참고1 2020년 7대 사이버 공격 전망 포스터

참고2 2020년 7대 사이버 공격 전망 주요내용

2020년 7대 사이버 공격 전망
1. 일상 속으로 파고든 보안 취약점, 보이지 않는 위협 (KISA)
▶ 지능형 CCTV, AI 스피커 등 IoT 결합 서비스 대상 사이버 위협 증가 ▶ 윈도우 RDP 취약점(블루킵) 미패치 시스템을 노린 제2의 워너크라이 등장 우려 ▶ 지원 중단 혹은 예정 운영체제(윈도우7/XP, 서버 2008/2003 등) 취약점 공격 시도
2. 랜섬웨어, 개인에서 공공기관·기업으로 피해 확대 (안랩)
▶ 공공기관·기업으로 사칭하여 APT와 결합된 랜섬웨어 유포 ▶ APT와 결합된 랜섬웨어 공격, PC 공격보다 높은 금액 요구 ▶ 랜섬웨어 감염 시 백업 파일까지 암호화 및 피해 발생
3. 취약한 가상통화 거래소, 반복되는 해킹 사고 (잉카인터넷)
▶ 가상통화 탈취 및 가치 조작을 목적으로 가상통화 거래소를 꾸준히 공격 ▶ 가상통화 거래소 사칭 및 지갑 프로그램으로 위장한 악성코드 유포 증가 ▶ 피해를 눈치채기 힘든 채굴형 악성코드의 지속적인 유포 및 감염 시도
4. 문자 메시지, 이메일 안으로 숨어드는 악성코드 (하우리)
▶ 문자 메시지, 이메일 속 링크를 이용하여 악성 앱을 감염시키는 모바일 표적 공격 ▶ IoT 기기 보급 확산에 따른 대규모 IoT 봇넷 등장 및 DDoS 공격의 재개 ▶ 유효한 코드서명 인증서 탈취 시도 및 이로 서명된 악성코드 유포·감염 증가
5. 은밀하게 정교하게, 진화하는 지능형 표적 공격 (이스트시큐리티)
▶ 견적 의뢰서, 보도자료 등 정상 문서 파일을 위·변조한 스피어 피싱의 정교화 ▶ 문서 소프트웨어의 자체 보안 기능을 통한 보안위협 탐지 시스템 회피 증가 ▶ 구글 드라이브나 드롭박스, 슬랙 등의 정상 서비스를 활용해 악성코드 통신 기법 활용
6. 모바일까지 확대되는 소프트웨어 공급망 공격 (NSHC)
▶ 모바일 앱, 스마트폰 제조사를 대상으로 S/W 공급망 공격 확대 ▶ 스마트카, 의료기기에 설치되는 S/W에 악성코드 삽입을 노리는 공격 시도 ▶ S/W의 특정 사용자만을 선별하여 감염된 악성코드를 실행하는 표적 공격
7. 융합 서비스를 노리는 새로운 보안 위협의 등장 (빛스캔)
▶ 교통 시스템 해킹을 통한 교통 마비와 CCTV 무력화와 같은 스마트 시티 보안위협 등장 ▶ 스마트 공장의 유지보수 과정에서 전파되어 정보를 수집하고 시스템을 파괴하는 악성코드 ▶ 의료 시스템 해킹을 통한 환자 개인정보·처방전 데이터 유출 및 의료기기 오작동 유발

1 일상 속으로 파고든 보안 취약점, 보이지 않는 위협 (KISA)

▶ 지능형 CCTV, AI 스피커 등 IoT 결합 서비스 대상 사이버 위협 증가
▶ 윈도우 RDP 취약점(블루킵) 미패치 시스템을 노린 제2의 워너크라이 등장 우려
▶ 지원 중단 혹은 예정 운영체제(윈도우7/XP, 서버 2008/2003 등) 취약점 공격 시도

□ 사이버 위협 전망

얼마 전, 미국과 일본의 대학에서는 음성 명령을 암호화한 레이저를 이용해 아마존 알렉사, 애플 시리, 구글 어시스턴트 등 AI 스피커들을 해킹하는데 성공했다. 이처럼, 지능형 CCTV, AI 스피커 등 일상에 많이 사용되고 있는 IoT 결합 서비스를 대상으로 하는 사이버 위협이 증가하고 있다. 2019년 상반기에 발견된 윈도우 RDP 취약점(블루킵, CVE-2019-0708)은 2017년 워너크라이가 악용했던 SMB 취약점(이터널블루, CVE-2017-0144)처럼 악성코드 전파에 악용될 수 있으며, 인터넷에 노출된 장비 중 100만대 정도(5월 기준)가 이 취약점에 대한 패치가 이루어지지 않은 것으로 알려져 있다. 이를 노린 제2의 워너크라이가 등장할 우려가 있다. 또한, 내년 1월 14일에 MS 윈도우 7 및 서버 2008에 대한 보안 업데이트 지원이 중단됨에 따라, 국내 PC의 25% 정도(9월 기준)가 해커의 표적이 될 전망이다. 2017년 당시, 워너크라이도 보안 업데이트 지원이 중단된 윈도우 XP를 집중 공략했었다.

안전한 인터넷 행복한 미래 KISA

2 랜섬웨어, 개인에서 공공기관·기업으로 피해 확대 (안랩)

▶ 공공기관·기업으로 사칭하여 APT와 결합된 랜섬웨어 유포
▶ APT와 결합된 랜섬웨어 공격, PC 공격보다 높은 금액 요구
▶ 랜섬웨어 감염 시 백업 파일까지 암호화 및 피해 발생

□ 사이버 위협 전망

2020년에도 랜섬웨어가 기승을 부릴 것으로 전망된다. 다만, 과거에는 주로 불특정 개인 PC를 대상으로 무차별 감염을 시도하는 공격 패턴이었다면, 점차 공공기관 및 기업을 대상으로 APT를 통해 랜섬웨어를 감염시키는 공격이 주를 이룰 것이다.
클롭 랜섬웨어 공격자도 올해 초부터 특정 기관을 사칭해 문서 파일이나 실행 파일을 첨부한 이메일을 통해 국내 기업을 대상으로 랜섬웨어를 유포하였다. 향후, APT를 통해 기업 내부망까지 랜섬웨어에 감염시킴으로써 피해를 확대시키고, 이에 따라 점차 높은 금액의 복구 비용을 요구할 것으로 보인다.
NAS 장비에 저장된 데이터가 암호화된 피해 사례가 국내에서도 보고된 바 있고, NAS 장비를 노리는 새로운 랜섬웨어 이코랙스(eCh0raix)가 발견되면서 백업만으로는 안심할 수 없는 환경이 될 것이고 그에 따라 사용자도 데이터 및 장비에 대한 보안에 관심을 더 가져야 할 것이다.

3 취약한 가상통화 거래소, 반복되는 해킹 사고 (잉카인터넷)

▶ 가상통화 탈취 및 가치 조작을 목적으로 가상통화 거래소를 꾸준히 공격
▶ 가상통화 거래소 사칭 및 지갑 프로그램으로 위장한 악성코드 유포 증가
▶ 피해를 눈치채기 힘든 채굴형 악성코드의 지속적인 유포·감염 시도

□ 사이버 위협 전망

국내 가상통화 거래소가 최근 3년간 해킹 사고로 1200억 원이 넘는 경제적 피해를 입었다고 한다. 해킹 사고로 인해 개인정보 유출은 물론, 가상통화도 탈취됐기 때문이다. 국외의 경우, 바이낸스 해킹 사고 이후 비트코인 시세가 급락하기도 하였다. 공격자는 거래소 시스템을 직접 공격할 뿐만 아니라 거래소 사용자들까지 노리고 있다. 거래소를 사칭하여 가상통화 투자계약서나 지갑 프로그램으로 위장한 악성코드를 사용자들에게 유포하고 있다. 거래소 사용자들이 이러한 악성코드에 감염될 경우, 가상통화 탈취는 물론 사용자 PC가 가상통화 채굴에 악용될 수도 있다. 이러한 채굴형 악성코드의 경우, 사용자들이 피해를 눈치 채기 힘들기 때문에 앞으로도 다양한 타깃을 대상으로 꾸준히 유포될 것이다.

4 문자 메시지, 이메일 안으로 숨어드는 악성코드 (하우리)

▶ 문자 메시지, 이메일 속 링크를 이용하여 악성 앱을 감염시키는 모바일 표적 공격
▶ IoT 기기 보급 확산에 따른 대규모 IoT 봇넷 등장 및 DDoS 공격의 재개
▶ 유효한 코드서명 인증서 탈취 시도 및 이로 서명된 악성코드 유포 및 감염 증가

□ 사이버 위협 전망

이제 APT 공격이 컴퓨터를 넘어서 스마트폰까지 노리고 있다. 얼마 전 탈북자와 대북 분야 관련자를 대상으로 한 모바일 APT 공격이 발견되었다. 문자 메시지나 이메일 속 링크를 이용함은 물론, 사진뷰어나 모바일 메신저를 사칭하여 악성 앱 설치를 유도하고 표적 공격에 악용하는 것이다. 공개된 플랫폼이 아니라, 링크로 공유되는 만큼 악성코드 유포 과정에서의 탐지가 매우 어렵기 때문에 주의를 기울여야 한다. 또한, IoT 기기의 보급 확산에 따라 수집만대가 넘는 IoT 봇넷이 등장하고 있다. IoT 봇넷의 경우, 복잡한 악성행위를 수행하기 보다는 간단한 DDoS 공격용으로 자주 사용된다. 따라서 미라이 봇넷 때와 같은 대규모 DDoS 공격이 재개될 가능성이 높다. 프로그램의 신뢰도를 높이기 위해 S/W 개발사들이 공인된 인증기관을 통해 발급받은 코드서명 인증서가 역으로 악성코드 유포 및 감염에 악용되고 있다. 프로그램 다운로드나 실행 단계에서 백신 프로그램의 탐지를 회피하기 쉽기 때문이다. 이러한 코드서명 인증서 악용 사례는 S/W 공급망 공격과 마찬가지로 보안이 취약한 개발사를 노리기 때문에 앞으로도 증가할 것이다.

5 은밀하고 정교하게, 진화하는 APT 공격 (이스트시큐리티)

▶ 기업 및 기관 대상, 정상 문서 파일을 위·변조한 스피어 피싱의 고도화
▶ 문서 소프트웨어의 자체 암호 설정 기능을 통한 맞춤형 표적공격
▶ 구글 드라이브, 슬랙 등의 상용서비스를 이용한 명령통신 기법 활용

□ 사이버 위협 전망

APT 공격에 사용되는 스피어 피싱이 날로 정교해 지고 있다. 주로 거래 업체의 견적의뢰서, 언론사의 보도자료 등 정상 문서 파일을 위·변조하여 악성코드를 유포하므로 사람이 육안으로 악성여부를 쉽게 판단하기 어렵다. 또한, 기존에는 자체 제작한 해킹 도구를 이용하여 표적 공격을 진행했던 것과 달리, 기업에서 일반적으로 활용하는 정상 서비스 등을 악용함으로써 보안 솔루션의 탐지를 우회하려는 시도가 늘어나고 있다. 특히, 문서 소프트웨어의 자체 암호 설정 기능을 악용할 경우, 맞춤형 표적공격과 함께 보안 솔루션의 탐지를 회피하고, 수신자의 신뢰를 얻기도 쉽다. 구글 드라이브나 드롭박스, 슬랙과 같은 상용 서비스를 활용해 악성코드와 통신하는 사례가 보고되었는데, 이러한 서비스들은 기본적으로 암호화 통신을 사용하기 때문에 보안 모니터링을 우회하기 용이하고, 정상 서비스처럼 위장하기 쉽다. 이 밖에도 공격자들이 국내외 웹 서버를 해킹하거나 호스팅 서비스를 받아 이메일 서버를 자체 구축해 발신지를 실제 공식 도메인처럼 조작하는 스피어 피싱 위협이 성행하여, 수신자로 하여금 신뢰기반의 APT 공격을 진행하고 있어 갈수록 위협이 증가할 전망이다.

6 모바일까지 확대되는 소프트웨어 공급망 공격 (NSHC)

▶ 모바일 앱, 스마트폰 제조사를 대상으로 S/W 공급망 공격 확대
▶ 스마트카, 의료기기에 설치되는 S/W에 악성코드 삽입을 노리는 공격 시도
▶ S/W의 특정 사용자만을 선별하여 감염된 악성코드를 실행하는 표적 공격

□ 사이버 위협 전망

기업의 업무활동에 모바일 앱의 도입이 활발해 지면서 소프트웨어 공급망 공격이 모바일까지 확대될 전망이다. 특히, 모바일 기기에는 미리 설치된 앱들이 PC에 비해 많고 삭제가 쉽지 않아, 모바일 앱 제조사뿐만 아니라 스마트폰 제조사도 공격의 대상이 될 수 있다. 특히, 스마트카나 의료기기들은 소프트웨어 업데이트 및 추가 설치가 쉽지 않아 기본적으로 설치된 소프트웨어가 악성코드에 감염되었을 경우, 피해가 클 수 있다. 이러한 융합 서비스들은 상대적으로 최신 기술로써, 보안이 검증되지 않거나 보안에 대한 투자가 미비하여 기존 S/W 공급망보다 공격에 취약할 수 있다. 이는 S/W 공급망 뿐만 아니라 H/W 공급망에 있어서도 마찬가지다. 지난 3월에는 대만의 한 PC 공급사의 소프트웨어 업데이트 시스템 해킹당하면서 전 세계적으로 100만대 이상의 PC가 악성코드에 감염되었다. 이 악성코드는 제작단계부터 특정 회사를 대상으로 정밀하게 제작되었을 뿐만 아니라, 소수의 PC만을 선택하여 내부 정보를 유출하도록 추가 악성코드에 감염시켰다. 이 밖에도 유효한 코드서명 인증서를 악용하여 악성코드를 유포하는 등 공격 기법이 점점 더 은밀하고 정교해질 전망이다.

7 융합 서비스를 노리는 새로운 보안 위협의 등장 (빛스캔)

▶ 교통 시스템 해킹을 통한 교통 마비와 CCTV 무력화와 같은 스마트 시티 보안위협 등장
▶ 스마트 공장의 유지보수 과정에서 전파되어 정보를 수집하고 시스템을 파괴하는 악성코드
▶ 의료 시스템 해킹을 통한 환자 개인정보·처방전 데이터 유출 및 의료기기 오작동 유발

□ 사이버 위협 전망

4차 산업혁명의 주요기술로 주목받고 있는 스마트 시티, 공장, 의료 등 융합 서비스의 구축이 본격화 되면서 이에 대한 보안 위협도 증가하고 있다. 2017년 미국 캘리포니아에서는 지역 버스와 경전철 시스템이 랜섬웨어의 공격을 당해, 결제 시스템이 작동하지 않은 사고가 발생했었다. 향후, 자율주행 및 무인셔틀 서비스가 대중화 될 경우, 해킹 사고로 인해 인명피해까지 발생할 수 있다. 스마트 공장의 경우, 수십에서 수만 개의 IoT 기기가 서로 연결되어 있어 해킹을 당한다면 공장 전체의 가동이 중단될 수도 있다. 또한, APT 공격을 통해 공장 시스템이 장악될 경우, 시스템 오동작 및 파괴를 목적으로 공장 곳곳에 악성코드를 감염시킬 수 있다. 최근 AI 기술의 발달로 인해, 의료기관에서 지능화된 의료 시스템을 적극적으로 도입하고 있다. 이러한 의료 시스템에는 환자의 개인정보는 물론 처방전 등 의료 데이터도 저장되어 있어, 해커들의 좋은 타깃이 될 수 있다. 뿐만 아니라, 의료기기에 악성코드를 삽입하여 오동작을 일으키거나 처방전이나 영상기록을 조작할 경우, 환자들의 생명도 위협할 수 있다.