KISA 한국인터넷진흥원	보도자료 4차산업혁명의 큰 길로 대한민국이 달려갑니다.	I-KOREA 4.0
2018년 12월 6일(목) 지면[온라인: 2018년 12월 5일(수) 12:00]부터 보도 가능합니다.		

담당부서	인텔리전스확산팀 이동연팀장(전화:02-405-5522, 전자우편:ryuni@kisa.or.kr) 인텔리전스확산팀 서상욱책임(전화:02-405-5541, 전자우편:woodruff@kisa.or.kr)	
참고자료	사진 있음 ■ 사진 없음 □	총 2 매

KISA 및 국내 보안업체, 2019년도 7대 사이버 공격 전망 발표

- 모바일 기기 공격 크립토재킹 확산, SNS 메신저 활용 표적 공격 확산, 보안취약 인터넷 단말기 공격 심화 등 -

한국인터넷진흥원(KISA, 원장 김석환)은 '사이버위협 인텔리전스 네트워크(이하 협의체)'에 참여하는 국내 주요 보안업체 6개사와 함께 2019년 주목해야 할 7대 사이버 공격 전망을 5일(수) 발표했다.

※ 사이버위협 인텔리전스 네트워크 : 사이버 위협정보 공유 및 침해사고 공동 대응을 위해 한국인터넷진흥원, 안랩, 이스트시큐리티, NSHC, 하우리, 잉카인터넷, 빛스캔 등 국내 보안업체가 2014년 12월부터 구성·운영하고 있음

협의체는 2019년도 사이버 보안 화두로 ▲모바일 기기 공격 크립토재킹, ▲SNS를 이용한 표적공격, ▲보안에 취약한 인터넷 단말기를 겨냥한 공격, ▲지능화된 스피어피싱과 APT 공격, ▲사물인터넷을 겨냥한 신종 사이버 위협, ▲소프트웨어 공급망 대상 사이버 공격 증가, ▲악성 행위 탐지를 우회하는 공격 기법 등 7대 사이버 공격 유형이 심화될 것으로 전망했다.

특히, 타인의 PC를 좀비 PC로 만들어 가상화폐를 채굴하도록 하는 크립토재킹이 모바일 기기, 사물인터넷(IoT) 등 다양한 경로로 확산될 전망이다. 안랩 안창용 책임은 "인터넷에 항시 연결되어 있고 연산 능력이 있는 IoT 기기들은 공격자에게 매력적인 대상"이라며, "사물인터넷(IoT) 기기를 좀비화한 후 가상화폐 네트워크를 공격할 수 있을 뿐 아니라 악성코드 유포의 숙주로 악용되는 경우가 늘어날 것"이라고 전망했다.

※ 크립토재킹 탐지 건수: 3건(2017년) → 1,188건(2018년 10월) (출처: KISA)

※ IoT 취약점 대응 건수: 156건(2015년) → 358건(2016년) → 867건(2017년) (출처: KISA)

또한, 소셜 네트워크 서비스(SNS)를 악용한 공격은 큰 파급력을 나타낼 것으로 보인다. 이스트시큐리티 문종현 이사는 “유명인의 SNS 계정을 해킹하여 악성코드를 다량으로 유포하거나, 지인을 가장하여 SNS 메신저를 활용한 맞춤형 표적공격이 많이 발생할 것” 이라고 전망했다.

그리고 협의체는 보안에 취약한 인터넷 단말기(엔드포인트)들이 2019년에 보안 관리자를 고민하게 만드는 주요 요소가 될 것으로 전망했다. 초기 비밀번호 변경 미흡 등 보안에 취약한 단말기들이 보안 공격의 시작점 또는 해킹 통로로 활용될 수 있기 때문이다.

공격자와 방어자 간 쫓고 쫓기는 추격전은 2019년에도 계속될 것으로 보인다. 협의체는 인공지능 기술을 활용하여 기존 악성 행위 탐지를 교묘하게 우회하는 지능화된 보안 위협들이 증가할 것으로 전망했다. 사물인터넷(IoT) 뿐만 아니라 민감한 사회 이슈를 이용한 스피어피싱과 지능형 지속 공격(APT), 소프트웨어 공격망을 악용한 해킹 시도 또한 내년에도 여전히 활개를 칠 것으로 전망했다.

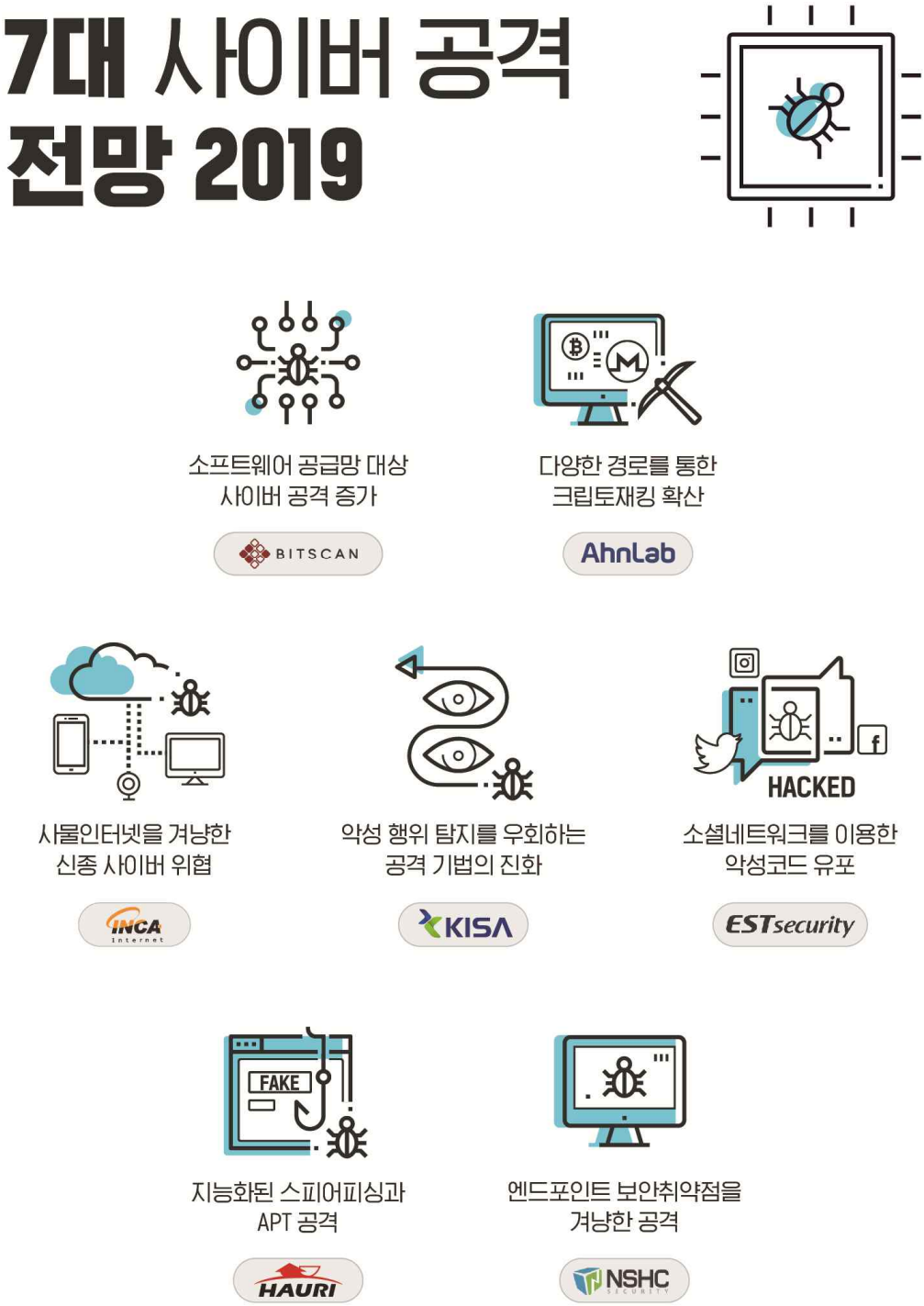
인터넷진흥원은 일반 국민과 기업들이 해킹 공격에 악용되지 않기 위해서는 소셜 네트워크 서비스(SNS), IP카메라 등 사물인터넷(IoT) 기기에 안전한 초기 비밀번호 설정, 최신 보안 업데이트, 취약점 점검 등 기본적인 보안 관리를 더욱 철저히 해야 한다고 당부했다.

인터넷진흥원 김석환 원장은 “인터넷진흥원은 빠르게 진화하는 사이버 위협에 능동적으로 대응할 수 있도록 인공지능 기반의 빅데이터센터를 구축하는 등 침해사고 대응역량을 강화하고, 민간 분야와 위협정보를 공유하는 허브 역할을 더욱 단단히 하겠다” 고 말했다.

붙임. 2019년 7대 사이버 공격 전망

2018년 보안위협 현황	2019년 보안위협 전망
1. 다양한 경로를 통한 크립토재킹 확산 : 안랩	
▶ 다양한 경로(ex 토렌트)와 유포 기법(ex MS17-010) 사용 ▶ 기업 서버를 대상으로 마이너 악성코드 감염 ▶ 백신의 업데이트 방해 및 감염 인지가 어렵도록 교묘하게 동작	▶ 모바일 기기의 보편화로 인한 채굴 악성 앱 유포 ▶ 취약한 IoT 기기를 대상으로 대량 감염 및 채굴 시도 ▶ 웹 브라우저에서 동작하는 채굴 스크립트 유포 지속
2. 소셜 네트워크를 이용한 악성코드 유포 : 이스트시큐리티	
▶ 페이스북 해킹으로 이용자 약5천만명 계정이 위험에 노출 ▶ 인스타그램, 카카오톡 등 연예인 계정 해킹과 송금 유도 ▶ '무료 항공권 드려요' SNS 가짜 이벤트 피싱 사기	▶ 유명한 소셜 네트워크 해킹을 통한 대규모 악성코드 유포 ▶ 허위 프로필을 이용한 미인계 SNP(Social Network Phishing) ▶ SNS 메신저를 이용한 맞춤형 APT
3. 엔드포인트 보안취약점을 겨냥한 공격 : NSHC	
▶ 매크로와 같은 일반 S/W의 정상기능을 악성코드 감염 기법으로 활용 증가 ▶ 인증서 도용과 정상 S/W의 업데이트 기능을 이용한 악성코드 유포 ▶ CPU에 존재하는 취약점을 악용한 공격코드 공개	▶ 스크립트 악성코드와 윈도우 OS의 시스템 관리 기능을 이용한 공격 심화 ▶ 공개용 코드와 모의해킹 S/W를 활용한 공격 심화 ▶ 보안 S/W의 정상기능을 악성코드 감염 및 제어 수단으로 활용한 공격 심화
4. 지능화된 스피어피싱과 APT 공격 : 하우리	
▶ 암호화폐, 부동산, 증시 등 민감한 사회 이슈를 이용한 공격 지속 ▶ 전통적인 소재 역시 꾸준히 등장 (이력서, 저작권 위반, 무료폰트 등) ▶ 워터링홀을 통해 ActiveX를 이용한 APT 공격	▶ 인공지능 기술로 강화된 개인 맞춤형 스피어 피싱 메시지 및 공격 등장 ▶ 가짜뉴스 등 자극적 이슈 소재를 이용한 악성코드 유포 가능성 증대 ▶ 보안이 취약한 중소기업을 대상으로 한 APT 공격 증대
5. 사물인터넷을 겨냥한 신종 사이버 위협 : 잉카인터넷	
▶ IP카메라, 음성인식스피커 등 스마트홈 기기 사용 증가에 따른 사이버 위협 증가 ▶ 스마트카, 교통 시스템, 전력망 등 도시 인프라 대상 사이버 공격 발생 ▶ IP카메라, 스마트 냉장고, 차량 블루투스 해킹 시연 (18.09. 노르마)	▶ IoT 봇넷의 변종 및 다양한 봇넷 출현으로 IoT기기의 좀비기기화 증가 ▶ IoT 봇넷을 이용한 DDoS 공격으로 블록체인 및 암호화폐 네트워크 공격 ▶ 좀비화된 IoT기기를 통한 개인정보 탈취 및 악성코드 유포의 숙주로의 악용
6. 소프트웨어 공급망 관련 사이버 공격 증가 : 빛스켄	
▶ 개발업체 대상 사이버 공격으로 홈페이지 서비스 중단 사고 발생 ▶ 쇼핑몰 웹 솔루션 업체의 S/W 취약점을 악용한 웹 해킹 ▶ 소프트웨어 코드서명 인증서가 해킹으로 외부에 유출	▶ 소프트웨어, 웹사이트 개발업체 대상 공격 증가 ▶ 소프트웨어 취약점을 악용한 해킹 및 정보유출 증가 ▶ 소프트웨어 코드서명 인증서를 해킹하는 공격 증가
7. 악성 행위 탐지를 우회하는 공격 기법의 진화 : 한국인터넷진흥원	
▶ 공격의 흔적을 지우고 악성기능을 모듈화한 IoT 봇넷 VPN필터 등장 ▶ 백신탐지를 우회하는 초소형 POS 악성코드(PinkKite, TinyPOS) 출현 ▶ 안티 머신러닝 기능을 갖추고 있는 파이록키 랜섬웨어 발견	▶ DGA를 이용하여 C&C 차단을 회피하는 악성코드 증가 ▶ 머신러닝기반 백신 및 탐지 시스템을 우회하는 사이버 위협의 진화 ▶ 패치관리, 보안관리 등 중앙관리 S/W의 취약점을 악용한 공격 지속

□ 인포그래픽


7대 사이버 공격 전망 2019
소프트웨어 공급망 대상 사이버 공격 증가
BITSCAN
다양한 경로를 통한 크립토재킹 확산
AhnLab
사물인터넷을 겨냥한 신종 사이버 위협
INCA Internet
악성 행위 탐지를 우회하는 공격 기법의 진화
KISA
HACKED
소셜네트워크를 이용한 악성코드 유포
ESTsecurity
FAKE
지능화된 스피어피싱과 APT 공격
HAURI
엔드포인트 보안취약점을 겨냥한 공격
NSHC

1 다양한 경로를 통한 크립토재킹 확산(안랩)

□ 2018년 보안위협 현황

▶ 다양한 경로(ex 토렌트)와 유포 기법(ex MS17-010) 사용
▶ 기업 서버를 대상으로 마이너 악성코드 감염
▶ 백신의 업데이트 방해 및 감염 인지가 어렵도록 교묘하게 동작

가상화폐는 작년에 비해 그 가치가 많이 하락한 상태이나 온라인 개인 거래 및 익명성 보장 등의 이유로 여전히 인기가 있으며, 이에 공격자들은 가상화폐를 탈취하기 위해서 다양한 악성코드를 제작 및 유포하고 있다. 올해는 특히 전용 채굴 시스템이 아닌 일반적으로 사용하는 시스템을 악성코드에 감염시켜 가상화폐를 채굴하는 크랩토재킹이 눈에 띄게 증가했으며, 다양한 경로를 통해 유포됐다. 대표적인 예로 토렌트를 통해 정상 프로그램으로 위장하여 유포됐거나, 워너크립터가 사용한 MS17-010 취약점을 사용하여 유포된 사례도 있으며, 그 경우 구형 운영체제를 사용하는 POS단말기에서 결제가 안 되는 장애가 발생하기도 했다. 백신업체들이 크립토재킹을 잘 대응하자 공격자들은 마이너에 채굴 기능뿐만 아니라 윈도우 방화벽에 백신 프로세스를 등록하여 백신의 업데이트가 불가능하도록 하는 기능도 추가했다.

□ 2019년 보안위협 전망

▶ 모바일 기기의 보편화로 인한 채굴 악성 앱 유포 증가
▶ 취약한 IoT기기를 대상으로 대량 감염 및 채굴 시도
▶ 웹 브라우저에서 동작하는 채굴 스크립트 유포 지속

□ 인텔리전스 전망

인터넷 이용 플랫폼이 PC에서 모바일로 이동하고 있고, 하드웨어 사양이 높아진 모바일 기기가 보급되면서 공격자들은 기존의 PC에서 동작하는 마이너뿐만 아니라 모바일 기기에서 동작하는 마이너 앱을 제작 및 유포할 것이다. 다양한 형태의 IoT 기기에 존재하는 취약점 그리고 기본 보안 설정의 문제점 등을 이용한 악성코드 감염으로 BotNet 구성 및 DDoS나 사생활 노출 등의 문제가 발생하고 있다. 이러한 문제들을 고려했을 때 공격자들은 취약한 IoT기기를 단순히 타 대상을 공격하는데 악용하는 것뿐만 아니라 IoT기기용 마이너를 제작 및 유포하여 취약한 IoT기기들을 감염시키고 채굴함으로써 금전적인 이득을 취할 수도 있다. 웹 브라우저에서 동작하는 스크립트 기반의 웹 브라우저, 운영체제 등의 플랫폼을 구분하지 않으며, 기존의 악성코드(ex 랜섬웨어)처럼 웹 브라우저의 취약점을 이용하는 것이 아니라 스크립트 기반의 마이너가 삽입된 웹 사이트에 접속 시 웹 브라우저에서 채굴을 수행한다는 장점이 있으므로 올해와 마찬가지로 내년에도 스크립트 기반의 마이너가 꾸준히 유포될 것이다.

2 소셜 네트워크를 이용한 악성코드 유포(이스트시큐리티)

□ 2018년 보안위협 현황

▶ 페이스북 해킹으로 이용자 약 5천만 명 계정이 위험에 노출
▶ 인스타그램, 카카오톡 등 연예인 잇따른 계정 해킹과 송금 유도
▶ ‘ 무료 항공권 드려요’ SNS 가짜 이벤트 피싱 사기

2018년 페이스북 해킹으로 이용자 약 5천만 명의 계정이 위험에 노출된 것으로 알려져 전 세계적으로 큰 보안이슈로 부상하였다. 이처럼 소셜 네트워크 서비스(SNS)를 대상으로 한 각종 보안위협은 오랜 기간 지속적으로 발생하고 있다. 사이버 공격자들은 가입 회원 수나 인기가 많은 서비스를 겨냥해 다양한 방식으로 고유한 개인정보 탈취를 시도하고 있다. 특히, 한국에서는 유명 연예인의 인스타그램 계정을 해킹해 신분을 무단도용하거나 예기치 못한 개인정보 유출피해로 이어졌고, 유명인의 지인을 사칭해 카카오톡 친구로 접근해 계좌송금을 유도하는 피싱 사기도 보고되었다. 또한, '무료 항공권을 드립니다' 등의 가짜 SNS 이벤트 내용으로 현혹해 불특정 다수에게 악의적인 링크를 클릭하도록 현혹하거나 보안위협에 노출될 수 있는 사이트로 접속을 유도하는 등 SNS를 기반으로 한 위협이 지속화되었다.

□ 2019년 보안위협 전망

▶ 유명한 소셜 네트워크 해킹을 통한 대규모 악성코드 유포
▶ 허위 프로필을 이용한 미인계 SNP (Social Network Phishing)
▶ SNS 메신저를 이용한 맞춤형 APT (Advanced Persistent Threat)

□ 인텔리전스 전망

소셜 네트워크 서비스는 아직까지 수많은 사람들이 이용하고 있고, 이에 비례적으로 SNS 기반 사이버 위협 노출 수위도 갈수록 지능화, 정교화 될 것으로 예상된다. 짧은 기간 대규모 악성코드를 유포하는데 있어 사용자가 많은 소셜 네트워크 서비스의 네트워크 인프라를 활용할 수 있다. 특히, 이성간 호기심을 유발할 수 있는 미남·미녀 허위 프로필 사진으로 불특정 다수를 노린 이른바 소셜 네트워크 피싱(SNP)에 노출될 수 있어, 사전에 알지 못한 사람이 접근할 경우 각별한 주의가 필요하다. 또한, 기존에 알려지지 않은 최신 Zero-Day 취약점 등의 파일을 특정 공격 대상에게만 은밀하게 보내는 SNS 기반 APT 공격으로 고도화될 수 있을 것으로 예상된다.

3 엔드포인트 보안취약점을 겨냥한 공격 (NSHC)

□ 2018년 보안위협 현황

▶ 매크로와 같은 일반 S/W의 정상 기능을 악성코드 감염 기법으로 활용 증가
▶ 인증서 도용과 정상 S/W의 업데이트 기능을 이용한 악성코드 유포
▶ CPU에 존재하는 취약점을 악용한 공격코드 공개

2018년에는 문서 작성과 열람을 위해 많이 사용하는 오피스 소프트웨어의 정상 기능인 매크로 기능을 악용한 악성코드 감염 시도 사례들이 다수 발견되었으며, 지능형 공격에서 랜섬웨어에까지 광범위 하게 활용되는 것이 발견되었다.
이와 함께 원격 제어 소프트웨어의 파일에 사용하는 인증서를 도용하여 해당 소프트웨어의 업데이트 기능을 악성코드 유포 수단으로 악용하는 사례도 발견되었다.
그리고, 2018년 초에는 CPU에 존재하는 명령어 처리 과정에서 존재하는 오류로 인한 취약점이 발견되어 하드웨어에 기반 한 해킹이 현실화 되었다.

□ 2019년 보안위협 전망

▶ 스크립트 악성코드와 윈도우 OS의 시스템 관리 기능을 이용한 공격 심화
▶ 공개용(Open Source) 코드와 모의해킹 S/W를 활용한 공격 심화
▶ 보안 S/W의 정상기능을 악성코드 감염 및 제어 수단으로 활용한 공격 심화

□ 인텔리전스 전망

2018년에는 스크립트 형태의 악성코드가 윈도우 기능인 WMI를 이용해 C2 서버와 통신하며 해킹을 시도하는 형태가 발견되었다. 2019년에는 이렇게 윈도우의 정상적인 시스템 관리 기능과 스크립트 악성코드라는 두 가지 조합의 해킹 기법이 더 많이 발견될 것으로 예상된다.
2018년에는 RAT 형태의 공개용 코드를 이용한 악성코드 제작이 발견되었으며, 일부 악성코드 중에는 모의 해킹 소프트웨어의 코드 일부분을 활용하는 형태가 발견되었다. 2019년에는 알려진 공개용 코드나 모의 해킹 소프트웨어를 활용한 공격이 증가하리라 예상 된다.
과거에도 보안 소프트웨어에 존재하는 기능이나 특정 취약점을 악용한 악성코드 감염 및 전파 수단으로 활용된 사례가 있었던 것과 유사하게, 보안 소프트웨어의 VPN 및 취약한 웹사이트 차단 기능 등을 이용해 악성코드 감염 및 제어 수단으로 활용하는 사례가 발견 될 것으로 예상된다.

4 지능화된 스피어피싱과 APT 공격 (하우리)

□ 2018년 보안위협 현황

▶ 암호화폐, 부동산, 증시 등 민감한 사회 이슈를 이용한 공격 지속
▶ 전통적인 소재 역시 꾸준히 등장 (이력서, 저작권 위반, 무료폰트 등)
▶ 워터링홀을 통해 ActiveX를 이용한 APT 공격

다양한 암호화폐들의 등장과 함께 해당 정책 자료를 위장한 악성코드가 등장하였다. 뒤를 이어 부동산과 증시 같은 금융투자 관련 내용을 이용한 악성코드들이 지속적으로 발견되면서, 사회적, 경제적 이슈를 이용한 악성코드들은 매년 꾸준히 발생한다는 사실을 확인할 수 있었다. 이력서 제출, 저작권 위반, 무료폰트 같은 일상적인 내용들로 위장한 스피어피싱 메일도 아직까지도 빈번히 배포되고 있다. 이러한 스피어피싱 메일은 정상 발신인 계정으로 위장하고 있기 때문에 악성코드에 감염될 가능성이 매우 높다.
또한, 특정 분야 웹 사이트의 방문객을 대상으로 하는 타겟형 공격인 "워터링홀" 공격도 발견되었다. 워터링홀 공격은 중요정보, 기밀정보들을 탈취하는 목적으로 사용되어져 왔다. 올해는 국내 모 소프트웨어가 액티브엑스(ActiveX)의 취약점 공격에 악용되었으며, 발생 당시 APT 공격형 악성코드를 유포하고 있었던 것으로 확인되었다.

□ 2019년 보안위협 전망

▶ 인공지능 기술로 강화된 개인 맞춤형 스피어 피싱 메시지 및 공격 등장
▶ 가짜뉴스 등 자극적 이슈 소재를 이용한 악성코드 유포 가능성 증대
▶ 보안이 취약한 중소기업을 대상으로 한 APT 공격 증대

□ 인텔리전스 전망

2019년부터는 개인 맞춤형 스피어 피싱이 등장하기 시작할 것으로 보인다. 지금까지는 주요 기관, 기업 연구소 등의 관심 내용으로 공격을 시도하였다면, 이제는 공개된 개인 정보를 바탕으로 개인의 관심사에 초점을 맞추어 공격이 이루어질 수 있을 것이다.
또한 급변하는 국제 정세와 국내 정치상황에 대해 가짜 뉴스들이 많이 배포될 것으로 보이며, 이를 틈타 가짜 뉴스와 함께 악성코드도 같이 유포될 가능성도 보이고 있다.
공격자들은 상대적으로 보안이 취약한 중소기업을 공격하여 개인정보 및 기업정보를 유출하고 랜섬웨어를 감염시키며, 악성코드 유포를 위한 경유지 등 다양한 방법으로 악용할 수 있다. 중소기업에서의 보안사고가 늘고 있는 점을 미루어 보아 중소기업을 대상으로 한 공격이 늘어나고 있다고 볼 수 있다.

5 사물인터넷을 겨냥한 신종 사이버 위협(잉카인터넷)

□ 2018년 보안위협 현황

▶ IP카메라, 음성인식스피커 등 스마트홈 기기 사용 증가에 따른 사이버 위협 증가
▶ 스마트카, 교통시스템, 전력망 등 도시 인프라 대상 사이버 공격 발생
▶ IP카메라, 스마트 냉장고, 차량 블루투스 해킹 시연(18.09. 노르마)

인터넷에 연결된 사물인터넷(IoT)가 급증하면서 IP카메라, 스마트 TV, 스마트 냉장고, AI(인공지능) 스피커 등 IoT 기기를 통한 해킹이 사회 문제로 대두되고 있다. 과거에도 스마트 홈 컨트롤러의 가스밸브 취약점, 스마트 냉장고의 악성코드 유포지로의 활용, 공유기의 취약점을 통한 개인 외부 계정 탈취 및 DDoS공격이 있어왔으나, 주로 DDoS에 활용하기 위한 좀비 기기화 및 IP카메라의 영상정보의 유출이 급격하게 증가하고 있다. 이는 더욱더 다양한 IoT 기기의 등장으로 댐, 철도 등 주요 인프라를 원격 감시하기 위해 설치한 IoT기기가 사이버 공격에 무방비로 노출된 경우에 주요 인프라의 IoT기기가 사이버공격, 테러 등에도 악용될 수도 있다는 우려를 보인다. KISA에 따르면 2012년부터 IoT 취약점 접수가 해마다 2배이상 증가하고 있는데, 이러한 취약점들은 주로 무선 공유기, 네트워크 장비 등에서 발견되고 DNS 변조 및 악성코드 유포 등에 악용되고 있다.

□ 2019년 보안위협 전망

▶ IoT 봇넷의 변종 및 다양한 봇넷 출현으로 IoT기기의 좀비기기화 증가
▶ IoT 봇넷을 이용한 DDoS 공격으로 블럭체인 및 암호화폐 네트워크 공격
▶ 좀비화된 IoT기기를 통한 개인정보 탈취 및 악성코드 유포의 숙주로의 악용

□ 인텔리전스 전망

2019년에는 가정 및 산업에서 사용되는 다양한 IoT 기기가 출시 될 예정으로 IoT 기기를 통한 대규모 사이버 공격이 현실화 되고 있다. 올해 2분기 평균 DDoS 공격 크기가 전년 동기 대비 543% 증가, 26Gbps(초당 기가비트)를 기록했다는 조사 결과를 볼 때, DDoS 공격 크기가 커진 것은 IoT 봇넷으로 인한 영향으로 분석된다. 이러한 영향은 미라이 봇넷의 변종 또는 새로운 봇넷의 증가로 볼 수 있으며 앞으로도 지속적으로 다양하고 많은 변종이 발견될 것으로 예상된다.

블록체인 네트워크도 DDoS 공격에 안전하지 않다. 넥서스가드에 따르면, 블록체인 네트워크 중 하나인 버지네트워크(XVG)의 경우, DDoS 공격으로 인해 170만 달러 이상의 버지 토큰 3천500만개가 유실되었다. 이러한 일반적인 DDoS 공격 뿐 만 아니라, 인프라 네트워크 및 산업용 네트워크 등을 대상으로 하는 DDoS 공격, 암호화폐를 요구하는 범죄 등으로 발전할 수 있을 것으로 예상된다. 앞으로 가능한 모든 기기가 IoT로 연결되고 IoT 활용이 늘면서 기기에 저장된 개인정보가 유출되거나 악성코드 유포지로 악용될 수도 있다.

6 소프트웨어 공급망 관련 사이버 공격 증가(빛스캔)

□ 2018년 보안위협 현황

▶ 개발업체 대상 사이버 공격으로 홈페이지 서비스 중단 사고 발생
▶ 쇼핑몰 웹 솔루션 업체의 S/W 취약점을 악용한 웹 해킹
▶ 소프트웨어 코드서명 인증서가 해킹으로 외부에 유출

2018년도 인터넷 위협 동향을 살펴보면 웹을 통해 유포하는 파밍, 피싱 등의 공격은 현저히 감소하였으나 정상사이트 하위에 은닉된 유해사이트는 지속적으로 발견되고 있다. 악성코드만 탐지되지 않을 뿐이지 지속적으로 홈페이지가 공격자에 의해 권한을 탈취당하고 공격자의 필요 목적에 따라 활용되고 있는 상황이다.

웹 개발업체가 공격에 의해 랜섬웨어에 감염되고 이를 통해 웹 서비스를 제공받는 수천여개의 홈페이지가 서비스가 중단되는 사고가 발생하였고, 모 쇼핑몰 웹솔루션에서 발견된 SQL 인젝션 취약점을 통한 웹 해킹으로 개인정보 유출 사고도 발생하였다. 또한 시장에 잘 알려진 원격 S/W 의 코드 사이닝 인증서가 해킹으로 외부에 유출되는 등 파급력이 큰 웹사이트 및 S/W 개발업체 등을 대상으로 하는 공격은 지속적으로 발생하고 있다.

□ 2019년 보안위협 전망

▶ 소프트웨어, 웹사이트 개발업체 대상 공격 증가
▶ 소프트웨어 취약점을 악용한 해킹 및 정보유출 증가
▶ 소프트웨어 코드서명 인증서를 해킹하는 공격 증가

□ 인텔리전스 전망

정상사이트 하위에 삽입된 유해사이트 링크는 수개월 이상 방치되어 조치되지 않고 공격자에 의해 계속 활용되고 있다. 공격의 통로는 열려 있으나 단지 악성코드를 뿌리지 않는다는 이유로 잠재적 위험에 노출된 채 방치된 상황이다. IP나 URL 기반 차단으로는 대응할 수 없는 사각지대이다.

신뢰하는 소프트웨어, 웹사이트 등도 지속적인 검증과 관리가 되지 않는다면 공격자의 타겟이 되기 쉽다. 보안투자가 열악하고 인원변동이 잦으며 관리가 되지 않는 웹에이전시, S/W 개발업체의 경우 공격의 조기 탐지 및 대응에 매우 어려움을 겪을 수 있다.

내부에서 오탐인지 여부를 판별하는 사이 공격자는 이미 공격을 마치고 소기의 목적을 달성할 수 있으므로 이에 대한 충분한 고민이 필요하다.

7 악성 행위 탐지를 우회하는 공격 기법의 진화

□ 2018년 보안위협 현황

▶ 공격의 흔적을 지우고 악성 기능을 모듈화한 IoT 봇넷 VPN필터 등장
▶ 백신 탐지를 우회하는 초소형 POS 악성코드(PinkKite, TinyPOS) 출현
▶ 안티 머신러닝 기능을 갖추고 있는 파이록키(PyLocky) 랜섬웨어 발견

올해 발견된 대형 사물인터넷 봇넷인 VPN필터(VPNFilter)는 악성 트래픽을 이용하여 전세계 50만대의 가정용 혹은 사무용 네트워크 장비를 감염시켰다. VPN필터는 장비 내 파일들과 데이터를 수집할 뿐만 아니라 장비를 벽돌로 만들어서 공격의 흔적을 지움으로써 VPN필터에 대한 추적을 방해할 수 있었다.

POS 단말기를 노리는 악성코드(PinkKite, TinyPOS 등)도 새롭게 발견되었다. PinkKite, TinyPOS라는 이름의 악성코드로 다양한 기능을 가지고 있음에도 불구하고 총용량이 수킬로 바이트로, 작은 용량을 이용하여 백신 탐지를 우회할 수 있었다.

스팸 메일을 통해 유포된 파이록키(PyLocky) 악성코드는 Locky 랜섬웨어를 모방하여 파이썬으로 작성된 신종 랜섬웨어입니다. 특히 파이록키는 안티 머신러닝 기능을 갖추고 있어 최근 시그니처 기반 백신의 대안 중 하나로 각광받고 있는 머신러닝 기술에 대한 우려를 낳았다.

□ 2019년 보안위협 전망

▶ DGA(Domain Generation Algorithm)를 이용하여 C&C 차단을 회피하는 악성코드 증가
▶ 머신러닝 기반 백신 및 탐지 시스템을 우회하는 사이버 위협의 진화
▶ 패치관리, 보안관리 등 중앙관리 S/W의 취약점을 악용한 공격 지속

□ 인텔리전스 전망

내년에는 DGA(Domain Generation Algorithm)와 같이 C&C 차단을 회피하는 악성코드가 증가할 것으로 보인다. 일부 관제업체와 보안장비에서는 악성코드로 인한 피해를 줄이기 위해 악성코드 백신탐지와 함께 C&C를 차단하는데, 악성 도메인을 자동 생성하는 신종 악성코드의 경우, 백신은 물론 네트워크 보안장비로도 탐지가 어렵다.

DGA와 같은 신종 공격기법에 대항하기 위해서 보안업체들은 머신러닝 기술을 연구하고 있으며 일부 백신의 경우, 시그니처가 아닌 머신러닝을 이용하여 신종 악성코드를 탐지하고 있다. 문제는 해커도 이러한 머신러닝을 공격에 이용할 수 있다는 점이다. 실제 인공지능 Watson을 보유하고 있는 IBM社는 세계적인 보안 행사인 블랙햇(Black Hat)에서 딥락커(DeepLocker)라는 인공지능 기반 악성코드를 소개한 바 있다.

패치관리, 보안관리 등 중앙관리 S/W의 취약점을 악용한 공격도 지속될 것으로 보인다. 특히, 보안이 취약한 S/W 개발업체의 경우, 인증서는 물론 S/W 소스코드도 노출될 수 있으며 해커는 이를 통해 악성코드를 은밀히 유포시킬 수 있다.