***Report***



**Security**

**제 출 일 : 2015. 05. 22**

**소 속 : 소프트웨어학과**

**과 목 : IT 세미나**

**이 름 : 정유석**

EMB000005ec6b9b

**Index**

1. Introduction
2. Security

2. 1 : CCTV

2. 2 : Biometrics

2. 3 : Hacking

2. 4 : Malware

2. 5 : Cyberwarfare

1. Conclusion

References

1. Introduction

사업을 운영하고 개인 정보를 관리함에 있어서 네트워크로 연결된 컴퓨터의 사용이 나날이 증가하고, 대부분의 기업 임직원들은 회사 IT 자원을 지역적으로나 원격적으로 액세스하고, 고객의 정보를 전산화 하면서, 그 어느 때 보다 컴퓨터 시스템 보안에 대한 필요성이 매우 강조되고 있다. 하지만 수많은 기업들과 정부 기관들이 IT 보안 기술에 엄청난 투자를 했음에도 불구하고 여러 사이버 공격의 피해자가 되었다. 따라서 이번 레포트를 통해 보안에 대해 깊숙이 알아보고, 여러 기업들과 사례, Malware에 대해서 알아보겠다.

2. Security

보안은 유형, 무형의 정보 생성과 가공, 유통, 배포, 그리고 정보를 사용하는 과정에서 발생하는 여러 부작용에 대처하기 위한 모든 정보 보호 활동을 포괄하는 광의의 개념이다.(1) 다음으로 이러한 여러 가지 정보 보호 활동과 사례들, 각 분야별 기업들을 보겠다.

2. 1 : CCTV

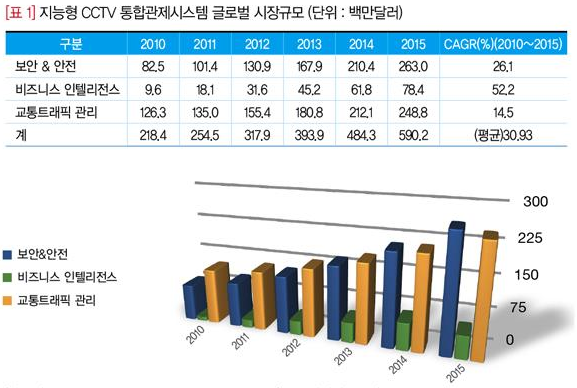


그림 1 : CCTV 세계 시장 규모

CCTV는 특정 수신자를 대상으로 화상을 전송하는 텔레비전 방식을 말하며, 산업용, 교육용, 의료용, 교통 관제용 감시, 방재용 및 사내의 화상정보 전달용 등으로 다양한 용도로 사용되고 있으며, 그림 (1)처럼 2014년 세계 시장 규모는 총 5조 2천억원의 규모이다.(7)

대표적인 CCTV 종류에는 ‘고정형 CCTV’, ‘SpeedDom CCTV’, ‘적외선 CCTV’, ‘IP CCTV’ 등이 있다.(2)

‘고정형 CCTV’는 실외와 실내에서 한정된 지역을 고정적으로 촬영을 하는 CCTV로, 실외 고정형 CCTV는 방수, 방진 등 환경적 요인에 보호하기 위해 외부가 감싸져 있고, ‘내부 고정형 CCTV’는 돔 형식으로 미관을 중요시하고, 영상 전송 케이블을 자연스럽게 숨길 수 있다. 하지만 이것은 Zoom 기능이 없고, 렌즈와 본체가 일체형 카메라에 비해서 성능이 떨어져 이러한 단점을 보완하고자 나온 CCTV가 ‘SpeedDome CCTV’이다.(2) 또한, ‘적외선 CCTV’는 적외선 기능을 통해 육안으로 식별이 불가능한 어두운 외곽경비지역에 주로 설치되며, 최근 CCTV 트렌드인 ‘IP CCTV’는 TCP/IP를 활용해 카메라가 촬영한 감시 영상을 저장하고, 전송하는 네트워크 감시 카메라이다.(3)

이러한 CCTV의 대표적인 기업으로 ‘IDIS’가 있다. IDIS는 총 임직원수 290명이며, 2015년 1분기 매출은 347억원으로 올해 1415억원의 매출액을 기록할 것으로 예측되고 있다.(4)

IDIS의 대표적인 제품군으로는 ‘IDR9832’, ‘IDR7816’ 등 디지털영상저장 및 전송장치인 ‘DVR’이 있다. IDIS의 DVR은 2014년 약 5,000억원의 규모로 측정되는 국내 시장에서 49%의 점유율을 차지하고 있고, 2014년 세계 DVR분야 시장에서 1위로 선정되었다.(5) 또한, ‘IP CCTV’와 네트워크를 통해 감시카메라에 입력된 영상 데이터를 저장하는 장치인 ‘NVR’을 같이 통합한 솔루션인 ‘다이렉트 IP’를 출시하며 세계시장에 진출하고 있다.(6)

현재 IDIS는 미국 CCTV 시장 진출에 본격화하고 있다. 미국 시장은 전세계 보안시장 점유율 30%에 해당하는 연간 5조원 규모의 세계 최대 보안시장이다. 따라서 IDIS는 차세대 영상표준인 H. 265와 UHD 해상도에 기반한 보안 솔루션을 통해 중남미 시장까지 공략할 계획이다.(7)

2. 2 : Biometrics

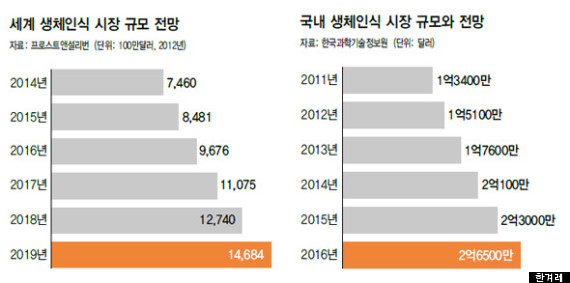


그림 2 : Biometrics 세계 및 국내 시장 규모

Biometrics란 생체인식 또는 생체 측정학으로, 사람의 생체적, 행동적인 특성을 이용하여 특정 개인을 식별하는 학문 또는 기술이며(1), 그림 (2)처럼 Biometrics의 2014년 세계 시장 규모는 81조 3천억원, 국내 시장 규모는 2192억이다.(8)

Biometrics의 대표적인 종류는 ‘fingerprinting’, ‘IRIS scanning’, ‘face recognition’등이 있다.(9)

지문인식(fingerprinting)은 사람의 손에 있는 지문을 읽는 것으로, 수용성, 편의성, 신뢰성 등의 장점으로 생체 인식 기술 중에서 가장 많이 이용되는 방법이다. 이러한 지문인식 기술은 출입 통제 및 근태관리, 키보드-마우스-모니터 등에 지문 인증장치를 추가하여 PC 및 각종 응용프로그램을 보안, 현금 인출 및 은행 금고 이용 시 통장 및 기타 물품에 대한 요구 대신 지문인식 등을 통해 보안을 강화하고 있다.(9)

홍채인식(IRIS scanning)은 사람의 눈에서 중앙의 검은 동공과 공막(흰자위)사이에 존재하는 도넛모양의 홍채 무늬 패턴을 이용하여 사용자를 인증하는 기술이다.(1) 이러한 홍채인식 기술은 민간 기업과 정부의 물리적 출입통제가 필요한 곳에 활용되고 있으며, 교통, 의료 및 국가 식별 프로그램과 다양한 경제 분야에서의 사용 증가로 이어지고 있다. 또한, 최근에는 근태관리 등 생산성 향상 응용 프로그램에서도 주로 채택되고 있다.(10)

얼굴인식(face recognition)은 사람마다 얼굴에 담겨있는 고유한 특징 정보(눈, 코, 입 등의 위치)를 이용하여 사용자를 식별하고 인증하는 기술이다. 이러한 얼굴인식 기술은 공항/항만 출입국심사, 인터넷 금융 결제, 개인 금고 보안 등의 ‘개인 인증’ 분야와 CCTV Surveilance(용의자 검색), 지능형 DVR시스템 등 ‘무인 영상 감사’분야, 지능형 비전로봇, 졸음운전 방지, Auto Focusing Camera 등 ‘자동화’ 분야에서 사용되고 있다.(10)

Biometrics의 대표적인 국내 기업으로는 ‘슈프리마’가 있다. 슈프리마는 지문인식 분야 세계 1위 기업으로 2013년 기준 임직원 수는 100여명 정도와 550억원의 매출을 기록하고 있다.(11)

슈프리마의 대표적인 제품으로는 지문인식을 통한 출입통제근태 단말기인 ‘BioEntry W’, ‘BioStation’를 통해 세계 시장에 진출하고 있으며, 얼굴인식 시스템인 ‘FaceStation’과 이것들을 관리하는 소프트웨어인 ‘BioStar’를 멕시코, 이란, 콜롬비아 등 여러 국가로 수출하고 있다.(12)

현재 슈프리마는 바이오인식 기술을 기반으로 하는 하드웨어, 소프트웨어를 모두 아우르는 솔루션을 개발해 ‘통합 보안 플랫폼’을 제공하는 ‘바이오 인식 기반 토털 보안 플랫폼’ 기업으로 나아갈 것이라는 목표를 잡았다. 또한, 웹 API를 지원해 CCTV, ERP, 포털 서비스에서도 이용 가능하고, 클라우드 시스템과의 연계 및 각종 기기에 연동이 가능하도록 확장성을 지원하려 한다.(12)

2. 3 : Hacking

해킹(hacking)은 전자 회로나 컴퓨터의 하드웨어, 소프트웨어, 네트워크, 웹사이트 등 각종 정보 체계가 본래의 설계자나 관리자가 의도하지 않은 동작을 일으키도록 하거나, 체계 내에서 주어진 권한 이상으로 정보를 열람, 복제, 변경 가능하게 하는 행위를 광범위하게 이르는 말이다.(1)

이러한 해킹이 가능한 이유 중 하나는 ARP의 단점을 이용한 것이 있다. ARP는 네트워크 통신에서 컴퓨터의 물리적 네트워크 주소를 모를 때, 각각의 컴퓨터를 구분할 수 있게 해주는 것이다. 하지만 이것은 누가 보냈는지 검증할 수 없기에 이것을 이용해 같은 네트워크상에서 악의적인 공격자가 패킷을 위조하여 위조된 정보를 보낸다면 검증할 방법이 없어 당할 수 밖에 없다. (이것을 ‘ARP 스푸핑’이라고 부른다.)(13)

또한 이것 이외에도 웹 보안의 취약성을 이용한 ‘Injecting Malicious Data’과 ‘Exploitiong Unchekced Input’, 네트워크상에서 사용자의 패킷 교환을 엿듣거나 가로채는 ‘Sniffing’, 각자리 숫자를 전부 대입하여 비밀번호를 알아내는 ‘Password Cracking’ 등이 있다.(13)

이러한 해킹의 대표적인 사례로는 ‘MS 윈도우 2000’ 소스코드 온라인 공개가 있다. 2004년 한 해커가 마이크로소프트 기업 네트워크에 침투해 윈도우 2000의 소스코드를 빼내어 온라인에 공개한 것이다. 또한, 2010년 구글은 일명 ‘오로라 공격(Aurora attacks)’이라는 수 개월에 걸친 네트워크 침입으로 구글의 주요 지적 자산이 유출되기도 했다. 국내에서도 이러한 해킹 사례가 있는데, 2011년 4월 농협의 서버 유지보수를 맡은 외주직원의 노트북에 악성코드를 심어 이를 통해 농협 전산망을 마비시키는 경우가 있고, 최근에는 Paros라는 프로그램을 사용하여 KT고객의 9자리 고유 번호를 맞춰 1200만명의 개인정보가 유출되는 사례가 발생되기도 했다.(14)

2. 4 : Malware

악성 소프트웨어를 일컫는 Malware는 사용자의 동의 없이 사용자의 시스템에 설치된, 원하지 않는 소프트웨어라고 정의할 수 있다. 이것들은 데미지를 주지 않는 약한 소프트웨어에서 심각한 보안문제를 야기해 PC안에 있는 모든 자료나 개인정보를 탈취할거나, PC를 고장나게 하는 것까지 그 종류가 다양하다.(1)

이러한 Malware의 종류에는 ‘virus’, ‘Trojan horse’, ‘worm’, ‘DDoS’, ‘rootkit’, ‘backdoor’ 등이 있다.

우선 ‘virus’는 특정한 파일을 감염시켜 해당 파일이 실행되면 동작하는 악성코드만을 일컫는 말이다. (1) ‘Trojan horse’는 실제 역사 속의 트로이 목마를 본뜬 이름으로 사용자의 컴퓨터에 침투하기 위해 겉으로는 무해해 보이는 프로그램이나 파일에 악의적인 코드를 감춰 침투하여 자신의 시스템을 설치한 뒤, 백그라운드에서 서버와 통신하여 제 3자가 사용자의 컴퓨터에 접근할 수 있도록 하는 것이다. (15) ‘worm’은 Network Aware virus라고 불리기도 하는데, 다른 프로그램의 감염 없이 자신 혹은 변형된 자신을 복사하는 명령어들의 조합이다. 이것은 기억장소에 코드 형태로 존재하거나 혹은 실행파일로 존재하며 실행되면 파일이나 코드 자체를 다른 시스템으로 복사한다.(16)

‘DDos’는 분산 서비스 거부 공격을 뜻하는 것으로 인터넷상에서 사이트 공격을 하는 방법 중 하나로 사이버 테러의 대표적인 경우다.(1) 이것은 여러 대의 컴퓨터에서 한 웹 서버에 비정상정인 트래픽을 흘려 보내 웹 서버가 과도한 트래픽 소모 및 프로세스 진행과 입-출력 등을 통해 서버를 다운시키는 기본적인 서버 공격 방법이다.(16)

‘rootkit’이란 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입을 위한 ‘backdoor’, 원격 접근, 내부 사용 흔적 삭제, 관리자 권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램의 모음이다.(1) 여기서 ‘backdoor’는 일반적인 인증을 통과, 원격 접속을 보장하고 시스템 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법을 일컫는다. ‘backdoor’는 설치된 프로그램의 형태를 취하기도 하고, 기존 프로그램 또는 하드웨어의 변형일 수도 있다.(16)

이러한 Malware는 해킹공격에 대한 우월적인 모습을 보이기 위한 이슈화가 목적이었다면, 이제는 여러 다양한 목적을 가지고 조직적으로 운영 되고 있으며, 지하 세계를 형성하고 있다. 이러한 조직들은 단순히 금전적 이득을 노리는 경우도 있지만, 군, 기업의 기밀 자료 또는 사용자 정보 등 기업의 지적 재산을 목적으로 하기도 하며, 정치적, 사회적 목적으로 계획하기도 한다.(16)

이러한 Malware underground를 국가에서 주도 하는 경우도 있다. 그 중 미국은 정치적, 사회적 목적 및 금전적 이득을 위해, 러시아는 에너지 산업 수출을 위한 정치적 목적, 중국은 경제적인 이유로 Malware 조직들을 이루고 있다. 그 외에 여러 Malware 조직들이 있지만 이러한 조직들을 추적하거나 제재하기는 어렵다. 이유는 배포자들이 사용자들에게 비즈니스를 익명으로 운영할 수 있게 해주기도 하고, 추격 과정을 어렵게 만드는 ‘proxy layering’ 구조를 사용하고 있기에 백신 업체가 이들을 발견하더라도 당국이 도착하기 전에 이미 도주를 한다는 것이다. 이러한 Malware underground 제품의 대표적인 예로는 은행 정보를 빼내기 위해 설계된 ‘제우스 트로이안’이 있다. 이것을 만든 조직은 고객의 요구에 따라 제품 기능을 커스터마이즈 해주기도 한다.(17)

Global Anti-Malware의 대표 글로벌 기업으로 ‘트렌드마이크로’가 있다. 트렌드마이크로의 2013년 기준 총 임직원수는 약 4,940명이며 총 매출액은 1조 2천억원이다.(18)

트렌드 마이크로의 대표적인 제품으로는 개인용 종합보안소프트웨어인 ‘AV-TEXST’가 있으며, 기업을 위한 클라우드 및 데이터센터 보안 솔루션인 ‘Deep Security’, 문서 보안을 위한 ‘Office Scan’, 중소기업용 클라우드형 보안 서비스인 ‘Worry-Free’ 등의 다양한 솔루션을 제공하고 있다.

최근 트렌드마이크로는 해당 PC에 잠복해 있다가 결정적인 순간에 공격하는 ‘APT 공격’을 대비해 네트워크 행위를 기반으로 의심스러운 악성코드를 탐지해내는 기법을 통합한 ‘샌드박스 기술’을 출시할 예정이다.(18)

‘APT 공격’은 국내 SK커뮤니케이션즈의 가입자의 개인정보가 유출된 사건에도 이용되었는데, 최근 이러한 공격이 다양해지고 치밀해지면서 국내 주요 Antil-Malware 기업들도 APT 보안 솔루션 기술 개발에 열을 올리고 있는데, 대표적인 기업으로 ‘안랩’이 있다.(19)

국내 기업인 안랩은 2014년 기준 총 임직원수는 약 950명이며 총 매출액은 1354억원이다.(20)

안랩의 대표적인 제품으로는 기업 및 개인 보안 소프트웨어인 ‘V3’ 시리즈와 ‘자녀 보호 서비스’, ‘명의 도용 차단 서비스’ 등이 있으며, 네트워크 보안 소프트웨어인 ‘TrusGard’시리즈가 있다.(20)

최근 안랩은 위에서 언급한 것처럼 현재 유행하는 APT 공격에 대비하여 클라우드 기반의 사전분석 기술을 활용해 APT 공격을 정확하게 탐지할 수 있는 솔루션을 출시할 예정이다. 또한 안드로이드 기반 스마트폰에 대한 원스톱 보안을 제공하는 ‘AhnLab V3 Mobile Security’를 출시하여 글로벌 시장 진출을 진행하고 있다.(18)

‘KISA’는 대한민국의 인터넷 진흥, 인터넷 정보보호 및 그에 대한 국제적 협력을 진행하는 미래창조과학부 산하 위탁집행형 준정부기관이다. 그리고 ‘NIS’는 국가안전보장에 관련되는 정보·보안 및 범죄수사에 관한 사무를 담당하는 대한민국의 중앙행정기관 및 대통령 직속기관이다.(1) 이 두 조직은 어떠한 Malware 또는 Hacking이 발견될 시, 서로 협조하여 공격에 사용된 악성 프로그램을 분석하고, 안랩ㆍ하우리 등 백신업체에도 샘플을 제공하여 백신개발을 독려하는 등 민간 전문업체와 공조체제를 가동한다.(21)

2. 5 : Cyberwarfare

사이버전쟁(Cyberwarfare)이란 국가간의 인터넷을 비롯한 사이버공간에서 일어나는 전쟁을 사이버전쟁(Cyberwarfe)이라고 한다.(1)

이러한 국가간의 사이버전쟁의 대표적인 예로는 우크라이나와 러시아가 있다. 2014년 친 러시아 세력으로 자처한 ‘사이버검독수리’가 러시아의 정치적 변절자인 700여 우크라이나 정부 기관의 전화를 불통시키고, 우크라이나 정부 산하 기관이나 위원회에 DDoS 공격 및 해킹을 하였다. 또한, 2013년 북한은 국내 언론사 및 은행 내부시스템 파괴를 목적으로 한 APT 공격과, 청와대ㆍ국무 조정실 등 정부 기관에 해킹 및 DDoS 공격을 했다. 또한, 현재에도 많은 주요 국가 및 기업에서 군수 업체 해킹 및 정부기관 DDoS 공격 등 여러 가지 목적으로 전쟁이 계속 이루어지고 있다.(22)

이러한 사이버전쟁도 실제 전쟁처럼 교전 규칙을 국제적으로 정리한 ‘탈린 매뉴얼(Tallinn Manual)’이 있다. 탈린 매뉴얼에서는 사이버 공격을 국가간 무력 분쟁의 한가지로 규정하고 있으며, 사이버 공격을 받았을 경우 이에 대한 대응 조치로 사이버 공격을 하는 것은 원칙적으로 가능하지만, 실제적이고 물리적인 무력을 사용한 공격은 사이버 공격으로 인해 실제 사망자나 부상자가 발생하였을 경우에만 허용할 수 있는 것으로 명시하였다. 또한, 국제적으로 잘못된 사이버행위로 피해를 본 민간인은 공격에 책임이 있는 국가들을 상대로 대응 조치를 취할 수 있도록 규정하였다.(23)

하지만 탈린 매뉴얼은 구속력이 없으며 사이버 전쟁을 둘러싼 국제법적 유권해석과 국제 사회의 대부분의 관계자들의 의견을 반영한 일종의 가이드라인으로 지침서의 형식을 취하고 있다.(23)

3. Conclusion

최근 기업, 국가들에게는 무엇보다 전산화된 정보를 보호하기 위한 보안 문제가 더욱 더 중요해지고 있다. 이런 이유로 많은 기업, 국가들이 보안 문제에 대해 많은 지원과 투자를 하고 있지만, 지속적으로 보안 사고들이 생기고 있다. 이러한 이유를 보안 전문가들은 솜방망이 처벌에 바이러스는 계속 생기고 있으며, 극단적인 처벌을 통해 바이러스 생성 및 해킹에 대비해야 된다고 한다.

이번 조사를 통해 Malware와 Hacking의 차이점에 대해 알게 되었고, Hacking과 Malware의 여러 종류와 그 형태들을 자세히 알게 되었다. 한국 인터넷 진흥원은 국내에서만 총 14만대의 컴퓨터가 바이러스에 감염되었고, 현재에도 수 많은 개인정보 유출이 있으며, 매일 국외에서 국내로 수 많은 DDoS 공격과 그 공격의 유형도 변화하고 있다고 한다. 이러한 유출과 공격을 막기 위해서는 개인과 기업은 수시로 자신들의 정보 보안에 신경 써야 하며, 국제적으로 해킹에 대한 처벌을 강화하고, 서로 협조해 정보를 공유하여 사이버공격에 대응해야 할 것이다.

References

(1) 위키트리 : [www.wikitree.co.kr/](http://www.wikitree.co.kr/)

(2) REALOG : <http://blog.63realty.co.kr/707>

(3) 리눅스포털 : <https://www.linux.co.kr/home2/board/subbs/board.php?bo_table=termboard&wr_id=367>

(4) Etnews : <http://www.etnews.com/20150430000279>

(5) IDIS : <http://www.idis.co.kr/product/product_view?firstpcIndex=1>

(6) 경제조선 : <https://economyplus.chosun.com/>

(7) CCTVnews : <http://www.cctvnews.co.kr/news/articleView.html?idxno=20562>

(8) THE HUFFINGTON POST : http://www.huffingtonpost.kr/2014/10/26/story\_n\_6051698.html

(9) secuIT : <http://www.secuit.com/>

(10) IRIS ID : <http://www.irisid.co.kr/productssolutions/technology-2/currentfutureuse/>

(11) DongA news : <http://news.donga.com/3/all/20130127/52625708/1>

(12) 슈프리마 : [www.suprema.co.kr/](http://www.suprema.co.kr/)

(13) IT 강국 : <http://blog.oe.je/entry/>

(14) IT World Korea : [www.itworld.co.kr/slideshow/86870](http://www.itworld.co.kr/slideshow/86870)

(15) 엔하위키미러 : <https://mirror.enha.kr/>

(16) 알약 : <https://alyac.co.kr/>

(17) IT world : <http://www.itworld.co.kr/print/74009>

(18) 트렌드마이크로 : <http://www.trendmicro.co.kr/kr/index.html>

(19) 아이뉴스 24 오피니언 : <http://opinion.inews24.com/>

(20) 안랩 : <http://www.ahnlab.com/kr/site/main.do>

(21) KISA(한국인터넷진흥원) : <http://www.kisa.or.kr/>

(22) UniKoea : <http://blog.unikorea.go.kr/4322>

(23) 경찰청 사이버안전국 : <http://www.netan.go.kr/board/boardView.do?board_id=cyber&id=5234&page=1>