이스트시큐리티

보안 동향 보고서

No.98 2017.11

No.98 2017.11

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

10 월에 발생했던 가장 큰 이슈도 역시 이전과 마찬가지로 랜섬웨어였습니다. 특히 10 월에는 한국 사용자들을 겨냥한 MyRansom(마이랜섬) 혹은 Magniber(매그니베르)라는 랜섬웨어가 발견되어 국내에서 많은 이슈가 되었습니다.

MyRansom(Magniber) 랜섬웨어의 경우 암호화 행위에 앞서 감염시키려는 시스템이 한국어 환경인지 확인을 한 후 동작을 수행하기 때문에 한국 사용자들을 겨냥한 랜섬웨어로 알려졌으며, 특히 이 MyRansom(Magniber) 랜섬웨어는 하반기부터 활동이 뜸해져서 거의 눈에 띄지 않았던 Cerber(케르베르) 랜섬웨어의 변종이 재등장하기 시작했다는 점에서 눈 여겨 보아야 합니다. 공격자들은 주로 익스플로잇 킷을 활용하여 취약점을 노린 공격을 시도하지만, Drive by Download 공격들도 계속적으로 시도하고 있다는 점도 유의하여야 합니다.

또한 10 월 말경 발견된 BadRabbit(배드래빗) 랜섬웨어도 국내에서는 별다른 피해가 발견되지 않았으나 러시아, 우크라이나 등 일부 동유럽 국가를 대상으로 유포된 랜섬웨어로 해외에서는 큰 주목을 받았습니다.

BadRabbit 랜섬웨어의 경우 WannaCry 와 NotPetya 랜섬웨어가 사용했던 EternalBlue 취약점 공격을 커스터마이즈한 EternalRomance 을 활용하는 부분이 특징이며, 여러가지 기존 오픈소스로 알려진 코드를 삽입해서 사용했다는 점에서도 향후 상황을 주목해 볼만 합니다. 특히 단순히 네트워크 관련 취약점을 활용하는 것뿐만 아니라, IPC$연결을 위해 미리 하드코딩된 사용자 이름과 패스워드를 무작위로 대입하여 원격 인증을 시도하는 상황도 점차 증가하고 있습니다. 때문에 랜섬웨어 공격에 효과적으로 대응하기 위해서는 별도 매체를 통한 중요 자료 백업, 취약점 패치도 매우 중요하지만, 기본적으로 PC 로그인 암호를 일반 패스워드처럼 복잡한 형태로 설정할 필요도 있어 보입니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2017 년 10 월의 감염 악성코드 Top 15 리스트에서는 지난 9 월에 각각 1, 2 위를 차지했던 Trojan.HTML.Ramnit.A 와 Trojan.Agent.gen 이 9 월 Top 15 리스트 자리를 바꾸었으며 지난달 4 위를 차지했던 Adware.SearchSuite 가 3 위를 기록했습니다. 전체 감염수는 소폭 상승하였다.

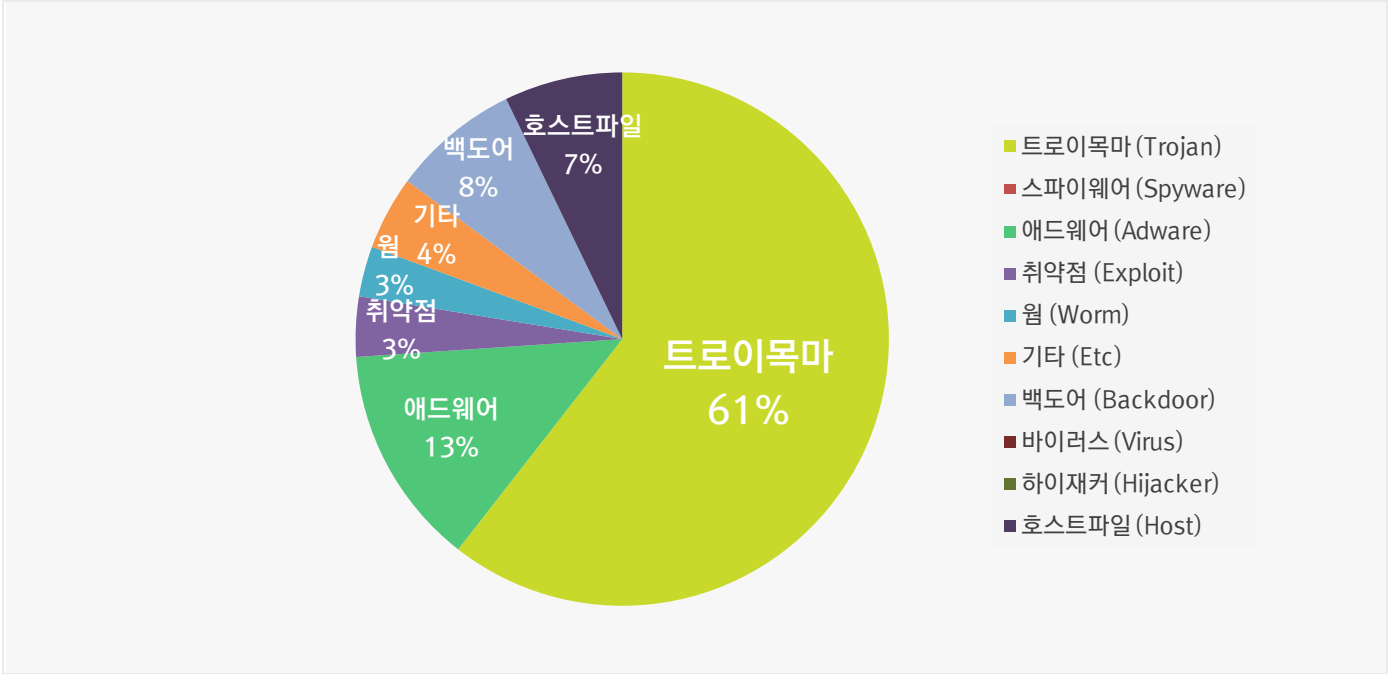
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	↑ 1	Trojan.Agent.gen	Trojan	1,156,003
2	↓ 1	Trojan.HTML.Ramnit.A	Trojan	899,432
3	↑ 1	Adware.SearchSuite	Adware	589,973
4	↑ 3	Hosts.media.opencandy.com	Host	442,379
5	↓ 2	Misc.Riskware.BitCoinMiner	Trojanr	440,522
6	New	Gen:Variant.Razy.107843	Trojan	362,493
7	↓ 1	Trojan.LNK.Gen	Trojan	347,851
8	↑ 3	Win32.Neshta.A	Trojan	300,781
9	↑ 3	Backdoor.Generic.792814	Backdoor	291,429
10	↓ 1	Misc.Keygen	Etc	276,376
11	↑ 2	Adware.GenericKD.5981996	Adware	236,260
12	↓ 4	Win32.Ramnit	Trojan	230,076
13	-	Exploit.CVE-2010-2568.Gen	Exploit	224,639
14	↓ 4	Worm.ACAD.Bursted.doc.B	Worm	188,287
15	↓ 10	Backdoor.Agent.Orcus	Backdoor	186,152

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 10 월 01 일 ~ 2017 년 10 월 31 일

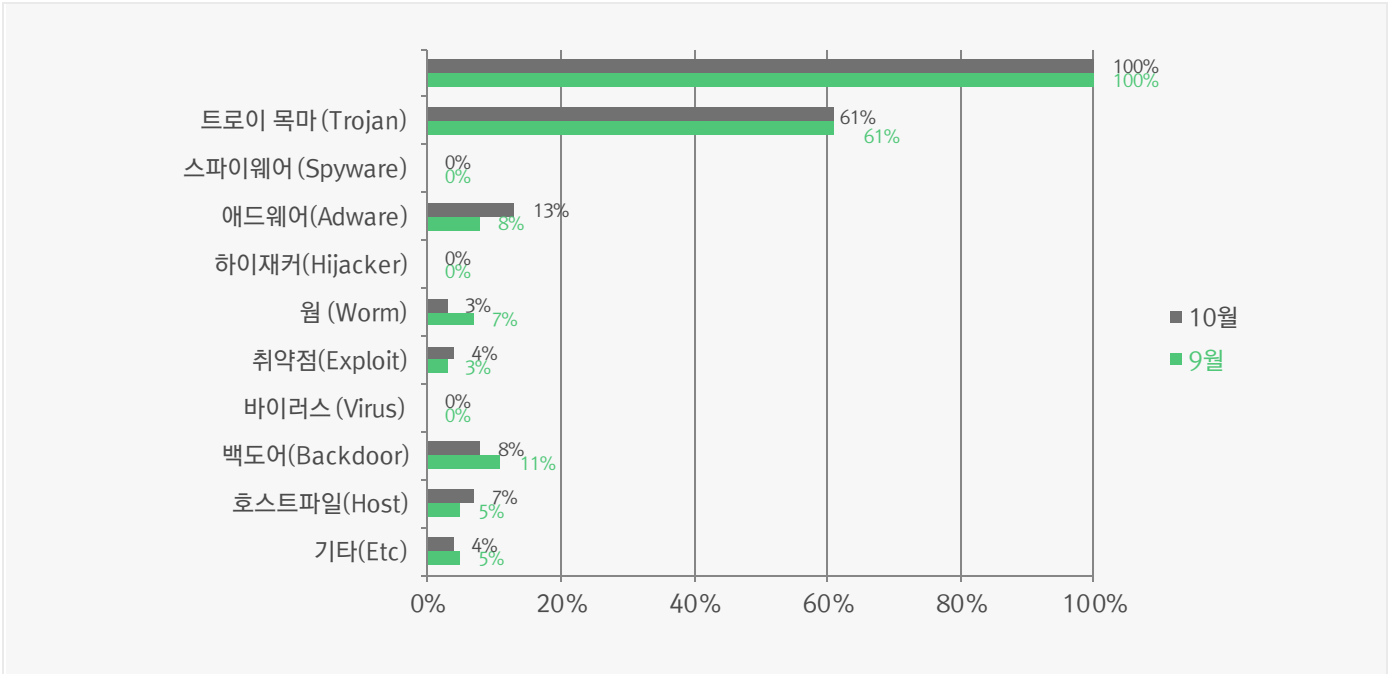
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 61%를 차지했으며 애드웨어(Adware) 유형이 13%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

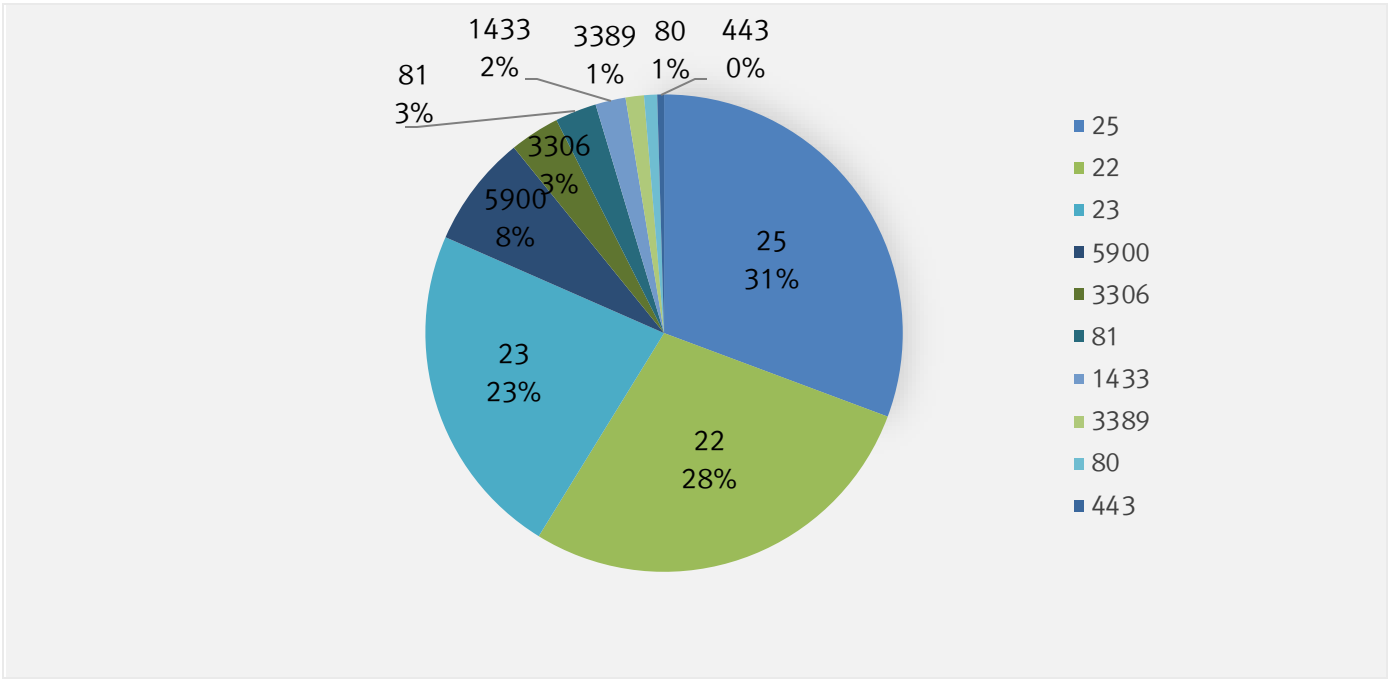
10 월에는 9 월에 비해 트로이목마 유형의 악성코드 비율이 감소하였으며, 백도어 유형의 악성코드 비율이 소폭 감소하였다. 전체적인 악성코드 감염 수치는 소폭으로 증가하였다.



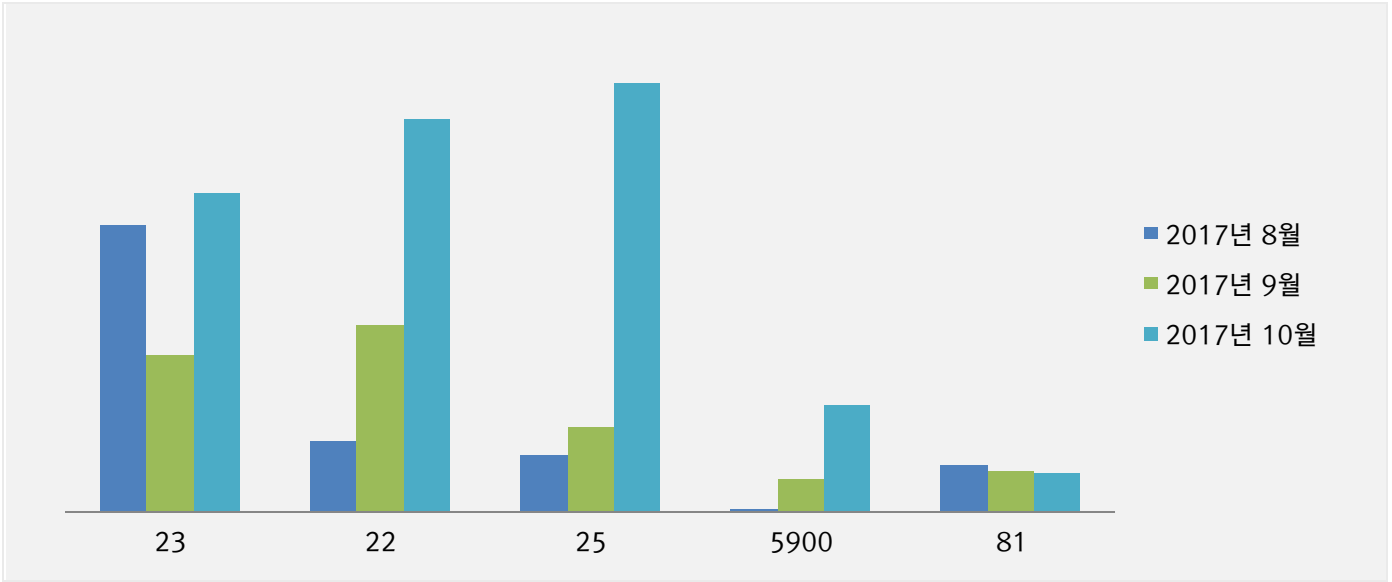
3. 허니팟/트래픽 분석

10 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 감지건수

2017년 5월 ~ 2017년 10월

4. 알약 M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017 년 10 월 01 일 ~ 2017 년 10 월 31 일
총 신고건수	2,462 건

키워드별 신고내역

키워드	신고 건수	비율
사진	147	5.97%
수령	40	1.62%
길	31	1.26%
택배	20	0.81%
추석	12	0.49%
간편조회	11	0.45%
청첩장	10	0.41%
보험료	9	0.37%
자세한것	7	0.28%
동영상	5	0.20%

스미싱 신고추이

지난달 스미싱 신고 건수 3,339 건 대비 이번 달 2,462 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 877 건 감소했다. 이번 달은 사진 관련 스미싱이 대부분을 차지했으며, 보험료 관련 스미싱이 새로 등장했다.

알약이 뽑은 10 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	빨^리 ^가^봐^봐 여^기 왜 ^니 ^사진 ^있지?
2	[Web 발신]수령확인
3	[Web 발신]오시는길
4	[Web 발신] [통운]도로명 불일치로 택배배송불가. 주소지를 변경해 주세요. 웹
5	추석은 ^곧 ^올거에요.이건 ^내가 드리고 ^싶은 ^선물 쿠폰인데 ^빨리 ^받으러 ^가요!즐거운 ^명절 ^보내세요!
6	[Web 발신]간편조회
7	[Web 발신]저희시작하는모습을여러분과함께하고싶습니다^^
8	[Web 발신]고객님 보험료 미납으로 인해 추가출금 일정 및 미납내역 안내드립니다. 내역보기:
9	[Web 발신]더 자세한것은
10	여^기^에^ 너 ^이상한 동영상^ 있^는데 바로 삭제하세요

02
전문가 보안 기고

1. 2017 년 되돌아 봐야 할 보안이슈 Top5 : RISEN

2. 지능화된 타깃 공격, 고도화된 대응 방안으로 맞서야

1. 2017 년 되돌아 봐야 할 보안이슈 Top5 : RISEN

2017 년은 각종 사이버 보안 위협과 신,변종 랜섬웨어, 악성코드의 공격이 증가(Risen)한 해였습니다. 이스트시큐리티 시큐리대응센터(ESRC)는 올해 되돌아 봐야 할 보안이슈 Top 5 로 RISEN 을 선정하였습니다.

1) 끊임없이 진화하는 랜섬웨어 : Ransomwares prevailing

랜섬웨어가 해커들에게 많은 돈을 벌어다 주는 주요 수익원으로 자리잡은 지 벌써 몇 년이 흘렀지만, 2017 년에도 랜섬웨어의 위협은 여전히 사이버 범죄에서 큰 비중을 차지했습니다. 특히 그동안 랜섬웨어의 공격대상이 불특정 다수였다면, 그 대상이 점차 특정 기업/기관으로 변해가고 있는 추세입니다. 그 이유는 개인에 비해 기업/기관이 랜섬웨어에 감염되어 중요 파일이 암호화 되면 그 피해가 막대하기 때문에, 랜섬 비용을 해커에게 지불하여 암호화된 문서를 복구하고자 할 가능성이 높은 타깃을 공격자가 노리고 있다고 볼 수 있습니다.

대다수의 랜섬웨어는 금전적인 수익을 목적으로 하지만, 올해에는 Petya(페트야) 랜섬웨어처럼 시스템 파괴를 목적으로 복호화가 불가능하도록 제작한 와이퍼 악성코드(Wiper Malware)가 등장하기도 하였습니다. 또한 5 월에는 WannaCry(워너크라이) 랜섬웨어를 시작으로 이전에는 거의 활용되지 않았던 네트워크 전파 기능 취약점을 악용해 감염 확산이 빠른 랜섬웨어 공격이 발생하기도 하였습니다. 랜섬웨어 공격은 더욱 새로운 형태로, 더욱 교묘한 방식으로 계속해서 이어지고 있습니다.

2) IoT(사물 인터넷) 기기 타깃 공격의 증가 및 고도화 : IoT targeted attacks

2016 년 말, Mirai(미라이) 악성코드의 등장 이후 IoT 디바이스를 타깃으로 하는 악성코드들의 숫자가 급속도로 증가하고 있으며, 계속해서 그 공격 기법이 고도화되고 있습니다. 기존 Mirai 악성코드가 취약한 비밀번호를 사용하는 IoT 기기를 공격하는 상대적으로 단순한 공격 방식을 택했다면, 2017 년에는 본격적으로 취약점을 악용한 공격이 주를 이루었습니다.

올해 초, Mirai 악성코드와 유사한 기술을 사용하여 IoT 기기들을 영구적으로 망가뜨려 버리는 (PDoS, Permanent Denial of Service) Brickerbot(브리커봇) 악성코드가 발견되었으며, 취약점이 있는 IoT 기기들을 타깃으로 하는 Amnesia(암네시아), Linux.ProxM, IoT_reaper 등의 악성코드들이 지속적으로 등장하였습니다. 특히 Amnesia 악성코드는 리눅스 기반 임베디드 기기에서 동작하는 악성코드로는 처음으로 가상화된 환경에서 실행중인지를 검사하여 우회하려는 등, 공격 기법이 점차 고도화 됨을 보여주었습니다.

최근 사물인터넷 기기 타깃 공격들이 취약점을 통하여 유포되는 만큼, 관련된 감염 기기의 수 또한 매우 빠르게 증가하였고, 그에 따라 IoT 를 이용한 DDoS 공격의 위협도 급격히 증가하고 있어 취약한 기기에 대한 보안이 재조명되고 있습니다.

3) 유명 SW 업데이트 서버를 노린 공격의 증가 : Server targeted attacks

2017 년에는 전 세계적으로 유명 SW 업데이트 서버를 해킹하여 악성코드를 유포하는 대규모 공격이 증가했습니다. 우크라이나 소프트웨어 벤더 사의 서버가 해킹 당해, 수 많은 공공기관들이 Petya(페트야) 랜섬웨어에 감염된 사례가 있었습니다. 또한 글로벌 백신 사의 다운로드 서버 해킹으로 악성코드가 포함된 버전으로 바꿔 치기 된 프로그램이 정상 프로그램을 위장하여 한 달 동안 수 백만명의 사용자들을 감염시키기도 했습니다. 여기에는 2 단계 페이로드가 포함되어 있었으며, 해당 페이로드는 세계적인 거대 IT 기업들을 감염시키기 위한 백도어를 포함하고 있는 것으로 확인되었습니다.

공격자들은 유명 SW 업데이트 서버 노려 단 시간에 전 더 많은 사용자들을 감염시킬 수 있었고, 다시 말해 보다 효율적인 공격이 가능했습니다.

4) 가상 화폐 인기 급상승으로 거래소를 노리는 공격의 증가 : Exchange targeted attacks

가상 화폐에 대한 식을 줄 모르는 관심과 늘어나는 투자자 수에 따라, 해킹이 어려운 가상 화폐 자체보다는 가상 화폐를 거래하는 거래소를 타깃으로 하는 공격이 빠르게 증가하고 있습니다. 국내에서도 최대 가상 화폐 거래소의 해킹 사태로 3 만명에 달하는 회원 정보가 유출된 바 있으며, 이로 인해 다수 고객이 금전적인 2 차 피해를 입었습니다. 뿐만 아니라, 한 거래소는 해킹으로 3,831 비트코인을 도난 당했으며, 21 억원 어치의 가상 화폐가 탈취당한 거래소도 존재했습니다.

가상 화폐 거래소를 노린 공격들은 물론 관련 피해도 현재까지 계속 진행되고 있어, 대책이 시급한 상황입니다.

5) NSA 해킹툴의 공개와 높아지는 위협 : NSA hacking tool hacked

지난 여름, 유명 해커 그룹 Shadow Brokers 가 미국 국가안보국(NSA)이 보유하고 있던 다수의 해킹 툴과 기밀 정보를 해킹했다고 주장했습니다. 이후 그들은 Windows 의 취약점을 공격하는 NSA 해킹 툴을 공개하였고, 전세계 온라인 범죄자들이 취약한 PC 를 해킹하는 데 이를 악용하기 시작했습니다.

그 중 SMB 취약점을 이용해 Windows 의 시스템을 손상시키는 취약점 공격 도구 EternalBlue(이터널블루)는 올해 7 월 WannaCry(워너크라이) 랜섬웨어에 사용되어 전 세계적으로 약 80 억 달러(약 8 조 9000 억 원)에 달하는 피해를 입혔습니다. 또한 최근 러시아를 시작으로 우크라이나와 유럽을 큰 혼란에 빠지게 한 BadRabbit(배드래빗) 랜섬웨어 또한 NSA 해킹 툴을 사용한 것으로 드러났습니다.

02 전문가 보안 기고

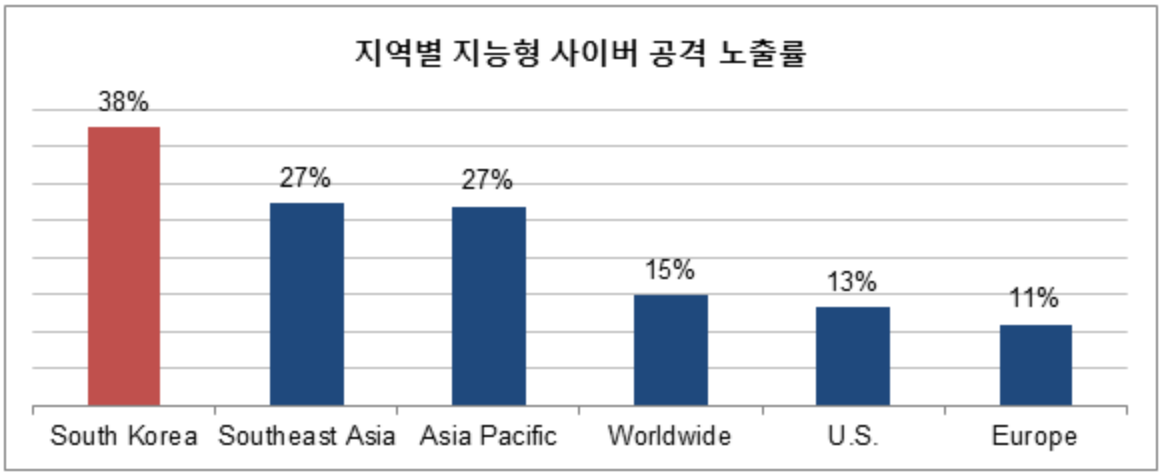
Shadow Brokers 는 이후에도 해킹 툴의 소스 코드와 패스워드를 공개하겠다고 위협했으며, 실제로 몇 차례에 걸쳐 공개된 해킹 툴로 인해 워너크라이 공격과 같은 악용 사례가 다수 발생하고 있습니다. 해킹 툴을 통해 공격 당할 가능성이 있는 취약점에 대한 패치는 꾸준히 진행되고 있으나, 최신 보안 패치를 진행하지 않은 사용자가 많기 때문에 앞으로도 지속적인 공격과 피해가 발생할 것으로 예상됩니다.

2. 지능화된 타깃 공격, 고도화된 대응 방안으로 맞서야

[IMAS 개발팀 백병민 책임]

사이버 공격자들이 점점 더 지능화된 공격을 행하고 있다. 불특정 다수를 대상으로 무차별적인 공격을 퍼붓고, 금전적인 수익을 취하기 위해 특정 기업에게 매우 정교하고 계산된 공격을 시도한다. 빅데이터 의 발달과 클라우드 서비스의 등장과 함께 감시해야 할 대상이 기하급수적으로 늘기까지 했다.

해외 보안 업체 파이어아이에 따르면, 우리나라의 경우 지능형 사이버 공격 노출율이 2015 년 기준 38%에 달한다. 이는 전 세계 평균의 두 배에 달하는 수치며, 미국 평균의 세 배에 육박한다.



[그래프1] 2015 7월-12월 전 세계 지능형 사이버 공격 노출률

급증하는 공격 방식의 발전과 규모에 비해, 국내 기업 및 기관의 대응 체계 고도화는 매우 느리게 진행되고 있다. 조직은 보안 인력을 확충하거나, 인적 대응 리소스의 한계를 극복하기 위해 방화벽과 같은 네트워크 장비를 구축하여 블랙리스트 기반의 접근 차단 방식을 적용하는 등 계속해서 노력해 왔다. 그러나 안타깝게도, 이러한 기존의 대응 방식은 지능화된 위협에 효과적으로 대처하지 못한다는 것이 사실이다. 공격자는 백신의 탐지 기능을 우회할 수 있도록 계속해서 버전을 업데이트하고, 악성 행위를 수행하는 기능을 고도화시킨다.

신·변종 악성파일 구별... 신속한 '분석'이 필요하다

앞서 언급했듯이 장비가 고도화되고, 방어해야 할 대상이 많아지면서 기존과 같은 블랙리스트, 화이트리스트 방식으로는 지능화된 위협에 효과적으로 대응하기 어렵게 됐다. 따라서 조직으로 유입되는 의심 파일에 대한 보다

'신속한 분석'이 필요하다. 파일이 정상인지 악성인지 분석한 후, 알려지지 않은 공격까지 신속하게 차단해내는 방안을 연구해야 한다.

유입 대상을 분석하는 기법에는 여러가지 방식이 있다. 대표적으로 정적 분석 방식과 동적 분석 방식의 두 가지로 구분할 수 있다. 정적 분석은 각종 도구를 이용하여 파일에 존재하는 스트링, imptable, apk 의 dex 정보 등 메타데이터를 추출하고, 특정 URL 의 HTML 과 같은 파일을 내려 받아 그 속의 스크립트와 같은 코드를 확인하여 분석하는 방식을 말한다. 동적 분석은 파일을 실행하여 네트워크 패킷 덤프와 파일이 하는 행위를 모니터링하는 방식이다. 이는 브라우저를 통해 URL 에 접근하여 파일이 다운로드되거나, 다른 사이트로 이동하는지 등을 확인하여 의심 파일 또는 URL 을 사용자가 실제로 실행하거나 접근했을 때 어떻게 동작하는지 모니터링한다. 따라서 악성 여부 판단에 있어 그 신뢰도가 높다. 그러나 동적 분석 시 하나의 샘플을 분석하기 위해 소모되는 하드웨어의 리소스는 정적 분석에 비해 상당하다는 단점이 있다. 기업으로 유입되는 모든 것들에 동적 분석을 적용할 수 있을까? 그 비용을 감당할 수 있는 기업은 그리 많지 않을 것이다.

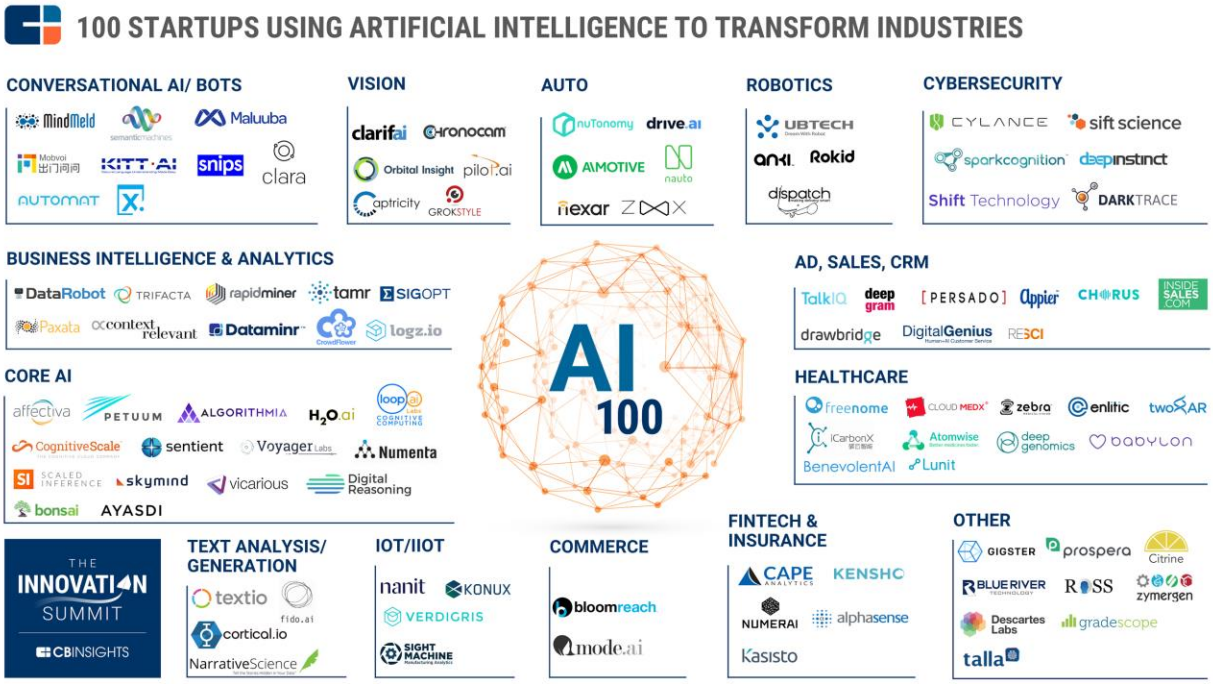
한편 현재 전세계적으로 정적 분석을 통한 사이버 위협 차단 방식이 연구되고 있으나, 단편적인 샘플 분석만으로는 나날이 지능화 되며 발전하는 공격을 막아내는 것은 쉽지 않다는 것이 업계 전반적인 생각이다.

지능화된 위협, 고도화된 방식으로 대응해야

지금 이 순간에도 수 십 만개의 신·변종 악성코드가 제작되고, 유포되는 것을 아는가? 공격을 방어하는 입장에서는 '알려지지 않은 공격'을 면밀히 분석하고, 신속하게 대응 방안을 마련해 대응 체계를 수립해야 한다. 그렇다면 어떠한 분석 기법이 효과적일 수 있을까?

첫째, 의심 파일 분석 시 복합적인 데이터를 이용한 '연관 샘플 선정 방식'을 활용하자. 단순히 의심 파일 하나, 의심 URL 하나만을 분석해서 얻는 데이터만으로 악성 여부를 판단한다면, 근거 데이터가 부족하여 기술적 한계가 발생할 수 있다. 분석가가 URL 분석을 통해 의심 파일 샘플을 획득하고, 이를 분석하여 파일명 또는 해쉬값 같은 정보를 확보했다고 가정해 보자. 이러한 연관 데이터를 조합하면 악성 파일의 유포지를 좀 더 쉽게 파악할 수 있을 것이다. 핵심 유포지를 파악해내면 C&C 서버뿐만 아니라, 악성 파일이 유포되고 있는 모든 사이트에 대한 접근을 막아낼 수 있다.

둘째, 기반 데이터를 축적하기 위해 광범위한 수집 센서를 확보해야 한다. 의심 파일에 대한 위협 여부를 좀 더 정확히 판단하기 위해서는 대량의 기반 데이터가 필요하다. 많은 보안 업체들이 다양한 센서를 광범위하게 보유하기 위해 노력하는 것도 이 때문이다. 그러나 이러한 센서는 하루 아침에 보유할 수 있는 것이 아니다. 개발한 센서를 광범위하게 배포하는 것 또한 매우 어려운 일이므로, 기술적으로 신뢰할 수 있는 업체들과의 제휴가 필요하다.



[그림 1. AI 를 활용한 100 여개 스타트업, 출처: CBInsights]

셋째, 요즘 화두로 떠오르는 AI(Artificial Intelligence)를 활용하는 것도 좋은 방법이다. 이는 앞으로 지능화 되는 공격 방어와 악성 위협 여부를 판단하는 데에 있어 핵심 기술이 될 가능성이 높다. 최근 들어 실제 인공지능이 도입된 악성 판단 기술이 시장에 공개되고 있으며, 나름의 성과를 거두고 있다. IBM 은 자사의 인공지능 솔루션인 왓슨을 보안 관제에 활용하고 있다. 또한 Cylance(사일런스) 사의 사일런스 프로텍트, 스파크코그니션의 DAE 등과 같은 인공지능을 도입한 엔드포인트 제품들이 그 사례이다.

올 초에 보안 전문 업체로 새롭게 출범한 이스트시큐리티의 보안 인텔리전스 플랫폼 IMAS(Intelligence Malware Analysis System)에도 인공지능을 통한 샘플 분석 기능이 적용되어 있으며, 이미 금융보안원과 경찰청, 한국인터넷진흥원 등 성공적인 구축 사례를 보유하고 있다. 또한 이스트시큐리티는 앞으로 보안 인텔리전스를 웹 서비스 형태로도 선보일 예정이다.

넷째, 전문가의 분석 결과를 이용한 '유사 샘플 선정 방식'도 좋은 방안이다. 대표 샘플을 선정하여 이를 상세히 분석하고, 해당 분석 결과를 통해 다른 샘플들과의 유사도를 측정하는 방식을 보조적인 수단으로 활용하는 것은 어떨까? 분석할 샘플이 너무 많다는 것이 문제이긴 하지만, 악성코드 분석 전문가가 직접 분석하는 만큼 정확도와 신뢰도가 높을 것이다.

지금 우리는 사물 인터넷 시대를 살고 있다. 상상했던 것들이 현실로 이뤄지면서 매우 편리해졌지만, 위협을 받을 수 있는 경로 또한 급증했다. 과거 컴퓨터가 다운되는 것에 그쳤던 사이버 공격이 지금은 아주 지능적으로, 조직과 개인의 안위를 위협하고 있다.

따라서 우리는 지능화된 공격에 고도화된 대응 방안으로 맞서야 한다. 앞서 언급한 방식뿐만 아니라, 샘플의 유입 경로, 악성코드의 트렌드, 연관 정보 등과 같은 각종 해석 정보를 활용해 지능화된 타깃 공격을 분석해야 발 빠른 업데이트와 대응 체계 수립이 가능할 것이다. 급증하는 사이버 공격에 맞서, 사이버 위협 대응 체계 또한 계속해서 빠르게 견고해지기를 기대해 본다.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Ransom.MyRansom] 악성코드 분석 보고서

1. 개요

한국을 집중 공격하는 신종 랜섬웨어 'Trojan.Ransom.MyRansom'(이하 마이랜섬 랜섬웨어)가 등장하였다.

케르베르(Cerber) 랜섬웨어의 변형으로 매그니튜드 익스플로잇 킷을 통해 광고 사이트에 악성코드를 심어 유포하는 멀버타이징 방식을 사용한다. 두 단어를 합쳐 매그니베르(Magniber) 라고도 불린다. 한국어 윈도우 운영체제 환경에서만 파일 암호화를 진행하는 특징이 있으며 암호화되는 파일의 확장자는 'hwp' 문서를 비롯해 800 개 이상이다.

본 분석 보고서에서는 MyRansom 랜섬웨어를 상세 분석 하고자 한다.

2. 악성코드 상세 분석

2.1. 40a5312f203f48759cbc1c08f91c499a 분석

1) 시스템 언어 확인

시스템 언어 환경이 한국어를 사용하는 사용자만 대상으로 파일 암호화를 진행한다. 언어 환경이 한국어가 아닐 경우 현재 프로세스를 종료한다.

```
if ( GetSystemDefaultUILanguage() != 1042 )
  sub_4075A0();                                 // exit
if ( sub_406CC0(&Name) )
{
  sub_408E00(&Dst, 260);
  ExpandEnvironmentStringsW(L"%TEMP%", &Dst, 0x103u);
  v132 = (LPVOID)sub_401040(&Dst);
```

[그림 1] 사용자 시스템 언어 확인

2) 중복 실행 확인

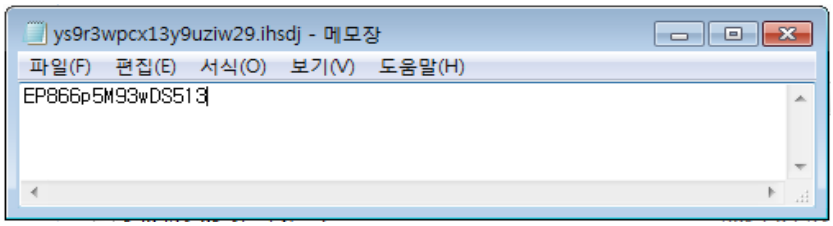
중복실행을 방지하기 위해 Mutex 를 사용한다. Mutex 의 이름은 "ihsdj"이며, 중복실행 중이라면 현재 프로세스를 종료하고 중복실행이 아니라면 랜섬웨어 코드를 진행한다.

```
{
  CreateMutexW(0, 0, lpName);                   // lpName="ihsdj"
  return GetLastError() != 183;
}
```

[그림 2] 중복실행 확인

3) 파일 생성

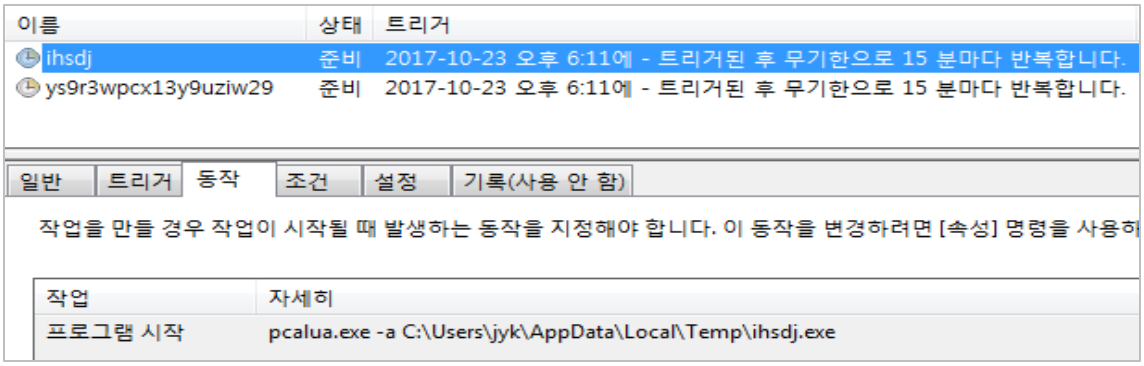
%temp% 경로에 [16 진수 – 19 자].ihsdj 파일을 생성한 후 파일 내용으로 “EP866p5M93wDS513” 문자열을 적어두었다. 이 문자열은 추후 파일 암호화시 Initialization Vector 로 사용될 값이다.



[그림 3] 파일 생성

4) 자가 복제 후 작업 스케줄러 등록

%temp% 경로에 자기 자신을 ihsdj.exe 이름으로 복제한 뒤 윈도우 작업 스케줄러에 랜섬노트 파일과 ihsdj.exe 을 등록하여 15 분마다 실행하도록 설정한다.



[그림 4] 윈도우 작업 스케줄러 등록

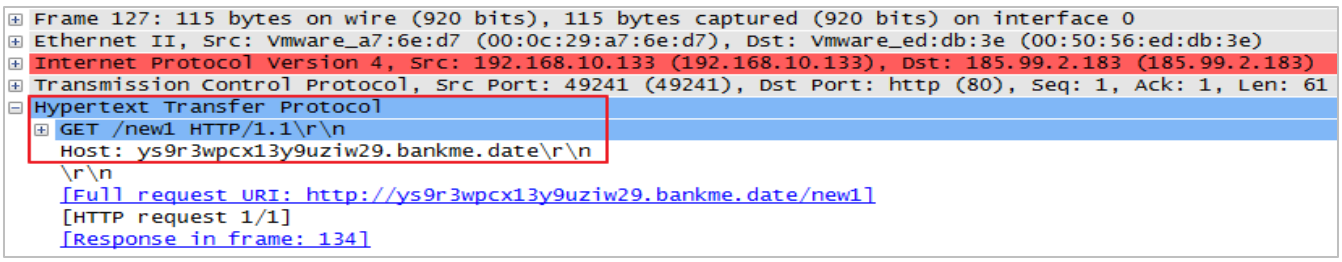
5) 가상화 확인 후 C&C 접속

해당 랜섬웨어는 4 개의 URL 을 사용하며 암호화 시작과 끝, 가상화 환경 여부를 확인 한다. 암호화 하기전 URL 파라미터로 “new” 라는 문자열이, 암호화가 완료된 후에는 "end"라는 문자열이 전송 되며 가상머신에서 구동되는지 확인하고, 그 결과를 URL 파라미터에 첨부한다.

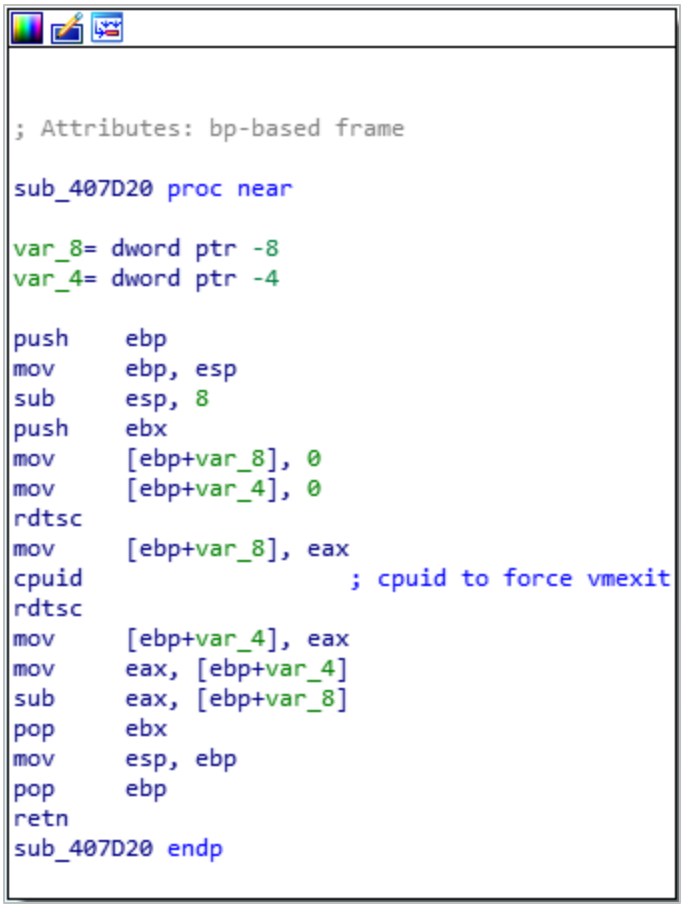
가상머신 확인은 평균적으로 실행에 소요되는 시간을 확인하기 위해 총 10 차례 걸쳐 진행하며, 평균 소요 시간이 1,000 보다 큰 경우 해당 시스템을 가상머신으로 분류한다. 가상머신으로 판단한 경우에는 URL 마지막에 숫자 1 을 기입하고, 가상머신이 아니라고 판단된 경우에는 숫자 0 을 기입한다.

URL 정보	IP 정보	URL 파라미터	가상화 환경체크
bankme.date	185.99.2.183	암호화 시작: new	가상화인 경우: 1
jobsnot.services	192.71.247.13	암호화 완료: end	가상화아닌 경우: 0
carefit.agency	51.255.51.208		
hotdisk.world	212.73.150.211		

[표 1] URL 파라미터 정보



[그림 5] C&C 접속



```
; Attributes: bp-based frame

sub_407D20 proc near

var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 8
push    ebx
mov     [ebp+var_8], 0
mov     [ebp+var_4], 0
rdtsc
mov     [ebp+var_8], eax
cpuid                   ; cpuid to force vmexit
rdtsc
mov     [ebp+var_4], eax
mov     eax, [ebp+var_4]
sub     eax, [ebp+var_8]
pop     ebx
mov     esp, ebp
pop     ebp
retn
sub_407D20 endp
```

[그림 6] 가상화 확인 코드

6) 암호화 대상 파일 검색

암호화 대상은 모든 논리 드라이브를 포함하며, 제외 경로를 제외한 모든 경로이며, 확장자는 “hwp"를 포함한 859 개이다.

```
v9 = L":\\documents and settings\\all users\\";
v10 = L":\\documents and settings\\default user\\";
v11 = L":\\documents and settings\\localservice\\";
v12 = L":\\documents and settings\\networkservice\\";
v13 = L"\\appdata\\local\\";
v14 = L"\\appdata\\locallow\\";
v15 = L"\\appdata\\roaming\\";
v16 = L"\\local settings\\";
v17 = L"\\public\\music\\sample music\\";
v18 = L"\\public\\pictures\\sample pictures\\";
v19 = L"\\public\\videos\\sample videos\\";
v20 = L"\\tor browser\\";
v21 = L"\\$recycle.bin";
v22 = L"\\$windows.~bt";
v23 = L"\\$windows.~ws";
v24 = L"\\boot";
v25 = L"\\intel";
v26 = L"\\msocache";
v27 = L"\\perflogs";
v28 = L"\\program files (x86)";
v29 = L"\\program files";
v30 = L"\\programdata";
v31 = L"\\recovery";
v32 = L"\\recycled";
v33 = L"\\recycler";
v34 = L"\\system volume information";
v35 = L"\\windows.old";
v36 = L"\\windows10upgrade";
v37 = L"\\windows";
v38 = L"\\winnt";
v40 = 0;
for ( i = 0; i < 30; ++i )
{
  if ( sub_406CF0(lpString2, (&v9)[i]) )
    return 0;
}
```

[그림 7]암호화 대상 검색 코드

암호화 제외 대상 경로	
"\documents and settings\networkservice\"	"\intel"
"\appdata\local\"	"\msocache"
"\appdata\locallow\"	"\perflogs"
"\appdata\roaming\"	"\program files (x86)"
"\local settings\"	"\program files"
"\public\music\sample music\"	"\programdata"
"\public\pictures\sample pictures\"	"\recovery"
"\public\videos\sample videos\"	"\recycled"
"\tor browser\"	"\recycler"
"\$recycle.bin"	"\system volume information"
"\$windows.~bt"	"\windows.old"
"\$windows.~ws"	"\windows10upgrade"
"\boot"	"\windows"
	"\winnt"

[표 2] 암호화 제외 대상 경로

암호화 대상 확장자
"doc", "docx", "xls", "xlsx", "ppt", "pptx", "pst", "ost", "msg", "em", "vsd", "vsdx", "csv", "rtf", "123", "wks", "wk1", "pdf", "dwg", "onetoc2", "snt", "docb", "docm", "dot", "dotm", "dotx", "xlsm", "xlsb", "xlw", "xlt", "xlm", "xlc", "xltx", "xltm", "pptm", "pot", "pps", "ppsm", "ppsx", "ppam", "potx", "potm", "edb", "hwp", "602", "sxi", "sti", "sldx", "sldm", "vdi", "vmx", "gpg", "aes", "raw", "cgm", "nef", "psd", "ai", "svg", "djvu", "sh", "class", "jar", "java", "rb", "asp", "php", "jsp", "brd", "sch", "dch", "dip", "p", "vb", "vbs", "ps1", "js", "asm", "h", "pas", "cpp", "c", "cs", "suo", "sln", "ldf", "mdf", "ibd", "myi", "myd", "frm", "odb", "dbf", "db", "mdb", "accdb", "sq", "sqlitedb", "sqlite3", "asc", "lay6", "lay", "mm", "sxm", "otg", "odg", "uop", "std", "sxd", "otp", "odp", "wb2", "slk", "dif", "stc", "sxc", "ots", "ods", "3dm", "max", "3ds", "uot", "stw", "sxw", "ott", "odt", "pem", "p12", "csr", "crt", "key", "pfx", "der", "1cd", "cd", "arw", "jpe", "eq", "adp", "odm", "dbc", "frx", "db2", "dbs", "pds", "pdt", "dt", "cf", "cfu", "mx", "epf", "kdbx", "erf", "vrp", "grs", "geo", "st", "pff", "mft", "efd", "rib", "ma", "lwo", "lws", "m3d", "mb", "obj", "x", "x3d", "c4d", "fbx", "dgn", "4db", "4d", "4mp", "abs", "adn", "a3d", "aft", "ahd", "alf", "ask", "awdb", "azz", "bdb", "bib", "bnd", "bok", "btr", "cdb", "ckp", "clkw", "cma", "crd", "dad", "daf", "db3", "dbk", "dbt", "dbv", "dbx", "dcb", "dct", "dcx", "dd", "df1", "dmo", "dnc", "dp1", "dqy", "dsk", "dsn", "dta", "dtsx", "dx", "eco", "ecx", "emd", "fcd", "fic", "fid", "fl", "fm5", "fo", "fp3", "fp4", "fp5", "fp7", "fpt", "fzb", "fzv", "gdb", "gwi", "hdb", "his", "ib", "idc", "ihx", "itdb", "itw", "jtx", "kdb", "lgc", "maq", "mdn", "mdt", "mrg", "mud", "mwb", "s3m", "ndf", "ns2", "ns3", "ns4", "nsf", "nv2", "nyf", "oce", "oqy", "ora", "orx", "owc", "owg", "oyx", "p96", "p97", "pan", "pdb", "pdm", "phm", "pnz", "pth", "pwa", "qpx", "qry", "qvd", "rctd", "rdb", "rpd", "rsd", "sbf", "sdb", "sdf", "spq", "sqb", "stp", "str", "tcx", "tdt", "te", "tmd", "trm", "udb", "usr", "v12", "vdb", "vpd", "wdb", "wmdb", "xdb", "xld", "xlgc", "zdb", "zdc", "cdr", "cdr3", "abw", "act", "aim", "ans", "apt", "ase", "aty", "awp", "awt", "aww", "bad", "bbs", "bdp", "bdr", "bean", "bna", "boc", "btd", "cnm", "crw", "cyi", "dca", "dgs", "diz", "dne", "docz", "dsv", "dvi", "dx", "eio", "eit", "emlx", "epp", "err", "etf", "etx", "euc", "faq", "fb2", "fb", "fcf", "fdf", "fdr", "fds", "fdt", "fdx", "fdxt", "fes", "fft", "flr", "fodt", "gtp", "frt", "fwdn", "fxc", "gdoc", "gio", "gpn", "gsd", "gthr", "gv", "hbk", "hht", "hs", "htc", "hz", "idx", "iil", "ipf", "jis", "joe", "jp1", "jrtf", "kes", "klg", "knt", "kon", "kwd", "lbt", "lis", "lit", "lnt", "lp2", "lrc", "lst", "ltr", "ltx", "lue", "luf", "lwp", "lyt", "lyx", "man", "map", "mbox", "me", "mel", "min", "mnt", "mwp", "nfo", "njx", "now", "nzb", "ocr", "odo", "of", "oft", "ort", "p7s", "pfs", "pjt", "prt", "psw", "pu", "pvj", "pvm", "pwi", "pwr", "qd", "rad", "rft", "ris", "rng", "rpt", "rst", "rt", "rtd", "rtx", "run", "rzk", "rzn", "saf", "sam", "scc", "scm", "sct", "scw", "sdm", "sdoc", "sdw", "sgm", "sig", "sla", "sls", "smf", "sms", "ssa", "sty", "sub", "sxg", "tab", "tdf", "tex", "text", "thp", "tlb", "tm", "tmv", "tmx", "tpc", "tvj", "u3d", "u3i", "unx", "uof", "upd", "utf8", "utxt", "vct", "vnt", "vw", "wbk", "wcf", "wgz", "wn", "wp", "wp4", "wp5", "wp6", "wp7", "wpa", "wpd", "wp", "wps", "wpt", "wpw", "wri", "wsc", "wsd", "wsh", "wtx", "xd", "xlf", "xps", "xwp", "xy3", "xyp", "xyw", "ybk", "ym", "zabw", "zw", "abm", "afx", "agif", "agp", "aic", "albm", "apd", "apm", "apng", "aps", "apx", "art", "asw", "bay", "bm2", "bmx", "brk", "brn", "brt", "bss", "bti", "c4", "ca", "cals", "can", "cd5", "cdc", "cdg", "cimg", "cin", "cit", "colz", "cpc", "cpd", "cpg", "cps", "cpx", "cr2", "ct", "dc2", "dcr", "dds", "dgt", "dib", "djv", "dm3", "dmi", "vue", "dpx", "wire", "drz", "dt2", "dtw", "dv", "ecw", "eip", "exr", "fa", "fax", "fpos", "fpx", "g3", "gcdp", "gfb", "gfie", "ggr", "gih", "gim", "spr", "scad", "gpd", "gro", "grob", "hdp", "hdr", "hpi", "i3d", "icn", "icon", "iqpr", "iiq", "info", "ipx", "itc2", "iwi", "j", "j2c", "j2k", "jas", "jb2", "jbig", "jbmp", "jbr", "jfif", "jia", "jng", "jp2", "jpg2", "jps", "jpx", "jtf", "jw", "jxr", "kdc", "kdi", "kdk", "kic", "kpg", "lbm", "ljp", "mac", "mbm", "mef", "mnr", "mos", "mpf", "mpo", "mrxs", "my", "ncr", "nct", "nlm", "nrw", "oc3", "oc4", "oc5", "oci", "omf", "oplc", "af2", "af3", "asy", "cdmm", "cdmt", "cdmz", "cdt", "cmx", "cnv", "csy", "cv5", "cvg", "cvi", "cvs", "cvx", "cwt", "cxf", "dcs", "ded", "dhs", "dpp", "drw", "dxb", "dxf", "egc", "emf", "ep", "eps", "epsf", "fh10", "fh11", "fh3", "fh4", "fh5", "fh6", "fh7", "fh8", "fif", "fig", "fmv", "ft10", "ft11", "ft7", "ft8", "ft9", "ftn", "fxg", "gem", "glox", "hpg", "hpg", "hp", "idea", "igt", "igx", "imd", "ink", "lmk", "mgcb", "mgmf", "mgmt", "mt9", "mgmx", "mgtx", "mmat", "mat", "ovp", "ovr", "pcs", "pfv", "plt", "vrm", "pobj", "psid", "rd", "scv", "sk1", "sk2", "ssk", "stn", "svf", "svgz", "tlc", "tne", "ufr", "vbr", "vec", "vm", "vsdm", "vstm", "stm", "vstx", "wpg", "vsm", "xar", "ya", "orf", "ota", "oti", "ozb", "ozj", "ozt", "pa", "pano", "pap", "pbm", "pc1", "pc2", "pc3", "pcd", "pdd", "pe4", "pef", "pfi", "pgf", "pgm", "pi1", "pi2", "pi3", "pic", "pict", "pix", "pjpg", "pm", "pmg", "pni", "pnm", "pntg", "pop", "pp4", "pp5", "ppm", "prw", "psdx", "pse", "psp", "ptg", "ptx", "pvr", "px", "pxr", "pz3", "pza", "pzp", "pzs", "z3d", "qmg", "ras", "rcu", "rgb", "rgf", "ric", "riff", "rix", "rle", "rli", "rpf", "rri", "rs", "rsb", "rsr", "rw2", "rw", "s2mv", "sci", "sep", "sfc", "sfw", "skm", "sld", "sob", "spa", "spe",

"sph", "spj", "spp", "sr2", "srw", "wallet", "jpeg", "jpg", "vmdk", "arc", "paq", "bz2", "tbk", "bak", "tar", "tgz", "gz", "7z", "rar", "zip", "backup", "iso", "vcd", "bmp", "png", "gif", "tif", "tiff", "m4u", "m3u", "mid", "wma", "flv", "3g2", "mkv", "3gp", "mp4", "mov", "avi", "asf", "mpeg", "vob", "mpg", "wmv", "fla", "swf", "wav", "mp3"

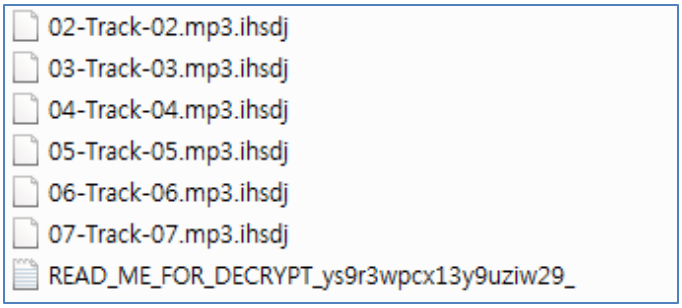
[표 3] 암호화 대상 확장자

7) 파일 암호화

① 파일 암호화는 AES128 를 이용하여 암호화를 하고 암호화가 완료되면 확장자 .ihsdj 가 기존 파일명 뒤에 추가된다.

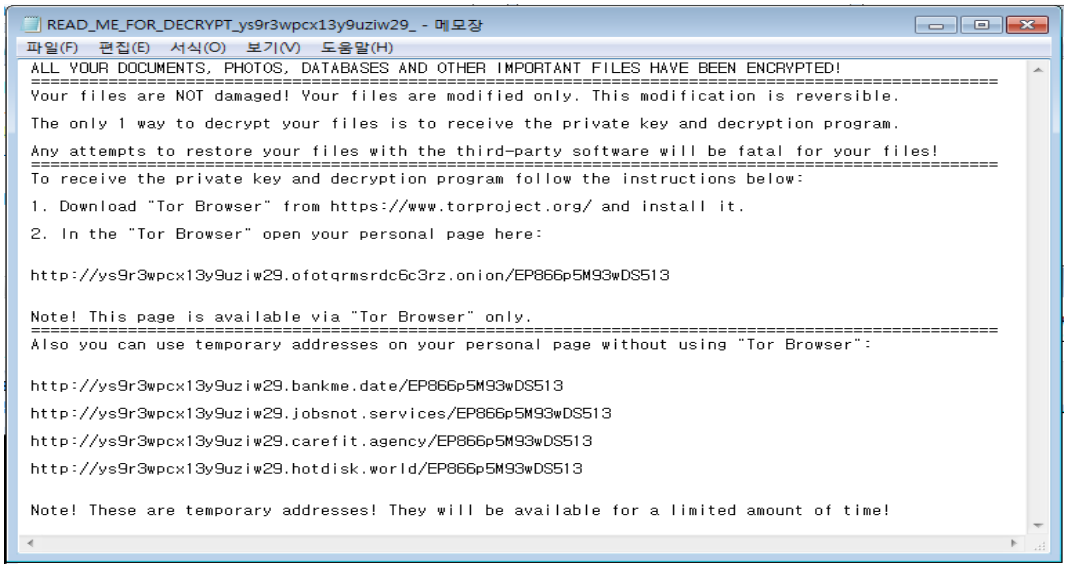
암호화 정보	
IV	EP866p5M93wDS513
AES 128 Key	S2C2E71C7K650Pyl

[표 4] 암호화 정보



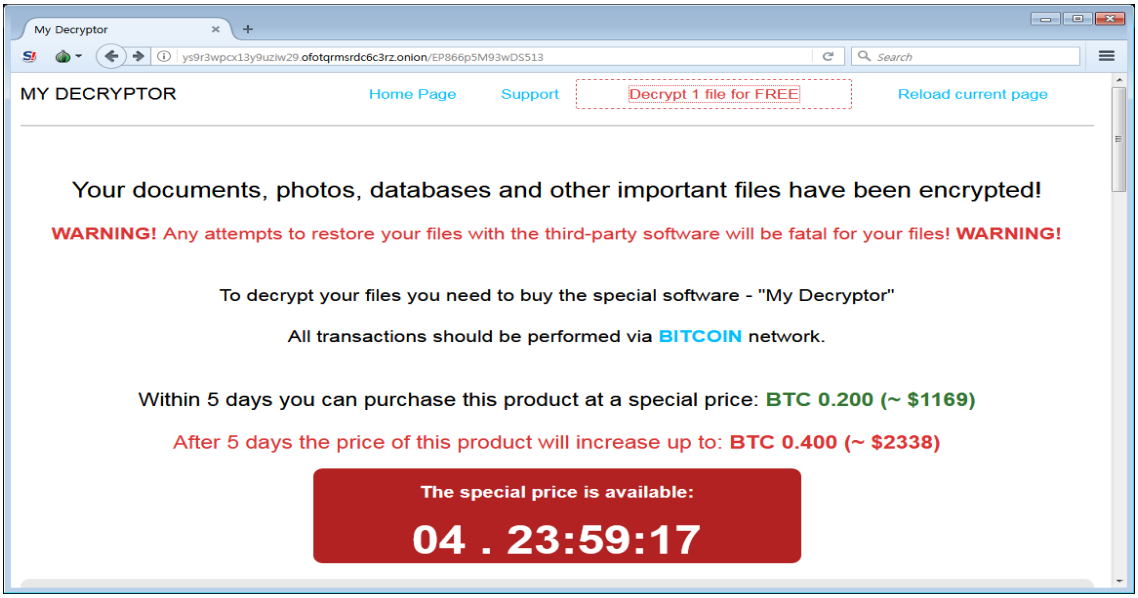
[그림 8]파일 암호화 완료 화면

② 암호화가 완료된 폴더에 생성된 READ_ME_FOR_DECRYPT_[16 진수-19 자] 이름의 랜섬 노트를 보면 사용자 ID 와 데이터 복구를 위해 토르 브라우저 설치를 유도한다.



[그림 9]랜섬 노트 화면

③ 토르 브라우저를 설치하고 personal page 에 접속하면 아래와 같은 화면이 보이고 데이터 복구를 위한 마이디크립터(My Decryptor) 구매를 요구한다. 5 일 이내 구매할 경우 비트코인 0.200(~$1169 – 한화 130 만원)이며, 5 일이 지난 후에는 기존 비트코인의 두 배이다. 참고로 2048KB(2MB) 미만의 1 개의 파일을 무료로 복원해 주는 기능을 제공해주고 있다. 이는 파일 복호화에 대한 가능성을 높여 비트코인 결제율을 올리기 위한 일종의 전략으로 보인다.



[그림 10] 토르 브라우저 접속 화면

3. 결론

한국어 윈도우 운영체제 환경에서만 동작하는 특성 때문에 파일 암호화 전 사용자의 PC 가 한국어 환경인지 확인한 후, 암호화를 진행한다. 암호화되는 파일의 확장자는 'hwp'문서를 비롯해 800 개 이상이다. 따라서 한국어 환경 사용자라면 더욱 주의를 기울여야하며 네트워크 연결이 되지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

또한 본 보고서에서 다룬 악성코드 외에도 확장자를 '.kgpvwnr', '.lhjjnetmm'로 변경하는 MyRansom 변종이 유포되고 있는 것으로 알려져 추가 피해가 발생할 것으로 보인다.

랜섬웨어를 사전에 예방하기 위해서는 메일에 첨부된 파일에 대해서 주의해야 하고, 윈도우 보안 업데이트나 컴퓨터에 설치된 애플리케이션을 항상 최신 상태로 유지해야 한다. 또한 중요한 자료들은 정기적으로 외장 매체에 백업하여 만일에 있을 사태에 대비해야 한다.

04
해외 보안 동향

영미권

중국

일본

1. 영미권

심각한 암호화 결점으로 인해 해커들이 수십억 대 기기에 사용 된 개인 RSA 키 복구 가능해져

Serious Crypto-Flaw Lets Hackers Recover Private RSA Keys Used in Billions of Devices

마이크로소프트, 구글, 레노보, HP, 후지쯔가 고객들에게 독일의 반도체 제작 업체인 Infineon Technologies 에서 제작한 RSA 암호화 라이브러리에 존재하는 심각한 취약점에 대해 경고하고 있다. 이 취약점 (CVE-2017-15361)은 타원 곡선 암호 방식과 암호화 표준 자체에는 영향을 미치지 않으나, Infineon 의 Trusted Platform Module(TPM)이 RSA 키 페어를 생성하는 부분의 구현에 존재한다. Infineon 의 Trusted Platform Module(TPM)은 광범위하게 사용 되며, 암호화 키를 기기에 도입해 하드웨어를 보호하도록 설계 된 전용 마이크로 컨트롤러이며, 보안 암호화 프로세스에 사용된다.

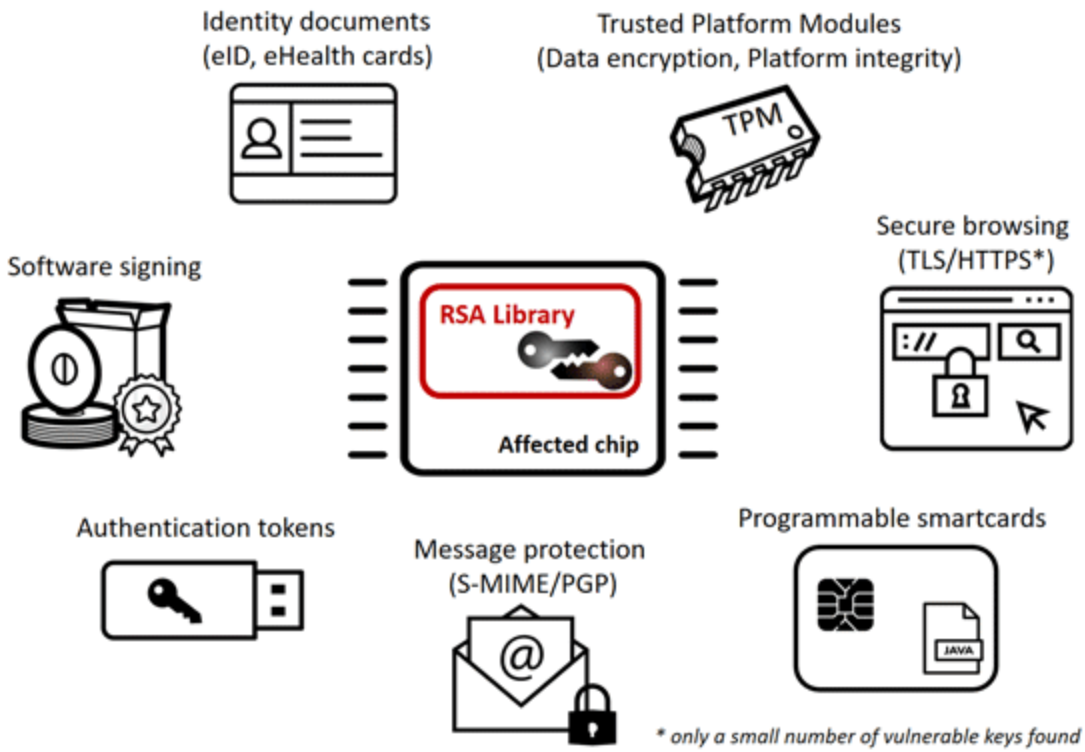
ROCA: 개인 RSA 키 복구를 위한 인수 분해 공격

ROCA(Return of Coppersmith's Attack)라 명명 된 이 인수분해 공격은 원격의 공격자가 타깃의 공개 키만 가지고 있어도 개인 암호화 키를 역계산(reverse calculate)할 수 있도록 허용할 수 있다.

연구원들은 "공개 키만 알면 되고, 취약한 기기에 대한 물리적인 접근은 전혀 필요 없다. 이 취약점은 약하거나 잘못 된 난수 생성기에 의존하지 않는다. 이 취약한 칩을 통해 생성 된 모든 RSA 키들이 영향을 받는다."고 밝혔다.

이로써 공격자가 키 주인을 사칭해 피해자의 기밀 데이터를 복호화 하고, 악성 코드를 디지털 서명 도니 소프트웨어에 주입하며, 접근 또는 침입을 막아둔 타겟 컴퓨터의 보호장치를 우회할 수 있게 된다.

ROCA 공격, 수십억 대의 기기들을 공격에 노출 시켜



ROCA 공격은 2012 년 초부터 Infineon 에서 제작 된 칩에 영향을 미치며 ID 카드, 패스워드를 안전하게 저장하기 위해 사용하는 PC 마더보드, 인증 토큰, 보안 브라우징, 소프트웨어 및 응용 프로그램 서명, PGP 와 같은 메시지 보호 등에도 사용 되는 2014 및 2048 비트를 포함한 키 길이에도 가능하다. 이 취약점은 Infineon 의 암호화 라이브러리 및 칩을 사용해 보호하는 정부 및 기업의 컴퓨터들의 보안에도 영향을 미친다.

HP, 레노보, 후지쯔에서 개발한 윈도우 및 구글 크롬북 기기들도 ROCA 공격에 영향을 받는다.

테스팅 툴 및 패치

보안 연구원들은 이 버그에 대한 탐지, 완화 및 해결법에 대해 공개했다. 이 취약점은 올 2 월 발견 되어 Infineon Technologies 에 제보 되었으며, 연구원들은 11 월 2 일 ACM 컨퍼런스에서 인수분해 방법을 포함한 모든 세부 정보를 공개할 예정이다. 이 취약점이 어떻게 동작하는지, 어떻게 악용할 수 있는지에 대한 세부 정보가 공개 되기 전까지 회사 및 조직들은 영향을 받는 암호화 키를 변경해야 할 것이다. Infineon, Microsoft, Google, HP, Lenovo, Fujitsu 와 같은 주요 벤더들은 이미 하드웨어/소프트웨어용 업데이트와 이 취약점의 완화를 위한 가이드라인을 발표한 상태이다. 따라서 사용자들은 되도록 빨리 기기를 패치 하기를 권고한다.

[출처] https://thehackernews.com/2017/10/rsa-encryption-keys.html

https://crocs.fi.muni.cz/public/papers/rsa_ccs17

급격히 증가하고 있는 새로운 IoT 봇넷, 인터넷 중단 위협해

New Rapidly-Growing IoT Botnet Threatens to Take Down the Internet

대규모 DDoS 공격을 실행해 인터넷 정전을 일으킨 가장 큰 IoT 기반의 멀웨어인 Mirai 가 등장한지 1 년 후인 지금, 보안 연구원들은 급격히 증가하고 있는 새로운 IoT 봇넷에 대해 경고했다. 'IoT_reaper'라 명명 된 이 새로운 멀웨어는 지난 9 월 30 일 처음 발견 되었다.

이 멀웨어는 IoT 기기의 더 이상 취약한 패스워드를 해킹하는 것에 의존하지 않는다. 대신, 이는 다양한 IoT 기기의 취약점들을 이용해 이들을 봇넷 네트워크에 종속시킨다. IoT_reaper 멀웨어는 현재 아래 9 개 제조사의 IoT 기기에 존재하는 취약점을 악용하고 있다:
Dlink (routers)
Netgear (routers)
Linksys (routers)
Goahead (cameras)
JAWS (cameras)
AVTECH (cameras)
Vacron (NVR)

연구원들은 IoT_reaper 멀웨어가 이미 2 백만 대의 기기들을 감염시켰으며, 하루 1 만대의 새로운 기기들을 감염시켜 놀라운 속도로 증가하고 있다고 밝혔다. Mirai 가 대규모 DDoS 공격을 통해 DNS 제공업체인 Dyn 을 중단시키는데는 단 10 만대의 감염된 기기가 사용 되었기 때문에, 이는 매우 우려스러운 일이라 볼 수 있다. 이 외에도 연구원들은 해당 멀웨어가 100 DNS 오픈 resolver 를 포함하고 있어 DNS 증폭 공격을 실행할 수도 있다고 밝혔다.

연구원들은 "현재 이 봇넷은 초기 확장 단계에 있다. 하지만 제작자는 활발히 코드를 수정하고 있기 때문에 경계가 필요하다."고 말했다. 또한 다른 연구원들도 이미 수 십만대의 기기들을 감염 시킨 "IoTroop" 멀웨어에 대해 경고하고 있다. 이 둘은 동일한 멀웨어인 것으로 추정된다.

연구원들은 "범죄자들의 의도를 확실히 파악하기에는 아직 이른 단계이지만, 인터넷을 근본적으로 차단한 과거의 봇넷 DDoS 공격이 다시 실행 될 경우 공격이 시작되기 전 조직들은 적절한 준비와 방어 메커니즘을 갖추는 것이 중요하다."고 밝혔다. 연구원들에 의하면 IoTroop 멀웨어들도 GoAhead, D-Link, TP-Link, AVTECH, Linksys, Synology 등에서 제조한 무선 IP 카메라의 취약점들을 악용한다.

아직까지는 이 봇넷을 만든 사람이 누구인지, 이유가 무엇인지는 알 수 없지만 이 DDoS 위협은 아주 급격히 증가하고 있으며 초당 수십 테라비트 규모에 이를 수 있다. 사용자들은 스마트 기기의 보안에 좀 더 주의를 기울여야 한다.

[출처] https://thehackernews.com/2017/10/iot-botnet-malware-attack.html

패치 되지 않은 마이크로소프트 DDE 익스플로잇, 광범위한 멀웨어 공격에 사용 돼

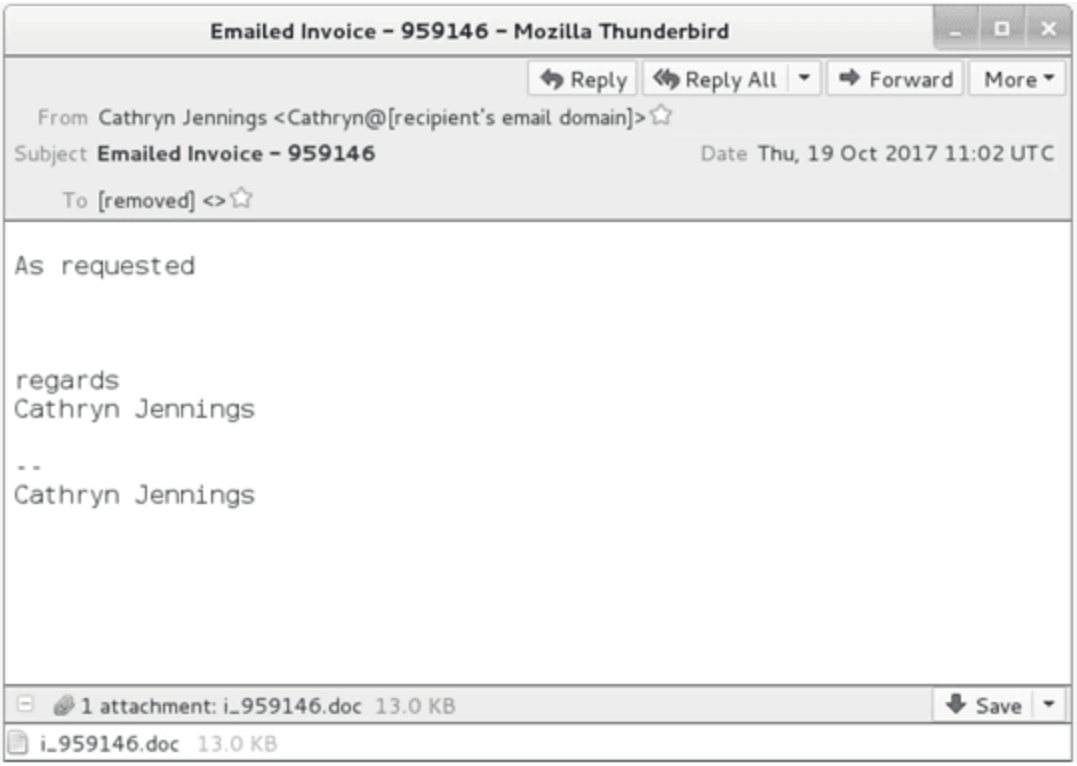
Unpatched Microsoft Word DDE Exploit Being Used In Widespread Malware Attacks

마이크로소프트의 내장 기능을 악용하는 패치 되지 않은 공격 방식이 현재 광범위한 멀웨어 공격 캠페인에 사용 되고 있는 것으로 나타났다. DDE 프로토콜은 마이크로소프트가 두 개의 실행 중인 프로그램들이 동일한 데이터를 공유할 수 있도록 하는 여러 방법들 중 하나다.

이 프로토콜은 엑셀, 워드, Quattro Pro, Visual Basic 을 포함한 수 천개의 프로그램들에서 1 회성 데이터 전송 및 지속적인 업데이트 교환 등을 위해 사용하고 있다. DDE 의 익스플로잇 기술은 피해자에게 해당 응용 프로그램을 실행할지 묻는 것 이외에는 어떠한 "보안"경고도 표시하지 않는다. 하지만 이 팝업 마저 "적절한 구문 수정"을 통해 제거될 수 있다.

연구원들은 DDE 공격 테크닉이 공개 된 직후, 이 공격을 활발히 악용하고 있는 공격 캠페인에 대한 보고서를 공개했다. 이는 파일이 없는 원격 접속 트로이목마(RAT)인 DNSMessenger 를 통해 여러 조직들을 공격하고 있었다.

Necurs 봇넷, Locky 랜섬웨어 배포를 위해 DDE 공격 사용해



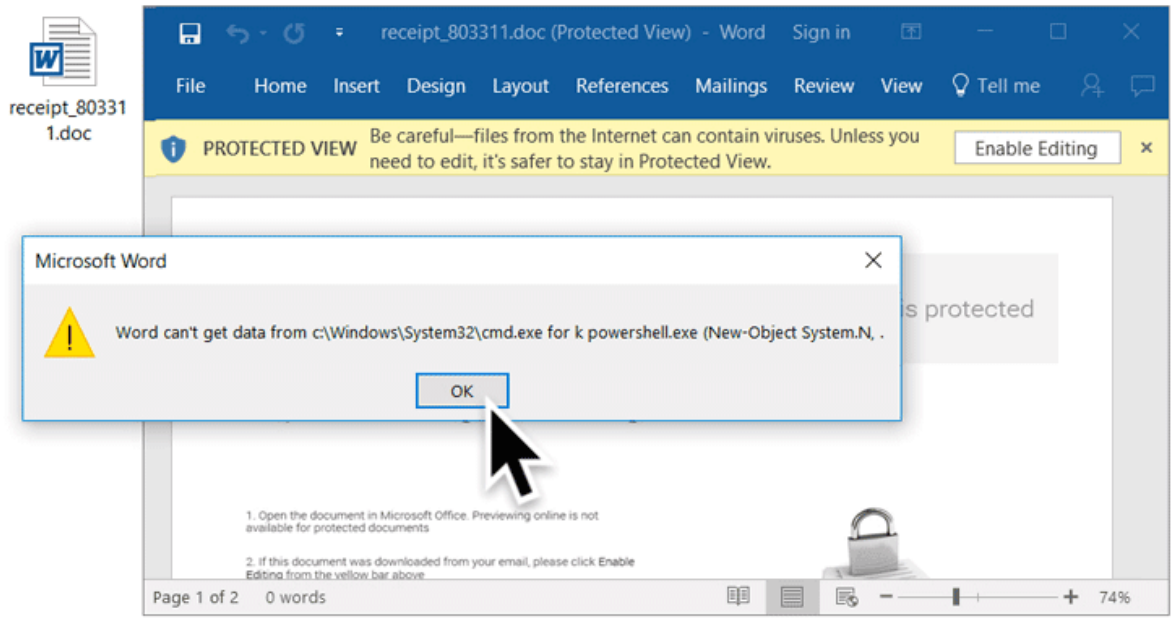
해커들이 전 세계 600 만대 이상의 감염 된 컴퓨터들을 제어하고 수 백만통의 이메일을 보내는 Necurs 봇넷을 이용해

Locky 랜섬웨어와 TrickBot 뱅킹 트로이목마를 배포하고 있는 것으로 나타났다. 이 공격에는 새로이 발견 된 DDE 공격 기술을 사용하는 워드 문서를 사용한다.

Locky 랜섬웨어의 해커들은 기존에는 매크로 기반의 마이크로소프트 오피스 문서를 사용했지만, 지금은 DDE 익스플로잇을 사용하도록 Necurs 봇넷을 업데이트해 멀웨어를 배포하고 피해자의 데스크탑 스크린샷을 촬영할 수 있는 기능을 추가했다.

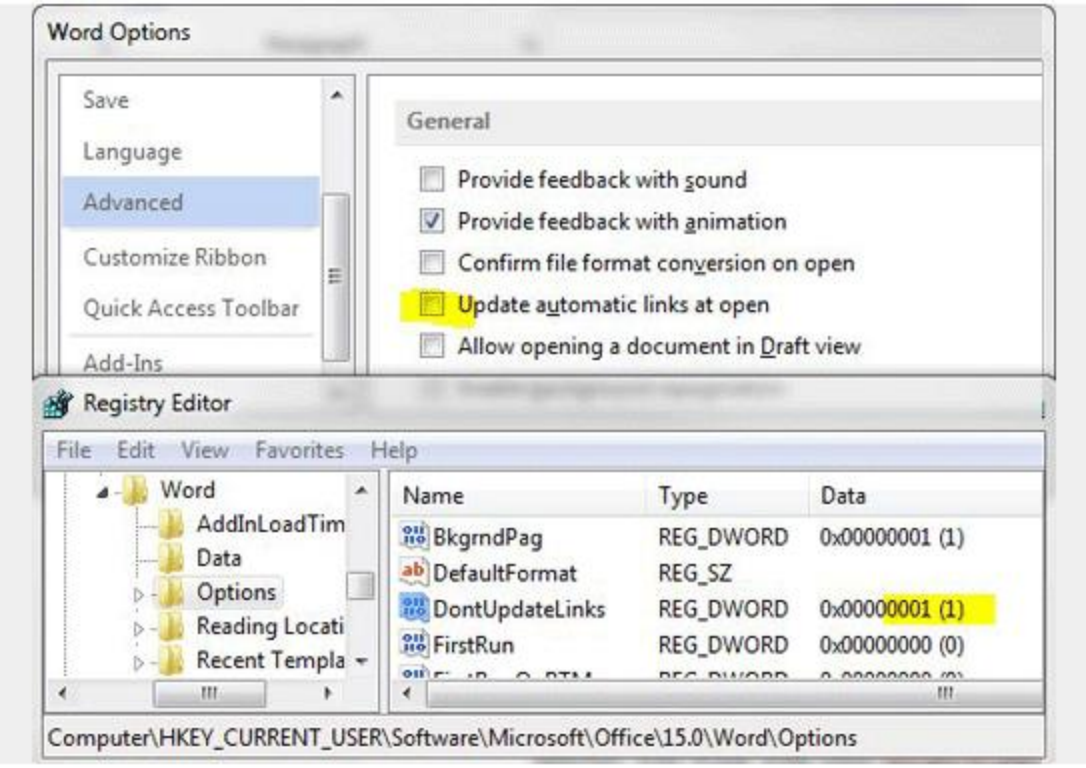
연구원들은 "이 새로운 공격의 흥미로운 점은, 피해자를 원격으로 조작할 수 있다는데 있다. 이는 스크린샷을 찍어 원격 서버로 보낼 수 있다. 또한 실행 도중 다운로더에 발생하는 모든 에러의 세부 사항들도 보낼 수 있다."고 밝혔다.

Hancitor 멀웨어도 DDE 공격 사용해



또 다른 멀웨어 스팸 캠페인도 마이크로소프트 오피스 DDE 익스플로잇을 악용해 Hancitor 멀웨어(Chanitor, Tordal 이라고도 알려짐)를 배포하고 있는 것으로 나타났다. Hancitor 는 감염 된 기기에 뱅킹 트로이목마, 데이터 탈취 멀웨어, 랜섬웨어 등 악성 페이로드를 설치하는 다운로더로 기존에는 매크로가 활성화 된 마이크로소프트 오피스 문서를 피싱 이메일에 첨부하는 방식으로 배포되었다.

Word DDE 공격으로부터 보호하는 법



DDE 는 마이크로소프트의 정식 기능이기 때문에, 대부분의 안티바이러스 솔루션들이 이에 대해 경고하거나 차단하지 않는다. 또한 마이크로소프트도 이 기능을 제거하기 위한 패치를 발행할 계획이 없다.

따라서 마이크로소프트 오피스의 "문서를 열 때 자동 연결 업데이트" 옵션을 비활성화 하는 방법으로 이 공격을 예방할 수 있다. 워드 프로그램을 열고 파일 〉 옵션 〉 고급 〉 일반으로 이동해 "문서를 열 때 자동 연결 업데이트"옵션의 체크를 해제하면 된다.

[출처] https://thehackernews.com/2017/10/ms-office-dde-malware-exploit.html

2. 중국

중국 코인 거래소 OK Coin 의 파생 거래소 OKEx, 해커 공격을 받아 304 만 달러 상당의 비트코인 탈취

OKCoin 国际站旗下交易所现大量账户被盗，用户称损失比特币价值过千万

OKEx, OKCoin 의 사용자 계정이 탈취당해 약 600 여개의 비트코인이 탈취당했다.

9 월 28 일 오전, OKEx 거래소의 계정 하나가 독일 IP 로 로그인이 되었으며, BTC-ETC 거래를 통하여 한 시간 만에 200 개의 비트코인을 모두 팔았다. OKEx 회원은 "해커의 계정 탈취에 대해서는 플랫폼과는 무관하다고 하고 있기 때문에, 피해자는 스스로 제보를 해야한다."고 말했다.

또 다른 블로거는 "현재까지 피해를 입은 사람들은 9 명이며, 그 수는 계속 늘어나고 있으며, 지금까지의 피해금액은 총 304 만달러로 추산된다. 사용자들은 OK 코인의 DB 가 해킹을 당했거나, 혹은 거래를 종료한 서비스의 임직원들이 해커에게 사용자 계정정보를 제공하여 해당 정보를 바탕으로 해커들이 사용자 계정을 해킹한 것이 아닌가라고 의심하고 있다"라고 밝혔다.

OKEx 는 중국의 가상화폐 거래소인 OKCoin 이 만든 거래소로, 가상화폐 거래 및 플러스 레버리지 가상화폐 선물거래 서비스를 제공한다. OKEx 는 레버리지와 헤징 기능이 모두 있는데, 이 두 디지털 자산 간 자유롭게 전환이 가능하며, 사용자는 비트코인을 이용하여 직접 라이트코인, 이더리움 등으로 전환할 수 있다.

공개된 자료에 따르면, OKCoin 글로벌 플랫폼과 OKEx 계정은 따로 분리가 되어 있어 두 플랫폼에서 각각 독립적으로 충전 및 인출이 가능하다고 한다. 또한 사용자는 OKCoin 글로벌 계정을 통하여 직접 OKEx 플랫폼에 로그인할 수도 있다고 밝혔다.

[출처] http://www.1caixin.com.cn/finance/37312823.html

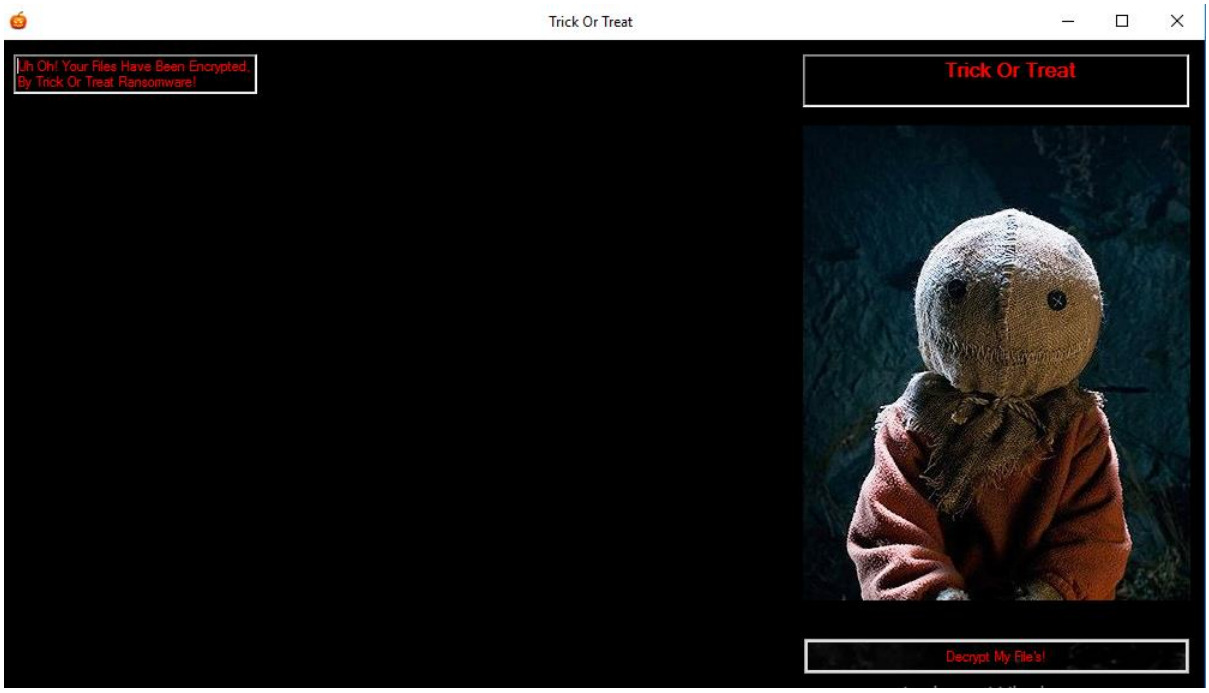
만우절을 노린 악성코드

病毒也爱万圣节,换装出行来"搞鬼"

악성코드 제작자들이 만우절을 맞이하여 들뜬 분위기를 이용하여 악성코드 유포 기회를 엿보고 있는 것으로 보인다. 악성코드가 컴퓨터에서 "만우절 축제" "만우절 즐기기" 등 검색 빈도수가 높은 키워드들을 노리고 있는 것으로 확인되었다.

악성코드들은 사용자들이 관심을 갖을 만한 컨텐츠를 제작해 놓고 사용자들의 다운로드를 유도한다. 만약 사용자들이 악성코드를 실행하면, 윈도우 후킹 프로그램을 이용하여 키보드와 마우스를 모니터링하며, 사용자의 개인정보를 탈취한다.

정보 탈취 악성코드 분만 아니라 만우절을 타깃으로 한 Fake Ransomware 도 유포되었다.



해당 랜섬웨어 역시 만우절과 관련된 컨텐츠와 아이콘으로 사용자들을 유혹한다. 사용자들이 해당 악성코드를 실행하면, 랜섬웨어 UI 가 뜨면서 비트코인을 요구하며 사용자들을 협박한다.

이러한 악성코드의 위협에서 안전하려면, 출처불분명한 곳에서 파일을 내려 받지 말고, 공식 사이트에서 SW 를 내려 받아야 한다.

[출처] http://news.yesky.com/hotnews/29/400007529.shtml

3. 일본

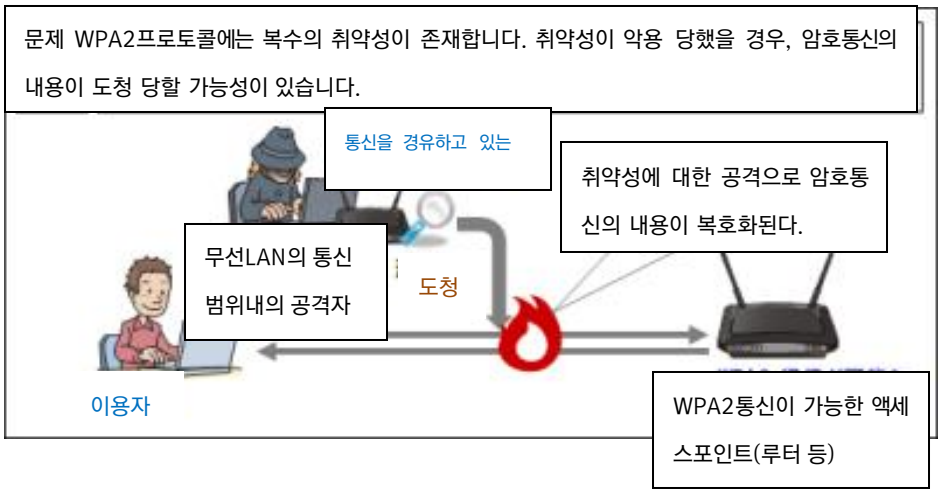
WPA2 취약성 'KRACKs', HTTPS 통신 시는 영향 받지 않아 무선 LAN 과 VPN 의 이용도 추천

WPA2 脆弱性「KRACKs」、HTTPS 通信時は影響受けず、有線 LAN や VPN の利用も推奨

독립행정법인 정보처리추진기구(IPA)를 비롯하여 주식회사 시만텍과 트렌드마이크로, 카스퍼스키 등의 보안업체가 WPA2 의 취약성 'KRACKs'에 대해서 주의를 권고하고 있다. IPA 에 따르면, 현 시점에서는 취약성의 실증코드와 피해는 확인되지 않았다. 그러나 향후 취약성을 악용한 공격이 발생할 가능성이 있다고 한다.

회피책으로는 OS 벤더와 Wi-Fi 기기 벤더 각 사가 제공하는 보안 수정 패치를 적용하면 좋지만, 패치가 제공되지 않는 기기의 경우는 IPA 와 시큐리티벤더 각 사에서는 무선 LAN 과 VPN 의 이용을 추천하고 있다.

또한 IPA 에서는 '본 취약성에 의해 HTTPS 의 통신이 복호되는 일은 없다'라고 한다. 웹사이트 열람 시에 유저 측에 HTTP 와 HTTPS 의 통신을 선택할 수는 없지만, 어떤 웹사이트와의 통신이 안전한 것인지를 파악하는 것은 가능하게 된다.



카스퍼스키는 공식 블로그에서 웹 브라우저의 어드레스 바에 녹색의 열쇠 아이콘이 표시되어 있는지 여부를 항상 확인하도록 권하고 있다. 그래서 현재 표시되고 있는 웹 사이트와의 통신에 HTTPS 인지 여부를 알 수 있는 것이다.

시만텍에서는 이 취약성에 대해서 WPA2 암호화를 이용하는 디바이스 모두가 대상이 되지만, 디바이스에 따라 차이는

있다고 한다. 취약성의 발견자인 Mathy Vanhoef 씨의 견해로는 이 공격이 Linux 와 Android 6.0 이후에 많이 이용되고 있는 Wi-Fi 클라이언트인 'wpa_supplicant'의 버전 2.4 이후에서는 '특히 치명적'이라는 점을 언급하고 해당되는 디바이스에서 송신되는 트래픽의 방수(傍受)라는 악용은 '아주 간단하다'고 한다.

트렌드마이크로에 따르면, 이 취약성은 WPA2 의 인증절차 중 하나로 통신 트래픽을 암호화하는 '키'의 생성 시에 사용되는 '4-way handshake'에 존재한다. 암호화 시에 키와 함께 이용되는 보조적 변수 'nonce'는 본래는 보안 보호를 위해 그때마다 생성되어야 하지만 취약성의 악용으로 이것이 몇 번이나 재이용될 우려가 있다.

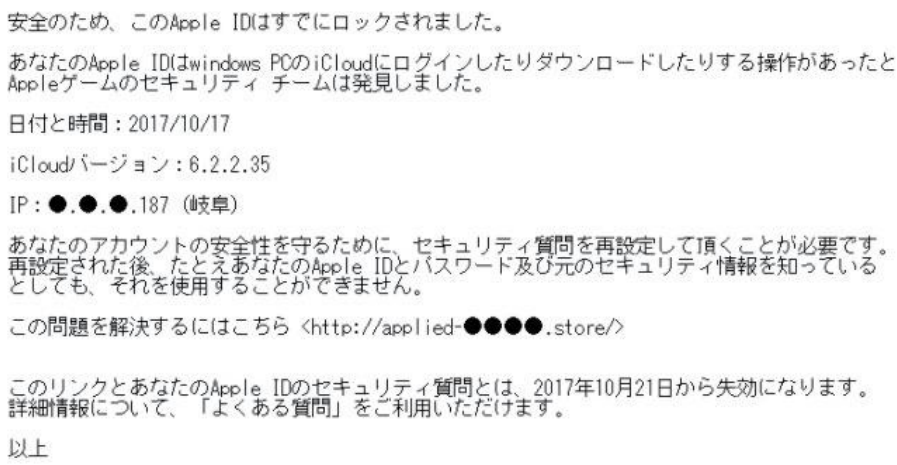
카스퍼스키에 따르면, 공격자가 취약성을 악용하기 위해서는 기존의 것과 같은 SSID 의 Wi-Fi 접속포인트를 설치하여 표적이 액세스 포인트에 접속하고자 했을 때 특별한 패킷을 보내 통신 채널을 교체하여 가짜 액세스포인트에 접속시키는 것이 가능하다고 한다. 그 이후는 통신 내용 조작과 도청이 가능하게 된다고 한다.

[출처] https://internet.watch.impress.co.jp/docs/news/1086546.html

‘Apple ID 의 시큐리티 질문을 재설정해 주십시오’ Apple 을 사칭하는 피싱메일 유포

「Apple ID のセキュリティ質問を再設定してください」 Apple かたるフィッシングメール出回る

‘당신의 Apple ID 의 시큐리티 질문을 재설정해 주십시오’ ——Apple 을 사칭하는 이런 제목의 피싱메일이 유포되고 있다고 해서 피싱대책협의회가 10 월 23 일, 주의를 권고했다.



安全のため、このApple IDはすでにロックされました。

あなたのApple IDはwindows PCのiCloudにログインしたりダウンロードしたりする操作があったと
Appleゲームのセキュリティ チームは発見しました。

日付と時間：2017/10/17

iCloudバージョン：6.2.2.35

IP：●.●.●.187 (岐阜)

あなたのアカウントの安全性を守るために、セキュリティ質問を再設定して頂くことが必要です。
再設定された後、たとえあなたのApple IDとパスワード及び元のセキュリティ情報を知っている
としても、それを使用することができません。

この問題を解決するにはこちら <http://applied-●●●●.store/>

このリンクとあなたのApple IDのセキュリティ質問とは、2017年10月21日から失効になります。
詳細情報について、「よくある質問」をご利用いただけます。

以上

안전 때문에 이 Apple ID 는 이미 차단되었다.

당신의 Apple ID 는 windows Pc 의 iCloud 에 로그인하거나 다운로드하거나 하는 조작이 있었다고 Apple 게임의 시큐리티 팀은 발견했다.

일자와 시간: 2017/10/17

iCloud 버전: 6.2.2.35

IP: ●.●.●.187

당신의 계정의 안전성을 지키기 위해 시큐리티 질문을 재설정해 두는 것이 필요하다.

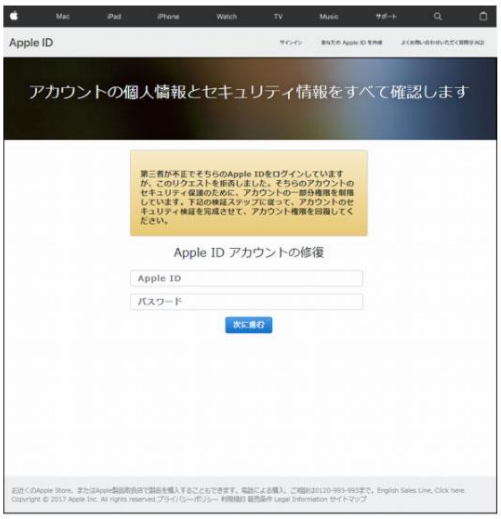
재설정된 후, 가령 당신의 Apple ID 와 패스워드 및 전 시큐리티 정보를 알고 있다고 해도 그를 사용할 수 없다.

이 문제를 해결하기 위해서는 이쪽 http://applied-●●●●.store/

이 링크와 당신의 Apple ID 의 시큐리티질문은 2017 년 10 월 21 일부터 실효가 되었다.

상세한 정보에 대해서 ‘자주 하는 질문’을 이용하시오.

이상



계정 개인정보와 시큐리티 정보를 모두 확인합니다
제삼자가 부정으로 이쪽 Apple ID를 로그인하고 있지만, 이 리퀘스트를 거부했습니다. 이쪽 계정의 시큐리티 보호를 위해서 계정의 일부 정보를 제한하고 있습니다. 아래의 검증스텝에 따라 계정 시큐리티 검증을 완성시켜서 계정권한을 회복해 주십시오.

메일 본문에는 '안전을 위해, 이 Apple ID 는 이미 차단되었습니다' 등으로 쓰여져 있고 피싱페이지로 유도한다. 피싱페이지에서는 Apple ID 와 패스워드, 성명, 주소, 신용카드번호, 시큐리티질문 등을 입력하도록 요구한다.

협의회는 이와 같은 사이트에 Apple ID 와 패스워드, 개인정보를 입력하지 않도록 주의를 호소하고 있다.

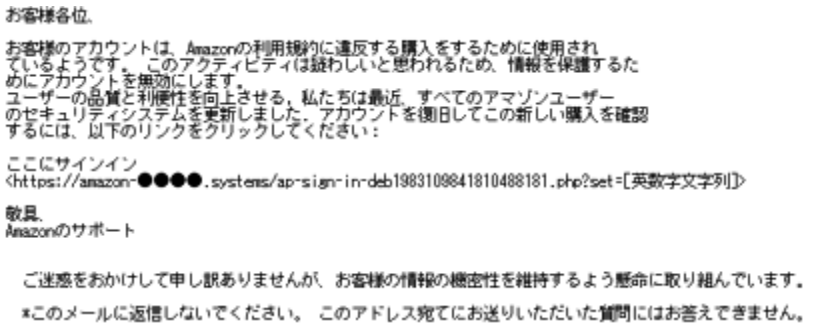
[출처] http://www.itmedia.co.jp/news/artides/1710/24/news047.html

‘Amazon 의 이용규약 위반 혐의로 계정을 무효로 한다’라고 속여 개인정보와 신용카드정보를 빼앗는 피싱메일 주의

「Amazon の利用規約違反の疑いでアカウントを無効にする」と偽り、個人情報やクレカ情報をだまし取るフィッシングメールご注意

Amazon 을 사칭하는 피싱 메일이 유포되고 있다고 해서 피싱대책협의회가 26 일, 긴급 정보를 공지했다. 유도하는 피싱사이트는 같은 날 11 시 현재도 가동 중이라고 하며 계정정보(메일어드레스, 패스워드 등)와 신용카드정보를 절대 입력하지 않도록 주의를 호소하고 있다.

메일 제목은 ‘필요한 액션: 당신의 Amazon 계정은 보안상의 이유로 차단되어 있다’ 또는 ‘이 계정은 일시적으로 정지되었다’였다. 본문에는 ‘Amazon 의 이용규약을 위반한 구입을 하기 위해 사용되고 있는 것으로 보인다. 이 액티브는 수상하다고 생각되기 때문에 정보를 보호하기 위해 계정을 무효로 하겠다’라고 설명하며 계정 복구를 권하여 본문의 링크에서 가짜 사이트로 유도한다.



お客様各位、

お客様のアカウントは、Amazonの利用規約に違反する購入をするために使用されているようです。 このアクティビティは疑わしいと思われるため、情報を保護するためにアカウントを無効にします。
ユーザーの品質と利便性を向上させる，私たちは最近、すべてのアマゾンユーザーのセキュリティシステムを更新しました。アカウントを復旧してこの新しい購入を確認するには、以下のリンクをクリックしてください：

ここにサインイン
<https://amazon-●●●●.systems/ap-sign-in-deb19831098418104881 81.php?set=[英数字文字列]>

敬具、
Amazonのサポート

ご迷惑をおかけして申し訳ありませんが、お客様の情報の機密性を維持するよう懸命に取り組んでいます。
*このメールに返信しないでください。 このアドレス宛てにお送りいただいた質問にはお答えできません。

메일에 기재되어 있는 가짜 사이트의 URL 은
‘https://amazon-●●●●.systems/ap-sign-in-deb19831098418104881 81.php?set=[영어 숫자]’,
‘https://amazon.co.jp.●●●●.com/case-id-18389149909.php?set=[영어 숫자]’였다.

전송처의 URL 은
‘https://amazon-●●●●.systems/identifier/signin.php?set=[영어 숫자]’
‘https://amazon.co.jp.●●●●.com/identifier/signin.php?set=[영어 숫자]’였다.

전송처의 가짜 사이트에서 ID 와 패스워드를 입력하여 사인 인 하면, 다음 화면에서 신용카드 정보의 입력 화면이 표시된다.

Amazon 에서는 피싱메일에서 자주 보이는 내용의 경향으로 1)주문하지 않은 상품의 주문 확인을 촉구하는 것, 2)계정에 등록된 개인정보와 지불 정보의 갱신을 요구하는 것을 들고 있다.

메일의 도메인에 이상한 점이 없는지 확인하고, 첨부파일과 소프트웨어 설치를 요구하는 내용의 메일에도 주의하도록 경고하고 있다.

[출처] https://internet.watch.impress.co.jp/docs/news/1088192.html

(주)이스트시큐리티

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