사이버위협 동향 분석을 통한 내부망 대응 방안

변예은*
*한국원자력통제기술원
hibye@kinac.re.kr

Internal Network Response Plan through Cyber Threat Trend Analysis

Ye-Eun Byun*
*Korea Institute of Nuclear Nonproliferation and Control

요 약

한국인터넷진흥원에서는 2020년 사이버 공격에 대한 7대 전망을 일상 속 보안 취약점, 공공기관·기업 대상 랜섬웨어, 가상통화 거래소를 통한 해킹 사고, 문자 메시지·이메일을 통한 악성코드 감염, 지능형 표적 공격, 소프트웨어 공급망 공격, 융합 서비스 보안 위협으로 제시하였다. 이에 본 논문에서는 신규 사이버위협에 대한 동향 분석을 통하여 기관의 정보보안을 위해 대응할 수 있는 방안에 대해 살펴보고자 한다.

1. 서론

국내·외에서 정보보안에 대한 필요성과 인식이 높아지면서 기업들의 보안 수준도 많이 향상되고 있지만, 여전히 새로운 사이버위협들은 계속해서 발전하고 있다. 작년에도 망분리 환경에서의 제로데이 취약점으로 인한 유출 사고, 공공기관 서버에 암호화폐 채굴 악성 프로그램이 깔리는 등 새로운 위협이 등장하였으며, 랜섬웨어가 끊임없이 기승을 부리는 와중에 소디노키비, 갠드크랩 등 새로운 랜섬웨어도 생겨나고 있다. 또한, 여전히 각종 기업에서 정보유출 사고도 다양한 경로를 통해 발생하고 있다. 이러한 상황에서 기업에서는 새로운 보안 이슈가 발생할 때마다 대책을 마련하는 것도 중요하지만, 사전에 위협에 대한 분석을 통해 대응 방안을 마련해 가는 것 또한 매우 중요하다고 할 수 있다. 이에, 본 논문에서는 한국인터넷진흥원에서 발표한 국내 주요 보안 업체에서 제시한 사이버위협 7대 전망을 살펴본 후에 이에 대해 기업의 입장에서는 어떠한 대응 방안을 마련할 수 있는지에 대해 살펴보고자 한다.

2. 사이버위협 분석

우선, 한국인터넷진흥원에서 발표한 2020년 사이버 공격 7대 전망에 대해 살펴보고자 한다.[1] 첫 번째로 한국인터넷진흥원에서 발표한 위협은 일상 속으로 파고든 보안 취약점에 관한 내용이다. 이는 지능형 CCTV, AI 스피커 등 IoT 결합 서비스를 대상으로 한 사이버 위협이 증가하고 있다는 것이다. 국내 IoT 시장이 확대되는 만큼, 보안 문제에 대한 우려 또한 증가하고 있다. 통신 암호화 문제, 원격 쉘 접근 문제, IoT 기기를 대상으로 한 서비스 거부 공격 문제 등 다양한 보안 문제가 대두되고 있다.[2] 다음으로, 안랩에서는 공공기관·기업으로 사칭한 랜섬웨어가 APT와 결합되어 유포됨으로써 이로 인한 피해가 확대될 것이라 발표하였다. 작년에 미국에서는 텍사스 주의 행정망에 랜섬웨어가 침투되어 이로 인한 피해는 발생하지 않았지만, 주 정부의 비상관리 대응 중 두 번째로 높은 등급인 2단계 대응 조치가 이루어진 사례가 있었다.

세 번째로, 가상통화 탈취 및 가치 조작을 목적으로 하는 가상통화 거래소 관련 해킹 사고가 꾸준히 증가하고 있다. 작년에 한 공공기관의 서버가 사용자 몰래 가상화폐 채굴 프로그램 악성코드를 심는 크립토재킹에 활용된 사실이 밝혀졌다. 이와 같이 피해를 눈치 채기 어려운 채굴형 악성코드가 지속적으로 유포되어 사용자의 감염을 시도할 것으로 전망하고 있다. 다음으로는 문자메시지나 이메일 속 링크를 이용하여 악성 앱을 감염시키는 모바일 표적 공격이 증가하고 있다. 웹 페이지를 통해 소프트웨어를 다운받을 때, 소프트웨어에 대한 무결성 검증과 배포자에 대한 인증을 제공해주는 것이 코드서명

기술이다.[3] 이러한 유효한 코드서명 인증서에 대해 탈취를 시도하고 이로 서명된 악성코드를 유포·감염시키는 공격이 증가하고 있다.

다섯 번째로, 문서 파일을 위·변조한 스피어피싱, 소프트웨어 자체 보안 기능을 통한 위협 탐지 시스템 회피, 정상 서비스를 활용한 악성코드 통신 기법 활용 등 다양한 지능형 표적 공격이 증가하고 있다. 정상 문서 파일을 위·변조하거나 암호화된 문서 파일을 이용하여 사용자에게 접근하는 방식이 보다 정교화되고 있다. 또한, 모바일 앱이나 스마트폰 제조사를 대상으로 한 소프트웨어 공급망 공격이 확대되고 있다. 이는 소프트웨어의 특정 사용자만을 선별하여 표적으로 하는 악성코드를 유포하여 공격한다. 마지막으로, 스마트시티나 스마트공장 등을 위협하거나 의료 시스템을 해킹하는 등 융합 서비스를 노리는 새로운 보안 위협이 등장할 것으로 예상하고 있다.

3. 보안 대응 방안

이번 장에서는 각 사이버위협에 대한 대응 방안에 대해 살펴보고자 한다. 우선, IoT 결합 서비스와의 보안 강화를 위해서는 기관에서 사물인터넷 결합 제품을 도입할 경우, 가급적 기관망과는 별도의 망을 활용할 수 있도록 하여 사물인터넷을 통한 기관의 망에 피해가 발생하지 않도록 하는 것이 가장 중요할 것이다. 또한, Windows7/XP 등의 지원이 중단된 혹은 예정인 운영체제를 통한 취약점이 대두되고 있는 만큼, 해당 운영체제를 업그레이드하여 취약점에 노출되지 않도록 하는 정책 적용이 필요하다.

공공기관·기업을 표적으로 한 랜섬웨어 감염 시, 파일 암호화 및 금전 요구 등의 피해가 발생할 수 있으므로 랜섬웨어가 가장 쉽게 유입될 수 있는 통로인 메일을 통한 감염에 유의해야 한다. 기술적으로 랜섬웨어 차단 솔루션 등을 도입하여 차단하는 것도 필요하겠지만, 무엇보다 의심스러운 메일을 열람하지 않는 등 사용자가 유의하는 것이 가장 필수적이라고 할 수 있다. 이러한 보안 대응 방안은 문자메시지나 이메일을 통한 악성코드 공격 대응 방안에도 동일하게 적용될 수 있을 것이다. 물론 기관에서 업무용 모바일 앱을 활용할 때는 개발 시에 보안 대책을 마련하여 추진하여야 한다.

또한, 가상통화 거래소 관련 해킹 사고를 방지하기 위해서도 악성 프로그램이 설치되지 않도록 기술적 보안대책을 마련하는 것 뿐만 아니라 작년 공공기관 사례에서는 용역업체 직원에 대한 관리 부족으로 사건이 발생한 만큼 제도적인 측면을 보완하는 것도 중요하다. 다음으로 지능형 지속위협(APT) 공격이 네트워크, 이메일 등 다양한 경로를 통해 증가하고 있는 만큼 유입되는 악성코드에 대해 분석 및 차단을 할 수 있는 시스템을 통해 근본적인 대응을 할 필요가 있다. 이를 통해 기업 내 사용자 PC들에 대한 감염 여부를 분석하여 외부 위협으로부터의 원내 전산망에 대한 안전성을 확보할 필요가 있다.

4. 결론

최근 메일 수신자가 관심을 가지는 내용의 제목으로 클릭을 유도하는 피싱 메일이나 특정 집단을 타겟으로 하여 정부기관 등을 사칭하는 해킹 메일 등 다양한 기법을 통해 이러한 해킹 메일이 사용자들에게 유포되고 있다. 이에, 정부에서도 각 기관에서의 피해를 방지하기 위해 SPF·DKIM·DMARC의 기술을 적용할 것을 요구하고 있고, 보안 업체에서도 발전하고 있는 공격 기법에 대응하기 위한 제품들을 출시하고 있다. 본 논문에서는 이러한 사회적인 환경에서 요구하고 있는 보안 기술들의 체계와 기술 문서에 대해 살펴보았다. 보안 기술을 적용하기 위해 해당 기술이 제안되거나 적용되고 있는 문서의 흐름을 파악하는 것은 기술 도입 전 이해를 돕기 위한 발판이 되었으며, 이를 통해 좀 더 폭 넓은 기술적인 이해를 할 수 있을 것이라 기대해본다. 물론 다양한 보안 기술을 적용함으로써 보안을 강화 시키는 것도 중요하지만 무엇보다 중요한 것은 의심되는 메일은 열어보지 않고, 기본적인 보안 수칙을 준수하는 사용자들의 보안 의식이 가장 중요할 것이다.

참고문헌

[1] 한국인터넷진흥원, “2020년 7대 사이버 공격 전망”, 2019

[2] 이동혁, 박남제, “IoT 기기의 보안성 확보를 위한 제도적 개선방안”, 한국정보보호학회 논문지 VOL.27, NO.3, 2017

[3] 이래, 이동훈, “코드 서명 기술의 국내 PKI 적용 방안 비교 연구”, 정보보호학회논문지 14권, 3호, 2014