이스트시큐리티

보안 동향 보고서

No.151 2022.04

No.151 2022.04

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 06-11

한국도로공사 통행료 납부를 위장하여 유포중인 피싱 메일 주의!

병·의료원 건강검진 증명서 발급으로 위장한 北 연계 공격 등장

03 악성코드 분석 보고 12-14

04 글로벌 보안 동향 15-27

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2022 년 3 월에는 Kimsuky 그룹의 소행으로 추정되는 APT 공격과 정품인증을 위장한 RAT 유포, 이메일을 통한 스피어 피싱, 러시아와 우크라이나의 사이버 전쟁 등 다양한 보안 위협이 발견되었습니다.

코로나 19 사태가 지속되고 있는 가운데 매출이 줄어든 소상공인을 대상으로 저금리 대출이라는 스미싱 문자를 이용한 보이스 피싱 범죄가 빈번하게 발생하고 있으며, 해당 조직에서는 저금리를 미끼로 작성하였기 때문에 문자를 받은 사용자들은 혹할 수밖에 없습니다. 정부지원과 무료 거부, 평일 상담 시간 등등 실제로 기업에서 보낸 것처럼 위장하여 사용자가 알아차리기 어렵습니다. 이외에도 자녀 사칭을 이용한 스미싱도 지속적으로 발생되고 있습니다.

3 월달에는 Kimsuky 그룹의 소행으로 보이는 APT 공격이 집중적으로 발견되었습니다.
건강검진 증명서 발급이나, 남북관계 주요일지, 가상 화폐와 관련 된 문서, 대북관계자를 노린 지방세입 고지서로 위장한 포털사이트 피싱 등 국내 기업 사용자를 노린 스피어 피싱이 다수 발견되었습니다.

또한 윈도우 운영체제와 오피스의 정품 인증툴로 위장한 RAT 악성코드가 웹하드 및 파일공유 사이트에서 대량 유포되고 있어 주의가 필요합니다.

외국 이슈로는 러시아와 우크라이나의 전쟁이 지속되면서, 국제적인 해커그룹인 Anonymous 는 러시아의 스트리밍 서비스, 파이프라인 회사 데이터 유출, 중앙은행 데이터 등을 해킹하거나 공격을 시도하고 있으며, 우크라이나의 인터넷 제공 기업인 Ukrtelecom 가 대규모 사이버 공격을 받아 우크라이나 전역에서 인터넷이 중단되는 현상이 발생하기도 했습니다.

이메일이나 자료 공유 사이트에서 다운받는 파일들은 실행에 각별히 주의해야하며, 필요한 프로그램들은 반드시 공식 홈페이지에서 다운로드 받아 사용할 것을 권장드리며, 스피어 피싱 관련 피해를 예방하기 위해 출처를 알 수 없는 메일에 첨부된 파일 및 URL 을 절대 클릭하기 않아야 하며 정부 기관 및 잘 알려진 조직으로부터 전달된 메일이라도 항상 의심하고 주의하는 보안 의식이 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2022 년 3 월의 감염 악성코드 Top 15 리스트에서는 국내 광고 소프트웨어를 설치하는 Hosts.media.opencandy.com 악성코드가 609,977 건에서 665,984 건으로 약 9.1% 증가하였고 여전히 지난달에 이어 지속적으로 1 위를 유지하고 있다.

오토캐드 파일을 감염 시키는 Worm.ACAD.Bursted, Trojan.Lisp.Agent.F 악성코드도 지속적으로 높은 탐지율을 보여주고 있으며, Filecoder Ransomware 관련 된 Trojan.Cryxos 악성코드도 꾸준히 탐지되고 있다. 윈도우 불법 정품 인증 프로그램과 관련된 AutoKMS 악성코드는 RAT 악성코드와 연결되어 유포되면서 지난달에 이어 많은 탐지율을 보여주고 있다.

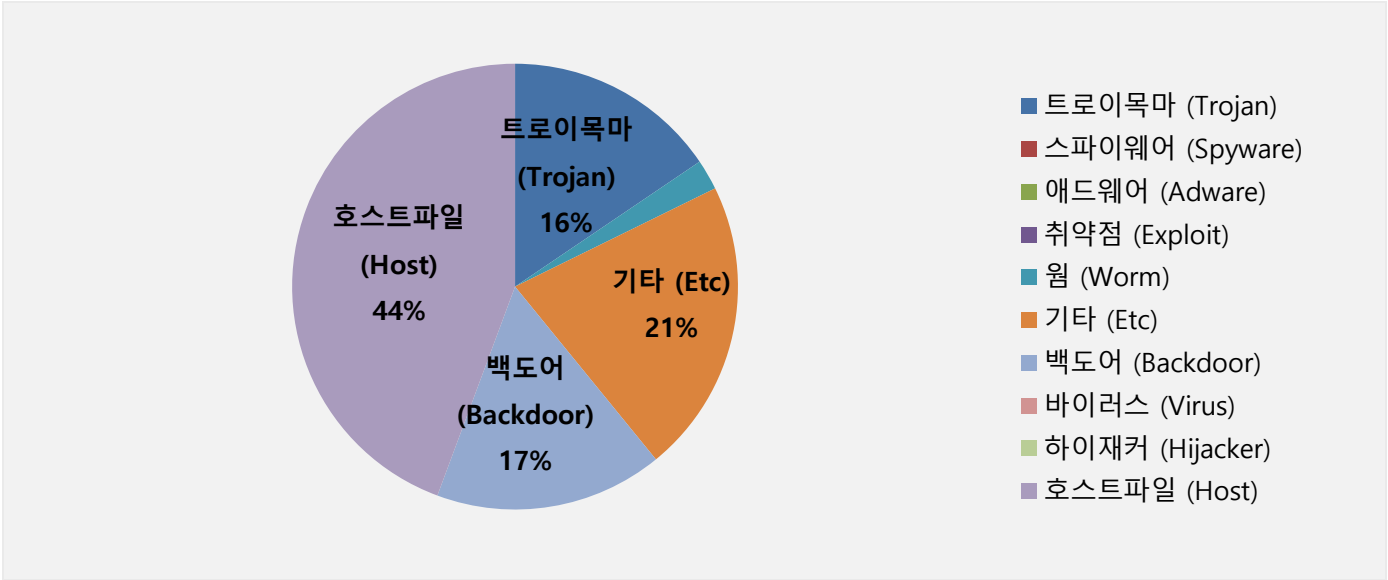
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	665,984
2	-	Backdoor.Generic.792814	Backdoor	248,700
3	-	Misc.HackTool.AutoKMS	ETC	95,013
4	-	Trojan.Lisp.Agent.F	Trojan	56,622
5	↓ 1	Trojan.Damaged.PE	Trojan	56,109
6	↑ 2	Misc.HackTool.KMSActivator	ETC	49,935
7	↑ 4	Application.Hacktool.KMSActivator.AI	ETC	42,689
8	↓ 1	Application.Hacktool.KMSActivator.HA	ETC	41,095
9	↑ 3	Application.Hacktool.KMSActivator.HJ	ETC	40,603
10	↓ 5	Trojan.Downloader.1481240	Trojan	38,450
11	New	JS:Trojan.Cryxos.5628	Trojan	36,267
12	↓ 2	Application.Hacktool.KMSActivator.AK	ETC	35,248
13	↑ 2	JS:Trojan.Cryxos.5175	Trojan	33,159
14	-	Application.Hacktool.KMSAuto.AT	ETC	32,334
15	↓ 2	Worm.ACAD.Bursted	Worm	29,988

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2022 년 3 월 01 일 ~ 2022 년 3 월 31 일

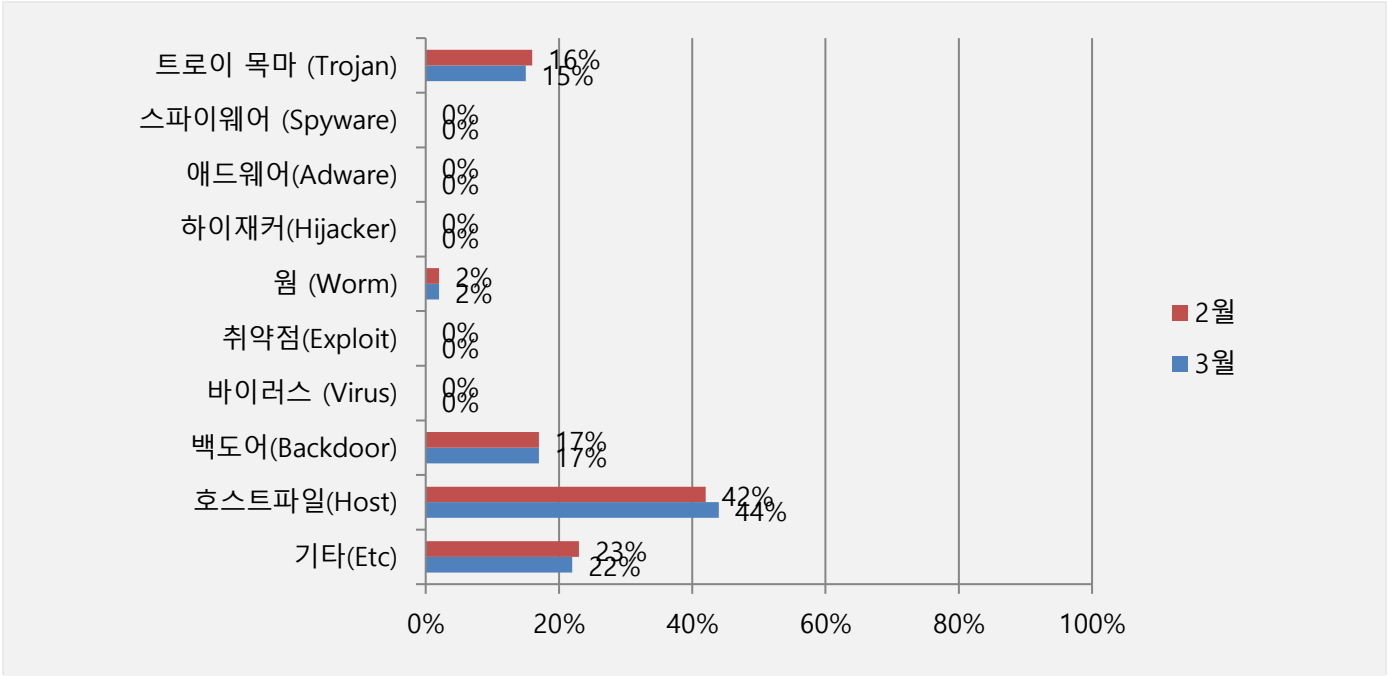
악성코드 유형별 비율

악성코드 유형별 비율에서 호스트파일(Host) 이 지난달에 이어 44%로 가장 높은 비율로 탐지 되었으며, 기타(ETC) 유형과 백도어(Backdoor) 유형이 22%, 17%로 트로이목마(Trojan)와 웜(Worm) 유형이 15%, 2%로 확인되었다. 2022 년 2 월과 비교하여 전체 감염 건수는 약 8.3% 증가하였다.



카테고리별 악성코드 비율 전월 비교

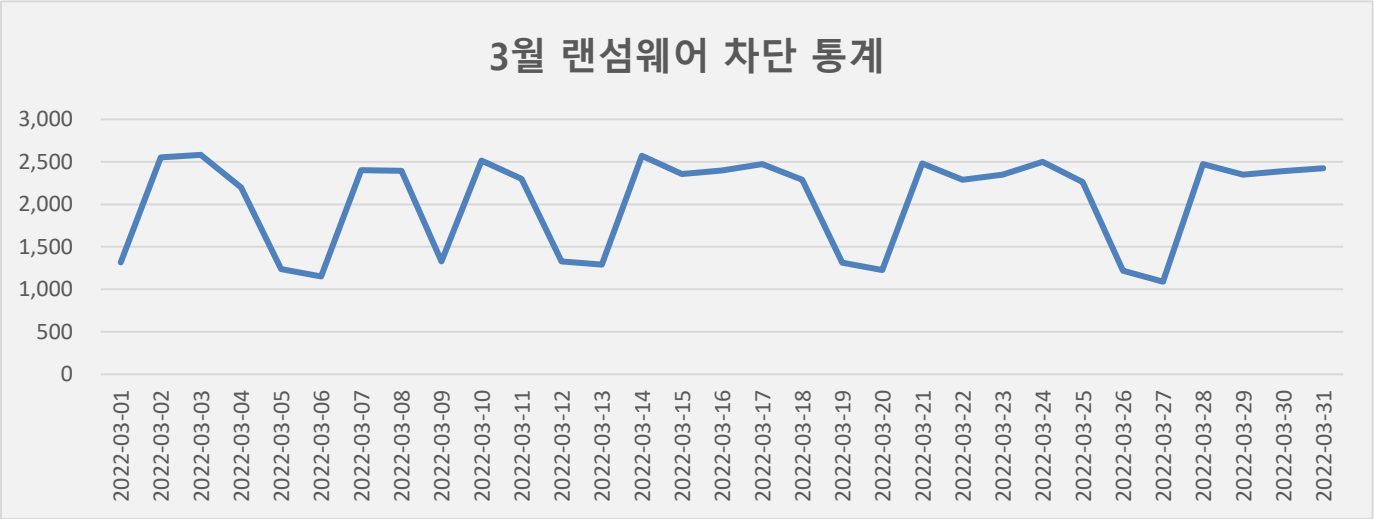
2022 년 3 월에는 지난 2 월과 비교하여 기타(ETC) 유형이 1% 감소했으며, 호스트파일(Host) 유형의 악성코드 감염이 2% 증가하면서 지속적인 높은 탐지율을 기록하고있다. 백도어(Backdoor), 트로이목마(Trojan) 유형은 전월 대비 비슷한 17%,15%를 기록하였고 웜(Worm) 유형이 2%로 지난 달과 동일한 탐지율을 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

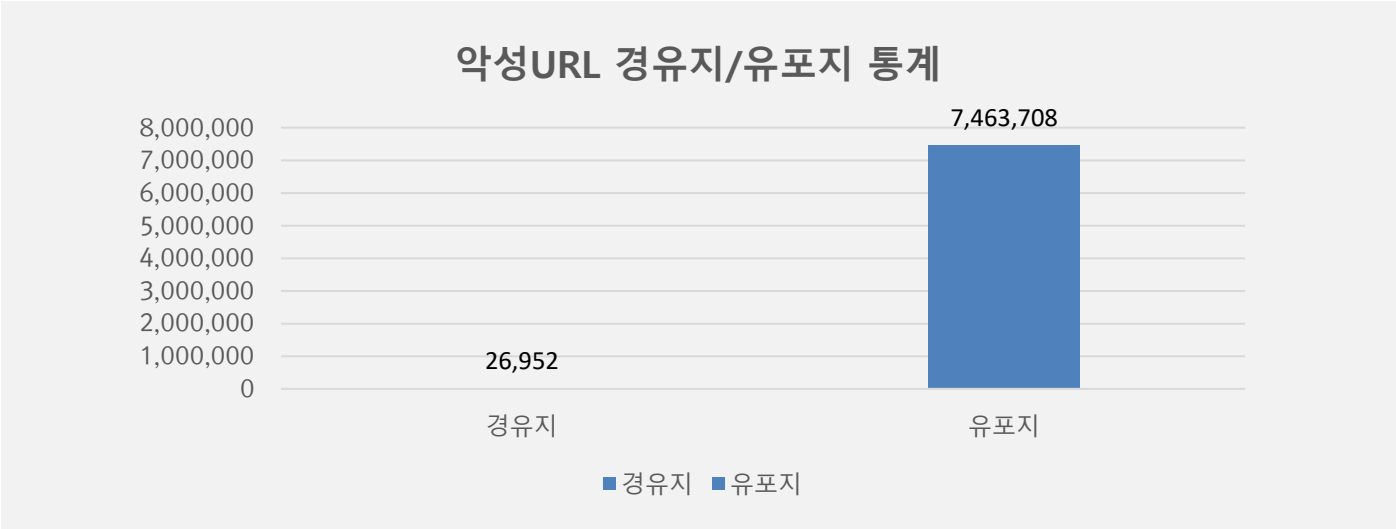
3 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 3 월 1 일부터 3 월 31 일까지 총 63,047 건의 랜섬웨어 공격 시도가 차단되었다. 2 월의 랜섬웨어 공격 건수인 54,997 건에 비해 약 14.6% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 3 월 한 달간 총 7,490,660 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 2 월 한 달간 확인되었던 6,555,240 의 악성코드 경유지/유포지 URL 수에 비해 약 14.2% 가량 증가한 수치다. 악성코드 경유지/유포지 URL 의 경우 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. 2022 년 1 분기 알약 랜섬웨어 행위기반 차단 건수: 177,732 건!

2. 비너스락커 조직, 또 다시 Makop 랜섬웨어 유포중

1. 2022 년 1 분기 알약 랜섬웨어 행위기반 차단 건수: 177,732 건!

2022 년 1 분기, 알약을 통해 총 177,732 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.

1 분기 알약을 통해 차단된 랜섬웨어의 공격은 총 177,732 건으로, 일간 기준으로 환산하면 일 평균 약 1,974 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다.

랜섬웨어의 공격 건수는 2021 년도 4 분기에 비해 약 1 만 4 천여건 증가하였습니다.

02 전문가 기고

ESRC 는 2022 년 1 분기 랜섬웨어 주요 동향을 다음과 같이 선정하였습니다.

1) 러시아,우크라이나 전쟁과 랜섬웨어
2) 꾸준히 랜섬웨어를 유포 중인 비너스락커 조직
3) 타이포스쿼팅을 통해 유포되는 매그니베르 랜섬웨어
4) 글로벌 기업들의 랜섬웨어 피해 지속

2022 년 1 분기, 러시아의 우크라이나 침공이 세계적인 이슈였습니다. 사회적, 경제적 등 다양한 방면에서 혼란을 야기하였으며, 해당 이슈를 이용한 랜섬웨어 공격도 발견되었습니다.

HermeticRansom 랜섬웨어는 우크라이나 시스템을 노린 타깃형 공격에 사용된 랜섬웨어로, 해당 랜섬웨어는 일반적인 랜섬웨어처럼 금전 갈취가 아닌 와이퍼 공격의 미끼 역할을 주 목적으로 하고 있습니다. 하지만 얼마 지나지 않아 Avast 에서 해당 랜섬웨어의 복호화툴을 개발하여 무료로 제공하였습니다.

또한 러시아를 타깃으로 하는 랜섬웨어가 발견되었는데, 일반 랜섬웨어와 다르게 랜섬머니를 요구하지 않으며, 대신 전쟁을 멈추라는 메시지를 띄웁니다.

우크라이나 연구원이 Conti 랜섬웨어의 소스코드를 포함한 정보를 유출시켰습니다. 이는 Conti 랜섬웨어가 우크라이나를 공격하는 러시아 정부를 지지한다는 공지를 띄운 것에 대한 보복으로 추측되고 있습니다.

비너스락커 조직의 활동도 활발히 이어지고 있습니다.
2017 년도부터 국내에 지속적으로 랜섬웨어를 유포하고 있는 비너스락커 조직은 최근에도 이력서, 저작권 위반 등의 내용을 통하여 국내에 꾸준히 랜섬웨어를 유포 중에 있습니다. 최근에는 꾸준히 Makop 랜섬웨어를 유포하다 처음으로 LockBit 랜섬웨어를 유포한 정황도 확인되었습니다.

타이포스쿼팅 방식을 이용한 매그니베르 랜섬웨어의 유포 정황도 다시 확인되었습니다. 매그니베르 랜섬웨어는 크롬 및 엣지 브라우저 사용자를 대상으로 사용자의 도메인 주소 오입력 혹은 철자가 틀리는 경우를 악용한 타이포스쿼팅 방식을 이용하여 유포 중이며, 사용자가 잘못된 도메인 주소를 입력하면 다른 페이지로 리디렉션 시켜 최종적으로 msi 파일을 내려줍니다. 만일 사용자가 해당 파일을 실행할 경우, 최종적으로 매그니베르 랜섬웨어에 감염됩니다.

글로벌 기업들의 랜섬웨어 피해도 지속되고 있습니다. 명품 의류 브랜드인 몽클레르는 21 년 12 월 AlphV/BlackCat 랜섬웨어의 공격을 받아 데이터가 유출되었으며, 21 년 1 월 중순 Tor 네트워크 내 유출된 데이터가 공개되었습니다. 항공 서비스 회사인 Swissport International 이 랜섬웨어의 공격을 받아 일부 항공편이 지연되었으며, Nvidia 역시 랜섬웨어의 공격을 받아 일부 시스템이 영향을 받은 것으로 확인되었습니다.

02 전문가 기고

이 밖에 ESRC 에서 선정한 2022 년 1 분기 새로 발견되었거나 주목할만한 랜섬웨어는 다음과 같습니다.

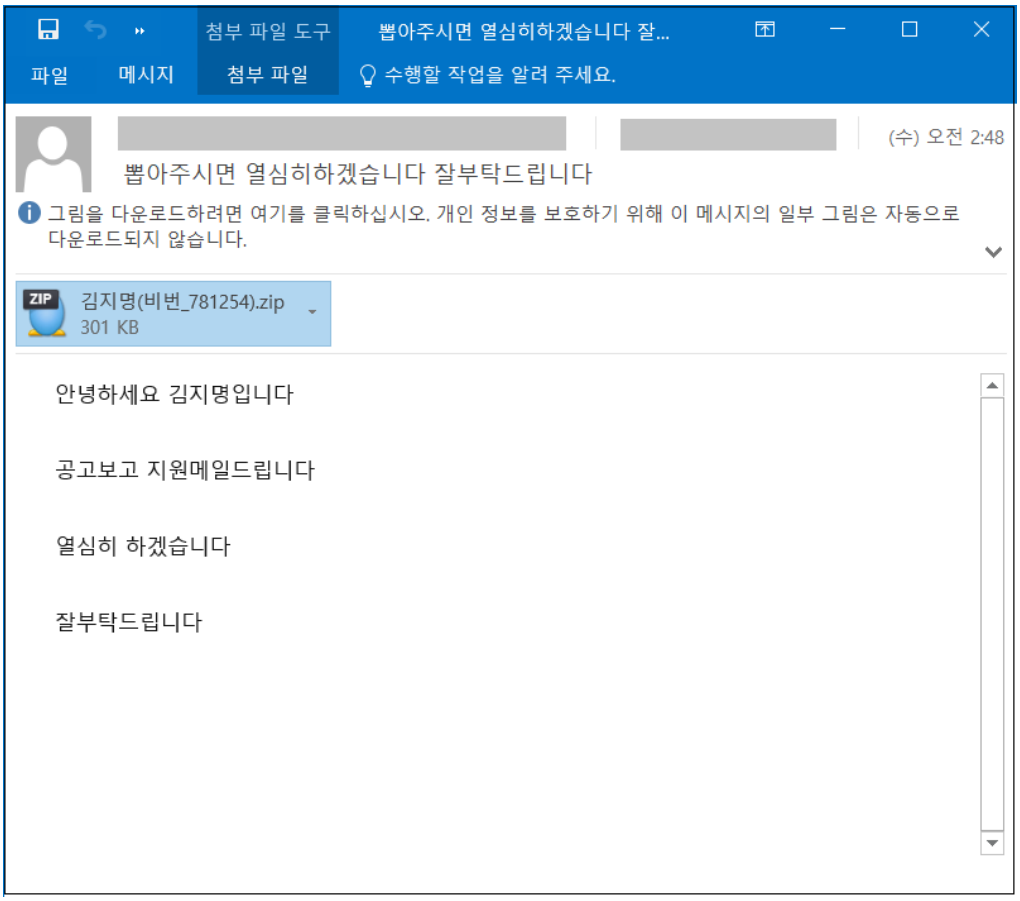
랜섬웨어 명	주요 내용
AvosLocker	2021 년 여름 처음 등장한 랜섬웨어. 보안 솔루션을 우회하기 위하여 안전모드로 재부팅 하여 암호화를 진행. 최근에는 VMware ESXi 가상 머신을 노린 리눅스 버전이 추가됨.
Night Sky	2021 년 말 등장한 랜섬웨어로 파일을 암호화 한 후 '.nightsky' 확장자를 추가하여 Night Sky 라 명명됨. 중국 공격자인 DEV-0401 조직의 새로운 캠페인으로, Log4shell 취약점을 악용하여 VMware Horizon 시스템에 Night Sky 랜섬웨어 유포함.
Sugar	2021 년 11 월 처음 등장한 악성코드로, 다른 랜섬웨어 패밀리 코드를 차용한 Delphi 랜섬웨어. 다른 랜섬웨어들과 달리 기업 전체보다는 개별 컴퓨터를 공격하는데 중점을 둠. REvil 랜섬웨어와 몇가지 유사점이 발견되었으며, 패스워드 복호화 페이지는 Clop 의 운영자가 사용하는것과 유사. 이에 랜섬웨어 개발자가 동일하거나, 주요 공격자가 계열사에 제공하는 서비스 중의 일부로 추정됨.
Putinwillburninhell	공격 대상은 러시아이며, 다른 랜섬웨어들과 다르게 랜섬머니를 요구하지 않고 대신 전쟁을 멈추라는 메시지를 띄움.
DeadBolt	1 월 처음 등장한 랜섬웨어로, 취약한 QNAP NAS 장치를 대상으로 공격을 진행하였으며, Asustor NAS 에 대해서도 공격 진행. Emsisoft 에서 복호화 툴 개발 및 공개.
Cuba	2019 년 말 등장하였으며 COLDDRAW 랜섬웨어라고도 불림. 20 년 21 년에 활발히 활동함. 최근에는 MS Exchange 취약점을 악용하여 기업 네트워크에 대한 초기 액세스 권한을 얻어 암호화 진행.
SunCrypt	2019 년 10 월 처음 등장하였으며 파일 암호화, 탈취한 데이터 공개 협박, 랜섬머니를 지불하지 않은 사용자를 대상으로 DDoS 공격을 진행하는 랜섬웨어. 2022 년 변종에는 프로세스 종료, 서비스 중지, 랜섬웨어 실행을 위한 시스템 정리 등의 기능이 추가됨. 아직 초기 개발 단계에 있는 것으로 추정됨.

2. 비너스락커 조직, 또 다시 Makop 랜섬웨어 유포중

13 일부터 이력서, 저작권 침해를 위장한 피싱 메일이 다수 유포되고 있어 사용자들의 주의가 필요합니다.

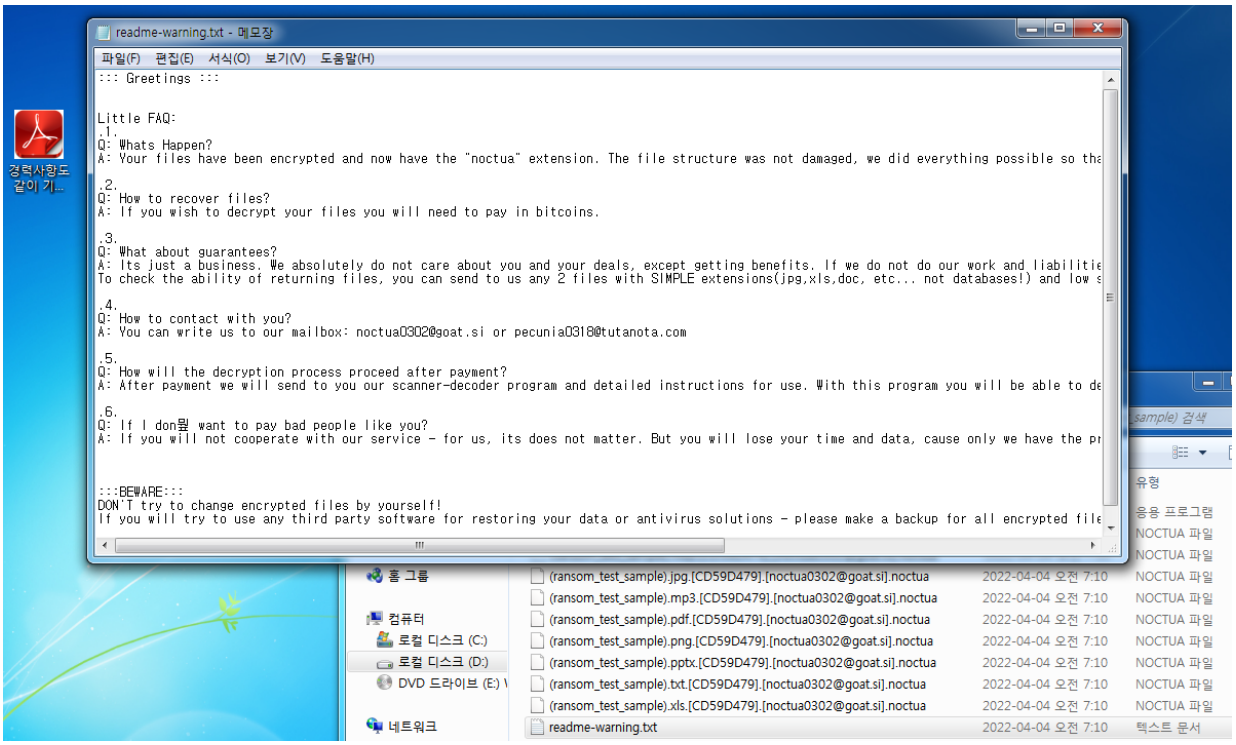
비너스락커 조직은 2017 년 부터 지속적으로 국내에 랜섬웨어를 유포중인 조직으로, 유포하는 랜섬웨어의 종류는 꾸준히 변화하고 있지만, 이력서, 저작권 위반 등의 내용을 위장한 피싱 메일을 통해 유포하는 방식은 동일합니다.

지금 대량으로 유포중인 피싱 메일 역시 이력서, 저작권 침해 내용을 위장하고 있으며, 피싱 메일 내부에는 악성 파일이 첨부되어 있습니다.



[그림 1] 이력서를 위장하여 유포중인 피싱 메일

첨부되어 있는 압축파일 내에는 한글, PDF 등의 파일을 위장한 랜섬웨어가 포함되어 있으며, 만일 사용자가 해당 파일을 정상파일로 오인하여 실행 시 랜섬웨어에 감염되게 됩니다.



[그림 2] 첨부파일 실행 후 랜섬웨어에 감염된 화면

현재 유포되고 있는 랜섬웨어는 Makop 랜섬웨어로, 실행 후에는 사용자 파일 암호화 후 확장자명을 .noctua 로 변경하며 랜섬머니를 요구합니다.

2017 년부터 지금까지 해당 조직은 이력서, 저작권 침해 관련 등 동일한 주제와 방식을 이용하여 랜섬웨어를 유포중이나, 그래도 여전히 많은 사용자들이 피해를 입고 있는 상황입니다.

사용자 여러분들께서는 낯선 사람에게서 수신한 이메일에 포함되어 있는 첨부파일의 실행을 지양해 주시기 바라며, 파일 탐색기 내 파일 확장명 표시 기능을 활성화 하여 파일 실행 전 확장자를 확인하시는 습관을 길러야 겠습니다.

[그림 3] 파일 확장명 활성화

현재 알약에서는 해당 랜섬웨어에 대하여 Trojan.Ransom.Makop 로 탐지중에 있습니다.

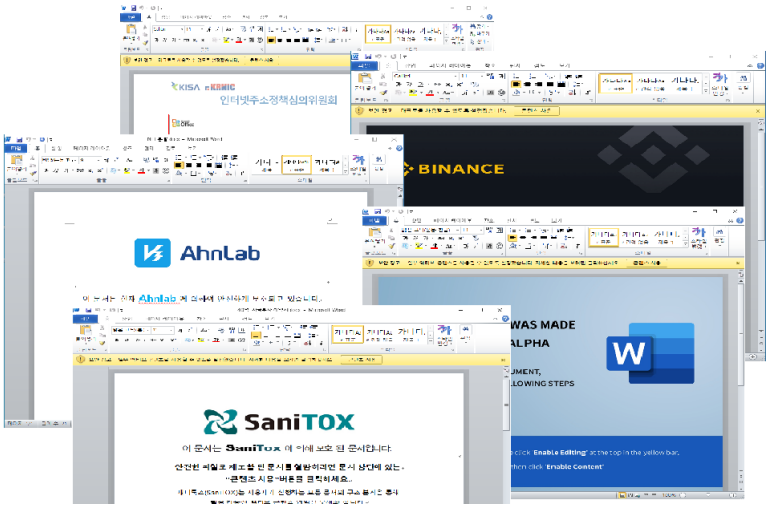
03
악성코드 분석 보고

[ACMS]
악성코드 분석 보고서

2022 년 3 월경부터 특정 기업을 사칭한 악성 피싱메일이 다량으로 유포중에 있으며 이 분석문서를 작성하는 현재까지도 변종들이 계속해서 발견되고 있다.

해당 악성코드는 주로 MS 워드 문서로 위장하고 있으며 사용자가 내용을 확인하기 위하여 "콘텐츠 사용" 을 선택하면 VBA 매크로가 실행되어 서버에서 암호화된 페이로드를 다운로드 받아서 악성코드를 실행한다.

악성행위의 확인을 어렵게 하기 위하여 최종 페이로드는 여러 단계의 확인을 거쳐서 실행된다.



[그림] 유사 피싱 메일들

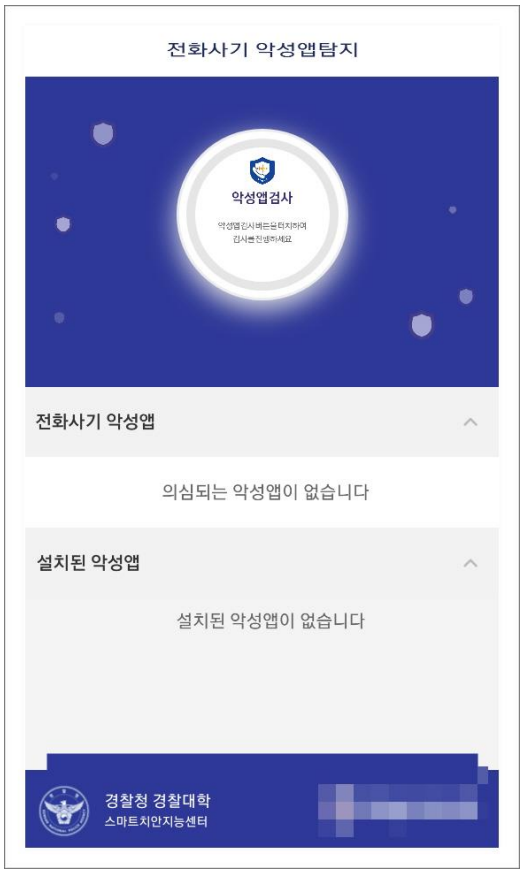
해당 악성코드는 doc 의 매크로를 이용하여 악성 파일을 다운로드 한 후 시스템 정보 전송 및 명령 제어 기능과 추가 페이로드를 다운로드 한다. 사용자의 백신 타입을 확인하여 전송하고 윈도우 빌더넘버가 7600(윈도우 7) 보다 작으면 프로그램을 종료하는 특징이 있다.

최근 국내에서 불특정 다수를 대상으로 다양한 파일명의 악성 파일들이 발견되고 있기때문에 사용자들의 주의가 필요하다.

따라서 이러한 악성코드에 감염이 되지 않도록 출처가 불분명한 이메일의 링크 혹은 첨부 파일에 대해 실행을 삼가야 하며, 백신을 항상 최신 버전으로 유지할 수 있도록 해야 한다.

[Trojan.Android.Dropper.Agent] 악성코드 분석 보고서

코로나 관련 대출 문자, 쇼핑몰 결제 문자, 택배 관련 문자 등등 온갖 스미싱으로부터 스마트폰을 보호하기 위해 보안 프로그램들을 사용하곤 한다. 하지만 이를 악용하여 보안 프로그램들로 위장한 악성 앱도 등장하고 있다. 예전에 한 번 살펴본 폴 안티스파이부터 피싱 아이즈, 내 정보 지키미까지 여러 가지 버전이 존재한다. 최근 공격 조직은 보이스피싱을 예방할 수 있는 앱인 시티즌 코난을 사칭하여 배포하고 있다.



[그림] 앱 메인 화면

스미싱 문자들이 점점 발전하면서 보안 프로그램도 강조되고 있다. 하지만 스미싱 공격 조직들은 이마저도 위장하여 사용자들을 속이고 있으며 점점 정교해진 형태로 발전되고 있다. 따라서 사용자는 공식 사이트를 이용하도록 하고 앱을 설치하는 순간 권한 확인 및 주의가 필요하다.

현재 알약 M 에서는 해당 앱을 'Trojan.Android.Dropper.Agent' 탐지 명으로 진단하고 있다.

04
글로벌 보안 동향

Log4J 를 악용하고 DNS 터널링으로 통신하는 새로운 리눅스 봇넷 발견

New Linux botnet exploits Log4J, uses DNS tunneling for comms

최근 Linux 시스템을 노려 민감 정보를 훔치고, 루트킷을 설치하고, 리버스 셸을 생성하고, 웹 트래픽 프록시 역할을 하는 봇넷에 사용자의 시스템을 추가하려 시도하는 활발히 개발 중인 봇넷이 발견되었습니다.

Qihoo 360 의 360 Netlab 의 연구원들이 새로이 발견한 악성코드인 B1txor20 은 Linux ARM, X64 CPU 아키텍처 기기를 공격하는데 중점을 두고 있습니다.

해당 봇넷은 Log4j 취약점을 노린 익스플로잇을 통해 새로운 호스트를 감염시킵니다. 공급 업체 수십 곳이 취약한 Apache Log4j 로깅 라이브러리를 사용하는 것으로 미루어 볼 때, 이는 매우 매력적인 공격 벡터입니다.

연구원들은 2 월 9 일 첫 번째 샘플이 허니팟 시스템 중 하나에서 발견되어 B1txor20 봇넷을 처음으로 발견했습니다.

이들은 백도어, SOCKS5 프록시, 악성코드 다운로드, 데이터 도용, 임의 명령 실행, 루트킷 설치 기능을 포함한 악성코드 샘플 총 4 개를 발견했습니다.

DNS 터널링으로 C2 통신 트래픽 숨겨

하지만 B1txor20 악성코드가 더욱 눈에 띄는 이유는 명령 및 제어 서버와의 통신 채널에 DNS 터널링을 사용한다는 점입니다. 이는 공격자가 DNS 프로토콜을 악용하여 DNS 쿼리를 통해 악성코드와 데이터를 터널링하는데 사용하는 기술로, 오래되었지만 여전히 안정적입니다.

연구원들은 아래와 같이 설명했습니다.

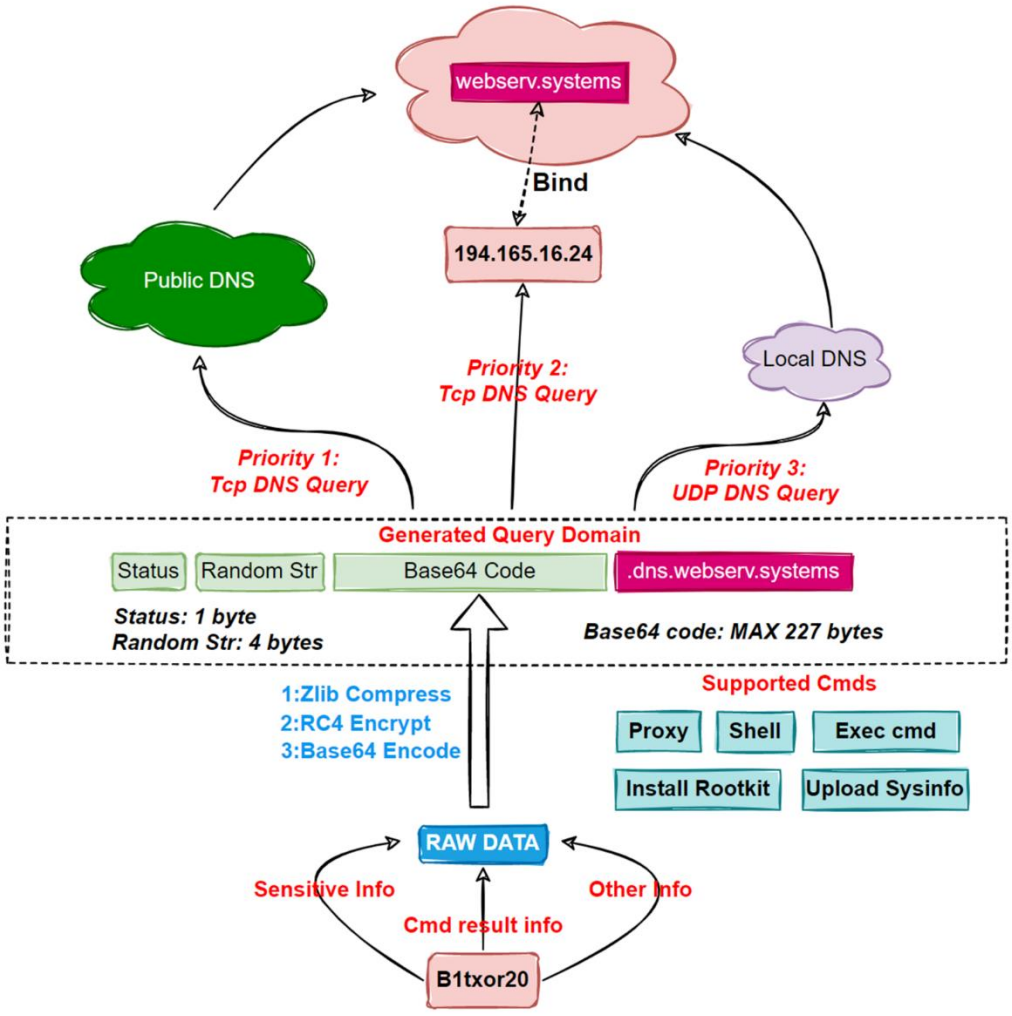
"봇은 훔친 특정 인코딩 기술을 통해 민감 정보, 명령 실행 결과, 전달해야 할 기타 정보를 숨긴 후 DNS 요청을 통해 C2 에 전송합니다."

"요청을 받은 후, C2 는 DNS 요청에 대한 응답으로 봇 측에 페이로드를 전송합니다. 이러한 방식으로 봇과 C2 는 DNS 프로토콜의 도움을 받아 통신합니다."

또한 연구원들은 악성코드의 개발자가 더욱 많은 기능을 개발했지만, 모든 기능이 활성화된 상태는 아니라 밝혔습니다.

이로써 비활성화된 기능에는 여전히 버그가 존재하고, 제작자는 향후 이를 사용하기 위해 여전히 기능을 개선하고 있다고 추측해볼 수 있습니다.

해당 악성코드에 대한 추가 정보는 360 Netlab 보고서에서 확인하실 수 있습니다.



[그림] B1txor20 의 DNS 터널링 통신
[이미지 출처] https://blog.netlab.360.com/b1txor20-use-of-dns-tunneling_en/

봇넷, 지속적으로 Log4J 악용해

Log4Shell 익스플로잇이 공개된 이후 여러 공격자가 공격에 이를 사용했습니다. 중국, 이란, 북한, 터키 정부와 연결된 정부의 지원을 받는 해킹 그룹 및 랜섬웨어 그룹이 사용하는 갱이 사용하는 액세스 브로커가 여기에 포함됩니다.

지난 12 월에는 한 공격자가 취약한 Linux 장치를 Mirai, Muhstik Linux 악성코드에 감염시키기 위해 Log4J 보안 취약점을 악용하는 것이 발견되었습니다.

이러한 봇넷은 IoT 장치 및 서버를 "고용"하여 크립토마이너를 배포하고 대규모 DDoS 공격을 실행합니다.

[출처]

https://www.bleepingcomputer.com/news/security/new-linux-botnet-exploits-log4j-uses-dns-tunneling-for-comms/

https://blog.netlab.360.com/b1txor20-use-of-dns-tunneling_en/ (IOC)

Mars Stealer 악성코드, 구글의 OpenOffice 광고 통해 푸시돼

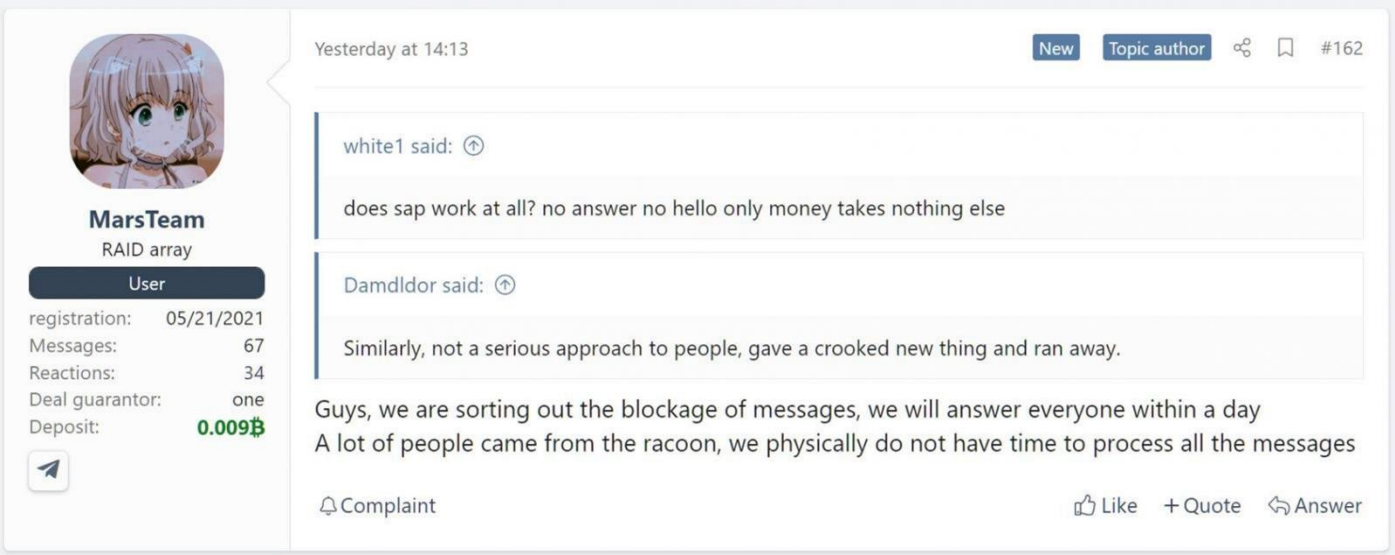
Mars Stealer malware pushed via OpenOffice ads on Google

새로이 출시된 인포 스틸러인 Mars Stealer 의 인기가 증가하고 있는 것으로 나타났습니다. 전문가들은 해당 악성코드를 사용한 대규모 캠페인을 처음으로 발견했다고 밝혔습니다.

Mars Stealer 는 2020 년 개발을 중단한 Oski 악성코드를 재설계한 것이며, 다양한 앱을 노리는 광범위한 정보 탈취 기능을 탑재했습니다.

Mars Stealer 는 해킹 포럼에서 다소 저렴한 가격인 $140 ~ $160 에 판매한다고 홍보되었으며, Raccoon Stealer 가 갑작스럽게 중단되어 사이버 범죄자들이 대안을 찾아야 할 때까지 천천히 성장해왔습니다.

Mars Stealer 의 서비스는 Raccoon 과 유사하게 운영되고 있기 때문에, 수 많은 신규 사용자가 유입되어 앞으로 발생할 신규 캠페인 다수의 발판이 될 예정입니다.

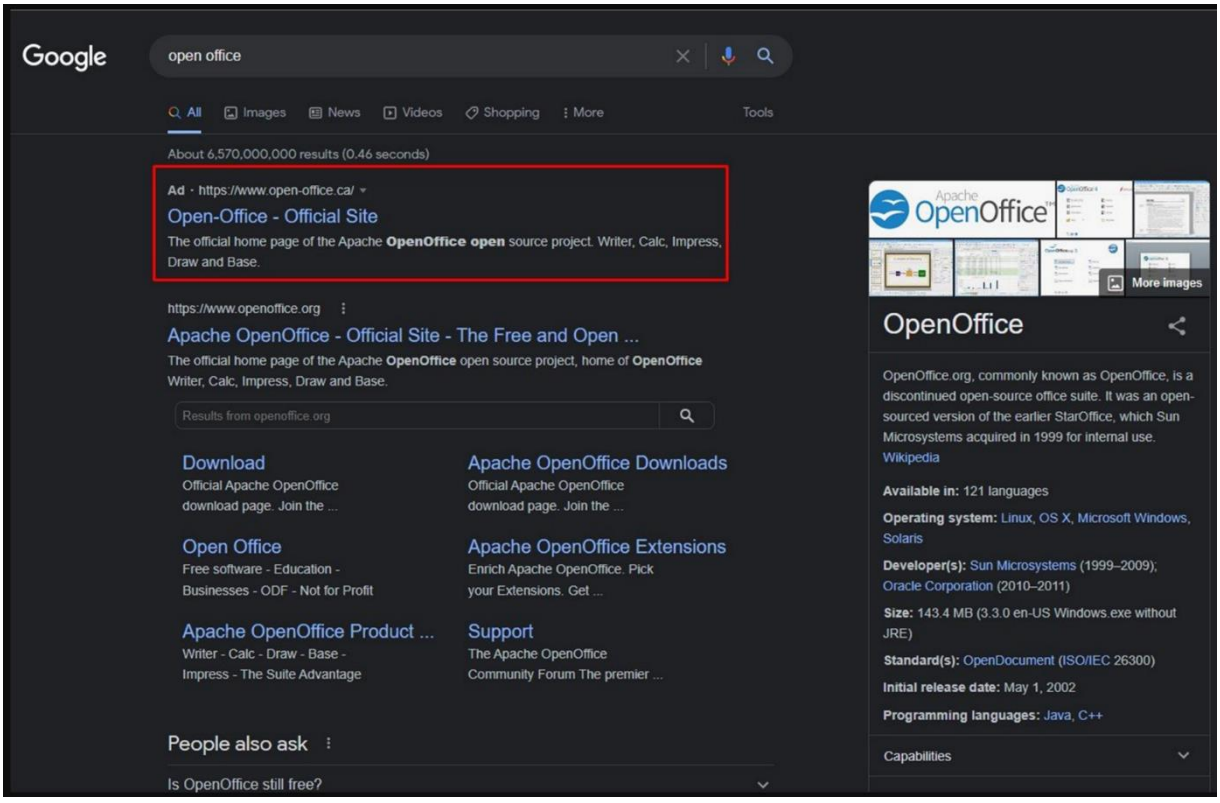


[그림] 수 많은 새로운 요청을 받고 있는 Mars Stealer 의 개발자
[이미지 출처] https://blog.morphisec.com/threat-research-mars-stealer

Morphisec 의 위협 분석가는 이 새로운 캠페인 다수를 발견했으며, 그 중 하나는 사용 방법을 포함한 해당 악성코드의 크랙 버전을 사용했다고 밝혔습니다.

OpenOffice 캠페인

Morphisec 이 발견한 새로운 Mars Stealer 캠페인은 Google Ads 광고를 통해 캐나다 검색 결과에서 복제된 OpenOffice 사이트를 검색 순위권에 띄웠습니다.

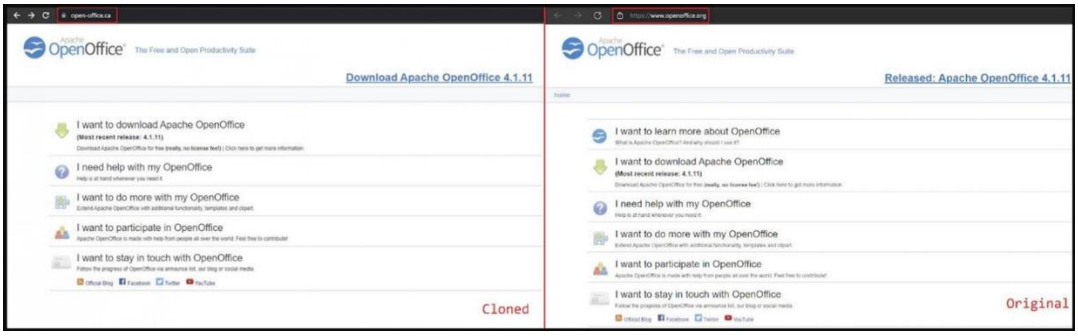


[그림] 악성 광고로 오염된 Google 검색 결과
[이미지 출처] https://blog.morphisec.com/threat-research-mars-stealer

OpenOffice 는 한때 인기 있었던 오픈 소스 오피스 제품군으로 현재는 Apache 재단에서 관리합니다. 하지만 지금은 2010 년 포크백으로 시작된 LibreOffice 에 추월 당했습니다.

그러나 OpenOffice 는 여전히 무료 문서 및 스프레드시트 편집기를 찾는 사용자들 덕분에 상당한 일일 다운로드 수를 기록하고 있습니다.

공격자들이 훨씬 더 인기 있는 LibreOffice 를 복제하지 않은 이유는 수 많은 제보로 악성 광고가 신속하게 제거될 것을 우려한 것으로 보입니다.

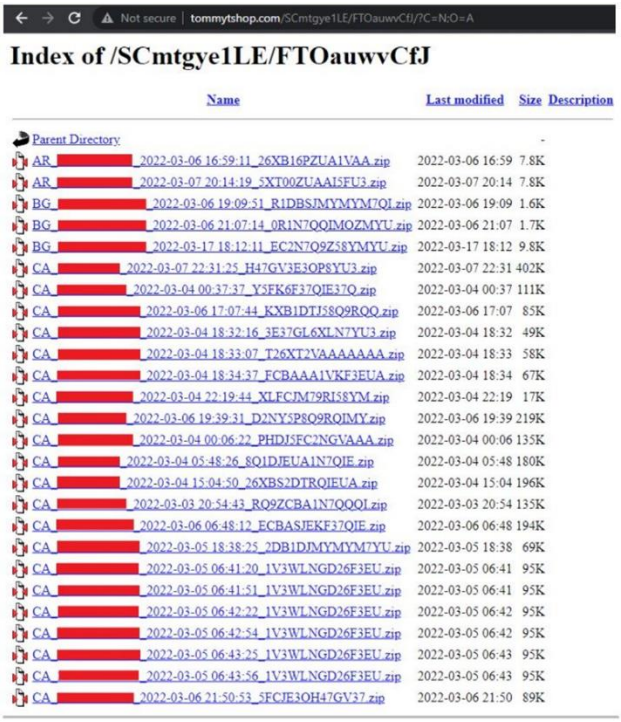


[그림] 악성 사이트와 실제 사이트
[이미지 출처] https://blog.morphisec.com/threat-research-mars-stealer

가짜 사이트의 OpenOffice 설치 프로그램은 실제로는 Babadeda 크립터나 Autoit 로더가 포함된 Mars Stealer 실행 파일이었습니다. 따라서 피해자는 자신도 모르는 사이에 감염될 수 있었습니다.

하지만 크랙 버전에 함께 포함된 구성 방법 오류 때문에, 운영자는 피해자의 '로그' 디렉토리를 노출시켜 모든 방문자에게 전체 액세스 권한을 부여했습니다.

로그는 인포 스틸링 트로이 목마가 훔쳐 공격자의 명령 및 제어 서버에 업로드된 데이터를 포함하는 zip 파일입니다.



[그림] 훔친 데이터(로그)를 저장하는 디렉토리
[이미지 출처] https://blog.morphisec.com/threat-research-mars-stealer

Mars Stealer 가 해당 캠페인에서 훔친 정보는 브라우저 자동 양식 채움 데이터, 브라우저 확장 데이터, 신용 카드, IP 주소, 국가 코드, 시간대가 포함된 것으로 보입니다.

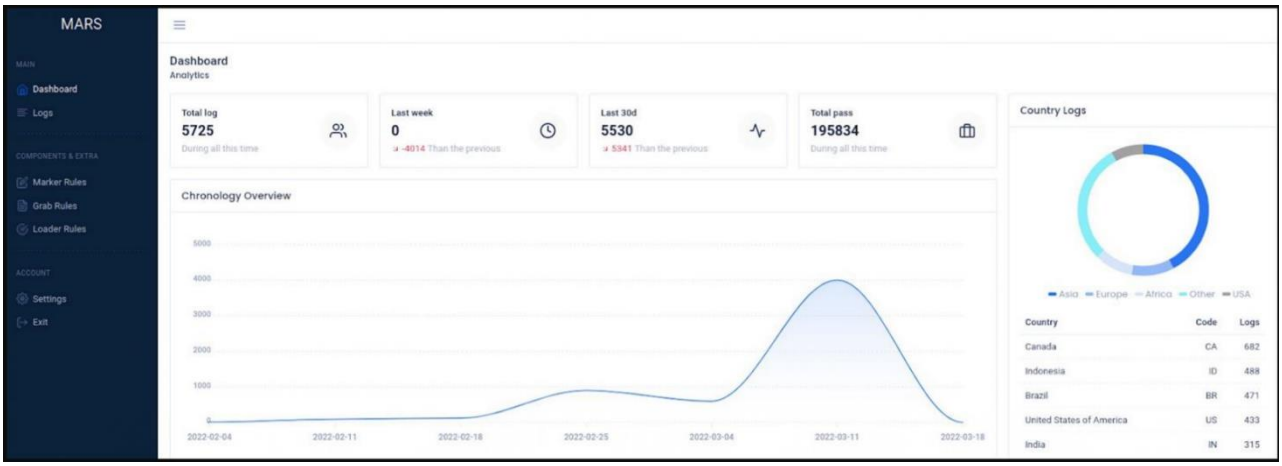
공격자는 디버깅 중 자신의 Mars Stealer 복사본에 감염되었기 때문에, 그들의 민감한 정보 또한 노출되었습니다.

이러한 실수로 인해 연구원들은 해당 공격이 러시아어를 구사하는 사용자의 소행으로 추정했으며 공격자의 GitLab 계정, Google Ads 비용을 지불하는 데 사용된 훔친 크리덴셜 등을 발견할 수 있었습니다.

암호화 자산에 대한 위협

Mars Stealer는 47개 이상의 다크넷 사이트와 해킹 포럼, 텔레그램 채널, 크랙 팩과 같은 "비공식" 배포 경로에서 홍보되고 있는 현재 증가 중인 위협입니다.

Morphisec 은 해당 인포 스틸러의 운영자가 가상 화폐 자산을 집중적으로 노리고 있다고 밝혔습니다.



[그림] 단일 캠페인 운영자의 훔친 로그 요약
[이미지 출처] https://blog.morphisec.com/threat-research-mars-stealer

분석된 캠페인에서 가장 많이 도난당한 브라우저 플러그인은 MetaMask 이며 Coinbase Wallet, Binance Wallet, Math Wallet 이 그 뒤를 이었습니다. 이들은 모두 암호화폐 자산 관리를 위한 "핫" 월렛입니다.

연구원들은 캐나다의 의료 인프라 제공업체의 크리덴셜 또한 발견했으며, 일부 유명 캐나다 서비스 회사에서 해킹의 징후를 발견했습니다.

인포 스틸러를 피하려면 Google Ad 결과가 아닌 공식 사이트를 클릭하고, 실행하기 전 안티바이러스 프로그램을 통해 다운로드한 실행 파일을 항상 스캔해야 합니다.

새로운 Mars Stealer 맬웨어에 대한 자세한 기술 정보는 3xp0rt 의 분석에서 확인하실 수 있습니다.

[출처]

https://www.bleepingcomputer.com/news/security/mars-stealer-malware-pushed-via-openoffice-ads-on-google/

https://blog.morphisec.com/threat-research-mars-stealer (IOC)

https://3xp0rt.com/posts/mars-stealer (IOC)

안드로이드 악성코드인 Escobar, 구글 인증기 MFA 코드 훔쳐

Android malware Escobar steals your Google Authenticator MFA codes

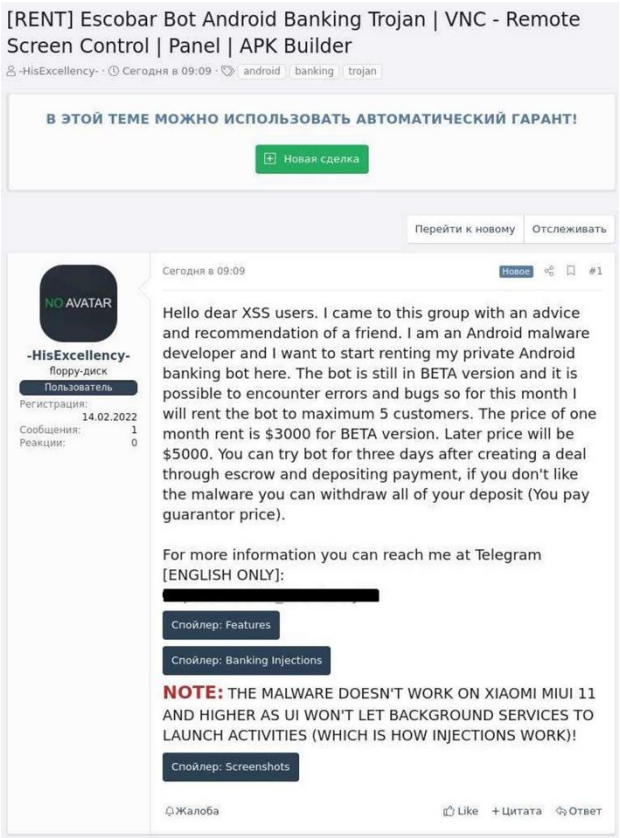
안드로이드 뱅킹 트로이 목마인 Aberebot 이 Google 인증기의 다단계 인증 코드를 훔치는 등 새로운 기능을 탑재한 후 'Escobar'라는 이름으로 다시 활동을 재개했습니다.

최신 Aberebot 버전은 VNC 를 통해 감염된 Android 장치를 제어하고, 오디오를 녹음하고, 사진을 촬용하고, 크레덴셜 탈취를 위해 타깃 앱 세트를 확장하는 등 새로운 기능을 포함하고 있습니다.

트로이 목마의 주된 목적은 공격자가 피해자의 은행 계좌를 탈취하고 사용 가능한 잔액을 인출하고 승인받지 않은 거래를 수행하는데 충분한 정보를 훔치는 것입니다.

Escobar 로 브랜드 변경해

BleepingComputer는 KELA의 사이버 인텔리전스 DARKBEAST 플랫폼을 통해 지난 2022년 2월 러시아어를 사용하는 해킹 포럼에서 Aberebot 개발자가 새 버전을 홍보한 포럼 게시물인 'Escobar Bot Android Banking Trojan'을 발견했습니다.



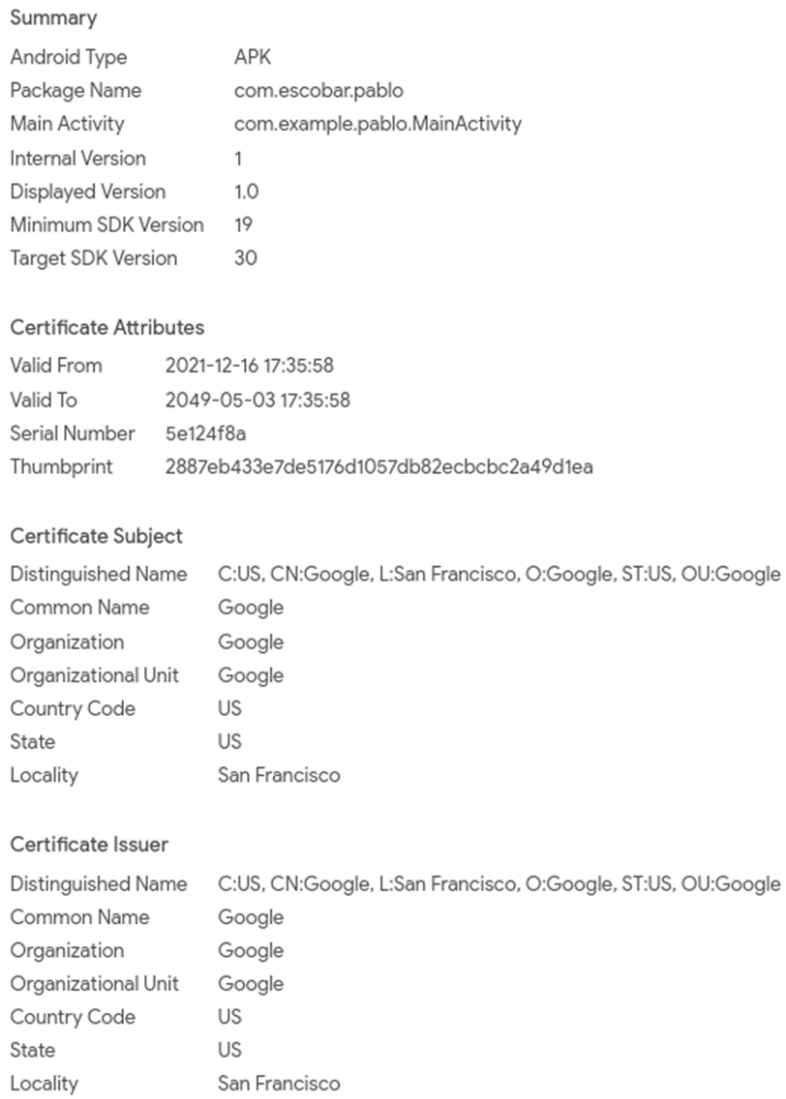
[그림] 다크넷 포럼 내 판매자 게시물

[이미지 출처] https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/

악성코드 제작자는 고객 최대 5명에게 월 3천달러에 악성코드 베타 버전 제공하고 있으며, 공격자는 3일 간 봇을 무료로 테스트 가능합니다.

공격자는 개발이 완료된 후에는 해당 악성코드의 가격을 5천달러로 인상할 계획이라 밝혔습니다.

MalwareHunterTeam 은 2022 년 3 월 3 일 처음으로 McAfee 앱으로 가장한 의심스러운 APK 를 발견하고, 해당 앱이 안티바이러스 엔진 대다수를 회피했다고 경고했습니다.



Summary

Android Type	APK
Package Name	com.escobar.pablo
Main Activity	com.example.pablo.MainActivity
Internal Version	1
Displayed Version	1.0
Minimum SDK Version	19
Target SDK Version	30

Certificate Attributes

Valid From	2021-12-16 17:35:58
Valid To	2049-05-03 17:35:58
Serial Number	5e124f8a
Thumbprint	2887eb433e7de5176d1057db82ecbcbc2a49d1ea

Certificate Subject

Distinguished Name	C:US, CN:Google, L:San Francisco, O:Google, ST:US, OU:Google
Common Name	Google
Organization	Google
Organizational Unit	Google
Country Code	US
State	US
Locality	San Francisco

Certificate Issuer

Distinguished Name	C:US, CN:Google, L:San Francisco, O:Google, ST:US, OU:Google
Common Name	Google
Organization	Google
Organizational Unit	Google
Country Code	US
State	US
Locality	San Francisco

[이미지 출처] https://twitter.com/malwrhunterteam/status/1499390775775293454

이는 Aberebot 트로이 목마의 새로운 'Escobar' 변종에 대한 분석을 진행한 Cyble 의 연구원이 발견했습니다.

해당 분석가에 따르면 Aberebot 은 2021 년 여름 처음 실제 공격에 사용되었으며 새로운 버전이 등장한 것은 해당 악성코드가 활발히 개발되고 있다는 것을 의미합니다.

기존 기능 및 새로운 기능

대부분의 뱅킹 트로이 목마와 마찬가지로, Escobar는 전자 뱅킹 앱과 웹 사이트와의 사용자 상호 작용에 인터셉트해 피해자의 크리덴셜을 훔칠 목적으로 오버레이 로그인 양식을 표시합니다.

이 악성코드는 오버레이 삽입이 차단되더라도, 모든 안드로이드 버전에 적용되는 여러 강력한 기능을 포함합니다.

제작자는 최신 버전에서 타깃 은행 및 금융 기관을 18 개국의 190 개 기업으로 확장했습니다.

해당 악성코드는 25 개의 권한을 요청하며, 이 중 15 개는 악의적인 목적으로 사용됩니다. 접근성, 오디오 녹음, SMS 읽기, 저장소 읽기/쓰기, 계정 목록 가져오기, 키 잠금 비활성화, 전화 걸기, 정확한 기기 위치 액세스 등과 같은 권한이 여기에 포함됩니다.

SMS 통화 기록, 키 로그, 알림 및 Google 인증기 코드를 포함한 악성코드가 수집하는 모든 정보는 C2 서버에 업로드됩니다.

```
else if (this.f5010oo000o.contains("Get Google Authenticator Codes")) {
    Intent launchIntentForPackage = getPackageManager().getLaunchIntentForPackage("com.google.android.apps.authenticator2");
    f4990oo0000 = true;
    flags = launchIntentForPackage.setFlags(268435456);
```

[그림] Google OTP 코드를 추출하는 코드
[이미지 출처] https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/

이로써 공격자는 전자 뱅킹 계정을 해킹할 때 이중 인증을 우회할 수 있게 됩니다.

2FA 코드는 SMS를 통해 수신하거나 Google의 인증기와 같은 HMAC 소프트웨어 기반 툴에 저장 및 순환됩니다. 후자는 SIM 스왑 공격에 취약하지 않기 때문에 더욱 안전하지만, 사용자 공간에 침투하는 악성코드는 방어할 수 없습니다.

공격자가 원격 제어 기능이 있는 플랫폼 간 화면 공유 유틸리티인 VNC 뷰어를 사용할 경우, 기기가 사용 중이 아닐 때 원하는 모든 작업을 수행할 수 있는 새로운 강력한 무기를 얻을 수 있습니다.

```
} else if (this.f5O1Ooo0O0o.contains("Start VNC")) {
    AccessibilityService.OooOOo = true;
} else if (this.f5O1Ooo0O0o.contains("Enable Notfication Access")) {
    if (!getApplicationContext().getSharedPreferences("sharedPrefs", 0).getBoolean("notification", false)) {
        SharedPreferences.Editor edit = getApplicationContext().getSharedPreferences("sharedPrefs", 0).edit();
        edit.putBoolean("uninstallProtection", false);
        edit.apply();
        flags = new Intent("android.settings.ACTION_NOTIFICATION_LISTENER_SETTINGS").setFlags(268435456);
    }
} else if (this.f5O1Ooo0O0o.contains("Stop VNC")) {
    AccessibilityService.OooOOo = false;
} else {
    try {
        if (this.f5O1Ooo0O0o.contains("VNCClick")){
            String str11 = this.f5O1Ooo0O0o;
            float floatValue = Float.valueOf(str11.substring(str11.indexOf("[") + 1, this.f5O1Ooo0O0o.indexOf("]"))).floatValue();
            String str12 = this.f5O1Ooo0O0o;
            AccessibilityService.OooOOO = Float.valueOf(str12.substring(str12.indexOf("(") + 1, this.f5O1Ooo0O0o.indexOf(")"))).floatValue();
            AccessibilityService.OooOOO = floatValue;
            AccessibilityService.f4670OooOOO = "click";
            str = this.f5O1Ooo0O0o;
        } else if (this.f5O1Ooo0O0o.contains("VNCHold")){
            String str13 = this.f5O1Ooo0O0o;
            float floatValue2 = Float.valueOf(str13.substring(str13.indexOf("[") + 1, this.f5O1Ooo0O0o.indexOf("]"))).floatValue();
            String str14 = this.f5O1Ooo0O0o;
            AccessibilityService.OooOOO = Float.valueOf(str14.substring(str14.indexOf("(") + 1, this.f5O1Ooo0O0o.indexOf(")"))).floatValue();
            AccessibilityService.OooOOO = floatValue2;
            AccessibilityService.f4670OooOOO = "hold";
            str = this.f5O1Ooo0O0o;
        } else if (this.f5O1Ooo0O0o.contains("VNCDrag")) {
```

[그림] Aberebot 의 VNC 뷰어 코드
[이미지 출처] https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/

이외에도 Aberebot 은 오디오 클립을 녹음하거나 스크린샷을 찍고, 모두 공격자의 C2 로 추출할 수 있습니다. 지원되는 명령 목록 전체는 아래와 같습니다.

Command	Description
Take Photo	Capture images from the device's camera
Send SMS	Send SMS to a particular number
Send SMS to All Contacts	Send SMS to all the contact numbers saved in the device
Inject a web page	Inject a URL
Download File	Download media files from the victim device
Kill Bot	Delete itself
Uninstall an app	Uninstall an application
Record Audio	Record device audio
Get Google Authenticator Codes	Steal Google Authenticator codes
Start VNC	Control device screen

[그림] Aberebot 명령 표
[이미지 출처] https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/

새로운 Escobar 악성코드는 사이버 범죄 커뮤니티에서 상대적으로 높은 가격으로 판매되고 있기 때문에 얼마나 인기 있을지는 아직까지 알 수 없습니다. 하지만 이는 수 많은 사람을 매료시킬 만큼 강력합니다.

[출처]

https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/

https://twitter.com/malwrhunterteam/status/1499390775775293454 (IOC)

https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/ (IOC)

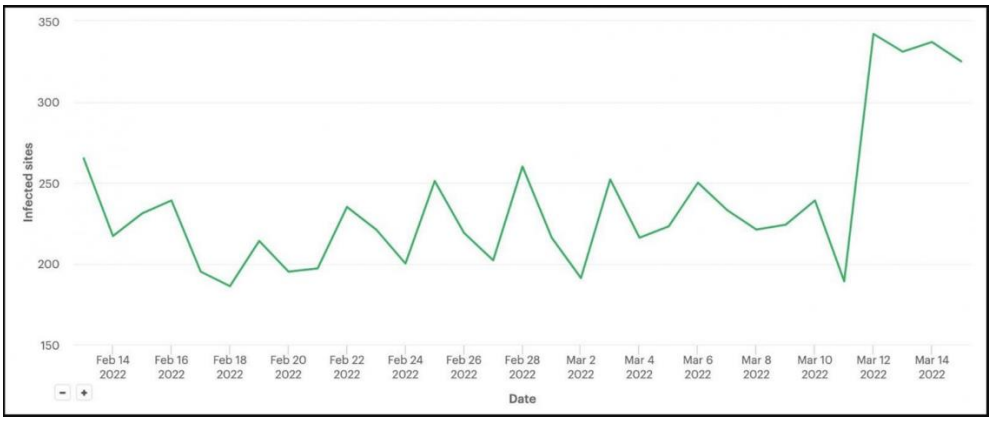
GoDaddy 호스팅 사이트 수백 곳, 단 하루 만에 백도어에 감염돼

Hundreds of GoDaddy-hosted sites backdoored in a single day

인터넷 보안 분석가들이 GoDaddy 의 Managed WordPress 서비스를 통해 호스팅되는 WordPress 웹사이트에서 백도어 감염이 급증하는 것을 발견했습니다. 해당 백도어는 모두 동일한 페이로드를 사용했습니다.

이로 인해 MediaTemple, tsoHost, 123Reg, Domain Factory, Heart Internet, Host Europe Managed WordPress 와 같은 인터넷 서비스 리셀러의 운영에 영향을 미쳤습니다.

이 사고는 2022 년 3 월 11 일 Wordfence 팀이 발견했습니다. 해당 공격이 처음 발견된 후 24 시간 이내에 웹사이트 298 곳이 백도어에 감염되었으며, 이 중 281 곳이 GoDaddy 에서 호스팅되고 있었던 것으로 나타났습니다.



[그림] 백도어 감염 수

[이미지 출처] https://www.wordfence.com/blog/2022/03/increase-in-malware-sightings-on-godaddy-managed-hosting

오래된 템플릿 스패머

이 모든 사이트를 감염시킨 백도어는 검색 결과에 악성 페이지를 삽입하는 데 사용되는 스팸 링크 템플릿을 C2 서버에서 가져오기 위해 wp-config.php 에 심어진 2015 구글 검색 SEO 포이즈닝 툴이었습니다.

해당 캠페인은 해킹된 웹사이트의 방문자에게 실제 콘텐츠 대신 제약 관련 스팸 템플릿을 표시했습니다.

이러한 템플릿의 목표는 피해자가 가짜 제품을 구매하도록 유도해 공격자가 돈과 지불 세부 정보를 얻는 것입니다.

또한 공격자는 위반 사항을 포함하도록 웹사이트의 내용을 변경해 사이트의 평판을 무너뜨릴 수 있지만, 현재 공격자의 목적은 아닌 것으로 보입니다.

또한 이러한 공격 유형은 브라우저가 아닌 서버에서 실행되기 때문에, 사용자가 탐지 및 차단하기가 더욱 어렵습니다. 따라서 로컬 인터넷 보안 툴은 해당 사이트에 대해 의심스러운 점을 찾아낼 수 없었습니다.

공급망 공격으로 의심돼

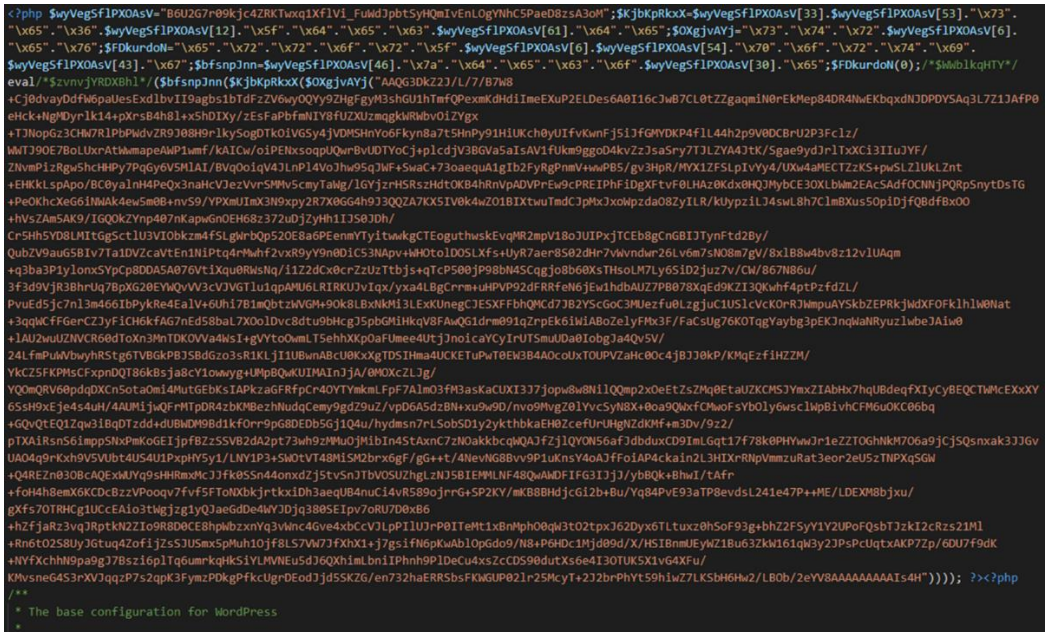
이 사고의 침입 벡터는 아직까지 밝혀지지 않았지만, 연구원들은 이를 공급망 공격으로 의심했습니다.

Bleeping Computer 에서는 이와 관련하여 자세히 알아보고자 GoDaddy 에 연락을 취했지만 아직까지 답변을 받지 못했다고 밝혔습니다.

GoDaddy 는 지난 2021 년 11 월 120 만 고객 및 Managed WordPress 서비스 리셀러에 영향을 미친 데이터 유출 사고에 대해 공개했습니다.

해당 사고에서 회사의 Managed WordPress 사이트를 프로비저닝하는 시스템에 무단 액세스 또한 발생했습니다. 따라서 두 사건이 관련이 있을 것이라 추측해 볼 수도 있습니다.

현재 웹사이트가 GoDaddy 의 Managed WordPress 플랫폼에서 호스팅되고 있을 경우, wp-config.php 파일을 스캔해 백도어가 설치되었는지 여부를 확인하시기 바랍니다.



[그림] 인코딩된 주입된 백도어

[이미지 출처] https://www.wordfence.com/blog/2022/03/increase-in-malware-sightings-on-godaddy-managed-hosting/

또한 Wordfence 는 관리자에게 물론 백도어를 제거하는 것이 먼저지만, 스팸 검색 엔진 결과를 제거하는 것도 우선되어야 한다고 당부했습니다.

[출처]

https://www.bleepingcomputer.com/news/security/hundreds-of-godaddy-hosted-sites-backdoored-in-a-single-day/

https://www.wordfence.com/blog/2022/03/increase-in-malware-sightings-on-godaddy-managed-hosting/

(주)이스트시큐리티

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