

코로나19 팬데믹에 따른 사이버공격 변화 양상과 대응방안

채재병 수석연구위원 | 김일기 책임연구위원
chaejb@inss.re.kr | ikkim@inss.re.kr

I. 문제 제기

II. 사이버공격 변화 양상

III. 대응방안

국문 초록

본 연구의 목적은 코로나19 팬데믹에 따른 사이버공격 변화 양상을 검토·분석함으로써 이에 대한 대응방안을 모색하는 것이다. 코로나19 팬데믹에 따른 원격근무로의 전환은 사이버공격 양상을 크게 변화시켰고, 코로나19 팬데믹 상황을 악용하는 사회공학적 공격도 급증했다. 인공지능(AI)과 머신러닝(ML) 활용으로 인해 자동화된 피싱 공격이 점점 더 정교해지고 있으며, 공급망에 대한 공격이 증가하고 있고, 지정학적 긴장 상태에 따른 사이버공격 양상의 변화도 목격되고 있다. 코로나19 팬데믹으로 사이버공격의 범위와 대상이 일상 활동 전반으로 확대되었고, 사이버공격의 방법도 크게 고도화되었다. 코로나19 팬데믹으로 확산된 원격근무는 전 세계 기관과 기업들에게 많은 과제를 안겨주었다. '제로 트러스트 네트워크 액세스(Zero-Trust Network Access, ZTNA)'는 중요한 데이터에 대한 원격 액세스를 제어하고 공격 가능성을 줄이기 위한 보다 안전한 방안이다. 이와 같은 방안들을 통해 네트워크와 클라우드를 포함한 사이버공격 범위 전체에 대한 감시, 탐지, 차단, 보호를 제공해야 한다. 그리고 코로나 19의 영향으로 확대된 공격 범위를 포괄할 수 있도록 기존의 사이버공격 대응체계를 개선하고, 새로운 취약점들을 보호할 수 있는 사이버안보 플랫폼을 구축해야 할 것이다.

핵심어: 코로나19 팬데믹, 사이버공격, 원격근무, 사회공학, 초자동화

목차

I. 문제제기

II. 사이버공격 변화 양상

1. 원격근무의 영향
2. 사회공학적 공격의 증가
3. 초자동화(hyperautomation)
4. 공급망 보안
5. 지정학적 긴장

III. 대응방안

I. 문제 제기

- 코로나19 팬데믹 상황은 전 세계적으로 우리의 일상 생활환경을 변화시켰다. 디지털 전환과 각 분야의 전통산업과 정보통신기술(ICT) 간 융·복합이 가속화되었고, 교육과 근무 등 다양한 일상 활동을 비대면 중심으로 변화시켰다. 일상생활에서의 비대면 활동의 확대는 사이버영역을 확장시키는 결과를 가져왔고, 이로 인해서 사이버공격 범위가 크게 확대되면서 네트워크 등 사이버영역 전반에 대한 사이버공격을 급증시켰다. 특히 교육, 근무, 상업의 온라인화 등 비대면 서비스의 증가는 이와 같은 전 방위적인 사이버공격의 급증을 가져오는 주요 요인으로 작용했다. 이에 작년 코로나19 팬데믹에 이어 금년에는 코로나19 바이러스처럼 사이버공격이 전 세계적으로 유행한다는 뜻을 가진 사이버 팬데믹이 올 것이라는 전망도 나오고 있다.¹⁾
- 코로나19 팬데믹으로 재택 원격근무가 뉴노멀이 된 운영모델이 적용되면서 전 세계는 새로운 도전에 직면했다. 대부분의 국가들은 디지털 전환을 가속화하고 있고, 사이버안보에 크게 주목하고 있다. 각국의 기관과 기업들은 코로나19 팬데믹에 대응하여 직원들이 재택근무를 하도록 장려하고 있다. 결과적으로 사이버 관련 기술은 일과 개인 생활 모두에서 훨씬 더 중요해졌다. 그러나 이러한 기술발전 요구의 증가에도 불구하고 많은 기관과 기업들이 여전히 사이버안전 원격근무 환경을 제공해주지 못하고 있는 것이 문제이다. 전통적으로 회의가 직접 열린던 곳에서는 대부분 가상으로 회의가 진행되고 있는데 집에서 일하는 개인이 근무환경에 있어서 사무실과 동일한 수준의 인터넷 보안의 고유한 보호조치를 누리지 못하고 있다.
- 정보기술(IT) 기업 VM Ware는 ‘2021 글로벌 보안 인사이트 보고서’에서 코로나19 팬데믹으로 글로벌 기업 76%에 대한 사이버공격이 급증했고, 원격근무로 인한 사이버위협도 크게 증가했다고 분석했다.²⁾ 글로벌 보안기업 체크포인트도 2021년 4-5월 동안 아태 지역에서 사이버공격 건수가 53% 증가했고, 특히 원격근무 환경이 해커들이 악용할 수 있는 보안상의 허점을 크게 하고 있다고 분석했다.³⁾

1) 이유지, “원격근무 확산·복합공격 급증, ‘사이버팬데믹’ 보안대책 필요,” 2021. 4. 13. <https://byline.network/2021/04/13-116/> (검색일: 2021. 6. 22).

2) 정태일, “글로벌 기업 76% ‘팬데믹에 사이버공격 급증, 원격업무로 위협 ↑’,” 2021. 6. 9. <http://news.heraldcorp.com/view.php?ud=20210609000994> (검색일: 2021. 6. 22).

3) 김윤희, “아태 지역 사이버공격 53% ↑ …원격근무가 보안 허점 확대,” 2021. 6. 14 <https://zdnet.co.kr/view/?no=20210614170657> (검색일: 2021. 6. 22).

- 이외에도 관리 감독 및 기술 통제력이 떨어지는 집에서 근무하는 악의적인 직원이 스캠(scam) 또는 기타 범죄 행위를 수행하려고 할 수 있다. 이러한 사이버위협 중 대부분은 코로나19 팬데믹 중에 발생한 다양한 기회 때문에 더욱 위협해졌다. 사이버공격이 급증한 이유 중 하나는 일부 기관과 기업들이 'BYOD(Bring Your Own Device)' 액세스 방식을 취하기 때문이며, 이는 직원들이 전화, 태블릿 또는 랩톱 등의 개인기기를 사용하여 조직 정보에 액세스할 수 있다는 것을 의미한다. 집에서 일하는 것이 사무실 환경과 같은 수준의 사이버 보안을 보장하지는 않기 때문에 개인 컴퓨터 또는 랩톱을 사용하여 회사 파일 및 데이터에 액세스할 때 사용자는 사이버공격에 훨씬 쉽게 노출된다. 예를 들어 직원은 바이러스 백신 또는 악성 프로그램 방지 검사를 정기적으로 실행하지 않을 수 있고, 집에서의 작업 환경은 정교한 기관이나 기업의 예방 및 탐지 조치를 갖고 있지 않다. 더욱이 가정용 와이파이 네트워크는 사이버공격에 훨씬 취약하다.⁴⁾
- 이와 같은 코로나19 팬데믹 상황에서 세계 각국은 기관과 기업들을 중심으로 안전한 비대면 사회 정착을 추구하고 있다. 미국은 연방기관의 원격근무 시 발생하는 사이버안보 이슈와 가이드라인을 발표했고, 유럽연합도 코로나19 팬데믹으로 인한 근무 형태의 디지털화와 디지털 인프라에 대한 의존 확대로 사이버안보전략을 개정했다. 중국이나 러시아도 코로나19 팬데믹으로 인한 정보환경의 변화에 대응하고 있다. 한국도 국가적 대응차원에서 비대면 시대의 위협에 대한 국가정보보안 기본지침 관련 내용을 개정하고, 원격업무 통합메뉴얼을 발표하는 등 일반화되는 재택근무와 원격서비스 확산에 대비하고 있다.⁵⁾
- 이처럼 급증하는 사이버공격에 적절히 대응하기 위해서는 코로나19로 인해 변화된 공격 양상을 파악하는 것은 매우 중요하다. 그럼에도 불구하고 코로나19 팬데믹과 관련된 사이버 공격의 변화 양상에 대한 본격적인 국내 연구는 거의 찾기 어렵고, 산발적인 변화 양상에 대한 언급 정도에 그치고 있다.⁶⁾ 그나마 해외에서는 보안 관련 기업이나 연구소 등에서 기본적인 연구가 소수 진행된 것을 찾아 볼 수 있는 정도이다. 향후 사이버공격에 대응하기 위해서는 공격 양상 변화에 대한 연구는 필수적이다. 따라서 본 연구는 국내외 사례들을 통해 코로나19

4) Cedric Nabe, "Impact of COVID-19 on Cybersecurity," <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html> (accessed: June 15, 2021).

5) 정순채, "코로나19와 포스트 코로나 시대의 정보보호," 2021. 6. 21. <https://www.asiatime.co.kr/article/20210621500119> (검색일: 2021. 6. 22).

6) 이동휘·김현아, "코로나19 관련 사이버 공격 사례분석을 통한 보안 연구," 한국정보통신학회 종합학술대회 논문집, 24(1), (2020).

팬데믹에 따른 사이버공격 변화 양상을 본격적으로 검토 분석함으로써 이에 대한 대응방안을 모색해 보고자 한다.

II. 사이버공격 변화 양상

- 코로나19 팬데믹은 새로운 취약점을 공략하는 사이버공격의 급증을 초래했는데, 우선 코로나 19 팬데믹으로 인해 감염병 예방을 위한 사회적 거리두기를 실천하고 있기 때문에 온라인을 통한 활동이 대폭 확대되면서 단기간에 성장한 비대면 서비스를 대상으로 한 원격접속에 대한 사이버공격이 급증했다. 코로나19와 그에 따른 재택 원격근무로의 전환이 사이버공격 양상을 크게 변화시킨 것이다. 원격근무자의 수가 크게 증가했기 때문에 기관과 기업들은 데이터 침해에 매우 취약해졌고, 사이버공격이 급증하고, 직원들의 업무 방식이 전례 없이 달라지면서 새로운 사이버안보 리스크가 대두되었다.
- 그리고 코로나19 팬데믹 상황을 악용해 피싱과 랜섬웨어 등 사람들의 취약점을 공략하는 사회공학적 공격도 급증했다. 과거에도 메르스와 에볼라 바이러스 발생 시 바이러스 관련 내용이 포함된 문자메시지나 이메일 등을 통해 악성코드 유포가 증가했었다. 또한 이러한 감염병 관련 정보제공 사이트로 위장한 사이버공격도 증가했었다. 현재 코로나19 팬데믹 상황을 활용하여 전 세계적으로 다양한 사이버공격이 시도되고 있는데, 의료, 통신, 기술, 금융, 교육 분야에서 코로나19 관련 내용을 미끼로 한 랜섬웨어 공격이 크게 증가했다.⁷⁾
- 한편 새로운 공격들 중 일부는 머신러닝(ML)의 형태를 사용한다. 인공지능(AI)과 머신러닝(ML) 활용으로 인해 자동화된 피싱 공격이 점점 더 정교해지고 있으며 문자나 음성 메시지와 같은 다양한 채널들을 사용하고 있다. 게다가 백신 개발에 관한 뉴스도 피싱 캠페인에 사용되고 있다. 이외에도 공급망에 대한 공격이 증가하고 있고, 지정학적 긴장 상태에 따른 사이버공격

7) 채재병, 『국제사회의 해킹 변화 추세 및 대응방안』, INSS 연구보고서 2020-17 (2020), p. 10.

양상의 변화도 목격되고 있다. 요컨대 코로나19 팬데믹으로 사이버공격의 범위와 대상이 일상 활동 전반으로 확대되었고, 사이버공격의 방법도 크게 고도화되었다.

1. 원격근무의 영향

- 기술 지형이 끊임없이 변화하고 있다는 사실은 새로운 현상은 아니지만 확실히 2020년에는 새로운 단계로 진입했다. 팬데믹 기간 동안 디지털화 및 클라우드(cloud)로의 마이그레이션(migration)과 같은 많은 추세가 가속화되었다. 대부분의 경우 새로운 원격 환경을 수용할 수 있도록 계획되지 않은 클라우드 마이그레이션과 정보기술 제품 및 서비스의 신속한 공급이 이루어졌다. 많은 기관과 기업들이 일반적인 보안 조치에 그치면서 클라우드, 홈 네트워크 등 모든 영역에 걸쳐 새로운 수준의 취약성과 위험이 초래되었다.

가. 클라우드 서비스 보안

- 코로나19 이후 원격근무가 빠르고 광범위하게 도입됨에 따라 클라우드 기반 서비스와 인프라에 대한 필요성이 급격히 증가했다. 원격근무는 직원이 어디에서나 효율적으로 업무를 수행할 수 있도록 지원하는 클라우드 컴퓨팅 애플리케이션을 사용한다. 클라우드를 통해 기관과 기업은 필요에 따라 워크로드를 조정할 수 있으며 분석 및 인공지능과 같은 새로운 기능을 보다 쉽게 추가할 수 있어 이러한 기능이 결합되어 조직의 탄력성이 향상되었다. 클라우드에서 작업을 수행하면 보안 패치가 즉시 설치되는데 이는 기존 시스템에서 흔히 발생하는 문제이다. 클라우드 서비스를 사용하는 조직의 위험은 일반적으로 잘못 구성된 스토리지, 잘못된 아이디(ID) 및 액세스 관리 제어, 안전하지 않은 애플리케이션 프로그래밍 인터페이스(API), 데이터 손실, 침해 및 누출과 관련된다. 이러한 위험은 점점 더 많은 기관과 기업들이 클라우드 호스팅 프로세스를 채택하고 있기 때문에 앞으로도 지속될 것이다. 클라우드 서비스는 확장성, 효율성 및 비용 절감과 같은 다양한 이점을 제공하지만 여전히 사이버공격에 매우 취약한 상태로 남아있게 되었다.⁸⁾

8) "11 Emerging Cybersecurity Trends in 2021," panda, <https://www.pandasecurity.com/en/mediacenter/tips/cybersecurity-trends/> (accessed: June 15, 2021).

나. 홈 네트워크

- 재택 원격근무의 증가로 기관이나 기업의 네트워크가 집에까지 확대됨에 따라 새로운 공격 기회가 제공되면서 사이버공격 범위가 확장되고 있다. 더 많은 엔드 포인트(end point)가 확산됨에 따라 위협 면이 증가했다. 해킹 방지 기업인 파이어아이(FireEye)에 대한 최근의 해킹은 기관이나 기업이 최고의 도구를 가지고 있더라도 동기부여가 된 해커가 외부 또는 내부 벡터를 통해 네트워크로의 길을 찾을 수 있다는 것을 보여주었다. 코로나19로 인한 재택근무의 일상화는 이러한 사이버공격을 더욱 증가시킬 것이다. 향후 5G는 더 빠른 속도와 용량을 제공하고 짧은 대기 시간을 제공하여 더 나은 연결을 제공할 것이다. 이는 개인과 기업의 연결성이 높아짐에 따라 엔드 포인트의 확산으로 이어진다. 2025년까지 27억 대의 기기가 5G에 연결되어 해커가 점점 더 많은 엔드 포인트와 연결 취약점을 공격하게 될 것이다. 앞으로 더 많은 사물인터넷(IoT) 기기들이 와이파이 라우터보다는 5G 네트워크에 직접 연결될 것이다. 이러한 패턴으로 인해 사물인터넷 장치는 직접 공격에 대해 점점 더 무방비 상태가 될 것이다. 가정용 클라이언트의 경우 중앙 라우터에서 모든 사물인터넷 기기가 벗어나기 때문에 더욱 취약해질 것이다. 특히 대량의 데이터를 효과적으로 클라우드 기반 스토리지에 백업하거나 전송할 수 있게 되면 해커가 공격할 수 있는 새로운 대상도 더 많이 확보될 수 있다.⁹⁾

다. 내부자 위협

- 2021년에는 내부자 데이터 위반이 전체 사이버 보안 사고의 3분의 1에 달할 것으로 예측되고 있다. 직원들이 원격근무로 전환함에 따라 미처 많은 기관과 기업들은 무단 원격 액세스를 모니터링하고 취약한 암호를 처리할 준비가 되어 있지 않다. 코로나19는 직원들이 업무에 개인용 기기를 사용할 수 있도록 허용할 것을 조직에 강요했다. ‘BYOD(Bring Your Own Device)’ 개념은 유연성을 통해 비용을 최소화하고 생산성을 높이는 방법이나 앞으로 원격 직원 및 해당 기기가 기관이나 기업의 정보 보안에 위협이 될 수도 있다. 홈 라우터는 보안 제어 기능이 충분하지 않은 경우가 많아 해커들은 보안 수준이 낮은 홈 네트워크를 통해 기관이나 기업의 시스템에 진입하기 위해 네트워크 취약점을 공격할 것이다. 또한 기관이나 기업들은 홈 모델에서 작업을 채택하고 있으며, 이로 인해 협업 보안에 대한 우려도 커지고 있다. 생산성을

9) Yulia De Bari, “2021 Cybersecurity Trends Report,” <https://www.infosys.com/iki/insights/2021-cybersecurity-trends-report.html> (accessed: June 15, 2021).

높이기 위해 원격 직원들은 슬랙(slack), 마이크로소프트 팀(microsoft teams) 및 줌(Zoom)과 같은 더 많은 협업 도구를 사용하고 있다. 이러한 애플리케이션은 더 큰 데이터 보안 및 규정 준수 문제를 야기하고 내부자 위협의 위험을 높일 것이다.¹⁰⁾

2. 사회공학적 공격의 증가

가. 랜섬웨어(ransomware)의 진화

- 2020년에는 랜섬웨어 공격 3건 중 1건이 서비스형 랜섬웨어(RaaS)인 소디노키비(Sodinokibi)를 포함했다. 소디노키비의 경우 이중 갈취(double extortion) 전술로 피해자의 약 67%가 대가를 지불한 것으로 추산된다.¹¹⁾ 그들은 손상된 데이터를 공개 또는 다크 웹(dark web)에 노출시킨 다음 대가를 요구하며 위협한다. 기관이나 기업이 지불을 거부하면 그들은 피해자의 서비스를 이용할 수 없게 만드는 디도스 공격을 감행한다. 또한 서비스형 랜섬웨어 모델은 랜섬웨어 개발자들이 해커들과 협력하여 수익을 얻게 만든다. 예를 들어 소디노키비는 39개 이상의 파트너들과 계약을 맺었다.¹²⁾ 이외에도 BazarLoader, Conti, Egregor, Phobos/EKING, Ragnar, Ryuk, Thanos, WastedLocker 등의 랜섬웨어가 활동했으며 이들은 의료, 전문 서비스 및 소비자 서비스 기업, 금융 서비스 기업 및 공공 조직 등 다양한 분야를 공격 대상으로 삼았다.¹³⁾ 이러한 랜섬웨어가 앞으로 기관과 기업들에는 가장 큰 위협이 될 것으로 보인다.
- 해커들은 병원, 의료 센터 및 공공기관을 주요 랜섬웨어 공격 대상으로 삼고 있다. 왜냐하면 건강 위기로 인해 시스템을 멈출 수 없으므로 해커들은 이들 기관이 대가를 지불할 가능성이 높다고 믿고 있기 때문이다. 실제로 코로나19는 랜섬웨어의 공격시간을 크게 단축시켰는데 이는 피해자가 피해를 최소화하기 위해 대가를 신속히 지불했기 때문이다. 랜섬웨어는 감염된 링크나 첨부 파일이 포함된 이메일, 손상된 직원 자격 증명 또는 시스템의 취약성을 이용하여

10) Eric Richardson and Jake MahleVorys, "Cyberattacks on the rise during the Covid-19 pandemic," Jun 1, 2020, <https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html> (accessed: June 15, 2021).

11) 원병철, "코로나19 관련 산업과 유럽 노린 사이버공격 늘었다," 2021. 2. 25. <https://blog.naver.com/widgetnuri4/222256085790> (검색일: 2021. 6. 22).

12) Yulia De Bari, "2021 Cybersecurity Trends Report."

13) 조경화, "포티넷, 사이버공격 확장으로 전례없는 사이버 위협 환경 직면," 2021. 3. 11. <http://www.efnews.co.kr/news/articleView.html?idxno=89125> (검색일: 2021. 6. 22).

시스템에 진입한다.¹⁴⁾ 많은 해커들이 기관이나 기업들이 원격근무로 전환하는 것을 활용하기 위해 그들의 시스템을 공격하고 침투하기 위한 새로운 악성 프로그램을 개발했다. 팬데믹 이전에 사이버공격의 약 20%는 이전에 보이지 않았던 악성 프로그램이나 방법을 사용했는데, 팬데믹 시기 그 비율은 35%까지 증가했다.¹⁵⁾ 해커들은 악성 프로그램, 스파이웨어 및 트로이 목마를 대화형 코로나 바이러스 지도 및 웹 사이트에 포함시키고, 사용자가 컴퓨터나 모바일 장치에 악성 프로그램을 다운로드하는 링크를 클릭하도록 속이고 있다.

나. 코로나19 피싱(phishing) 체계

- 인터넷에는 ‘corona-virus’, ‘covid-19’ 등의 용어를 포함하는 등록된 도메인들이 상당히 많이 있다. 일부는 합법적인 웹 사이트이지만 해커들은 스팸 캠페인(spam campaign), 피싱 또는 악성 프로그램 확산을 위해 매일 수천 개의 새로운 사이트를 만들고 있다.¹⁶⁾ 전 세계 사이버 공격의 90%는 여전히 피싱 메일을 통해 이루어지며, 피싱 메일은 인터넷 사용자들로부터 개인정보를 탈취하는 가장 오래된 방법 중 하나이다. 최근에는 인터넷 사용자들의 호기심과 불안감을 이용하는 사회공학적 공격 등 다양한 방법을 활용하고 있다.¹⁷⁾ 해커들이 개인이나 기업, 기관의 특성을 사전에 파악하여 관심을 끌만한 주제로 이메일 등을 발송하는 ‘스피어 피싱(spear phishing)’¹⁸⁾ 공격도 자주 활용되고 있다.¹⁹⁾
- 코로나19 백신 접종이 계속 발표되면서 사람들은 백신이 어디서 제공되고 있는지, 누가 백신을 받을 수 있는지와 같은 백신 정보를 점점 더 많이 찾고 있다. 불행히도 이것은 코로나19 백신과 관련된 상당한 수준의 피싱 공격을 초래했다. 예방접종 약속 이메일을 가장한 이메일 피싱 공격과 함께 제약회사와 백신 유통업체에 대한 사이버공격이 급증하고 있다.²⁰⁾

14) “COVID-19 cyberthreats,” INTERPOL, <https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats> (accessed: June 15, 2021).

15) Cedric Nabe, “Impact of COVID-19 on Cybersecurity.”

16) “COVID-19 cyberthreats.”

17) “포스트 팬데믹 시대 속 주목받는 ‘사이버 보안,’” 안랩(AhnLab), 2020. 5. 11. <https://blog.naver.com/facebookera/221970136175> (검색일: 2021. 6. 22).

18) 잡을 물고기를 노려서 작살(spear)로 낚시하는 것에 빗대어, 해커들이 특정 대상에 집중하여 최적화된 공격을 수행하는 사이버 공격 기법.

19) 금융위원회, “코로나19 관련 상황을 틈탄 사이버공격에 대응하여 금융회사 등의 보안조치를 강화하고, 해킹 등 피해 예방 수칙을 마련하였습니다,” 보도자료, 2020. 3. 9.

20) “11 Emerging Cybersecurity Trends in 2021.”

다. 코로나19 스캠(scam)

- 스캠(scam)도 코로나19 팬데믹 상황에서 더욱 자주 발생하고 있다. 2020년 4월 FBI는 코로나 19를 이용한 스캠을 포함하여 자금 이체를 수행하는 기업을 대상으로 하는 비즈니스 이메일 타협(BEC) 스캠이 증가하고 있다고 경고했다. 미국 연방수사국(FBI)은 코로나19와의 싸움에서 필요한 개인 보호 장비나 기타 물자를 구입하는 자치 단체를 대상으로 한 비즈니스 이메일 타협 스캠의 증가에 크게 주목했다.²¹⁾ 앞으로도 코로나19가 기업과 사회에 미치는 영향을 고려하면 이러한 공격은 해가 거듭될수록 커질 것으로 보인다. 기관이나 기업들이 새로운 현실에 계속 적응함에 따라 해커들은 이러한 취약한 시기를 이용하여 사이버공격을 확대할 것이다. 2020년에 해커들이 어떻게 코로나19를 둘러싼 공포와 불확실성을 이용하고 테마 피싱 캠페인(theme phishing campaign), 위반 시스템 및 악성 프로그램을 전달했는지 잘 알려져 있다. 코로나19가 뉴스의 헤드라인을 계속 차지함에 따라 해커는 이 주제를 피싱 캠페인에 사용할 것이고, 국가나 국가와 연계된 악의적인 해커들은 이 상황을 이용할 기회를 계속 모색할 것이다.

3. 초자동화(hyperautomation)

가. 인공지능(AI) 통합

- 인공지능(AI)과 머신러닝(ML) 활용이 사이버안보 환경에서 주목받고 있다. 혁신적인 기술은 사이버위협을 최소화하고 중요한 인프라를 보호하며 원치 않는 침입을 막는 데 도움이 되는 여러 가지 이점을 제공한다. 인공지능은 다양한 소스에서 대량의 위험 데이터를 분석하여 중요한 위험 정보를 제공할 수 있다. 위협 식별 시스템은 완전히 새로운 위험을 식별함으로써 사이버 보안 팀이 탐지, 대응 및 문제 해결에 소비하는 시간을 줄일 수 있다. 앞으로는 인공지능과 머신러닝 기술이 더욱 성숙해지고 보다 높은 효과를 제공할 것이다. 기관과 기업들은 또한 사이버 보안 위험 관리 시스템을 개선하기 위해 이러한 솔루션을 채택하고 구현할 것이다. 그런데 인공지능이 기관이나 기업 간 위협 탐지를 강화할 수 있는 중요한 기회도 제공하지만 이 기술의 진화와 활용 증가는 실제 양방향으로 진행된다. 즉 범죄 네트워크는 인공지능을 이용해 공격을 자동화하고 있다. 인공지능은 해커들이 공격을 개선하는 데 사용할 수 있기

21) Eric Richardson and Jake MahleVorys, "Cyberattacks on the rise during the Covid-19 pandemic."

때문에 해커들에게도 매우 유익하다. 따라서 해커들은 비용이 적게 들고 더 자동화되며 규모 면에서 더 쉽게 사이버공격을 실행할 수 있게 된다. 해커들은 인공지능과 머신러닝을 사용하여 오래된 악성 프로그램의 새로운 변형을 만들고, 취약성을 찾고, 암호를 추측하고, 음성을 복제한다. 인공지능이 제어하는 자동화 시스템은 시스템과 네트워크를 테스트하여 악용될 수 있는 새로운 취약점을 검색할 수도 있다. 이 기술은 또한 사회공학적 공격의 성공률을 크게 높일 수 있다. 향후에는 해커가 인공지능을 조작해 새로운 스마트 악성 혁신을 설계할 것으로도 예상된다.²²⁾

나. 자동화된 피싱

- 데이터 가용성, 자동화 및 높은 가치의 사용자에게 대한 타겟팅 증가로 인해 자동화된 피싱 공격을 탐지하기는 매우 어렵다. 오늘날 해커는 보다 고급 방법을 사용하여 제대로 실행되는 이메일 손상 공격을 만든다. 피싱 위협은 고도로 지역화되고 개인화되고 지역적으로 대상이 지정된다. 이메일이 여전히 공격 벡터 1위로 남아 있는 한 해커들은 피해자들에게 개인 정보나 로그인 자격 증명을 포기하게 하거나 심지어 돈을 보내도록 속이기 위해 다양한 방법들을 사용하고 있다. 점점 더 많은 피싱이 모바일 장치에 대한 문자 메시지 공격 또는 소셜 미디어 및 게임 플랫폼에서의 메시지 사용을 포함하고 있다. 향후 자동화된 윈도우 피싱 공격이 감염병, 정치, 경제를 둘러싼 공포를 넘어설 것으로 예상된다. 역사적으로 악성 행위자들은 악성 첨부파일이나 하이퍼링크로 윈도우 피싱 이메일을 만드는 데 많은 시간을 보냈다. 그러나 해커들이 수작업 과정을 자동화하기 위해 인공지능과 머신러닝을 사용함에 따라 이러한 경향은 변화할 것으로 보인다. 예를 들어, 고급 피싱 도구 키트를 사용하는 국가 지원 해커는 소셜 미디어 네트워크 및 조직 웹 사이트를 검색하여 엄청난 양의 데이터를 얻을 수 있다. 이 데이터를 사용하면 각 피해자에게 맞춤형된 신뢰할 수 있는 콘텐츠를 사용하여 대량의 윈도우 피싱 공격을 시작할 수 있다. 이 자동화된 프로세스는 해커가 한 번에 보낼 수 있는 윈도우 피싱 이메일의 수를 증가시켜 성공 가능성도 높일 것이다.²³⁾

22) Yulia De Bari, "2021 Cybersecurity Trends Report."

23) Ibid.

4. 공급망 보안

- 공급망은 모든 기관과 기업들의 글로벌 운영에 있어서 매우 중요한 요소이다. 사이버공격 10건 중 4건은 조직이 아니라 공급망 링크 중 하나에서 발생한다. 그러므로 공급망 보안의 성패는 그것의 가장 약한 고리에 달려 있다. 타 기관이나 기업의 공급업체가 조직의 데이터를 손상시킬 수 있도록 허용하면 많은 조직들이 공급업체 시스템을 통해 위반을 경험하게 된다. 기관이나 기업은 중요한 정보를 공급업체와 지속적으로 공유해야 하는데 일단 정보가 공유되면 조직은 그것에 대한 직접적인 통제력을 잃게 된다. 이로 인해 정보의 기밀성, 가용성 및 무결성이 위협받게 된다. 이와 같은 공급망에 대한 공격은 상당 기간 동안 계속되어져 왔다. 특히 2020년 12월 대규모 글로벌 공급망 공격을 유발했던 미국의 소프트웨어 개발업체인 솔라윈즈(SolarWinds)에 대한 해킹은 공급망 보안의 중요성을 한 단계 높인 사례로 당시 피해 조직들은 상당한 양의 정보를 노출시켰다. 이와 함께 공급망 공격의 상호 연결된 범위를 보여주고, 공급망 위험 관리의 중요성도 보여주는 여러 최신 사례들도 확인되었다.²⁴⁾ 코로나19로 인한 신속한 디지털화는 기관과 기업들이 더 많은 제3자 관계를 갖게 했고 그러한 제3자가 더 많은 디지털 연결을 가질 것이기 때문에 더 많은 취약성을 야기한다. 공급망이 점점 더 연결되고 복잡해짐에 따라 향후에는 타 기관이나 기업의 리스크 관리가 최우선 순위가 될 수도 있을 것이다.

5. 지정학적 긴장

- 지정학은 공격적인 사이버 활동의 중요한 원동력이다. 앞으로 이러한 긴장감이 높아지면서 사물인터넷(IoT) 기기 및 산업제어시스템(ICS)에 대한 파괴적인 사이버공격이 나타날 수 있다. 의료, 에너지, 석유, 가스, 제조업이 그러한 공격의 최우선의 목표가 될 것이다. 그리고 다크 웹에서는 산업제어시스템 인프라를 공격하기 위해 특수하게 조작된 파괴적인 악성 프로그램의 판매가 급증할 것이다. 해커는 공격 수명 주기에 잘못된 플래그를 배치하여 공격 뒤의 자신의 흔적과 이유를 감추기도 한다. 예를 들어, 북한의 라자루스(Lazarus) 그룹이 러시아어를 사용하는 것과 특이한 도구 세트를 사용하는 것은 분석가의 초점을 다른 조직으로 돌리게 할 수 있다. 보안 전문가는 조사 중에 증거를 매핑하는 데 있어 문제에 직면할 수 있으며 이것은 잘못된 판단과 거짓 주장으로 이어질 수도 있다.²⁵⁾

24) 조경화, “포터넷, 사이버공격 확장으로 전례없는 사이버 위협 환경 직면.”

25) Yulia De Bari, “2021 Cybersecurity Trends Report.”

- 미국의 경우 바이든 대통령은 러시아가 미국에 가장 큰 안보 위협이 되는 국가이자 적국이라고 규정했다. 또한 중국을 미국 경제와 안보에 대한 위협으로 인식하고 있다. 향후 미국과 러시아 및 중국 간에 주요 인프라를 겨냥한 사이버공격이 더욱 증가할 것으로 예상할 수 있다. 러시아도 2020년에는 팬시 베어(Fancy Bear)로도 알려진 러시아 사이버 스파이 단체 스트론튬(Strontium)이 미국의 정당과 캠페인, 옹호 단체, 미국 공화당과 민주당에 봉사하는 컨설턴트 등 200여 개 단체를 사이버공격 대상으로 삼기도 했다. 또 러시아 해외정보국(SVR)의 APT29는 미국의 최고 사이버 보안업체와 재무부, 상무부, 에너지부, 국가원자력안전국 등 정부 기관들을 공격했다. 앞으로도 러시아 해커들이 정치인과 정책입안자들의 계획과 동기를 파악하기 위해 정부 기관을 대상으로 계속 공격할 것으로 전망된다. 중국의 경우, 2020년 중국이 새로운 코로나 바이러스를 무기로 만든다고 비난한 국가들을 대상으로 하는 중국 국가 해킹 그룹의 공격이 있었다. 앞으로는 중국이 지원하는 해커들이 모바일 네트워크를 공격해 미국 국민을 상대로 대대적인 감시·스파이 캠페인을 벌일 것으로 예상할 수도 있다.²⁶⁾

III. 대응방안

- 코로나19 팬데믹으로 확산된 원격근무는 전 세계 기관과 기업들에게 많은 과제를 안겨주었다. 그들은 정교한 사이버공격의 급증에 대한 충분한 준비가 되어 있지 않았으며, 사이버 보안 인식을 높이기 위해 앞으로 많은 노력이 필요하다. 코로나19가 유행하기 전에 일부 기관과 기업들은 원격근무, 특히 기밀 데이터에 대한 액세스에 대해 반대했다. 단기간에 그들은 원격근무를 위한 용량과 기능을 늘려야 했지만 불행히도 원격근무 기능의 신속한 배치에서 사이버 보안이 항상 중요한 우선순위는 아니었다. 예를 들어 일부 기관과 기업은 직원이 회사 데이터에 액세스하기 전에 개인 기기가 표준 보안 보호 기능을 갖추고 있는지 확인하지 않았으며, 기본적으로 설계되지 않은 작업을 ‘가상 사설망(Virtual Private Network, VPN)’

26) Ibid.

기술에 의존했다.²⁷⁾ 많은 정보기술 부서와 기관이나 기업이 가상 사설망에 의존하여 조직 네트워크에 쉽게 액세스할 수 있지만 가상 사설망은 불완전하다. 랜섬웨어의 가장 일반적인 입력 벡터는 피싱이며 기관과 기업은 이러한 공격에 대응해야 한다. ‘제로 트러스트 네트워크 액세스(Zero-Trust Network Access, ZTNA)’는 중요한 데이터에 대한 원격 액세스를 제어하고 공격 가능성을 줄이기 위한 보다 안전한 방안이다. 2023년까지 60%의 기관과 기업이 가상 사설망을 단계적으로 폐지하고 제로 트러스트 네트워크 액세스로 전환할 계획으로 제로 트러스트 네트워크 액세스로 전환하여 조직의 원격 액세스 네트워크를 강화하여 공격 위험을 줄이겠다는 것이다.²⁸⁾

- 구체적인 대응방안을 살펴보면, 첫째, 점점 더 많은 기관과 기업들이 클라우드로 마이그레이션 함에 따라 안전하게 정보를 보호하는 것이 매우 중요하다. 클라우드에서 발생하는 대부분의 사고는 기관이나 기업의 강력한 사이버 보안 전략이 부족하기 때문에 발생한다. 기관과 기업들은 클라우드 설계를 보호하고, 효과적인 리스크 관리를 허용하며, 클라우드 거버넌스를 안전하게 보호할 수 있는 보안 위협의 문제 해결을 위한 영구적인 모델을 구축하는 것이 중요하다. 기관과 기업에서는 클라우드와 함께 발생하는 보안상의 영향을 파악하고 현재 인프라에 존재하는 취약성을 파악해야 한다.
- 둘째, 홈 네트워크는 기관이나 기업 네트워크보다 최소 하나의 악성 프로그램 제품군을 가질 가능성이 3배, 5개 이상의 고유한 유형의 악성 프로그램을 가질 가능성이 7배 더 높다. 홈 오피스를 확보하기 위해 기관이나 기업은 범용 멀티 팩터 인증을 요구할 필요가 있다. 기관이나 기업은 바이러스 백신 업데이트 및 보안 패치를 통해 시스템을 업데이트해야 한다. 데이터 유출을 방지하기 위해 기관이나 기업은 보안되지 않은 장치와 프로토콜을 비활성화하고 엔드 포인트 제어를 시행하며 업무 및 개인 사용 장치를 분리해야 한다. BYOD(Bring Your Own Device)와 모바일 기기의 보안을 유지하려면 직원들이 암호나 개인식별번호(PIN)를 보호하고, 정기적으로 새 업데이트를 설치하고, 신뢰할 수 있는 개발자의 애플리케이션만 설치하고, 개인 정보는 문자 메시지에 노출되지 않도록 하는 등 위험한 온라인 행동에 대해 교육하는 것이 중요하다.²⁹⁾

27) Cedric Nabe, "Impact of COVID-19 on Cybersecurity."

28) "11 Emerging Cybersecurity Trends in 2021."

29) Yulia De Bari, "2021 Cybersecurity Trends Report."

- 셋째, 원격 인력을 계속 탐색함에 따라 내부자 위협은 더욱 우려되는 영역이 되고 있다. 모든 사이버 보안 위협이 외부 영향력에 의해 발생한다고 쉽게 믿지만, 기관이나 기업은 자신의 조직 내에서 증가하는 위협 행위자의 현실과 정교함을 무시해서는 안 된다. 특히 전 세계에 흩어져 있고, 가상으로 만난 뒤 채용했을 가능성이 있는 원격 전담 직원을 기관이나 기업이 계속 채용하고 있기 때문에 더욱 그렇다. 보안 침해 사고의 15%~25%가 신뢰할 수 있는 비즈니스 파트너에 의해 발생한다는 사실에서 기관이나 기업은 내부자 위협과 데이터 도난 가능성에 더 주의해야 한다. 내부 위협은 보안 리더에 의해 심각하게 받아들여지고 실제 위협으로 간주되어야 하며, 조직이 보안 위협을 발견하고 차단할 수 있는 적절한 도구를 갖추고 있어야 한다.³⁰⁾
- 넷째, 사회공학적인 피싱 공격은 원격근무자가 널리 분포하는 상황에서 더욱 큰 문제이며 이를 해결하기 위해 조직은 신원 관리 및 보안 전략을 고려하고, 적시에 필요한 리소스에 적합한 인력만 적절한 수준으로 액세스할 수 있도록 해야 한다.
- 다섯째, 해커들이 공격 전략을 개선하기 위해 인공지능을 사용한다는 점에서 기관이나 기업이 혁신적인 기술 솔루션을 채택하는 것이 중요하다. 인공지능과 머신러닝이 탑재된 플랫폼을 활용해 행동 기반 분석을 대규모로 수행할 수 있으며, 이러한 액세스 방식은 프로세스 초기에 지능적인 사이버 위협을 탐지 및 해결하기 위해 사용될 수 있다. 매일 증가하는 데이터의 양으로 인해 기관이나 기업이 가능한 한 많은 정보기술 프로세스를 자동화하는 프로세스인 초자동화(hyperautomation)가 그 어느 때보다 절실하다. 자동화된 보안 시스템을 구현하면 데이터 도난 및 위반을 완화하는 기관이나 기업의 능력이 강화될 뿐만 아니라 운영 효율성과 사이버 보안 위협에 대한 전반적인 복원력도 향상된다.
- 여섯째, 기관이나 기업은 전체 공급망에서 가시성을 제공하고, 위협과 약점을 식별하며, 새롭게 부상하는 위협을 모니터링하는 강력한 리스크 관리 프로그램이 필요하다. 타사 리스크를 효과적으로 관리하려면 조직은 책임, 소유권 및 통합 워크플로우를 명확히 구분하는 통합 거버넌스 및 에스컬레이션 프레임워크를 생성해야 한다. 취약성을 해결하려면 ‘제로 트러스트 (Zero-Trust)’ 원칙을 사용하여 보안 제어를 만들고 파트너 액세스를 평가해야 한다. 조직은 적절한 시스템 액세스 인증을 위해 위험 기반 파트너 세분화를 구현해야 하고, 공급업체 보안 상태와 파트너 리스크를 평가해야 한다.

30) “11 Emerging Cybersecurity Trends in 2021.”

- 일곱째, 지정학적 동기와 국가가 지원하는 사이버 활동 사이의 명확한 연관성에서 보듯이 기관이나 기업은 지정학적 영향을 충분히 이해해야 한다. 이는 심각한 사이버위협이 발생하기 전에 이를 예측하고 대비할 수 있기 때문이다. 기관이나 기업들이 목표 대상이 되는 방법, 시기, 장소를 결정하려면 지정학적 정보와 기존의 위협 정보 수집 기술을 결합해야 한다.
- 여덟째, 잘 훈련된 사이버 보안 전문가를 찾는 것은 항상 모든 기관과 기업에서 어려운 과제였지만 기관과 기업들은 조직 네트워크의 보안을 강화하기 위해 잘 훈련된 전문가를 구해야 한다. 사이버 보안 인력 부족은 오늘날 기관과 기업들이 직면한 보안 위협을 계속 커지게 하고 있으며, 기관과 기업들은 빠르게 확장되고 있는 디지털 세계를 보호하기 위해 사이버 보안 인력을 늘리고 이에 대한 기술 교육에 우선순위를 두어야 한다.³¹⁾
- 이와 같은 방안들을 통해 네트워크와 클라우드를 포함한 사이버공격 범위 전체에 대한 감시, 탐지, 차단, 보호를 제공해야 한다. 그리고 코로나19의 영향으로 확대된 공격 범위를 포괄할 수 있도록 기존의 사이버공격 대응체계를 개선하고, 새로운 취약점들을 보호할 수 있는 사이버 안보 플랫폼을 구축해야 할 것이다.³²⁾

31) Ibid.

32) 채재병, 『국제사회의 해킹 변화 추세 및 대응방안』, p. 84..

참고문헌

- 금융위원회. “코로나19 관련 상황을 틈탄 사이버공격에 대응하여 금융회사 등의 보안조치를 강화하고, 해킹 등 피해 예방수칙을 마련하였습니다.” 보도자료, 2020. 3. 9.
- 김윤희. “아태 지역 사이버공격 53% ↑ …원격근무가 보안 허점 확대.” 2021. 6. 14. <https://zdnet.co.kr/view/?no=20210614170657> (검색일: 2021. 6. 22).
- 안랩(AhnLab). “포스트 팬데믹 시대 속 주목받는 ‘사이버 보안.’” 2020. 5. 11. <https://blog.naver.com/facebookera/221970136175> (검색일: 2021. 6. 22).
- 원병철. “코로나19 관련 산업과 유럽 노린 사이버공격 늘었다.” 2021. 2. 25. <https://blog.naver.com/widgetnuri4/222256085790> (검색일: 2021. 6. 22).
- 이동휘·김현아. “코로나19 관련 사이버 공격 사례분석을 통한 보안 연구.” 한국정보통신학회 종합 학술대회 논문집, 24(1), (2020).
- 이유지. “원격근무 확산·복합공격 급증, ‘사이버팬데믹’ 보안대책 필요.” 2021. 4. 13. <https://byline.network/2021/04/13-116/> (검색일: 2021. 6. 22).
- 정순채. “코로나19와 포스트 코로나 시대의 정보보호.” 2021. 6. 21. <https://www.asiatime.co.kr/article/20210621500119> (검색일: 2021. 6. 22).
- 정태일. “글로벌 기업 76% ‘팬데믹에 사이버공격 급증, 원격업무로 위협 ↑’.” 2021. 6. 9. <http://news.heraldcorp.com/view.php?ud=20210609000994> (검색일: 2021. 6. 22).
- 조경화. “포티넷, ‘사이버공격 확장으로 전례없는 사이버 위협 환경 직면’.” 2021. 3. 11. <http://www.efnews.co.kr/news/articleView.html?idxno=89125> (검색일: 2021. 6. 22).
- 채재병. 『국제사회의 해킹 변화 추세 및 대응방안』, INSS 연구보고서 2020-17 (2020).
- De Bari, Yulia. “2021 Cybersecurity Trends Report,” <https://www.infosys.com/iki/insights/2021-cybersecurity-trends-report.html> (accessed: June 15, 2021).
- INTERPOL. “COVID-19 cyberthreats,” <https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats> (accessed: June 15, 2021).
- Nabe, Cedric. “Impact of COVID-19 on Cybersecurity,” <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html> (accessed: June 15, 2021).
- panda. “11 Emerging Cybersecurity Trends in 2021,” <https://www.pandasecurity.com/en/mediacenter/tips/cybersecurity-trends/> (accessed: June 15, 2021).

Richardson, Eric and Jake Mahle – Vorys. “Cyberattacks on the rise during the Covid-19 pandemic,” Jun 1, 2020, <https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html> (accessed: June 15, 2021).

Abstract

Changes in Cyberattacks due to Covid-19 pandemic and Countermeasures

Jae-Byung, Chae

Il-Gi, Kim

(Institute for National Security Strategy)

The purpose of this study is to examine and analyze changes in cyberattacks due to the Covid-19 pandemic and to find countermeasures against them. The shift to remote work due to the Covid-19 pandemic has greatly changed the cyberattack pattern, and social engineering attacks that exploit the Covid-19 pandemic situation have also increased rapidly. Automated phishing attacks are becoming increasingly sophisticated due to the use of artificial intelligence(AI) and machine learning(ML), attacks on supply chains are increasing, and changes in cyberattacks due to geopolitical tensions are also being witnessed. With the Covid-19 pandemic, the scope and target of cyberattacks have been expanded throughout everyday activities, and methods of cyberattacks have also been greatly enhanced. The spread of remote work due to the Covid-19 pandemic has posed many challenges for institutions and businesses around the world. Zero-Trust Network Access(ZTNA) is a safer way to control remote access to sensitive data and reduce the likelihood of attacks. These

Abstract

measures should provide surveillance, detection, prevention and protection across the entire range of cyberattacks, including networks and clouds. In addition, it will be necessary to improve the existing cyberattack response system and establish a cybersecurity platform that can protect new vulnerabilities to cover the expanded scope of attacks under the influence of Covid-19.

Keywords: covid-19 pandemic, cyberattack, remote work, social engineering, hyperautomation

INSS

전략보고

August 2021. No.128

국가안보전략연구원

📍 06295 서울시 강남구 언주로 120 인스토피아 빌딩
☎ 02-6191-1000 📠 02-6191-1111 🌐 www.inss.re.kr