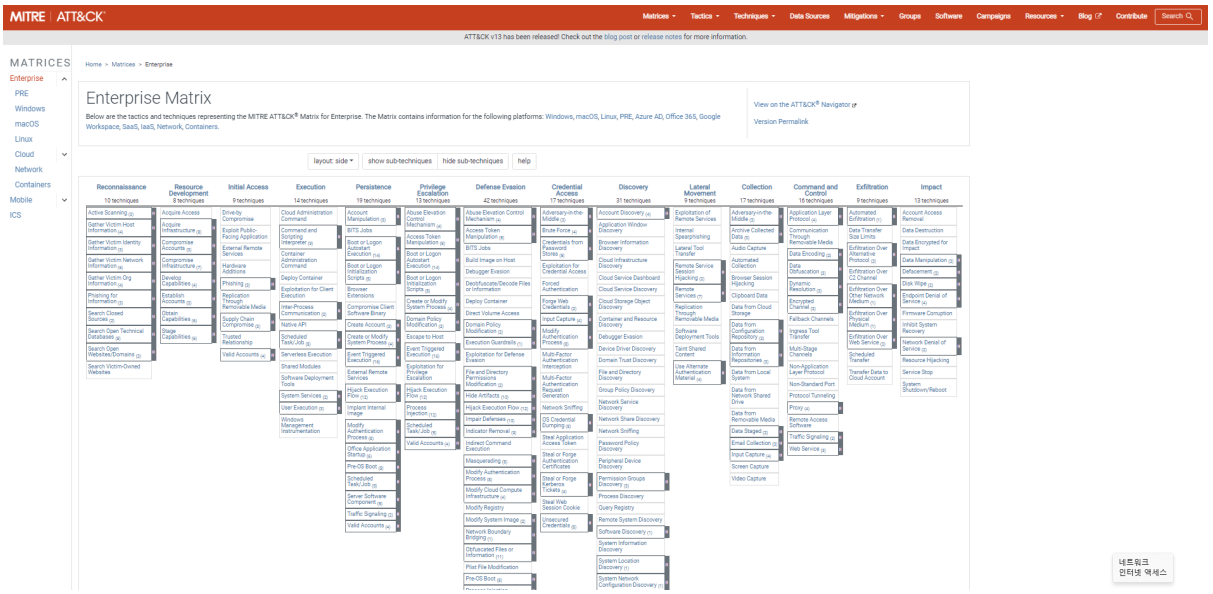
3.1 MITRE ATT&CK TTPS 매핑

사이버 킬체인에 맞추어 각 공격 시나리오를 단계별로 분류했다. 하지만 단계별 시나리오를 구분하여도 각 단계에서 발생할 수 있는 공격은 다양하다. 우리는 이를 각 단계에서 발생가능한 공격을 나열하여 효과적인 대응책을 구성할 수 있다.

MITRE ATT&CK이란?

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)은 실제 사이버 공격 사례를 관찰한 후 공격자가 사용한 악의적 행위(Adversary behaviors)에 대해서 공격방법(Tactics)과 기술(Techniques)의 관점으로 분석해 다양한 공격그룹의 공격기법 들에 대한 정보를 분류해 목록화 해 놓은 표준적인 데이터이다.

전통적인 사이버 킬체인의 개념과는 약간 관점을 달리하여 지능화된 공격의 탐지를 향상시키기 위해 위협적인 전술과 기술을 체계화(패턴화)한 것인데, 원래 ATT&CK는 MITRE에서 윈도우 기업 네트워크 환경에 사용되는 해킹 공격에 대해서 방법(Tactics), 기술(Techniques), 절차(Procedures) 등 TTPs를 문서화하는 것으로 시작되었으며 이후 공격자로부터 발생한 일관된 공격 행동 패턴에 대한 분석을 기반으로 TTPs 정보를 매핑하여 공격자의 행위를 식별해 줄 수 있는 프레임워크로 발전하였다.



[그림8] MITRE ATT&CK 홈페이지

Tactics(공격 전술 정보)

- Tactics는 공격자의 공격목표에 따른 행동을 나타냄
- 상황에 따른 각각의 Techniques에 대한 범주 역할
- 공격 목적에 따라 지속성, 정보탐색, 실행, 파일 추출 등 다양하게 분류

Techniques(공격 기술 정보)

- 공격자가 목표에 대한 Tactic 을 달성하기 위한 방법을 나타냄
- 공격자의 공격(Technique)을 통해 발생하는 결과(피해)를 명시
- 앞서 분류된 Tactics에 따라 다양한 Techniques 들이 존재할 수 있음

MITRE ATT&CK Navigator

앞서 말했던 TTPS를 시각적으로 매핑하여 보여줄 수 있는 기능이다.

여러가지의 시나리오를 구성하고 각 시나리오를 합침으로써 하나의 공격과정을 시각적으로 보여줄 수 있다.

먼저 각 시나리오에 Tatics를 매핑한다.

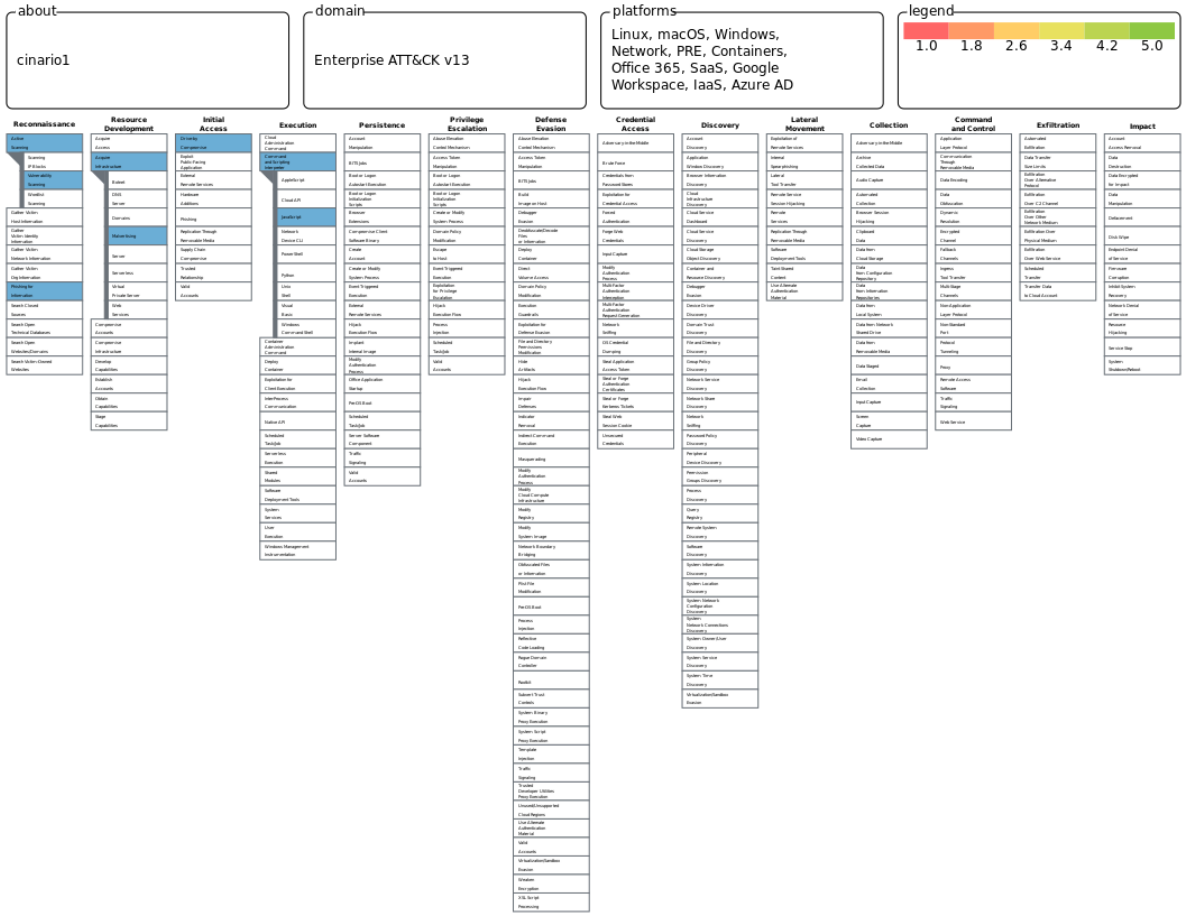
1) Drive-by-download TTPS Mapping

Drive-by download을 사이버 킬체인으로 분류하는 과정을 통해 공격과정을 단계적으로 볼 수 있게 되었다. 이번 과정에서는 MITRE ATT&CK의 tatics를 사이버 킬체인에 맞게 매핑하여 공격과정을 더욱 상세하게 분류한다.

정찰(Reconnaissance)	Active scanning - 스캐닝 도구(ex: metaexploit, nmap)
자원개발 (Resource Development)	Acquire Infrastructure - Malvertising(악의적인 광고)
초기접근(Initial Access)	Drive-by Compromise - Drive-by download
실행(Execution)	Command and Scripting Interpreter - javascript

[표4] Drive-by dowload tatics mapping

Tatics 매핑 이후 다음 표를 활용해 MITRE ATT&CK navigator를 제작한다.



[그림9] 시나리오1 TTPS 매핑

2) Watering hole TTPS Mapping

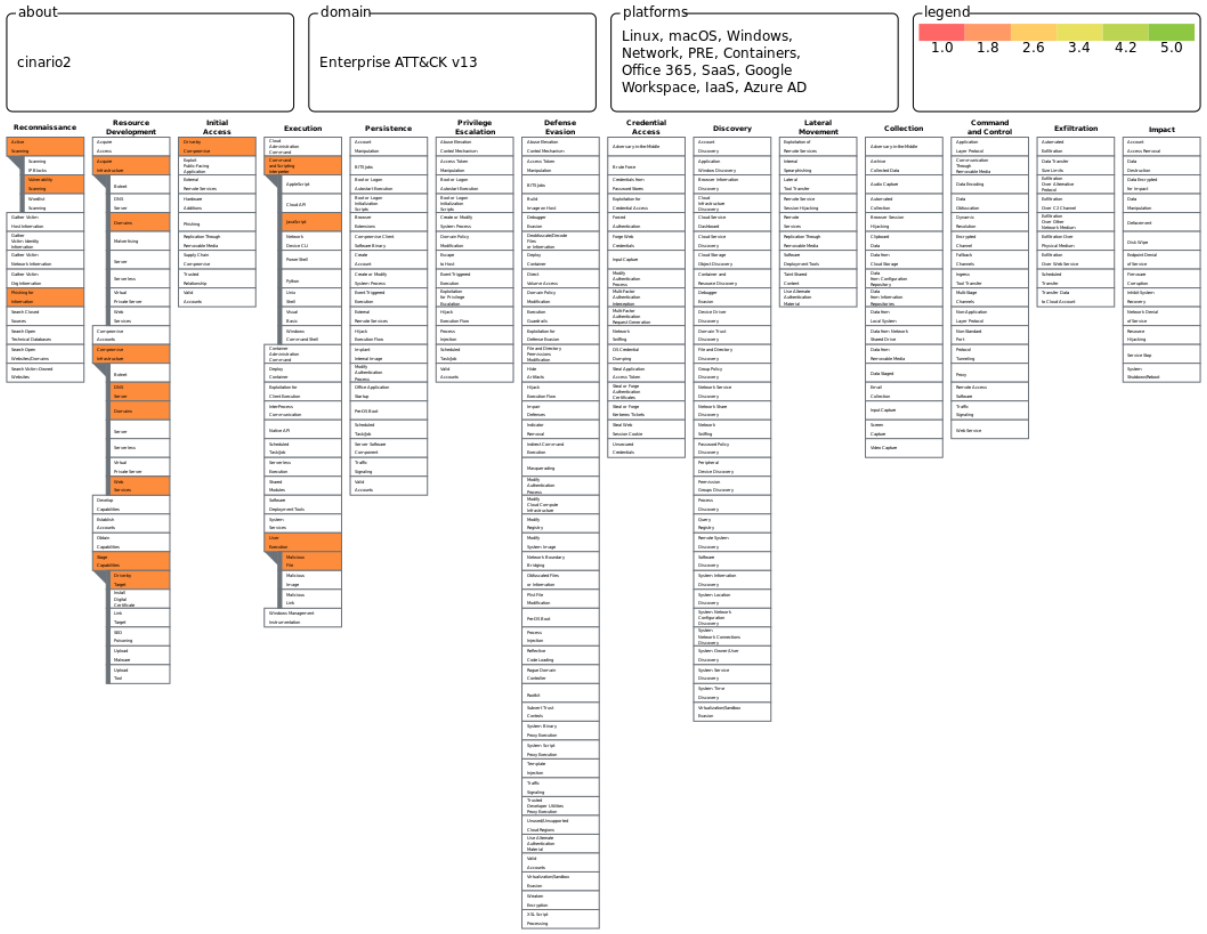
Watering hole 공격 시나리오도 Tatics를 매핑하여 볼 수 있다.

정찰(Reconnaissance)	Active scanning - 스캐닝 도구(ex: metaexploit, nmap)
자원개발(Resource Development)	Stage capabilities – Drive-by target Acquire infrastructure - Domains Compromise infrastructure - DNS server, Domains, web services

초기접근(Initial Access)	Drive-by Compromise – Watering hole
실행(Execution)	Command and Scripting Interpreter – javascript User Excution – Malicious file

[표5] Watering hole tactics mapping

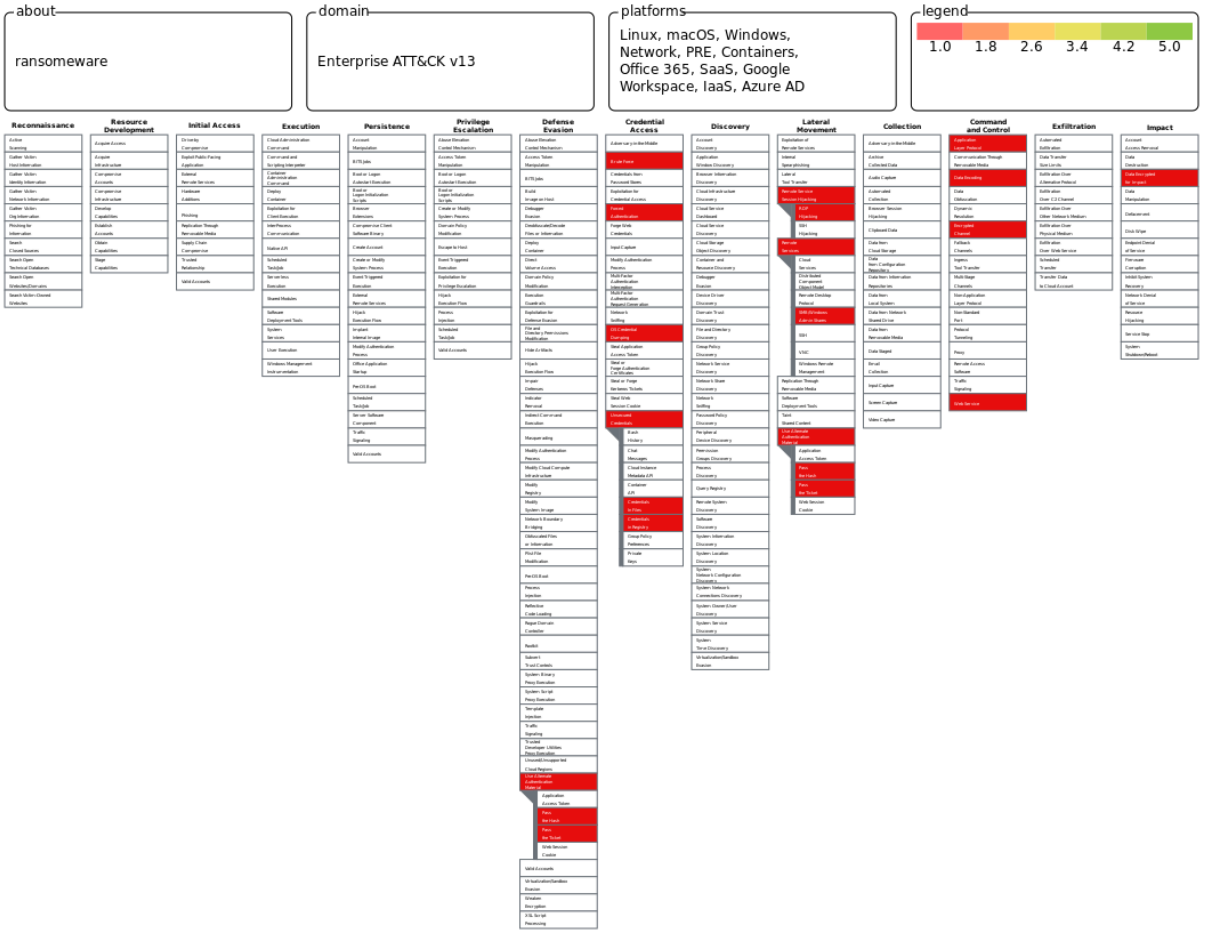
Tatics 매핑 이후 다음 표를 활용해 MITRE ATT&CK navigator를 제작한다.



[그림10] 시나리오2 TTPS 매핑

3) Ransomware TTPS Mapping

다음은 랜섬웨어가 공격대상 내부로 접근한 이후 확산 및 공격과정을 MITRE ATT&CK Navigator로 매핑하였다.



[그림11] 랜섬웨어 TTPS 매핑

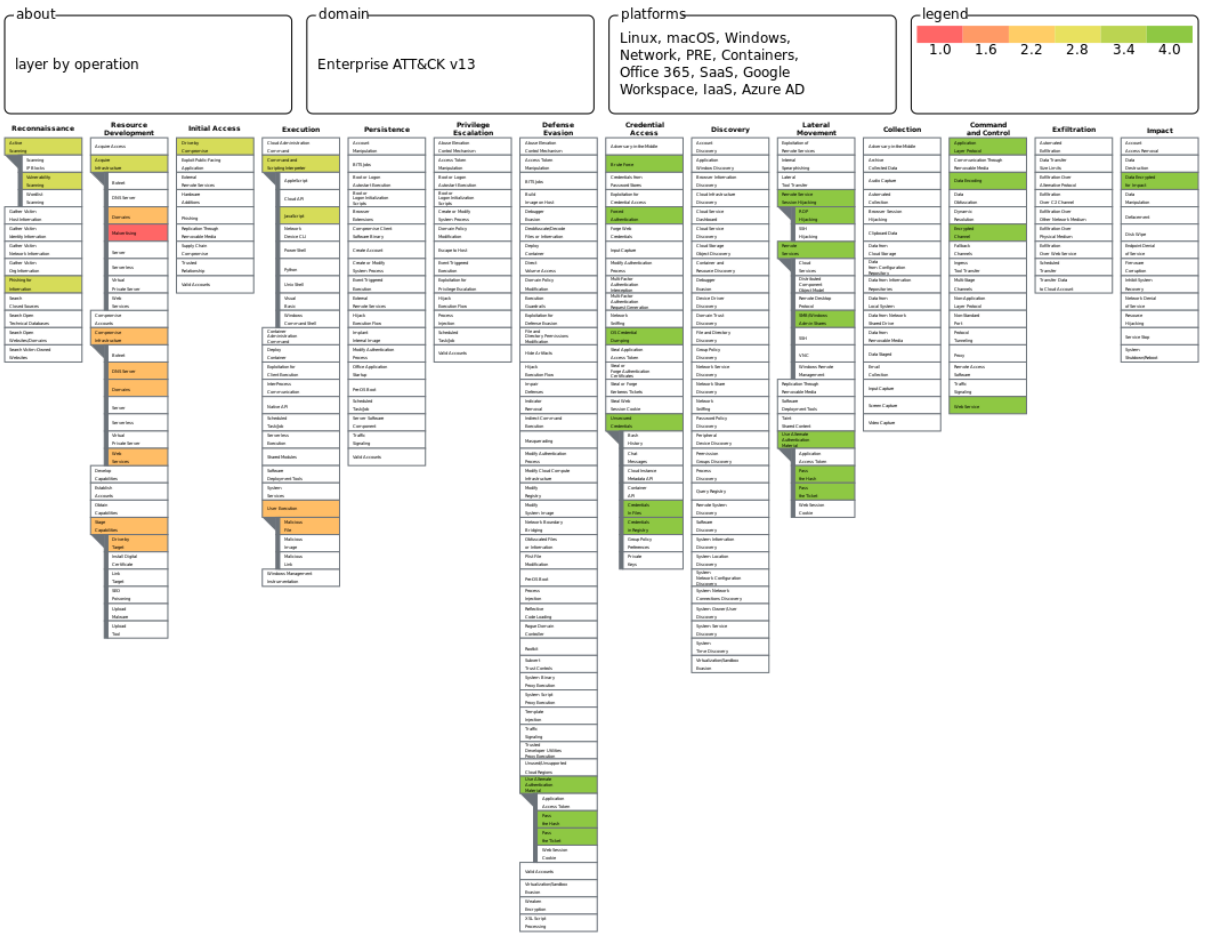
4) Linking TTPS Mapping

MITRE ATT&CK Navigator로 각 시나리오를 TTPS로 매핑하였다.

이를 통해 웹에서 발생할 수 있는 랜섬웨어 공격과정을 시각적으로 볼 수 있다.

Navigator로 생성하는 과정에서 각 공격에 값을 매겨 합쳤기 때문에, 공격의 색이 초록색에 가까울수록 두 시나리오에서 모두 발생 가능한 공격이란 뜻이고 더욱 신경써야 할 공격이란 뜻이다.

다음 단계에서는 초반 두가지 Tatics인 정찰(Reconnaissance)과 자원개발(Resource Development)에 대해 실습 및 대응방법을 설명한다.



[그림12] 통합 TTPS 매핑

04| 공격 및 대응책

해당 공격은 사이버 킬체인에 맞추어 정찰(Reconnaissance)과 자원개발(Resource Development) 단계에 대해 환경 설정 후 해당 의심할 수 있는 취약한 부분에 대해 간단하게 해결할 수 있는 방법을 제시한다.

WORD PRESS란?

워드프레스는 세계 최대의 자유-오픈 소스 소프트웨어 저작물 관리 시스템로 최근 W3Techs의 정보에 의하면 최근 2022년도 기준으로 2023년 5월까지의 통계를 보면 여전히 wordpress는 전세계적으로 약 43%를 차지 할 정도로 수많은 wordpress를 통해 제작된 웹 상용 및 연구 목적으로 사용되고 있다.

	2022 1 May	2022 1 Jun	2022 1 Jul	2022 1 Aug	2022 1 Sep	2022 1 Oct	2022 1 Nov	2022 1 Dec	2023 1 Jan	2023 1 Feb	2023 1 Mar	2023 1 Apr	2023 1 May	2023 23 May
None	33.1%	33.0%	33.1%	33.1%	33.0%	33.1%	32.9%	32.8%	32.3%	32.0%	31.9%	31.7%	31.7%	31.8%
WordPress	43.0%	42.9%	43.0%	43.0%	43.0%	43.0%	43.1%	43.0%	43.1%	43.2%	43.2%	43.2%	43.2%	43.1%
Shopify	4.3%	4.3%	4.2%	4.2%	4.1%	4.1%	4.1%	4.0%	3.8%	3.8%	3.8%	3.8%	3.8%	3.8%
Wix	2.3%	2.3%	2.3%	2.3%	2.3%	2.3%	2.3%	2.4%	2.4%	2.5%	2.5%	2.5%	2.5%	2.5%
Squarespace	2.0%	2.0%	2.0%	2.0%	2.0%	2.0%	2.0%	2.0%	2.0%	2.1%	2.1%	2.1%	2.1%	2.1%
Joomla	1.7%	1.6%	1.6%	1.6%	1.6%	1.6%	1.6%	1.7%	1.8%	1.8%	1.8%	1.8%	1.8%	1.8%
Drupal	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%
Adobe Systems	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%	1.1%
PrestaShop	0.5%	0.5%	0.5%	0.6%	0.6%	0.6%	0.6%	0.6%	0.7%	0.7%	0.7%	0.7%	0.8%	0.8%
Google Systems	1.0%	0.9%	0.9%	0.9%	0.9%	0.9%	0.9%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%
Bitrix	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.8%	0.7%	0.7%	0.7%	0.7%	0.7%
Webflow	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%	0.6%
OpenCart	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%	0.6%	0.6%	0.6%

[그림13] W3Techs에서 제공하는 콘텐츠 관리 시스템 사용 통계의 과거 추세 표

해당 환경 구축은 대중적으로 사용되고 있는 word press 최신 버전인 6.2버전을 기반으로 제작된 웹으로 진행한다.

4.1 자원개발(Resource Development)

환경 설정

1) Server 설정
   - Ubuntu 20.04 (메일서버 및 웹서버)
   - Ubuntu-Server 20.04(메일서버)
2) Client 설정

- Kali Linux 22.04(공격자PC)
- Windows 10(Client PC)

3) Web Scanner(open source)
   - OWASP Zap(GUI 기반)
   - Arachni (Web 기반)

각각의 환경은 서버용, 클라이언트용, 사용할 도구를 이용하여 환경 설정 후 도구를 이용해 취약점 및 제공하는 웹의 취약할 만한 부분을 스캔한다.

해당 과정에서 scanner는 공격자 PC인 kali에서 진행되었지만, 해당 scanner는 Client PC인 window에서도 설치 후 바로 사용이 가능하다.

4.2 정찰(Reconnaissance)

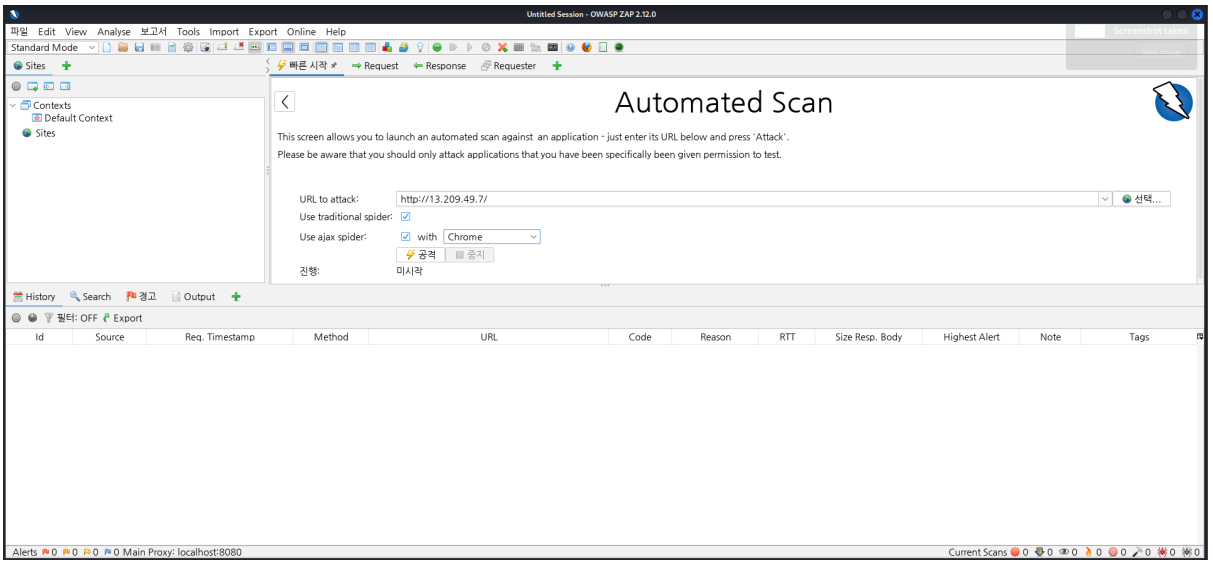
OWASP Zap

OWASP ZAP은 오픈 소스 웹 애플리케이션 보안 스캐너로 GUI 기반으로 이루어져 있다.

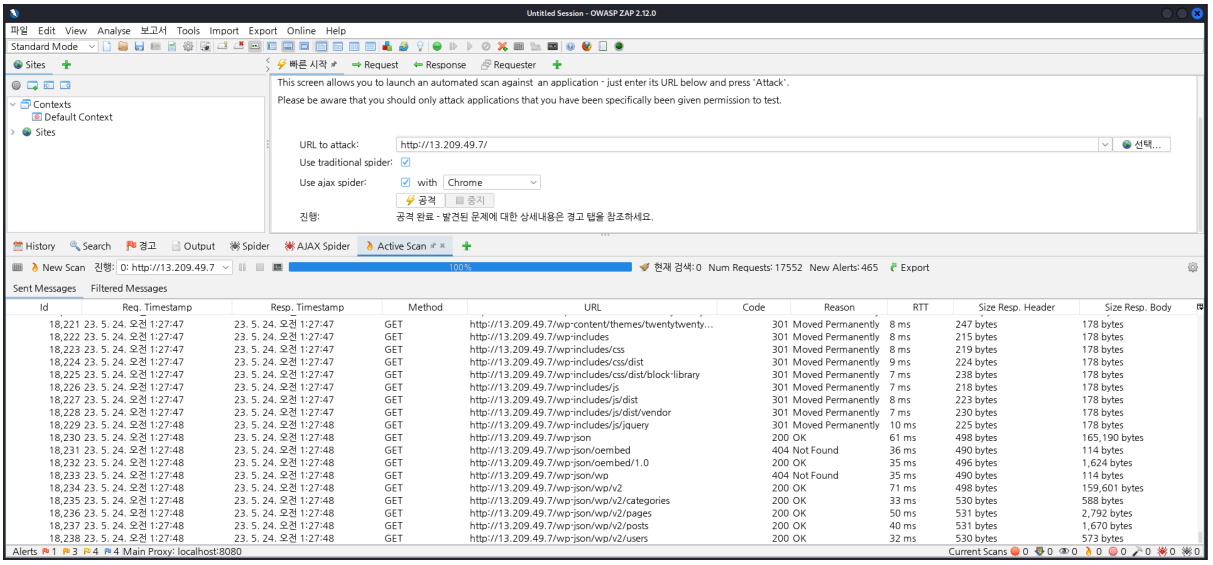
우분투 기반의 경우 sudo apt install zaproxy를 통해 설치가 가능하다.

윈도우의 경우 zaproxy.org를 통해 설치가 가능하다.

OWASP Zap 이용한 간편 취약 분석 과정 및 대응책

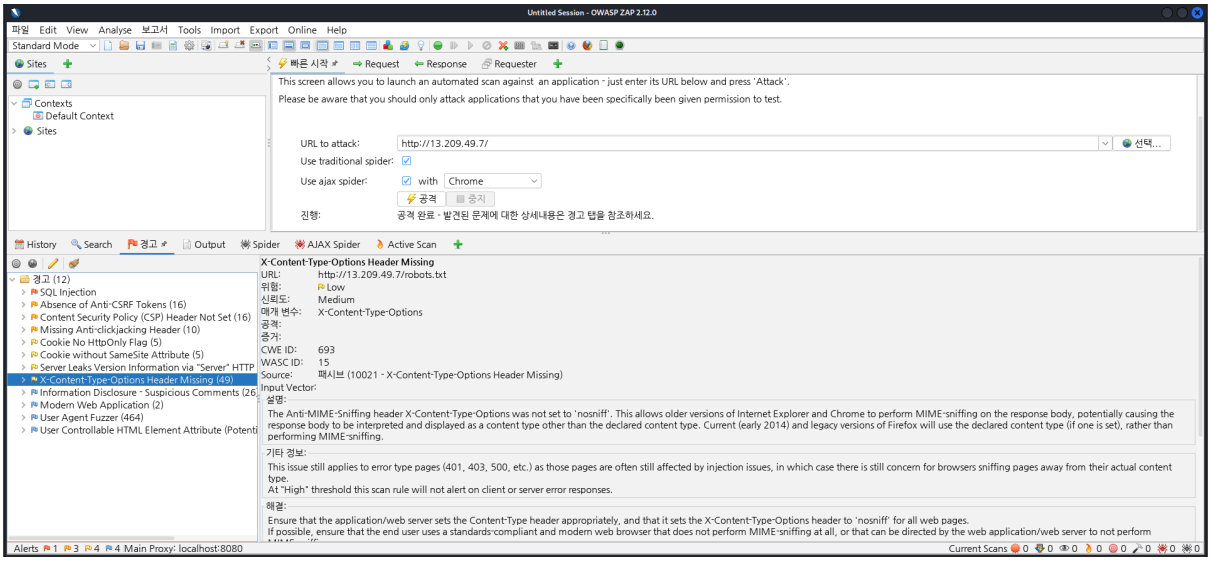


[그림14] 취약점을 찾고 싶은 홈페이지를 대상으로 Automated Scan 진행



[그림15] 취약점을 찾고 싶은 홈페이지를 대상으로 Automated Scan 완료

해당 자동화 도구는 get 방식으로 http 통신을 진행하면서 웹 관련된 페이지 및 해당 페이지에 파라미터에 적당한 값을 대입해서 취약점을 찾는 과정을 진행한다.



[그림16] 취약점 및 문제가 발생할 수 있는 경고

경고 페이지를 이용하여 해당 취약점 및 웹에서 문제가 발생할 수 있는 문제들을 제공한다.

해당 웹 페이지에서 취약점이 발생할 수 있는 문제들은 다음과 같다.

1. SQL 인젝션
2. Anti-CSRF 토큰 부재
3. 콘텐츠 보안 정책(CSP) 헤더가 설정되지 않음

4. 클릭재킹 방지 헤더 누락
5. 쿠키 HttpOnly 플래그 없음
6. SameSite 속성이 없는 쿠키
7. 서버가 "서버" HTTP 응답 헤더 필드를 통해 버전 정보 유출
8. X-콘텐츠 유형 옵션 헤더 누락
9. 사용자 제어 가능한 HTML 요소 속성(잠재적 XSS)

발생하는 문제는 다음과 같이 대응할 수 있다.

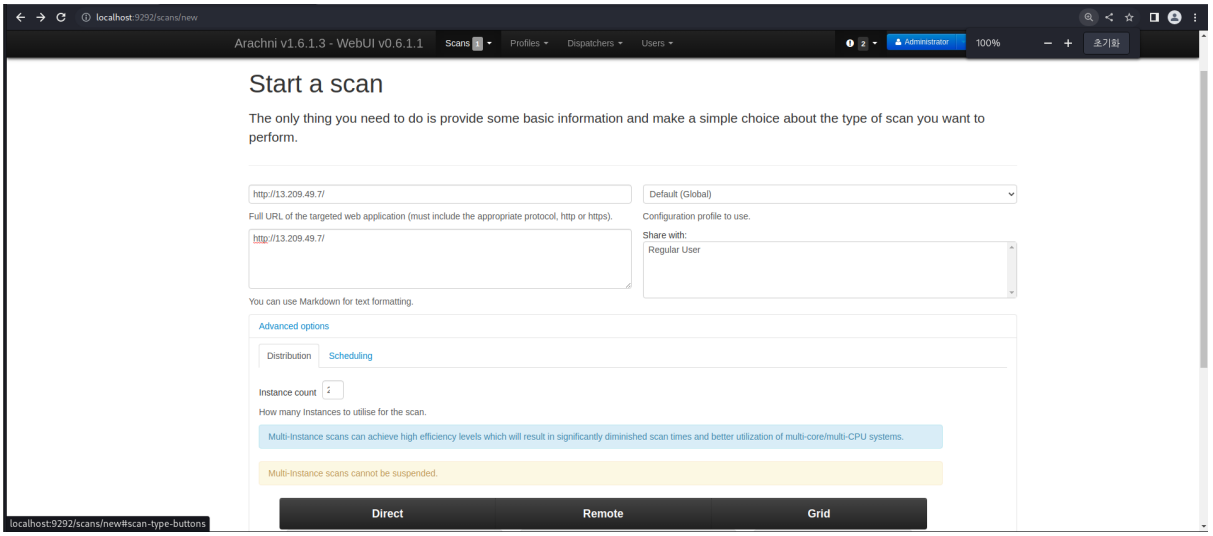
1. 문자열을 쿼리로 연결, 실행, 즉시 실행과 같은 기능 사용 금지, 클라이언트로부터 받은 모든 데이터 이스케이프 처리, 입력에 허용되는 문자 허용 목록을 적용하거나 허용하지 않는 문자 거부 목록을 만들어서 운영하고 최소 권한 원칙 적용해서 사용자의 액세스 권한을 부여한다.
2. CSRF 방지 패키지 사용하기
3. 최신버전의 익스플로러를 사용하여 CSP header를 세팅한다.
4. 콘텐츠 보안 정책 및 X-Frame-Options HTTP 헤더 설정이 되어있는지 확인한다.
5. 모든 쿠키에 대해 HttpOnly 플래그가 설정 확인
6. SamSite(웹 애플리케이션에서 CSRF(교차 사이트 요청 위조) 공격을 방지하기 위해 HTTP 쿠키에서 설정할 수 있는 속성)가 허용이 되어있는지 확인한다.
7. 웹 서버, 애플리케이션 서버, 부하 분산 장치 등이 '서버' 헤더를 표시하지 않거나 일반 세부 정보를 제공하도록 구성되어 있는지 확인
8. Content-Type 헤더를 적절하게 설정하고 모든 웹 페이지에 대해 X-Content-Type-Options 헤더를 'nosniff'로 설정했는지 확인한다.
9. HTML 속성에 쓰기 전에 모든 입력의 유효성을 검사하는지 확인한다.

Arachni

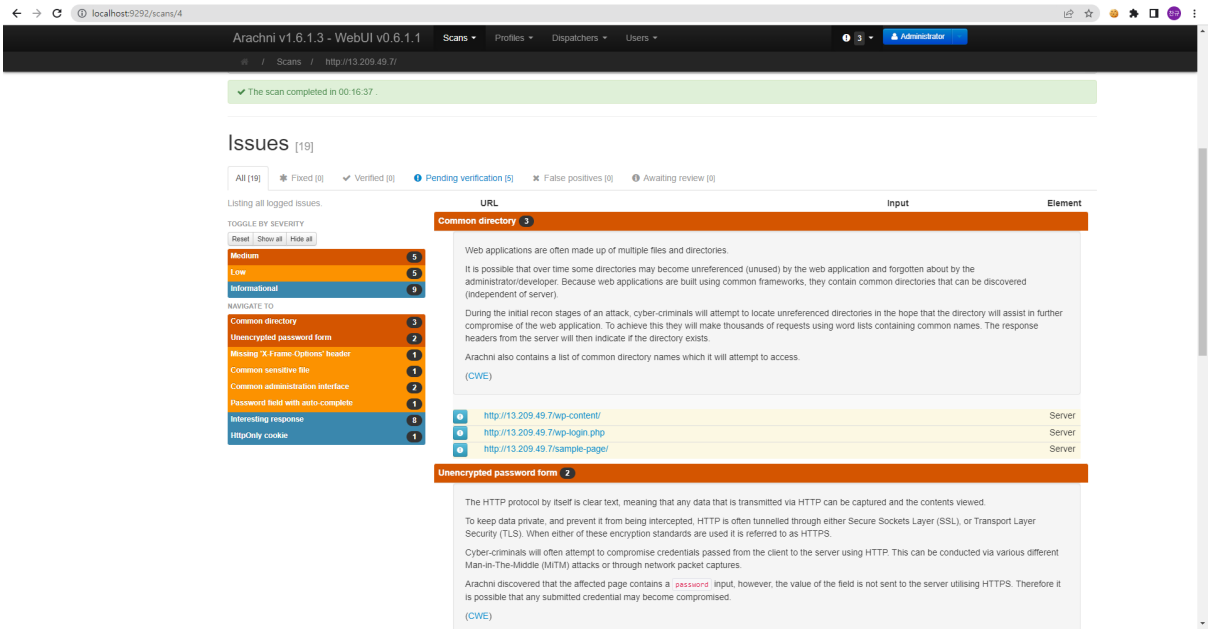
Arachni는 웹 기반으로 이루어져 있으며, 기본적으로 XSS, Injection과 같은 취약점에 대한 취약점들을 찾는데 도움을 주는 웹 자동화 툴이다. 이외의 다른 기능들은 추가를 함으로써 사용이 가능하다.

윈도우/우분투/리눅스 모두 다 arachni-scanner.com을 통해 설치가 가능하다.

Arachni 이용한 간편 취약 분석 과정 및 대응책



[그림17] 취약점을 찾고 싶은 홈페이지를 대상으로 Scanning 진행



[그림18] 취약점을 찾고 싶은 홈페이지를 대상으로 Scanning 완료

해당 과정에서 취약점 및 웹에서 문제가 발생할 수 있는 문제들을 제공하고 위험도를 구분하며 해당 문제가 발생하는 디렉토리 파일을 도출한다.

해당 웹 페이지에서 취약점이 발생할 수 있는 문제들은 다음과 같다

1. 참조하지 않는 공용 디렉토리 사용.
2. HTTP 프로토콜 사용으로 인한 데이터 전송 간에 데이터 유출 가능성 존재.
3. X-Frame-Options 헤더 누락.
4. 자동 완성을 비활성화 하지 않은 비밀번호 필드 존재.

해당 웹 페이지에서 주로 발생하는 부분은 login.php에서 발생되는 데이터 유출에 관련된 취약점이다.

발생하는 문제는 다음과 같이 대응할 수 있다.

1. 디렉토리 목록 비공개 및 웹 방화벽 사용
2. HTTP 대신 HTTPS 적용 및 사용
3. 콘텐츠 보안 정책 및 X-Frame-Options HTTP 헤더 설정
4. 개인정보 및 민감한 정보가 사용되는 부분 자동 완성 비활성화

취약점 분석 후 기초적인 대응책

지금까지 발견된 취약점을 종합하여 발생시킬 수 있는 문제들은 다음과 같은 대부분 기초적인 취약한 문제는 이와 같이 방법으로 해결한다.

1. 최신 브라우저 사용
2. 웹 사이트에 적절한 검증을 하는 과정을 추가한다.
3. 신뢰할 수 있는 사이트를 이용한다.
4. 브라우저에 내장된 검증 기능이 있다면 필수로 사용한다.
5. 확장 프로그램을 이용하여 보안성을 높인다.

05| 결론

이때까지 랜섬웨어에 대한 각종 동향을 비롯하여 WebSE에서 제공하는 MITRE ATT&CK Navigator 기반 취약점 분석 프레임워크를 소개하였다. 랜섬웨어의 발달로 의료 및 공중보건 분야에 속한 기관에서 랜섬웨어 공격 사례가 증가하는 만큼, 랜섬웨어에 대한 각별한 주의가 필요하다.

다음은 KISA에서 제공하는 랜섬웨어 피해 예방 5대 수칙이다.

1. 모든 소프트웨어는 최신 버전으로 업데이트하여 사용한다**.**

2. 백신 소프트웨어를 설치하고**,** 최신 버전으로 업데이트한다**.**

3. 출처가 불명확한 이메일과 **URL** 링크는 실행하지 않는다**.**

4. 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의한다**.**

5. 중요 자료는 정기적으로 백업한다**.**

(출처 **: KISA** 한국인터넷진흥원**)**

이미 감염되었다면 KISA에서 일부 랜섬웨어에 대해 복구도구를 제공한다.

https://seed.kisa.or.kr/kisa/adverse/SearchRansomware.do

팀 WebSE에서는 MITRE ATT&CK을 기반하여 의뢰인의 시스템을 분석하여 시스템에 위협이 될만한 취약점을 분석한다. 기업 시스템에 어떠한 취약점이 있는지 알고 싶다면 WebSE에 방문해 문의할 수 있다.