이스트시큐리티

보안 동향 보고서

No.122 2019.11

No.122 2019.11

이스트시큐리티 보안 동향 보고서

CONTENTS

01 악성코드 통계 및 분석 01-05

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

02 전문가 보안 기고 06-21

위협 인텔리전스 결합한 EDR로 승부 – 김준섭 부사장 인터뷰

금성121, 북한 이탈주민 후원 사칭 '드래곤 메신저' 모바일 APT 공격 수행

03 악성코드 분석 보고 22-24

04 글로벌 보안 동향 25-34

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2019 년 10 월에는 랜섬웨어와 더불어 다양한 APT 공격이 발견된 달이었습니다.

10 월 초 코니(Konni)조직의 HWP 취약점을 악용한 'Coin Plan' 작전을 시작으로 10 월 중순에는, 김수키(Kimsuky)조직의 '대북 분야 국책연구기관'을 사칭한 스피어피싱 공격이 발견되었고, TA505 조직의 회계법인 송장, 견적서등을 사칭한 악성 오피스 문서의 매크로 기능을 활용한 공격이 발견되기도 하였습니다. 또한, 라자루스(Lazarus)그룹에서는 '미국 라스베가스 CES2020 참관단 참가신청서'를 사칭한 APT 공격을 시도한 정황이 포착되기도 하였습니다. 각 APT 공격에 대한 내용은 이스트시큐리티 알약 블로그에 공개되어 있고, 조금 더 상세한 분석자료와 IoC 정보들은 ThreatInside.com 을 통해 확인하실 수 있습니다.

랜섬웨어쪽에서는 10 월에도 역시나 Sodinokibi 랜섬웨어가 가장 많은 유포와 감염이 이뤄졌으며, 8 월말경부터 국내에 급속도로 전파되기 시작한 Nemty 랜섬웨어가 10 월에도 여전히 일정수준의 유포가 이뤄졌습니다. 다행히도, 10 월 11 일에 Tesorion 이란 보안업체가 이 Nemty 랜섬웨어에 대한 무료 복호화툴을 개발해 공개해서 실제로 Nemty 랜섬웨어로 인해 암호화되었던 파일들이 복호화되기도 하였습니다. 그러나 곧 Nemty 랜섬웨어 제작자들은 이러한 복호화툴 제작에 대해 발빠르게 대응하여 10 월 말경 Nemty Revenge 2.0 을 업데이트하는 기민한 모습을 보여주고 있는 상황입니다.

Sodinokibi 랜섬웨어와 Nemty 랜섬웨어 외에도 국내에서 발생했던 랜섬웨어 이슈 중 가장 큰 이슈는 10 월 30 일에 있었던 국내 모 웹호스팅 업체가 랜섬웨어 공격을 받아 전체 서버 데이터가 암호화된 사건이 아닐까 합니다. 해당 건은 운영중인 서버뿐만 아니라 백업 데이터가 저장된 백업 서버까지 모두 랜섬웨어에 의해 감염된 것으로 보이며, 업체가 공격자와 협상 중이라고 공지를 띄웠지만 아직까지 해결의 기미가 보이지 않는 건이기도 합니다. 2 년전 '나야나' 이슈와 1 년전 '아이웹' 이슈와 마찬가지로 웹호스팅 전문기업을 노린 랜섬웨어 공격이 지속적으로 발생하고 있고, 공격자는 일단 내부로 침투해 백업서버로의 침투에 성공할 때까지 아무런 행위를 하지 않고 대기를 하고 있다가 백업서버로의 연결고리를 인지하고 접근에 성공할 때 전체 서버에 대한 공격을 수행하여, 암호화된 서버 데이터를 볼모로 커다란 금액을 요구했습니다.

APT 공격과 랜섬웨어 공격의 시발점은 특정 타깃을 노리는 스피어피싱 공격, 그리고 그를 통한 타깃에 대한 지속적인 내부정보 수집으로부터 시작됩니다. 항상 출처를 알 수 없는 이메일에 대한 열람을 주의하는 동시에 보안패치 최신 업데이트, 계정 권한 설정 및 접근 로그에 대한 주기적 점검을 권장드립니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계다.

2019 년 10 월의 감염 악성코드 Top 15 리스트에서는 지난 2019 년 9 월에 각각 2,1 위를 차지했었던 Misc.HackTool.AutoKMS 과 Trojan.Agent.gen 이 10 월에 자리를 바꿨으며, 3 위, 4 위 역시 자리를 바꾼 순위를 차지했다. 전반적으로 감염통계 10 위권내의 악성코드들은 대동소이했다.

10 위권 밖에서는 기존에 자주 Top15 리스트에 오르던 BitCoinMiner 와 Neshta 등이 순위에 재진입하였다.

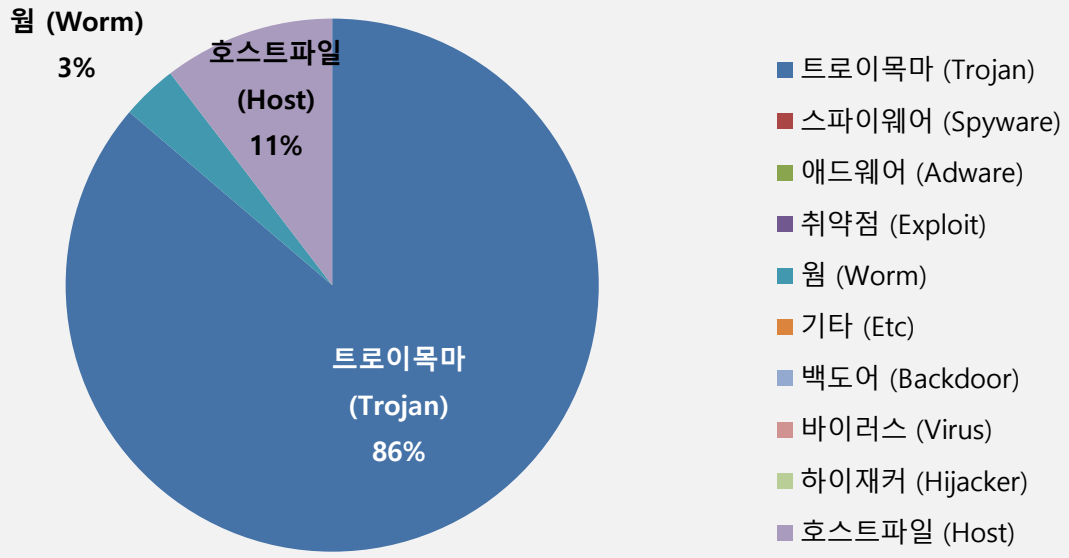
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 1	Misc.HackTool.AutoKMS	Trojan	726,986
2	↓ 1	Trojan.Agent.gen	Trojan	639,236
3	↑ 1	Hosts.media.opencandy.com	Host	565,486
4	↓ 1	Trojan.HTML.Ramnit.A	Trojan	521,478
5	-	Trojan.ShadowBrokers.A	Trojan	401,194
6	-	Misc.HackTool.KMSActivator	Trojan	373,887
7	New	Gen:Variant.Razy.553929	Trojan	364,573
8	↑ 2	Trojan.LNK.Gen	Trojan	324,797
9	↑ 4	Misc.Riskware.TunMirror	Trojan	322,668
10	↓ 2	Misc.Keygen	Trojan	234,371
11	New	Heur.BZC.YAX.Linx.15.029FD0F2	Trojan	216,925
12	↓ 1	Misc.Riskware.BitCoinMiner	Trojan	209,753
13	↓ 4	Misc.Riskware.TunMirror	Trojan	194,015
14	↓ 2	Worm.ACAD.Bursted	Worm	183,757
15	New	Gen:Variant.Kazy.794257	Trojan	166,674

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2019 년 10 월 01 일 ~ 2019 년 10 월 31 일

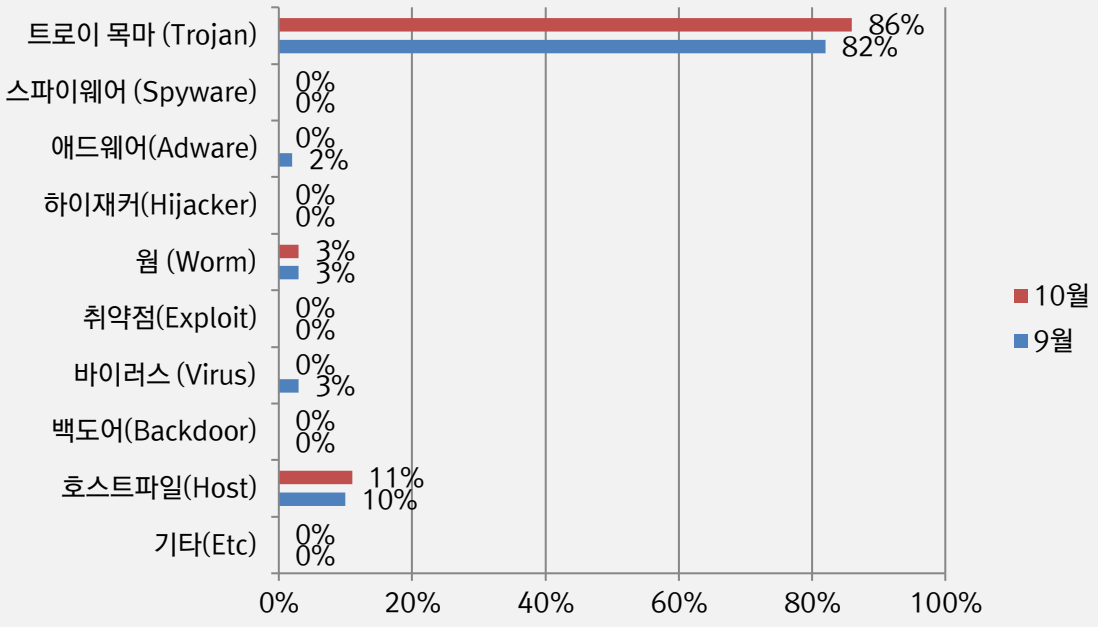
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 86%를 차지했으며 호스트파일(Host) 유형이 11%로 그 뒤를 이었다. 전반적으로 9 월에 비해 전체 감염건수는 9% 증가했다.



카테고리별 악성코드 비율 전월 비교

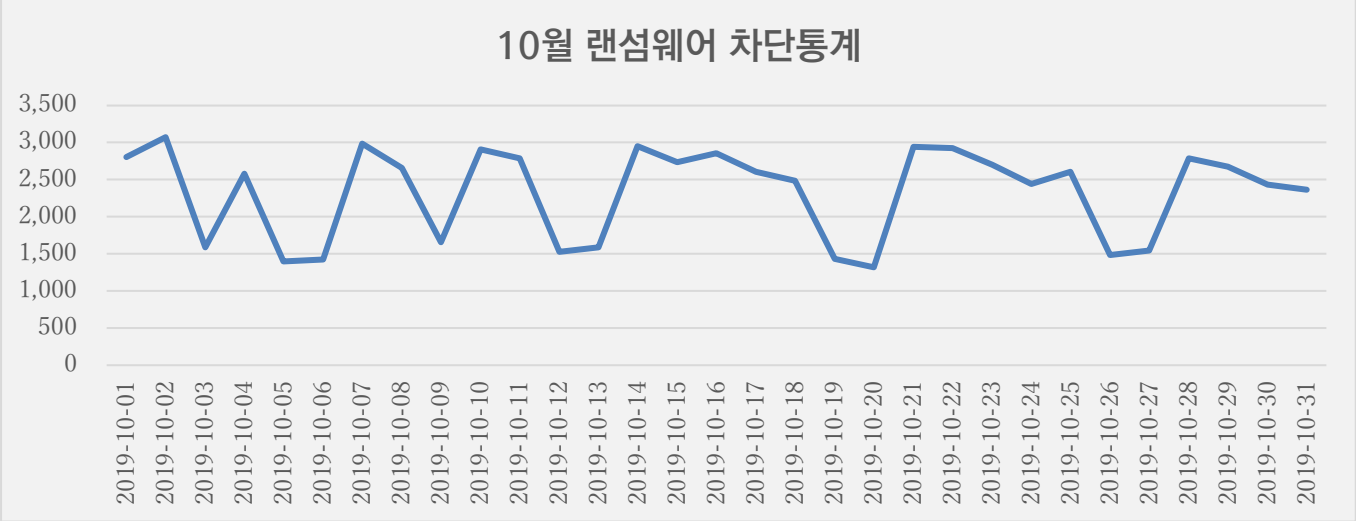
10 월에는 9 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 소폭 증가했으며, 호스트파일(Host) 유형 악성코드 비율은 거의 유사했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

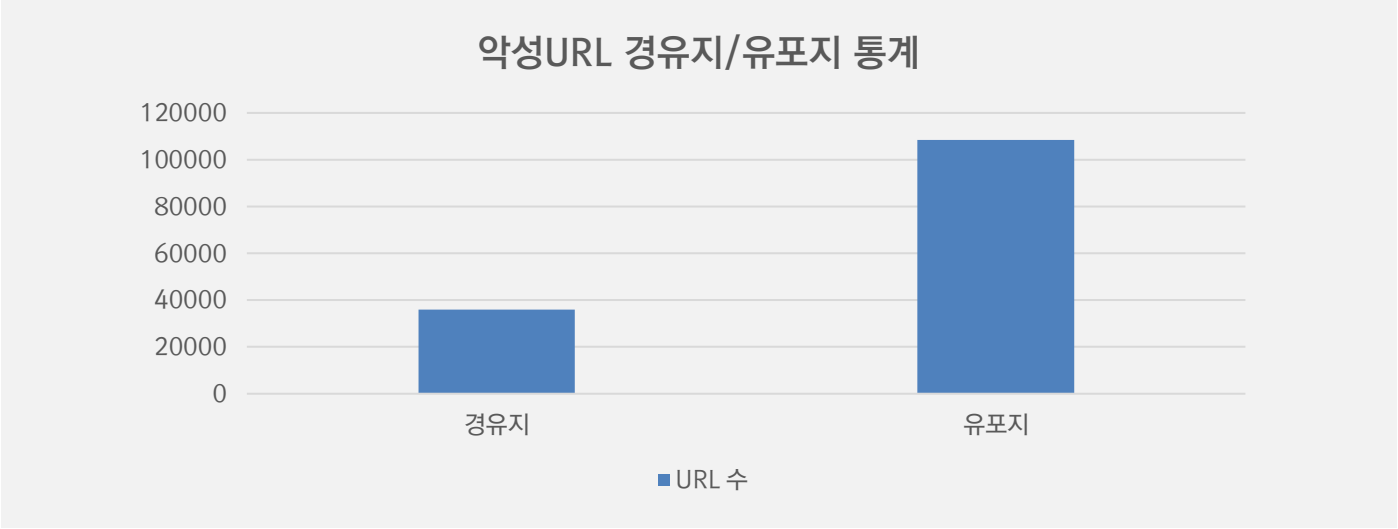
10 월 랜섬웨어 차단 통계

해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 10 월 1 일부터 10 월 31 일까지 총 72,321 건의 랜섬웨어 공격시도가 차단되었다. 9 월에 비해 랜섬웨어 공격건수는 2.2% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 10 월 한달간 총 144,420 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 9 월 한달간 확인되었던 1,117,976 건의 악성코드 유포지/경유지 건수에 비해 약 87% 가량 크게 감소한 수치다. 다만 9 월달 수치가 이전달에 비해 5 배 이상 크게 높았던 점을 감안하면 예전 수준의 수치로 돌아온 것으로 보인다. 악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 봐주시기 바란다.



02

전문가 보안 기고

1. 위협 인텔리전스 결합한 EDR 로 승부 – 김준섭 부사장 인터뷰

2. 금성 121, 북한 이탈주민 후원 사칭 '드래곤 메신저' 모바일 APT 공격 수행

1. 위협 인텔리전스 결합한 EDR로 승부 – 김준섭 부사장 인터뷰

국내 여러 기관에서 EDR 검토, 도입에 적극적으로 나서며 엔드포인트 위협 탐지 및 대응(EDR) 시장의 윤곽이 점차 드러나기 시작했습니다. 장애와 충돌이 잦은 문제, 악성코드 및 포렌식 전문인력이 있어야 운영할 수 있었던 한계점 등 그동안 EDR 솔루션 도입에 장벽으로 작용했던 부분들이 해결되고 있기 때문인데요.

김준섭 이스트시큐리티 부사장과 IT 전문 인터넷신문 데이터넷이 국내 EDR 시장의 현주소와 이상적인 통합 엔드포인트 보안 모델에 관해 나눴던 심도깊은 대화를 전달드리려고 합니다.

[사진] 김준섭 이스트시큐리티 부사장

Q. 이스트시큐리티의 EDR 무엇이 다른가?

A. 이스트시큐리티는 '알약'과 '알약 EDR', 위협 인텔리전스 서비스인 '쓰렛인사이드(TI)'를 결합해 차세대 엔드포인트 보안의 이상을 완성한다.

02 전문가 기고

기존 시그니처 기반 엔드포인트 보안 솔루션을 보완하기 위해 EDR 솔루션이 해결책으로 부상했지만, EDR 은 수많은 노이즈로 인해 관리 업무가 증가한다는 결정적인 문제가 있었다. 이 같은 EDR 의 한계는 위협 인텔리전스를 통해 탐지된 위협을 제거하고 새롭게 발견된 위협을 파악, 자동화된 대응을 통해 해결할 수 있다.

이스트시큐리티는 악성코드 분석에 있어 국내 최고 수준의 전문성을 보유하고 있으며, 국내 최대 사용자로부터 수집한 위협을 분석한 TI 를 통해 발견된 위협의 성격과 패턴, 공격 조직의 특징 등을 파악할 수 있어 발견된 공격에 대한 최적의 대응 방안을 제공할 수 있다.

이스트시큐리티 차세대 엔드포인트 보안 솔루션의 경쟁력은 신세계조선호텔 전 사업장에 공급되면서 입증된 바 있다. 특히 외산 솔루션이 국산 솔루션에 비해 탐지기술이 뛰어나다고 생각했던 고정관념을 깬 사례로, 국산 솔루션이라도 높은 정확도와 고도의 전문성을 기반으로 제공되는 보안 솔루션이 있다는 사실을 고객이 알아주기를 바란다.

Q. 백신과 비교했을 때 EDR 은 어떻게 접근해야 하는가?

A. EDR 은 백신처럼 운영해선 안된다.

EDR 은 기존 보안 솔루션이 탐지하지 못한 지능형 공격을 방어하기 위한 것으로, 보안조직의 리소스가 추가로 투입되어야 하는 솔루션이다. 자동 탐지·차단이 가능한 백신처럼 운영해서는 EDR 도입에 성공할 수 없다.

백신이나 EDR, 어느 하나의 솔루션만으로 진화하는 위협에 대응할 수 없다. 알려진 공격은 백신으로 차단하고, 알려지지 않은 공격은 행위기반 분석 기술을 탑재한 EDR 을 통해 탐지하며, 위협 인텔리전스와 비교해 빠르게 대응한 후, 솔루션이 판단하지 못한 고도화된 위협은 전문 조직이 직접 대응하면서 엔드포인트 보안 위협을 낮춰야 한다.

무엇보다 EDR 은 악성코드 분석 전문성이 반드시 필요하다. EDR 은 엔드포인트에서 발생하는 행위를 모니터링해 공격 정황이 발견되거나 평소와 다른 이상행위가 발생했을 때 이벤트를 발생시킨다. 이 점을 강조하며 지능적인 행위분석 기술로써 EDR 을 완성할 수 있다는 주장이 있지만, 악성코드 분석 전문성이 없으면 엔드포인트에서 발생하는 위협 행위를 판단하기 어렵다. 예를 들어 프로세스를 후킹하는 행위는 악성코드 뿐 아니라 보안 솔루션도 발생시키는데, 이를 모두 비정상 행위라고 이벤트를 발생시키면 오탐이 많아 결국 관리가 어려워지게 된다.

또한 공격은 지속적으로 변하고 있어 행위분석 기술을 우회하는 공격도 쉽게 개발할 수 있다. 공격자의 특성, 공격 도구에 대한 전문적인 기술이 없으면 엔드포인트에서 발생하는 수 많은 위협 행위를 제대로 파악하지 못한다. 악성코드 분석 기술을 이용해 이상정황을 분류하고 전문가 분석을 통해 대응하지 못하면 피해가 확산되는 것을 막을 수 없다.

Q. 국내 EDR 시장 전망은 어떻게 보는가?

A. 대규모 성공사례가 완성되면 EDR 시장이 급성장 할 것이다.

우리나라에 EDR 이 소개된 것은 꽤 오래 됐지만 국내 환경에 맞지 않는 솔루션 운영 방식으로 인해 확장 속도는 매우 더뎠다. 설치하면 자동으로 위협을 탐지·차단하는 기존 엔드포인트 보안 솔루션처럼 운영하려다보니 탐지된 위협에 대한 추가 분석과 대응이 필요한 EDR 은 운영이 어려운 솔루션으로 인식됐다.
EDR 시장은 아직 시작 단계에 있으며, 대규모 성공사례가 완성되기까지 많은 시행착오를 겪게 될 것이다. 그러나 누구나 인정하는 성공사례가 만들어지면 엔드포인트 보안 시장의 질서를 재편하게 될 것이다. EDR 솔루션만으로는 시장의 발전을 이루지 못하며 백신과 위협 인텔리전스, 전문 대응조직의 결합을 통해 성공적인 차세대 엔드포인트 보안을 완성할 수 있다.

EDR 시장 초기임에도 불구하고 시장 선점 경쟁이 치열해져, 일부 대형 프로젝트에는 출혈경쟁이 나타나고 있다. 가격이 무너지면 시장 규모를 키울 수 없으며, 가격이 아닌 기술로 승부하는 시장 질서를 만들어가야 엔드포인트 보안 시장을 성장시킬 수 있을 것이다.

2. 금성 121, 북한 이탈주민 후원 사칭 '드래곤 메신저' 모바일 APT 공격 수행

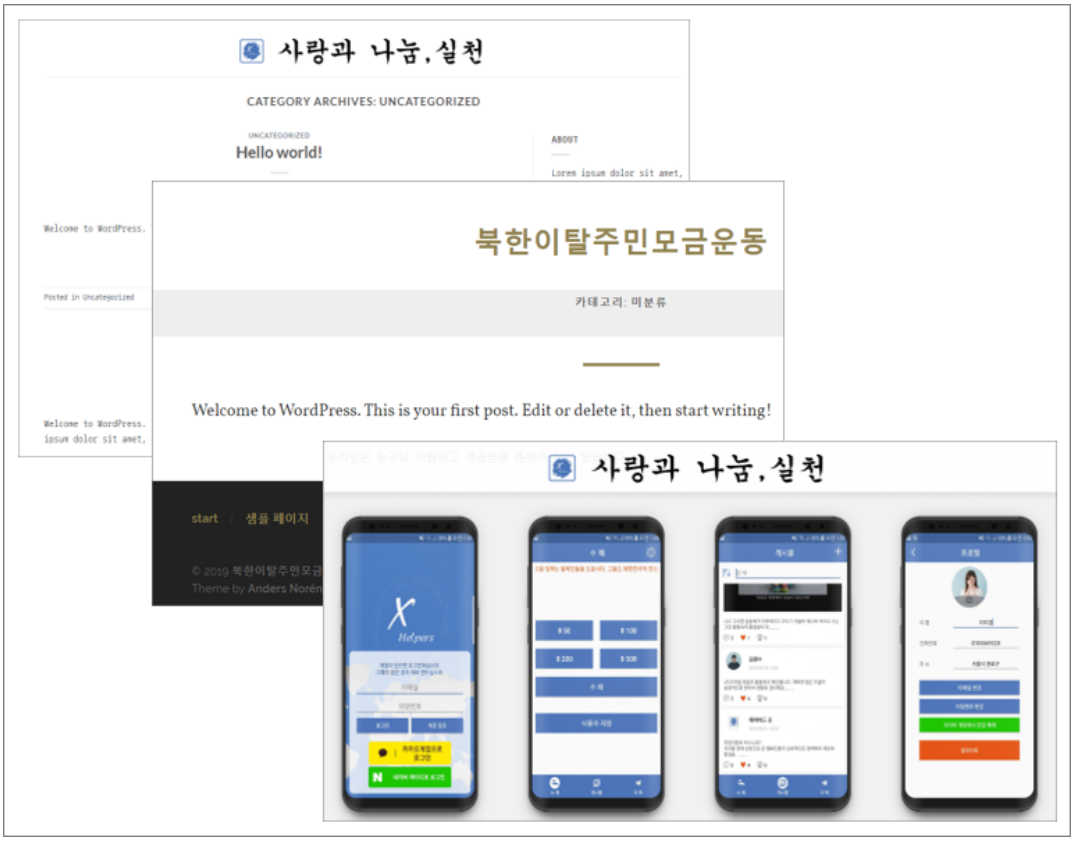
'드래곤 메신저(Dragon Messenger)' APT 작전 배경

시큐리티대응센터(이하 ESRC)에서는 '금성 121(Geumseong121)' APT 공격조직이 진행한 은밀한 모바일 APT 공격정황을 포착했습니다.

또한, 북한 이탈주민 후원 모금 서비스로 위장한 사이트를 개설해 악성앱(APK)을 유포한 사실도 드러났습니다. 해당 웹사이트는 워드프레스 기반으로 제작되었고, 도메인은 2019 년 08 월 23 일 생성되어 10 월 22 일 업데이트된 것으로 조회됩니다.

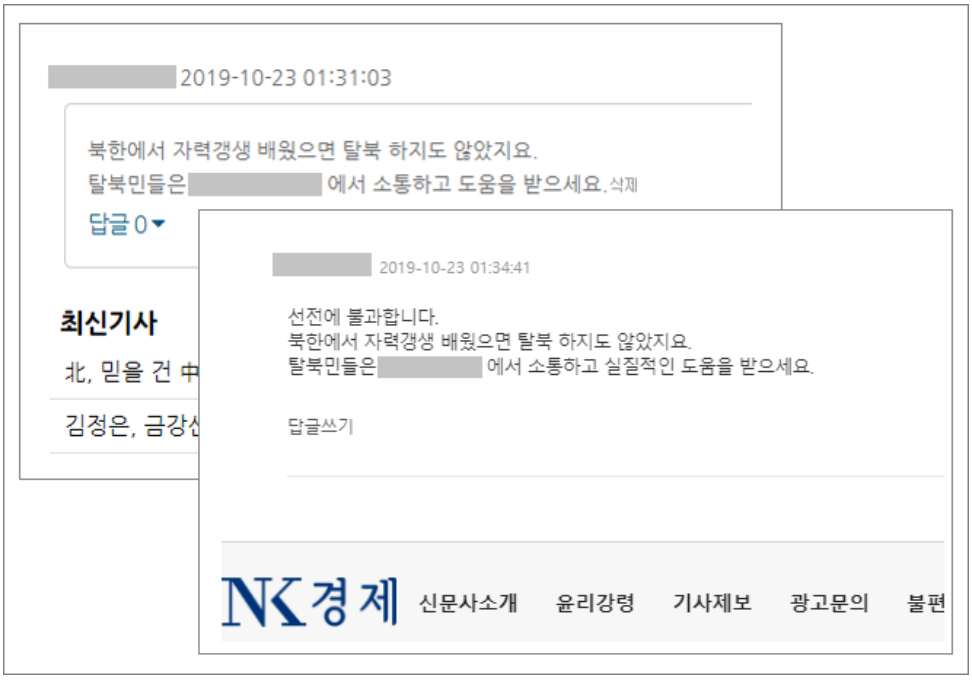
지난 09 월 11 일부터 표시된 스냅샷을 타임라인으로 확인해 보면 타이틀에 북한 이탈주민 모금운동 사이트로 소개한 것을 알 수 있고, 10 월에는 안드로이드 앱 설치 링크(구글 플레이)가 추가됩니다. 마치 북한 이탈주민 기부관련 웹사이트로 위장해, 주로 탈북민과 대북단체에 다양한 홍보로 앱 설치를 유도하고 있었습니다.

ESRC 에는 이들이 배포한 앱에서 흥미로운 위협 단서를 다수 포착하였고, 동일한 공격자가 사용한 악성앱이 'DragonTask' 경로로 정보를 수집했던 점과 보안 메신저로 위장해 공격한 점을 결합해, 이번 오퍼레이션 이름을 '드래곤 메신저(Dragon Messenger)'로 명명했습니다.



[그림 1] 북한 이탈주민 모금운동 사이트로 위장한 화면 이력

상기 북한 이탈주민 모금운동 사이트가 개설된 이후 여러 채널(이메일, SNS)로 관련 앱 안내와 전파가 이뤄지는데, 주로 대북분야에 종사하는 사람들이 주요 타깃이 됩니다. 그리고 북한(North Korea)분야를 다루는 언론사 웹 사이트에 댓글 등으로 홍보가 이뤄지는데 이때 사용되는 아이디는 '데이비드 김'이고, 해당 사이트의 관리자로 소개하고 있습니다.



[그림 2] 북한 언론 관련 사이트에 올려진 댓글 화면

02 전문가 기고

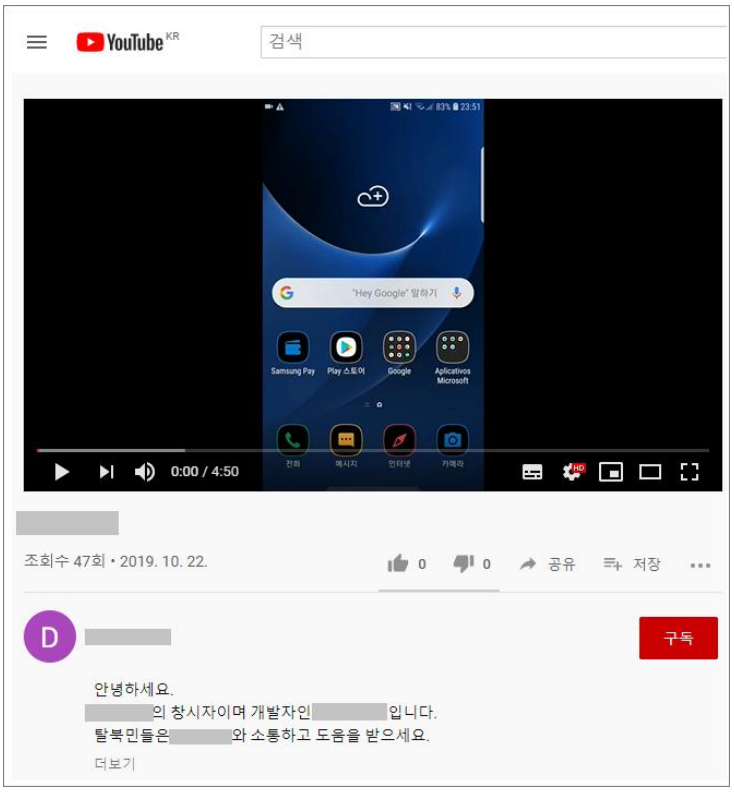
ESRC 에서는 이 사이트를 조사하는 과정에서 북한식 표현이 다수 사용된 점에 주목했습니다. 물론, 탈북민 관련 사이트라 실제 그런 표현이 존재할 가능성도 충분합니다.
이에 해당 사이트에서 배포하는 안드로이드 앱과 동일한 관리자가 운영하는 유튜브(YouTube) 사이트에 대한 정밀 조사를 진행했습니다. 당시 구글 플레이 공식 마켓에는 2 개의 앱이 등록되어 있었으며, 현재는 구글에서 삭제조치한 상태입니다. 해당 앱은 탈북민들이 생활상 문제를 공유하고 지원을 받을 수 있으며, 기부 서비스를 지정할 수 있다고 안내합니다.

[그림 3] 구글 플레이에 등록된 앱 화면

구글 플레이 공식마켓에 설명된 이미지에는 북한식 표현인 '계정 창조' 버튼이 존재합니다. 참고로 한국에서는 보통 '계정 생성'이라고 표현합니다. 그리고 화면 캡처할 때 쓴 스마트폰 단말기에는 유심칩이 없이 와이파이(Wifi)로만 접속한 것을 알 수 있습니다.

[그림 4] 구글 플레이에 등록된 이미지 중 일부

지난 10 월 23 일 해당 사이트에는 코스모스팜 소셜댓글 게시판 서비스가 존재했는데, 10 월 28 일 전후로 게시판이 사라진 상태입니다. 당시 사용되었던 게시판을 확인해 보면, 여러 사람들이 해당 서비스를 호응하는 식의 댓글과 유튜브 링크가 포함되어 있습니다.



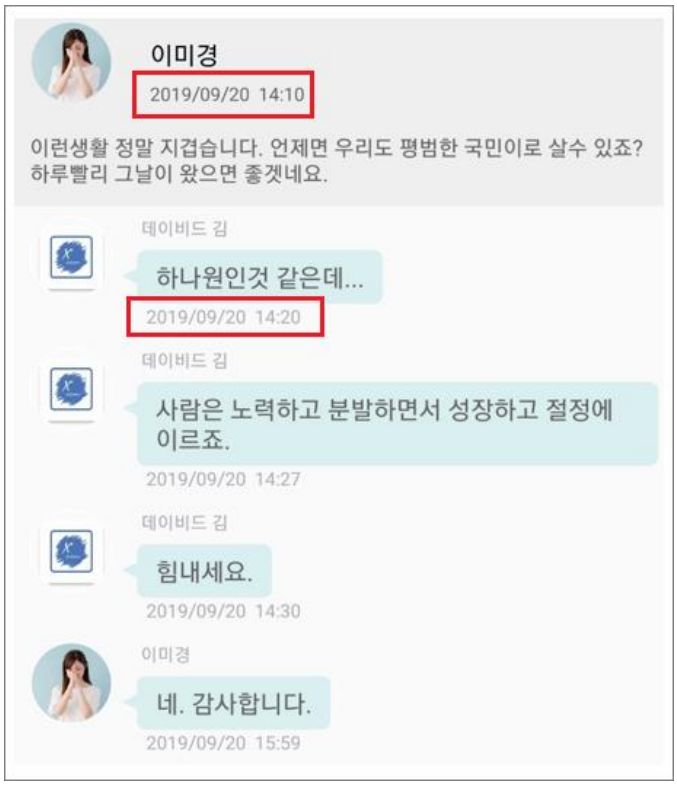
[그림 5] 유튜브 사이트에 등록된 앱 사용 화면

유튜브에는 한국 스마트폰 화면의 동영상이 올려져 있으며, 해당 앱의 설치부터 사용방법을 안내해 주고 있습니다. 페이스북은 유튜브랑 동일한 계정으로 활동하고 있으며, 약 330 여명 정도의 친구가 등록되어 있습니다. 페이스북을 통해 다양한 사전준비가 진행된 점을 충분히 짐작해 볼 수 있고, 친구관계인 이들은 잠재적인 위협대상이 될 수 있습니다.

[그림 6] 페이스북에 등록된 화면

유튜브에는 실제 앱 설치부터 사용법을 데모형태의 동영상으로 보여주고 있는데, 이 동영상을 상세히 살펴보면 동영상 제작시 '이미경' 이름과 'borisanatoly' 계정으로 로그인하는 것을 볼 수 있습니다. 그리고 '이미경'이라는 이름은 2019 년 09 월 20 일 14 시 10 분에 앱 서비스 내부 게시물에 처음으로 글을 올린 인물입니다.

웹 사이트의 관리자로 보이는 '데이비드 김' 계정은 해당 게시글에 09 월 20 일 14 시 20 분 바로 댓글을 다수 등록하며, 거의 10 분 간격으로 글을 주고 받습니다. 이외에도 구글 플레이 공식마켓 앱 정보에 '이미경' 내용이 담긴 화면도 그대로 사용되었다는 점을 보아 두개의 계정은 초기부터 밀접하게 연관되어 있는 것으로 볼 수 있고, 각각의 계정을 하나의 인물이 관리하고 있을 것으로 추정됩니다.



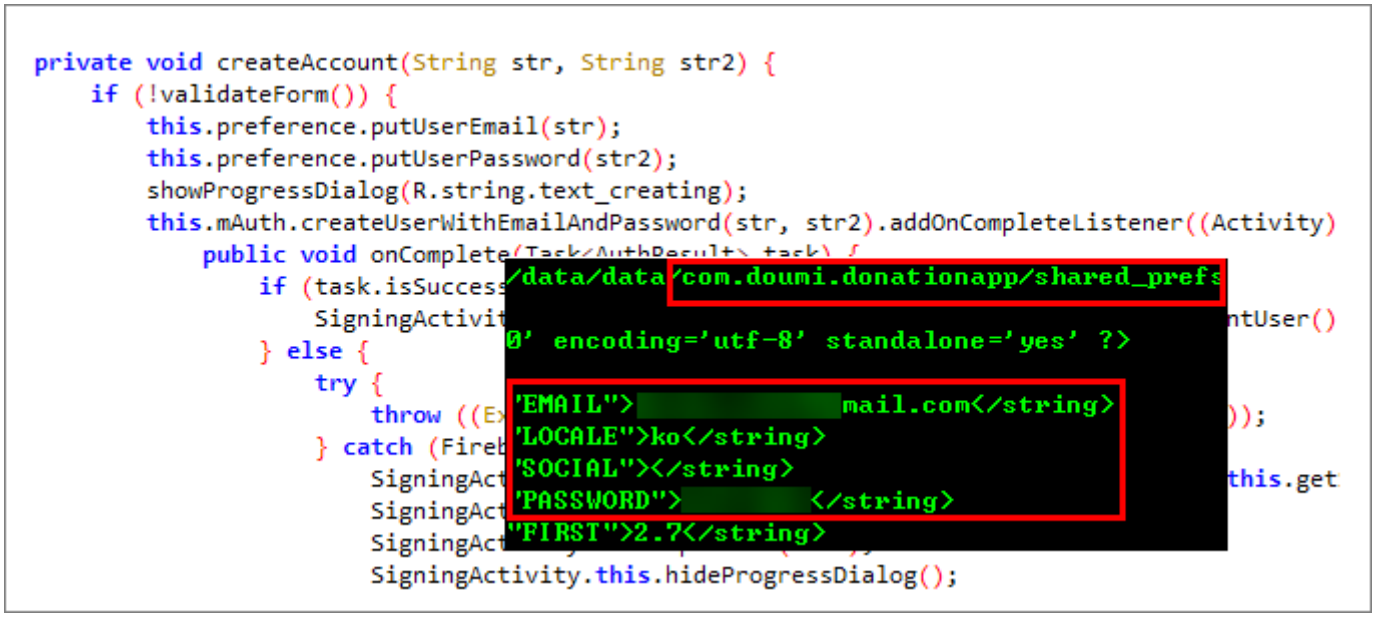
[그림 7] 앱 서비스 내부 대화 장면

APT 공격자는 커뮤니티 기반 탈북민 후원 앱을 제작해, 표적 대상자들이 한 곳에 모이게 만드는 고도의 전략전술 시나리오를 계획했습니다. 이를 통해 자신들이 구축한 특수 공간에 많은 탈북민들이 모이도록 만들고 대화정보를 은밀히 염탐하고, 실제 기부 및 광고를 통한 금전적 수익까지 노린 치밀함을 보였습니다.

ESRC 에서는 '금성 121(Geumseong121)' 조직의 이러한 활동이 앞으로 새로운 모바일 위협의 신호탄이 될 것으로 보고 있습니다.

탈북민 후원 단체로 위장한 스마트 위협

공격배후는 다양한 형태의 악성앱을 제작 유포하였고, 주로 은밀한 비밀 대화 목적의 전용 메신저로 위장하였습니다. 그 중에 탈북민 후원용으로 위장한 이 앱은 구글 플레이 공식 마켓에 정식으로 등록되어 있었습니다. 초기 회원 가입시 카카오나 네이버가 아닌 별도의 이메일로 등록할 경우 'createUserWithEmailAndPassword' 메소드를 통해 사용자가 입력한 아이디와 비밀번호가 'Firebase'의 계정 생성 및 로그인에 사용됩니다. 그리고 앱의 'shared_prefs' 경로의 'config.xml' 파일에 평문으로 계정 정보가 저장되어, 보안위협에 노출될 위험성이 존재합니다.

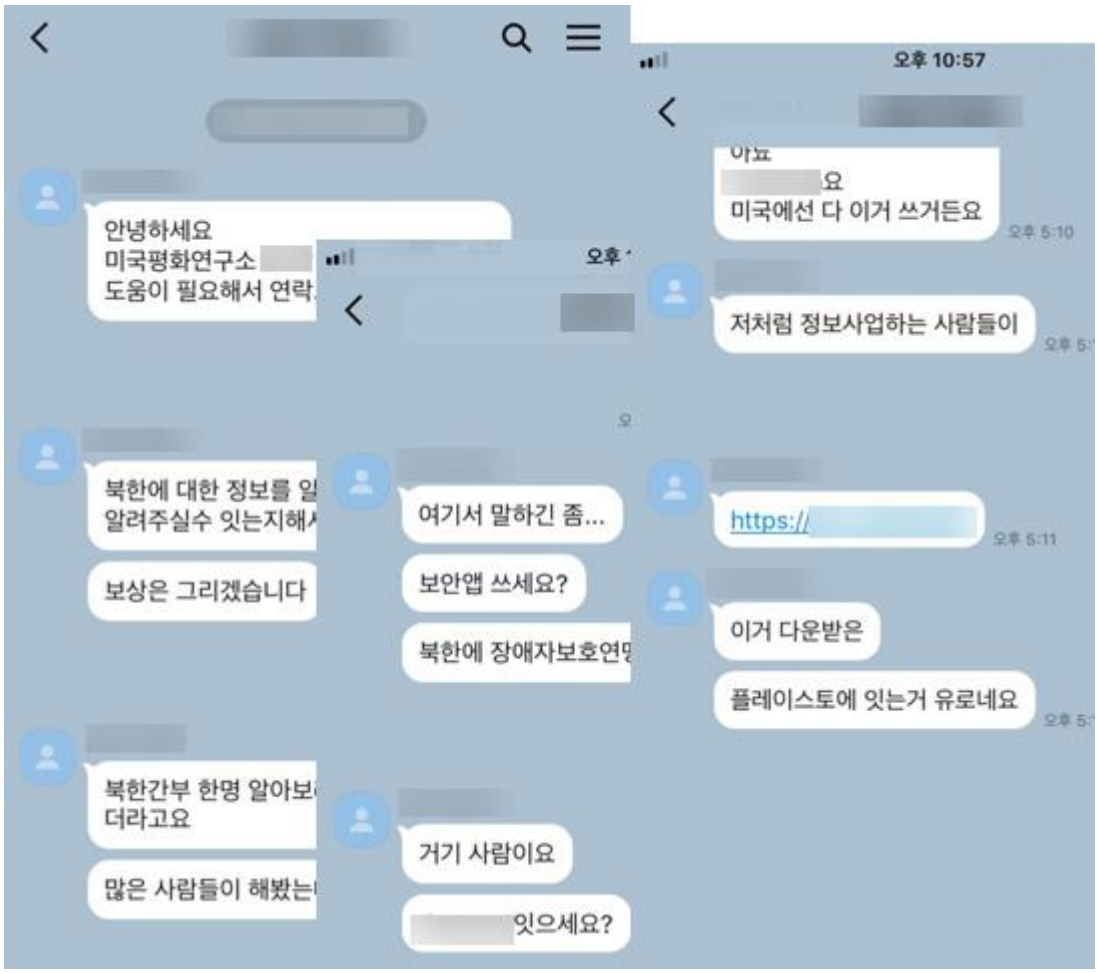


[그림 8] 평문으로 저장된 로그인 계정 정보

ESRC는 구글 플레이 공식마켓에 등록된 마지막 버전의 경우, 초기 가입시 계정 노출 위협가능성 외에 추가적인 위협 근거를 확보하는데 분석을 집중하였고, 이 과정에서 다른 유사 코드를 발견했습니다. 추가 확보된 코드를 분석하는 과정에서 기존 '금성 121' APT 조직의 모바일 침해사건과 연결되는 고리를 발견하였습니다.

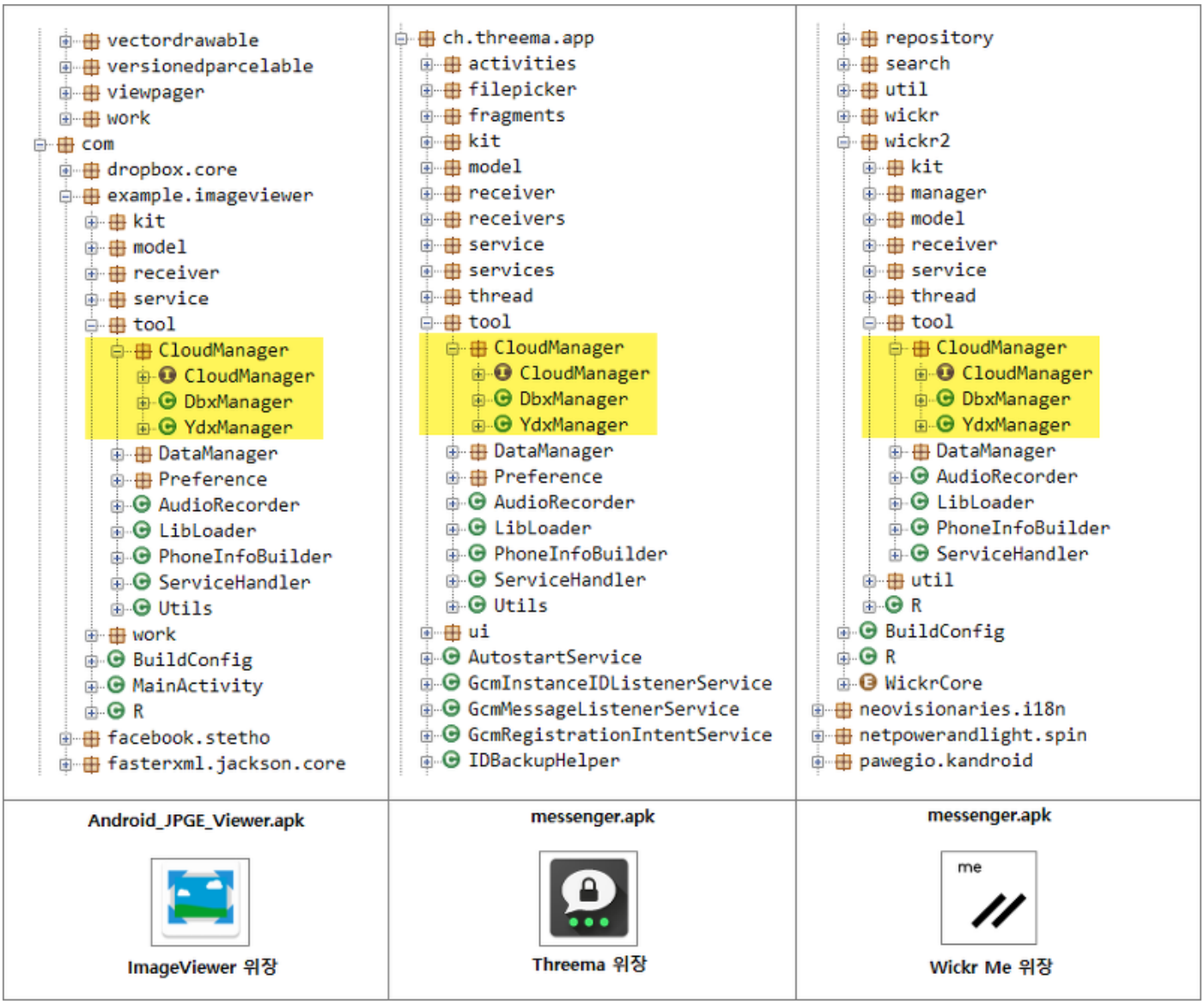
카카오톡 메시지를 통한 은밀한 표적공격

2019년 06월부터 최근까지 다양한 사람들에게 악성앱 유포 시도 정황이 포착되었습니다. 공격자는 미국에 실존하는 특정 인물의 이름과 프로필 사진을 무단 도용해 카카오톡 계정을 생성하고, 대북분야에 종사하는 한국 사람들에게 접근을 시도합니다. 휴대폰 전화번호만 알면 카카오톡 친구를 추가할 수 있기 때문에 공격 대상자를 선별하는데 전화번호가 활용됩니다. 공격자는 미국내 한인협회 부회장이나 자문위원, 또는 평화연구소 연구원 등을 사칭해 접근을 시도합니다.



[그림 9] 카카오톡 메신저로 악성앱을 전달하는 사례

카카오톡 대화를 통해 마치 미국내 평화연구원처럼 자신을 속이고, 북한관련 정보를 수집하고 있다면서 보안앱으로 대화를 하자고 제안합니다. 그러면서 특정 URL 링크를 클릭하도록 유도하고, 메신저 앱으로 위장한 악성앱을 설치 유도합니다. 공격자는 보안에 특화된 암호화 메신저로 위장한 특징을 가지고 있으며, 스위스에서 개발한 '쓰리마(Threema)'나 미국의 '위커(Wickr)' 등을 사칭하였습니다. 악성앱들은 실제 정상적인 암호화 메신저 기능을 그대로 제공해 최대한 의심을 받지 않도록 만들었습니다. 이 악성앱들은 모두 유사한 기능을 수행합니다.
그리고 지난 8 월 5 일 공개된 '금성 121 APT 조직, 스테가노그래피 기법과 스마트폰 노린 퓨전 공격 수행' 내용에서 발견된 안드로이드 악성앱과도 유사성이 높게 분석됩니다.



[그림 10] 악성앱 종류별 내부 코드 비교화면

ESRC 에서는 해외 보안메신저로 위장한 악성앱 공격 대상자가 북한이탈주민모금운동 사칭 공격에도 노출된 것을 확인했습니다. 구글 플레이 공식마켓에 있던 최종 버전에서는 확인하기 어려웠지만, 공격자가 만든 초기 버전을 확보하는데 성공했고 해당 앱에서 동일한 함수부분을 발견했습니다.

[그림 11] 메신저 위장 시리즈와 탈북민 기부 앱 위장 악성코드 비교

탈북민 모금운동 앱처럼 사칭한 악성앱은 최대한 기존 악성앱 조직처럼 보이지 않기 위해 나름대로 노력을 한 것으로 보입니다. 그러나 초기에 만들어졌던 변종에서 드롭박스(Dropbox)와 얀덱스(Yandex) 등으로 통신을 시도하는 기능이 동일하게 포함된 것을 확인했습니다. 또한, 악성앱들이 사용한 일부 변수 선언부분이 거의 동일함을 확인했습니다.

<table>
<tr>
<td>탈북민 기부 앱 위장</td>
<td>

```
Config.TAG = "NCSCLog";
Config.PERIODIC_WORKER_TAG = "LoadAppPeriodic";
Config.ONETIME_WORKER_TAG = "LoadAppOneTime";
Config.REQUEST_ALARM_CODE = 101;
Config.REQUEST_RESTART_CODE = 102;
Config.JOB_SERVICE_ID = 333;
Config.FOREGROUND_ID = 444;
Config.NOTIFICATION_ID = "NCSC_NotificationID";
Config.FOREGROUND_KEY = "LoadAppForeground";
Config.EXTRA_KEY = "CMD_KEY";
Config.P_NUMBER_KEY = "P_NUMBER";
Config.S_DATE_KEY = "S_DATE";
Config.E_DATE_KEY = "E_DATE";
Config.TYPE_KEY = "TYPE";
Config.R_STATE_KEY = "R_STATE";
Config.S_TIME_KEY = "S_TIME";
storeConfig();
```

</td>
</tr>
<tr>
<td>messenger.apk
Threema 위장</td>
<td>

```
Config.TAG = "NCSCLog";
Config.PERIODIC_WORKER_TAG = "LoadAppPeriodic";
Config.ONETIME_WORKER_TAG = "LoadAppOneTime";
Config.REQUEST_ALARM_CODE = 101;
Config.REQUEST_RESTART_CODE = 102;
Config.JOB_SERVICE_ID = 333;
Config.FOREGROUND_ID = 444;
Config.NOTIFICATION_ID = "NCSC_NotificationID";
Config.FOREGROUND_KEY = "LoadAppForeground";
Config.EXTRA_KEY = "CMD_KEY";
Config.P_NUMBER_KEY = "P_NUMBER";
Config.S_DATE_KEY = "S_DATE";
Config.E_DATE_KEY = "E_DATE";
Config.TYPE_KEY = "TYPE";
Config.R_STATE_KEY = "R_STATE";
Config.S_TIME_KEY = "S_TIME";
storeConfig();
```

</td>
</tr>
<tr>
<td>messenger.apk
Wickr Me 위장</td>
<td>

```
Config.TAG = "NCSCLog";
Config.PERIODIC_WORKER_TAG = "LoadAppPeriodic";
Config.ONETIME_WORKER_TAG = "LoadAppOneTime";
Config.REQUEST_ALARM_CODE = 101;
Config.REQUEST_RESTART_CODE = 102;
Config.JOB_SERVICE_ID = MjolnirRecyclerAdapter.TYPE_ITEM;
Config.FOREGROUND_ID = 444;
Config.NOTIFICATION_ID = "NCSC_NotificationID";
Config.FOREGROUND_KEY = "LoadAppForeground";
Config.EXTRA_KEY = "CMD_KEY";
Config.P_NUMBER_KEY = "P_NUMBER";
Config.S_DATE_KEY = "S_DATE";
Config.E_DATE_KEY = "E_DATE";
Config.TYPE_KEY = "TYPE";
Config.R_STATE_KEY = "R_STATE";
Config.S_TIME_KEY = "S_TIME";
storeConfig();
```

</td>
</tr>
</table>

[그림 12] 메신저 위장 시리즈와 탈북민 기부 앱 위장의 설정변수 비교

이외에도 공격자가 명령을 수행하는 경로나 수집정보, 추가 다운로드 데이터에서 유사성이 높은 근거가 다수 확보되었습니다.

안드로이드 스마트폰을 통한 도청 공격

ESRC 에서는 특정 정부의 지원을 받아 활동하는 '금성 121(Geumseong121)' APT 조직이 안드로이드 스마트폰 이용자를 겨냥한 위협활동에 주목하고 있습니다. 개인들이 소지한 스마트 폰이 좀비화되어 사이버 작전에 악용된다는 점은 절대 간과해선 안될 중요한 위협으로 부상하고 있습니다. 실시간 문자 메시지(SMS) 탈취부터 전화 주소록, 통화 녹음(도청), 알림창에 나오는 카카오톡 메시지 유출 시도 까지 일부 확인되었습니다. 또한, 이름만 들어도 누군지 알 수 있는 유명 인사들이 이번 '드래곤 메신저' APT 공격에 노출되었다는 점입니다.
안드로이드 스마트폰이 악성앱에 노출될 경우 개인 사생활뿐만 아니라, 기관 및 기업 내부에서 진행되는 회의내용, 갤러리에 포함된 사진 등이 실시간으로 유출됩니다. 저희는 이번 모바일 APT 공격을 추적 분석하는 과정에서 다양한 사람들이 공격을 받아 좀비화된 것을 확인했습니다. 그러나 대체로 감염여부 자체를 인지하지 못하거나 스마트폰이 오랜 기간 공격자에게 감시당하고 있다는 점에 충격을 받았습니다.

주요 침해지표(Indicator of Compromise)

1594679f51bdebe4701d062f3c8f0dc3
dfb8e001b3ecfc63200dd4c5c21f53d5
02d5e68bef32871765b7e6e71f50499d
c36de50fe488e5015a58a241eb9b2411
1e32cd693a0dd137959b87ca359b2831

ESRC 에서는 해당 위협에 사용된 추가 침해지표(IoC) 등을 '쓰렛 인사이드(Threat Inside)' 위협 인텔리전스 리포트를 통해 별도로 제공할 예정입니다

03
악성코드 분석 보고

[Backdoor.RAT.Netwire] 악성코드 분석 보고서

최근 사용자 PC를 감염시키고 원격제어를 수행하는 악성코드가 발견되었다. 이 악성코드는 PDF 문서파일 아이콘과 '.SCR'확장자를 사용하여 화면 보호기 파일로 위장했다. 이는 사용자로 하여금 악성 파일을 정상 파일로 착각해 실행을 유도하기 위함이다.

```
v6 = MapVirtualKeyA(uCode, 0);
if ( ToAscii(uCode, v6, &KeyState, &Char, 0) == 1 )
{
  v9 = GetKeyState(17);
  if ( v5 || v9 <= 1u )
  {
    result = sprintf_0(&v16, 0x20u, "%c", Char);
  }
  else
  {
    v10 = Char;
    lpKeyState = DecodeString("[P50i+%Y]");
    result = sprintf_0(&v16, 0x20u, lpKeyState, v10 + 64);
  }
}
else
{
  v7 = MapVirtualKeyA(uCode, 0);
  result = GetKeyNameTextA(v7 << 16, &String, 32);
  if ( result <= 0 )
    return result;
  v8 = GetKeyState(17);
  if ( v5 || v8 <= 1u || uCode - 48 > 9 )
  {
    result = sprintf_0(&v16, 0x20u, "[%s]", &String);
  }
```

[그림] 키로깅 코드 일부

감염된 PC는 공격자의 명령에 따라 제어되므로 원치 않는 악성 행위를 시도한다. 명령의 일부로 감염 PC의 폴더 및 프로세스, 브라우저 정보 등을 탈취하고 키로깅을 수행한다.
이는 특히 사용자의 민감한 정보가 유출될 우려가 있고, 2차 피해로 이어질 수 있기 때문에 각별한 주의가 필요하다.

현재 알약에서는 해당 악성 코드를 'Backdoor.RAT.Netwire' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android. Banker] 악성코드 분석 보고서

스미싱을 통한 악성 앱의 종류가 점점 더 다양해지고 있다. 해당 악성 앱은 택배 앱으로 속이고 있으며 기기 정보와 문자 정보를 탈취한 후 아이콘을 숨겨 사용자가 알아차리기 어렵게 하고 원격 명령을 통해서 감염 기기로 문자 전송도 가능하다.

또한, 몇몇 앱들을 감시하는데 그 중 국내 은행 앱이 있으면 추가 다운로드한 악성 앱으로 바꿔치기하고 모바일 백신이 존재하면 해당 앱의 삭제를 유도한다.

```
lic class v3 extends Activity {
public v3() {
    super();
}

public void onCreate(Bundle arg3) {
    super.onCreate(arg3);
    this.setContentView(2130903048);
    if(MainActivity.a != null) {
        MainActivity.a.add(this);
    }

    AlertDialog$Builder v3 = new AlertDialog$Builder(this.getApplicationContext());
    v3.setMessage("악성코드를 발견했습니다");
    v3.setTitle("V3 Mobile Plus 2.0");
    v3.setPositiveButton("확인", new v(this));
    AlertDialog v3_1 = v3.create();
    v3_1.getWindow().setType(2003);
    v3_1.show();
```

[그림] 백신 삭제 유도 코드 중 일부

해당 악성 앱은 택배 앱으로 속인다. 기기와 관련된 다양한 정보를 탈취하고 특정 앱을 바꿔치기하고 삭제를 유도한다. 또한, 원격 명령을 통해서 문자 메시지 전송이 가능하며 앱의 분석을 어렵게 하도록 jiami 패킹을 적용했다.
따라서 악성 앱으로부터 피해를 최소화하기 위해서는 백신 앱을 통한 주기적인 검사가 중요하다. 출처가 불명확한 URL 과 파일은 실행하지 않는 것이 기본이고 공식 마켓인 구글 플레이스토어를 통해서 확보한 앱이라도 백신 앱을 추가 설치하여 주기적으로 업데이트하고 검사해야 한다.

현재 알약 M 에서는 해당 악성 앱을 'Trojan.Android.Banker' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

자기 자신을 재설치하는 악성 코드, 안드로이드 기기 45,000 대 이상 감염시켜

Mysterious malware that re-installs itself infected over 45,000 Android Phones

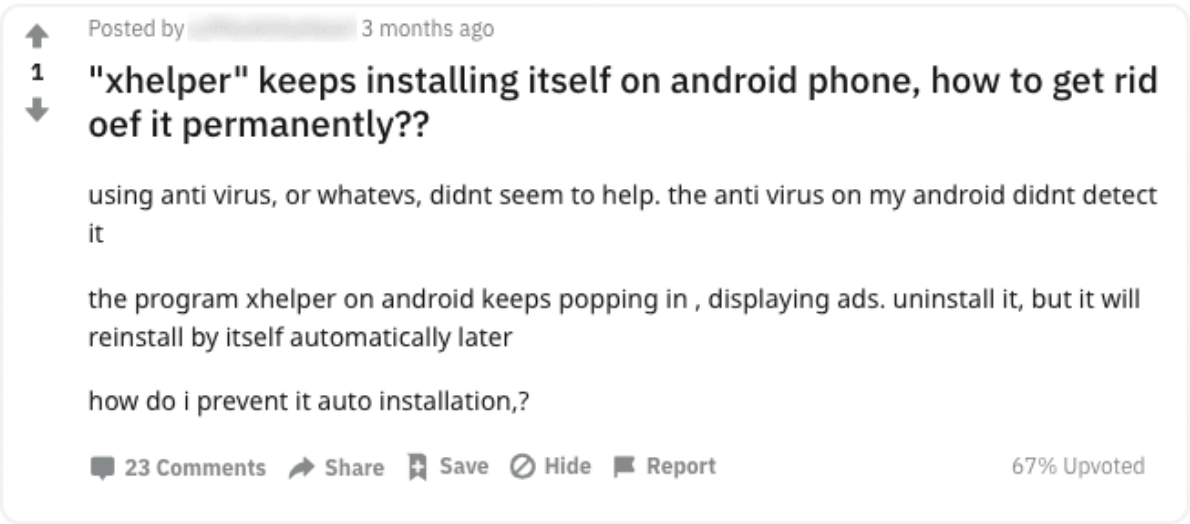
지난 몇 달 동안, 안드로이드 사용자 수백 명이 감염된 기기에 숨어 사용자가 삭제한 후에도 자기 자신을 재설치하거나 기기를 공장 초기화하는 새로운 악성코드에 대한 불만을 제기했다.
시만텍의 보고서에 따르면, Xhelper 라 명명된 이 악성코드는 이미 지난 6 개월간 안드로이드 기기 45,000 대 이상을 감염시켰으며 계속해서 매달 평균 최소 2,400 대 기기를 감염시키고 있다.

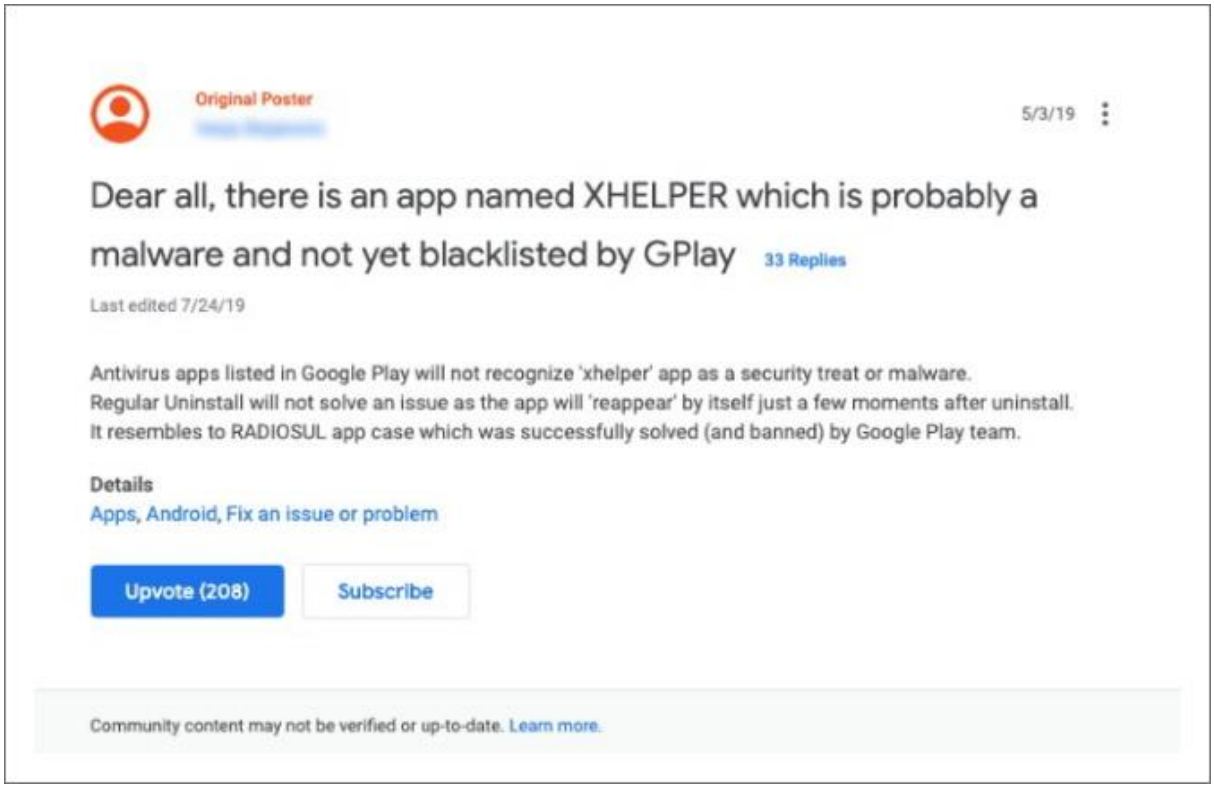
아래는 Xhelper 안드로이드 악성코드의 삭제 방법을 문의하는 온라인 포럼 글에 해당 악성코드에 감염된 안드로이드 사용자들이 작성한 댓글이다:

"Xhelper 는 정기적으로, 거의 매일 자신을 재설치합니다!"
"출처를 알 수 없는 앱 설치' 설정이 저절로 켜집니다."
"폰을 재부팅하고 초기화했지만, Xhelper 가 다시 설치되었습니다."
"Xhelper 는 중국에서 제조한 폰에 선 탑재되어 출시됩니다."
"저렴한 브랜드 기기를 사지 마세요."

Xhelper 안드로이드 악성코드, 어디에서 감염되었을까?

시만텍 연구원들은 Xhelper 악성코드가 포함된 악성 앱의 정확한 출처는 알아낼 수 없었지만, 특정 브랜드 안드로이드 기기에 선 탑재되어 출시되는 악성 시스템 앱이 악성 코드를 다운로드하는 것으로 의심했다.





"저희가 분석 한 샘플 중 어떤 것도 구글 플레이 스토어에서 찾을 수 없었다. 사용자가 알려지지 않은 출처에서 악성코드를 다운로드했을 가능성도 있지만, 이것이 유일한 배포 채널은 아닐 것으로 추측된다."

"조사 결과, 이 앱들이 특정 전화 기기 브랜드에 더 빈번히 설치된다는 것을 발견했다. 따라서 공격자는 특정 기기 브랜드를 중점적으로 노리는 것으로 생각된다."

Malwarebytes 는 두 달 전 발표한 보고서에서 Xhelper 악성코드가 사용자를 신뢰할 수 없는 써드파티 출처로부터 앱을 다운로드하도록 이동시키는 "웹 리디렉션" 또는 "기타 수상한 웹사이트"에서 확산된다고 추측했다.

Xhelper 악성코드의 동작 방식

일단 설치되면, Xhelper 는 일반적인 사용자 인터페이스를 제공하지 않는다. 대신 사용자로부터 숨기 위해 기기의 애플리케이션 런쳐에는 나타나지 않는 애플리케이션 컴포넌트로써 설치된다.

Xhelper 는 전원 공급 장치에 감염된 기기를 연결 또는 연결 해제, 기기 재부팅, 앱 설치 또는 제거 등 사용자가 트리거 한 외부 이벤트 일부를 통해 자기 자신을 실행한다.

이 악성코드는 일단 설치되면 암호화된 채널을 통해 원격 C&C 서버에 연결하여 해킹된 안드로이드 기기에 드롭퍼, 클릭커, 루트킷과 같은 추가 페이로드를 다운로드한다.

"우리는 C&C 서버에 저장된 악성코드 풀이 매우 방대하고 다양한 기능을 포함하고 있어 공격자가 데이터 탈취, 기기 제어 권한 탈취 등 여러 공격을 실행할 수 있을 것으로 추측한다."

연구원들은 "일부 이전 변종들에 당시 구현되지 않은 빈 클래스가 포함되어 있었으나, 해당 기능은 이제 완전히 활성화되었다"며 Xhelper 의 소스 코드가 여전히 작성 중이라 추측했다.

Xhelper 악성코드는 주로 인도, 미국, 러시아의 안드로이드 스마트폰 사용자들을 노리고 있는 것으로 나타났다.

많은 안드로이드 안티바이러스 제품이 Xhelper 악성코드를 탐지하지만, 감염된 기기에서 이를 영구적으로 제거하거나 재 설치되는 것을 막지는 못했다.
이 악성코드의 출처가 아직 밝혀지지 않았기 때문에, 안드로이드 사용자들은 기본적이지만 아래의 효과적인 보안 기본 수칙을 준수할 것을 권장한다:

- 기기와 앱을 최신 버전으로 유지하기
- 익숙하지 않은 출처에서 앱 다운로드하지 않기
- 앱이 요구하는 권한에 항상 주의를 기울이기
- 데이터 자주 백업하기
- 안티바이러스 앱 설치하기

[출처] https://thehackernews.com/2019/10/remove-xhelper-android-malware.html
https://www.symantec.com/blogs/threat-intelligence/xhelper-android-malware

이미 전 세계에서 피해자 10 만명 이상을 감염 시킨 Raccoon 인포 스틸러 발견

Raccoon info stealer already infected 100,000+ worldwide

Cybereason 의 보안 전문가들이 새로운 인포스틸러인 Raccoon 을 발견했다. 이 악성코드는 이미 전 세계 수십만 명을 감염시킨 것으로 드러났다.

이 악성코드는 피해자의 신용카드 데이터, 이메일 크리덴셜, 가상 화폐 지갑 및 기타 민감 정보를 훔치기 위해 설계되었다.

이 악성코드는 서비스형 악성 코드(MaaS: malware-as-a-service)모델로 제공 되어 사이버 범죄 생태계에서 빠르게 인기를 끌었다.

"Raccoon 스틸러는 언더그라운드 생태계에서 2019 년 가장 많이 언급된 10 가지 악성코드 중 하나이며, 정교하거나 혁신적이지 않아도 전 세계 수십만 대 기기를 감염시킨 것으로 유명하다."

Raccoon 은 서비스형 악성코드 모델을 사용하며, 사용이 쉬운 자동화된 백엔드 패널을 구현했다. 또한 운영자들은 보안이 철저한 호스팅 및 영어/러시아어 24 시간 고객 지원 서비스를 제공한다. Raccoon 서비스의 가격은 1 달에 200 달러다.

연구원은 Raccoon 악성코드에 대해 정교하지는 않지만 여러 잠재적 공격 벡터를 활용해 대량의 민감 데이터를 훔치는 것이 가능하다고 설명했다.

Raccoon 은 러시아 개발자가 C++로 작성했으며, 처음에는 러시아어를 사용하는 해킹 포럼에만 독점적으로 홍보되었다. 이제 이 악성코드는 영어를 사용하는 해킹 포럼에까지 홍보되고 있으며, 32 비트 및 64 비트 환경에서 모두 작동한다.

언더그라운드 커뮤니티의 판매 로그를 분석한 결과, 전문가들은 Raccoon 이 이미 전 세계 10 만 명 이상의 사용자를 감염시켰을 것이라 추측했다. 이 악성코드가 성공할 수 있었던 핵심적인 이유는 서비스형 악성코드 모델을 통해 간단히 악성 캠페인을 실행할 수 있도록 해 기술이 있든 없든 모든 사용자들이 수익을 낼 수 있기 때문인 것으로 보인다.

이 악성코드는 2019 년 4 월 처음으로 발견되었으며 Fallout, RIG 를 포함한 익스플로잇 키트 다수와 피싱 캠페인을 통해 활발히 배포된다.
“커뮤니티의 많은 사람들이 Raccoon 의 악성코드의 기능과 팀이 제공하는 서비스를 찬양하고 지지한다. 일부 사람들은 이 악성코드가 악명 높은 Azorult 스틸러를 대체할 것이라고 말하고 있다.”
“Raccoon 스틸러는 악성 코드 시장에서 가장 혁신적인 인포스틸러는 아닐지라도, 언더그라운드 커뮤니티에서 매우 큰 관심을 불러일으키고 있다. Raccoon 팀은 사이버 범죄자들에게 막대한 개인적 투자 없이도 쉽고 빠르게 사이버 범죄를 저지를 수 있도록 안정적인 고객 서비스를 제공한다.”

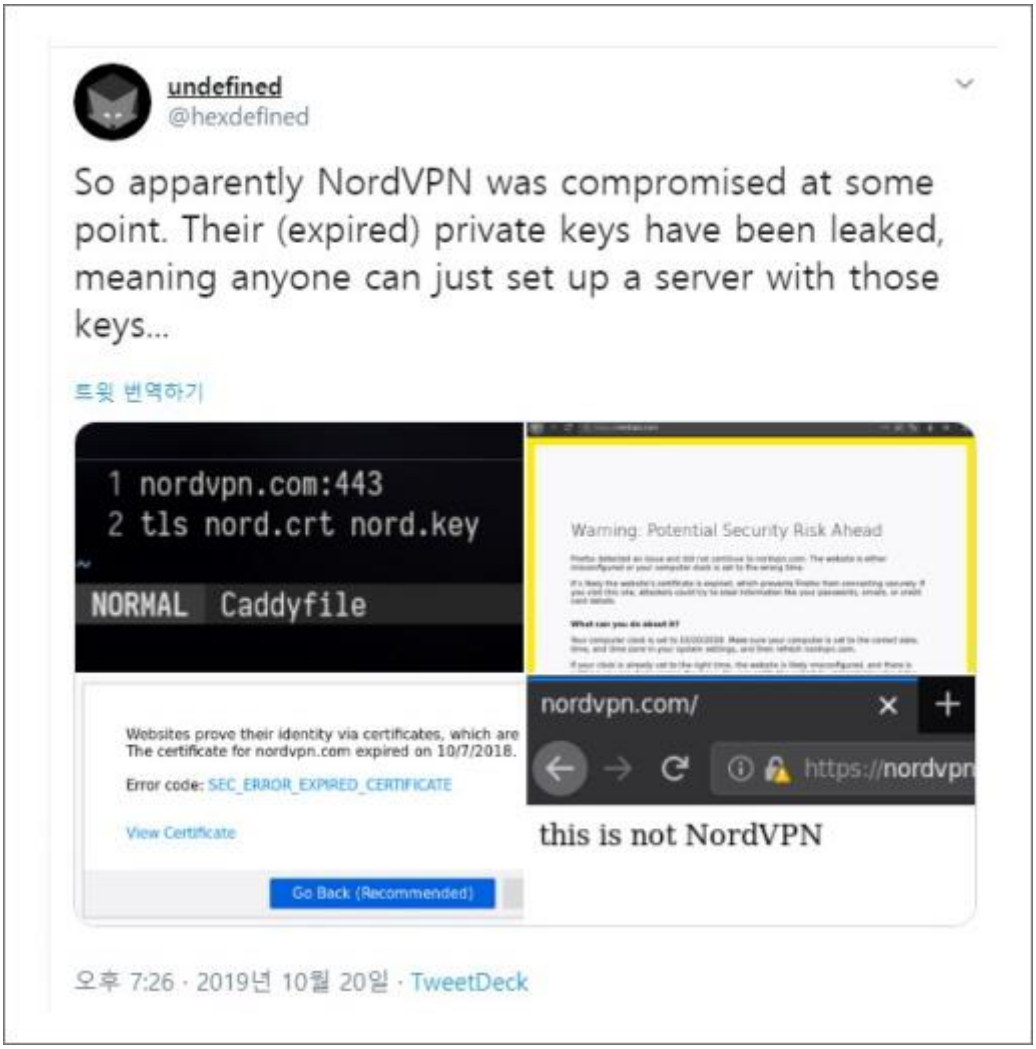
[출처] https://securityaffairs.co/wordpress/93028/malware/raccoon-info-stealer-maas.html

https://www.cybereason.com/blog/hunting-raccoon-stealer-the-new-masked-bandit-on-the-block

VPN 업체인 NordVPN, TorGuard, VikingVPN 에서 보안 유출 사고 발생해

NordVPN, TorGuard, and VikingVPN VPN providers disclose security breaches

해커가 NordVPN, TorGuard VPN 에서 사용 되는 시스템을 해킹하고 이들의 웹 서버와 VPN 구성 파일을 보호하는 데 사용된 개인 키를 공개했다.
온라인으로 유출된 NordVPN 의 정보는 작년 NordVPN 의 서버에서 훔친 것이었다.



공격자들은 회사의 개인 키 중 최소 3 개를 공개했다. 하나는 오래된 NordVPN 사이트 인증서에서, 두 개는 OpenVPN 키에서 가져왔다.
이 인증서는 2018 년 10 월 만료 되어 해킹이 작년에 발생했음을 나타내지만, 해당 서버가 만료된 인증서의 키를 저장하고 있었을 가능성도 배제할 수는 없다.
키가 온라인에 공개된 후, 전문가들은 공격자가 악성 VPN 서버를 설정하여 사용자의 트래픽에 중간자 공격(MiTM)을 실행하는 데 사용했을 수 있음을 지적했다.

출처: https://twitter.com/cryptostorm_is/status/1185976505203118081

Golem.de 의 전문가들은 만료된 인증서는 중간자 공격을 실행하는데 이용될 수 있었으나, 트래픽을 복호화할 수는 없었다고 밝혔다.

“유출된 키를 사용하여 저장된 VPN 트래픽을 직접 복호화할 수는 없다. 구성 파일을 통해 OpenVPN 구성에서 Diffie-Hellman 키 교환을 사용함을 알 수 있으므로, 이 연결은 소위 순방향 비밀 속성이 있어 추후 복호화를 막을 수 있게 된다.”

“이 키는 중간자 공격에 사용될 수 있다. 또한 공격자는 해킹 도중 트래픽에 접근할 수 있을 것이라 가정할 수 있다.”


```
root@vm-    :~# lxc-ls
     .nordvpn.com
     .nordvpn.com
     .nordvpn.com
     .nordvpn.com
root@vm-fi6:~# lxc-console --name      .nordvpn.com
root@fi30:~# cat /etc/openvpn/server.cfg
# This file is managed by puppet

dev tun
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys      .nordvpn.com.crt
key /etc/openvpn/keys/      nordvpn.com.key
dh /etc/openvpn/keys/dh2048.pem
username-as-common-name
client-cert-not-required
push "redirect-gateway def1"
push "sndbuf 524288"
push "rcvbuf 524288"
sndbuf 524288
rcvbuf 524288
topology subnet
```

NordVPN 은 해당 사고가 2018 년 3 월 발생했으며, 타사에서 운영 중이었던 핀란드에 위치한 데이터 센터 중 하나에 해커가 액세스 했다고 인정했다.

“몇 달 전, 2018 년 3 월 우리가 서버를 렌트 한 핀란드의 데이터센터 중 하나에 해커가 무단으로 액세스 했다는 사실을 발견했다.”

“공격자는 데이터센터 업체의 보호되지 않은 원격 관리 시스템을 악용해 해당 서버에 접근했다. 저희는 그러한 시스템이 있다는 사실 조차 알지 못했다. 이 서버는 사용자의 활동 기록을 저장하고 있지 않았다. 자사의 어떤 프로그램도 사용자가 인증을 위해 생성한 크리덴셜을 보내지 않았기 때문에, 사용자 계정 및 패스워드는 가로챌 수 없었다.”

NordVPN 은 해킹된 핀란드의 서버에는 만료된 TLS 키가 저장되어 있었다는 사실을 강조하며 다른 서버의 VPN 트래픽을 복호화하는 데는 사용될 수 없었을 것이라 밝혔다. 웹사이트 트래픽을 악용할 수 있는 유일한 방법은 nordvpn.com 에 접근을 시도하는 단일 연결에 인터셉트하기 위한 개인화된 정교한 중간자 공격(MiTM)을 실행하는 것뿐이다.

사고 후 NordVPN 은 즉시 조사에 착수했으며 해당 서버 제공업체와의 계약을 종료했다.

이 사고는 동일한 데이터센터를 이용하는 다른 VPN 업체인 VikingVPN 과 TorGuard 에도 영향을 미쳤다.

TorGuard 는 이 사고에 영향을 받은 업체 3 곳 중 안전한 PKI 관리 시스템을 구현한 유일한 VPN 제공업체였다. 이 회사의 메인 CA 키는 영향을 받은 VPN 서버에 저장되어 있지 않았다.

TorGuard는 “해킹된 TorGuard 서버 한 대는 2018년 초 네트워크에서 제거되었다. 또한 의심스러운 활동이 반복적으로 일어나 해당 호스팅 업체와의 모든 계약을 종료한 상태다.”
“이 사고로 인해 TorGuard VPN이나 프록시 트래픽은 해킹되지 않았으며, 어떠한 민감 정보도 해킹되지 않았다. 지금까지 어떠한 보안 위험도 발견되지 않았지만, TorGuard는 올해 초 자사의 보안 프로토콜에 따라 모든 인증서를 재발급받았다.”라 밝혔다.

[출처] https://securityaffairs.co/wordpress/92808/hacking/nordvpn-torguard-vikingvpn-hack.html

(주)이스트시큐리티

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