

COREA

Monthly Security News Letters



December. 2010

NETSOL
S Y S T E M

Table of Contents

SECTION 1. 보안뉴스 국/내외 동향..... 3

- 1.1 정보 새지 않게 막아라" "알권리 위해 차단 맞설 것"3
- 1.2 페이스북 채팅 악성코드 주의4
- 1.3 안드로이드 Banking 앱 마구 이용시 '낭패'5
- 1.4 美 FBI, 오픈소스에 해킹코드 '심었다'? (해외)6
- 1.5 위키리크스 지지자들, 페이스북 사이버 공격 (해외).....6
- 1.6 2010년 세계 10대 보안사건 (해외).....6

SECTION 2. 보안취약점 정보(VULNERABILITY) 6

- 2.1 애플 쿼타임 플레이어 보안업데이트 권고.....6
- 2.2 BLACKBERRY DESKTOP SOFTWARE DEVICE BACKUPS ENCRYPTION WEAKNESS6
- 2.3 2010년 12월 MS 월간 보안 업데이트 권고.....6
- 2.4 PHP MULTIPLE CODE EXECUTION AND DENIAL OF SERVICE VULNERABILITIES.....6

SECTION 3. 보안 팁(TECHNOLOGY TIP & IT GOVERNANCE)..... 6

- 3.1 스마트폰의 QR(QUICK RESPONSE)CODE를 이용한 악성코드6
- 3.2 악성코드 자동 분석.....6
- 3.3 웹서버 보안 도구 -URLSCAN3.16

SECTION 1. 보안뉴스 국/내외 동향

1.1 정보 새지 않게 막아라” ‘알권리 위해 차단 맞설 것”

국제 사회와 위키리크스 간 전면전이 점입가경이다. 미국 등 국제 사회는 서버 및 도메인 차단, 결제 서비스 중단에 이어 설립자인 줄리언 어샌지 체포에 이르기까지 위키리크스에 대한 전방위 압박 수준을 높이고 있다. 이에 맞서 위키리크스 지지자들은 복사사이트(미러사이트)를 개설해 도메인 차단에 맞서는가 하면 후원금 모집 등 대대적인 반격에 나서고 있다. 특히 어샌지가 체포된 7일을 기점으로 지지와 반대 세력들이 상대에 대한 무차별적인 사이버 테러 공격에 나서는 등 양측 간 대립이 극단으로 치달고 있다.

◆‘막아라’

지난달 28일 위키리크스가 미 국무부 외교 문건을 공개하기 시작한 이래 미국 등 세계 각국이 이를 막기 위해 다양한 방법을 동원하고 있다. 첫 번째 타깃은 위키리크스의 은신처, 아마존 위키리크스 서버를 차단한 데 이어 세계 각국의 서버 및 도메인 제공업체들이 잇따라 자신들의 홈페이지 접근 봉쇄에 나섰다. 또 미국 언론 중 유일하게 위키리크스 문건을 보도해온 뉴욕타임스도 동참했다.

이어 어샌지의 계좌 폐쇄 조치로 돈줄 죄기에도 나섰다. 스위스 우체국 은행인 포스트파이낸스는 이달 초 어샌지의 계좌를 부정확한 고객 정보를 이유로 동결 조치했다. 앞서 위키리크스의 후원금 모금 수단의 하나로 알려진 페이팔도 이달 4일 불법활동을 전파하는데 이용된다는 이유로 스스로 위키리크스의 후원 계좌를 차단한 바 있다. 마스터카드와 비자도 이에 합류했다. 이 같은 움직임에도 추가 폭로가 이어지자 결국 7일 어샌지를 긴급체포하는 초강수를 뒀다. 또 최근에는 세계의 주요 해커 모임들이 어샌지의 체

포에 반발, 반위키리크스 세력에 대해 사이버 공격에 나서자 ‘대의를 위한 핵티비스트(해커+행동주의자)’라고 불리는 군 출신 해커(제스터)들이 세계 곳곳에 존재하고 있는 위키리크스 사이트를 찾아 마비시키는 등 반위키리크스와 전쟁을 선포하고 나섰다. 위키리크스 사태는 국제 사회의 지지 세력과 반대 세력 간의 전면전으로 확대되고 있는 것이다.

◆뚫어라=이 같은 외부의 압력에도 위키리크스 측은 언론 자유와 알 권리를 강조하며 문서 공개 의지를 굽히지 않고 있다. 특히 위키리크스와의 접속 통로를 열어놓으려 안간힘을 쓰고 있다. 먼저 아마존 닷컴 등의 서버 제공 중단에 맞서 스웨덴과 프랑스 등지로 서버를 분산 배치해 전열을 재정비했다. 이 같은 노력으로 실제 7일 어샌지가 구속된 이후에도 폭로가 이어지고 있다. 계좌 폐쇄 등의 조치에 대해서는 온라인 후원금 모금으로 맞서고 있다.

정보 공개 및 공유를 추진하는 일명 ‘인터넷 해적’들도 앞다퉈 속속 위키리크스 진영에 가담하고 있다. 인터넷 해적들은 어샌지의 호소에 부응해 이미 1천여 개의 ‘미러사이트’를 만들어 미국 등 세계 정부의 위키리크스 폐쇄 노력을 무력화시키고 있다. 미국 시민단체들도 속속 지원 사격에 나섰다. 미국의 최대 시민단체인 ‘유나이티드 포 비스 & 저스티스’는 7일 성명을 통해 위키리크스 서비스를 중단한 아마존 불매운동에 나서는 한편 위키리크스 지지 서명운동을 시작했다.

특히 어샌지가 체포된 후 기존의 소극적 방어수준을 넘어 위키리크스의 결제 서비스를 중단한 카드사 사이트에 대해 사이버 공격에 나서는 등 적극적인 행동에 돌입했다. ‘익명’으로 불리는 해킹그룹은 8일 거대 카드사인 마스터카드와 비자가 위키리크스에 대한 지불 결제를 중지한 데 대응해 두 카드사의 홈페이지를 공격했다. 이들의 공격으로 마스터카드는 온라인 결제

를 하기 위한 보안 암호 시스템이 수시간 동안 마비되고 비자 사이트는 일시적으로 접속이 불가능했다. 어센지의 계좌를 폐쇄한 스위스 은행과 그를 기소한 스웨덴 검찰과 정부의 웹사이트도 한때 다운됐다. 이 밖에도 트위터에는 위키리크스에 대한 충성을 서약하는 메시지가 넘쳐나고 있으며 페이스북 방문자는 100만 명을 넘어서는 등 온라인상의 위키리크스 지지자들이 급속히 뭉치고 있다.

◆ 위키리크스란?

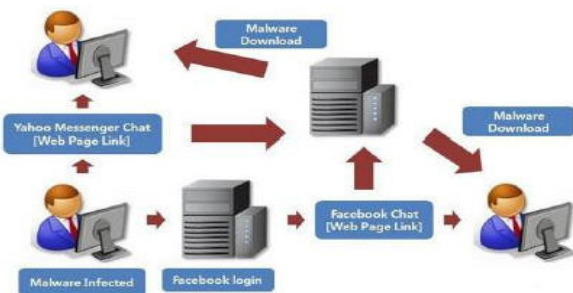
위키리크스는 정부와 다른 단체로부터 온 민감한 문서를 누설하는 웹사이트로 2006년 12월에 처음 문을 열었으며 2007년 1월에 처음 웹상의 대중에게 공개됐다. 위키리크스는 흔히 협업 문서 작업에 쓰이는 위키 기반의 사이트다. 백과사전 위키피디아와 구조는 비슷하다. 누구나 글을 쓰고 링크를 걸고 수정할 수 있다. 정보 제공자를 보호하기 위해 스웨덴과 아이슬란드 등 취재원 보호가 보장된 나라에 서버를 두고 있다. 위키리크스는 미국 외교 전문 등 그동안 수많은 비밀 문서들을 공개해 파문을 일으키고 있다.

[원문출처]

(매일경제 - 최창희기자)

http://www.imaeil.com/sub_news/sub_news_view.php?news_id=50018&yy=2010

1.2 페이스북 채팅 악성코드 주의



▲ 페이스북 채팅 메시지로 전파되는 악성코드 유포도식도

지난달 인터넷을 뜨겁게 달군 악성코드는 ‘페이스북 채팅 메시지로 유포되는 악성코드’인 것으로 나타났다.

안철수연구소(대표 김홍선)는 13일 ‘시큐리티대응센터(ASEC) 보고서 11월호’를 통해 SNS인 페이스북의 채팅 메시지를 통해 유포되는 악성코드가 국내에서도 계속 확인되고 있다고 경고했다.

그간 악성코드가 페이스북의 쪽지로 널리 유포됐으나 이번에는 채팅메시지로 악의적인 링크를 보내 페이스북 사용자 감염을 유도하는 형태의 악성코드 유포 방식이 등장했다고 안철수연구소 측은 설명했다.

안철수연구소 측은 “페이스북 채팅 메시지로 인한 악성코드 전파는 과거 메신저 웜의 전파 방식과 유사하지만 페이스북 채팅 메시지로 링크를 전달받은 경우 사용자가 의심하지 않고 클릭해 감염이 확산되고 2차 피해가 커진다”고 말했다.

이 회사 전성학 ASEC센터장은 “최근 SNS 사용자 급증함에 따라 이를 겨냥한 악성코드 유포가 적지 않다”며 “페이스북·트위터 등을 통해 전달된 의심스러운 URL 또는 단축 URL 등은 발신인을 확인하고 클릭하는 것이 좋다”고 말했다.

그는 “특정 애플리케이션이 페이스북 계정의 권한을 요구할 때는 필요한 애플리케이션인지 다시 한번 확인하고 설치하는 것이 안전하다”고 당부했다

이외에도 안철수연구소는 지난달 G20 국제행사, 노벨 평화상 시상식, 아시안게임, 경찰청 등을 사칭한 이메일에서 악성코드가 발견됐고 이 같은 사회공학적 방법의 악성코드 전파를 주의하라고 전했다.

한편 지난 11월 월별 악성코드 감염 보고 건수는 1326만건으로 지난 10월 1173만건에 비해 152만건 증가했다. 이중 트로이잔이 72%로 1위를 차지했으며 스크립트가 10%, 애드웨어가 6%를 차지한 것으로 나타났다

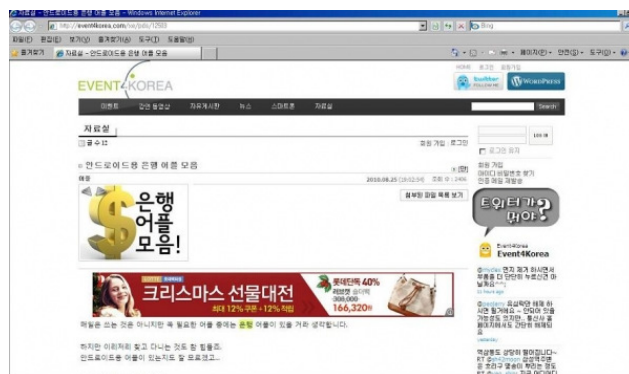
반면 웹사이트에서 악성코드가 발견된 건수는 지난 11월 약 8만 5000건이므로 전달 10만건에 비해 다소 감소했다.

[원문출처]

(보안뉴스- 장윤정기자)

<http://www.boan.com/news/articleView.html?idxno=3688>

1.3 안드로이드 뱅킹앱 마구 이용시 '낭패'



▲ 출처가 불분명한 개인이 올려둔 은행 어플들을 현재 웹 사이트에서 쉽게 찾을 수 있다

안드로이드 마켓에 올라간 금융기관의 뱅킹 애플리케이션(이하 앱)이 사용자 계좌에서 돈을 해킹하는 도구로 전략할 개연성이 높은 것으로 지적됐다.

해커가 정상 뱅킹 앱을 내려 받아 변조한 앱으로 다시 올리면 이를 무심코 내려 받은 사용자의 금융 정보를 가로 챌 수 있기 때문이다.

숭실대학교 이정현 교수(컴퓨터학부)는 안드로이드 마켓 등록 절차는 애플의 앱스토어와 달리 25달러를 지불하고 개발자 본인이 셀프 사인(개인 인증)한 앱을 마음대로 올릴 수 있는 데 해커가 이같은 허점을 노릴수 있다고 14일 말했다.

즉, 해커가 정상적인 뱅킹 앱의 코드를 일부 변조해 셀프 사인한 후 재등록하면 안드로이드 마켓에선 이를 정상 앱으로 인정하고 다시 이를 내려 받아 계좌 이체 서비스에 사용하면 지정된 사용자가 아닌 해커의 계좌로 송금된다는 것이다.

실제, 이정현 교수는 안드로이드 마켓의 운영 허점을 이용해 정상적인 국내 27개 금융기관 뱅킹 앱을 변조한 후 해커의 계좌로 송금하는 해킹 과정을 최근 세미나에서 시연을 통해 입증했다.

이 교수는 “구글이 앱의 등급을 다양하게 설정, 셀프 사인한 뱅킹 앱을 설치하지 못하도록 하는 근본적인 대책이 필요하다”며 “행안부도 이러한 취약점을 인식하고 적절한 대안을 찾기 위해 구글코리아와 논의 중인 것으로 안다”고 설명했다.

각종 인터넷 카페·블로그에서 사용자간 앱을 서로 주고받는 행동도 자제해야 한다. 현재 각종 검색 사이트에서 ‘안드로이드 은행 앱’이란 검색어를 치면 인터넷 카페·블로그 등에 개인이 올려놓은 은행 앱을 어렵지 않게 찾을 수 있다.

안철수연구소 이성근 책임연구원은 “은행 앱을 간편히 다운받기 위해 카페나 블로그에 올린 뱅킹 앱을 의심 없이 다운받아 이용하는 경우가 많은데 보안을 미검증한 앱을 사용하면 자칫 큰 금전적 피해를 입을 수 있다”고 경고했다.

그는 또, “뱅킹 앱은 반드시 지정된 금융기관의 홈

페이지에서 내려 받아 사용하고 안드로이드 마켓에서 banking 앱을 내려 받을 땐 다운로드 횟수·이용자들 사용 후기·개발자 주소 등을 자세히 살피는 세심한 주의가 필요하다”고 덧붙였다.

[원문출처]

(보안뉴스- 장윤정기자)

<http://www.boan.com/news/articleView.html?idxno=3695>

1.4 美 FBI, 오픈소스에 해킹코드 ‘심었다’?(해외)

미국 연방수사국(FBI)이 오픈소스 운영체제 ‘오픈BSD’에 백도어 코드를 심어 해킹을 시도했다는 의혹이 일면서 미국 보안 커뮤니티가 술렁이고 있다.

15일(현지시간) IT전문미디어 씨넷에 따르면 미국 보안 관련 커뮤니티 사이에서는 FBI 오픈소스 백도어 의혹이 알려지면서 오픈소스 감시를 강화하자는 목소리와 사실이 아닐 것이라는 의견이 팽팽히 맞서고 있다.

FBI 오픈소스 백도어 의혹은 지난 14일 FBI에 협력했다고 주장하는 한 IT 개발자가 “오픈BSD에 다수의 백도어 코드를 심어 넣었다”고 주장한 메일에서 비롯됐다.

이메일을 보낸 주인공은 네트워크 시큐리티 테크놀로지(NETSEC)에서 근무하던 그레고리 페리라는 개발자다. 페리씨는 “FBI와 10년 동안 유지하기로 한 비밀 보장계약 기한이 종료됐다”며 오픈BSD 설립자 테오드 라트에게 백도어 관련 내용이 담긴 이메일을 보냈다.

페리씨는 씨넷과의 인터뷰에서 “FBI 프로젝트가 끝난

직후 회사를 매각했다”며 “당시 프로젝트는 법률을 위반한 것”이라고 주장했다. 페리씨의 주장에 따르면 관련 프로젝트는 지난 1999년 미 국방부 산하 안전보장국(NSA) 주도 아래 진행됐다.

오픈BSD 프로젝트는 보안 기능이 강력한 것으로 알려졌으며 과거 국방위고등연구계획국(DARPA)가 자금을 지원하기도 했다. DARPA는 지난 2003년 이유없이 지원을 중단했다.

오픈BSD 코드는 탁월한 보안 기능으로 마이크로소프트를 비롯해 독일, 스위스 업체 등이 방화벽에도 적용됐다.

페리씨의 주장에 대해 전 FBI 수사관도 동조하고 나섰다. 힐버트라는 전 FBI 수사관은 트위터에 “FBI는 실제로 오픈BSD 프로젝트를 진행했었다”며 “그러나 프로젝트는 실패로 끝났다”는 글을 올리기도 했다.

[원문출처]

(지디넷코리아- 송주영기자)

<http://www.zdnet.co.kr/Contents/2010/12/16/zdnet20101216170450.htm>

1.5 위키리크스 지지자들,페이팔 사이버 공격 (해외)

폭로전문 웹사이트 위키리크스의 후원계좌 접근을 차단한 온라인 대금결제 및 송금서비스업체인 페이팔이 사이버공격을 당한 것으로 확인됐다고 미 경제전문지 포브스 인터넷판이 사이버보안업체인 팬더 랩스를 인용해 6일(이하 현지시간) 보도했다.

보도에 따르면 이번 공격은 페이팔이 지난 3일 자정 직전에 블로그를 통해 “위키리크스가 불법활동에 종사하는 사람들을 격려하거나 돕고, 불법활동을 전파하

는데 페이팔이 사용될 수 없도록 돼 있는 규정을 어겼다고 판단해 후원계좌접근을 차단한다"고 발표한 후 몇시간 만에 일어났다.

자신들을 `익명(Anonymous)` 이라고 칭한 해커집단은 위키리크스 관련 발표를 한 블로그의 서버를 공격했으며 4일 오전 4시께 이 사이트는 가동을 멈췄다.

`익명`의 트위터 계정은 "위키리크스의 후원계좌 접근을 차단한 페이팔 블로그(thepaypalblog.com)를 차단했다"고 주장하는 글을 게시했다.

`작전:페이팔`이라고 명명된 이번 공격은 이후에도 8시간 이상 계속됐으며, 페이팔 블로그는 4일 오후 1시30분이 돼서야 정상 가동됐다.

페이팔은 그러나 이번 공격 등에 대한 확인요청에 답하지 않았다고 포브스는 전했다.

이들 해커는 다음 공격목표로 위키리크스에 제공했던 서버와 도메인 서비스를 중단한 아마존과 미국의 도메인제공업체 에브리DNS, 프랑스 내 서버제공업체에 압력을 가한 프랑스 정부 등을 지목했다. 이들은 트위터에 연결된 `작전:복수`라는 한 사이트에 "우리는 위키리크스와 긴밀한 관계를 맺고 있는 것은 아니지만 같은 대의명분을 위해 싸우고 있다. 우리는 투명성을 원하고 검열에 반대한다"고 말했다.

이들은 "위키리크스를 침묵하게 만드는 시도는 우리가 생각하는 것을 말할 수 없게 하고, 우리의 주장과 아이디어를 표현하지 못하게 하는 세계에 맞달아있다"고 주장했다.

[원문출처]

(보안닷컴)

<http://www.boan.com/news/articleView.html?idxno=3650>

1.6 2010년 세계 10대 보안사건 (해외)

오래된 구문이지만 2010년에 발생한 보안 업계의 혼란스러운 사건들을 언급할 때 SNAFU(Situation Normal All Fked Up)이라는 표현이 가장 어울린다.

영망진창 대혼란을 일으켰던 2010년 보안 업계의 10대 뉴스를 2일 네트워크월드가 선정, 발표했다.

1. 오로라 공격

지난 1월 구글은 지난 2009년 12월 네트워크를 통해 자사의 지적 재산을 도난당했다고 인정하면서, 이른바 '오로라 공격(Aurora attacks)'이라는 사이버 공격의 진원지가 중국임을 암시했다.

중국 정부는 이에 대해 전면 부인했으나 구글은 이 사이버 공격에 격분하며 중국내 서비스 전격 철수하겠다고 나서는 등 소동이 일어났다. 하지만 구글은 연말 중국 라이선스를 갱신하고는 중국의 검열을 받아들였다.

2. 중국 ISP의 인터넷 리라우팅

중국의 IDC 차이나 텔레커뮤니케이션이라는 소규모 ISP가 허위 경로 데이터를 전송해 인터넷을 짧은 시간 하이재킹하고 이를 국영 차이나 텔레커뮤니케이션즈로 재전송하며 전세계의 서비스 제공업체에 영향을 미쳤다. 이 사태는 11월 국회에 제출된 '2010년 미국-중국경제안보검토' 위원회 보고서에서 언급됐다.

차이나 텔레콤은 4월의 트래픽 경로 변경이 단순한 사고라면서 의도적인 해킹이 아니라며 이러한 의혹을 전면 부인했다

3. 맥아피의 결함있는 백신 유포

보안전문 회사 맥아피가 결함 있는 안티바이러스 업데이트를 유포했다. 'McAfee DAT file 5958'이라

는 파일은 마이크로소프트의 블루스크린 같은 기능과 DoS 효과로 수많은 맥아피 고객들의 PC를 망가뜨렸다. 맥아피는 CEO가 머리숙여 사과하며 갖가지 해결책을 내놓았지만 고객들의 불만은 사그라들지 않았다.

4. 시스코의 쇼타임

시스코 라이브 2010 이용자 컨퍼런스의 참가자 명단이 해킹됐다. 시스코는 자세한 언급을 꺼리고 있지만 한 거래 기업이 '행사 사이트인 'ciscolive2010.com'을 통해 참가자 정보에 접근하려는 예기치 않은 시도가 있었음을 시스코에 알렸다. 시스코는 이 유출을 신속히 차단했지만 명단 일부가 유출됐다.

노출된 정보는 시스코 라이브 행사 명찰 번호, 이름, 직위, 회사 주소 및 이메일 주소 등의 참가자 개인정보다. 시스코는 행사 참가자들에게 이메일을 통해 사과했다.

5. 구글 스트리트 뷰 사건

구글이 전 세계를 대상으로 한 스트리트 뷰 촬영차 프로젝트(Street View car projects)를 진행하면서 지도 서비스에 쓰일 정보를 수집하기 위한 목적으로 암호화되지 않은 Wi-Fi 네트워크에서 개인으로부터 데이터를 무선으로 스니핑하고 수집한 것에 대해 사과했다.

또한 구글은 수집한 데이터를 폐기하겠다고도 약속했지만 미국, 유럽, 아시아 등 각지에서 정부의 규제와 프라이버시 보호 단체들의 격렬한 항의를 받았다.

6. 아이패드 해킹

자칭 고츠 시큐리티(Goatse Security)라는 해커 집단이 AT&T의 한 웹 애플리케이션의 보안 결함을 악용해 아이패드 고객 10만 명 이상의 이메일 주소 기록을 유출시켰다. FBI는 이 해커들 중 한 명을 마약 관련 범죄 혐의로 체포했다.

7. 건강하지 않은 보안

미국 매사추세츠의 사우스쇼어(South Shore) 병원이 15년치에 해당하는 환자, 거래 기업, 직원의 건강 및 금융 정보와 연관된 약 80만 건의 파일을 분실했다. 하지만 자료를 분실한 대상에게 개별적으로 접촉하겠다는 처음의 발표와 달리 데이터 유출로 피해를 입은 개인들에게 이를 알리지 않아 문제가 됐다. 매사추세츠 검찰 측은 사우스쇼어 병원에 이를 시정토록 하고 각 개인에게 통지 하도록 촉구했다.

8. 스파이 드라마

러시아 스파이 안나 채프먼(Anna Chapman)은 미국에서 다른 10여명의 러시아 스파이와 함께 FBI에게 체포되어 스파이 교환을 통해 모스크바로 송환됐다. 이후 안나는 모스크바의 한 잡지에서 검은 란제리의 도발적인 포즈의 사진을 찍었다.

안나는 IT 지식이 별로 없음에도 불구하고 한 러시아 은행의 IT 혁신 담당으로 일했으며 FBI는 안나를 감시하는 동안 그녀의 무선 네트워크를 일상적으로 스니핑했다. 심지어 안나는 미국의 비밀 첩보원에게 자신의 노트북 수리를 맡기기까지 했다. 그런 그녀가 러시아로 귀환하자 러시아의 은행인 폰드서비스뱅크가 IT 기술 혁신을 위해 그녀를 고용한 것을 두고 웃음거리가 됐다.

9. 스텍스넷

스텍스넷(Stuxnet) 웜은 SCADA(Supervisory Control and Data Acquisition) 시스템을 겨냥한 멀

웨어로서 주로 이란의 핵 시설을 겨냥한 것으로 밝혀졌다.

이란의 핵폭탄 제조 시도를 저지하는 사이버 전쟁 무기로 쓰인 스텍스넷은 이란의 최대 3만개에 이르는 시스템에 영향을 끼쳤음이 확인됐다.

이어 11월 마흐모드 아마디네자드(Mahmoud Ahmadinejad) 대통령은 이란의 적들이 스텍스넷이 일부 원심분리기에 문제를 야기하는데 성공했다'고 밝히면서 이를 '사악한 행위'라고 맹비난했다.

10. 위키리크스의 귀환

미국 국무부 대외 관계와 관련된 각종 외교 통신문과 세계 지도자들의 공공연한 비밀을 담고 있는 25만 건 이상의 메시지가 위키리크스에서 공개됐다.

힐러리 클린턴 국무장관은 이를 '공격'이라고 부르는 한편 전 세계의 상대국에게 데이터 유출에 대해 서둘러 사과를 표명했다. 2

5만 건의 국무부 문건에서 발견된 정보 중에는 중국 정부가 구글에 대한 사이버 침입을 지시했음을 밝힌 문건이 있다. 중국 정부는 이를 전면 부인했다. 현재 유출된 국무부 전문이 게시되어 있는 위키리크스 웹사이트로의 접속은 차단된 상태다.

[원문출처]

(보안닷컴- 장윤정기자)

<http://www.boan.com/news/articleView.html?idxno=3635>

SECTION 2. 보안취약점 정보(Vulnerability)

2.1 애플 쿼타임 플레이어 보안업데이트 권고

□ 개요

○ 애플사는 악성코드 전파에 악용될 수 있는 다수의 취약점에 대한 보안업데이트를 포함하는 애플 쿼타임 플레이어 7.6.9를 발표[1]

○ 국내 쿼타임 플레이어 이용자는 보안업데이트가 포함된 최신 버전으로 업데이트할 것을 권고

□ 해당시스템

○ 애플사는 아래와 같은 취약점에 대한 보안업데이트를 포함하는 쿼타임 플레이어 7.6.9를 발표함

- 악의적으로 제작된 JP2 이미지 파일을 처리하는 과정 중 버퍼오버플로우가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3787)[2]

- 악의적으로 제작된 JP2 이미지 파일을 처리하는 과정 중 초기화 되지 않은 메모리영역에 접근하는 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3788)[3]

- 악의적으로 제작된 동영상파일(.avi)를 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3789)[4]

- 악의적으로 제작된 동영상파일(.mov)를 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3790)[5]

- 악의적으로 제작된 MPEG 인코딩 파일

(.mpg,mp3,mp4등)을 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3791, CVE- 2010- 3792)[6,7]

- 악의적으로 제작된 Sorenson 인코딩 파일을 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3793)[8]

- 악의적으로 제작된 FlashPix 이미지 파일을 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3794)[9]

- 악의적으로 제작된 GIF 이미지 파일을 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3795)[10]

- 악의적으로 제작된 PICT 이미지 파일을 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3800)[11]

- 악의적으로 제작된 FlashPix 이미지 파일을 처리하는 과정 중 초기화 되지 않은 메모리 영역에 접근하는 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3801)[12]

- 악의적으로 제작된 QTVR 파일을 처리하는 과정 중 메모리 손상 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 3802)[13]

- 악의적으로 제작된 MPEG- 4(.mp4)파일을 처리

하는 과정 중 버퍼 오버플로우 문제가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음 (CVE- 2010- 1508)[14]

- 쿼타임을 이용하여 다른 컴퓨터에 비정상적인 접근이 가능하므로 중요한 정보가 유출될 수 있음 (CVE- 2010- 0530)[15]

- 악의적으로 제작된 동영상파일(.mov)를 처리하는 과정 중 정수 오버플로우가 발생하여 응용프로그램이 비정상 종료되거나 임의코드실행이 가능하여 이용자 PC에 악성코드가 감염될 수 있음(CVE- 2010- 4009)[16]

□ 업데이트 방법

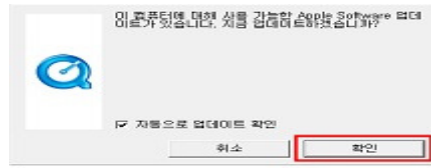
o Adobe Shockwave Player 11.5.8.612 이하 버전 (윈도우, 맥킨토시)

□ 해결 방안

o 애플 쿼타임 플레이어 실행 후 “도움말 > 기존의 소프트웨어 업데이트” 클릭



o 다음과 같은 업데이트 확인창이 뜨면 “확인” 버튼을 클릭하여 업데이트



□ 용어 정리

o JP2 이미지 파일 : JPEG파일(이미지 파일)을 개선한 JPEG2000의 이미지 파일

o MPEG(Moving Picture ExpertsGroup, 동영상 전문가 그룹) : 비디오와 오디오등 압축을 위한 표준 규격

o Sorenson : Sorenson Media라고 하는 회사에서 개발한 비디오 코덱

o FlashFix 이미지 파일 : 비트맵 형태의 그림파일

o PICT 이미지 파일 : 매킨토시에서 이미지를 처리하는 표준 파일 포맷

o QTVR(QuickTime Virtual Reality) : 쿼타임에서 VR(가상현실)타입의 이미지를 지원하는 포맷

□ 참고 사이트

- [1] <http://support.apple.com/kb/HT4447>
- [2] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3787>
- [3] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3788>
- [4] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3789>
- [5] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3790>
- [6] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3791>
- [7] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3792>
- [8] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3793>
- [9] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3794>
- [10] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3795>
- [11] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3800>
- [12] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3801>
- [13] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3802>
- [14] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-1508>
- [15] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0530>
- [16] <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-4009>

2.2 BlackBerry Desktop Software Device Backups Encryption Weakness

□ 개요

BlackBerry Desktop Software에서 원격 공격자에 의해 중요 정보를 획득할 수 있는 취약점이 발견됨. 이는 BlackBerry의 장치 백업 파일의 암호화 어플리케이션에 관련된 에러 때문에 발생하며, 이를 통해 악의적인 사용자가 무작위 대입공격(Brute-force attack)에 의해 백업 파일을 복호화 할 수 있음.

□ 해당 시스템

- o BlackBerry Desktop Software version 4.7 (PC OS)
- o BlackBerry Desktop Software version 5.0 (PC OS)
- o BlackBerry Desktop Software version 6.0 (PC OS)
- o BlackBerry Desktop Software version 1.0 (Mac OS)

□ 해결 방안

- o BlackBerry Desktop Software 의 업그레이드
 - Upgrade to BlackBerry Desktop Software (PC OS)
 - Upgrade to version 6.0.1 or later
 - Upgrade to BlackBerry Desktop Software (Mac OS) - Upgrade to version 2.0 or later

□ 참고 사이트

- [1] <http://www.vupen.com/english/advisories/2010/3262>
- [2] <http://www.blackberry.com/btsc/KB24764>

2.3 2010년 12월 MS 월간 보안 업데이트 권고

2010년 MS社에서 MS10- 087~ 089 12월간 보안패치 내용입니다. [12/01~12/21 기준]

- [MS10- 090] Internet Explorer 누적 보안 업데이트
- [MS10- 091] Open Type Font 드라이버 취약점으로 인한 원격코드실행 문제점
- [MS10- 092] Task Scheduler 취약점으로 인한 권한 상승 문제
- [MS10- 093] Movie Maker 취약점으로 인한 원격코드 실행 문제
- [MS10- 094] Media Encoder 취약점으로 인한 원격코드 실행 문제
- [MS10- 095] 윈도우 취약점으로 인한 원격코드실행 문제
- [MS10- 096] Address Book 취약점으로 인한 원격코드 실행 문제
- [MS10- 097] Internet Connection Signup Wizard 취약점으로 인한 원격코드실행 문제
- [MS10- 098] Kernel- Mode 드라이버 취약점으로 인한 권한상승 문제
- [MS10- 099] Routing 및 Remote Access NDPProxy 컴포넌트 취약점으로 인한 권한상승 문제
- [MS10- 100] Consent User Interface 취약점으로 인한 권한상승 문제
- [MS10- 101] Netlogon 서비스 취약점으로 인한 서비스거부 문제
- [MS10- 102] Hyper- V 취약점으로 인한 서비스거부 문제
- [MS10- 103] MS Publisher 취약점으로 인한 원격코드 실행 문제
- [MS10- 104] MS SharePoint 취약점으로 인한 원격코드 실행 문제
- [MS10- 105] MS Office Graphics Filter 취약점으로 인한 원격코드실행 문제

[MS10- 106] MS Exchange Server 취약점으로 인한 서비스거부 문제

□ 참고 사이트

<http://www.microsoft.com/technet/security/Bulletin/MS10-0090~106.msp>

2.4 PHP Multiple Code Execution and Denial of Service Vulnerabilities

□ 개요

o PHP에서 보안 제한을 우회하거나 서비스 거부 공격을 일으킬 수 있는 다수의 취약점이 발견됨.

- 1) zip 방식의 압축 방식에 관련된 에러로 인해 서비스 거부 공격을 발생시킬 수 있음
- 2) NULL 캐릭터가 포함된 경로를 처리할 때 발생하며 보안 제한을 우회할 수 있음
- 3) imap 확장자에서의 double free(메모리 할당) 에러에 의해 발생하며 특정 코드를 실행시킬 수 있음
- 4) "ZipArchive::getArchiveComment" 에서의 NULL 포인터 역참조 에러에 의해 발생하며 서비스 거부 공격을 발생시킬 수 있음
- 5) "open_basedir"에 관련된 오류로 보안 제한 우회시킬 수 있음
- 6) "phar_stream_flush()"에서의 포맷스트링 에러로 임의 코드를 실행시킬 수 있음
- 7) 해상도 지원에 관련된 에러가 존재함
- 8) "filter_var"에 관련된 에러로 서비스 거부 공격을 일으킬 수 있음

□ 해당 시스템

o PHPversions prior to 5.3.4

□ 해결 방안

o PHP version 5.3.4 로의 업그레이드

- <http://www.php.net/downloads.php>

□ 용어 정리

o PDF(Portable Document Format) : Adobe社가 개발한 다양한 플랫폼을 지원하는 전자문서 파일 형식

o Adobe Acrobat : PDF 문서 편집/제작을 지원하는 상용 프로그램

o Adobe Reader : PDF 문서의 편집 기능은 없이 보기/인쇄만 할 수 있는 무료 프로그램

□ 참고사이트

[1] <http://www.vupen.com/english/advisories/2010/3168>

[2] http://www.php.net/releases/5_3_4.php

SECTION 3. 보안 팁(TECHNOLOGY TIP & IT GOVERNANCE)

3.1 스마트폰의 QR(Quick Response)Code를 이용한 악성코드

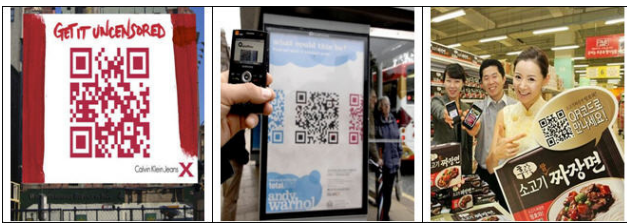
□ 개요

최근 스마트폰 이용자가 증가하면서 QR Code의 사용 빈도가 높아지고 있습니다. 하지만 QR Code는 SNS의 단축URL과 동일하게 Cross Site Script 및 악성코드 유포 등의 공격에 악용될 수 있기 때문에 사용자들의 주의가 필요합니다. QR Code에 대해 알아보고 어떠한 취약점이 존재하는지 확인하여 그 대응방안에 대해 알아보려고 합니다.

□ QR Code란?

QR Code는 바코드의 기능을 확장한 2차원 코드로 1994년 일본 도요타의 자회사인 Denso-Wave에서 만들었으며 QR Scanner, 카메라, 휴대전화, 스마트폰으로 인식이 가능합니다.

이 코드는 흰 바탕에 사각형 모양으로 배열된 검은 모듈로 구성되어 있습니다. 인코딩 정보는 텍스트, URL 등을 포함할 수 있습니다. (출처- Wikipedia)



[그림 1] QR Code를 활용한 마케팅

바코드보다 방대한 자료의 표현이 가능하며 특정 URL정보를 담아 QR Code를 생성하여 스마트폰의 QR Code Scanning 어플리케이션으로 해당 QR Code를 찍게 되면 자동으로 해당 URL에 접속이 가능합니다.

QR Code 활용 예, 명함, 이메일, 전화번호 기록, 상품의 QR Code를 통한 이벤트 참여, 상세정보, 구매자 리뷰보기, 어플리케이션 구매를 위한 APP Market 접속



[그림 2] QR Code 활용 사례

이러한 QR Code는 인터넷에서 생성기를 구해 쉽게 제작 할 수 있으며 국내 유명 포털 사이트에서도 QR Code 생성 서비스를 제공하고 있습니다.



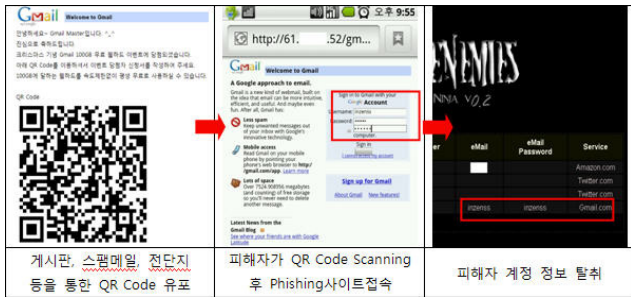
[그림 3] QR Code 생성기

QR Code를 보는 것만으로는 해당 QR Code의 숨겨진 의도를 전혀 파악 할 수 없으며 QR Code Scanning 어플리케이션의 종류에 따라 사용자가 접속 URL을 확인하지 못한 채 자동으로 접속하게 됩니다. 또한 온라인/오프라인 모두를 통해 악의적으로 제작된 QR Code를 유포할 수 있습니다. 이를 악용하여 악성 URL에 접속하도록 제작되어 유포된 QR Code를

스마트폰 사용자가 Scanning한다면 사용자의 확인을 거치지 않고 악성 URL에 접속이 가능하여 아래와 같은 취약점이 존재 할 수 있습니다.

a. Phishing사이트와 Cookie 탈취(XSS Attack)로 인한 개인정보 유출

사용자를 현혹하는 광고성 스팸메일, 게시판, 전단지 등을 통해 Phishing사이트 URL을 포함한 QR Code를 유포하여 개인정보가 유출될 수 있습니다.



[그림 4] Phishing사이트

b. 악성파일 유포

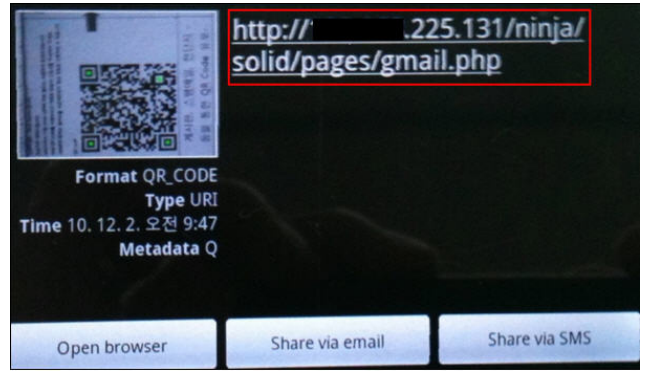
악성파일 제작자가 악성파일 다운로드 URL에 접속하는 QR Code를 유포해 스마트폰 사용자들이 주의를 기울이지 않고 접속하여 해당 악성파일을 다운로드, 설치하게 된다면 개인정보 유출 및 DDoS 공격에 악용되는 좀비스마트폰이 될 수 있습니다.



[그림 5] 악성파일유포

□ 예방 및 대응방안

다양한 QR Code Scanning 어플리케이션이 존재하며 [그림 6]과 같이 자동으로 URL에 접속하지 않고 사용자에게 URL을 확인하는 절차를 가진 어플리케이션을 사용합니다.



[그림 6] URL확인

스팸메일, 광고성 게시글 등 주로 사회공학적 기법을 이용해 사용자가 QR Code를 Scanning하도록 유도하므로 출처가 불확실한 QR Code를 Scanning하지 않도록 주의를 기울여야 합니다.

3.2 악성코드 자동 분석

□ 개요

정보보호 전문 업체 판다시큐리티는 2010년 1월에서부터 2010년 10월까지 10개월에 이르는 동안 발견된 악성 코드가 지금까지 발견된 전세계 악성코드의 1/3에 달한다고 밝혔습니다. 악성코드는 지속적으로 신종 및 변종이 발견되고 있으며, 블랙마켓의 활성화로 인하여 더욱 많은 악성코드가 발생할 것으로 예측되고 있습니다.

악성코드에 대항하는 움직임 또한 활발하게 이뤄지고 있으나, 악성코드의 증가 및 변화가 너무나 빠르게 진행되고 있기 때문에 의심 파일에 대한 빠른 대처를 위해 사용자의 확인이 필요합니다.

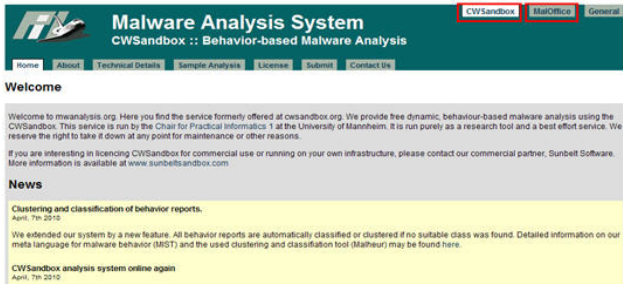
이에 인젠시큐리티서비스에서는 악성코드를 분석하여 리포트를 제공해주는 사이트를 소개하고, 기능 및 확인해야 할 사항들을 소개하도록 하겠습니다.

□ mwanalysis.org

인터넷 주소창에 <http://mwanalysis.org> 주소를 입력

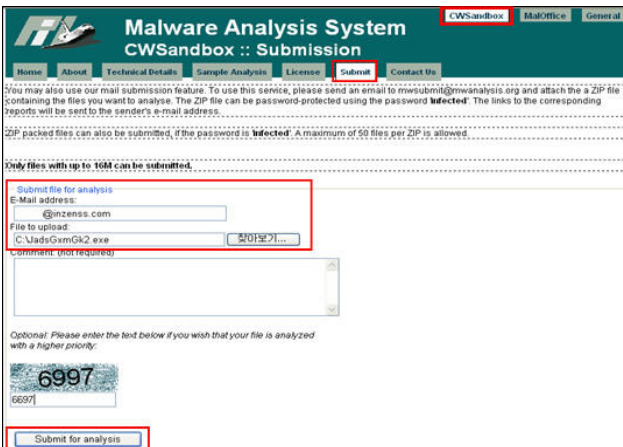
하면 [그림 1]과 같은 화면을 확인할 수 있습니다. mwanalysis에서는 CWSandbox와 MalOffice 메뉴를 제공합니다.

CWSandbox 항목에서는 PE(Portable Executable) 악성코드에 대한 분석을 제공하며, MalOffice 항목에서는 Word, Excel, PowerPoint, PDF 등 오피스 파일의 분석을 제공합니다



[그림 7] http://mwanalysis.org

□ CWSandbox를 이용한 악성코드 동적분석
CWSandbox 항목을 클릭한 후 “Submit”를 선택합니다. 채증한 악성코드를 선택한 후 분석결과를 받을 이메일 주소를 입력합니다. 그 후 “Submit for analysis”를 클릭합니다.



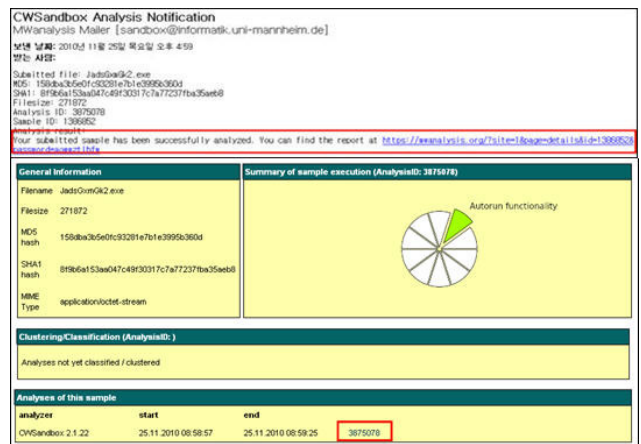
[그림 8] Upload Malware

분석결과는 입력한 이메일로 전송되며 해당 메일에 포함된 링크를 클릭하게 되면 분석 결과를 확인 할 수 있습니다.



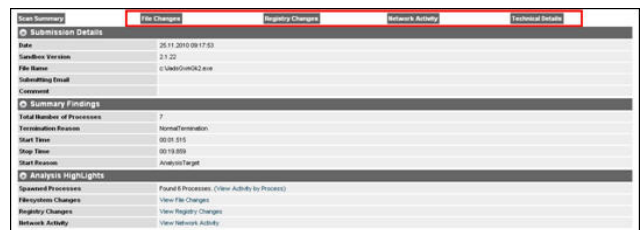
[그림 9] 이메일확인

위의 링크를 클릭하면 [그림 4]와 같이 악성파일의 MD5값 등 간단한 정보가 나오며 “Analyses of this sample” 항목의 오른쪽 숫자를 클릭하면 상세 분석 결과를 확인 할 수 있습니다.



[그림 10] General Information

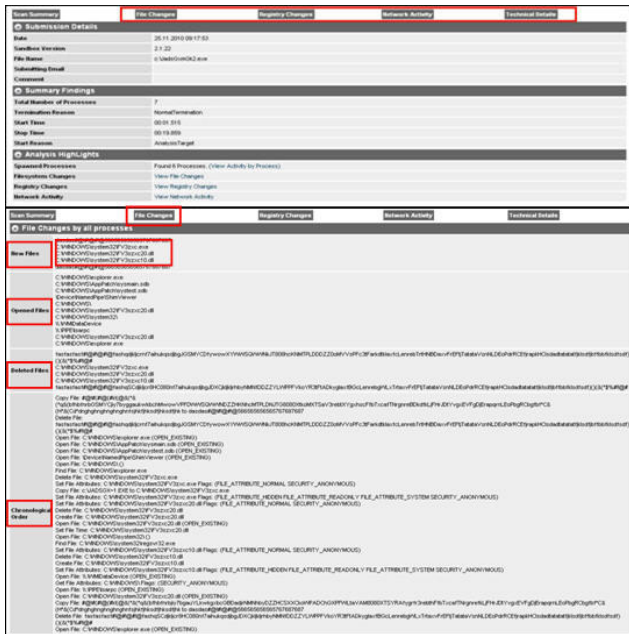
상세분석 메뉴를 통해 파일/레지스트리/네트워크활동/프로세스 동작 상태를 확인 할 수 있습니다.



[그림 11] 상세분석 메뉴

□ File Chagnes
“File Chagnes” 항목을 통해 악성코드가 생성/삭제/접근한 파일들의 정보를 확인 할 수 있습니다. 또한 File system의 변화과정도 볼 수 있습니다. 악성코드가 생성한 파일명들로 이루어 보아 최근 유

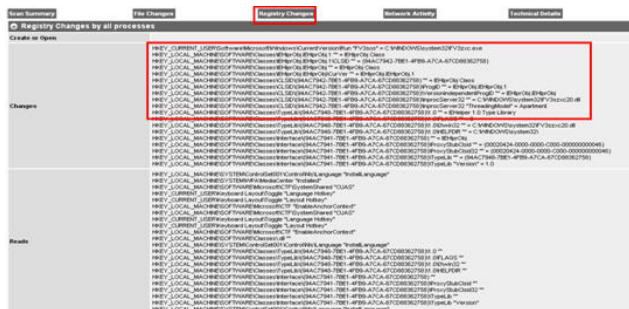
행 중인 온라인게임계정 탈취 목적의 악성코드로 추정됩니다.



[그림 12] File Changes

□ Registry Changes

“Registry Changes” 항목은 레지스트리의 변화를 확인할 수 있으며 해당 악성코드는 자동실행을 위해 인터넷익스플로러의 BHO로 등록하는 작업을 하는 것으로 추정할 수 있습니다.



[그림 13] Registry Changes

□ Network Activity

“Network Activity” 항목은 분석을 의뢰한 의심 파일의 네트워크 활동에 대한 리포트를 보여주는 것으로 외부 서버로부터 악성 파일 다운로드 여부, 의심스러

운 외부 IP와의 통신 여부 등을 확인할 수 있습니다. 현재 분석한 파일은 네트워크 활동이 없는 것으로 확인되었습니다.

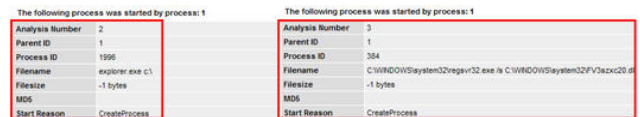


[그림 14] Network Activity

□ Technical Details

“Technical Details” 항목은 분석한 파일의 상세 정보를 확인할 수 있으며, 레지스트리, 프로세스의 생성 및 종료, 쓰레드의 생성, 가상 메모리의 사용, 사용되는 DLL 모듈 등이 나타나게 됩니다.

또한, 분석한 파일이 다른 파일을 드랍한다면, 드랍된 파일들까지 분석을 수행해서 정보를 나타내줍니다.



[그림 15] 드랍된 파일 분석

□ Virus Total 이용한 백신탐지 검사

VirusTotal(www.virustotal.com) 서비스를 이용해 의심스러운 파일의 백신프로그램 탐지여부로 악성파일인지 확인할 수 있습니다. 하지만 변종 및 신종 악성코드는 백신프로그램에서 탐지를 못할 수 있으므로 검사파일이 백신프로그램에 탐지가 되지 않더라도 정상파일로 확인해서는 안됩니다. CWSandbox로 분석한 파일을 VirusTotal로 검사한 결과 온라인게임핵 종류로 명명하고 있습니다



[그림 16] VirusTotal

□ 결론

상기 사이트 외에도 <http://www.iseclab.org>,

http://www.threatexpert.com,
http://camas.comodo.comodo.com 등 악성코드를
자동으로 분석해 주는 유사한 사이트들이 존재합니다.
이러한 서비스의 결과를 100% 신뢰 할 수는 없지만
의심스러운 파일의 전반적인 행위 분석이 필요할 경
우 사용한다면 유용한 도구가 될 것으로 판단됩니다.

3.3 웹서버 보안 도구 - *UrlScan3.1*

□ 개 요

최근 악성코드의 대부분은 취약한 웹서버의 해킹을
통해 유포되고 있습니다. Cross Site Script, Mass
SQL Injection 등에 취약한 웹서버를 자동화 공격툴을
이용하여 무차별적으로 공격을 시도하고 있습니다. 이
러한 공격을 예방할 수 있는 최선책은 Secure-
Coding을 통해 웹소스코드에 취약점이 존재하지 않
도록 개발 및 소스코드 수정을 하는 것입니다.

또한 웹서버 관리자는 Microsoft에서 제공하는
UrlScan을 활용하여 웹서버 요청에 대한 필터링을 통
해 보안을 강화할 수 있습니다. 이에 UrlScan3.1 버
전의 테스트를 통해 활용 가능성을 알아보려고 합니
다.

□ UrlScan3.1 이란

UrlScan3.1은 클라이언트의 HTTP요청을 검사하여 제
한하는 보안모듈입니다. UrlScan.ini의 지정된 설정을
통해 악의적인 HTTP요청을 웹서버가 처리하기 전에
차단하여 웹서버를 보호합니다.

UrlScan3.1은 Windows Vista, Windows2003,
Windows2008의 IIS5.1, IIS6.0, IIS 7.0을 지원합니다.

□ UrlScan3.1을 이용한 웹서버 보안

1. UrlScan3.1 설치

2. %windir%\ system32\ inetsrv\ urlscan\ urlscan.in
i 수정을 통한 HTTP 요청 제한 정책 설정

3. 인터넷정보서비스 → IIS 웹서버 속성의 “ISAPI 필
터”에 urlscan.dll 추가

4. IIS 웹서버 재시작 (명령프롬프트 or 실행창 →
iisreset)

◆ 제거 방법 : 제어판 → 프로그램 추가 / 제거 →
IIS UrlScan (제거) → IIS 웹서버 재시작

UrlScan.ini의 설정에 따라 특정 서비스(Ex: Outlook
Web Access)가 작동하지 않을 수 있으므로 실서버에
적용하기 전 동일한 환경의 테스트 서버에서 충분한
테스트를 거친 후 실서버에 적용하시기 바랍니다.

1. http://www.iis.net/download/UrlScan에서UrlScan
을 다운로드 받아 설치합니다.

(설치경로 - %WINDIR%\ System32\ Inetsrv\
UrlScan)

2. %WINDIR%\ System32\ Inetsrv\ UrlScan\ UrlSca
n.ini를 편집하여 차단할 HTTP 요청에 대해 설정합니
다. UrlScan.ini 항목에 대한 자세한 설명은 Microsoft
에서 제공하고 있습니다. (http://support.microsoft.
com/kb/326444/ko)

UrlScan.ini 주요 항목 요약 설명

[Options] - UrlScan의 일반적인 설정과 하단의 각
항목에 대해 어떻게 적용할지 설정합니다.

예를 들어 Options의 UseAllowVerbs 값이 “1”이면
하단의 [AllowVerbs] 항목에 나열된 Method를 사용
하는 HTTP요청만 허용합니다. 이 값이 “0”이면
[DenyVerbs] 구역에 나열된 Method를 사용하는
HTTP요청만 차단하게 됩니다.

[AllowVerbs],[DenyVerbs] - UrlScan이 허용하는
Method를 정의합니다.

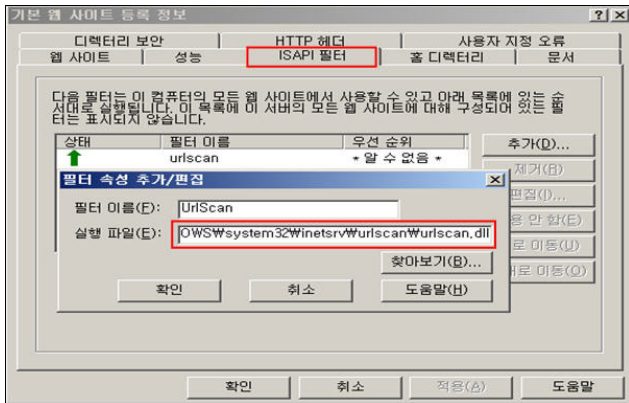
[DenyHeaders] - HTTP 요청에 허용되지 않는 HTTP
헤더 목록을 정의합니다.

[AllowExtensions],[DenyExtensions] - UrlScan이 허

용/제한하는 파일 확장명을 정의합니다.

[DenyURLSequences] - HTTP 요청 URL에서 허용되지 않는 문자열 목록을 제공합니다.

설치 후 인터넷정보서비스 → 웹서버 속성의 “ISAPI 필터”에 urlscan.dll을 추가한 후 IIS 웹서버를 재시작합니다.

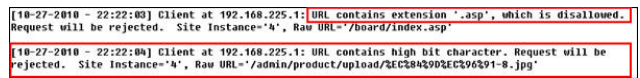


[그림 1] UrlScan.dll 필터등록

UrlScan.ini 설정에 따라 웹페이지 접속이 되지 않는 문제가 발생할 수 있습니다.

%WINDIR%\ System32\ Inetsrv\ UrlScan\ log\ UrlScan.날짜.log 파일에 접속을 차단한 HTTP 요청에 대한 기록을 분석해 UrlScan.ini를 수정하여 문제를 해결 할 수 있습니다. 테스트 환경에서 UrlScan 설치 후 UrlScan.ini의 기본설정을 적용 한 결과 웹페이지 접속 시 에러가 발생했으며 UrlScan의 로그파일을 확인하여 [그림 2]과 같이 .asp 확장자와 High Bit Character가 허용되지 않아 웹페이지 접속이 차단되었습니다.

High Bit Character가 허용되지 않으면 ASCII 코드가 아닌 문자(Ex: 한글)가 포함된 HTTP요청을 차단하게 됩니다. 테스트 서버에서 한글이름의 그림파일을 불러오는 과정에서 차단된 것으로 확인되었습니다.



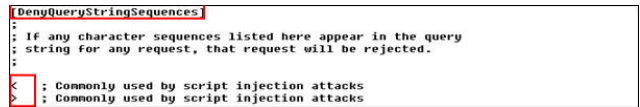
[그림 2] UrlScan Log

UrlScan.ini의 [DenyExtensions]에서 .asp를 제거하고 [Options]의 AllowHighBitCharacters 값을 “0”에서 “1”로 변경한 후 웹서버를 재실행한 결과 웹페이지에 정상 접속이 되었습니다.



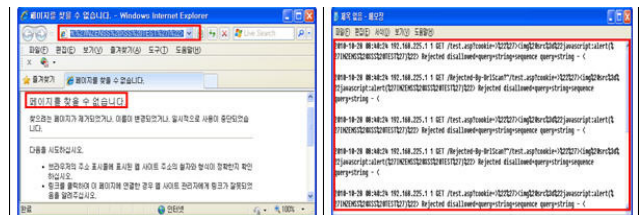
[그림 3] UrlScan.ini 변경 후 정상접속

[DenyQueryStringSequences] 항목에 XSS 공격에 사용되는 “<”, “>” 등의 문자를 추가하여 XSS 공격을 차단합니다.



[그림 4] DenyQueryStringSequences

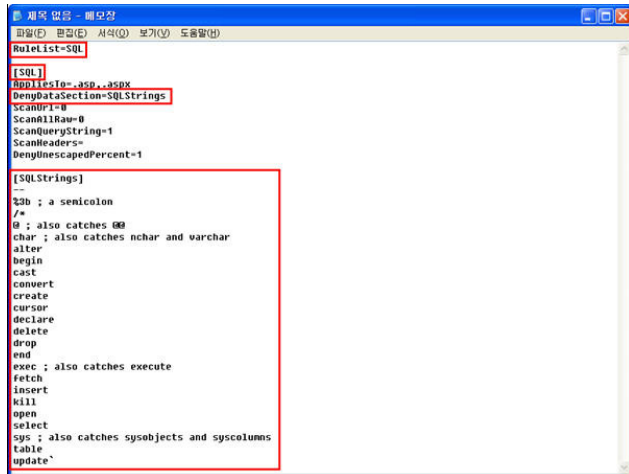
[DenyQueryStringSequences] 항목 설정에 의해 [그림 5]와 같이 XSS 공격을 시도하는 HTTP 요청이 차단되고 로그파일에 기록됩니다.



[그림 5] XSS 차단 및 로그확인

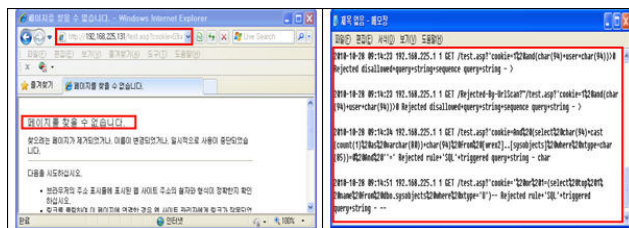
UrlScan3.1은 [Options]의 RuleList 항목을 이용하여 사용자 지정물을 추가할 수 있으며 [그림 6]과 같이 SQL Injection공격에 사용되는 스트링을 추가하여 해당 스트링이 포함된 HTTP요청에 대해 차단하도록 설

정 할 수 있습니다.



[그림 17] 사용자 지정 룰 추가 – SQL Injection 차단

해당 룰을 추가하고 웹서버를 재시작 한 후 SQL Injection 공격을 시도한 결과 [그림 7]와 같이 HTTP요청이 차단되고 로그파일에 기록이 저장됩니다.



[그림 7] SQL Injection 차단 및 로그확인

사용자 지정룰에 대한 자세한 정보는 <http://learn.iis.net/page.aspx/476/common-urlscan-scenarios> 에서 확인 할 수 있습니다.

□ 결 론

Microsoft에서 제공하는 웹서버 보안도구인 UrlScan 사용 결과 충분한 테스트를 거친 후 UrlScan.ini의 각 항목에 대한 이해를 바탕으로 적절한 HTTP 요청 제한 정책을 작성한다면 IIS웹서버의 보안 향상에 큰 도움을 줄 것으로 판단됩니다.

하지만 <http://support.microsoft.com/kb/325965/ko>, <http://support.microsoft.com/kb/307976/ko>에서 확인 할 수 있듯이 FrontPage, Outlook 등의 서비스

사용 시 오류가 발생할 수 있으므로 반드시 실서버와 동일한 테스트환경에서 충분한 테스트를 거친 후 적용시켜야 합니다.