TREND MICRO
Securing Your Journey to the Cloud

3Q 위협 보고서

TrendLabs℠

트렌드마이크로 분기별 위협 보고서는
최신 위협 상황과 관련된 주요 보안
하이라이트와 개발 동향을
정리하여 제공합니다.

분기별 트렌드마이크로 보고서 | 2011

이번 호 내용

트렌드마이크로 연구원과 분석가들은 이번 분기 동안 다양한 사이버 범죄 활동을 적발하는 데에 많은 기여를 하였습니다. 법률 집행 기관들을 돕기 위한 노력의 일환으로써 이들은 몇 가지 FAKEAV 제휴 네트워크와 특수한 SpyEye 활동들을 적발하였으며 이로써 법률 집행 기관들은 좀 더 수월하게 범죄자들을 체포할 수 있을 것입니다.

2분기와 마찬가지로 지난 3개월 동안 우리는 안드로이드 멀웨어가 증가하였고, ZeuS나 SpyEye와 같은 악명 높은 크라임웨어 툴킷이 대폭 강화되었으며 소셜 미디어의 설문 조사 사기 행위가 확산된 것을 확인할 수 있었습니다. 지난 달과 마찬가지로, 사이버 범죄자들은 대상을 끌어들이기 위해 상당히 유혹적인 소셜 엔지니어링 전술을 계속 사용하고 있습니다.

하지만 지난 상반기와는 달리 대규모 피해 사례는 줄어 들었는데 이는 공격 형태가 표적 공격으로 바뀌었기 때문인 것으로 보여지며 이러한 표적 공격은 대기업과 정부 기관들을 주 대상으로 하였습니다.

데이터 유출 및 표적 공격

Epsilon 데이터 유출

올 7월 한국에서 발생된 SK 커뮤니케이션즈 데이터 유출 사건은 최소 3,500만 명의 사용자들에게 영향을 미쳤습니다. SK 커뮤니케이션즈의 자회사이자 높은 인기를 얻고 있는 소셜 네트워킹, 텔레커뮤니케이션 및 인스턴트 메시징 서비스 공급업체인 싸이월드와 네이트가 이번 사고로 가장 큰 영향을 입었으며 전자메일 주소, 사용자 이름, 연락처 세부 정보와 같은 고객 정보가 유출되었습니다. SK 커뮤니케이션즈는 데이터 유출 사고가 확인된 직후 경보를 발령하였습니다.

SK 커뮤니케이션즈 데이터 유출 사고에 관한 보고서가 발표된 지 일주일 만에, 트렌드 마이크로의 분석가들은 이번 사건과 관련이 있을 것으로 보이는 BKDR_SOGU.A로 명명된 멀웨어를 발견하였습니다. 분석을 통해 우리는 이 멀웨어가 실행되면 백도어가 감염된 시스템에 저장된 데이터베이스에 액세스하여 데이터를 수집할 수 있게 된다는 것을 확인하였습니다. 또한 원격지의 악의적 사용자가 감염된 시스템에 명령을 전송하여 보안을 손상시킬 수도 있었습니다.

그로부터 일주일 후 한국의 소프트웨어 업체인 ESTsoft는 그들도 동일한 공격에 의해 피해를 입었음을 밝혔습니다. 공식 성명서를 통해 회사는 자사의 소프트웨어 업데이트 서버들 중 한 대가 SK 커뮤니케이션즈 공격에 사용된 것과 동일한 백도어 프로그램에 의해 손상되었음을 시인하였습니다. ESTsoft의 자체 조사에 의하면 자사의 DLL 업데이트 모듈 중 하나에서 공격자가 제품 사용자의 시스템에 BKDR_SOGU.A를 설치할 수 있도록 허용하는 취약점이 발견되었다고 합니다. 문제 해결을 위해 ESTsoft는 8월 4일 해당 취약점에 대한 패치를 발표하였고 업데이트로 제공하였습니다.

빈번해진 "LURID Downloader" 표적 공격

최근, LURID 멀웨어 제품군의 변종이 러시아, 카자흐스탄 및 우크라이나를 포함한 61개국의 대형 기업과 기관들을 표적으로 했던 LURID Downloader 공격"에 사용되었습니다. 이는 지능형 지속 위협(APT)으로 간주되며 공격의 배후의 사이버 범죄자들은 300개 이상의 멀웨어 활동을 실시하여 표적 대상으로부터 데이터를 수집합니다.

트렌드마이크로의 분석에 의하면, 가해자들은 공격 대상이 악의적 첨부 파일을 열도록 현혹하는 전자메일을 전송한다고 합니다. 이러한 유혹에 넘어간 사용자들이 메일을 열면 Microsoft Office와 Adobe Reader의 취약점을 악용하는 악성 코드(예, CVE-2009-4324와 CVE-2010-2883)가 실행되고 공격자는 장기간에 걸쳐 감염된 사용자의 시스템에서 기밀 정보를 수집하고 시스템을 완전히 제어할 수 있게 됩니다.

백도어 프로그램 역시 15개의 도메인 이름과 10개의 IP 주소를 사용하는 명령 및 통제(C&C) 서버 네트워크에 액세스할 수 있게 되어 공격자는 손상된 시스템에 명령을 내릴 수 있습니다. 특정 지역과 대상을 공략하는 이러한 표적화 특성과 빈번한 공격의 높은 성공률 덕분에 이들은 1,465대에 이르는 시스템을 손상시킬 수 있었습니다.

순위	국가	감염 수
1	러시아	1,063
2	카자흐스탄	325
3	우크라이나	102
4	베트남	93
5	우즈베키스탄	88
6	벨라루스	67
7	인도	66
8	키르기스스탄	49
9	몽골	42
10	중국	39

표 *1.* LURID Downloader 공격의 주 표적 국가

LURID Downloader 공격에 관한 자세한 정보는 트렌드마이크로 연구 논문, "The 'Lurid' Downloader"에서 확인할 수 있습니다.

앞서 소개한 데이터 유출과 표적 공격은 위협 상황이 변화하고 있음을 보여주고 있습니다. 사이버 범죄자들은 한국의 데이터 유출 사건처럼 지역 별로 혹은 LURID Downloader 공격처럼 산업 별로 범죄 대상에 대한 범위를 제한하고 있습니다.

취약점 악용

osCommerce 대규모 피해 사례

7월, *osCommerce* 소프트웨어의 여러 취약점이 악용되어 대규모 피해로 이어졌습니다. 사용자들을 익스플로잇 킷(exploit kit)을 호스팅하는 악의적 사이트로 이동시키는 iframe이 대략 90,000개의 웹 페이지에 주입되었습니다.

많은 전자상거래 웹사이트가 이 공격의 희생양이 되었습니다. 트렌드마이크로 위협 대응 엔지니어에 의하면, 이 공격에 사용된 멀웨어인 TROJ_JORIK.BRU는 필요한 정보를 수집한 즉시 감염된 시스템에서 자신을 삭제하여 탐지를 피했다고 합니다. osCommerce의 개발자들은 이 공격에 악용된 취약점을 해결하려면 osCommerce의 소프트웨어를 사용하는 사이트의 소유자들이 소프트웨어를 최신 버전으로 업데이트하고 코드가 삽입된 징후가 없는지 사이트를 점검할 것을 강력히 권장하고 있습니다.

방위 산업체 표적

이번 사분기에 사이버 범죄자들은 미국과 일본을 포함한 여러 국가의 방위 산업체를 표적으로 하는 익스플로잇 공격을 시도하였습니다. 첫 번째 공격에는 트렌드마이크로가 TROJ_PIDIEF.EED로 명명한 악성 .PDF 첨부 파일이 포함된 스팸이 포함되었습니다. 분석에 따르면, 이 트로이 목마가 실행되면 BKDR_ZAPCHAST.QZ로 명명된 백도어 프로그램이 설치된다고 합니다. 이 백도어는 원격지의 악의적 사용자로부터 명령을 받아 피해자의 시스템 보안을 손상시킬 수 있습니다.

공격자들은 손상된 시스템에 명령을 내려 네트워크 정보를 수집하고 특수한 사용자 지정 .DLL 파일을 다운로드 하였는데 트렌드마이크로는 이 파일을 BKDR_HUPIG.B로 명명하였습니다. 이 외에도 이들은 피해자의 네트워크를 자유롭게 돌아다닐 수 있도록 허용하는 특수한 도구를 다운 로드하도록 손상된 시스템에 명령을 내렸습니다. 이 도구들은 BKDR_HUPIGON.ZXS와 BKDR_HUPIGON.ZUY로 명명된 원격 액세스 트로이목마(RAT)으로 밝혀졌습니다. 이 원격 액세스 트로이목마(RAT)는 원격지의 악의적 사용자들이 손상된 시스템을 완벽하게 제어할 수 있도록 허용합니다.

수일 후, 어도비 역시 *CVE-2011-2444*를 해결하기 위한 대역 외 보안 패치를 발표하였는데, 이는 피해자의 시스템과 네트워크를 손상시키기 위해 사이버 범죄자들이 표적 공격에 사용해오던 또 다른 취약점이었습니다.

각종 취약점 통계

2분기에 보고된 제품 취약점 부문에서 1위를 차지했던 마이크로소프트가 이번 분기에는 3위로 순위가 떨어졌습니다. 크롬(Chrome)의 취약점들이 대거 보고된 이후 구글이 지난 분기의 1위를 몰아내고 선두를 차지하였습니다. 하지만, 크롬(Chrome)의 취약점들은 마이크로소프트 제품에서 발견된 취약점만큼 심각하지는 않았습니다. 크롬을 표적으로 하는 공격 횟수가 증가한 것은 브라우저의 사용률과 인기도가 상승했기 때문일 것입니다. 크롬의 빠른 개발 속도로 볼 때, 제품 출시 전 내/외부에서 버그 테스트를 실시할 충분한 시간이 없었으며 이것이 구글의 순위를 높이는 데 상당한 기여를 했을 것입니다.

오라클 제품에 대한 보고된 취약점의 수 역시 증가하였는데, 이는 썬 마이크로시스템즈와 이들의 Java 제품을 인수한 것이 주된 원인인 것으로 보입니다. 오라클의 코드베이스가 방대하고 복잡하여 유지 관리가 어렵다는 사실이 제품의 악용 가능한 버그 수를 높이는데 기여한 것으로 보이며 이로써 2분기에 5위를 했던 오라클이 이번 분기에는 2위로 순위가 상승하였습니다.

순위	2Q 2011		3Q 2011	
	업체	보고된 취약점 수	업체	보고된 취약점 수
1	마이크로소프트	96	구글	82
2	구글	65	오라클	63
3	어도비	62	마이크로소프트	58
4	HP	57	애플	49
5	오라클	50	어도비	43
6	IBM	48	IBM	39
7	모질라	38	모질라	39
8	리눅스	31	오페라	36
9	시스코	30	HP	25
10	썬	29	시스코	20

Source: http://cve.mitre.org/

표 2. 보고된 취약점 수 부문 상위 10개 업체

2분기에는 4월에서 6월 사이에 악용 가능한 버그의 수가 지속적으로 감소한 것을 확인한 바 있습니다. 반면 이번 분기에는 악용 가능한 버그의 수가 매월 불규칙적으로 증가했다가 감소하는 추세를 보였습니다.

2Q 2011		3Q 2011	
월	보고된 취약점 수	월	보고된 취약점 수
April	312	July	307
May	295	August	294
June	294	September	389

Source: http://cve.mitre.org/

표 3. 월별 보고된 취약점 수

모바일 공격

제3세대 DroidDreamLight 변종

트렌드마이크로 위협 분석가들은 기능과 루틴이 강화된 새로운 DroidDreamLight 변종을 발견하였습니다. 배터리 모니터링 또는 작업 목록 표시 도구 또는 설치된 앱들의 사용 권한 목록을 보여주는 앱으로 위장한 이 새로운 안드로이드 멀웨어의 사본은 중국의 타사 앱 스토어에 널리 퍼져있었습니다. 트렌드마이크로가 ANDROIDOS_DORDRAE.N으로 명명한 이 특수한 변종은 통화 기록, 텍스트 메시지, 연락처 정보, 구글 계정 정보 및 감염된 장치에 저장되어 있는 각종 정보를 수집할 수 있습니다. 부가적인 데이터 도용 루틴 외에도, 이 새로운 변종의 코드는 구성 파일을 업데이트하도록 허용하기도 합니다. 이전 변종들과 마찬가지로, 이 멀웨어는 훔친 데이터를 특정 URL로 전송합니다.

그 밖의 주목할 만한 안드로이드 멀웨어 공격

트렌드마이크로 보안 전문가들은 안드로이드 마켓과 타사 앱 스토어에서도 다양한 안드로이드 멀웨어를 발견했습니다. 여기에는 "Fast Racing"이라는 게임의 Trojanized(트로이 목마) 버전으로 GoldDream이라고 불리는 멀웨어가 포함되었고 트렌드마이크로는 이 멀웨어를 ANDROIDOS_SPYGOLD.A로 명명하였습니다. 그리고 ANDROIDOS_PIRATES.A로 명명된 "Coin Pirates"도 포함되었습니다.

트렌드마이크로 엔지니어들은 다양한 앱들로 위장하고 있는 안드로이드 멀웨어들도 발견하였습니다. 여기에는 사랑 테스트, 전자책 리더(reader) 또는 위치 추적 앱으로 위장한 ANDROIDOS_LUVRTAP.B와 ANDROIDOS_AUTOSUBSMS.A로 명명된 프리미엄 서비스 어뷰저(abuser) 그리고 감염된 장치에서 기밀 정보를 수집하는 ANDROIDOS_NICKISPY.A 및 ANDROIDOS_NICKISPY.C와 같은 가짜 스파이 도구들이 포함되었습니다.

NICKISPY 변종은 텍스트 메시지, 전화 통화 기록 및 위치 정보를 포함하여 감염된 사용자의 활동과 소재를 모니터링하는 것으로 알려져 있습니다. 오랫동안 우리는 감염된 안드로이드 장치에서 도용한 정보가 어떻게 이용되는지 궁금했었는데 지난 8월, 트렌드마이크로 연구원은 안드로이드 장치에서 훔친 정보를 유료로 판매하고 있는 중국 사이트를 찾아냈습니다. 이는 사이버 범죄자들이 감염된 모바일 장치에서 유출한 데이터를 통해 수익을 얻는 하나의 사례입니다.

지금까지 우리가 확인한 다양한 안드로이드 멀웨어에 대한 자세한 정보는 "안드로이드 위협 스냅샷[인포그래픽]"을 참조하십시오.

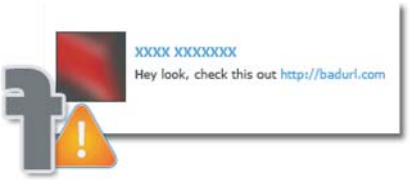
가짜 오페라 앱

최근 오페라 미니로 위장한 모바일 멀웨어(ANDROIDOS_FAKEBROWS.A)와 오페라 모바일로 위장한 멀웨어(J2ME_FAKEBROWS.A)가 발견되었습니다. 이 멀웨어들은 사용자 모르게 프리미엄 서비스 번호로 텍스트 메시지를 전송하는 프리미엄 서비스 어뷰저였습니다. J2ME_FAKEBROWS.A는 Java ME 환경용 CLDC(제한적 접속 장치 구성)의 MIDP(모바일 정보 장치 프로파일)을 이용하는 애플리케이션인 MIDlets을 지원하는 모바일 장치에 영향을 미칩니다.

사이버 범죄자들은 플랫폼 공격에 있어서 표적에 제한이 없으며 안드로이드가 아닌 모바일 운영 체제를 실행하는 장치를 표적으로 하는 멀웨어도 제작하고 있습니다.

소셜 네트워킹 신용 사기

유명 인사의 사망 소식 및 자연 재해



이번 분기에 우리는 사용자의 관심을 자극하는 두 가지 이슈(유명 인사 소식과 자연 재해)를 악용하는 세 건의 페이스북 사기를 확인했습니다. 이 중 한 가지는 에이미 와인하우스의 죽음에 대한 기사를 악용하였고 또 다른 사기는 레이디 가가의 사망설을 악용하였습니다. 이 두 건의 사기는 담벼락을 이용하여 사용자들을 설문 조사 페이지나 광고 사이트로 유도하여 위험에 빠지게 만들었습니다.

팬층이 두터운 영화 "The Twilight Saga"도 사이버 범죄자들의 관심을 벗어나지 못했습니다. 8월 초, 공격자들은 "The Twilight Saga: Breaking Dawn Part 2"의 무료 티켓을 받으려는 사용자들로 하여금 악성 링크를 클릭하도록 현혹하는 페이스북 담벼락 게시물을 퍼뜨렸습니다. 다른 설문 조사 사기와 마찬가지로, 이 사용자들 역시 보안 위험에 노출되었습니다.

사이버 범죄자들은 허리케인 아이린 기사를 검색하는 페이스북 사용자들을 자신의 덫으로 끌어들이기 위한 기회도 간과하지 않았습니다. 이들은 아이린 관련 동영상을 시청하고자 하는 사용자들을 광고 사이트로 유인하였습니다.

소셜 네트워킹 사이트 증가와 더불어 증가하는 위협들

소셜 미디어 부문에서 높은 인기를 얻고 있는 페이스북뿐 아니라 구글 플러스와 링크드인과 같이 덜 알려진 소셜 네트워킹 사이트들도 사이버 범죄의 주목을 받았던 시기가 있었습니다. 7월 상반기, 트렌드마이크로 엔지니어들은 구글이 최근 발표한 소셜 미디어인 구글 플러스를 무료로 사용해볼 수 있는 초대장을 제공하는 링크를 클릭하도록 사용자들을 유인하는 페이지를 발견하였습니다. 하지만, 사용자들이 받은 것은 사이트 가입 초대장이 아니라 설문 조사에 참여할 수 있는 "기회"였습니다.

일주일 전, 링크드인 역시 사이버 범죄자들에 의해 리디렉터 역할을 하게 되어 주목을 받은 적이 있었습니다. 저스틴 비버 동영상을 보기 위해 악성 링크를 클릭하게 된 사용자들 링크드인 도메인을 사용하는 페이지로 리디렉트되었고 그곳에서 트렌드마이크로가 JS_FBJACK.D로 명명한 악성 스크립트가 적용된 또 다른 설문 조사 페이지로 이동되었습니다.

그 밖의 주목할 만한 소셜 미디어 공격

이번 분기에 확인된 여러 설문 조사 사기 행위 외에도, 트렌드마이크로 전문가들은 가짜 친구 요청 알림을 이용하여 사용자의 시스템에 TSPY_ZBOT.FAZ로 명명된 ZBOT 변종을 감염시키는 페이스북 사기 행위를 발견하였습니다.

소셜 네트워킹 사이트에서 사용자들이 자주 접하게 되는 위협들에 대한 자세한 정보는 "소셜 미디어 위협 현황[인포그래픽]"을 참조하십시오.

주요 시스템 감염원

스팸 실행과 뱅킹 트로이 목마

이번 분기에 발견된 가장 악명 높은 스팸은 두 개의 뱅킹 트로이 목마를 다운 로드하여 실행하도록 유도하는 내용이었습니다. 첫 번째 스팸은 스페인 경찰청에서 발송한 것으로 위장한 내용이었습니다. 메시지 본문에 포함된 링크를 클릭한 사용자들의 시스템에는 TROJ_BANLOD.QSPN이 다운 로드되었습니다. 이 멀웨어가 실행되면 트렌드마이크로가 TSPY_BANCOS.QSPN로 명명한 또 다른 멀웨어가 다운 로드됩니다. 다른 BANKER 트로이 목마와 마찬가지로, 이는 감염된 사용자의 시스템에서 개인 정보를 수집하는데 그 중에서도 Caixa, Cajasol 및 Banco Popular와 같은 금융 기관과 관련된 정보를 수집합니다. 하지만 이 공격에서 가장 주목할 만한 특징은 사이버 범죄자들이 손상된 사이트와 폰 홈(phone-home) URL을 이용할 수 있었다는 점이며 이로써 범죄자들은 시스템 감염 성공을 확인하고 스파이웨어를 업데이트할 수 있게 되어 더 효과적으로 탐지를 피할 수 있게 되었습니다.

두 번째 스팸은 국세청에서 발송한 것으로 위장한 내용이었습니다. 메시지 본문에 포함된 링크를 클릭한 사용자들의 시스템에는 TSPY_ZBOT.WHZ로 명명된 LICAT 변종이 다운 로드 되었습니다. 다른 LICAT 변종들과 마찬가지로, 이 멀웨어는 구성 파일을 업데이트하기 위해 액세스하는 URL을 생성하는데 여기에는 모니터링 할 사이트 목록과 훔친 정보를 전송할 사이트 목록이 들어있습니다.

상기에 소개한 두 건의 데이터 도용 스팸 외에도 우리는 악의적 첨부파일이 포함된 스팸의 양이 눈에 띄게 급증한 것을 확인하였으며 이러한 스팸들 중에는 휴가와 관련된 내용이 많았습니다.

스팸 통계

이사분기와 마찬가지로 인도와 한국은 이번에도 스팸을 가장 많이 전송하는 상위 3개 국가에 포함되었습니다. 하지만 놀랍게도 상위에 선정되곤 하던 미국이 이번에는 스팸을 가장 많이 전송하는 상위 10개 국가 목록에 포함되지 않았습니다. 스팸을 가장 많이 전송하는 국가는 곧 스팸봇에 가장 많이 감염된 국가를 의미하기 때문에 미국의 순위가 하락했다는 것은 감염 수준도 낮아졌다고 볼 수 있습니다. 이는 지난 몇 달 동안 이루어진 봇넷 근절 노력에 의한 결과인 것으로 보여집니다.

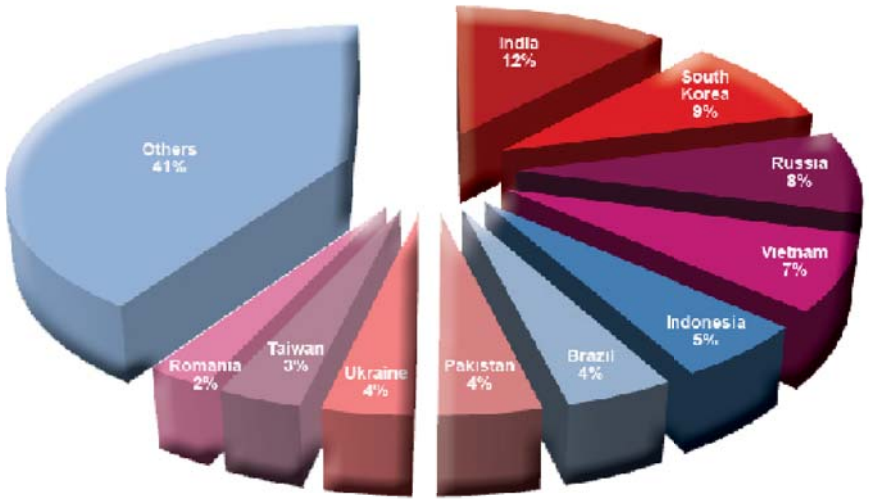


그림 1. 3Q 2011 상위 10개 스팸 전송국

스팸에 가장 많이 사용된 상위 3개 언어는 이번에도 영어, 독일어 및 러시아어가 순위를 유지했습니다.

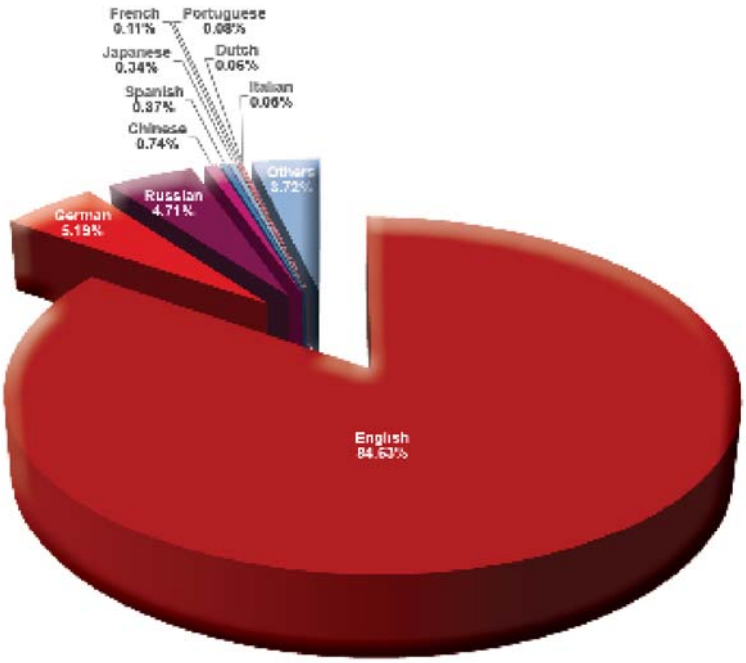


그림 2. 3Q 2011 상위 10개 스팸 언어

스팸의 현 상황에 대한 포괄적인 설명은 "현대 비즈니스 세상의 스팸"을 참조하십시오.

ZeuS 업데이트 및 Stealthier 변종

ZeuS의 소스 코드 유출이 "Ice IX"라는 별칭의 변종을 확산시킨 원인이 된 것으로 보입니다. 이러한 새로운 유형의 ZeuS 변종은 더 교묘하게 추적을 회피하고 있습니다.

트렌드마이크로 연구원들은 TSPY_ZBOT.IMQU라고 명명한 업데이트된 ZBOT 샘플도 확보하였는데 이는 ZeuS 버전 2.3.2.0에서 생성된 것으로 보입니다. 이 변종은 암호 해독 및 암호화 루틴이 강화되어 이전 변종에 비해 구성 파일을 분석하기가 훨씬 어렵습니다. 이 역시 미국, 독일, 브라질, 스페인 및 홍콩과 같은 국가의 금융 기관을 표적으로 하는 국제적 활동에 사용될 가능성이 있는 것으로 밝혀졌습니다.

그 밖의 주목할 만한 멀웨어 공격

이번 분기에도 트렌드마이크로는 루트킷, 두 건의 웜 및 비트코인(Bitcoin) 마이너를 포함하여 여러 가지 눈에 띄는 멀웨어를 발견하였습니다. RTKT_POPUREB.A로 명명된 이 루트킷은 감염된 시스템의 마스터 부트 레코드(MBR)를 덮어쓸 수 있습니다. TROJ_POPUREB.SMB와 함께 이 루트킷은 감염된 시스템의 디스크 상의 TROJ_POPUREB.SMA에 의해 만들어집니다. 이러한 멀웨어는 사용자가 악의적 사이트를 방문할 때 사용자의 시스템에 침입하여 시스템에 저장된 개인 정보를 도용합니다.

ZeuS와 SpyEye만큼 악명 높지는 않지만 KOOBFACE 갱은 토렌트 P2P 공유 네트워크에 WORM_KOOBFACE.AV로 명명된 트로이 목마 애플리케이션을 전파하였습니다. 이 멀웨어는 사용자 모르게 감염된 시스템에서 토렌트 클라이언트 프로세스를 실행시키고 사용자들을 피어(peers)로 전환시켜 악성 바이너리를 퍼뜨리거나 호스팅하도록 합니다. 소셜 미디어를 통해 멀웨어를 전파시키던 방식에서 P2P를 통한 방식으로 전환된 것은 KOOBFACE 봇넷이 프레임워크를 악용하지 못하도록 차단한 소셜 네트워킹 사이트들의 적극적인 노력 때문일 것입니다. 그러나 범죄자들이 소셜 네트워킹 사이트를 통해 피해자를 유인하는 활동을 중단한 것은 아닙니다.

우리 엔지니어들은 원격 데스크톱 프로토콜(RDP)를 통해 전파되는 WORM_MORTO.SMA도 발견하였습니다. 이 웜은 .DLL 구성 요소(WORM_MORTO.SM)를 통해 공격자들이 관리자 계정으로 로그인할 수 있도록 허용하여 감염된 시스템과 전체 네트워크를 완벽하게 제어할 수 있도록 합니다.

우리는 여러 가지 "비트코인 마이너"를 포함하고 있는 비트코인-관련 공격도 확인하였습니다. 지난 3개월 동안, BKDR_BTMINE.MNR 및 BKDR_BTMINE.DDOS와 같은 비트코인 마이너뿐 아니라 관련 그레이웨어인 HKTL_BITCOINMINE도 발견하였습니다. 사이버 범죄자들은 사용자의 시스템을 비트코인 마이너로 전환시키므로 사용자들은 리소스 집약적인 마이닝 프로세스로 인해 자신의 시스템을 충분히 활용할 수 없게 됩니다. 비트코인이 무엇인지, 비트코인 마이닝은 어떻게 작동되는지 그리고 위협 환경에서 비트코인 마이너가 증가하는 이유는 무엇인지에 대한 자세한 정보는 "사이버 범죄를 통한 수익 창출: 새로운 멀웨어 표적, 비트코인"을 참조하십시오.

멀웨어 통계

2분기와 마찬가지로, WORM_DOWNAD.AD와 CRCK_KEYGEN(시리얼 키 생성 프로그램)이 상위 2개 멀웨어 순위를 차지했습니다. 흥미로운 점은 DOWNAD/Conficker가 사용자들을 자신의 홈페이지로 유인하기 위해 사용하던 URL이 오래 전에 만료되었음에도 불구하고 DOWNAD 변종은 여전히 상위 멀웨어 순위에서 1위를 차지하고 있다는 것입니다. 이는 멀웨어를 차단하기 위한 시스템 보호와 관련된 문제가 아니라 우수한 보안 정책을 설정하여 실행해야 하는 문제입니다. 한편, ADW_SAHAGENT(애드웨어)는 HKTL_KEYGEN(해킹 도구)에 멀웨어 3위 자리를 내주었고 이번 분기에는 5위권에서도 제외되었습니다.

순위	멀웨어 명칭
1	WORM_DOWNAD.AD
2	CRCK_KEYGEN
3	HKTL_KEYGEN
4	PE_SALITY.RL
5	HKTL_ULTRASURF

표 4. 3Q 2011 상위 5대 멀웨어

위협 환경의 변화

탐지와 근절을 피하기 위한 ZeuS의 발전 외에도, 트렌드마이크로 연구원들은 모바일 멀웨어 역시 눈에 띄게 개선된 것을 확인하였습니다. TDL4와 같은 기존의 멀웨어도 악의적 루틴과 전술 면에서 크게 개선되었습니다.

여러 가지 법률 집행 노력을 통해 Anonymous와 LulzSec 공격이 감소하긴 했지만, 표적 공격의 수와 범위는 증가하였습니다. 사이버 범죄자들은 그 어느 때 보다 규모가 크고 수익성이 높은 대상을 모색하고 있습니다.

주목할만한 보안 성과

Soldier의 SpyEye 활동

트렌드마이크로 연구원들은 "솔져(Soldier)"를 이용했던 사이버 범죄자들이 제어하는 SpyEye 활동을 탐지하였습니다. 이 봇넷 활동은 미국의 대기업들과 정부 기관들을 주로 표적으로 삼았지만 캐나다, 영국, 인도 및 멕시코의 조직들도 영향을 받았습니다.

올해 3월부터 이를 모니터링해 온 우리 연구원들은 이들이 6개월 동안 솔져 활동을 통해 미화 320만 달러 이상의 금액을 취득한 것을 확인했습니다. 트렌드마이크로가 이러한 활동을 모니터링한 것은 얼마나 많은 사용자들이 이러한 위협에 노출되어 있는지 그리고 손상된 시스템으로 인한 피해 규모가 어느 정도인 지를 알려주기 위한 것입니다. 그리고 하나의 SpyEye 봇넷을 통해 사이버 범죄자들이 얻을 수 있는 수익성이 어느 정도인지도 가늠할 수 있습니다.

최근 트렌드마이크로의 성과에 대한 자세한 정보는 우리의 연구 논문, "러시아에서 헐리우드로: SpyEye 사이버 범죄 조직의 활동 영역의 변화"를 참조하십시오.

FAKEAV 제휴 네트워크

SpyEye 활동 탐지 외에도 트렌드마이크로 연구원들은 FAKEAV 공급자들이 이용한 서버들에 대한 철저한 모니터링을 통해 가장 규모가 큰 두 개의 FAKEAV 제휴 네트워크 (BeeCoin과 MoneyBeat)에 대한 세부 정보를 수집할 수 있었습니다. 연구원들은 2011년 1월과 6월 사이, BeeCoin과 이들의 제휴사들이 214,000대 이상의 시스템에 FAKEAV 멀웨어를 설치한 사실을 확인하였습니다. 또한 멀웨어를 설치한 44명의 사람들 중 한 명의 비율로 불량 안티바이러스 소프트웨어 전체 버전을 실제로 구입하였으며 이를 통해 BeeCoin은 미화 123,475달러를 벌어들였습니다.

FAKEAV 제휴 네트워크, 봇넷 및 그 밖의 악의적 활동들 간의 관계를 밝혀냄으로써, 우리 연구원들은 이와 같은 악의적 수익 창출 전략이 현 방어 및 수사 체제에 어떠한 해결 과제를 제시하고 있는지를 보안 커뮤니티와 법 집행 기관들이 더 정확하게 이해할 수 있기를 기대합니다.

FAKEAV 제휴 네트워크의 활동 방식에 대한 자세한 정보는 트렌드마이크로 연구 논문인 "Targeting the Source: FAKEAV 제휴 네트워크"를 참조하십시오.

LURID Downloader 공격

표적 공격으로 전환되고 있는 공격 형태를 조사하던 트렌드마이크로 연구원들은 "LURID Downloader"를 이용하는 일련의 표적 공격을 탐지하였습니다. 연구원들은 61개 국가에서 1,465대의 컴퓨터들이 이와 관련된 공격 활동으로 손상된 사실을 확인하였습니다. 이들은 외교사절단, 정부 부처, 우주 관련 정부 기관 및 여러 기업들과 연구 기관들을 포함하여 47곳의 피해 업체를 확인할 수 있었습니다.

LURID가 속해 있는 멀웨어 집단인 Enfal은 중국의 위협 행위자들과 연계되어 있었습니다. 이번 경우 우리가 분석한 공격 벡터(첨부파일이 포함되어 있는 악의적 전자메일)는 티벳 커뮤니티와 관련된 것이었으며 많은 이들이 중국과 연관되어 있을 것으로 생각하고 있습니다. 하지만, 중국도 피해를 입었기 때문에 반드시 중국과 관련된 것으로 판단하지는 않습니다.

LURID Downloader 공격에 대한 자세한 정보는 연구 논문, "The LURID Downloader"를 참조하십시오.

향후 전망

트렌드마이크로 연구원들은 향후 모바일 멀웨어의 양, 특히 안드로이드 기반 장치를 표적으로 하는 멀웨어의 양과 표적 공격의 수가 지속적으로 증가할 것으로 예측하였습니다.

하지만, 사이버 범죄자들의 활동을 단순히 따라잡기 보다는 이들보다 앞서 가기 위해 트렌드마이크로 연구원들은 전 세계 법률 집행 기관들과 협력하여 올해 더 많은 성과를 달성하고 있습니다. 이러한 노력은 계속될 것이며 우리는 사이버 범죄자를 체포하는데 중요한 역할을 담당하게 될 것입니다.

이처럼 나날이 진화해 가는 최신 위협 동향을 파악하고, 직원 시스템 및 기업 네트워크를 기업에 심각한 결과를 초래할 수 있는 각종 문제들로부터 안전하게 보호하기 위해서는 오늘 12월에 나오는 "2011년 4분기 위협 보고서"에도 큰 관심을 기울여야 하겠습니다.

부록 A: 악의적인 URL 통계

다음 표는 2011년 3분기에 트렌드마이크로 스마트 프로텍션 네트워크 인프라에서 차단한 10대 악성 URL 및 IP 도메인 주소를 정리한 것입니다

순위	차단된 악성 URL	설명
1	www.bit89.com:80/download/dpclean/ibdp.exe	멀웨어 배포
2	trafficconverter.biz:80/4vir/antispyware/loadadv.exe	멀웨어, 특히 DOWNAD 변종 배포
3	trafficconverter.biz:80/	멀웨어, 특히 DOWNAD 변종 배포
4	serw.clicksor.com:80/newserving/getkey.php	불법 응용 프로그램, 안드로이드 멀웨어, 허위 안티바이러스 소프트웨어 및 기타 악의적인 행동들과 연관된 도메인 목록에 포함되어 있음
5	serw.myroitracking.com:80/newserving/tracking_id.php	다양한 서버에 접속하여 팝업 광고를 다운 로드해 마구 표시함
6	ad.globe7.com:80/imp	TDSS 및 ZBOT 멀웨어 배포
7	cherry-lovepour.com:80/con1.php	멀웨어 배포
8	www.myroitracking.com:80/newserving/tracking_id.php	다양한 서버에 접속하여 팝업 광고를 다운 로드해 마구 표시함
9	221.8.69.25:80/search	멀웨어, 특히 DOWNAD 변종 배포
10	zs11.cnzz.com:80/stat.htm	멀웨어 배포

표 *A-1.* 3Q 2011에 차단된 상위 10대 악성 URL

순위	차단된 악성 IP 주소	설명
1	www.bit89.com	멀웨어 배포
2	trafficconverter.biz	멀웨어, 특히 DOWNAD 변종 배포
3	serw.clicksor.com	불법 응용 프로그램, 안드로이드 멀웨어, 허위 안티바이러스 소프트웨어 및 기타 악의적인 행동들과 연관된 도메인 목록에 포함되어 있음
4	serw.myroitracking.com	다양한 서버에 접속하여 팝업 광고를 다운 로드해 마구 표시함
5	d3lvr7yuk4uaui.cloudfront.net	멀웨어 배포
6	ad.globe7.com	TDSS 및 ZBOT 멀웨어 배포
7	dl.91rb.com	멀웨어 다운로드
8	cherry-lovepour.com	멀웨어 배포
9	conf.baidupapa.com	멀웨어 배포
10	www.myroitracking.com	다양한 서버에 접속하여 팝업 광고를 다운 로드해 마구 표시함

표 *A-2.* 3Q 2011에 차단된 상위 10대 악성 도메인 IP 주소

트렌드마이크로

트렌드마이크로는 인터넷 컨텐츠 보안의 글로벌 리더로서 일본 도쿄에 본사를 두고 있는 다국적 기업이다. 전세계 46개국에 5,000명 이상의 직원을 두고 있으며, 기업과 개인 사용자를 위한 디지털 정보 교환을 보안하는 분야에 주력하고 있다.
트렌드마이크로는 악성코드, 스팸, 데이터 유출과 최신 웹 위협으로부터 지속적인 운영, 개인정보 및 재산을 보호하는 분야를 관리하는 데 있어 선두적인 기업이다.
여러 솔루션 구현을 통해 다양한 서비스가 가능하며, 365일 24시간 전세계 위협 관리 전문가들이 지원하고 있다.
트렌드마이크로 제품 및 서비스에 대한 자세한 내용은 웹사이트 www.trendmicro.co.kr를 참고하기 바란다.

트렌드랩

트랜드랩은 트렌드마이크로의 글로벌 네트웍 연구센터로 365일 24시간 전세계 위협 관리 전문가들이 지원하고 있다. 검색 패턴 파일을 45분 이내에 완전히 테스트하여 최신 안티바이러스 기술 또는 업데이트로 트렌드마이크로 고객들을 신속히 보호한다.