

# 이스트시큐리티 보안 동향 보고서

No.145 2021.10



# 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	06-12
알약 3분기 랜섬웨어 행위기반 차단 건수: 143,321건!	
국세청 세무조사통지서를 위장하여 유포중인 Lokibot 주의!	
03 악성코드 분석 보고	13-15
04 글로벌 보안 동향	16-22

# 01

## 악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

# 1. 악성코드 동향

2021 년 9 월에는 REvil 랜섬웨어 공격 그룹의 활동이 재개되었습니다.

지난 7 월 14 일, Kaseya 를 공격한 REvil(Sodinokibi) 랜섬웨어 그룹이 운영하는 웹사이트 및 인프라가 이유를 밝히지 않은 채 중단되었습니다. 그리고 약 2 개월 만에 다시 활동을 재개했습니다. 해당 그룹의 데이터 유출 사이트인 Happy Blog 와 지불/협상 사이트를 포함한 다크웹 포털 두 개가 다시 온라인에 나타났습니다. 또한 Bitdefender 가 REvil 랜섬웨어 피해자가 사용 가능한 복호화 툴을 개발하여 공개하였으며, 해당 툴을 통해서 7 월 13 일 REvil 랜섬웨어로부터 피해를 입은 파일들을 복호화 할 수 있습니다.

새로운 DDoS 봇넷 Meris 가 러시아의 IT 기업인 Yandex 를 공격했습니다. 해당 공격은 초당 요청 2180 만 건으로, 이는 러시아 역사상 가장 큰 규모의 DDoS 공격이었습니다. 또한 악성코드들 역시 점점 고도화 되고 있는 추세입니다. FinSpy, Wingbird 라고도 불리는 FinFisher 는 Gamma Group 에서 개발한 감시 솔루션으로 스파이웨어 변종에서 흔히 찾아볼 수 있는 악성코드와 유사한 기능도 함께 제공합니다. 이번에 FinSpy 를 로드하는 UEFI 부트킷이 발견되었으며, UEFI 부트킷에 감염된 모든 컴퓨터는 윈도우 부트 관리자(bootmgfw.efi)를 악성 프로그램으로 교체합니다. 이러한 방식은 펌웨어 보안검사를 우회할 필요 없이 부트킷을 설치할 수 있으며, 회피 및 지속성이 뛰어납니다.

국내에서는 북한 배후로 추정되는 APT 그룹들의 공격이 지속되었습니다. 금성 121 APT 조직은, 스피어피싱 공격 방식을 사용하여 북한 인권단체의 대표를 공격 타겟으로 삼았으며, 탈륨 (Thallium) (또는 김수키(Kimsuky)) 라고도 부름) 조직은 ‘불법사용 전화번호 이용중지시스템(UNMS) 이용자 점검 안내’라는 제목의 악성 메일을 유포하였습니다.

개인정보 유출 또한 지속되었습니다. 서울 성모병원이 해킹을 당해 고객정보가 유출되었으며, 야놀자 등의 4 개사가 클라우드 관리소홀로 개인정보 938 만 건이 유출되었습니다. 또한 삼성생명 채팅상담내역 유출, 개인 메일 사용으로 인해 15 명의 개인정보가 유출되었습니다. 답웹에서는 한국 부동산 경매 사이트 정보 및 여권 정보가 거래 중인 내용이 확인되기도 했습니다.

악성코드 및 해킹 공격들이 점점 정교화 되고 고도화 되면서 그 위협성 역시 점점 증가하고 있습니다. 또한 신규 혹은 이미 발견된 취약점을 악용한 공격들도 꾸준히 발생하고 있는 만큼, 보안담당자는 신규 취약점 등을 꾸준히 모니터링 하고, 주기적인 취약점 점검 및 보안패치를 통하여 잠재적인 위협의 가능성을 낮추려는 노력이 필요합니다.

## 2. 알약 악성코드 탐지 통계

### 감염 악성코드 TOP15

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

2021 년 9 월의 감염 악성코드 Top 15 리스트에서는 지난달에 4 위를 차지했던 Gen:Variant.Razy.767621 이 3 계단 상승하여 1 위를 차지했다. 이번 달에는 지난달과 비교하여 대체적으로 눈에 띄는 상승폭을 보이는 악성 코드가 없이 비슷한 순위 양상을 보였으며, 그 중 트로이목마 악성코드 유형에 속하는 Trojan.ShadowBrokers.A 가 5 계단 상승하여 2 위를 기록했다. 9 월에는 Gen:Variant.Razy.864420 을 비롯 하여 7 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다.

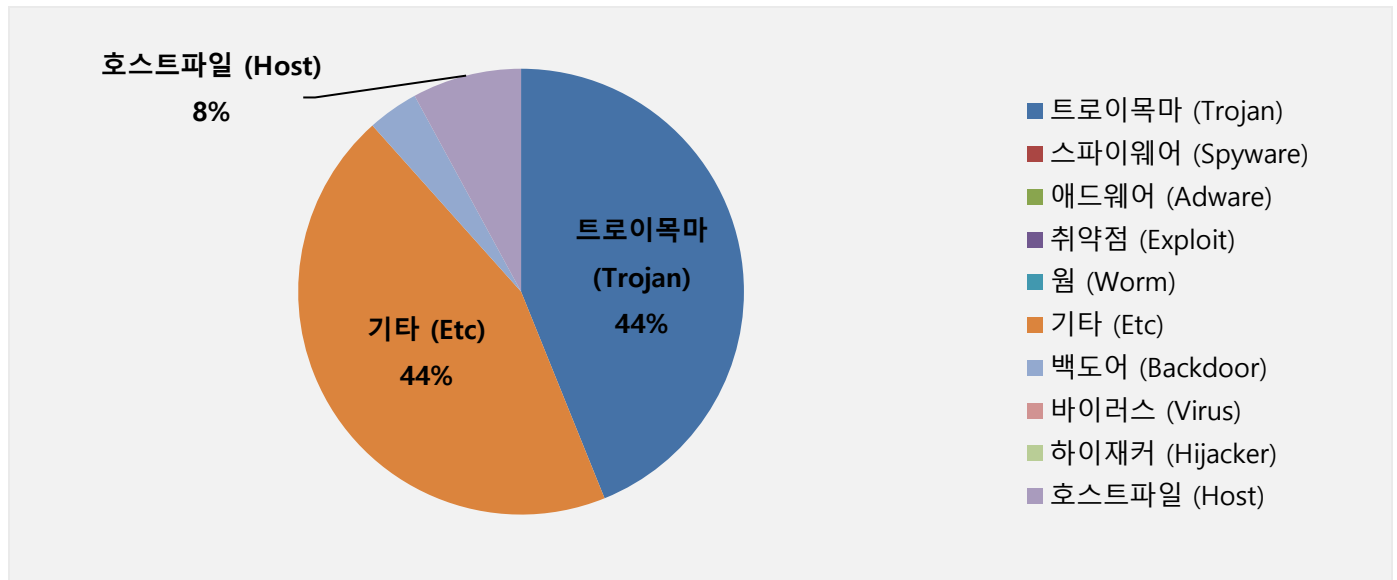
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 3	Gen:Variant.Razy.767621	ETC	391,059
2	↑ 5	Trojan.ShadowBrokers.A	Trojan	359,121
3	New	Gen:Variant.Razy.864420	ETC	319,913
4	New	Dropped:Trojan.GenericKD.40639357	Trojan	296,877
5	New	Gen:Variant.Bulz.624281	ETC	287,179
6	↓ 1	Hosts.media.opencandy.com	Host	272,024
7	↑ 2	Misc.HackTool.AutoKMS	ETC	262,180
8	New	Trojan.GenericKD.46767978	Trojan	194,944
9	New	Trojan.GenericKDZ.77118	Trojan	184,268
10	New	Trojan.Generic.15762280	Trojan	159,972
11	↑ 1	Trojan.Agent.Injector.Gen	Trojan	157,359
12	↑ 1	Trojan.Agent.Zpevdo.A	Trojan	153,561
13	↑ 1	Misc.HackTool.KMSActivator	ETC	136,226
14	New	Gen:Variant.Application.Keygen.16	ETC	130,446
15	↓ 1	Backdoor.Generic.792814	Backdoor	126,711

\*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 09 월 01 일 ~ 2021 년 09 월 30 일

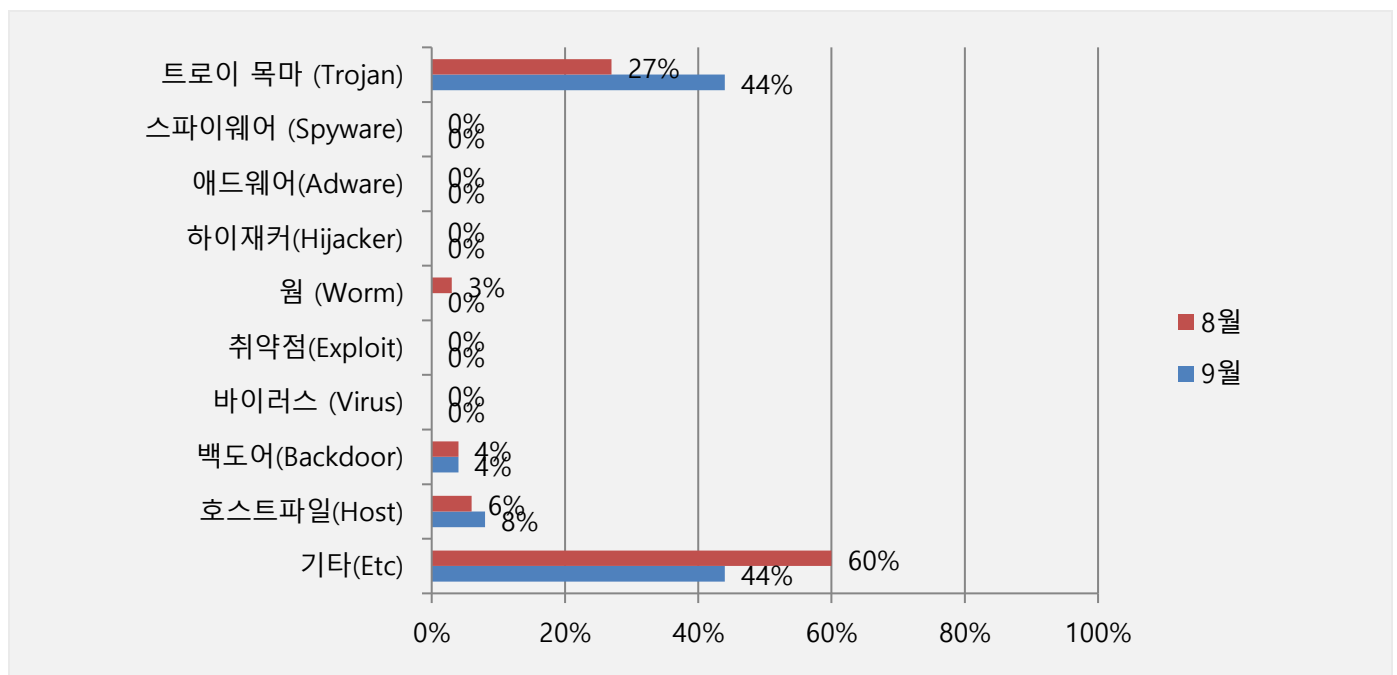
### 악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형과 트로이목마(Trojan) 유형이 각각 44%로 동일한 비율로 탐지됐으며, 호스트파일(Host)과 백도어(Backdoor) 유형이 8%와 4%로 그 뒤를 이었다. 2021년 8월과 비교하여 전체 감염 건수는 약 40.37% 감소하였다.



### 카테고리별 악성코드 비율 전월 비교

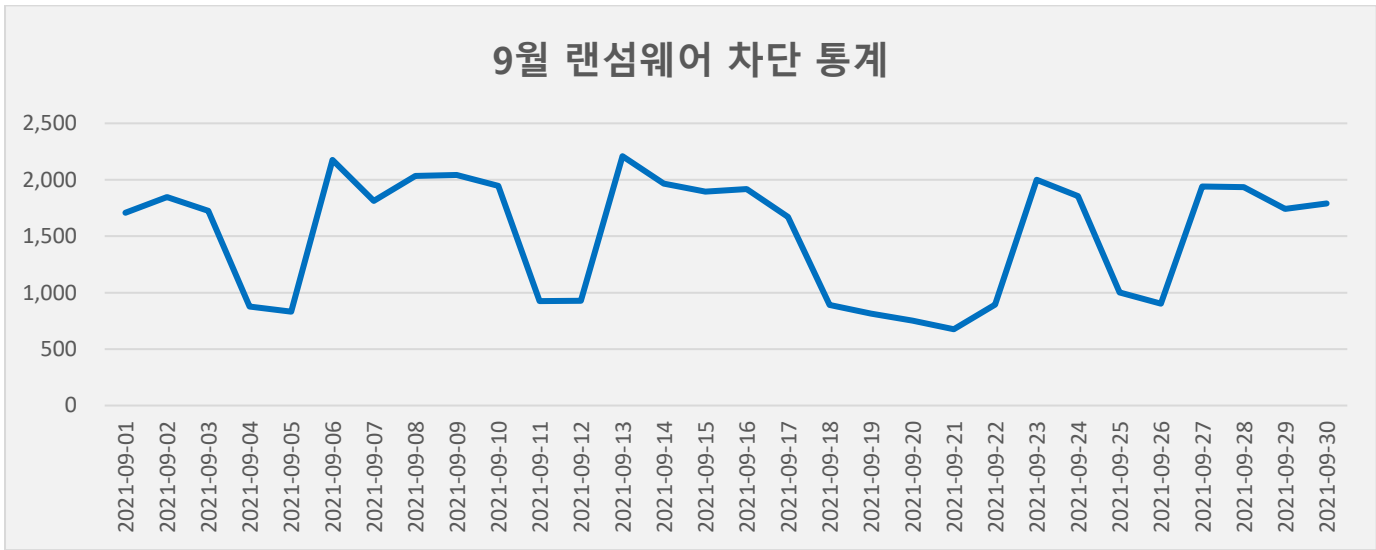
9월에는 지난 8월과 비교하여 트로이목마(Trojan) 유형이 17% 증가하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율이 2% 증가했습니다. 8월에 3%를 차지했던 웜(Worm) 악성코드 유형이 이번 달에는 낮은 탐지율을 기록하여 Top15 탐지명에 기록되지 못했습니다. 지난달에 4%를 기록했던 백도어(Backdoor) 악성코드 유형은 이번 달에도 4%를 기록하며 유사한 수치를 보였습니다.



### 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

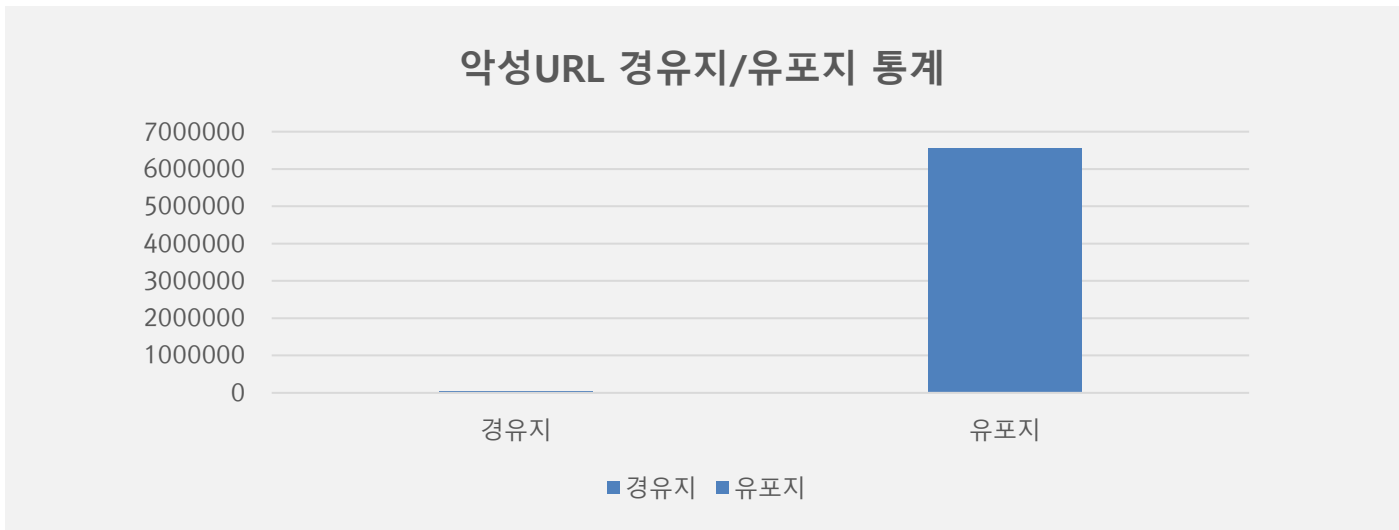
#### 9 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 ‘랜섬웨어 차단’ 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 9 월 1 일부터 9 월 30 일까지 총 45,706 건의 랜섬웨어 공격 시도가 차단되었다. 8 월의 랜섬웨어 공격 건수인 44,962 건에 비해 약 1.65% 가량 증가하였다.



#### 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 9 월 한 달간 총 6,584,480 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 8 월 한 달간 확인되었던 6,561,087 의 악성코드 경유지/유포지 URL 수에 비해 약 0.36% 가량 증가한 수치다. 악성코드 경유지/유포지 URL 의 경 우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바란다.



## 02

# 전문가 보안 기고

1. 알약 3 분기 랜섬웨어 행위기반 차단 건수: 143,321 건!
2. 국세청 세무조사통지서를 위장하여 유포중인 Lokibot 주의!



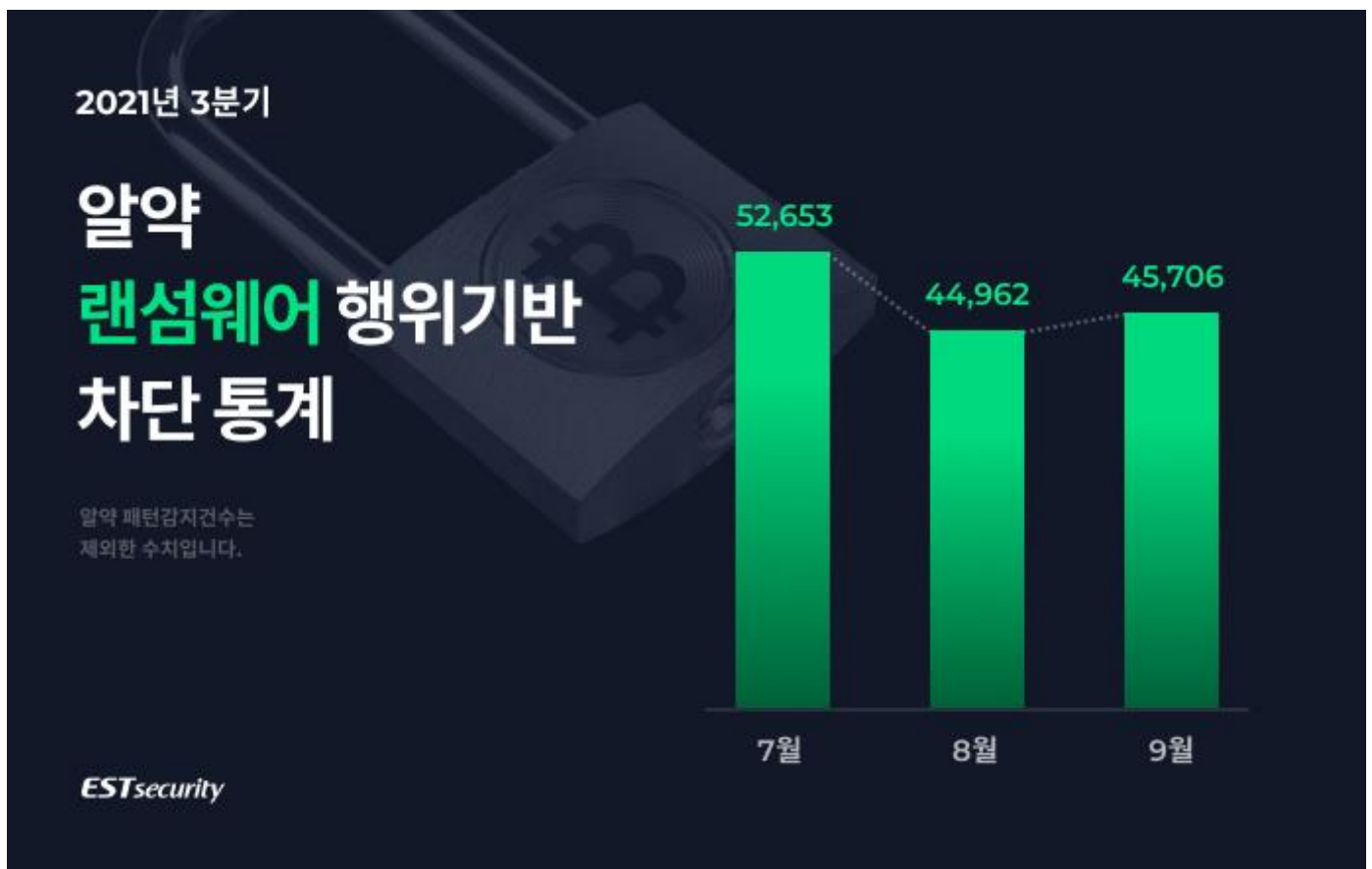
# 1. 알약 3분기 랜섬웨어 행위기반 차단 건수: 143,321 건!

2021년 3분기, 알약을 통해 총 143,321 건의 랜섬웨어 행위기반 공격이 차단된 것으로 확인되었습니다.

이번 통계는 개인 사용자를 대상으로 무료 제공하는 공개용 알약의 ‘랜섬웨어 행위기반 차단 기능’을 통해 차단된 공격만을 집계한 결과로, 패턴 기반 탐지 건까지 포함한다면 전체 공격은 더욱 많을 것으로 예상됩니다.

통계에 따르면, 2021년 3분기 알약을 통해 차단된 랜섬웨어 공격은 총 143,321 건으로, 이를 일간 기준으로 환산하면 일 평균 약 1,592 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다.

최근 2년에 걸쳐 전체 랜섬웨어 공격 건수는 지속적으로 감소하는 추세를 보였으며, 2021년 3분기에도 지난 2분기에 비해 소폭 감소한 것으로 나타났습니다.



[그림] 알약 랜섬웨어 행위기반 차단 기능을 통해 차단된 2021년 3분기 랜섬웨어 공격 통계

ESRC는 2021년 3분기 랜섬웨어 주요 동향을 다음과 같이 선정하였습니다.

- 1) Sodinokibi 랜섬웨어, 대규모 Kaseya 공급망 공격 수행
- 2) 유명 랜섬웨어 기능 포함하는 BlackMatter 랜섬웨어 발견
- 3) Lockbit 2.0 공격 기승으로 국내외 다수의 기업에서 피해 발생
- 4) '비너스락커' 그룹이 유포하는 Makop 랜섬웨어 공격 꾸준히 발생

2021년 3분기에는 피싱 이메일 내 입사 지원서, 저작권 침해 관련, 견적 문의 등 다양한 테마의 첨부파일 형태로 유포되는 Makop 랜섬웨어가 꾸준히 상위권을 유지했습니다. 또한 Sodinokibi 랜섬웨어 그룹이 대규모 Kaseya 공급망 공격을 수행하여 최소 1500 곳 이상의 조직이 피해를 입었습니다. Darkside, Sodinokibi 등 유명 랜섬웨어의 기능을 포함하여 제작된 BlackMatter 랜섬웨어가 발견된 점도 주목할 만합니다. 그 밖에도 새로운 버전을 도입한 LockBit 2.0 랜섬웨어 공격으로 다수의 국내외 기업이 피해를 입었습니다. 3분기 랜섬웨어 공격 건수는 2분기에 비해 다소 감소하는 추세를 보였습니다.

3분기에 주목할만한 위협으로는 7월에 발생한 Sodinokibi 랜섬웨어 그룹이 수행한 Kaseya 공급망 공격이 가장 눈에 띕니다. 지난 7월 러시아 해커들로 구성된 Sodinokibi 랜섬웨어 그룹이 IT 관리 소프트웨어인 Kaseya 업데이트를 통해 공급망 공격을 수행함으로써 최소 1,500 개 이상의 기관이 해당 공격으로 인한 피해를 입은 것으로 확인되었습니다. 공격자들은 Kaseya VSA 소프트웨어의 제로데이 취약점 (CVE-2021-30116)을 악용했고, Sodinokibi 해커들은 랜섬 머니로 초기에 7천만 달러를 요구했으며 이후 5천만 달러로 협상 가격을 낮추었습니다. 지난 5월에도 미국에서 발생한 송유관 기업 콜로니얼 파이프라인(Colonial Pipeline)에서 DarkSide 랜섬웨어 공격으로 인해 막대한 피해가 발생한 바 있습니다. 또한 9월에는 약 2개월 간의 공백을 깨고 Sodinokibi 랜섬웨어 인프라 일부가 다시 가동되어, 새로운 피해자가 발생한 것으로 확인되었습니다.

또한 7월 말, Colonial Pipeline 과 Kaseya 공격 이후 활동을 중단한 DarkSide 과 Sodinokibi 등 유명 랜섬웨어의 기능을 이어받은 BlackMatter 랜섬웨어가 발견되었습니다. 일본의 올림푸스(Olympus)를 공격한 것으로 알려진 'BlackMatter' 랜섬웨어는 RaaS 형태로 운영되며, 윈도우, 리눅스 등 다양한 운영 체제 버전 및 아키텍처 용으로 제공됩니다. BlackMatter 그룹은 Exploit, XSS 와 같은 해커 포럼에 게시된 광고를 사용하여 계열사 네트워크를 구축하고 있습니다. 또한 연간 매출이 1 억 달러 이상이며 네트워크 상의 호스트가 500 개에서 15,000 개 사이인 대기업 네트워크에 액세스할 수 있는 해커를 모집하고 있습니다. BlackMatter 그룹은 의료, 주요 인프라, 국방, 비영리, 정부 기관 등을 대상으로 공격을 수행하지 않을 것이라고 밝혔으며, 미국, 캐나다, 호주, 영국 소재의 기업 네트워크 접근 권한을 구매한다고 홍보 중입니다.

8월에는 윈도우 도메인 과정 자동화 등을 포함하여 새로운 버전으로 업그레이드된 LockBit 2.0 랜섬웨어를 악용한 공격으로 국내외 다수의 기업에 피해가 발생했습니다. 자동차, 은행, 정부, 기술, 에너지, 통신 등 다양한 산업 분야에 서비스를 제공하는 것으로 알려진 글로벌 IT 컨설팅 기업인 'Accenture'와 국내 기업 '진양오일셀'과 '풀무원'의 미국 법인이 LockBit 2.0 랜섬웨어 공격으로 인한 피해를 입었으며, 공격자들은 공격을 통해 획득한 기업 데이터를 유출하겠다고 협박하면서 랜섬 지불을 요구하는 '이중 갈취' 전략을 사용했습니다. 최근 랜섬웨어 해커 조직에 의해 대기업은 물론 중견 및 중소기업 등 국내외 기업들의 피해가 연이어 발생하고 있어, 다크웹 모니터링을 통해 해킹 조직의 활동 감시를 강화하고 피해 기업에 대한 지원을 확대하는 조치가 필요할 것으로 보입니다.

지난 2 분기에 이어 3 분기에도 비너스락커 그룹이 유포하는 Makop 랜섬웨어가 꾸준히 발견되었습니다. Makop 공격자들은 주로 입사지원서, 이력서, 경력 사항, 포트폴리오, 견적 문의 또는 이미지 저작권 침해 관련 문서로 위장한 EXE 파일을 첨부한 스피어피싱 이메일 형태로 랜섬웨어를 유포했습니다. 특히 지난 2 분기에도 발견된 HWP 아이콘을 사용한 Makop 샘플이 9 월부터 다시 발견되고 있으며, 8 월에는 새로운 파일 설명인 'GOMPlayerGlobal Setup File'과 PDF 아이콘을 이용한 사례도 확인되었습니다. 공격자들은 파일명, 파일 설명, 확장명, 메일 주소 등을 다양하게 변경해가며 탐지망을 교묘히 피해가는 수법을 이용했고, 그 외 특징들은 이전과 유사합니다.

이밖에도 Babuk 랜섬웨어를 기반으로 하는 새로운 랜섬웨어 'Groove'가 발견되었습니다. 8 월부터 활동을 시작한 Groove 운영자들은 다른 조직들과 마찬가지로 이중 갈취 전략을 사용하며, 9 월에는 약 50 만 개의 Fortinet VPN 자격 증명 목록을 유출한 것으로 확인되었습니다. 해당 유출은 바북(Babuk) 랜섬웨어 운영자 중 'Orange'와 동일인물인 RAMP 해킹 포럼 관리자에 의해 이루어졌으며, RAMP 포럼과 Groove 랜섬웨어 서비스 운영을 홍보하기 위해 수행한 것으로 추정됩니다. 유출된 자격 증명은 지난 몇 개월 동안 Fortigate 어플라이언스에서 실행되는 Fortinet FortiOS의 디렉터리 접근 취약점(CVE-2018-13379)을 악용해 수집되었으며, 해당 취약점이 현재는 패치된 상태이지만 많은 VPN 자격 증명이 여전히 유효하다고 Groove 운영자들은 주장하고 있습니다.

9 월에는 추석 키워드를 활용한 Penta 랜섬웨어 공격이 발견되었습니다. 해당 랜섬웨어는 피싱 메일을 통해 유포된 것으로 추정되며, '추석\_이벤트\_당첨.zip'이라는 파일명을 가진 ZIP 파일 내 2 개의 PDF 파일을 위장한 EXE 실행파일이 포함되어 있습니다. 2 개의 파일은 동일한 파일로, 사용자가 PDF 파일로 오인해 실행하면, 사용자 기기에서 Penta 랜섬웨어가 실행됩니다. 악성코드가 실행되면 현재 실행 중인 프로세스를 확인하여 중복 실행을 방지하고, 자가 복제 및 시작 프로그램 등록을 통해 PC 실행 시 자동으로 실행되도록 설정합니다. 또한 볼륨 새도 복사본 및 백업 카탈로그를 삭제함으로써 사용자의 파일 복구를 차단하며, 파일 암호화를 진행합니다. 파일 암호화 후 확장자를 [기존 파일명.확장자].PENTA로 변경하며, 파일 복호화를 위해 공격자 이메일로 연락하라는 내용이 포함된 랜섬노트를 띄웁니다. 추석 등의 명절 연휴 기간 동안에는 관련 테마를 활용한 다양한 공격들이 성행할 수 있음을 인지하고, 사용자들은 출처가 불분명한 이메일에 포함된 파일이나 링크를 클릭하지 않도록 함으로써 랜섬웨어 공격을 예방해야 합니다.

2021 년 3 분기에도 여전히 비너스락커 그룹의 Makop 랜섬웨어를 활용한 공격이 지속적으로 발견되고 있습니다. 최근에는 해커들이 제로데이 취약점을 악용하거나 이전에 대규모 공격에 이용된 악명 높은 랜섬웨어를 기반으로 공격을 제작함으로써 공격 효율성을 높이고 있으며, 데이터 유출을 빌미로 협박하는 '이중 갈취' 전략과 특정 시기에 따른 키워드 활용 등의 수법도 꾸준히 사용하고 있습니다. 또한 지난 2 분기에 발생한 미국 송유관 시설 공격에 이어, 3 분기에는 Kaseya 공급망 공격이 발생하는 등 국가 핵심 인프라 시설 및 IT 관리 소프트웨어 기업을 대상으로 하는 대규모 공격을 지속적으로 수행하고 있어, 추후 심각한 피해로 이어지는 것을 예방하기 위해서는 기업과 개인들은 주기적인 백업 및 안전한 보안 시스템 구축 등을 통해 사전에 대비하는 자세가 필요합니다.

이밖에 ESRC 에서 밝힌 2021 년 3 분기에 새로 발견되었거나, 주목할만한 랜섬웨어는 다음과 같습니다.

랜섬웨어 명	주요 내용
BlackMatter	Darkside 와 Sodinokibi 등 유명 랜섬웨어의 기능을 이어받은 랜섬웨어로, RaaS 형태로 운영되며, 윈도우, 리눅스 등을 포함한 다양한 운영 체제 및 아키텍처 용으로 제공됨. 주요 인프라는 타깃에서 제외하며, 다양한 국가의 기업 네트워크 접근 권한을 구매한다고 홍보함.
LockFile	PetitPotam NTLM 릴레이 공격 방식을 활용해 전 세계 다양한 네트워크의 윈도우 도메인을 공격하는 랜섬웨어로, 원본 PetitPotam(CVE-2021-36942)의 변종을 악용함. LockBit 의 랜섬노트와 매우 유사한 랜섬 노트를 사용하며, 이메일 주소에서 Conti 랜섬웨어와의 유사성도 확인됨.
Groove	Babuk 랜섬웨어를 기반으로 하는 새로운 랜섬웨어 그룹으로, '이중 갈취' 전략을 사용하며, 2021 년 8 월부터 활동을 시작해 9 월에 Fortinet VPN 자격 증명 유출 공격을 통해 발견됨. Fortinet FortiOS 의 디렉터리 접근 취약점(CVE-2018-13379)을 악용해 데이터를 수집하며, Babuk 랜섬웨어 운영자인 RAMP 해킹 포럼 관리자에 의해 유출이 이루어진 것으로 확인됨.
Chaos	웜 형태로 유포되며, 와이퍼 기능을 탑재한 랜섬웨어로 egg 확장자를 포함한 파일을 암호화 대상으로 함. 8 월에 최신 버전이 출시되었으며, Ryuk 랜섬웨어의 .NET 버전임을 내세워 Ryuk 랜섬웨어와 같은 계열사인 것처럼 홍보하였으나, 유사성은 확인되지 않음.
Penta	해외에서 제작되어 인터넷에 공개된 Chaos 제작물을 이용해 국내에서 제작된 것으로 추정되는 랜섬웨어로, 지난 9 월에 '추석' 키워드를 활용해 유포됨. ZIP 압축 파일 내 PDF 로 위장한 EXE 실행 파일을 통해 유포되며, 중복 실행 확인, 자가 복제 및 시작 프로그램 등록, 볼륨 새도 복사본 삭제를 통한 복구 무력화 순서로 공격이 진행됨.
DeepBlueMagic	디스크 드라이브를 암호화하여 사용이 불가능한 상태로 만드는 랜섬웨어로, 주로 Windows Server 2012 R2 를 사용하는 시스템을 공격함. D 드라이브를 제일 먼저 암호화하지만, C 드라이브는 암호화 대상에서 제외함. 디스크를 암호화하여 시스템 자체를 사용 불가능한 상태로 만들기 때문에 매우 위협적이며, 공격 효율성을 높이기 위해 디스크 암호화 시작 후 즉시 중단함.
AvosLocker	Microsoft Exchange 서버를 활용해 공격을 수행하는 랜섬웨어로, MS Exchange 서버를 활용해 도메인 컨트롤러에 침투하여 랜섬웨어를 유포함. 포럼에서 자신들의 제품을 'C++로 작성된 다중 스레드 랜섬웨어'라고 광고했으며, 은밀한 방식이 아닌 콘솔 애플리케이션으로 동작하여 세부 정보가 확인됨. 강력한 암호화 체계를 특징으로 하며, 공격자의 수동 접근 방식을 통해 수동으로 데이터를 탈취했을 것으로 추정됨.
Xiaoba	Windows 11 셋업 파일을 위장한 랜섬웨어로, 'Windows11 正式版(Windows 정식버전)'을 위장하고 있으며, 중국에서 제작되어 유포 중인 것으로 추정됨. 파일 복구 방지를 위해 볼륨 새도 복사본을 삭제하고, 암호화 완료 후 바탕화면을 일본어로 된 이미지로 변경하며, 카운트다운 숫자가 포함된 팝업창을 띄움으로써 일정 시간 후 암호화 파일이 모두 삭제된다는 메시지와 함께 복호화 키 입력란을 제공함.

랜섬웨어 유포 케이스의 대다수는 이메일 형태지만, 코로나 19 바이러스 확산 방지를 위해 재택 근무를 수행하는 임직원이 증가함에 따라 기업 내부망 접속을 위해 사용되는 재택 근무 단말기 OS/SW 보안 업데이트 점검을 의무화하고 임직원 보안 인식 교육도 병행해야 합니다.

이스트시큐리티는 랜섬웨어 감염으로 인한 국내 사용자 피해를 미연에 방지하기 위해, 한국인터넷진흥원(KISA)과의 긴밀한 협력을 통해 랜섬웨어 정보 수집과 유기적인 대응 협력을 진행하고 있습니다.

참고: 알약 2 분기 랜섬웨어 행위 기반 차단 건수: 158,188 건!

## 2. 국세청 세무조사통지서를 위장하여 유포중인 Lokibot 주의!

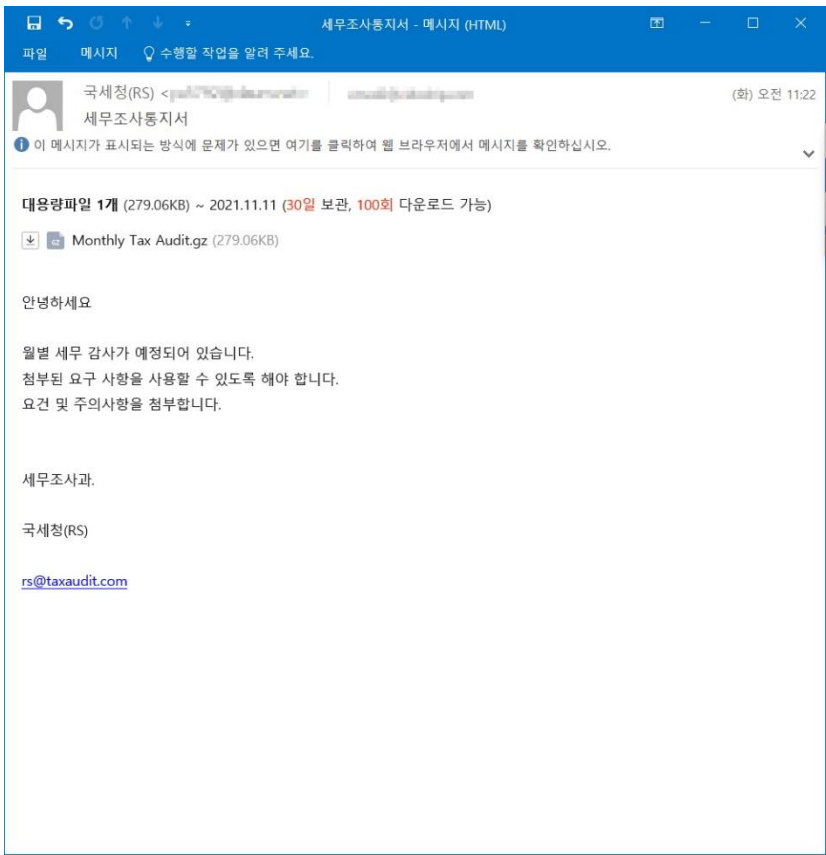
국세청 세무조사통지서를 위장하여 Lokibot 이 발견되어 사용자들의 주의가 필요합니다.

Lokibot 은 다양한 주제를 위장한 피싱 메일을 통해 꾸준히 유포되고 있으며, ESRC 에서도 이미 여러차례 관련하여 포스팅 한 적이 있습니다.

### 이전글 보기

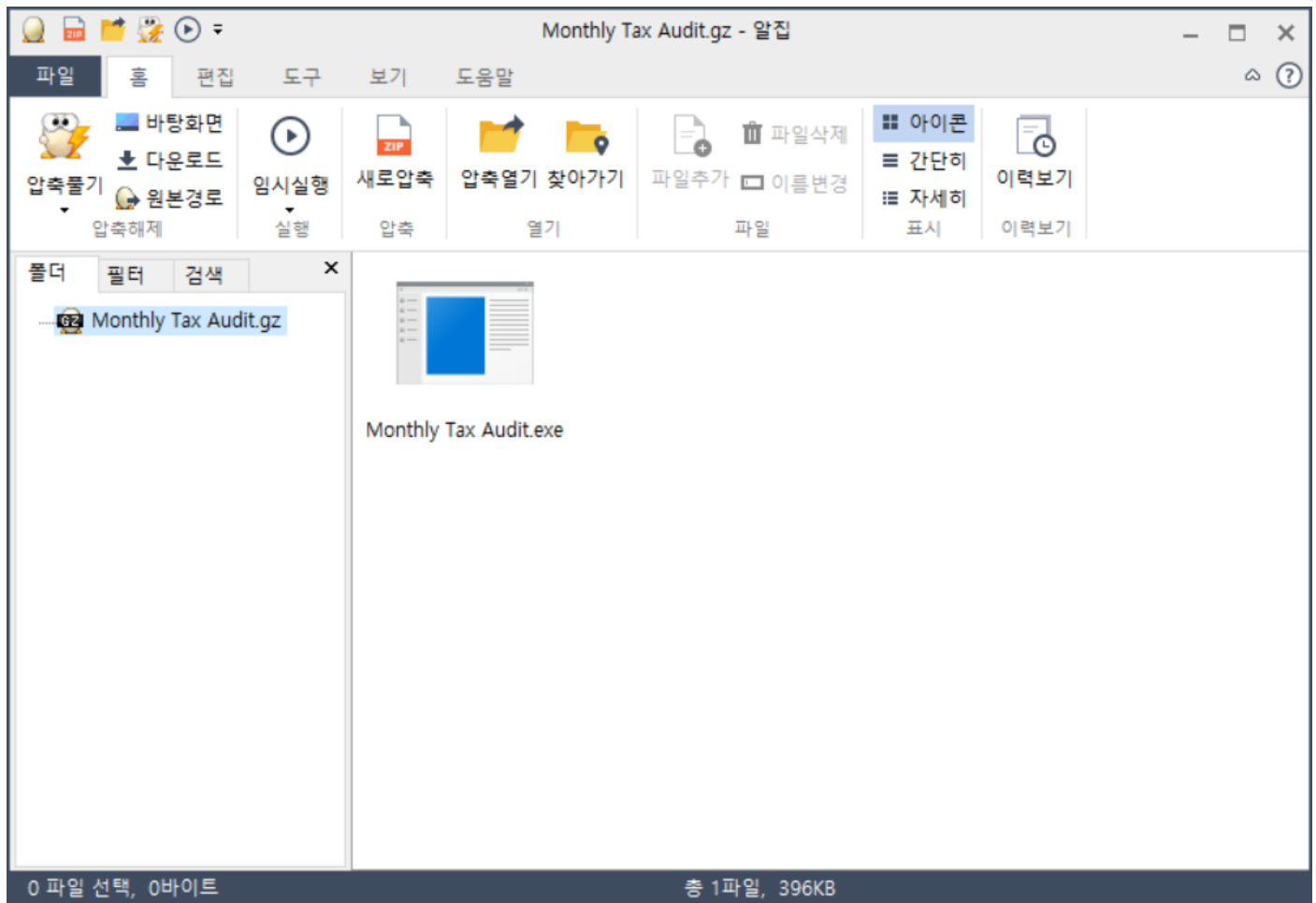
- ▶ 회계명세서, 견적문의 피싱 메일로 유포 중인 Lokibot 주의!(21.08.18)
- ▶ 네이버 전자세금계산서를 위장한 피싱 메일 주의!(21.07.15)
- ▶ 발주서로 위장한 LokiBot 악성 메일 유포중! (21.06.23)

이번 악성 메일은 '세무조사통지서'라는 제목으로 유포되고 있으며, 월별 세무 감사가 예정되어 있다며 첨부되어 있는 파일을 열람하도록 유도합니다.



## 02 전문가 기고

이메일에 첨부되어 있는 압축파일 안에는 Monthly Tax Audit 파일명을 가진 실행파일이 포함되어 있습니다.



만약 사용자가 해당 악성파일을 정상파일로 오인하여 실행한다면, 압축파일 내에 있던 Lokibot 악성코드가 실행되게 됩니다.

Lokibot 이 실행되면 사용자 PC 정보와 함께 웹 브라우저, 메일 클라이언트, FTP 프로그램 등에 저장해 놓은 계정 비밀번호를 탈취하여 공격자의 C&C 서버로 전송합니다.

### C&C 서버 정보

[hxxp://136.243.159.53/~element/page.php?id=505](http://hxxp://136.243.159.53/~element/page.php?id=505)

사용자 여러분들은 출처가 불분명한 사용자에게서 온 메일에 포함된 링크 클릭이나 첨부파일 실행을 지양해 주시기 바라며, 링크 클릭 혹은 첨부파일 실행 전 미리보기를 통해 링크 주소 및 파일 확장자를 확인해야 합니다.

현재 알약에서는 해당 악성코드에 대해 **Spyware.Lokibot** 으로 탐지중에 있습니다.

## 03

# 악성코드 분석 보고



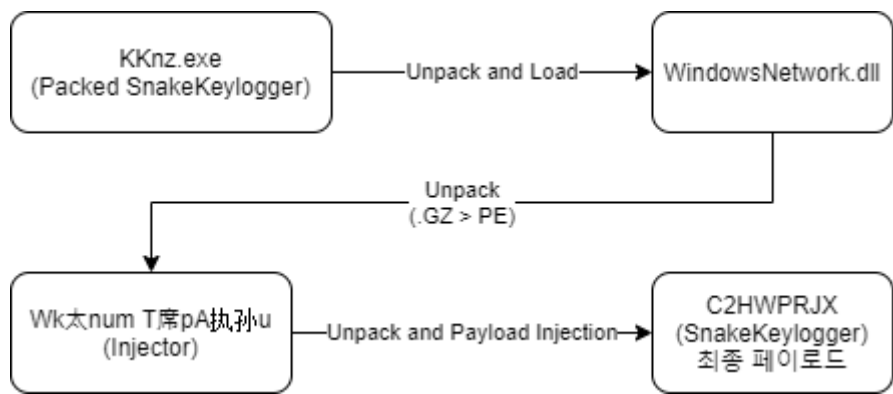
# [Trojan.GenericKD.37011310]

## 악성코드 분석 보고서

2020년 11월에 처음 등장한 스네이크 키로거(Snake Keylogger)는 닷넷으로 만들어진 인포스틸러 악성코드로서, 주로 피싱 이메일을 통하여 공격이 이루어 지고 지속적으로 유포해 오고 있다.

Snake Keylogger는 여러 웹 브라우저 및 이메일 클라이언트 등 다양한 프로그램의 계정 정보와 이외에도 PC 이름, 스크린샷, 클립보드, 키로깅 기능등 정보 탈취 기능을 가지고 있다.

또한, 닷넷 악성코드들은 빌더를 이용해 파일 진단을 회피하고 분석을 어렵기 하기 위한 목적으로 난독화를 수행한다.



[그림] SnakeKeylogger 로드 과정

스네이크 키로거(Snake Keylogger)는 처음 나온 이후로 지금까지 꾸준히 유포되고 있고 분석 환경을 우회하기 위해 난독화 수행, 로드된 모듈, 리소스 영역 인젝션 등을 이용한다.

본 악성코드는 사용자 정보를 탈취하는 것을 주목적으로 하며 키로깅, 클립보드 및 다양한 프로그램에서 민감한 사용자 계정 정보를 탈취하기 때문에 추가적인 피해가 야기될 수 있어 각별한 주의가 필요하다.

따라서, 악성코드 감염을 방지하기 위해 출처가 불분명한 이메일의 첨부 파일 확인을 지양해야 하며 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

현재 알약에서는 해당 악성코드를 ‘Trojan.GenericKD.37011310’ 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 [Threat Inside 웹서비스](#) 구독을 통해 확인이 가능하다.

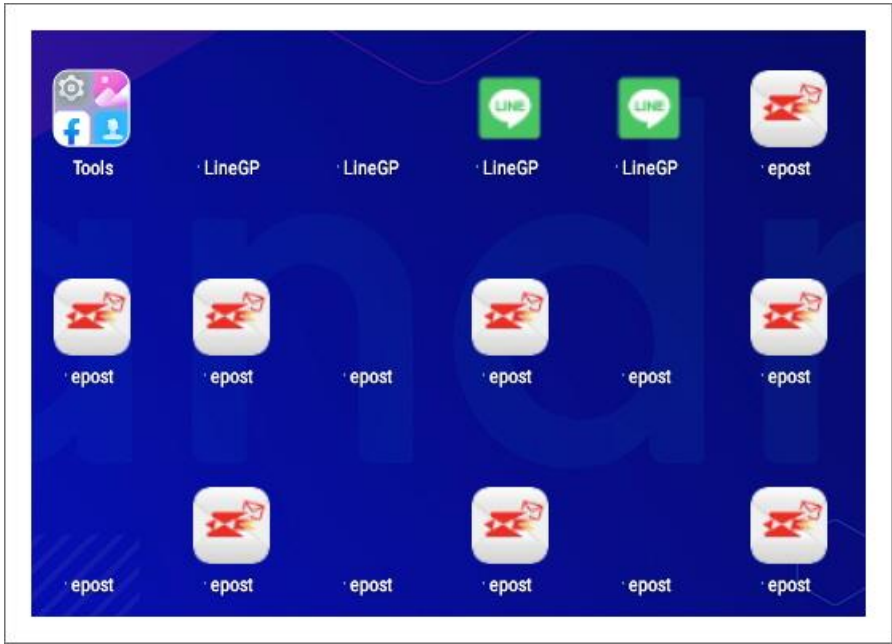


# [Trojan.Android.InfoStealer]

## 악성코드 분석 보고서

일반 사용자들의 스마트폰을 장악해 문자, 녹음, 갤러리 등등 사생활을 몰래 감시하고 정보를 탈취하는 악성 앱은 꾸준히 발견되고 있다. 최근 분석을 어렵게 하기 위해 다양한 방법을 사용한 앱을 발견하였으며 해당 앱 설치 시 개인정보 유출 및 원격제어가 가능하다. 여기서 유출된 계정과 기타 정보들은 판매되거나 또 다른 피해를 발생시킬 수 있다.

기존 크롬 브라우저 아이콘으로 위장했던 악성 앱은 현재 한국의 우체국과 라인 앱 등으로 위장하고 있다. 또한, 앱 실행 시 별다른 화면이 나타나지 않고 앱 목록에서 숨김 처리가 이루어진다.



[그림] 유사 앱 목록

위의 분석에서 앱 실행 시 화면이 나타나지 않았지만, 이 또한 웹 사이트에 있는 텍스트를 참고하여 피싱 사이트를 열어주기 때문에 화면에 표시되지 않았었다. 피싱 사이트는 pinterest 사이트의 몇몇 계정을 참고하며 공격자가 임의로 피싱 사이트 주소를 변경할 수 있다. 인포스틸러로써 다양한 정보들을 탈취하고 C2 와 피싱 사이트를 숨기기 위해 여러 장치들을 해놓은 이 앱은 앞으로도 분석을 더욱 어렵게 할 것으로 보인다.

현재 알약 M 에서는 해당 앱을 ‘Trojan.Android.InfoStealer’ 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 [Threat Inside 웹서비스](#) 구독을 통해 확인이 가능하다.

## 04

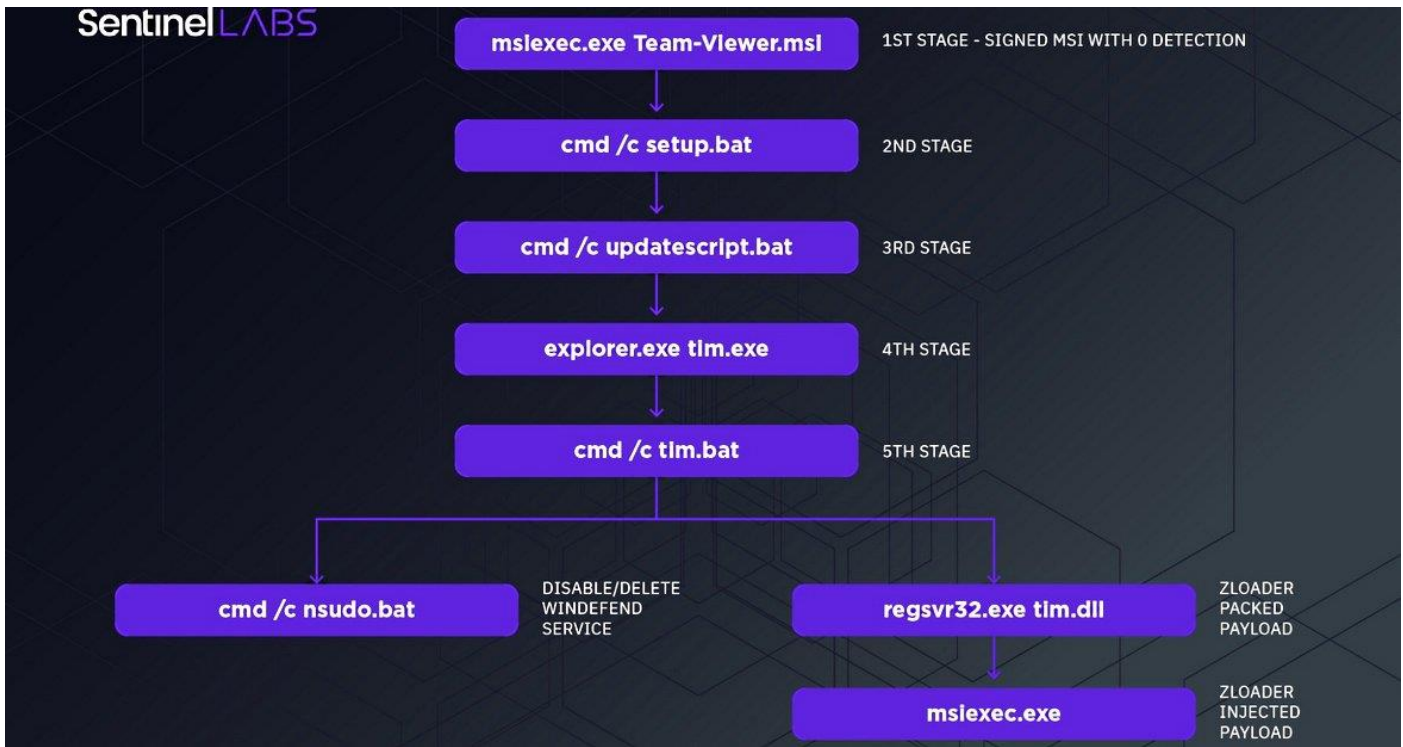
# 글로벌 보안 동향

## 새로운 Zloader 공격, 탐지를 피하기 위해 마이크로소프트 디펜더 비활성화 시켜

New Zloader attacks disable Windows Defender to evade detection

현재 진행 중인 Zloader 캠페인이 피해자의 컴퓨터에서 탐지를 피하기 위해 마이크로소프트 디펜더(구 윈도우 디펜더) 안티 바이러스 솔루션을 비활성화하는 새로운 감염 체인을 사용하는 것으로 나타났다. 마이크로소프트의 통계에 따르면, 마이크로소프트 디펜더 안티바이러스는 윈도우 10 을 사용하는 시스템 10 억 대 이상에 선 설치되어 있다.

공격자는 악성코드의 전달 벡터를 스팸 또는 피싱 이메일에서 구글 애드워드를 통해 게시되는 팀뷰어 구글 광고로 변경했다. 이 광고는 타깃을 가짜 다운로드 사이트로 이동시킨다. 해당 사이트에서는 사용자가 Zloader 악성코드 페이로드를 컴퓨터에 설치하도록 설계된 서명된 악성 MSI 인스톨러를 다운로드하도록 속인다. SentinelLabs 의 보안 연구원인 Antonio Pirozzi 와 Antonio Cocomazzi 는 보고서를 통해 다음과 같이 언급했다. "이 연구를 통해 분석한 공격 체인은 더욱 높은 은폐 수준에 도달하기 위해 공격의 복잡성이 어떻게 증가했는지 보여준다." 1 단계 드롭퍼는 고전적인 악성 문서에서 서명된 은밀한 MSI 페이로드로 변경되었다. 이는 백도어 바이너리와 일련의 LOLBAS 를 사용해 방어를 손상시키고 대신 그들의 페이로드를 실행한다.



[그림] Zloader 공격 체인

[이미지 출처] <https://www.sentinelone.com/labs/hidden-and-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/>

### 호주 및 독일 은행 고객에 집중된 공격

Zloader(Terdot, DELoader 로도 알려짐)는 2015 년 8 월 영국 금융 기관으로 타깃으로 한 공격을 수행했을 당시 처음 발견된 बैंकिंग 트로이목마다. Zeus Panda, Floki Bot 과 마찬가지로 이 악성코드는 약 10 여년 전 온라인에 유출된 Zeus v2 트로이 목마의 소스코드를 기반으로 한다. 해당 बैंकिंग 트로이목마는 호주와 브라질, 북미에 이르기까지 전 세계 은행을 노렸으며, 소셜 엔지니어링 기법을 통해 감염된 고객이 인증 코드 및 크리덴셜을 제공하도록 유도하는 웹 인젝션을 사용하여 금융 관련 데이터를 수집하려 시도했다.

최근에는 Ryuk, Egregor 등 랜섬웨어 페이로드를 전달하는 데도 사용되었다. 또한 Zloader 는 백도어 및 원격 액세스 기능을 포함하고 있으며 감염된 장치에 추가 페이로드를 드롭하는 악성코드 로더로도 사용될 수 있다. 연구에 따르면, 이 최신 캠페인은 주로 독일과 호주 은행 기관의 고객을 중점적으로 노리는 것으로 나타났다. 연구원들은 다음과 같이 결론지었다. "ZLoader 캠페인에서 해당 공격 체인을 관찰한 것은 이번이 처음이다. 이 글을 쓰는 지금, 우리는 해당 전달 체인이 특정 협력 파트너가 구현한 것인지, 주 운영자가 제공한 것인지에 대해 알 수 있는 증거는 찾아볼 수 없었다."

2020 년 초부터 Malsmoke 라 명명된 이 악성 광고 캠페인을 추적해온 MalwareBytes 는 공격자가 성인용 악성 사이트를 통해 Fallout 익스플로잇 키트를 사용하여 타깃을 Smoke Loader 악성코드 드롭퍼에 감염시킨 사례를 목격했다. 이는 2021 년 8 월 말부터 Discord, TeamViewer, Zoom, QuickBooks 를 모방한 사이트로 전환했으며, 보안 연구원인 nao\_sec 에 따르면 개인이 아닌 기업을 노릴 가능성이 높다.

[출처]

<https://www.bleepingcomputer.com/news/security/new-zloader-attacks-disable-windows-defender-to-evade-detection/>

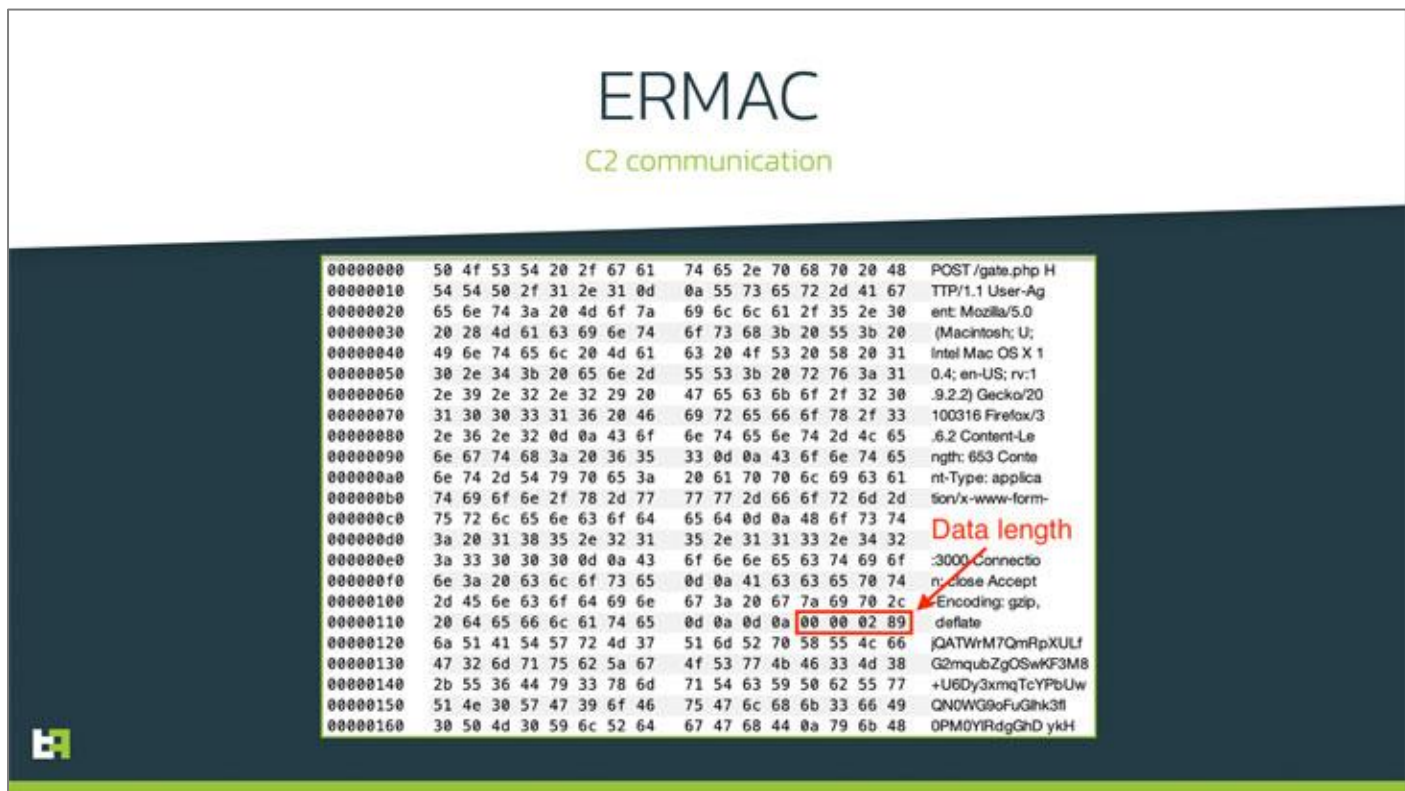
<https://www.sentinelone.com/labs/hidden-and-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/>

## ERMAC 안드로이드 뱅킹 트로이목마, 378 개 앱에서 금융 데이터 훔쳐

New Android Malware Steals Financial Data from 378 Banking and Wallet Apps

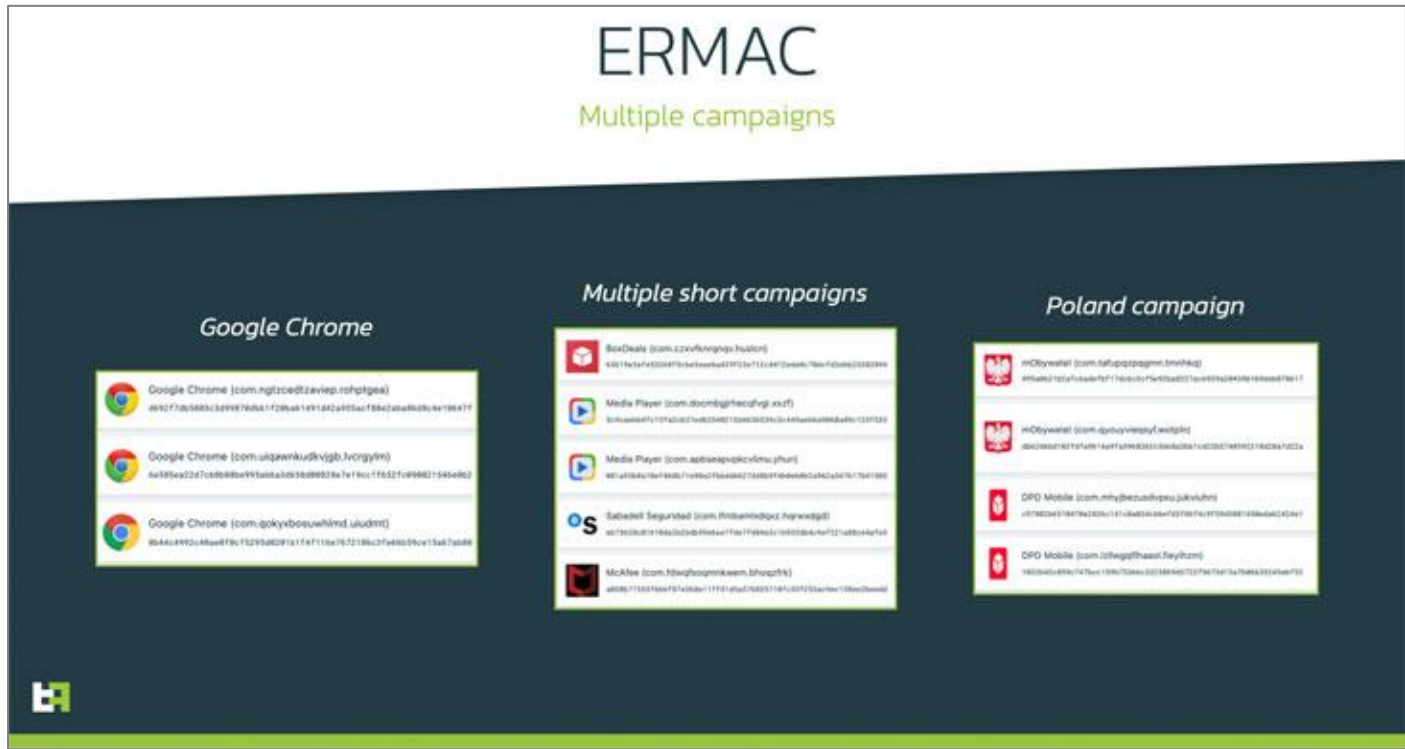
최신 연구에 따르면 BlackRock 모바일 악성코드의 운영자가 ERMAC 라는 새로운 안드로이드 뱅킹 트로이목마로 다시 활동을 시작해 폴란드 지역을 노리고 있는 것으로 나타났다. 이 트로이목마는 악명 높은 Cerberus 악성코드를 기반으로 제작됐다. ThreatFabric 의 CEO 인 Cengiz Han Sahin 은 이메일을 통해 "이 새로운 트로이목마는 이미 활발한 캠페인을 통해 배포 중이며 오버레이가 있는 은행 및 지갑 앱 378 건을 노린다"라고 밝혔다. ERMAC 을 사용한 첫 번째 캠페인은 지난 8 월 말 시작되었으며 구글 크롬 앱으로 위장했다. 이후 공격은 은행, 미디어 플레이어, 배달 서비스, 정부 앱, McAfee 와 같은 바이러스 백신 솔루션 등 다양한 앱을 포함하도록 확장되었다.

ERMAC 악성코드는 지난달 8 월 17 일 DukeEugene 이라는 공격자가 게시한 포럼 게시물에서 발견되었다. 그는 한 달에 3 천 달러에 “좁은 범위의 사람들에게 다양한 기능을 갖춘 새로운 안드로이드 봇넷을 임대”한다고 광고했다. DukeEugene 은 2020 년 7 월에 밝혀진 BlackRock 캠페인의 운영자로도 알려져 있다. 다양한 데이터 도난 기능을 갖춘 인포스틸러와 키로거는 2019 년 5 월 작성자가 소스코드를 공개한 다른 뱅킹 트로이목마 변종인 Xerxes 을 기반으로 한다.



[이미지 출처] <https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html>

또한 ThreatFabric 은 ERMAC 이 나타난 이후 새로운 BlackRock 샘플이 중단됨을 강조하며 "DukeEugene 이 공격에 기존에 사용하던 BlackRock 대신 ERMAC 을 사용하기 시작했을 가능성이 높다"고 밝혔다. 새롭게 발견 된 변종은 Cerberus 와 많은 점이 유사한 것 이외에도 난독화 기술, Blowfish 암호화 체계를 사용하여 C&C 서버와 통신하는 것으로 유명하다.



[이미지 출처] <https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html>

ERMAC 은 기타 बैंकिंग 약성코드와 마찬가지로 연락처 정보, 문자 메시지를 훔치고, 임의 앱을 열고, 로그인 자격 증명을 훔치기 위해 금융 앱 다수에 오버레이 공격을 실행하도록 설계되었다. 또한 악성 소프트웨어가 특정 응용 프로그램의 캐시를 지우고 기기에 저장된 계정을 도용할 수 있는 새로운 기능을 개발했다.

ERMAC 은 약성코드 소스코드 유출이 어떻게 해당 약성코드 패밀리의 증발을 늦출 뿐 아니라 위협 환경에 새로운 위협/행위자를 가져올 수 있는지를 보여주는 사례이다. 이는 RAT 과 같은 몇 가지 강력한 기능이 부족하지만 전 세계 모바일 बैंकिंग 사용자와 금융 기관에 여전히 위협이 되고 있다.

[출처]

<https://thehackernews.com/2021/09/new-android-malware-steals-financial.html>

<https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html>



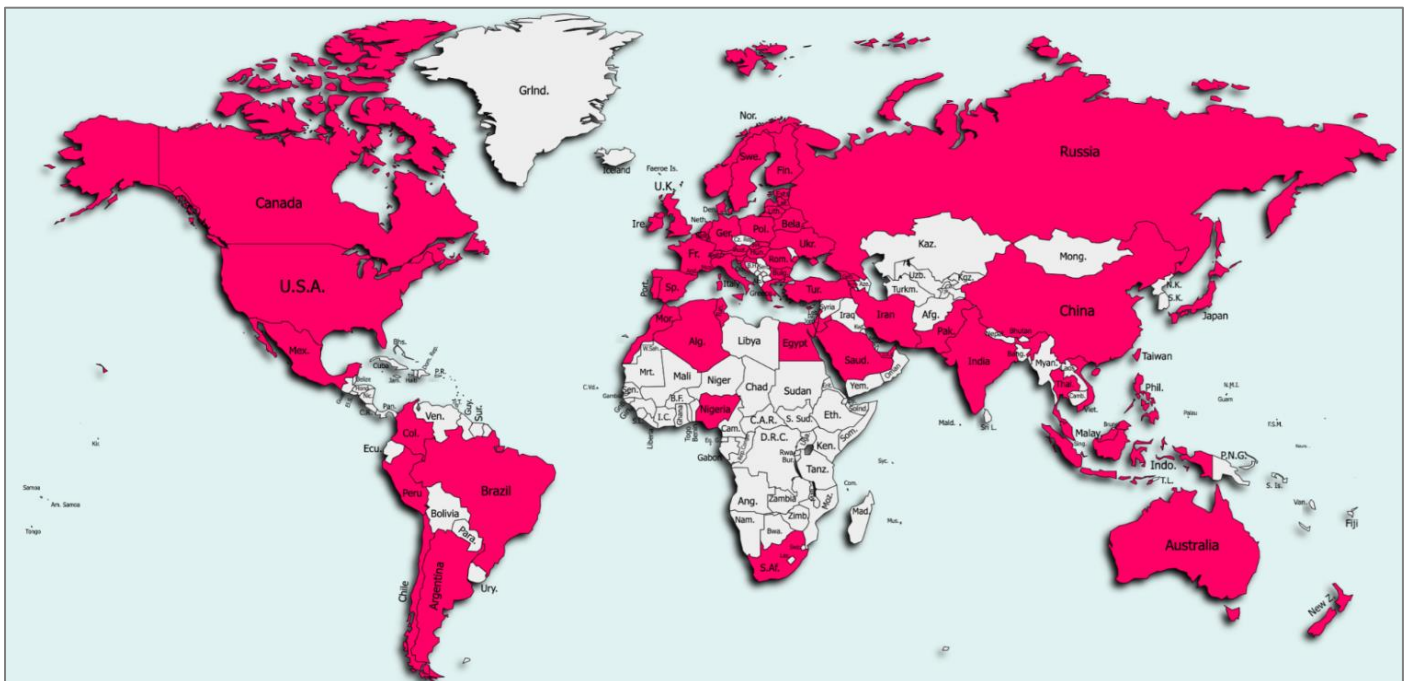
## 천만 명 이상의 사용자로부터 수백만 달러를 훔친 안드로이드 악성코드

## GriftHorse 발견

## New Android malware steals millions after infecting 10M phones

공격자가 대규모 악성코드 캠페인을 통해 70 개 이상의 국가에서 안드로이드 기기 천만 대 이상을 감염시켜 사용자가 모르는 사이 유료 서비스에 가입하여 수백만 달러를 훔쳤을 가능성이 있는 것으로 나타났다. 위 공격에 사용된 트로이목마인 GriftHorse 는 이 불법 글로벌 유료 서비스 캠페인을 처음 발견한 Zimperium zLabs 연구원이 발견했다. 이 캠페인은 악성 앱이 마지막으로 업데이트된 날짜인 2020년 11월부터 2021년 4월까지 약 5개월 동안 활성화되었다.

이 악성코드는 구글의 공식 플레이스토어와 타사 앱스토어에 등록된 트로이목마 안드로이드 애플리케이션 200개 이상을 통해 배포되었다. Google 은 해당 악성 앱에 대한 제보를 받은 후 이를 제거했지만, 타사 앱스토어에서는 여전히 다운로드가 가능하다. 연구원들은 이 사이버 범죄자가 전 세계 피해자로부터 매달 반복적으로 유료 서비스 요금을 받아 수백만 달러를 훔칠 수 있을 것으로 추정했다.

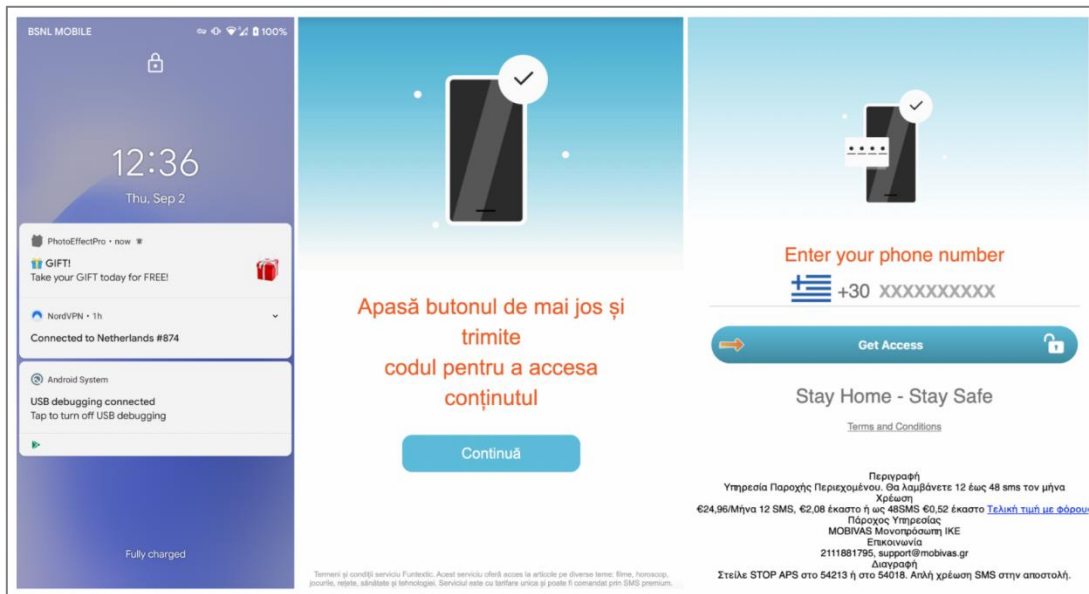


[그림] 70 개국 이상에 위치한 피해자

[이미지 출처] <https://blog.zimperium.com/grifhorse-android-trojan-steals-millions-from-over-10-million-victims-globally/>

### 전 세계 피해자로부터 수익 달러 훔쳐

공격자들은 GriftHorse 악성코드를 사용하여 피해자를 감염시키고 이들을 유료 서비스에 가입시켜 수백만 달러의 수익을 창출했다. 이 트로이목마 애플리케이션 200 개는 대부분의 백신에서 탐지되지 않았으며, GriftHorse 캠페인이 수행된 몇 달 동안 탐지를 회피할 수 있었다. GriftHorse 개발자는 앱의 양을 늘리는 것 이외에도 트로이목마 앱이 여러 범주에 분산되어 최대한 많은 피해자를 공격하도록 했다. 이 악성 앱이 피해자의 전화 기기에 설치되면, 휴대폰 번호에 접근이 가능해져 피해자가 전화 요금을 월 30 유로 이상 청구하는 유료 SMS 서비스에 가입하는데 사용했다. Zimperium 은 이에 대해 "최근 전 세계적으로 피해자 천만 명 이상이 발생한 공격적인 모바일 유료 서비스 캠페인을 발견했으며, 도난당한 총 금액은 수익 유로에 달할 수 있다"고 밝혔다.



[그림] Grifthouse 트로이목마

[이미지 출처] <https://blog.zimperium.com/grifthouse-android-trojan-steals-millions-from-over-10-million-victims-globally/>

### 도난당한 돈은 회수가 거의 불가능해

피해 사실을 즉시 알아차리지 못한 피해자(은행 계좌를 통해 반복 결제를 설정한 사람들)는 이미 해당 비용을 수개월 동안 지불했으며, 이를 회수할 수 있는 방법은 거의 없었다. "첫 번째 피해자 중 한 명이 이 사기 행각을 알아채지 못했다면, 이 글을 쓰는 시점에 이미 200유로 이상을 잃었다는 것을 의미한다. 피해자의 누적 손실은 사이버 범죄 그룹의 막대한 이익이 된다. 통계에 따르면 전 세계적으로 1 천만 명 이상의 안드로이드 사용자가 이 캠페인에 피해를 입었으며 재정적 손실을 입었다. 공격자는 시간이 지남에 따라 더 많은 돈을 벌어들였으며 더욱 동기 부여가 되었다."

피해자들은 유료 서비스 구독을 통해 도난당한 돈을 되찾기 위해 여전히 노력하고 있지만, GriftHorse 트로이 목마의 운영자들은 이미 수백만 달러를 벌어들인 후였다. GriftHorse 캠페인에 사용된 모든 트로이목마 앱의 전체 목록은 Zimperium 보고서에서 확인할 수 있다.

[출처]

<https://blog.zimperium.com/grifthouse-android-trojan-steals-millions-from-over-10-million-victims-globally/>





**(주)이스트시큐리티**

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

[www.estsecurity.com](http://www.estsecurity.com)