

안랩 보안 매거진

월간 安

2012. 12

Forensic Service



CONTENTS

3 SECURITY ISSUE

‘월간 安’으로 돌아본 2012년 보안 동향

6 SPECIAL REPORT

사전 예방 관점의 포렌식 서비스

1부_ 포렌식, 차세대 보안을 예고하다

2부_ "사후 대응을 넘어 사전 예방의 키워드 될 것"

14 SPOTLIGHT

안랩의 차세대 보안관제를 주목하라

16 THREAT ANALYSIS

한글 파일 악용한 공격 잇따라...기업·기관 ‘주의보’

19 TECH REPORT

아이폰 백업 파일 포렌식

2부_ 앱을 읽으면 사용자의 라이프스타일이 보인다

23 IT&LIFE

보이지 않는 세상 속 악의 ‘손’, 사이버 범죄

2부_ 사이버 범죄의 피해 현황과 ‘크رائم웨어’

26 AHNLAB NEWS

안랩, ‘파트너 엔지니어 기술 강화’ 나서

‘특허 경영’으로 안랩의 기술 리더십 강화

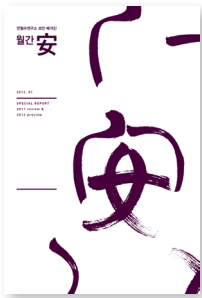
안랩, 글로벌 보안 기업들과 제휴 및 파트너십 체결

29 STATISTICS

10월 보안 통계 및 이슈

‘월간 安’으로 돌아본 2012년 보안 동향

안랩의 온라인 보안 매거진 월간 安은 매달 보안 동향과 위협 대응을 위한 최신 정보를 다루고 있다. 월간 安의 스페셜리포트 (Special Report)만 모아놓아도 한 해의 보안 위협을 한 눈에 볼 수 있다고 해도 과장은 아닐 것이다. 2012년 월간 安은 다양한 보안 위협은 물론 개인정보보호법, 정보통신망법 등 기업의 컴플라이언스 이슈부터 드라마 ‘유령’까지 보안과 사회 전반의 트렌드를 빠짐 없이 담아냈다.



2012년 1월호 보안 위협, 2012년 ‘더욱 교활하고 정교해진다’

안랩은 월간 安 1월호를 통해 2011년에 이어 2012년에도 APT(Advanced Persistent Threat) 형태의 공격들이 지속될 것으로 예상했다. 특히 소셜네트워크서비스(SNS) 등으로 수집된 개인 정보들을 이용하여 목표한 기업이나 단체의 특정 구성원을 대상으로 업무 메일 등으로 위장해 내부 침투를 시도할 것으로 내다봤다. 특히 국내에서는 일반적으로 널리 사용되는 소프트웨어의 업데이트 관련 파일의 변조를 통해 다수의 목표 대상 기업의 직원들이나 특정 산업군에 대한 넓은 범위에서의 공격도 이뤄지고 있다는 점을 강조했다.



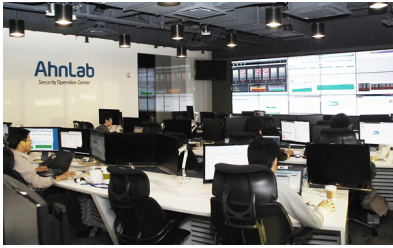
2012년 2월호 모바일 시대 겨냥한 악성코드 급증

월간 安 2월호는 안랩 시큐리티대응센터(AhnLab Security Emergency response Center, 이하 ASEC)의 분석 자료를 토대로 2012년을 뒤흔들 악성코드 동향을 전했다. 스마트폰, 태블릿 PC의 증가로 인한 모바일 환경 변화를 강조하고, 이에 대한 보안 위협을 설명했다. ▲과금형 악성코드의 폭발적인 증가 ▲유명 애플리케이션인 ‘척’을 하는 허위(fake) 모바일 앱 ▲디지털 세계의 스토킨거 할 수 있는 사생활 침해형 애플리케이션 증가 ▲온라인 뱅킹 정보를 노리는 악성코드 급증 등이 그것이다. 이 밖에도 트로이목마의 고도화와 윈도우 취약점을 악용하는 악성코드에 대해 경고했다.



2012년 3월 안랩, 세계로 가다!

2012년은 대한민국 대표 보안 기업 안랩이 글로벌 기업들과의 본격적인 경쟁을 선언한 해이다. 그 첫 격전지는 세계 최대 규모의 정보보호 콘퍼런스인 ‘RSA 콘퍼런스 2012’였다. 예상을 뛰어넘는 미국 현지의 반응은 그동안 안랩이 세계 보안 시장 진출을 위해 꾸준히 준비해온 노력의 결과였다. 350여 개 글로벌 보안 기업들의 보이지 않는 치열한 경쟁과 그 속에서 ‘RSA 2012의 핫 벤더(hot vendor)’로 꼽힌 안랩의 모습이 월간 安 3월호에 고스란히 녹아 있다.



2012년 4월 컴플라이언스와 리스크 관리의 해법

월간 安 4월호는 APT 등 고도화된 위협을 비롯해 개인정보보호법 등 컴플라이언스 이슈 등 기업의 비즈니스 환경을 둘러싼 보안 위협을 해소할 수 있는 방법을 제시했다. 안랩의 융·복합 보안관제 서비스(Managed Security Service)가 그것이다. 특히 자체 통합보안관제센터를 갖추고 IT 전반 및 보안에 대한 깊은 지식을 갖춘 많은 인력을 상시 배치하기 어려운 일반 기업에서 안랩의 보안관제 서비스가 새롭게 각광받고 있다. 안랩의 관제 서비스는 24시간 365일 종합 모니터링을 통해 각 보안 솔루션에서 데이터를 수집하고, 이를 분석해서 공격의 실체를 파악한다. 이어 각 시스템과 서비스, 보안 인프라를 연동해 공격을 방어하고, 사후조치까지 연결되는 종합 대책을 제시한다.



2012년 5월 악성코드, 문서를 파고들다

불과 얼마 전까지만 해도 문서 파일에 악성코드가 있으리라는 것은 상상하기 어려운 일이었다. 그러나 올해는 운영체제와 관련된 보안 위협 못지 않게 문서 파일을 둘러싼 보안 위협이 자주 등장했다. 특히 올해 상반기부터 국내에서 문서 파일 등에 탑재된 비실행(non-PE) 악성코드 유포가 증가했다. 월간 安 5월호는 비실행 파일을 처리하는 과정에서 발생하는 응용 프로그램 취약점을 이용하는 악성코드 감염 사례를 다뤘다. 국내의 악성 비실행 악성코드 사례를 소개하고, 악의적인 비실행 파일이 전파 또는 기업 내부 네트워크로 유입되는 감염 경로와 기법을 설명했다.



2012년 6월 개인정보 보호에 대해 고민하는 이들에게 고함

2012년 기업 보안의 화두는 단연 '개인정보 보호'일 것이다. 안랩은 올해 월간 安을 통해 여러 차례 개인정보보호법, 정보통신망법을 다루며 개인정보 보호의 중요성을 강조하고 기업의 컴플라이언스 이슈 대응을 위한 조언을 제시했다. 특히 월간 安 6월호에서는 기업 내 직원들이 수행해야 할 컴플라이언스 준수 대책부터 기업의 개인정보 보호 담당자를 위한 상세한 가이드를 공유했다. 컴플라이언스 이슈 대응을 위한 필수 아이템으로는 ▲직원들의 PC에서 개인정보를 검색해 주는 톨 마련 ▲개인정보 파일을 완전 삭제하고 한꺼번에 패스워드를 설정해 주는 솔루션, 그리고 ▲부서별 또는 직원별 개인정보 관리 현황을 집계하고 통제할 수 있는 관리 솔루션 등을 꼽았다.



2012년 7월 드라마 '유령', 기업의 '악몽'을 그리다

올해 초, ASEC에 흥미로운 의뢰가 들어왔다. 사이버 범죄를 주제로 한 드라마의 자문역이다. SBS 드라마 '유령'은 독특한 소재와 긴박한 스토리 전개로 많은 관심을 모았다. 월간 安은 드라마에 등장한 사이버 공격 기술 중 현실 세계에 큰 위협이 될 수 있는 에피소드를 중심으로 개인과 기업의 안전을 위해 주의해야 할 사항을 짚어냈다.



2012년 8월

컨설팅, 보안을 디자인하다

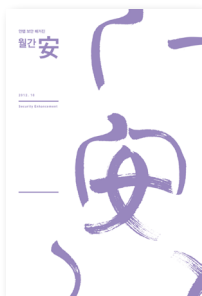
2012년은 기업의 IT 보안을 둘러싼 컴플라이언스 이슈가 증가함에 따라 보안 컨설팅에 대한 수요가 그 어느 때보다 높았던 해다. 그러나 복잡다단한 최신 기업 IT 시스템을 전체적으로 조망하여 실질적이고 효과적인 보안 체계를 구축하기 위해서는 검증된 컨설팅 능력은 물론, 비밀 유지 측면에서도 믿을 수 있는 업체를 찾아야만 한다. 월간 安 8월호는 보안 컨설팅 도입을 고려하는 기업이 꼭 따져보아야 하는 요소들을 상세하게 설명했다.



2012년 9월

맥(Mac)은 악성코드로부터 안전하다?

얼마 전만 해도 맥 OS는 비교적 악성코드의 위협으로부터 자유로운 것으로 여겨졌다. 그러나 그것은 희망사항에 불과했다. 맥 OS 사용자 수가 윈도우 OS 사용자 수를 바짝 추격하면서 악성코드 등을 비롯한 맥 OS의 보안 문제가 증가하고 있기 때문이다. 그럼에도 불구하고 여전히 많은 맥 사용자들은 안티바이러스 프로그램의 중요성을 느끼지 못하고 있다. 이에 안랩은 월간 安 9월호를 통해 맥 OS 보안 위협 사례를 설명하고 맥 OS 사용자들의 보안 인식 제고를 강조했다.



2012년 10월

고성능, 고가용성, 고효율성 관점의 Security Enhancement

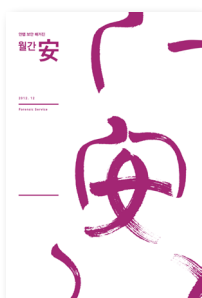
월간 安 10월호는 3부에 걸쳐 최근의 IT 패러다임 변화에 따라 기업에 요구되는 보안 대응 전략 강화를 상세하게 설명했다. ▲스마트폰, 태블릿 PC 등의 증가와 빅데이터 환경으로의 변화에 따른 기존 네트워크 보안 솔루션의 한계를 지적하고 ▲APT 공격 사전 대응과 관련한 악성코드 탐지 기법의 허와 실을 분석했으며 ▲나날이 지능화되고 있는 DDoS 공격 대응을 위한 차세대 보안 솔루션을 소개했다.



2012년 11월

BYOD, 이것만은 꼭!!

‘개인정보’ 못지 않게 올 한 해 기업 보안 담당자의 관심을 끈 키워드는 바로 BYOD, 즉 Bring Your Own Device다. 보안뿐만 아니라 최신 IT 동향을 전하는 월간 安은 2012년 11월호를 통해 올해의 키워드인 BYOD와 함께 기업의 모바일 보안 이슈를 구체적으로 설명했다. 특히 스마트폰이 각광받는 핵심인 편의성은 해치지 않으면서 기업의 정보 자산을 보호할 수 있는 방안은 무엇인지 BYOD 도입을 고려하고 있는 기업의 고민을 속 시원하게 풀어냈다.



2012년 12월

사후 대응을 넘어 사전 예방으로!

2012년을 마무리하는 월간 安 12월호는 최근 고도화되는 위협과 컴플라이언스 이슈 대비를 위한 새로운 대안으로 주목 받고 있는 사전 예방 관점의 포렌식 서비스를 상세하게 소개한다. 또한 지난 몇 달 사이에 잇달아 발생하고 있는 한글 파일 취약점 공격을 분석하고 기업의 보안 관리자 및 책임자들이 연말을 안전하게 마무리하기 위해 주의해야 할 점은 무엇인지 살펴본다.

APT부터 정보 유출 방지까지 사전 예방을 위한 포렌식 서비스

포렌식, 차세대 보안을 예고하다

“포렌식 서비스를 받아보는 것이 어떨까 합니다.”

대표적인 금융 기업 A사의 임원 회의는 CSO(최고보안책임자)의 발언으로 삼시간에 혼란에 휩싸였다.

“그게 무슨 소린가? 우리 회사가 해킹을 당했다는 말인가?”

A사는 막대한 예산을 들여 다양한 보안 솔루션을 도입했을 뿐만 아니라 컨설팅을 통해 빠진 부분을 점검하고 실질적인 보안 솔루션 운용을 위해 관제 서비스도 받고 있다. 그런데 갑자기 포렌식이라니. 당황한 임원들의 질문에 돌아온 CSO의 대답은 더욱 혼란스러운 것이었다.

“아닙니다. 그렇기 때문에 포렌식 서비스를 받아봐야 한다는 것입니다.”

해킹을 당한 것도 아니라면서 포렌식을 받아야 한다니, 이 무슨 이해 못할 소린가? ‘포렌식 서비스’란 건 또 뭔가? 뭇보다 해킹을 당한 것도 아닌데 그 ‘포렌식 서비스’라는 것을 받아야 하는 이유는 대체 무엇인가?

최근 기업 보안의 화두는 ‘APT(Advanced Persistent Threat)’와 ‘정보 유출’이다. 해외 APT 공격 사례로는 오퍼레이션 오로라, 스텝스넷, EMC RSA 침해사고 등을 들 수 있다. 대표적인 국내 APT 공격 사례로는 지난 2011년 4월 발생한 N사의 전산망 마비 사태가 있다. 당시 조사 결과에 따르면, 30분만에 N사의 서버 절반 이상을 파괴하는데 이용됐던 악성코드는 사건이 발생하기 7개월 전인 2010년 9월경부터 N사의 시스템 내부에 은닉하고 있었다. 국내외 APT 공격 사례를 살펴보면 한 가지 공통점을 발견할 수 있다. 공격에 사용된 악성코드가 평균 4개월 이상 타깃의 시스템 내부에 은닉하고 있었다는 점이다.

이처럼 시스템 내부에 장기간 은닉하여 정보를 유출하거나 시스템을 파괴하는 고도의 지능형 공격이 증가하면서 정확한 공격 발생 지점과 피해 규모를 파악하기 위해 정밀한 시스템 분석 기술, 포렌식에 대한 요구가 증가하고 있다. 개인정보보호법 등 컴플라이언스와 관련해서도 포렌식이 관심을 받고 있다. 포렌식 진단 기법을 활용해 USB 등 이동형 저장 장치는 물론, 각 클라이언트 PC나 데이터베이스 등에서의 개인정보 오·남용 여부와 개인정보 처리에 대한 확인이 가능하다는 것이 그 이유다.

왜 포렌식인가?

위키피디아(Wikipedia)는 ‘디지털 포렌식(Digital Forensics, 또는 포렌식)’에 대해 ‘디지털 정보를 저장하는 모든 단말기(device)의 정보(증거)를 복구하고 분석하는 과학 수사 기법의 일종’으로 설명하고 있다. 사이버 범죄 수사나 법적 증거를 찾기 위해 이용되는 기술 또는 방법을 의미하는 포렌식은 주로 경찰의 영역으로 인식되어 왔다.

하지만 민간 보안 분야에서도 위협 분석과 대응을 위해 포렌식의 기본적인 개념이나 기술이 활용되어 왔다. 다만 패턴 매칭이나 단순한 의심 정도를 판단하는 수준에서 포렌식 기술을 일부 활용했기 때문에 그 깊이가 깊지 않았을 뿐이다.

기존의 보안 솔루션이나 서비스는 ‘내부에 어떠한 위협이 있으니 어떻게 조치를 해야 한다’는 식의 가이드 정도가 대부분이었다. 실제로 해당 위협이 어떤 원인으로, 어떤 경로를 통해 내부로 유입됐는지, 또 그 위협으로 인해 어떤 보이지 않는 피해를 입었는지에 대해서는 기존의 방식으로 충분한 해답을 얻을 수 없었다. 게다가 고도화된 위협이 증가하면서 보다 정밀한 기술이 투영되어야 하는 상황을 맞이하게 됐다.

이에 IT 시스템을 정밀하게 살펴보고 그 안의 디지털 정보를 해부하여 실제 위협의 원인을 근본적으로 분석할 수 있는 기술인 포렌식이 새로운 대안으로 주목 받기 시작했다. ▲하드디스크, USB 등의 메모리 정보를 비롯해 ▲네트워크 트래픽 및 로그 ▲스마트폰 등 모바일 기기에 이르기까지 디지털 정보를 완벽하게 분해하여 사고(incident)에 대한 명확한 팩트(fact)를 찾아내고 정보에 대해 설명할 수 있는 유일한 기술이 바로 포렌식이기 때문이다.

과학수사는 CSI, 디지털 포렌식은 A-FIRST!

안랩은 지난 2011년 6월, 디지털 포렌식 전문조직인 A-FIRST(AhnLab Forensic & Incident Response Service Team)를 신설하고 본격적인 포렌식 서비스 제공에 나섰다. '포렌식 서비스'를 간단히 정의하면, 경찰이 수사의 목적으로 수행했던 디지털 포렌식을 민간 보안 업체가 민간 고객을 대상으로 서비스의 형태로 제공하는 것이다. 국내에서는 2011년부터 포렌식 서비스에 대한 관심이 나타나기 시작했고, 안랩은 축적해온 경험과 전문성을 기반으로 시장의 요구에 발 빠르게 대응할 수 있었다.

그동안 안랩은 여러 침해사고를 분석하면서 고도화된 위협을 효과적으로 예방하기 위한 방법을 꾸준히 모색해왔다. 아울러 수차례의 대규모 사이버 사건을 대응해온 경험을 바탕으로 연구한 결과 단순히 네트워크, 시스템 전문가뿐만이 아니라 악성코드와 바이너리 분석가, 커널 분석가 등 다양한 전문가 집단이 필요하다는 것을 확인했다.

A-FIRST는 모의해킹 전문가, 네트워크 전문가, 취약점 분석 전문가, 악성코드 분석 전문가, 커널 및 리버스 엔지니어링 전문가 등으로 구성되어 있다. 이들의 전문성을 기반으로 침해사고 대응은 물론, 전문적인 포렌식 기반의 고도화된 서비스를 제공한다.

대표적으로 ▲공격자의 타임 라인과 감염 경로를 추적할 수 있도록 해킹과 악성코드를 분석하고 ▲고객사 현장 지원과 사고 원인 분석 및 피해 조치, 결과 보고서 제공 등이 그것이다. 또한 ▲방화벽 로그, 서버 로그 등을 분석해 사고의 원인을 규명하고 ▲수사 등의 목적을 위한 증거 보존 및 데이터 복원 서비스를 제공한다. 최신 공격 기법에 대한 연구를 통해 ▲사이버 사고 대응 프로세스를 제시하고 ▲법적 대응을 위한 기술적 법적 자문 역할도 수행한다.



[그림 1] A-FIRST 분석실 내부

포렌식 서비스, 이럴 때 딱!

서비스 제공 초기에는 사이버 사고가 발생했을 때 기업·기관 고객에 급파돼 조기 수습으로 피해를 최소화하는 것이 A-FIRST의 주된 역할이었다. 그러나 그간의 경험을 통해 기업의 비용 절감을 위해서는 침해사고 발생 후 피해를 최소화하는 것보다 사전에 예방하는 것이 효과적이라는 결론에 도달했다. 이에 최근에는 고객사의 정보보호 조직과 협력해 전문화, 조직화하는 다양한 사이버 사고에 효과적·능동적으로 대비하는 고도화된 사전 예방 서비스까지 지원하고 있어 ▲APT 등 고도화된 공격 대응 및 피해 방지 ▲전체적인 보안 수준 강화 ▲중요 정보 유출 방지 등의 목적으로 이용할 수 있다.

첫째, 포렌식은 APT 대응 및 피해 방지에 필수적이다. APT 공격의 가장 큰 특징은 장기간 은닉하여 정보를 유출하거나 시스템을 파괴하는 등의 피해를 야기하는 것이다. 침해 사실을 미처 인지하지 못한 타깃의 내부에 위협 요소가 유입되어 오랜 시간에 걸쳐 악의적인 행위를 준비하거나 수행한다. 이 같은 APT 공격 대응의 관건은 실시간 가시성 확보다. 위협 요소가 유입되는 순간, 또는 위협이 확산되는 것을 방지하기 위해서는 시스템에 대한 실시간 가시성 확보가 반드시 필요하다. 포렌식은 서버 침해, 메모리 포렌식, 패킷 분석, 악성코드 및 네트워크 행위 분석 등 다양한 기술을 통해 데이터의 흐름을 파악하고 실시간 가시성을 확보할 수 있다. 특히 각 클라이언트 PC부터 IT 시스템 전체에 대한 정밀한 분석을 통해 침해가 시작된 지점부터 실제로 피해가 발생한 지점, 그리고 정확한 피해 규모까지 파악이 가능하다.

둘째, 포렌식을 통해 전체적인 보안 수준 강화를 꾀할 수 있다. 컨설팅과 관제를 통해 솔루션을 도입하고 적절한 보안 인프라를 기 구축한 고객들을 중심으로 추가적으로 도입할 수 있는 것, 또는 추가적으로 점검할 수 있는 방법에 대한 문의가 이어지고 있다. 지금까지의 포렌식이 주로 침해사고가 발생한 후 사고의 원인을 찾거나 피해를 최소화하기 위한 소극적인 의미의 활용이었다면, 최근에는 보다 능동적이고 사전 예방적인 차원에서의 포렌식 도입을 고려하는 추세라 할 수 있다.

셋째, 중요 정보 유출 방지를 위해 포렌식을 이용할 수 있다. 포렌식 기술을 이용해 삭제된 증거, 외부 저장장치의 활용, 악의적 이용에 대한 증거 및 관련자와의 공모 행위 등을 모두 추적해낼 수 있다. 특히 단순히 시스템 내에서의 정보의 흐름만을 분석하는 것이 아니라 사용자의 행위를 포렌식으로 함께 풀어낸다면 사전에 정보 유출 행위를 감지하고 이를 방지할 수 있다. 이러한 측면에서 개인정보보호법 등 기업의 컴플라이

언스 이슈와 관련해 포렌식을 활용할 수 있다. 포렌식 기술을 이용해 PC의 개인정보 보유 현황을 세세하게 파악할 수 있으며 기업 내부에서 개인정보가 유통되는 흐름을 파악하고 점검할 수 있다.

포렌식 기술로 무장한 고도화된 전문 서비스

A-FIRST는 포렌식 기술을 기반으로 보안 진단, 침해 분석/대응, 정보 감사 등 세 가지 영역의 고도화된 전문 서비스를 제공하고 있다.

1. 보안 진단

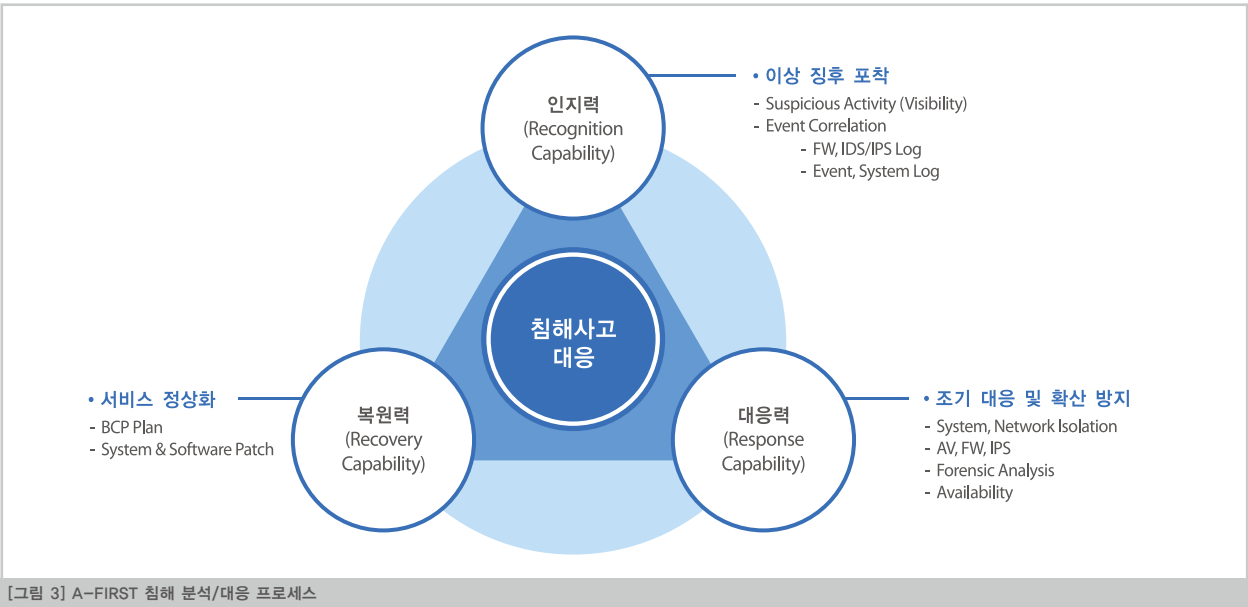
보안 진단이란 시스템이나 보안 수준을 평가 또는 확인하고 싶은 고객을 위한 서비스로, 관리적·기술적·물리적 보안뿐만 아니라 침해사고 영향 평가 등을 제공한다. 주요 진단 항목은 ▲의심 이벤트 정보 확인 ▲의심 파일 확인 ▲악성코드 감염 이력 ▲유해 사이트 접근 이력 ▲외부 저장 장치 사용 이력 ▲개인정보 파일 보유 및 관리 등이다.

침해사고 영향 평가, 시스템 안전성 평가는 기존에 볼 수 없었던 보안 진단 서비스로, 기업 내부의 모든 PC를 분석해 악성코드에 감염된 이력이 있는지, 메모리 포렌식 등을 진행하는 차별적인 서비스다. 이력만 파악하는 것이 아니라 그 동안 미처 인지하지 못했던 정보 유출, 내부 위협 확산 등 고객이 궁금해하는 실제 피해를 확인한다. 그 이력으로 어떤 변화가 유발됐는지, 그것으로 앞으로 어떤 일이 있을 수 있는 지까지 상세하게 분석하여 실제 리스크를 꼼꼼하게 점검한다.



2. 침해 분석/대응

침해분석/대응 서비스는 현재 발생한 침해사고에 대한 대응을 원하는 고객을 위한 서비스로, 기업의 보안 담당자들이 분석하기 어려운 시스템 및 네트워크에 대한 가시성을 확보하고 위협을 제거하는 서비스다. 침해사고 대응을 위해서는 이상 징후를 포착하는 인지력이 중요하며, 조기 대응 및 확산을 방지할 수 있는 대응력이 필요하다. 또한 피해를 복구할 수 있는 역량도 요구된다.



3. 정보 감사

정보 감사 서비스는 '정보 감사'를 원하는 고객을 지원하는 서비스로, 기업 기밀 유출의 경로를 파악하거나 사내 불법 행위를 탐지한다. ▲소스 코드 및 문서 목록 ▲외부 이메일 사용 기록 ▲웹 사용 기록 ▲USB 사용 기록 등이 주요 감사 항목이다.

최근 기밀 정보 유출이나 내부자에 의한 정보 유출이 증가하고 있어 기업의 정보 자산이 외부로 나간 적이 있는지 확인하고자 하는 기업이 늘고 있다. 포렌식은 디지털 정보 안에서 모든 것을 꼬집어내서 고객이 원하는 모든 정보를 제공하고 설명할 수 있다. 지금까지는 전문가를 이용한 시장이 크지 않았지만 법률 시장 개방과 함께 소송 사례가 많아지고 있기 때문에 이에 미리 준비할 수 있는 대책으로서의 정기적인 보안 감사 활동도 이어질 것으로 보인다.

포렌식도 안랩이 하면 다르다!

안랩 포렌식 서비스의 차별점은 바로 악성코드 분석 능력이다. 침해사고는 악성코드와 연관된 경우가 대부분이다. 고도화되고 지능적인 공격도 시작은 악성코드다. 따라서 악성코드에 대한 분석 능력이 있어야만 사건을 효과적으로 분석해낼 수 있다. 그러나 포렌식 서비스를 운영하는 대부분의 업체에서는 악성코드 분석 능력을 갖추지 못한 경우가 많아 침해사고와 특정 악성코드의 연관성을 파악하기가 어렵다.

안랩은 국내 최고의 악성코드 분석 전문 조직인 ASEC(안랩 시큐리티대응센터)을 보유하고 있기 때문에 차별적인 포렌식 서비스 제공이 가능하다. 특히 클라우드 기반의 자동화된 악성코드 분석 시스템인 ASD(AhnLab Smart Defense)의 행위 분석 기능을 통해 실시간 악성코드 분석 및 가시성 확보가 가능하다.

포렌식 전문가는 기본적으로 시스템, 메모리 관점에서 IT를 구성하고 있는 모든 역량을 갖추고 있어야만 한다. 하나의 PC 안에 디지털 정보는 수백만 개 이상이 존재하기 때문에 사람이 일일이 본다는 것은 불가능하다. 대용량 정보를 분석할 수 있는 툴, 기술, 전문성이 있어야 한다.

A-FIRST에는 IT 분야 전반에 대한 경험과 역량을 갖추고 있는 전문가들이 모두 모여 있다. 타 업체의 경우 보통 네트워크나 관제 등 일부 영역에 대해서만 특화된 조직을 갖고 있다. 이에 반해 A-FIRST는 각 분야별 전문가들이 한 데 모여 있어 전체적인 시각에서 사건을 들여다보기 때문에 차별적인 인사이트 확보가 가능하다. 또한 기업의 관리적·물리적인 취약성을 진단하는 서비스는 많지만, 기업 내 각 PC 자체가 어떤 위협에 노출되어 있는지, 악성코드에 감염된 적은 있는지, 또 악성코드 감염 등을 통해 정보 유출이 이루어졌는지를 진단하는 서비스는 A-FIRST 외에 찾아보기 어렵다.

물론, 악성코드를 이용한 공격 외에 정상적인 원격 접속 툴이나, 예약 스케줄 등의 명령어를 이용한 정상적인 경로를 통해서 공격이 발생하는 경우도 있다. 따라서 악성코드 분석 외에도 정상적인 명령 실행의 타임라인(timeline) 분석을 통해 위협 발생의 징후를 포착할 수 있어야 한다. 이것이 바로 분석가의 뛰어난 역량이 요구되는 이유다. 안랩의 포렌식 전문가들은 파일의 행위를 해석해 낼 수 있는 전문성과 숙련도를 보유하고 있다.

A-FIRST, 포렌식 서비스의 진화를 꾀하다

지금까지의 포렌식은 침해사고의 피해를 최소화하기 위한 사후 대응 중심이었다. 그러나 안랩은 A-FIRST를 통해 침해사고 대응뿐만 아니라 사전 예방 관점의 포렌식 서비스를 확대해 나가고 있다.

대표적으로 '침해 보안 영향도 진단 서비스'가 있다. 기업이 정기적으로 주요 시스템에 대해서 침해 영향도 진단을 받아봄으로써 실제 발생할 수 있는 위협들이 있었는지, 위협들로 인해 실제적인 피해를 입었었는지, 혹은 미처 인지하지 못했던 피해까지 정기적으로 진단하는 것이다. 단순히 포렌식 서비스를 통한 악성코드 발견에서 그치는 것이 아니라 그 악성코드 위협이 실제 시스템에 어떤 영향을 주었는지를 '침해 위험도'를 기준으로 진단함으로써 기업의 사전 예방 활동이 가능하다.

이 밖에도 안랩은 사전 예방 관점의 다양한 포렌식 서비스 모델을 연구·개발해 고객이 실제로 필요로 하는 전문화된 최고급 보안 서비스를 제공할 계획이다.

안랩 포렌식 전문 조직 A-FIRST 김지훈 팀장

“사후 대응을 넘어 사전 예방의 키워드 될 것”

포렌식(Forensics)이라고 하면 해킹 등 침해사고가 발생했을 때 피해를 최소화하기 위한 분석 작업으로 인식되어 왔다. 그러나 그것은 포렌식 활용의 기초적인 수준에 불과하다는 것이 안랩 포렌식 조직 A-FIRST 김지훈 팀장의 지적이다. “침해사고의 피해 최소화를 위한 사후 대응뿐만 아니라 기업의 리스크 관리를 위한 사전 예방까지 포렌식을 다각도에서 적극적으로 활용할 필요가 있다”고 김지훈 팀장은 강조했다.

ISP 업체부터 호스팅센터(IDC)까지 대한민국 IT 환경의 진화를 현장에서 겪어온 김지훈 팀장은 지난 2003년 1.25 대란을 계기로 보안 분야에 뛰어들었다. 악성코드 분석부터 네트워크 취약점 분석, 그리고 포렌식 기술과 노하우를 바탕으로 안랩의 포렌식 전문 조직 A-FIRST를 이끌고 있다. 최근 기업을 둘러싼 고도화된 위협과 구체적인 포렌식 서비스의 활용 방안에 대한 그의 조언을 들어본다.

“디지털 증거를 얼마나 보존하고
관리할 수 있는지가 기업의 보안과
비즈니스의 관건”

A-FIRST 김지훈 팀장



A-FIRST란 무엇인가?

A-FIRST는 AhnLab Forensic & Incident Response Service Team의 약자로, 안랩의 포렌식 전문 조직이다. A-FIRST는 침해사고에 대한 사후 대응뿐만 아니라 고도화된 위협에 대비하기 위한 사전 대응까지 아우르는 포렌식 서비스를 제공하고 있다.

본래 A-FIRST는 기업의 침해사고 발생 시 긴급한 대응을 지원하기 위한 포렌식 서비스 조직이었다. 그런데 지난 1년여 간 여러 고객사의 침해사고 대응 서비스를 수행하면서 한 가지 공통점을 발견했다. 기업들이 보안 강화를 위해 많은 노력을 기울이기는 하지만 그 과정에서 미처 발견하지 못한 부분이 사후 침해로 이어져 결국에는 막대한 피해를 입는 경우가 대부분이라는 점이다. 이에 안랩은 A-FIRST를 통해 침해사고의 피해를 최소화하는 사후 대응뿐만 아니라 사전 예방을 위한 서비스까지 포렌식의 영역을 확대하고 있다.

A-FIRST의 서비스는 어떤 과정으로 진행되나?

먼저 고객과의 인터뷰를 통해 고객의 요구를 어떻게 지원할 수 있을지 협의하고 프로젝트의 목표를 정한다. 포렌식 서비스는 정밀 분석과 피해 최소화 목적에서 시작하는 만큼 단기간 내에 완료해야만 하는 서비스다. 따라서 뚜렷하고 구체적인 프로젝트 목표 설정이 최우선이다. 감염 경로 확인, 또는 정보 유출 발생 여부 확인 등 명확한 목표를 정하고 단기간 내에 집중적으로 진행된다. 설정된 목표에 따라 기업의 네트워크 시스템부터 모든 클라이언트 PC까지 포렌식 범위를 정하고 그에 따른 전문적이고 세밀한 기술을 통해 포렌식을 수행한다.

포렌식 서비스는 관제나 컨설팅 등 기존의 보안 서비스와는 무엇이, 어떻게 다른가?

결론부터 말하자면 관제와 컨설팅, 포렌식은 단계별로 이어지는 보안 서비스이다. 컨설팅은 기업 보안의 토대(base)를 다지는 것이다. 기본적인 보안 수준이 마련되어 있지 않으면 고도화된 포렌식 기술을 쓴다한들 아무런 도움이 되지 않는다. 위협이 유입될 수 있는 경로가 많으면 일시적인 조치로 급한 불만 끄는 격일 뿐, 근본적인 원인 해결은 불가능하다. 실제로 포렌식 서비스를 의뢰한 고객에게 컨설팅부터 받아야 한다고 조언하는 일이 종종 있다.

컨설팅을 통해 기본적인 틀을 확립하고 나면 관제를 통해 알려져 있는 보안 위협에 대해 지속적으로 경계하고 내부 시스템을 모니터링함으로써 인사이트(Insight)를 확보할 수 있다. 그러나 비용과 우선 순위를 고려해야 하는 기업의 입장에서는 기업의 IT 시스템 전체에 대한 관제를 수행한다는 것은 현실적으로 불가능하다. 관제는 정해 놓은 부분에 대해 이벤트를 정의해놓고 그에 대한 대응 및 모니터링을 수행하는 것이기 때문에 정해진 관제 범위를 벗어난 부분에서 발생하는 위협을 파악하는데 어려움이 있다.

문제는, 예측한 범위를 우회하는 위협들이 존재하기 마련이며, 그 위협들이 유입될 수 밖에 없다는 것이다. 포렌식이 필요한 이유는 현재의 보안 수준과 체계를 벗어난 위협이 발생할 경우 이에 대응할 수 있는 무언가가 필요하기 때문이다. 포렌식 서비스는 기존에 보호하지 않고 있던, 또는 보호의 우선 순위에서 제외해 두었던 영역까지 추가적인 검토와 가이드를 할 수 있다.

컨설팅이나 관제 서비스를 비롯해 기존의 보안 솔루션들이 기업의 보안 수준을 향상시키는 훌륭한 툴임은 분명하다. 그러나 우리는 그 동안의 경험을 통해 공격이 항상 예측할 수 있는 범위 내에서 발생하는 것이 아니라는 것을 알고 있다. 기존에 마련해둔 보안 대응 수준을 넘어서는 위협, 알려지지 않은 방식에 대해서 분석하고 정보를 얻기 위해서는 포렌식 서비스가 필요하다.

주로 어떤 고객들이 A-FIRST의 포렌식 서비스를 찾는가?

주요 시스템에 대한 상시적인 보안 진단과 실질적인 침해 영향도 분석을 받고 싶을 때 포렌식 서비스를 이용한다. 주로 관리 범위가 넓은 대기업에서 포렌식 서비스를 의뢰하고 있다.

분야별로는 게임사나 금융사가 주를 이룬다. 게임 시장은 공격자들에게 가장 매력적인(?) 분야다. 게임 계정 탈취의 목적뿐만 아니라 게임 머니 등 금전적인 활동이 발생하기 때문에 끊임없이 공격자들에게 시달린다. 게임사는 다양한 솔루션과 고도의 관제 서비스를 도입하는 한편, 현재의 보안 체계 범위 밖의 해결되지 않은 부분에 대해 분석을 요청하는 경우가 대부분이다. 금융 분야는 비즈니스 자체가 금전적인 것과 연결되어 있는 만큼, 정밀한 분석



A-FIRST의 경쟁력을 꼽는다면?

포렌식 서비스를 수행하는데 있어 어려운 점이 있다면?

을 통해 추가적으로 내부 시스템과 위협 요소를 확인하고자 하는 목적으로 포렌식 서비스를 찾고 있다.

이 밖에도 일말의 불안도 해소하고 싶은 기업이나 메인 사업 외의 위탁 또는 관리하고 있는 사업장에서 발생할 수 있는 위협을 방지하고 싶은 사업체에서 포렌식 서비스를 찾고 있다.

한 마디로 '기술력'이다. 모든 제품이나 서비스에서도 기술력이 핵심이지만 포렌식 분야는 전문가의 기술 숙련도에 따라 기술을 활용하는 방식, 적용하는 범위가 천차만별이기 때문에 사건 해결 능력 자체가 확연히 달라진다. 다양한 침해사고 분석 경험과 기술을 기반으로 효율적이고 체계적인 분석 방법론, 빅데이터를 분석해낼 수 있는 툴도 보유하고 있어야 한다.

또한 포렌식의 핵심은 타임라인이다. 하나의 사건을 조사할 때 타임라인을 살펴 의심스러운 부분이나 행위를 찾아내는 방법론의 효율성은 얼마나 뛰어난 기술력을 보유하고 있는냐가 관건이다. 이런 면에서 안랩의 포렌식 서비스 A-FIRST는 단연 독보적이라 할 수 있다. 안랩의 포렌식 전문가들은 탁월한 기술력과 전문성을 기반으로 독자적인 툴까지 보유하고 있다.

A-FIRST의 전문가들을 뒷받침하는 안랩의 인프라 또한 차별성을 자랑한다. 안랩은 막대한 악성코드 분석 DB와 콘텐츠를 보유하고 있으며, 조직적인 면에서도 관제 조직과 CERT(침해사고대응팀)를 모두 보유하고 있어 다양한 보안 위협에 즉각적이고 효율적인 대응이 가능하다.

포렌식 서비스는 관제나 컨설팅 서비스와 달리 단기간 내에 결과를 내야만 한다. 하지만 빅데이터 시대의 수많은 정보와 고객사에서 벌어진 모든 일을 짧은 시간 내에 파악한다는 것은 결코 쉽지 않다. 장기간에 걸쳐 세밀하게 벌어진 공격 과정을 짧은 기간 안에 모두 재구성해서 고객과 우리 자신이 납득할 수 있는 상황을 만들어야 하기 때문에 상당한 노력과 고도의 집중을 요하는 경우가 대부분이다. 또한 디지털 정보에 남은 흔적은 시간이 지나면 지워지기 때문에 그 부분을 예측으로 채워야 하는 경우도 있다. 이미 지워진 정보로는 완벽한 퍼즐을 완성할 수 없기 때문에 그런 경우에는 사건이 해결되어도 안타깝고 아쉬움이 남는다.

포렌식 서비스를 수행하기 전부터 어려움을 겪는 경우도 있다. 침해사고에 대한 포렌식 서비스를 수행해야 하는 경우가 그것이다. 침해사고에 대한 포렌식을 진행할 때는 고객사의 침묵하고 심각한 분위기 속에서 작업을 하게 된다. 서비스를 요청하는 고객이 기대나 희망에 찬 분위기로 우리를 맞아주기 보다는 긴장하고 위축된 분위기에서 작업을 해야 하기 때문에 작업에 착수하기 전부터 어려움이 많다. 그러다 보니 가끔 우리 스스로를 '상조회' 같다고 느끼기도 한다. 또는 영화 '맨인블랙(Man in Black)'의 요원들 같다고 생각한다. 우리는 우리가 고객사를 방문했다는 것 자체를 드러내지 않는다. 고객사는 외부뿐만 아니라 내부 직원들에게도 침해사고로 포렌식을 받았다는 것을 결코 알리고 싶어하지 않기 때문이다.

A-FIRST의 향후 비전이 궁금하다.

포렌식 서비스를 원하는 고객에게 당부하고 싶은 말이 있다면?

고도화되는 위협에 대응하기 위해 고심하는 기업의 보안 관리자들에게 조언을 준다면?

오늘날 대부분의 기업 비즈니스가 IT 시스템을 기반으로 이루어지고 있다. 때문에 IT 시스템에 문제가 생길 경우, 비즈니스 연속성의 문제뿐만 아니라 법적 소송으로 이어져 기업의 평판 자체에 막대한 영향을 끼칠 수 있다. 최근 개인정보 유출에 따른 손해배상청구 등이 그 조짐이다. 이제는 디지털 증거를 얼마나 보존하고 관리할 수 있는지가 기업의 보안과 비즈니스의 관건이다. 이러한 관점에서 디지털 포렌식은 차세대 기술이자 서비스라 해도 과언이 아니다.

아직까지 고객들은 주로 침해사고와 관련해 A-FIRST의 서비스를 찾고 있다. 그러나 앞으로는 기업의 보안 진단 및 정보 감사 등 사전 예방으로서의 활용이 늘어날 것으로 보인다. 특히 점점 내부자에 의해 기업 기밀 정보가 유출되는 것이 늘어날 것으로 예측돼 단순히 정보 유출 방지 솔루션으로만 대응하기 보다는 전문가 서비스가 접목된 서비스 시장에 대한 요구가 높아질 것이다.

이에 안랩은 솔루션과 전문가 서비스의 접목으로 시장을 리드할 계획이다. A-FIRST의 역할은 그 과정에서 포렌식 기술을 기존 솔루션과 보안 체계와 연계하여 더욱 진화하고 효과적으로 위협에 대응할 수 있는 토대를 만들어 나가는 것이다. 동시에 기존의 보안 서비스보다 상위 개념의 서비스, 고품질 서비스로 고객들의 실질적인 리스크 관리에 도움이 될 수 있는 방향으로 시장에 접근하고 있다.

최근에는 고객사에서 내부의 정보를 외부에 공개한다는 불편한 인식보다는 개방적인 태도로 협력 대응을 위해 노력하는 모습이 많이 나타나고 있어 다행스럽게 생각한다. 한 가지 고객들에게 바라는 점이 있다면 침해사고가 발생한 후에 A-FIRST를 찾기 보다는 사전에 고객 시스템의 위험 요소를 정밀하게 진단하기 위해 서비스를 활용했으면 한다. 기존에는 많은 고객들이 피해가 발생한 후 더 이상 내부적으로 손 쓸 수 없을 때 A-FIRST를 찾았다. 그러나 사전 예방 활동이 고도화되지 않는다면 나날이 고도화되는 위협을 제대로 막을 수 없다. 사후 피해 수습에만 급급하면 고도화된 위협에 대응하기는 점점 더 어려워질 것이다.

고객사와 유기적인 협력을 통해 불가능해 보이는 디지털 정보 분석과 파악을 가능하게 하는 것이 바로 A-FIRST의 역할이다. 침해사고 시에만 포렌식이 필요하다는 선입견에서 벗어나 사전에 피해를 예방할 수 있도록 기업과 A-FIRST의 협력 모델로 더욱 고도화된 보안 체계를 만들어 갈 수 있기를 고대한다.

안전하다고 믿고 있는 시스템이 알고 보면 미세한 틈을 내포하고 있을 가능성이 높다. 실제로 A-FIRST를 찾는 고객들 중에는 최고의 보안 수준을 자랑하고 있는 고객들도 많다. 문제는 발생하고 있는 위협을 사전에 판단할 수 있는 전문성을 일반 기업에서 보유하기는 어렵다는 점이다.

따라서 새로운 솔루션을 도입하기에 앞서 기존에 구축해놓은 보안 시스템을 토대로 사전에 위협을 인지할 수 있는 방법을 찾는 것이 필요하다. 융·복합 관제와 같이 보안 솔루션에서 발생하는 다양한 이벤트를 한 곳에 집중시켜 이벤트간의 상관 분석을 수행할 수 있는 체계를 구축하는 것도 방법이 될 수 있다.

APT와 같이 고도화된 공격에 대응하기 위해서는 기업 시스템 전체에 대한 실시간 가시성 확보가 필요하다. 그러나 기존과 같은 로그 기반만으로는 실시간 가시성을 확보하기 어렵다. 실시간 가시성 확보를 위해서는 시스템 안에서 움직이는 정보에 대해 일거수일투족을 놓치지 않고 파악할 수 있어야 하기 때문이다. 시스템 및 네트워크에서 발생하는 행위에 대해 효과적으로 모니터링 할 수 있는 사전 모니터링 툴을 도입하는 것도 고려해 볼만 하다.

무엇보다 위협에 대한 탐지에서 한 발 나아가 실제적인 공격 시나리오를 예측할 수 있어야 고도화된 위협에 효율적인 대처가 가능할 것이다. 그러나 일반 기업에서는 이러한 부분을 해결할 수 없기 때문에 A-FIRST가 존재하는 것이다. 전문가 서비스를 통해 시스템을 진단하고 향후의 보안 체계를 어떻게 가져가야 하는지 구체적인 의견을 제시하는 것이 바로 안랩의 포렌식 서비스 A-FIRST의 역할이다.

기업 보안의 미래 트렌드가 될 안랩의 차세대 보안관제를 주목하라

안랩이 주요 고객사를 대상으로 차세대 보안관제 서비스를 소개하는 자리를 마련했다. 안랩은 지난 11월27일 오후 서울 서초구 양재동 엘타워 8층 엘하우스홀에서 '안랩 보안관제 리더십 포럼 2012'를 개최했다. 이 행사에는 안랩의 보안관제 서비스를 이용하고 있는 고객 100여 명이 참석해 차세대 보안관제 서비스에 대한 높은 관심을 입증했다.



▲ 안병규 안랩 서비스사업본부 이사

안병규 안랩 서비스사업본부 이사는 행사에 앞서 인사말을 통해 “보안은 비용 개념이 아닌, 기업의 이익을 창출하는 인프라 투자로 봐야 한다”며 “각 기업의 보안담당자는 급변하는 보안 트렌드를 빠르게 체득해야 한다”고 말했다.

이어 안 이사는 “오늘 이 포럼이 기업의 리스크를 줄이고 관리의 의무를 다하는 데에 도움이 되는 자리가 되길 바란다”고 말했다.

이번 포럼에서는 모두 세 가지 주제로 발표가 진행됐다. 이는 ▲APT 대응을 위한 차세대 보안관제 전략 ▲차세대 방화벽을 이용한 네트워크 보안 전략 ▲개인정보 보호를 위한 기술적 방어 전략 등이다.

“APT 대응? 차세대 보안관제가 해답”

곽희선 안랩 책임연구원은 발표를 통해 APT(Advanced Persistent Threat)와 같이 고도화된 사이버 공격이 날로 증가하고 있어 이를 대비하기 위한 보안 체계가 긴요하다는 점을 강조했다.

일부 원격 보안관제의 경우 “보안 위협이 전문화·정교화 되고 있어 ‘인터넷 점점 위주의 탐지’는 한계가 있다”고 말했다. 또한 시스템이 복잡하며 관리해야 하는 보안 솔루션도 적지 않다는 지적이다.

곽 책임연구원은 이에 반해 안랩의 경우 ASD 등을 이용한 악성코드 다운로드 모니터링을 비롯해 APT 공격 시나리오를 사전 예측 및 대응, 안랩의 APT 대응솔루션 AhnLab TrusWatcher와의 연계, 행위기반 분석과 동적 콘텐츠 분석이 가능하다고 밝혔다.



▲ 지난 11월 27일 서울 서초구 양재동 엘타워 8층에서 열린 '안랩 보안관계 리더십 포럼 2012' 현장

“차세대 방화벽, 앱 정책 수립 용이”

정진교 안랩 솔루션서비스팀 부장은 엔터프라이즈 2.0 시대로 접어들면서 인터넷 애플리케이션에 대한 사용이 폭발적으로 늘어나고 있으나 이에 대한 관리나 현황파악은 어려운 실정이라고 지적했다.

정 부장은 “최근 발견되는 보안 위협은 인터넷 애플리케이션에 존재하는 취약점을 악용하는 추세”라며 “대부분의 기업들이 IPS, URL 필터링 솔루션을 보유하고 있어도 효과적으로 관리하지 못해 애플리케이션이 악성코드의 전파나 내부 정보 유출의 경로로 이용되고 있다”고 말했다.

그러면서 정 부장은 최근 안랩과 엔터프라이즈 플래티넘 파트너십을 체결한 글로벌 방화벽 솔루션 기업 ‘팔로알토네트웍스’의 차세대 방화벽을 소개했다. 그는 “팔로알토네트웍스는 전세계 1500여 개 애플리케이션에 대해 가시성을 제공한다”며 “사용자 기반의 정교한 애플리케이션 제어 정책 수립이 가능하다”고 밝혔다.

개인정보보호에 대한 기술적 방어는?

김행수 소프트웨어개발실 책임연구원은 개인정보보호법의 주요 내용을 개괄적으로 소개했다. 그는 기업들이 개인정보보호법을 준수하기 위해서는 “기술적으로 다양한 솔루션과 제품, 관리가 필수적이다”고 주장하며 원활한 정보보호를 위해서는 “정보유통에 대한 ‘라이프 사이클’ 자체를 관리해야 한다”고 강조했다. 김 책임연구원은 ‘개인정보 라이프 사이클(Life Cycle) 방어 시스템’은 검색과 처리, 유출방지, 통합관리 등의 역할을 수행해야 한다고 지적했다.

이어 안랩 프라이버시 매니지먼트(AhnLab Privacy Management)는 백신과 패치, 개인정보 통합관리는 물론, 뉴런검색 등 지능화 검색 등이 가능하다고 소개했다.

한편 올해 안랩의 보안관계 서비스 사업은 11월 현재까지 금융 기업 5곳에 대한 융합관계 서비스 및 융합관계센터 시스템 구축 고객으로 확보하는 등 작년 대비 50% 이상의 성장을 기록했다.

그 저력은 안랩의 보안관계 서비스가 ▲이벤트가 아닌 시나리오(책·행위) 중심으로 분석하고 ▲내·외부 통합 보안관계 프로세스를 운영하며 ▲신종 악성코드의 실시간 발생·확산, 유포지 정보를 제공하고 ▲알려지지 않은 공격까지 탐지·대응하며 ▲내부 위협 요소까지 분석·대응한다는 점에서 다른 보안관계 서비스와 차별되기 때문으로 파악된다.

안랩은 올해 금융권과 엔터프라이즈 고객을 확보한 데에 힘입어 내년에 이 분야에 공급을 확대하고 공공 부문에서 신규 고객을 확보할 계획이다.

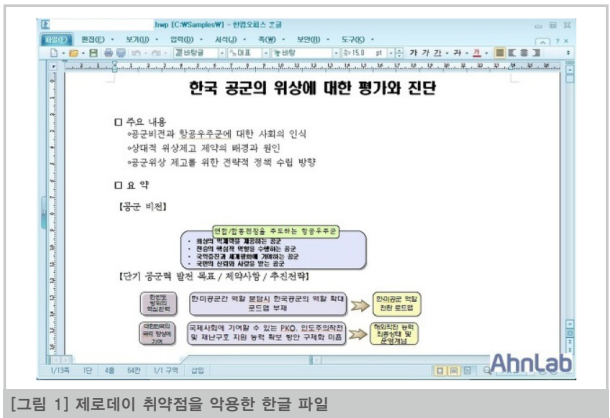
한글 파일 악용한 공격 잇따라... 기업·기관 ‘주의보’

어느 날 당신에게 ‘연봉협상 통지서’나 ‘인사평가보고서’ 문서가 날아든다면?
게다가 이 문서가 본인이 아는 지인이 보낸 것으로 위장을 했다면?
사회공학적인 공격 기법이 최근 기승을 부리면서 각종 문서 파일에 대한 경계 수위도 날이 갈수록 높아 지고 있다. 특히 국내에서는 최근 ‘한글과컴퓨터’의 ‘한글 파일’을 이용한 공격이 늘고 있어 적잖은 공공기관과 기업들이 긴장하고 있다.

국내에서 한글 파일을 이용한 공격이 급격히 증가한 것은 정부기관과 각종 공기업 및 일반 기업, 언론사 등 사용처가 많기 때문인 것으로 분석된다. 공격자들이 국내 실정에 맞는 ‘맞춤형 공격’을 감행하면서 국지화, 지능화된 공격 기법을 사용하고 있는 것이다. 이에 한글 파일을 악용한 최근 공격 사례를 살펴보고자 한다.

한글 파일 제로데이 공격 발견

지난 11월26일 국방 관련 내용의 제로데이 취약점을 악용한 한글 파일이 발견됐다.



[그림 1] 제로데이 취약점을 악용한 한글 파일

해당 파일은 ‘한국 공군의 위상에 대한 평가와 진단’이라는 문서 내용을 담은 채로 유포됐다. 파일의 타깃은 아직 명확히 밝혀지지 않았으나 안랩 시큐리티대응센터(이하 ASEC)에 따르면 11월21~22일 사이 정부기관을 상대로 유포된 것으로 추정되고 있다.

이 파일에는 [그림 1]과 같이 ‘공군비전과 항공우주군에 대한 사회의 인식’ 등 일반인들로 하여금 국방에 관한 중요 문서인 것처럼 인식하게 하는 내용이 비교적 상세히 기술돼 있다. 공격자가 타깃을 고려해 지능적으로 접근했음을 알 수 있는 대목이다.

파일에 포함된 악성파일의 동작 방식을 살펴보면, 한글과컴퓨터에서 제공하는 최신 보안 패치가 모두 적용된 ‘한글2010’이 설치된 시스템에서 열 경우 아래에 적힌 경로에 ‘HncCtrl.exe(139,264바이트)’ 파일을 생성한다.

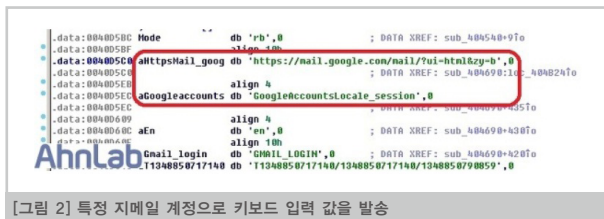
C:\Documents and Settings\[사용자 계정명]\Local Settings\Temp\HncCtrl.exe

또한 생성된 ‘HncCtrl.exe(139,264바이트)’ 파일은 아래 경로에 추가로 ‘sens.dll(36,864바이트)’과 ‘taskmgr.exe(61,440바이트)’를 만든다.

C:\WINDOWS\system32\IE\sens.dll
C:\WINDOWS\system32\taskmgr.exe

먼저 ‘sens.dll(36,864바이트)’은 윈도우 시스템에 존재하는 정상 ‘svchost.exe’ 프로세스에 스레드(Thread)로 인젝션 시킨 후 감염된 시스템에서 사용자가 입력하는 모든 키보드 입력 값을 ‘report.tmp’에 기록한다.

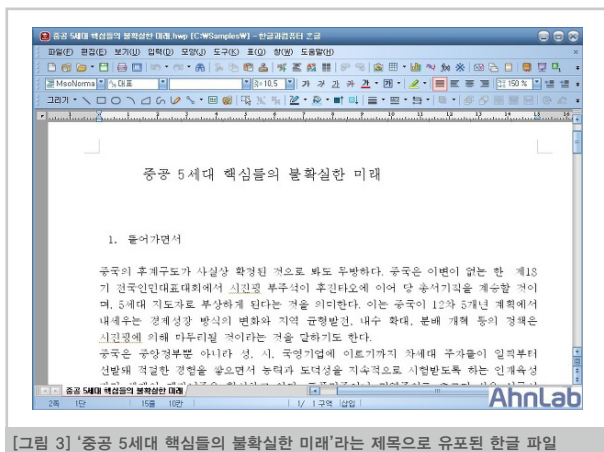
‘taskmgr.exe(61,440바이트)’는 감염된 시스템이 인터넷 접속이 가능한지 여부를 확인하기 위해 구글(Google) 웹사이트로의 접속을 시도한다. 만약 구글 접속이 성공하면 특정 이메일 계정으로 키보드 입력 값들이 기록된 ‘report.tmp’를 첨부([그림 2])해 발송한다.



이와 관련된 패치는 11월 말 기준, 아직 배포되지 않았다. 이에 ASEC에서는 이메일에 첨부된 한글 파일을 실행할 시에 각별한 주의를 당부했다.

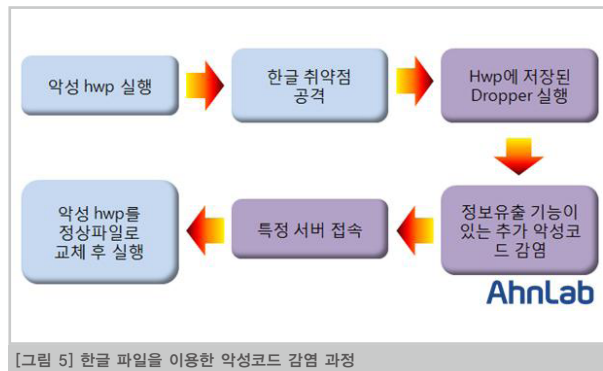
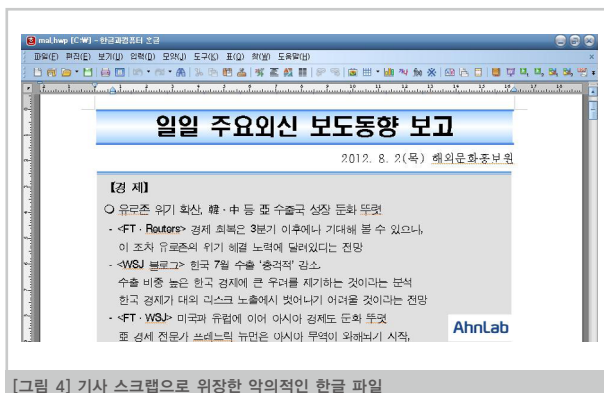
한글 파일 취약점 악용한 공격 기승

이에 앞서 지난 9월에는 한글 소프트웨어의 알려진 취약점을 악용한 악성코드가 잇달아 발견되기도 했다. ‘중공 5세대 핵심들의 불확실한 미래.hwp(241,873바이트)’([그림 3])와 ‘미래모임.hwp(104,448바이트)’ 등이 그것이다.



이들 파일은 모두 알려진 취약점을 악용해 백도어 기능을 수행하는 악성코드를 생성하고 실행시키는 역할을 하고 있었다. 한글과컴퓨터는 해당 취약점과 관련한 보안 패치를 이미 배포했다. 보안 패치는 '한컴 자동 업데이트'를 실행하여 설치할 수 있으며 '한글과컴퓨터' 웹 사이트(www.hancom.com)를 통해서도 보안 패치를 다운로드 할 수 있다.

한편 지난 8월에는 마치 기사를 스크랩해 둔 내용을 전달하는 것처럼 위장한 한글 파일이 유포되기도 했다. 해당 파일은 특정 언론사의 기사 내용을 그대로 복사하거나 해외 뉴스를 스크랩한 내용(그림 4)이 담겨 있었다.



해당 파일은 아래의 경로로 파일을 생성한 뒤 부팅 시 자동 실행되기 위해서 생성 파일을 서비스로 등록시켰다. 또 이 파일은 키로거 등 다양한 정보유출 기능을 지니고 있는 백도어였다.

- C:\Documents and Settings\All Users\Application Data\SxS.
DLL

이 악성코드는 아래의 파일에 키로깅 데이터를 저장하는 한편, 제작자가 원하는 시점에 저장된 파일을 수집하기도 했다.

- C:\Documents and Settings\All Users\Application Data\SSK.
LOG

이 파일은 지난 8월13일 유포된 것으로 확인됐는데, 8월9일 등록된 기사를 이용하는 신속함을 보였다. 단시간 내에 기사를 도용하고 악성 코드를 제작한 것이다. 공격자들이 사람들의 경계심을 풀고 눈속임을 하기 위해서 얼마나 ‘공 들여(?)’ 공격을 벌이고 있는지 단적으로 보여주는 예다.

해당 악성코드의 목적은 감염된 PC를 지속적으로 모니터링하고 내부 정보를 탈취하는 것이었다. 더욱이 이 악성코드는 실행이 된 뒤 감염의 원인인 악성 한글파일을 삭제하고 정상 한글 파일을 생성함으로써 사용자가 전혀 감염 여부를 눈치 채지 못하도록 했다.

업데이트 서버를 이용한 고도화된 공격도

이제까지 살펴본 사례들은 주로 한글 파일의 취약점을 악용해 공격하는 형태의 악성코드들이었다. 그런데 최근 아래이한글 자동 업데이트 기능을 악용한 악성코드 유포 시도가 발견돼 충격을 주었다.

지난 11월12일 발견된 악성코드는 모두 2종으로 아래아한글 업데이트 서버를 통해 유포된 것으로 추정된다. 현재까지 파악된 바로는 악성코드 제작자는 아래아한글 업데이트 서버를 매개체로 삼아 프로그램을 업데이트하기 위해 서버에 접속하는 사용자 PC를 감염시키고자 한 것으로 보인다. 해당 악성코드는 키보드 입력 값을 저장한 뒤 홍콩에 있는 특정 서버로 정보를 전송하는 것으로 확인됐다. 랜랩에서는 해당 악성코드 대응을 위해 긴급 엔진을 제작, 배포했다.

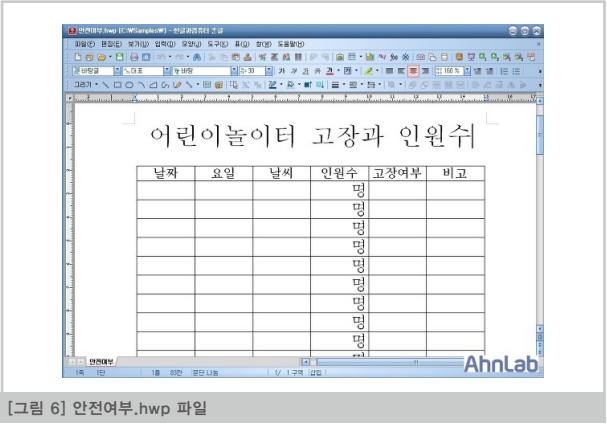
한글 파일을 이용한 공격 꾸준히 증가

이밖에 한글 파일의 취약점을 이용하지 않는 공격도 꾸준히 늘고 있다.

지금까지 자주 등장했던 ▲HncTextArt_hplg에 존재하는 스택(Stack)의 경계를 체크하지 않아 발생하는 버퍼 오버플로우로 인한 임의의 코드 실행 취약점 ▲HncApp.dll에 존재하는 문단 정보를 피싱

하는 과정에서 발생하는 버퍼 오버플로우로 인한 임의의 코드 실행 취약점 ▲혹은 EtcDocGroup.DFT에 존재하는 버퍼 오버플로우로 인한 임의의 코드 실행 취약점뿐만 아니라, 이 범주 안에 속하지 않는 공격도 속속 나타나고 있는 것이다.

ASEC은 지난 11월 ASEC Report vol. 33을 통해 알려진 취약점을 이용하지 않는 한글파일[그림 6]이 다수 발견되고 있다고 전했다.



[그림 6] 안전본부.hwp 파일

이들 문서는 파일 자체에는 취약점을 악용할 수 있는 익스플로잇 (Exploit) 코드와 셸코드(Shellcode)가 포함돼 있지 않았다. 때문에 열어보는 것만으로 악성코드에 감염되지는 않았다.

그러나 인코딩된 'ahnurl.sys' 파일을 내부에 임베디드된 형태로 가지고 있었으며, 어떤 파일은 레지스트리에 쓸 수 있는 데이터인 ahnurl, ahnurl.sys 파일을 모두 가지고 있었다.

이처럼 한글 파일에 대한 위협이 증가하고 있어 사용자들은 한글과컴퓨터에서 제공하고 있는 취약점 제거 보안 패치 업데이트를 확인 및 적용해야 한다.

안랩 분석팀 장영준 선임 연구원은 “기업 내부에서 사용하는 소프트웨어의 리스트를 작성한 뒤 주기적인 관리가 필요하다”며 “기업 내부 사용자가 직접 기업 외부망을 통해 패치나 소프트웨어를 다운로드 하는 것보다는 보안 관리 담당 부서에서 기업이 사용하는 소프트웨어를 관리하도록 정책적인 유도를 해야 한다”고 강조했다. 또한 “사용하는 소프트웨어의 패치나 버전 업그레이드가 필요할 때도 보안 담당부서가 이를 먼저 설치하고 안전성을 검토해야 한다”고 조언했다.

아이폰 백업 파일 포렌식_2부

앱을 읽으면 사용자의 라이프스타일이 보인다

<연재목차>

1부_아이폰 백업 파일의 흔적을 찾아라(2012년 11월 호)

2부_앱을 읽으면 사용자의 라이프스타일이 보인다(이번 호)

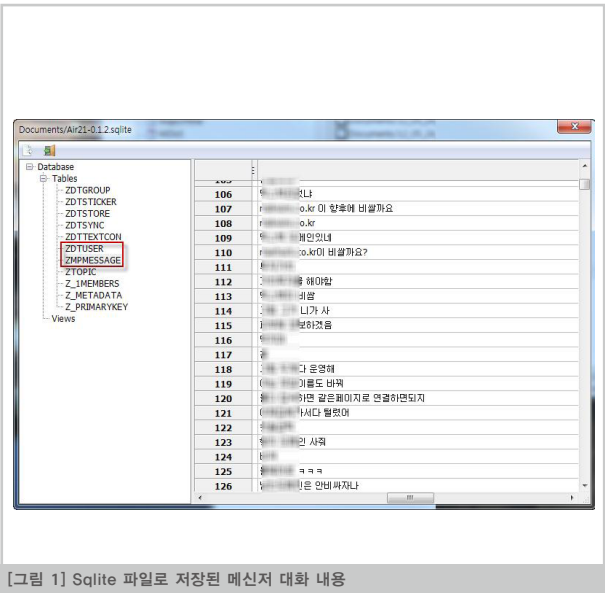
월간 안 2012년 11월 호부터 2회에 걸쳐 아이폰 백업 파일 포렌식에 대해 살펴보고 있다. 11월 호에서는 스마트폰 백업 파일이 어떤 경로에 존재하고, 어떠한 정보를 갖고 있으며, 특히 포렌식 측면에서 가치 있는 데이터는 무엇인지 알아봤다. 이번 호에서는 스마트폰 사용자들이 주로 이용하는 앱 유형에 따른 포렌식 분석 방법을 알아보자.

시장조사 전문기관 닐슨 미디어 리서치(Nielsen Media Research)의 조사에 따르면 전 세계 스마트폰 사용자는 평균 41개의 스마트폰 앱을 사용하고 있는 것으로 나타났다. 주로 사용하는 앱은 SNS(소셜 네트워크 서비스), 동영상 서비스, 메일 등이었다. 또한 우리나라 스마트폰 사용자들이 가장 많이 사용하는 앱은 메신저 앱으로 조사됐다. 이 외에도 실제 스마트폰 사용자들이 자주 이용하는 기능을 꼽으라면 카메라, 음악 및 동영상 재생, 그리고 웹 브라우저나 GPS 기반의 앱 등이 있을 것이다. 이 글에서는 메신저 앱(Messenger App), GPS 앱을 중심으로 앱 유형에 따른 포렌식 분석 방법과 취약한 앱을 활용한 포렌식 분석 방법 등에 대해 살펴본다.

메신저 앱(Messenger App)

1. 마이피플(MyPeople)

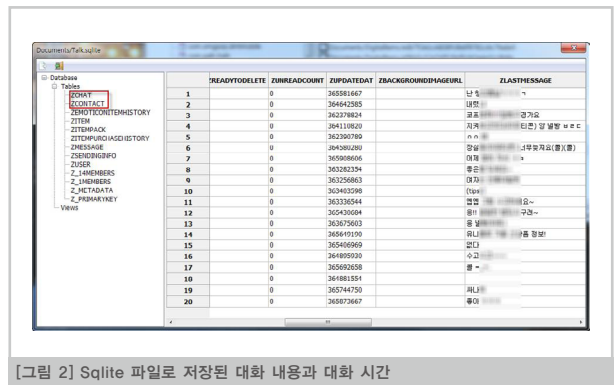
마이피플은 사용자와 상대방이 대화를 나누었던 내용을 전부 기록한다. 대화 내용은 Sqlite 파일로 저장된다. 대화했던 내용과 시간 정보가 기록되어 있어 사용자 행위 분석에 활용할 수 있다.



[그림 1] Sqlite 파일로 저장된 메신저 대화 내용

2. 카카오톡(KaKao Talk)

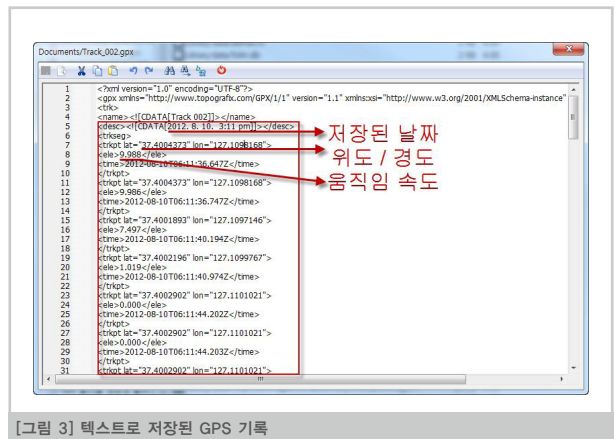
카카오톡도 마이피플(MyPeople)과 마찬가지로 대화한 내용을 Sqlite 파일로 저장한다. 또한 마지막 대화 내용과 대화 내용 시간(MAC Absolute Time)도 저장하고 있다. 이러한 대화 내용과 시간 정보는 사용자 행위 분석에 유용하다.



GPS 앱

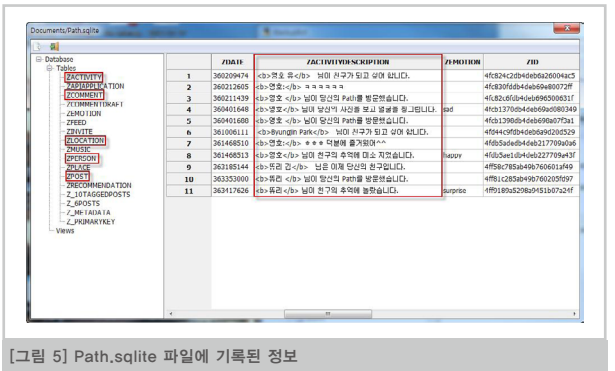
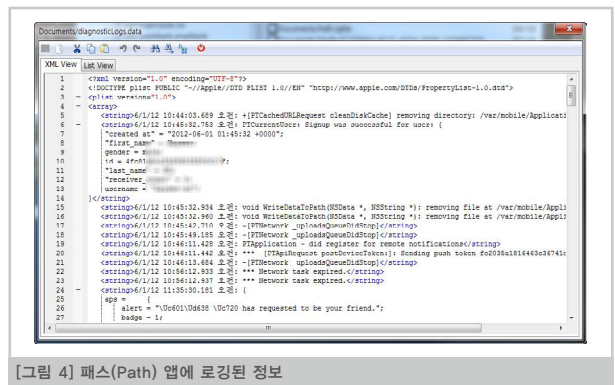
1. MotionXe

GPS를 기록하는 앱들은 대부분 텍스트(text)형태로 GPS를 기록한다. 이러한 기록은 구글 어스(Google Earth)나 구글 맵(Google Map) API를 사용하여 트래킹(tracking) 할 수 있다.



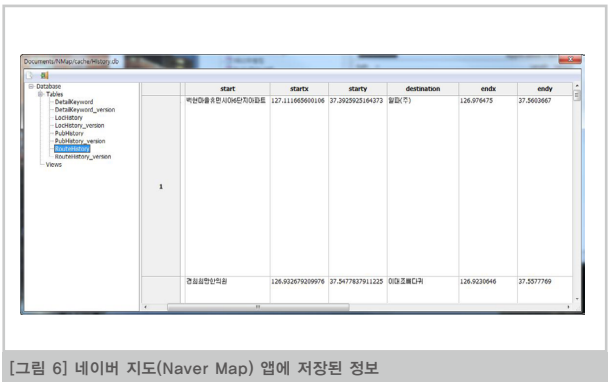
2. 패스(Path)

패스(Path)는 폐쇄형 소셜 네트워크 서비스다. 이 앱은 앱 자체의 상태 정보와 사용자 정보를 로깅(logging)한다. 특히 'Path.sqlite'라는 파일은 포스팅한 내용의 GPS와 시간 정보, 대화 내용 등을 기록하기 때문에 사용자의 개인 정보를 확보하는 데 매우 유용하다.



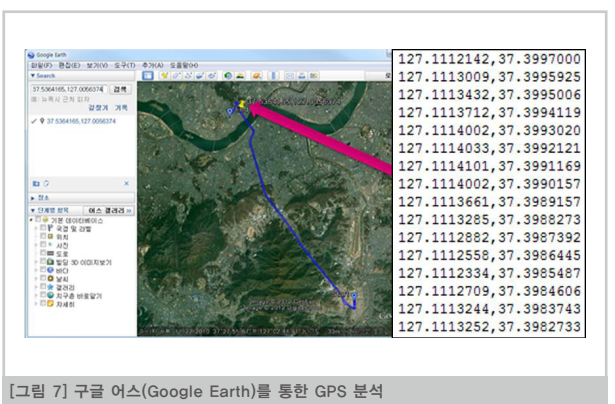
3. 네이버 지도(Naver Map)

네이버 지도는 사용자가 장소를 검색했던 시간과 GPS 기록 전부를 저장하고 있다. 만약 특정 사용자의 스마트폰을 분석할 경우, 해당 앱을 통해 사용자가 이동한 기록을 전부 확인할 수 있으므로, 사용자의 행동 범위를 추적할 수 있다.



GPS 정보 분석

스마트폰 안에 다양하게 분포된 GPS 기록이 저장되어 있다. 다양하게 분포되어 있는 GPS 정보를 하나로 모아서 살펴봄으로써 분석가는 굉장히 중요한 정보를 얻을 수 있다. GPS 분석을 위해 사용하는 도구는 구글 어스(Google Earth)가 있다. 구글 어스 확장자인 KML(Keyhole Markup Language) 파일을 사용하면 전체 이동 경로 및 장소를 지도에 표시할 수 있다. 구글 개발자 페이지 KML(<https://developers.google.com/kml/documentation/>)에서 자세한 내용을 참고할 수 있다.

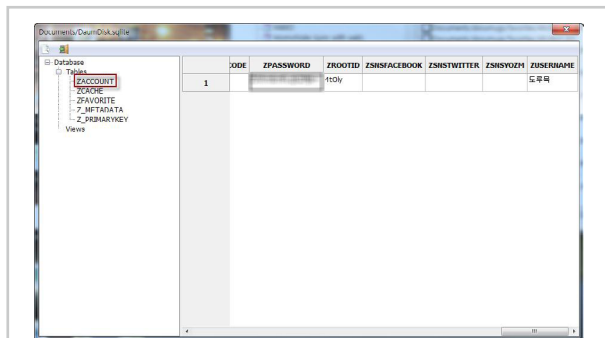


취약한 앱과 관련 포렌식

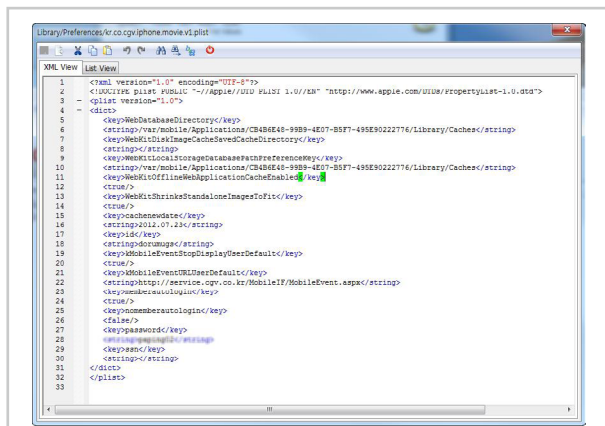
1. 비밀번호를 저장하는 앱

앱을 사용할 때 비밀번호를 입력해야만 동작하는 앱이 있다. 사용자가

비밀번호를 입력하면 앱이 실행되고 필요한 정보를 이용할 수 있다. 문제는 간혹 비밀번호를 평문(clear text)으로 저장하거나 손쉽게 디코딩 할 수 있는 형태로 저장하는 앱이 있다는 것이다. 이러한 앱은 'base64'로 인코딩하거나 조금만 수고(?)하면 단순한 알고리즘을 이용해 쉽게 디코딩 할 수 있다. 보안의 관점에서 본다면 취약한 방법으로 비밀번호를 저장하고 있어 우려되지만 포렌식 관점에서 본다면 용의자의 비밀번호를 쉽게 풀어내는 데 도움이 된다.



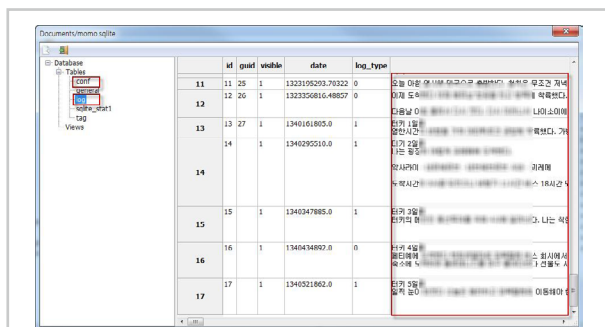
[그림 8] 앱이 저장하고 있는 비밀번호



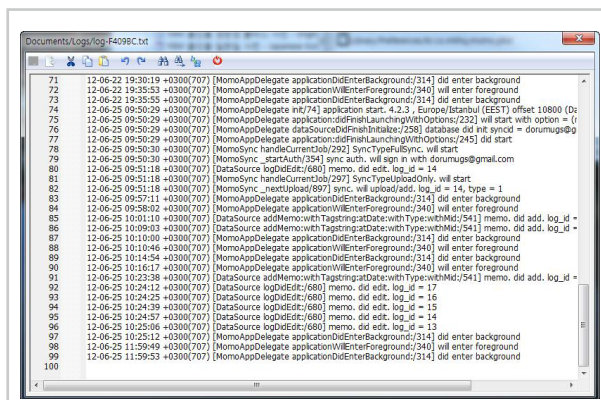
[그림 9] 앱이 저장하고 있는 비밀번호 2

2. 사용자 정보

사용자의 정보는 스마트폰의 곳곳에 존재한다. 기본 설정 파일에도 존재하며, 앱이 남기는 파일도 다양한 사용자 정보를 포함하고 있다. 그 중에서도 다이어리 앱이나 메모 앱은 특히 더 많은 정보를 저장하고 있다. 아마도 이러한 앱에는 비밀번호를 적용하여 사용할 것이다. 그러나 백업 파일에는 권한에 따른 별 다른 영향 없이 분석가가 원하는 내역을 확인할 수 있는 경우가 종종 있다. 작성된 내용은 작성 당시의 시간 정보도 포함하고 있어 사용자에 대한 행위 분석이 가능하다. 물론, 모든 앱이 보안에 취약한 것은 아니다.

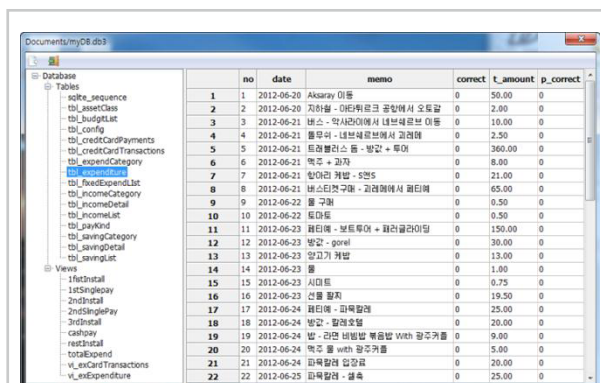


[그림 10] 다이어리 앱에 저장된 내용



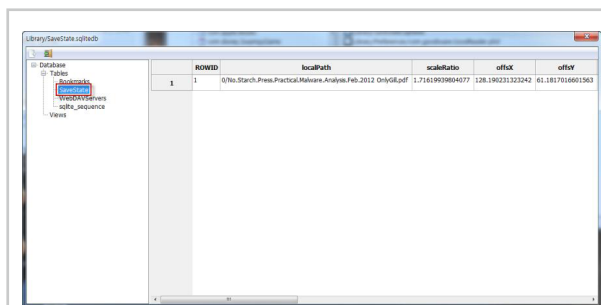
[그림 11] 다이어리 앱에 저장된 작성 시간 정보

용돈 기입장이나 가계부 앱을 이용하는 사용자라면 백업 파일에 용돈이나 월급을 사용한 내역이 저장되어 있을 수도 있다. 이러한 내역은 XML이나 sqlite 파일로 저장되며 돈을 언제, 얼마나 사용했는지에 대한 정보를 제공한다.



[그림 12] 가계부 앱에 저장되는 사용자 정보

도서나 PDF 리더 등은 사용자가 가장 최근에 무엇을 보거나 읽었는지에 대한 내용을 저장한다. 해당 기록을 바탕으로 사용자가 최근에 읽었던 서적이 무엇인지, 또 어떠한 문서에 관심을 두고 있는지 등에 대한 정보를 확인할 수 있다.



[그림 13] 문서 리더 앱에 저장된 사용자 정보

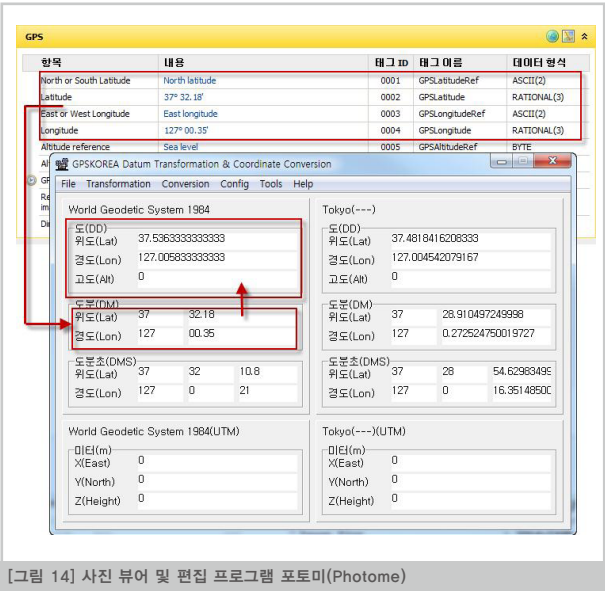
사진 파일 분석

스마트폰으로 사진을 찍으면 사진 자체뿐만 아니라 상당히 많은 정보가 저장된다. 그 중에서도 포렌식 측면에서 중요한 데이터는 GPS 정보와 GMT 기록 시간, 그리고 수정과 생성 시간 등이다. GMT 기록시간은 GMT 시간이 아닌 현지 시간(Local Time)으로 저장되며, 파일 수정 시간은 GMT 시간으로 기록된다. 또한 사진으로 남은 JPEG 파일은 사진을 찍은 단말기의 이름과 업체명을 저장하고 있다. 이러한 정보를 해석

하기 위해 사용하는 도구들과 관련 웹사이트는 각각 다음과 같다.

1. 포토미(Photome)

- http://www.photome.de/download_en.html



[그림 14] 사진 뷰어 및 편집 프로그램 포토미(Photome)

2. Exiftool

- <http://www.sno.phy.queensu.ca/~phil/exiftool/install.html>



[그림 15] 디지털 사진 정보 편집 프로그램 Exiftool

아이폰 백업 파일 분석 결과와 사용자 권고 사항

지금까지 살펴본 바를 통해 아이폰 백업 파일을 로컬에 남기는 경우, 다양한 사용자 정보를 로컬 PC에 생성하는 것과 같다는 것을 알았다. 만약 해당 PC를 이미징하게 되면 ▲사용자가 어떤 App을 사용했는지 ▲비밀번호는 어떤 것을 쓰는지 ▲언제, 어디를 갔으며 ▲돈을 얼마를 썼는지 ▲누구와 언제 통화를 했는지 ▲누구와 메신저 채팅을 통해 어떤 대화를 했는지 등의 정보를 쉽게 획득할 수 있다.

이러한 정보를 로컬 PC에 남기지 않으려면 기본 설정으로 제공되는 아이클라우드(iCloud)를 사용하는 것이 좋다. 만일 네트워크 정책에 의해 아이클라우드를 사용할 수 없는 경우라면 백업 경로에 남아있는 아이폰 백업 파일을 주기적으로 삭제하는 것이 바람직하다. 특히 파일을 삭제하더라도 일부 복구가 가능하므로 PC에서 파일을 삭제할 때는 파일 완전 삭제 프로그램(Wiping)을 사용하는 것이 좋다.

또한 아이폰은 비밀번호를 기록하고 있는 파일이 존재할 수 있다. 비밀번호를 사용하도록 하는 앱은 가급적 이용하지 않을 것을 권한다. 반드시 이러한 앱을 사용해야만 하는 경우라면 해당 앱을 사용한 후 삭제하는 등의 방법도 생각해볼 수 있겠다.

보이지 않는 세상 속 악의 ‘손’, 사이버 범죄

사이버 범죄의 피해 현황과 ‘크라임웨어’

〈연재목차〉

1부_사이버 범죄의 정의와 구체적인 형태들(2012년 11월 호)

2부_사이버 범죄의 피해 현황과 크라임웨어(이번 호)

IT 기술이 발달하면서 사이버 범죄도 날이 갈수록 증대되고 있다. 과거 사이버 범죄는 개발자들이 주로 자신의 이름을 알리기 위한 도구로 사용했다. 그 피해도 사이버 세계에 국한되는 양상을 보였다. 하지만 최근 사이버 범죄는 악성 프로그램 등을 이용해 돈을 갈취하는 등 현실 세계와 밀접한 관련이 있는 범죄로 발전하고 있다.

이에 지난 호(11월) 월간 안은 사이버 범죄가 포함하고 있는 영역은 어디까지이며, 실제 어떠한 범죄들이 일어나고 있는지 살펴보았다. 이번 호에서는 국내외의 사이버 범죄 현황을 알아본 뒤, 금전적 피해까지 유발하는 사이버 범죄 용어인 ‘크라임웨어’에 대해 알아보고자 한다.

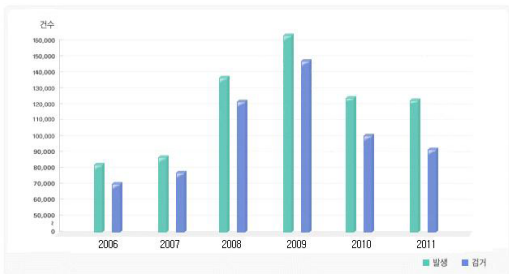
사이버 범죄(Cyber Crime)로 인한 피해 현황

경찰청 사이버테러대응센터가 공개한 자료([표 1])에 따르면 지난 2003년 국내에서 발생한 사이버 범죄는 총 6만8445건이었다. 하지만 8년이 지난 2011년에는 11만6961건으로 배 이상 증가했다. 약 58.5%가 늘어난 것이다.

특히 국내에서 벌어지고 있는 사이버 범죄들은 악성코드의 유포나 해킹과 같은 ‘사이버 테러’형 범죄보다 ‘일반 사이버 범죄’가 급증하는 추세다. 지난 호 <월간 안>에서 살펴보았듯이 경찰청은 사이버 범죄를 사이버 테러와 일반 사이버 범죄 등 크게 두 가지로 구분하고 있다.

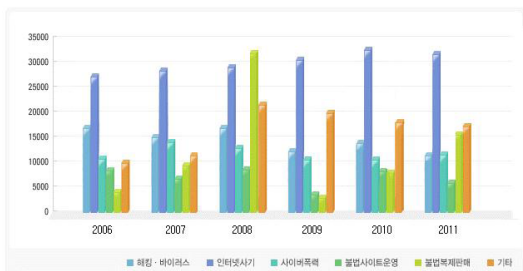
이를 바탕으로 [표 1]을 살펴보면 사이버 테러형 범죄의 경우 2003년 1만4241건이었고 2011년에도 1만3396건으로 제자리에 그쳤다. 반면에 일반 사이버 범죄는 2003년 5만4204건이었으나 2011년엔 10만3565건으로 53% 가량 늘어난 사실을 알 수 있다.

또한 경찰청 사이버테러대응센터가 집계한 사이버 범죄의 세부 유형([표 2])을 통해서도 테러형 사이버 범죄보다 일반 사이버 범죄가 늘고 있다는 사실을 미루어 짐작할 수 있다.



구분	총계		사이버테러형 범죄		일반 사이버 범죄	
	발생	검거	발생	검거	발생	검거
2003	68,445	51,722	14,241	8,891	54,204	42,831
2004	77,099	63,384	15,390	10,339	61,709	52,991
2005	88,731	72,421	21,389	15,874	67,342	56,547
2006	82,186	70,545	20,186	15,979	62,000	54,566
2007	88,847	78,890	17,671	14,037	71,176	64,853
2008	136,819	122,227	20,077	16,953	116,742	105,274
2009	164,536	147,069	16,601	13,152	147,935	133,917
2010	122,902	103,809	18,287	14,874	104,615	88,935
2011	116,961	91,496	13,396	10,299	103,565	81,197

[표 1] 사이버 범죄 발생 및 검거 현황(출처: 경찰청 사이버테러대응센터)



[표 2] 사이버 범죄 유형별 현황(출처: 경찰청 사이버테러대응센터)

[표 2]와 같이 해킹과 바이러스 등 테러형 범죄는 전체 사이버 범죄에서 차지하는 비중도 낮을 뿐만 아니라, 2008년을 기점으로 줄어드는 경향을 보이고 있다. 하지만 인터넷사기 등 일반 사이버 범죄는 전체 범죄의 3분의 1가량을 차지할 정도로 높은 비중을 나타내고 있다.

이를 볼 때 한국에서 발생하는 사이버 범죄는 해킹 등과 같은 기술에 기반한 사이버 범죄보다는, 인터넷 사기 사건처럼 기술을 기반하지 않는 유형들이 주를 이루고 있음을 유추할 수 있다.

그렇다고 결코 안심할만한 결과는 아니다. 인터넷 사기의 비중이 높다는 것은 '인터넷 공간을 이용해 비교적 손쉽게 금전적 이윤을 확보할 수 있는 사이버 범죄의 발생 가능성이 높다'는 의미로도 해석이 되기 때문이다.

이 대목에서 최근 사이버 범죄 시장이 급성장하고 있는 러시아의 사례를 눈여겨볼 필요가 있다. 러시아의 사이버 범죄 전문 연구업체인 'Group-IB'가 작성한 <State and Trends of The Russian Digital Crime Market 2011>([표 3]) 자료를 보면, 러시아는 한국과 달리, '스팸(Spam)'이나 '온라인 뱅킹 사기(Online banking fraud)' 사건이 전체 사이버 범죄의 대부분을 차지하는 것을 알 수 있다.

TREND	TOTAL MARKET SHARE	AMOUNT
ONLINE FRAUD		
Online banking fraud	21.3 %	490 million \$
Cashing	16 %	367 million \$
Phishing	2.4 %	55 million \$
Theft of electronic funds	1.3 %	30 million \$
Total:	41 %	942 million \$
SPAM		
Spam	24 %	553 million \$
Pharma and counterfeits	6.2 %	142 million \$
Fake software	5.9 %	135 million \$
Total:	36.1 %	830 million \$
INTERNAL MARKET (C/C)		
Sale of traffic	6.6 %	153 million \$
Sale of exploits	1.8 %	41 million \$
Sale of loaders	1.2 %	27 million \$
Anonymization	0.4 %	9 million \$
Total:	10 %	230 million \$
DDOS ATTACKS		
DDoS attacks	5.6 %	130 million \$
Total:	5.6 %	130 million \$
OTHER		
Other	7.3 %	168 million \$
Total:	7.3 %	168 million \$

[표 3] 러시아 블랙 마켓의 사이버 범죄 형태별 수익 현황(출처: Group-IB)

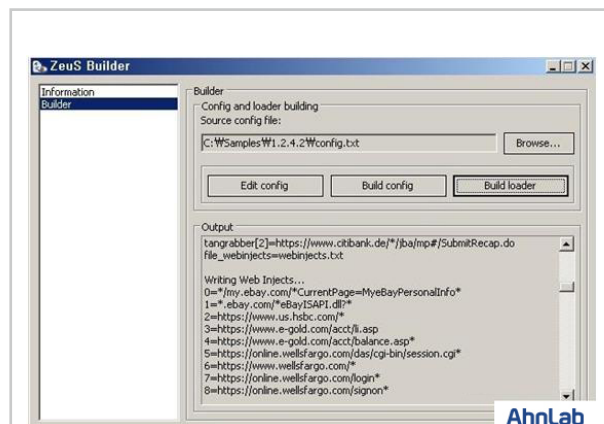
특히 러시아에서는 온라인 뱅킹 사기 사건이 금융기관 홈페이지로 위장한 '피싱(Phishing)' 웹사이트로 인해 발생하기 보단, 온라인 뱅킹 정보 탈취를 목적으로 제작된 악성코드들인 '크라이웨어(Crimeware)'에 의해 주로 발생하는 것으로 나타났다. 그렇다면 금전적 이윤을 탈취하는 사이버 범죄에 악용되는 크라이웨어는 구체적으로 무엇을 뜻하는지, 그리고 대표적인 악성코드는 무엇인지 간단히 살펴보기로 하겠다.

'온라인 뱅킹 트로이목마'로 대표되는 크라이웨어

크라이웨어(Crimeware)라는 용어는 대략 2008년부터 일부 해외 보안업체들을 중심으로 등장했다.

과거 악성코드 제작자들은 단순 장난이나 취미활동 등을 목적으로 보안에 위협적인 악성코드 등을 만들었다. 하지만 최근 들어 금전적인 이윤 확보를 목적으로 하는 경우가 늘어나고 이에 최적화된 악성코드들이 대량 생산되면서 크라이웨어라는 용어가 사용되기 시작했다.

특히 크라이웨어는 해당 소프트웨어 사용자가 알지 못하는 사이 불법적인 동작을 수행함으로써 제작자에게 금전적인 이익을 안겨준다. 이 같은 크라이웨어의 대표 형태를 살펴보면 온라인 뱅킹에 사용되는 개인 정보를 탈취해 악성코드 제작자에게 전달하는 '제우스(Zeus)'와 '스파이아이(Spyeye)'를 들 수 있다.



[그림 1] 온라인 뱅킹 트로이목마인 Zeus 악성코드 생성도구



[그림 2] 온라인 뱅킹 트로이목마인 Spyeye 악성코드 생성도구

제우스와 스파이아이는 주로 유럽지역을 중심으로 퍼져 있다. 이들은 각 금융기관들이 고객 편의를 목적으로 만들어 놓은 웹사이트에 고객이 접속해 아이디와 비밀번호를 입력하면 그것을 후킹(Hooking)해 특

정 서버로 전송하는 구조를 가지고 있다. 어느 날 갑자기 은행잔고에 '제로(0)'나 '마이너스'가 찍히는 일이 벌어지는 것이다.

사이버 범죄 예방, 윤리 확립이 우선

우리는 이제까지 사이버 범죄가 무엇이며 어떤 특징과 형태를 가지고 있는지 살펴보았다.

또한 러시아의 사이버 범죄 사례를 통해 크라임웨어를 이용한 온라인 बैं킹 사기가 높은 비중을 차지하고 있음을 알 수 있었다. 한국도 크라임웨어의 한 형태인 온라인 बैं킹 트로이목마에 의해 금융피해가 유발되고 있고 지속적인 피해가 발생하고 있다는 사실 역시 알 수 있었다.

그러면 이런 사이버 범죄를 예방하기 위해서는 어떠한 대책을 세울 수 있을까. 현재로서는 크게 세가지 측면에서 대비책이 제시될 수 있을 것으로 보인다.

먼저 법과 제도적인 면에서 대책을 세울 수 있다. 한국의 경우 지난 1992년부터 컴퓨터 범죄에 관한 규정이 만들어졌다. 1995년에는 개정 형법 특별법을 통해 컴퓨터 및 인터넷 범죄에 대한 규정을 만들었다. 이들을 비롯해 최근 대두되고 있는 사이버 범죄의 대표 법률로는 '정보통신망이용촉진및정보보호등에관한법률'을 들 수 있다.

문제는 지속적으로 새로운 형태의 사이버 범죄가 발생하고 있어 현행 법과 규제만으로 대응하기에 한계가 존재한다는 점이다.

두 번째, 기술적인 대응도 한 방법이 될 수 있다. 기술적 대응은 인터넷에서 발생하는 기술 기반의 사이버 범죄를 예방 및 차단하는 용도로 사용될 수 있다. 그러나 이 역시 기술적인 대응이 발달할수록 이를 우회하는 사이버 범죄도 발달하기 때문에 예방을 하기에는 역부족인 측면이 있다.

세 번째, 사회·문화적인 차원에서 인터넷 윤리를 확립하는 방안이다. 인터넷이라는 공간은 다수가 이용하는 곳으로 사회 규범과 문화가 존재하는 하나의 사회라는 인식이 무엇보다 중요하다. 그 안에서 사이버 범죄를 예방하기 위한 자정적 노력이 뒷받침되어야 한다. 이는 자발적 문화운동 성향이 강해 강제력 면에서는 다른 대책에 비해 약할지라도 예방과 근본해결에는 가장 좋은 처방이 될 수 있다.

인터넷 윤리 확립을 위해서는 우선 사회적으로 건전한 인터넷 이용 문화가 자리잡도록 다양한 교육 프로그램을 운영해야 한다. 교육 프로그램은 인터넷에서 발생하는 사이버 범죄를 점차 감소시킬 수 있으며 그와 동시에 사이버 범죄로 인한 피해도 감소될 수 있을 것으로 기대된다.

참고

- 경찰청 사이버테러대응센터 – <http://www.ctrc.go.kr>
- 사이버 범죄학 원인 유형 대책 – 이성식 저 (2011)
- Crimeware Understanding New Attacks and Defenses – Markus akobsson, Zulfikar Ramzan 저 (2008)
- Cyber Fraud Tactics, Techniques and Procedures – Graham, James 저 (2009)
- (The) Myths of Security: What the Computer Security Industry Doesn't Want You Know – John Viega 저 (2010)
- State and Trends of the Russian Digital Crime Market 2011 – Group-IB (2011)
- Carberp and the reshipping incident – CSIS Security Group (2012)
- Shylock and the "Man in the Chat" – CSIS Security Group (2012)
- ASEC Threat Research & Response Blog

안랩, ‘파트너 엔지니어 기술 강화’ 나서



▲ 지난 11월 9~10일 강원도 홍천에서 열린 ‘안랩 베이스업 트레이닝 데이’에 참석한 엔지니어 및 안랩 관계자들이 기념촬영을 하며 ‘파이팅’을 외치고 있다.

안랩은 지난 11월 9~10일 이틀간 강원도 홍천 대명리조트에서 ‘2012 엔지니어를 위한 안랩 파트너 베이스업 트레이닝 데이’를 개최했다. 파트너사 엔지니어들의 기술향상과 소통 강화를 위해 이번 행사를 마련했으며 소프트웨어(SW) 총판 및 파트너사 엔지니어 40여 명이 참석했다.

행사에선 올해 첫 시행되는 ‘채널 엔지니어 인증 평가’가 중점 소개됐다. 또한 인증평가에 발맞춰 다각도로 진행될 예정인 파트너 지원 방향에 대해서도 구체적으로 전달됐다.

안랩 솔루션지원팀이 밝힌 ‘채널 엔지니어 인증평가’의 시행 방안에 따르면 인증 평가는 ‘기술 및 교육 부문의 지원 방향성을 검토 및 수립’하는 등의 목적으로 기획됐다.

평가는 필수적으로 응시해야 하는 ‘필수과목’과 기타 ‘선택과목’으로 진행된다. 필수에는 악성코드가, 선택에는 ▲AhnLab Policy Center(APC) ▲AhnLab Online Security(AOS) ▲TrusLine01 각각 포함됐다.

제1회 인증평가 시행일은 오는 12월11일이며 사전 신청은 12월7

일 오후 6시에 마감된다. 온라인 평가에 이어 추후 실습평가도 이뤄질 계획이다.

아울러 안랩은 인증 평가가 단순 평가에 그치지 않도록 추가적인 지원책도 마련했다고 행사를 통해 밝혔다.

기술 지원 통합 인프라 시스템, 즉 ‘ATAC(AhnLab Technical Assistance Center)’을 새롭게 구축해 엔지니어들의 기술 향상을 도모하겠다고 전한 것이다.

ATAC는 체계적인 이슈 관리와 신속한 업무 피드백 및 지원을 맡는다.

이외에도 행사에서는 차세대 악성코드 분석기술인 ‘MDP’와 ‘AOS Secure Authentication’ 솔루션이 소개됐으며 엔지니어 인증 평가와 ATAC 도입에 대한 조별 토론, 설문조사도 실시됐다.

안랩 솔루션지원팀 관계자는 “안랩과 파트너사 엔지니어들이 긴밀히 소통하고 상생하자는 의미로 워크숍을 열었다”며 “향후 진행될 교육과 지원에 더욱 내실을 기하도록 노력하겠다”고 말했다.

‘특허경영’으로 안랩의 기술 리더십 강화

안랩이 최근 ‘특허 경영’으로 기술 리더십을 강화하고 있어 주목된다.

‘특허권 확보’는 기업의 원천 기술 보유, 제품 경쟁력 강화, 해외 시장 개척의 원동력이 된다는 점에서 중요하게 받아들여진다. 때문에 보안산업계는 특허권 확보를 위해 경쟁업체들과 ‘총탄 없는 전쟁’을 벌이고 있는 상황이다.

이런 가운데 안랩은 지난 11월6일 기업의 모바일 환경에 적용할 수 있는 보안 기술인 ‘모바일 단말 간 서버 네트워크 지원 관리 서버, 모바일 단말 서버 및 방법’의 국내 특허를 획득했다.

이번 특허 기술은 기업 내 구성원이 사용하는 모바일 기기(스마트폰, 태블릿PC 등)를 통합 관리해주는 MDM(Mobile Device Management) 솔루션인 ‘안랩 모바일 센터(AhnLab Mobile Center)’에 적용되어 있다. 또 지식경제부가 추진한 ‘월드 베스트 소프트웨어’ 과제의 주요 성과 중 하나로써 의미가 적지 않다.

이번 모바일 기술 특허 획득을 비롯해 안랩이 올해(11월19일 현재) 획득한 국내특허 출원은 모두 39건이며, 해외 관련 특허 출원은 20건(PCT 출원 포함)이다. 이는 전년 대비 국내 출원은 77%, 해외 출원은 42%가 각각 늘어난 수치다.

안랩은 창립 이후 지금까지 모두 196건의 국내 특허 출원을 했다. 이 중 과반 이상인 117건은 실제 특허 취득까지 마친 상태다.

등록 연장을 하지 않은 것을 제외해도 누적 특허 획득 건수는 113건에 달한다. 해외에서도 PCT 국제 출원 50건, 국가별 출원 21건을 각각 기록하고 있다.

이는 국내 보안 소프트웨어 업계 중 최고 기록으로, 해외에서도 세계적 소프트웨어 기업들과 어깨를 견줄 정도다.

안랩은 ‘연구개발’ 중심의 기업문화에서 이 같은 성과가 도출될 수 있었다고 설명한다. 실제로 안랩은 전체 직원의 50% 가까운 인원이 연구개발(R&D) 인력이며 매년 매출액의 20% 이상을 연구개발에 투자하고 있다.

이 같은 성과에는 사내에서 운영하고 있는 ‘iQ’도 한 몫을 하고 있다는 전언이다. 안랩은 작은 아이디어(idea)도 소중히 여겨 프로젝트 자격을 부여(Qualify)하고 있다.

이를 통해 개인정보보호 솔루션인 ‘안랩 프라이버시 매니지먼트(AhnLab Privacy Management)’를 비롯해 APT 대응솔루션인 ‘트러스와처(TrusWatcher)’의 핵심 기술로 악성 문서 파일을 정밀 검진 및 차단하는 ‘DICA(Dynamic Intelligent Contents Analysis)’, V3 제품군에 탑재돼 은폐형 악성코드를 완벽하게 진단·치료하는 ‘트루파인드’ 등의 기술이 나왔다.

이외에도 안랩은 특허 기술 발명자에게 특허 출원·취득, 해외 출원 등 단계별로 포상을 하고 있다. 특허 출원을 팀 목표에 포함시키는 등 특허 출원을 장려하고 있으며 전담 인력이 특허 관리를 맡아 체계적으로 관리하고 있기도 하다.

또한 안랩은 다양한 특허 기술을 제품에 적용해 신기술의 상용화에도 노력하고 있다. 클라우드 기반의 보안 기술을 V3 제품군을 포함해 전 제품에 적용하는가 하면, 온라인 게임 해킹 방지 기술을 온라인 게임보안 제품인 ‘핵실드’에 탑재했다. DDoS 공격 방어 기술을 네트워크 보안 장비인 ‘트러스가드’에 적용한 예도 있다.

김홍선 안랩 대표는 “안랩은 최근 미국 사업을 본격화했다. 기술 경쟁력이 있어야 생존할 수 있는 IT 본토에서 안랩의 특허 기술은 큰 무기가 될 것”이라며 “지속적인 혁신과 기술개발로 글로벌 무대에서 국산 소프트웨어의 위상을 높이겠다”고 밝혔다.

안랩, 글로벌 보안기업들과 제휴 및 파트너십 체결

안랩이 최근 글로벌 보안기업들과 잇달아 제휴 및 파트너십을 체결하고 국·내외 보안시장 공략에 박차를 가하고 있다.

안랩은 지난 11월26일 미국의 전력 솔루션 업체인 줄렉스(JouleX)와 제휴, IT 에너지 관리 솔루션인 '줄렉스 에너지 매니저'를 국내에 공급한다고 밝혔다.

줄렉스 에너지 매니저는 IP 주소가 있는 사내의 모든 서버, 네트워크 장비, PC, 프린터, 전력관리 시설 등 소비 전력을 모니터링 해 관리 및 제어해준다.

더구나 IP를 이용해 관리하기 때문에 일반 오피스는 물론 분산 오피스, 데이터센터, 가상화, 클라우드 환경 등 다양한 환경에 적용이 가능하다.

안랩은 이 제품을 사용할 경우 최대 40~60%의 전력을 절감할 수 있다고 밝히고 있다. 실제 안랩이 시범 운영한 결과, PC 1대 당 월 최대 3000원까지 비용 절감 효과가 나타났다.

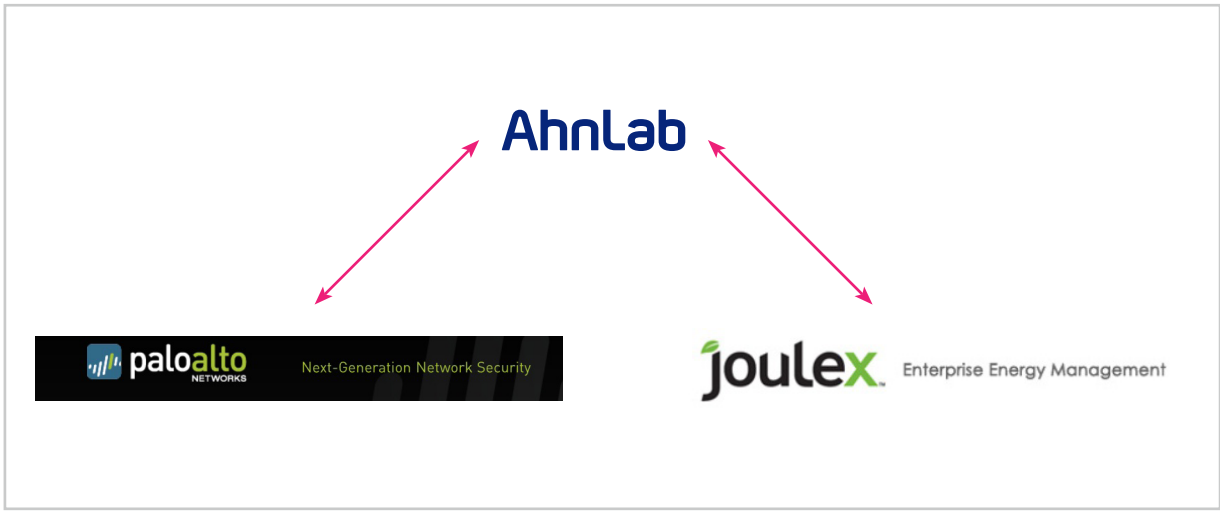
1만대 이상의 PC를 보유한 기업은 PC 관리만으로 월 3000만원 이상의 비용 절감 효과를 거둘 수 있는 것이다.

김홍선 안랩 대표는 “에너지 관리에 대한 기업들의 관심이 높아져 IT 기반의 에너지 절감 솔루션은 IT 산업의 차세대 아이템이 될 것”이라며 “앞으로 보안 및 에너지 절감 분야 융합 제품 개발과 해외 판로 개척에 박차를 가할 것”이라고 밝혔다.

이에 앞서 안랩은 지난 11월20일 글로벌 차세대 방화벽 솔루션 기업인 '팔로알토네트웍스(www.paloaltonetworks.com)'와 '엔터프라이즈 플래티넘 파트너십' 계약을 체결하고 기업 보안시장 공략 강화에 나섰다.

안랩은 이번 파트너십을 통해 팔로알토네트웍스의 차세대 방화벽인 PA 시리즈 전 제품을 기업 고객에 제공기로 했다. 아울러 안랩의 보안 분야 경험과 기술력, 컨설팅 역량을 결합해 차별화된 지원능력을 선보일 예정이다.

또 보안관계 사업과 연계를 통해 기업 보안 시장 공략을 강화하는 한편 향후 양사 간 협력을 발전시켜 해외 진출의 교두보를 마련한다는 계획이다.



ASEC, 10월 통계 및 보안이슈 발표

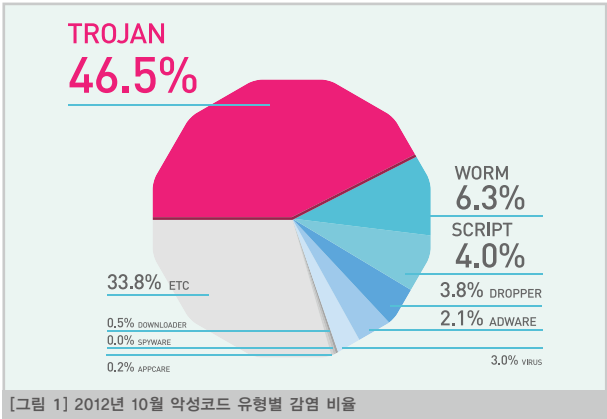
악성코드 ‘트로이목마’ 과반 가까이 기록

안랩 시큐리티대응센터(ASEC)는 ASEC Report Vol.34를 통해 2012년 10월의 보안 통계 및 이슈를 전했다. 지난 10월의 주요 보안 이슈를 살펴본다.

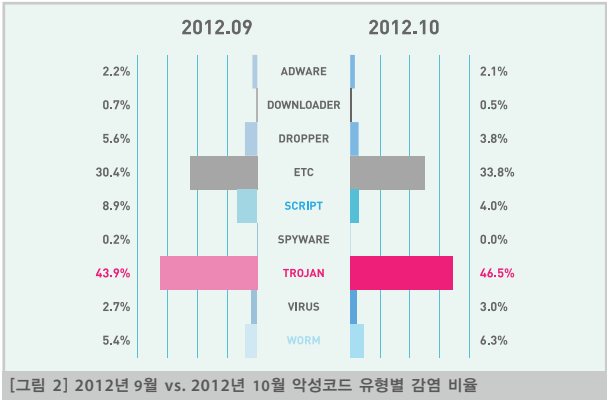
10월 악성코드, ‘트로이목마’ 여전히 높은 비중

ASEC이 집계한 바에 따르면 2012년 10월에 감염이 보고된 악성코드는 전체 805만 9522건으로 나타났다. 이는 지난 9월의 986만 6860건에 비해 108만 7338건이 감소한 수치다.

악성코드를 유형별로 살펴보면, 트로이목마(Trojan)가 46.5%로 가장 높은 비율을 나타냈다. 웜(Worm) 6.3%, 스크립트(Script) 4%가 뒤를 이었다. [그림 1]은 10월 한 달 동안 안랩의 고객들로부터 감염이 보고된 악성코드를 유형별로 집계한 결과다.



[그림 2]는 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 드롭퍼(Dropper), 스크립트(Script)가 전월에 비해 감소세를 보였으며 트로이목마, 웜(Worm)이 증가세를 보였다. 스파이웨어(Spyware), 애드웨어(Adware) 계열은 전월과 유사한 수준을 유지했다.



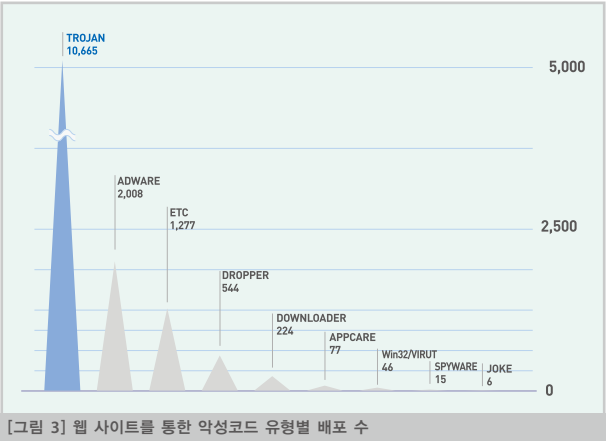
악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 10월에 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 1만 4862건이었다. 악성코드 유형은 282종, 악성코드가 발견된 도메인은 163개, 악성코드가 발견된 URL은 608개였다. 이는 2012년 9월과 비교해서 다소 감소한 수치다.

구분	건수
악성코드 발견 건수	14,862
악성코드 유형	282
악성코드가 발견된 도메인	163
악성코드가 발견된 URL	608

[표 1] 2012년 9월 웹 사이트 악성코드 동향

이들 웹 사이트를 통해 배포된 악성코드 유형은 [그림 3]과 같다. 트로이목마가 1만 665건(71.8%)로 가장 많았고, 애드웨어가 2008건(13.5%)인 것으로 조사됐다.



2012년 10월 주요 보안 이슈

■미국 대선 뉴스로 위장한 스팸 메일을 조심하라

ASEC에서는 지난 2009년부터 웹 익스플로잇 툴킷(Web Exploit Toolkit)이라는 웹을 기반으로 해 웹 브라우저나 웹 기반 애플리케이션(Web Application)들에 존재하는 취약점들을 자동으로 이용하도록 제작된 툴킷의 위험성에 대해 언급한 바 있다.

또한 웹 익스플로잇 툴킷의 하나인 '블랙홀(Blackhol)'을 이용해 사회적 주요 이슈나 대중이 관심을 가질 만한 내용을 포함한 스팸 메일(Spam Mail)을 통해 악성코드 유포를 시도한 사례들이 다수 등장하고 있음을 경고했다.

- 2012년 6월 - 스팸 메일과 결합된 웹 익스플로잇 툴킷
- 2012년 7월 - 링크드인 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷
- 2012년 8월 - 페이스북 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷

특히 올해 4분기의 경우 미국과 한국에서 '대통령 선거'라는 이슈를 악용한 사례도 등장했다. 해당 이슈를 이용해 스팸 메일을 발송한 뒤 악의적인 웹 사이트로 유도하는 사례가 발견된 것이다. 이번에 발견된 스팸 메일에는 [그림 4]와 같이 미국 대통령 선거의 후보 중 한 명인 미트 롬니(Mitt Romney)가 60% 차이로 앞서고 있다는 내용이 담겨 있었으며, 메일을 받은 사람으로 하여금 하단에 존재하는 웹 사이트 링크를 클릭하도록 유도했다.



[그림 4] 미국 대통령 선거 관련 내용으로 작성된 이메일

해당 링크를 클릭하면 블랙홀 웹 익스플로잇 툴킷의 악의적인 웹 사이트로 연결됐다. 게다가 사용자의 시스템에 웹 브라우저 및 웹 애플리케이션에 취약점이 존재하면 이를 이용해 다른 악성코드의 감염을 시도하기도 했다.

향후에도 한국의 대통령 선거와 관련된 사회적 중요 이슈들을 악용한 보안 위험이 발생할 가능성이 높으므로 각별한 주의가 요구된다. 지난 10월 발견된 미국 대통령 선거 뉴스로 위장한 스팸 메일을 통해 유포된 악성코드들은 V3 제품군에서 다음과 같이 진단한다.

<V3 제품군의 진단명>

PDF/Exploit

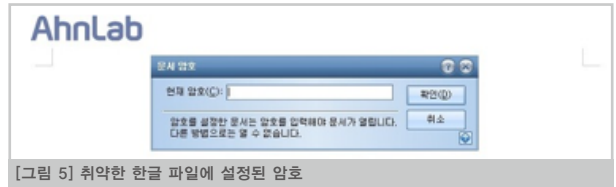
Java/Cve-2012-1723

Trojan/Win32.Pakes

■마이크로소프트워드, PDF 취약점 악용 악성코드 다수 발견

마이크로소프트 워드(Microsoft Word)와 한글 소프트웨어, 어도비 리더(Adobe Reader) PDF의 '알려진 취약점' 등을 악용하는 악성코드가 동시에 발견됐다.

최근 발견된 취약한 한글 파일은 [그림 5]와 같이 문서 암호가 설정되어 있는 '122601.hwp (213,133 바이트)'와 동일한 파일명에 파일 크기만 다른(217,231바이트) 두 종류의 파일이 있다.



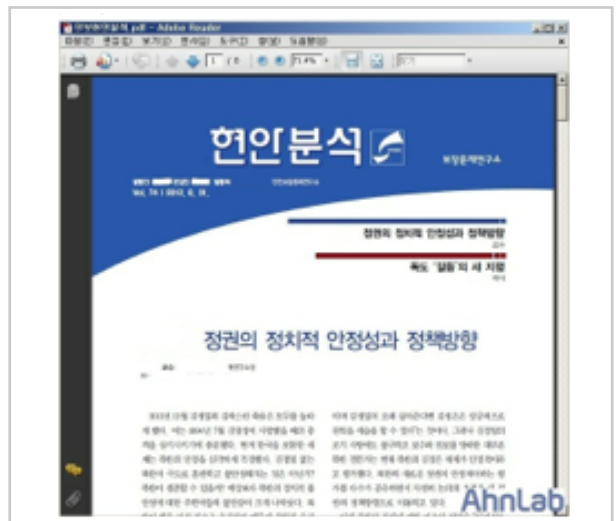
[그림 5] 취약한 한글 파일에 설정된 암호

해당 한글 파일들의 내부에는 [그림 6]과 같은 특이한 자바 스크립트가 포함되어 있다. 해당 자바 스크립트를 디코딩 하면 특정 시스템에서 'ie67.exe(99,328 바이트)'의 또 다른 악성코드를 다운로드 해 실행한다.



[그림 6] 취약한 한글 파일 내부에 포함된 자바 스크립트

어도비 아크로벳(Adobe Acrobat)에 존재하는 알려진 취약점을 악용하는 PDF 파일은 [그림 7]의 내용을 포함하고 있는 'XX현안분석.pdf(679,753 바이트)' 파일명으로 유포됐다.



[그림 7] XX현안분석 관련 내용을 취약한 PDF 파일

해당 PDF 파일은 'CVE-2009-0927' 취약점을 이용하고 있다. 지난 2009년 3월 어도비에서 보안 권고문 'APS809-04 Security Updates available for Adobe Reader and Acrobat'을 통해 취약점에 대한 보

안 패치를 배포했다.

마지막으로 마이크로소프트 워드에 존재하는 취약점을 이용하는 워드 파일은 유포 당시의 정확한 파일명은 확인 되지 않았으나 '265,395 바이트'의 크기다.

해당 PDF 파일은 'CVE-2009-0927' 취약점을 이용하고 있다. 지난 2009년 3월 어도비에서 보안 권고문 'APSB09-04 Security Updates available for Adobe Reader and Acrobat'을 통해 취약점에 대한 보안 패치를 배포했다.

마지막으로 마이크로소프트 워드에 존재하는 취약점을 이용하는 워드 파일은 유포 당시의 정확한 파일명은 확인 되지 않았으나 '265,395 바이트'의 크기다.

해당 워드 파일이 이용한 'CVE-2012-0158' 취약점은 보안 권고문 'Microsoft Security Bulletin MS12-027-긴급 Windows'공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점(2664258)'을 통해 보안 패치가 배포되었다.

<V3 제품군의 진단명>

HWP/Exploit

Dropper/Exploit-HWP

Dropper/Cve-2012-0158

PDF/Exploit

Backdoor/Win32.PcClient

Dropper/Win32.OnlineGameHack

Win-Trojan/Infostealer.28672.K

Win-Trojan/Infostealer.81920.B

<TrusWatcher 탐지명>

Exploit/HWP.AccessViolation-SEH

Exploit/DOC.AccessViolation-DE

앞서 언급한 바와 같이 이번에 발견된 취약한 문서 파일들은 모두 기존에 알려진 취약점들을 악용하고 있다. 마이크로소프트와 한글과컴퓨터, 어도비는 모두 해당 취약점들을 제거할 수 있는 보안 패치들을 배포 중이다. 향후 유사한 보안 위협들로 인한 피해를 예방하기 위해서는 관련 보안 패치를 설치해야 한다.

이 밖에 더 자세한 보안 관련 통계 및 이슈에 관한 자세한 내용은 ASEC Report 홈페이지(<http://www.ahnlab.com/kr/site/securitycenter/asec/asecReportView.do?groupCode=VNI001>)을 통해서 확인할 수 있다.

발행인 : 김홍선

발행처 : 주식회사 안랩

경기도 성남시 분당구 삼평동 673

T. 031-722-8000 F. 031-722-8901

편집인 : 안랩 세일즈마케팅팀

디자인 : 안랩 UX디자인팀

Copyright(c) AhnLab, Inc. 2012 All Rights Reserved.

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지없이 변경될 수 있습니다.



<http://www.ahnlab.com>

<http://blog.ahnlab.com>

http://twitter.com/ahnlab_man



AhnLab

경기도 성남시 분당구 삼평동 673

T. 031-722-8000 F. 031-722-8901

Copyright (c) AhnLab, Inc. 2012 All rights reserved.

