이스트시큐리티

보안 동향 보고서

No.150 2022.03

No.150 2022.03

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 06-10

한국도로공사 통행료 납부를 위장하여 유포중인 피싱 메일 주의!

병·의료원 건강검진 증명서 발급으로 위장한 北 연계 공격 등장

03 악성코드 분석 보고 11-13

04 글로벌 보안 동향 14-24

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2022 년 2 월에는 신규 악성코드 및 랜섬웨어의 발견부터 탈륨(Thallium) 그룹의 지속적인 APT 공격까지 다양한 보안 위협이 발견되었습니다.

코로나 19 백신 3 차 접종 이후 이상반응에 대한 모니터링을 사칭하여 악성 링크를 열람하도록 유인하거나, 디지털 자산 지갑 서비스 고객센터로 위장하여 사용자에게 접근했으며 국내 외교 안보 국방분야 교수 및 민간분야 전문가를 겨냥한 악성 메일 등이 다수 발견되었습니다. 이외에도 중앙 선거 관리 위원회, 보안기관 및 기업, 국내 유명 손해보험사를 위장한 피싱 메일들이 이번 달에 집중적으로 발견되었습니다.

또한 가상 자산 거래소의 금융자산을 노리며 지난달 국내에서 첫 사례를 발행시킨 “심 스와핑(SIM Swapping)”의 해킹 시도가 이후 지속적으로 증가하고 있으며, 세계 최대 NFT 거래소인 “오픈씨(OpenSea)”에서도 악성 페이로드를 통해 계약을 임의로 진행하여 약 2400 억 원의 NFT 를 훔친 사례도 확인되었습니다.

피싱 관련 피해를 예방하기 위해 사용자는 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.

또한 이번 달에는 러시아와 우크라이나의 관계가 악화되면서 두 국가 간의 사이버 공격이 전개되고 있습니다. 우크라이나의 국방부, 군대, 정보 사령부들 군 관련 사이트들과 주요 은행 관련 사이트들이 사이버 공격을 받아 다운되었으며, 러시아의 크렘린궁을 포함한 정부 주요 웹사이트를 해킹하거나 탈취하는 행위들이 지속적으로 진행되는 만큼 두 국가 간의 사이버 전쟁으로 인해 주변 국가들도 공격 대상에 포함될 수 있어 각별한 주의가 요구되고 있습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2022 년 2 월의 감염 악성코드 Top 15 리스트에서는 국내 광고 소프트웨어를 설치하는 Hosts.media.opencandy.com 악성코드가 810,614 건에서 609,977 건으로 약 24.7% 감소하였지만 여전히 지난달에 이어 1 위를 유지하였으며, 오토캐드 파일을 감염 시키는 Worm.ACAD.Bursted 악성코드도 다시 새롭게 진입하였다.

지난달과 마찬가지로 윈도우 불법 정품 인증 프로그램과 관련된 AutoKMS 악성코드가 Top 15 중 과반수를 차지할 만큼 많은 탐지율을 보여주고 있다.

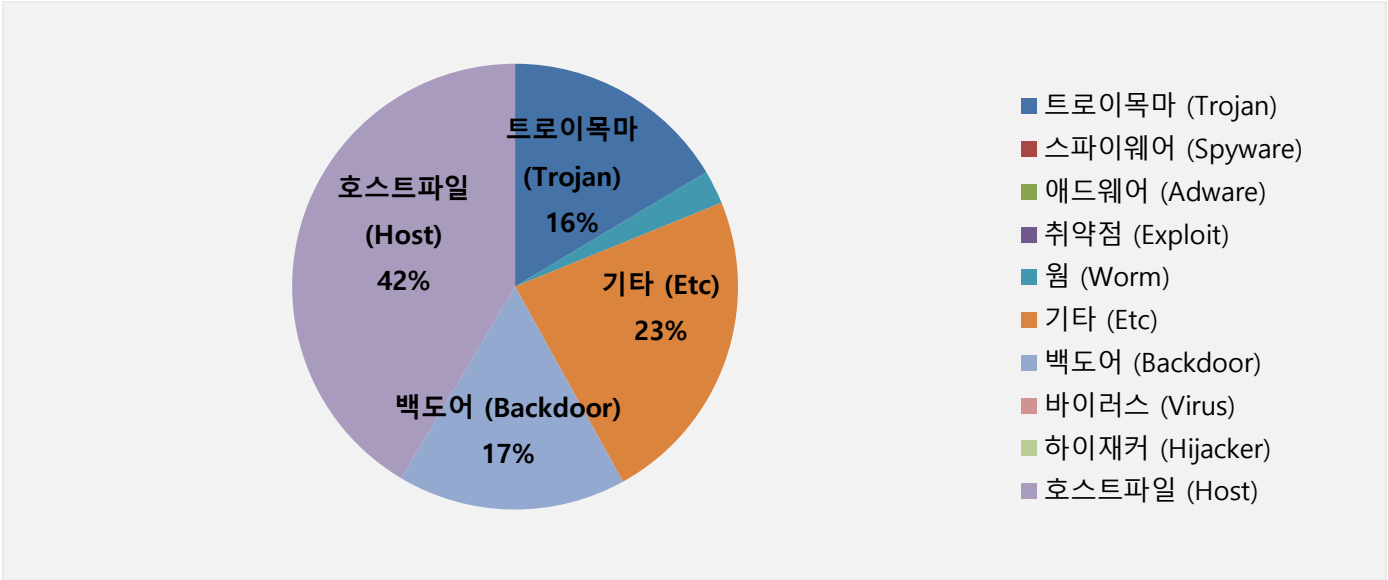
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	609,977
2	-	Backdoor.Generic.792814	Backdoor	244,196
3	↑ 1	Misc.HackTool.AutoKMS	ETC	89,160
4	↓ 1	Trojan.Lisp.Agent.F	Trojan	62,197
5	New	Trojan.Downloader.1481240	Trojan	50,621
6	↑ 4	Trojan.Damaged.PE	Trojan	50,170
7	↑ 2	Application.Hacktool.KMSActivator.HA	ETC	45,951
8	↑ 6	Misc.HackTool.KMSActivator	ETC	44,609
9	New	JS:Trojan.Cryxos.6026	Trojan	44,060
10	↑ 2	Application.Hacktool.KMSActivator.AK	ETC	42,594
11	↑ 2	Application.Hacktool.KMSActivator.AI	ETC	41,467
12	↓ 2	Application.Hacktool.KMSActivator.HJ	ETC	41,185
13	New	Worm.ACAD.Bursted	Worm	35,885
14	↑ 1	Application.Hacktool.KMSAuto.AT	ETC	34,769
15	New	JS:Trojan.Cryxos.5175	Trojan	34,570

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2022 년 2 월 01 일 ~ 2022 년 2 월 28 일

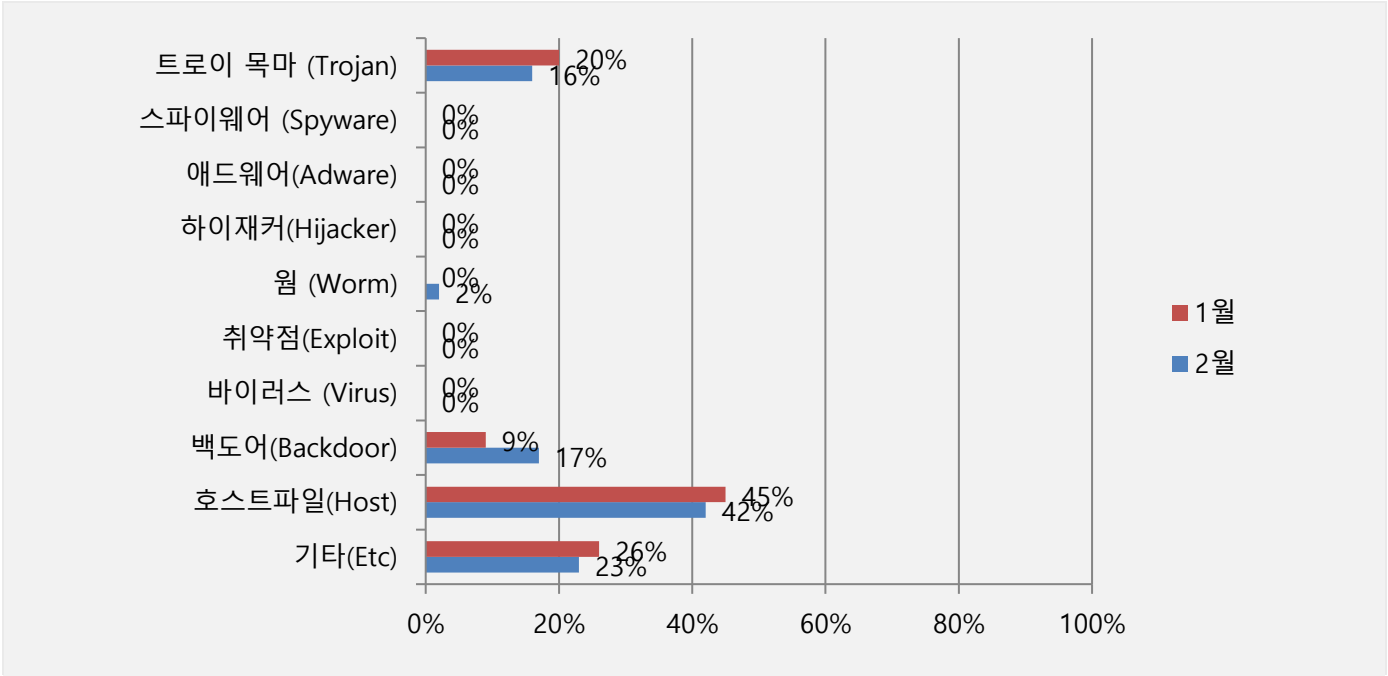
악성코드 유형별 비율

악성코드 유형별 비율에서 호스트파일(Host) 이 42%로 가장 높은 비율로 탐지 되었으며, 기타(ETC) 유형과 트로이목마(Trojan) 유형이 23%, 16%로 웜(Worm)과 백도어(Backdoor) 유형이 각각 2%, 17%로 확인되었다. 2022 년 1 월과 비교하여 전체 감염 건수는 약 19.2% 감소하였다.



카테고리별 악성코드 비율 전월 비교

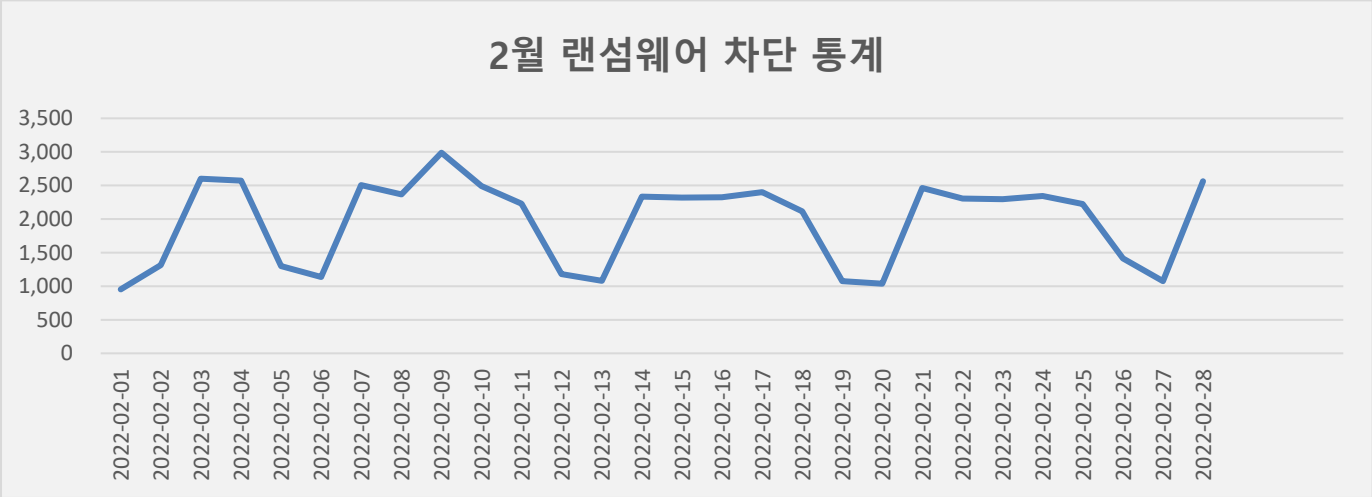
2022 년 2 월에는 지난 1 월과 비교하여 기타(ETC) 유형이 3% 감소했으며, 호스트파일(Host) 유형의 악성코드 감염이 3% 감소하였지만 여전히 높은 탐지율을 기록하고있다. 백도어(Backdoor), 트로이목마(Trojan) 유형은 전월 대비 비슷한 17%, 16%를 기록하였다. 2 월에는 웜(Worm) 유형이 2%로 새롭게 확인되었다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

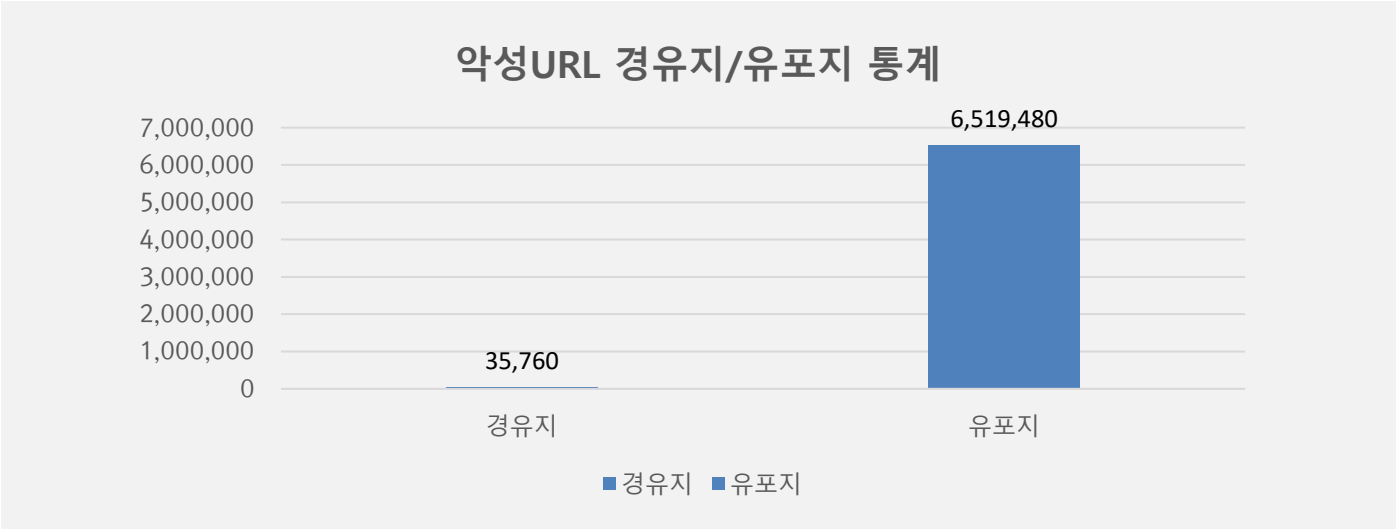
2 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 2 월 1 일부터 2 월 28 일까지 총 54,997 건의 랜섬웨어 공격 시도가 차단되었다. 1 월의 랜섬웨어 공격 건수인 59,688 건에 비해 약 7.8% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 2 월 한 달간 총 6,555,240 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 1 월 한 달간 확인되었던 7,448,632 의 악성코드 경유지/유포지 URL 수에 비해 약 11.9% 가량 감소한 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. 한국도로공사 통행료 납부를 위장하여 유포중인 피싱 메일 주의!

2. 병·의료원 건강검진 증명서 발급으로 위장한 北 연계 공격 등장

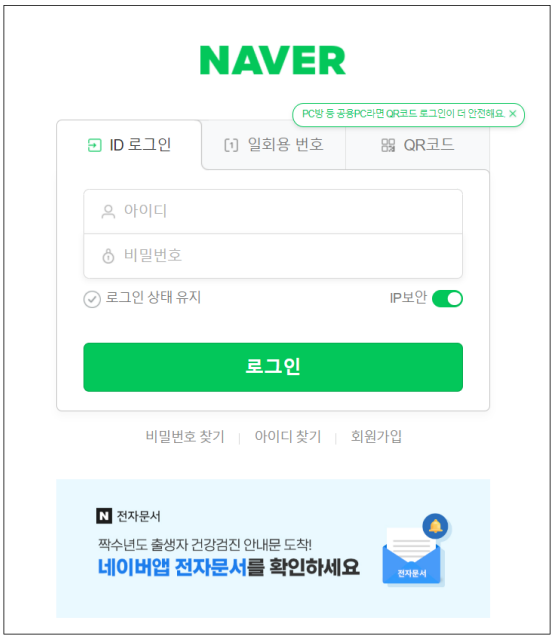
1. 한국도로공사 통행료 납부를 위장하여 유포중인 피싱 메일 주의!

3 일부터 한국도로공사 통행료 납부를 위장한 피싱 메일이 대량으로 유포되고 있어 사용자들의 주의가 필요합니다.

해당 피싱 메일은 '회원님께 도착한 새 전자문서를 확인하세요'라는 제목으로 유포중이며 해당 메일을 클릭하면 마치 한국도로공사에서 보낸 메일처럼 위장하고 있습니다.

[그림 1] 한국도로공사 통행료 납부 위장 피싱 메일

만일 사용자가 전자문서 홈으로 버튼을 클릭하면 네이버를 위장한 피싱 페이지로 연결되며 사용자에게 로그인을 유도합니다.



[그림 2] 네이버 피싱 페이지

만일 사용자가 해당 페이지를 실제 네이버 페이지로 오인하여 계정정보를 입력한다면, 입력한 계정정보는 공격자에게 넘어가게 됩니다. 이렇게 유출된 계정정보는 동일한 아이디, 비밀번호를 사용하는 다른 웹사이트 및 금융페이지를 통해 2 차, 3 차 피해를 입을수도 있습니다.

사실, 해당 페이지는 공식 네이버 페이지 주소와 다르기 때문에, 사용자가 주소창만 확인한다면 쉽게 피싱 페이지라는 것을 인지할 수 있습니다. 그렇기 때문에 사용자 여러분들께서는 링크를 통해 접속한 페이지의 경우 반드시 주소를 확인하는 습관을 길러야 합니다.

[그림 3] 한국도로공사 공식 홈페이지에 게재된 피싱 주의 공지사항

현재 한국도로공사 공식 홈페이지에도 해당 피싱메일에 대한 주의 공지가 게재되어 있습니다. 사용자 여러분들께서는 이러한 이메일을 수신하시면 바로 삭제하시기를 권고드립니다.

2. 병·의료원 건강검진 증명서 발급으로 위장한 北 연계 공격 등장

국내에서 병·의료원 증명서 발급처럼 위장한 北 연계 해킹 공격이 등장했다며, 각별한 주의와 대비가 요구됩니다.

이번 공격은 마치 건강 검진 결과 인터넷 조회 및 발급 서비스로 교묘히 위장해 악성 파일을 유포했으며, 실제 국내 병원 및 의료기관 증명서 발급에 필요한 정상 플러그인 프로그램을 함께 결합해 신뢰 기반 속임수를 사용한 것이 특징입니다.

따라서 해당 프로그램이 설치될 경우 정상적인 병원 증명서 발급 진행이 가능하지만, 동시에 예기치 못한 사이버 보안 위협에 노출되게 됩니다.

분석결과, 악성 파일은 지난 2 월 25 일 만들어졌으며, 실제 공격이 진행된 시기는 3 월이며, 윈도(Windows) 64 비트 기반으로 개발됐습니다.

해당 파일 내부에는 각각 암호화된 형태로 2 개의 리소스가 존재하는데, 하나는 정상적인 병원 증명서 발급 프로그램이고, 나머지 다른 하나는 은밀히 백도어(Backdoor) 기능을 수행하는 악성 파일입니다. 이러한 구조로 악성과 정상 두 개의 모듈이 동시에 설치되지만, 컴퓨터 화면에는 정상 설치 화면만 보이게 됩니다.

발견된 악성 파일의 유사도 및 연관성 조사를 통해 지난 2 월 국내 공중파 방송국 기자 및 북한 전문 언론사 등에 '사내 금융업무 상세내역.zip' 파일로 수행된 APT(지능형지속위협) 공격과 일본의 외교안보 싱크탱크인 일본국제문제연구소의 동북아시아 군사적 긴장 고조와 일본의 대응전략 연차 보고서처럼 사칭한 공격 사건의 연장선으로 공식 확인되었습니다.

당시 국내 방송사 대상 공격에서 발견된 위협 지표 중에는 북한 표기식 단어인 '현시'와 공격자가 사용한 'Freehunter' 계정, 그리고 명령 제어(C2) 서버인 'ms-work[.]com-info[.]store' 등의 고유한 흔적이 발견됐습니다. 특히, 해당 위협과 연결된 침해사고에서 'KGH' 이니셜이 발견된 바 있습니다.

이번 공격에 사용된 C2 서버는 'ms-work[.]com-pass[.]online' 도메인으로 앞서 언급한 특정 방송사 대상 공격 주소와 유사하고, 주요 함수 구조 역시 일치한 것으로 분석됐습니다. 아울러 2021 년 7 월경 발견된 변종은

02 전문가 기고

웨일(Whale) 브라우저의 확장 프로그램처럼 위장했고, 'KGH_Backdoor.dll' 익스포트 함수명과 'support-hosting[.]000webhostapp[.]com' 주소가 사용되었습니다.

ESRC 는 'KGH' 키워드가 계정 또는 폴더 이름에 사용된 여러 자료를 조사하고 있으며, 영문 이니셜 등 모든 가능성을 염두에 두고 면밀한 위협 배후 조사를 진행하고 있습니다. 유사 위협 중 2012 년경 북한 아이피(IP) 주소에서 해외 특정 서비스에 접근한 이력이 보고된 바 있습니다.

러시아 소행으로 알려진 데이터 파괴용 악성 파일이 우크라이나에서 다수 보고되고 있는 가운데, 국내도 北 연계 사이버 위협이 꾸준히 발견되고 있습니다. 특히 다가오는 대한민국 대통령 선거와 관련해 사회공학적 해킹 공격이 등장할 수 있다며 각별한 주의와 대비가 필요합니다.

현재 이스트시큐리티는 이와 관련된 악성 파일을 알약(ALYac) 백신 프로그램에 업데이트를 완료하였고, 사이버 위협 정보를 한국인터넷진흥원(KISA) 등 관계 당국과 긴밀히 공유해 기존에 알려진 위협이 확산되지 않도록 협력을 유지하고 있습니다.

03
악성코드 분석 보고

[Trojan.JAVA.Agent.Gen] 악성코드 분석 보고서

Trojan.JAVA.Agent.Gen (이하 'STRRAT')는 지난 2020 년에 공개된 Java 언어 기반의 명령 제어 악성코드이며, 최근까지 이메일 등으로 유포가 이루어지고 있는 것으로 알려져 있다.

특징적으로 이 STRRAT 는 브라우저 크리덴셜 정보 유출 등의 일반적인 RAT 기능과 더불어 'Crimson'이라고 불리우는 랜섬웨어 기능이 함께 포함되어 있는 점이 특징이다.

```
public static String[] a() {
    String[] a0 = null;
    try {
        java.io.InputStream a1 = carLambo.FirstRun.class.getResourceAsStream("resources/config.txt");
        StringBuilder a2 = new StringBuilder();
        byte[] a3 = new byte[1024];
        while(true) {
            int i = a1.read(a3, 0, 1024);
            if (i == -1) {
                break;
            }
            a2.append(new String(a3, 0, i));
        }
        a1.close();
        a0 = new String(carLambo.j.a("strigoi", javax.xml.bind.DatatypeConverter.parseBase64Binary(a2.toString())),
    } catch(Exception ignoredException) {
        String[] a4 = null;
        return a4;
    }
    return a0;
```

[그림] 'config.txt' 디코딩 코드의 일부

'STRRAT' 악성코드는 정보 전송 및 명령 제어 기능을 수행하는 Java 기반의 RAT 이다. 특징적으로 이 악성코드는 다른 명령 제어 악성코드와 달리 랜섬웨어 기능이 탑재되어 있는 점, EXE 기반 대신 Java 파일(*.jar) 혹은 스크립트를 실행하는 코드만이 존재한다는 점에 있다.

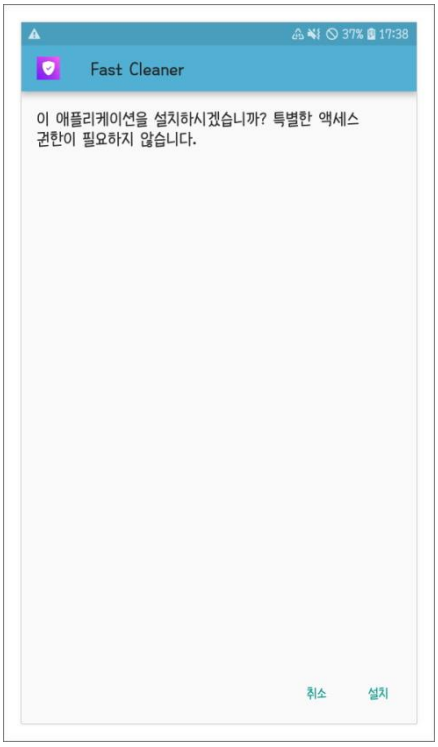
만일 기업체나 개인이 이러한 악성코드에 감염이 이루어지는 경우, 공격자의 의도에 따라 정보 유출 혹은 랜섬웨어 감염으로 금전 피해가 발생할 수 있다.

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

현재 알약에서 관련 악성코드를 'Trojan.JAVA.Agent.Gen'로 진단하고 있다.

[Trojan.Android.Banker] 악성코드 분석 보고서

구글 플레이 스토어를 통해 유포되는 악성 앱들이 꾸준히 발견되고있다. 최근에는 구글 플레이 스토어를 통해 'Xenomorph"라 불리는 악성 앱이 유포되었다. 이 악성 앱은 피해자의 뱅킹 정보 탈취를 목적으로 제작되었다. 타겟은 유럽의 은행들을 이용하는 스마트폰 사용자들이며 뱅킹 정보를 탈취한 후 금전 획득을 위해 탈취한 정보를 활용한다.



[그림] 악성 앱 설치 화면

Trojan.Android.Banker 공격은 금전 갈취가 주요 목적이다. 이 악성 앱의 유포 방법은 공식 스토어인 구글 플레이 스토어를 통해 이루어지기에 피해자가 공격을 인지하기 더욱 어렵다. 그리고 공식 스토어를 통한 설치이기에 OS 에서 제공하는 프로텍트 서비스도 무용지물이 된다.

따라서, 공식 스토어를 이용하더라도 신뢰할 수 있는 앱 제작자인지 확인이 필요하며 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지하는 것이 위협으로부터 자신을 지키는 첫걸음이라 할 수 있을 것이다.

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

04
글로벌 보안 동향

TeaBot 악성코드, 구글 플레이 스토어에 잠입해 미국 사용자들 노려

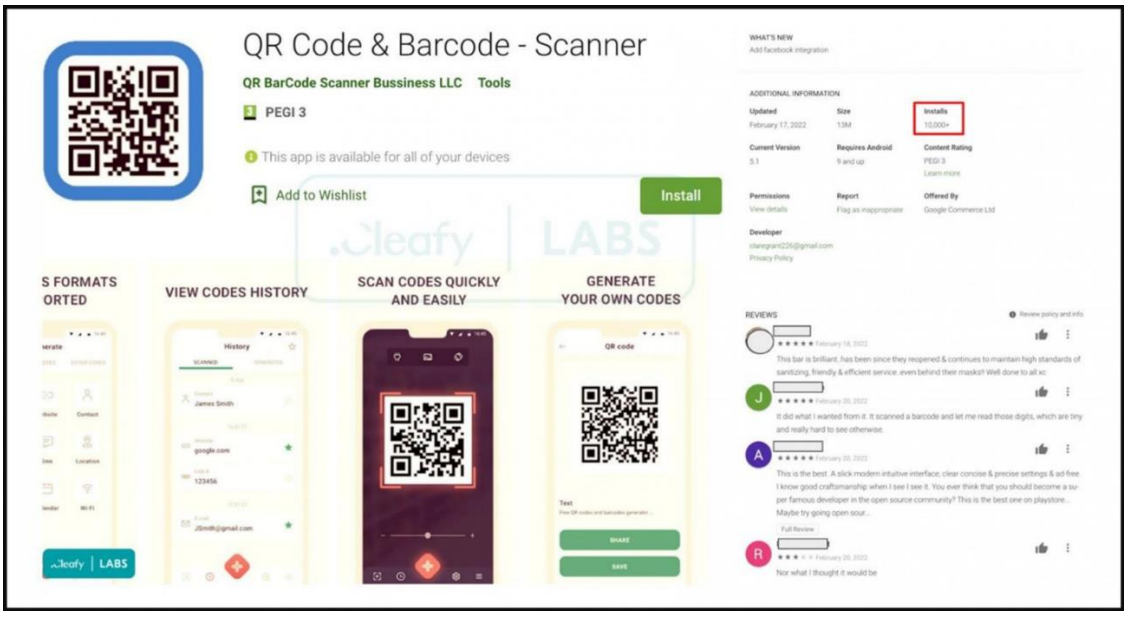
TeaBot malware slips back into Google Play Store to target US users

TeaBot 뱅킹 트로이 목마가 또 다시 구글 플레이 스토어에서 발견되었습니다. 이는 QR 코드 앱으로 위장해 이미 기기 1 만대 이상을 감염시킨 것으로 나타났습니다.

제작자들은 이미 지난 1 월 이러한 전략을 사용한 전적이 있으며, 구글은 이를 퇴출시켰지만 악성코드 제작자는 또 다시 안드로이드 공식 앱 스토어에 침투할 방법을 찾은 것으로 보입니다.

온라인 사기 관리 및 예방 회사인 Cleafy 에서 발행한 보고서에 따르면, 해당 애플리케이션은 드롭퍼의 역할을 합니다. 앱 자체에는 악성코드가 없으며 최소한의 권한을 요청하기 때문에 구글에서 이상한 점을 발견하기 어려웠던 것으로 보입니다.

또한 해당 트로이 목마 앱은 홍보된 기능을 포함하고 있기 때문에 사용자 리뷰는 긍정적인 편입니다



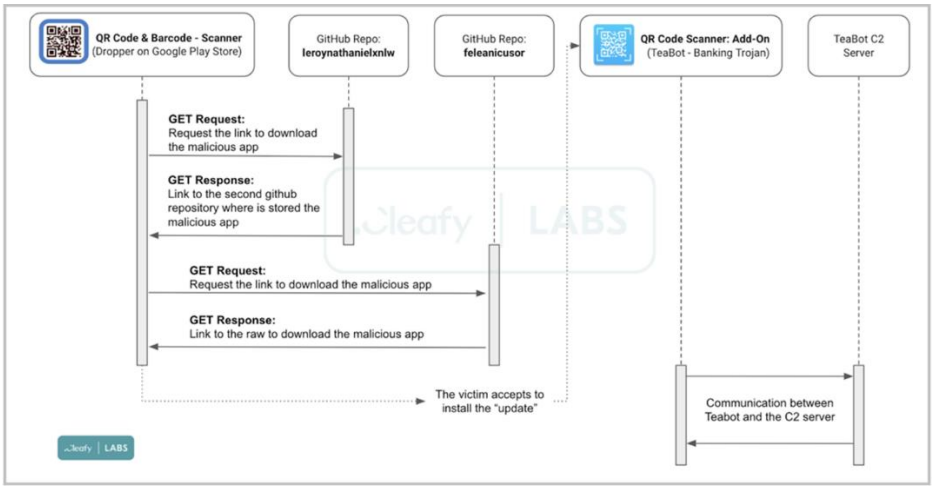
[그림] 플레이 스토어 내 TeaBot 로더 앱
[이미지 출처] https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

TeaBot 페이로드 가져오기

지난 2 월, 연구원들은 TeaBot 이 합법적인 QR 코드 스캔 유틸리티인 'QR Code & Barcode – Scanner'라는 앱으로 위장한 것을 발견했습니다.

앱은 설치 시 팝업 메시지를 띄워 업데이트를 요청하지만, 플레이 스토어 가이드라인에 따른 표준 절차와는 달리 외부 소스에서 업데이트를 가져옵니다.

Cleafy 는 다운로드 출처를 추적한 결과 동일한 사용자(feleanicusor)가 소유한 GitHub 저장소 2 곳에서 2022 년 2 월 17 일 업로드된 여러 TeaBot 샘플을 발견했습니다.

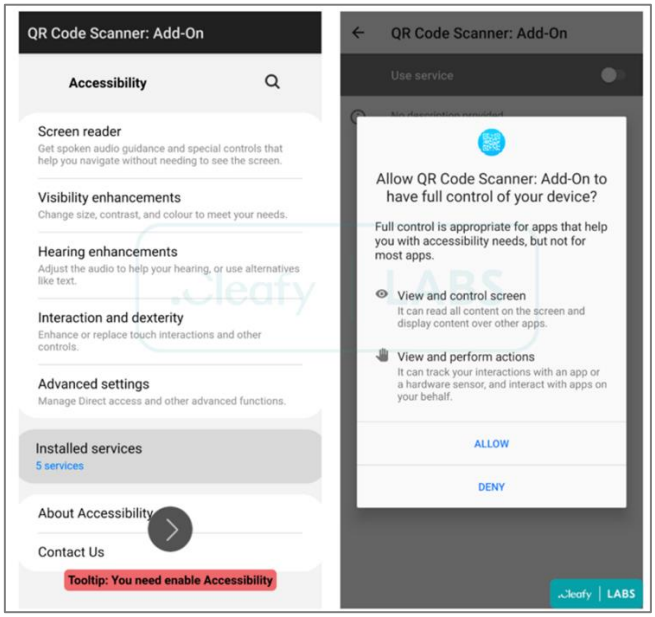


[그림] TeaBot 로딩 및 감염 과정
[이미지 출처] https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

피해자가 신뢰할 수 없는 출처로부터 받은 업데이트 설치를 수락하면, TeaBot 은 'QR Code Scanner: Add-On' 이라는 이름의 새로운 앱으로 기기에 로드 됩니다.

새 앱은 자동으로 실행되고, 아래 기능을 수행하기 위해 사용자에게 접근성 서비스 사용 권한을 요구합니다.

- 기기의 화면을 보고 로그인 크리덴셜, 2FA 코드, SMS 콘텐츠 등을 노출하는 스크린샷 캡쳐
- 사용자 상호 작용 없이 백그라운드에서 추가 권한 자동 부여 등 작업 수행



[그림] 접근성 서비스 악용
[이미지 출처] https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

Google 은 접근성 서비스에 대한 보안을 높일 수 있도록 Android 12 의 API 를 변경했지만, 이는 아직까지 뱅킹 트로이 목마가 가장 흔히 악용하는 권한입니다. 또한 대부분의 안드로이드 휴대 기기는 여전히 OS 버전 11 또는 이전 버전을 실행하고 있습니다.

타깃 범위 확장돼

Bitdefender 가 2021 년 1 월 플레이 스토어에서 발견해 분석한 TeaBot 은 당시 피해자의 위치가 미국일 경우 앱을 종료했습니다.

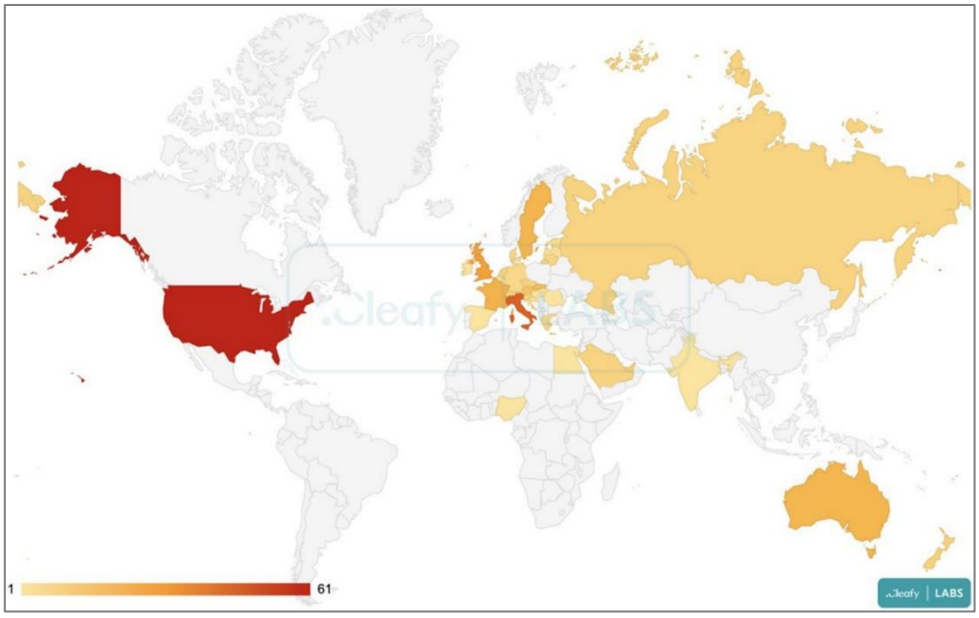
하지만 이제 TeaBot 은 미국 내 사용자를 적극적으로 노리고 있으며 러시아어, 슬로바키아어, 중국어도 추가해 악성코드로 전 세계 피해자를 노리고 있는 것으로 나타났습니다.

```
if(v1 == 3201) {
    v0_1 = v0.equals("de") ? 3 : -1;
}
else {
    switch(v1) {
        case 0xCAE: {
            v0_1 = v0.equals("es") ? 0 : -1;
            break;
        }
        case 0xCCC: {
            v0_1 = v0.equals("fr") ? 6 : -1;
            break;
        }
        case 0xD2B: {
            v0_1 = v0.equals("it") ? 4 : -1;
            break;
        }
        case 0xDBE: {
            v0_1 = v0.equals("nl") ? 5 : -1;
            break;
        }
        case 0xE04: {
            v0_1 = v0.equals("pt") ? 7 : -1;
            break;
        }
        case 0xE43: {
            v0_1 = v0.equals("ru") ? 8 : -1;
            break;
        }
        case 0xE58: {
            v0_1 = v0.equals("sk") ? 2 : -1;
            break;
        }
        default: {
            v0_1 = v1 == 0xF2E && (v0.equals("zh")) ? 1 : -1;
```

```
switch(v0_1) {
    case 0: {
        return "desinstalar";
    }
    case 1: {
        return "卸载";
    }
    case 2: {
        return "odinšta";
    }
    case 3: {
        return "deinstallieren";
    }
    case 4: {
        return "disinst";
    }
    case 5: {
        return "verwijderen";
    }
    case 6: {
        return "désinst";
    }
    case 7: {
        return "desinst";
    }
    case 8: {
        return "удалить";
    }
    default: {
        return "uninstall";
```

[그림] TeaBot 의 코드에 추가된 새로운 언어
[이미지 출처] https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

TeaBot 의 운영자는 소규모 시장에서 "테스트" 기간을 거쳤고, 이제 그들의 툴이 대규모 작업을 수행할 준비가 되었다고 생각한 것으로 보입니다.



[그림] TeaBot 피해자 히트맵
[이미지 출처] https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

이 악성코드의 2021 년 초 샘플과 비교했을 때, 현재 버전은 더욱 강력한 문자열 난독화 기능을 제공하며 은행, 보험, 암호화 지갑, 암호화 교환 애플리케이션을 500%로 더욱 집중적으로 노립니다.

사용자들은 플레이 스토어에서만 앱을 다운로드 할 경우에도 이 뱅킹 트로이목마를 예방하기 위해서 최소한의 앱 만을 설치할 것을 권장합니다.

또한 기기에 새 앱을 설치할 때마다 며칠간 배터리 소모와 네트워크 트래픽 양을 모니터링하여 의심스러운 패턴을 찾아내는 것이 중요합니다.

[출처]

https://www.bleepingcomputer.com/news/security/teabot-malware-slips-back-into-google-play-store-to-target-us-users/

https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

인기있는 게임의 복사본에 숨은 악성코드, 마이크로소프트 스토어에 침투해

Malware infiltrates Microsoft Store via clones of popular games

Electron Bot 이라는 악성코드가 인기 있는 게임인 Subway Surfer, Temple Run 등의 복사본에 숨어 마이크로소프트 공식 스토어에 침투해 스웨덴, 이스라엘, 스페인, 버뮤다의 컴퓨터 약 5,000 대를 감염시켰습니다.

사이버 보안 회사인 Check Point 가 발견 및 분석한 이 악성코드는 공격자가 해킹된 시스템을 완벽하게 제어할 수 있도록 하는 백도어로 원격 명령 실행, 실시간 상호 작용 등을 지원합니다.

공격자의 목표는 소셜 미디어 홍보 및 클릭 사기로 보입니다. Electron Bot 은 이러한 목적을 위해 페이스북, 구글, 유튜브, 사운드 클라우드와 같은 SNS 플랫폼에서 새 계정 등록, 댓글 달기, 좋아요 누르기 등과 같은 기능을 지원하며, SNS 계정을 제어합니다.

3 년 동안 진화해

이 공격은 지난 2018 년 말 스푸핑된 Google LLC 에서 마이크로소프트 스토어에 “Album by Google Photos” 라는 앱을 등록해 처음으로 발견되었습니다. 해당 앱에는 초기 Electron Bot 의 변종이 숨겨져 있었습니다.

그 이후로 악성코드 제작자는 툴에 새로운 기능 다수와 동적 스크립트 로딩 등과 같은 고급 탐지 회피 기능을 추가했습니다. 이 악성코드는 Electron 으로 작성되었으며, 자연스러운 브라우징 동작을 모방하여 실제 웹사이트 방문자인 것처럼 행동할 수 있습니다.

이는 Electron 프레임워크의 Chromium 엔진을 사용해 새로운 숨겨진 브라우저 창을 열고 적절한 HTTP 헤더를 설정하고 요청된 HTML 페이지를 렌더링하며 마우스 이동, 스크롤, 클릭, 키보드 입력 등을 수행 가능합니다.

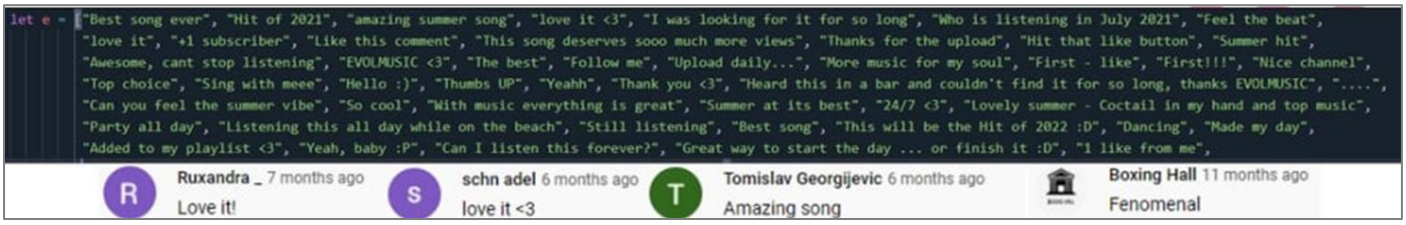
```
264  let humanMouseMove = async function(e, n = 40, o = 20, t = 50) {
265      e = e || {
266          x: randomGenerator(0, window.innerWidth),
267          y: randomGenerator(220, window.innerHeight)
```

[그림] 인간의 마우스 움직임 에뮬레이션

[이미지 출처] https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store/

Check Point 연구원들이 분석한 Electron Bot 캠페인의 주요 목적은 아래와 같습니다

SEO 포이즈닝 – Google 검색 결과 높은 순위를 차지하는 악성코드 드롭 사이트 생성
광고 클릭 – 백그라운드에서 원격 사이트에 연결해 보이지 않는 광고 클릭하기
SNS 계정 홍보 – SNS 플랫폼의 특정 콘텐츠로 트래픽 보내기
온라인 제품 홍보 – 광고를 클릭하여 스토어 평점 높이기



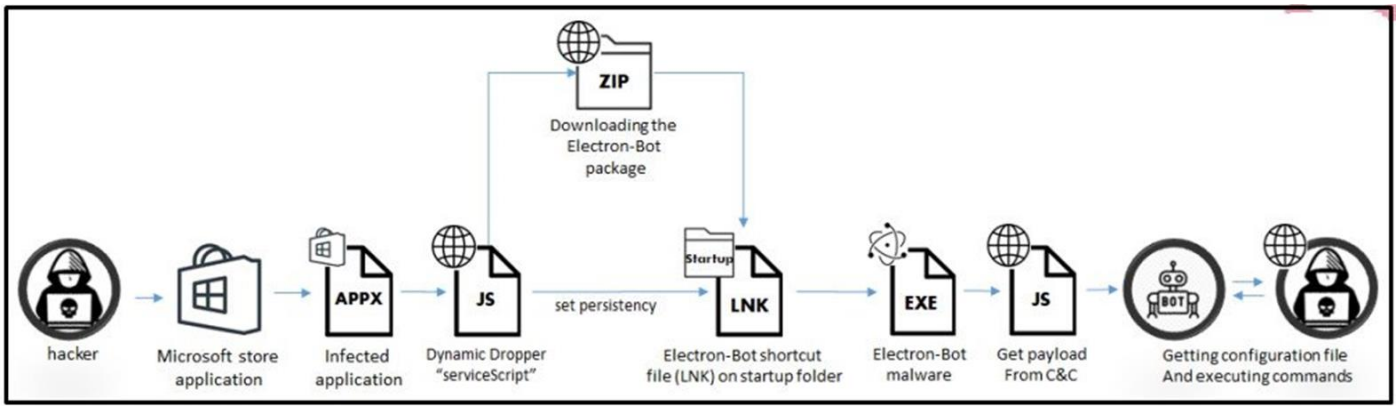
[그림] 하드코딩된 YouTube 댓글
[이미지 출처] https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store

이러한 기능은 서비스 형태로 불법적으로 온라인 수익을 늘리려는 사용자에게 제공되기 때문에, 악성코드 운영자는 간접적으로 수익을 벌어들일 수 있습니다.

Check Point 는 공격자가 불가리아에 기반을 둔 것으로 추측할 수 있는 증거를 발견했다고 밝혔습니다. 하지만 이외 공격자의 신원이나 위치는 알려지지 않았습니다.

감염 체인

감염 체인은 피해자가 소프트웨어 출처로 신뢰할 수 있는 마이크로소프트 스토어 내에서 악성코드가 포함된 앱 중 하나를 다운로드 및 설치하는 것으로 시작됩니다.



[그림] Electron Bot 감염 체인
[이미지 출처] https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store/

애플리케이션이 시작되면, 백그라운드에서 JavaScript 드로퍼가 동적 로드되어 Electron Bot 페이로드를 가져온 다음 설치합니다.

이 악성코드는 다음 시스템 시작 시 실행되어 C2(Electron Bot[.]s3[.]eu-central-1[.]amazonaws.com, 11k[.]online)에 연결하고 구성을 가져오고, 파이프라인 내 모든 명령을 실행합니다.

메인 스크립트는 런타임에 동적으로 로드되기 때문에, 머신의 메모리에 드롭되는 JS 파일은 매우 작고 보기에는 무해합니다.

```
switch (links[0].type) {
    case constants.linksTypes.IDLE:
        return runIdleLogic(links[0]);
    case constants.linksTypes.POPUNDER:
        return console.log("POPUNDER"), runPopUnderLogic(links[0]);
    case constants.linksTypes.DIRECTLINK:
        return console.log("DIRECT LINK"), runDirectlinkLogic(links[0]);
    case constants.linksTypes.FAST:
        return console.log("FAST"), runFastLogic(links[0]);
    case constants.linksTypes.GOOGLE_SEO:
        return runGoogleSEOLogic(links[0]);
    case constants.linksTypes.PROM_UA:
        return runPromUaLogic(links[0]);
    case constants.linksTypes.YOUTUBE:
        return runYoutubeLogic(links[0]);
    case constants.linksTypes.SUBSCRIBE:
        return runSubscribeLogic(links[0]);
    case constants.linksTypes.MEDIUM:
        return runMediumLogic(links[0]);
    case constants.linksTypes.BANNER:
        return runBannerLogic(links[0]);
    default:
        return console.log("default"), new Promise((e => e()))
}
```

[그림] Electron Bot 에서 지원하는 명령

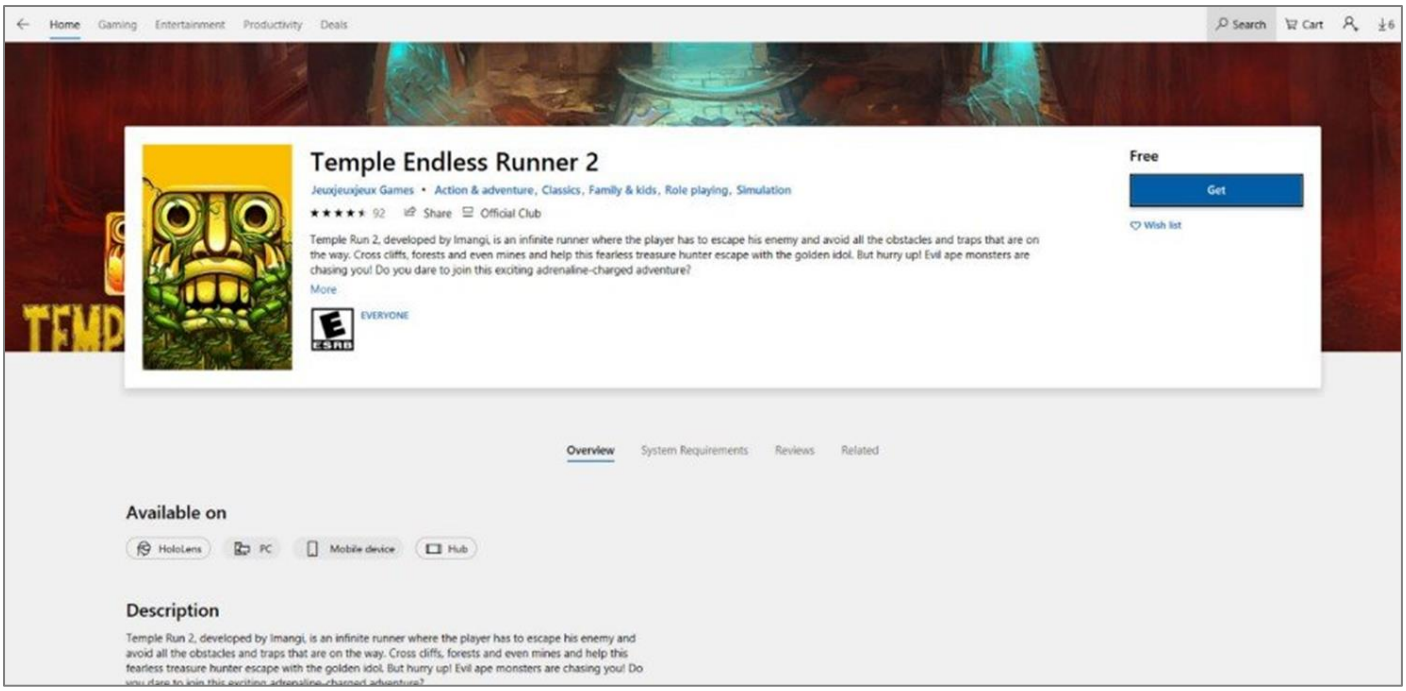
[이미지 출처] https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store/

단순한 게임 그 이상

Check Point 에서 발견한 악성코드가 포함된 모든 게임은 실제로 게임 기능을 제공했으며, 악성 작업은 백그라운드에서 진행되었습니다.

그 결과, 해당 앱은 마이크로소프트 스토어에서 긍정적인 사용자 리뷰를 얻을 수 있었습니다. 2021 년 9 월 6 일에 게시된 Temple Endless Runner 2 는 별점 5 개에 가까운 리뷰 92 개를 받았습니다.

물론, 공격자들은 계속해서 새로운 미끼를 업로드하고 또 다른 게임 및 앱을 통해 피해자에게 악성코드 페이로드를 전달합니다.



[그림] 악성코드가 포함된 마이크로소프트 내 게임
[이미지 출처] https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store/

사용자들은 아래의 이름으로 악성 게임을 등록한 퍼블리셔를 주의해야 합니다.

Lupy games
Crazy 4 games
Jeuxjeuxkeux games
Akshi games
Goo Games

기존 버전의 Electron Bot 이 감염된 시스템에 치명적인 피해를 입히는 것은 아니지만, 공격자가 코드를 쉽게 수정하는 것이 가능해 RAT 또는 랜섬웨어와 같은 2 차 페이로드를 가져올 수 있기 때문에 주의해야합니다.

Check Point 는 윈도우 사용자에게 리뷰가 적은 앱을 다운로드하는 것을 피하고 개발자/게시자의 정보를 자세히 알아본 후 앱 이름이 정확하고 오타가 없는지 확인할 것을 권고했습니다.

[출처]

https://www.bleepingcomputer.com/news/security/malware-infiltrates-microsoft-store-via-clones-of-popular-games/

https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store/ (IOC)

Trickbot 악성코드, 2020 년부터 유명 기업 60 곳 노려

Trickbot Malware Targeted Customers of 60 High-Profile Companies Since 2020

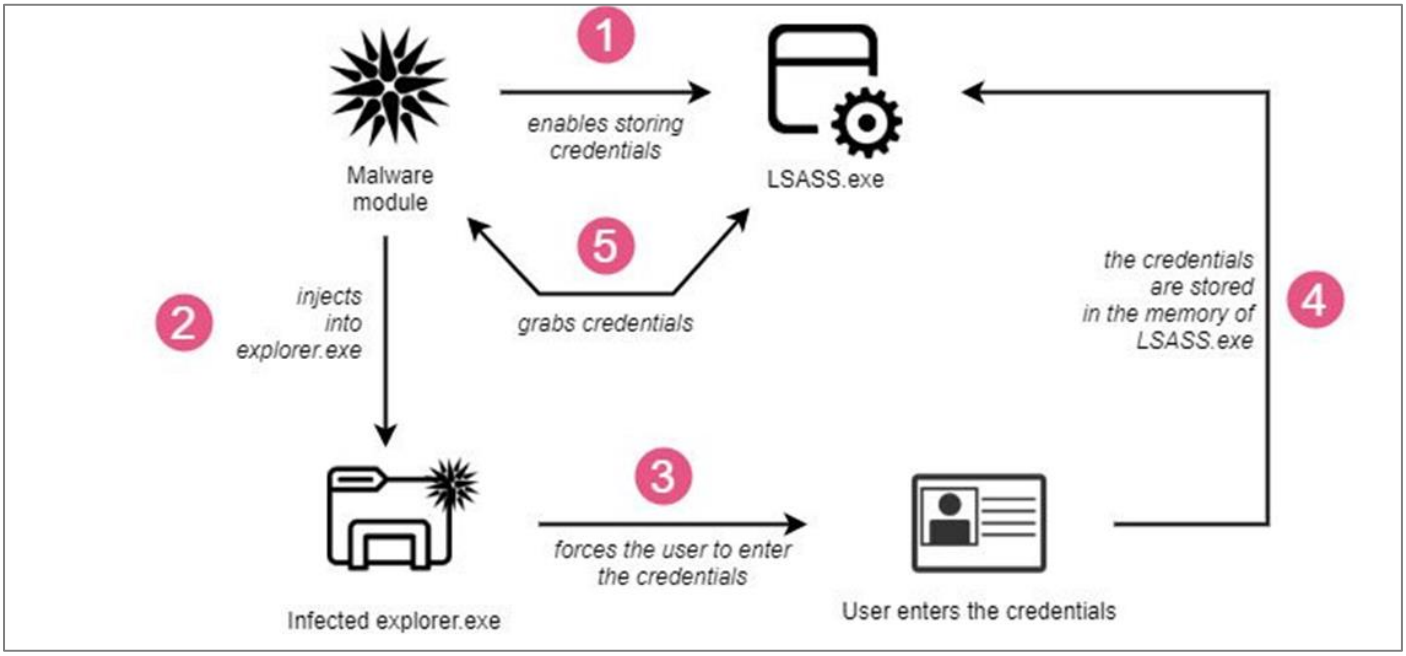
악명 높은 TrickBot 악성코드가 주로 미국에 위치한 가상화폐 회사를 포함 금융 및 기술 기업 60 곳의 고객을 노려온 것으로 나타났습니다.

CheckPoint 의 연구원인 Aliaksandr Trafimchuk 과 Raman Ladutska 는 금일 보고서를 발표해 "TrickBot 은 원하는 대로 다운로드 및 실행이 가능한 20 개 이상의 모듈을 가진 정교하고 다재다능한 악성코드"라 밝혔습니다.

TrickBot 은 광범위하게 확산되어 있고, 지속성을 가질 뿐 만 아니라 보안 및 탐지 레이어를 뚫기 위해 지속적으로 전략을 발전시켜 왔습니다.

이를 위해, 악성코드에서 뱅킹 및 크리덴셜 데이터를 훔치는 역할을 하는 웹 주입 모듈인 "injectDll"은 난독화 해제 방지 기술을 통해 웹 페이지를 충돌시켜 소스 코드를 조사하려는 시도를 막습니다.

또한 보안 연구원이 새로운 웹 주입을 찾아내기 위해 C2 서버에 자동화된 요청을 보내는 것을 방지하는 '분석 방지 가드레일'을 설치해 두었습니다.



[이미지 출처] https://research.checkpoint.com/2022/a-modern-ninja-evasive-trickbot-attacks-customers-of-60-high-profile-companies/

TrickBot 의 또 다른 강점은 "tabDLL" 모듈을 통해 사용자의 크리덴셜을 훔치고, EternalRomance 익스플로잇으로 SMBv1 네트워크 공유를 통해 악성코드를 확산시키는 자체 전파 기능입니다.

TrickBot 의 세 번째 메인 모듈은 "pwgrabc"입니다. 이는 웹 브라우저와 Outlook, Filezilla, WinSCP, RDP, Putty, OpenSSH, OpenVPN, TeamViewer 와 같은 응용 프로그램 다수에서 패스워드를 훔치도록 설계된 크리덴셜 스틸러입니다.

연구원들은 이에 대해 아래와 같이 밝혔습니다.

"TrickBot 은 유명한 피해자를 공격하여 크리덴셜을 도용하고, 운영자가 민감 데이터가 포함된 포털에 접근할 수 있도록 해 운영자에게 더욱 큰 피해를 입힙니다."

"해당 인프라의 운영자는 수준이 높은 악성코드를 개발한 경험이 있습니다."

이러한 발견은 TrickBot 그룹이 코드를 숨기고 역설계를 방어하여 시그니쳐 기반 탐지를 피하고자 하는 궁극적인 목적으로 Bazar 패밀리를 위한 메타프로그래밍 방식을 사용했기 때문에 밝혀졌습니다.

[출처]

https://thehackernews.com/2022/02/trickbot-malware-targeted-customers-of.html

https://research.checkpoint.com/2022/a-modern-ninja-evasive-trickbot-attacks-customers-of-60-high-profile-companies/ (IOC)

(주)이스트시큐리티

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