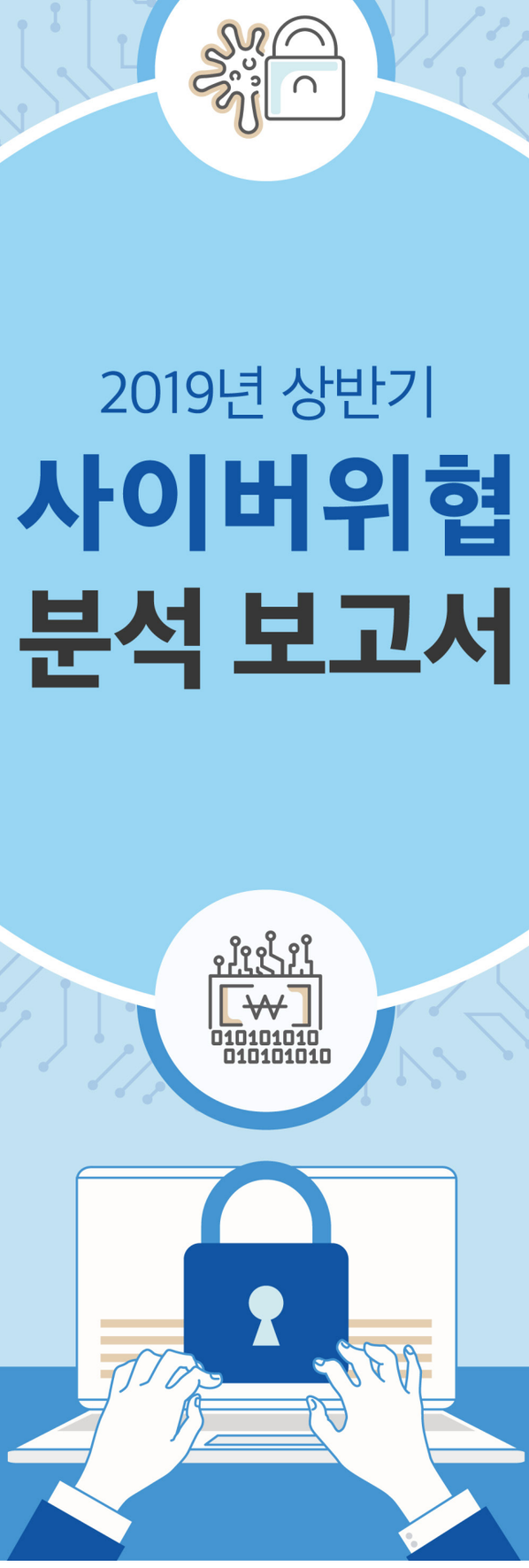

경 찰 청
KOREAN NATIONAL POLICE AGENCY

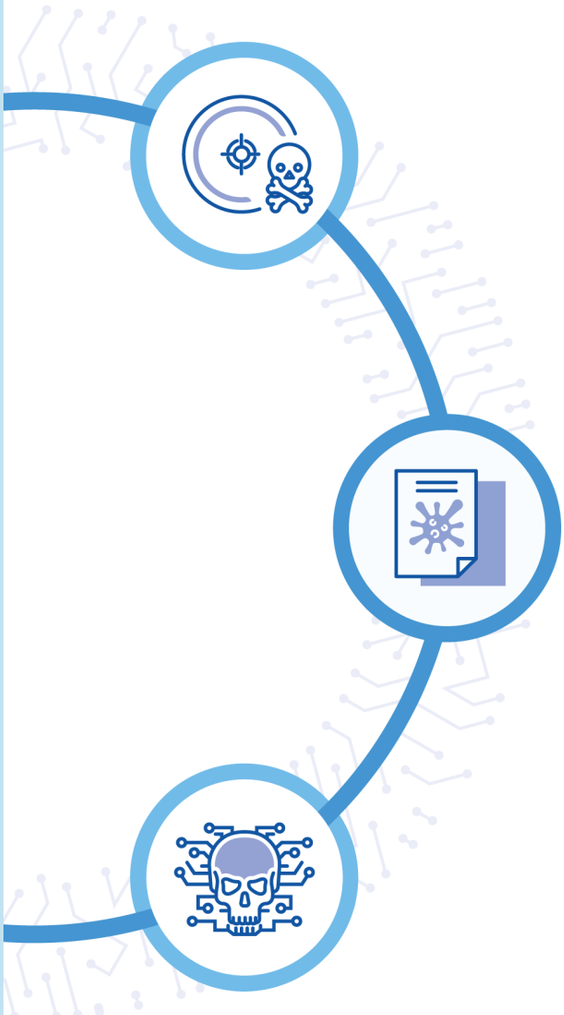
경찰청
KOREAN NATIONAL POLICE AGENCY

2019년 상반기

사이버위협 분석 보고서



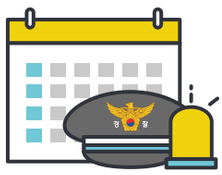
목차



Ⅰ ’19년 상반기 사이버범죄 동향

2019년 상반기 사이버범죄는 85,953건이 발생하였으며, 전년도 같은 기간(70,224건)과 비교해 보면 발생 건수가 약 22.4% 증가하였다.

사이버범죄
85,953건 발생



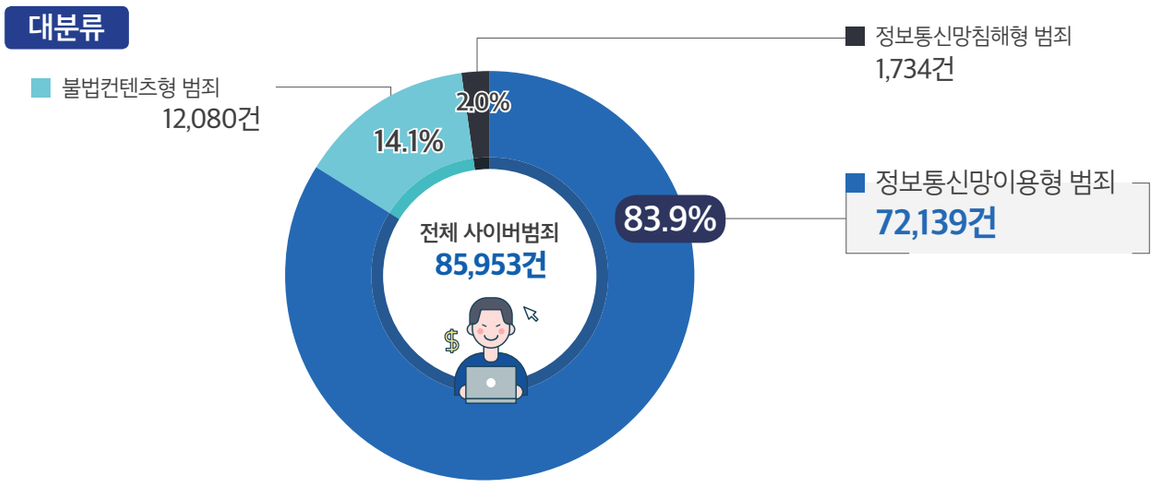
하루에
약 475건

약 **3분**마다
1건 발생

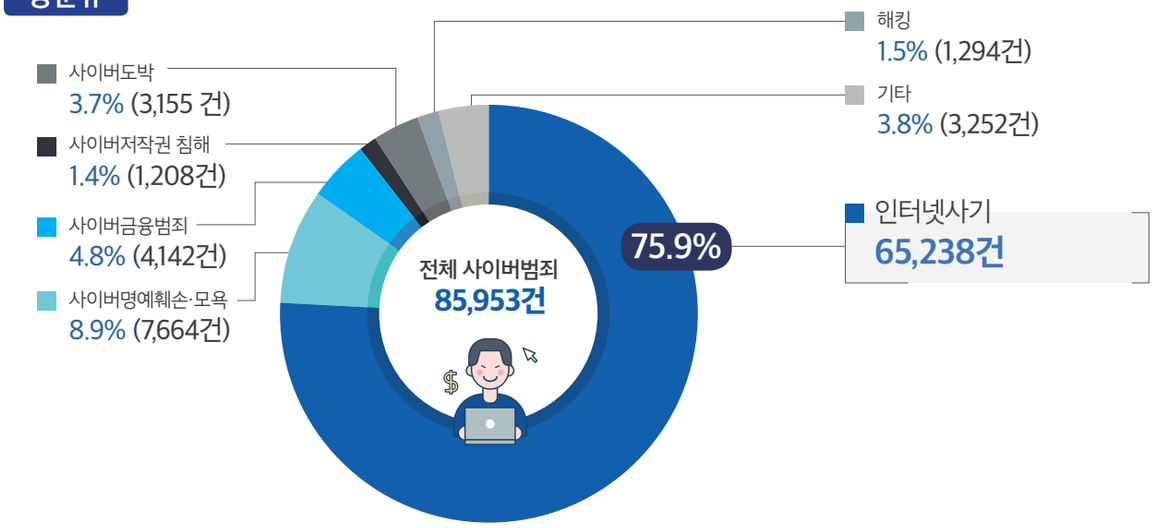
해킹, 악성프로그램 유포 등 정보통신망에 불법적으로 침입하는 방식으로 저지른 범죄(정보통신망 침해 범죄)는 전년 동기간 대비 19.4% 증가하였으며, 인터넷사기, 사이버금융범죄 등 정보통신망을 이용해 저지른 범죄(정보통신망 이용범죄)는 전년 동기간 대비 21.5% 증가했다.
또한 사이버음란물, 사이버도박 등 법이 금지하는 재화를 생산·유포하는 범죄(불법컨텐츠 범죄)도 전년 동기간 대비 28.7% 증가하는 등 모든 유형에서 증가 추세를 보이고 있다.

인터넷 사기(65,238건)가 전체 사이버범죄(85,953건) 발생 건수의 75.9%로 사이버범죄의 대다수를 차지하고 있다. 다음으로 사이버명예훼손·모욕(7,664건)이 전체 사이버범죄의 8.9%를 차지하였으며, 이 외에 사이버금융범죄(4,142건), 사이버도박(3,155건), 사이버저작권 침해(1,208건) 등의 세부 유형이 사이버범죄의 주종을 이루고 있다.

사이버범죄 유형별 발생 비율



중분류

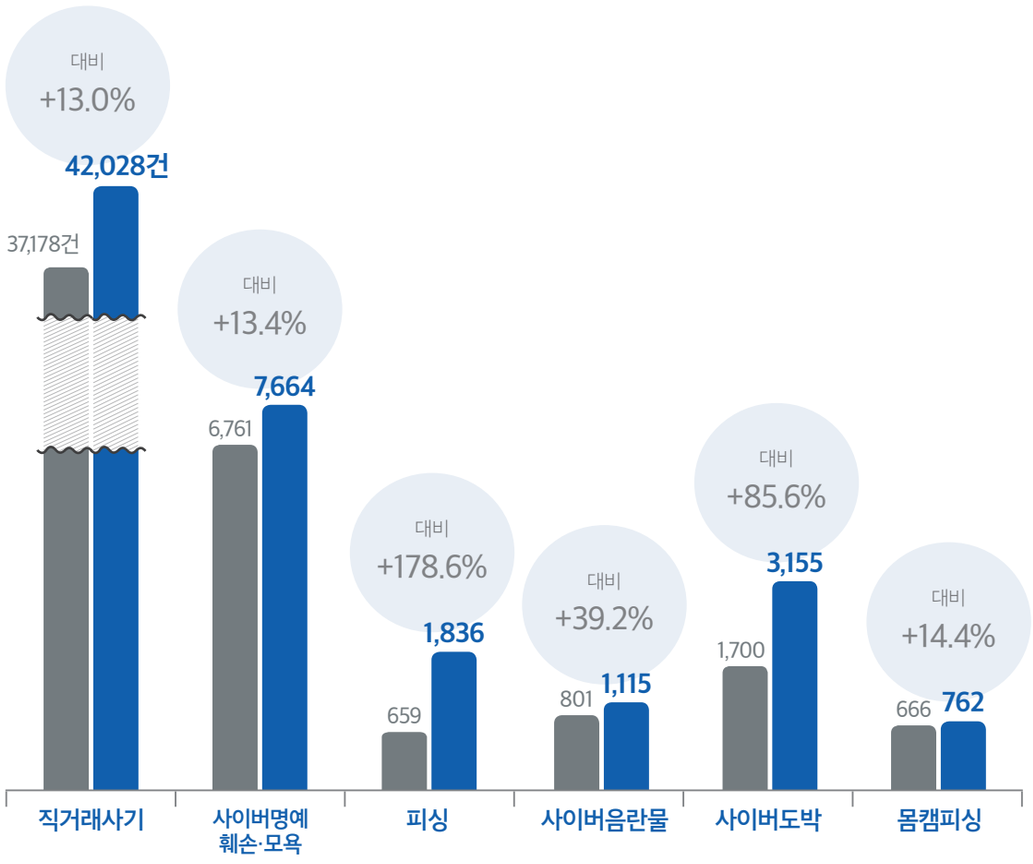

사이버도박
3.7% (3,155 건)
사이버저작권 침해
1.4% (1,208건)
사이버금융범죄
4.8% (4,142건)
사이버명예훼손·모욕
8.9% (7,664건)
해킹
1.5% (1,294건)
기타
3.8% (3,252건)
인터넷사기
65,238건
75.9%
전체 사이버범죄
85,953건

직거래사기·사이버 명예훼손(모욕)·피싱·사이버음란물·사이버도박·몸캠피싱의 발생건수가 증가한 반면, 이메일 무역사기·사이버저작권침해·파밍 등의 유형이 감소하였다.

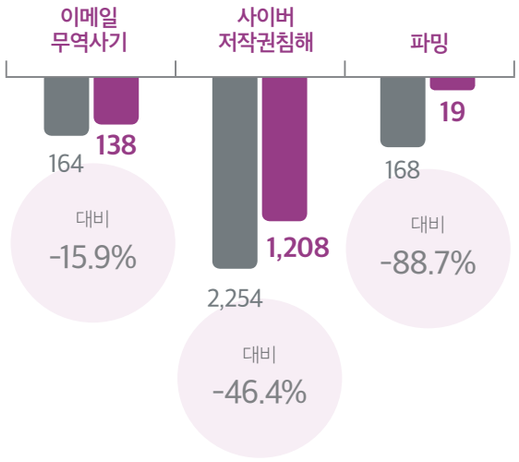
주요 세부유형별 증감(단위 : 건)

2019년 상반기 2018년 상반기

증가



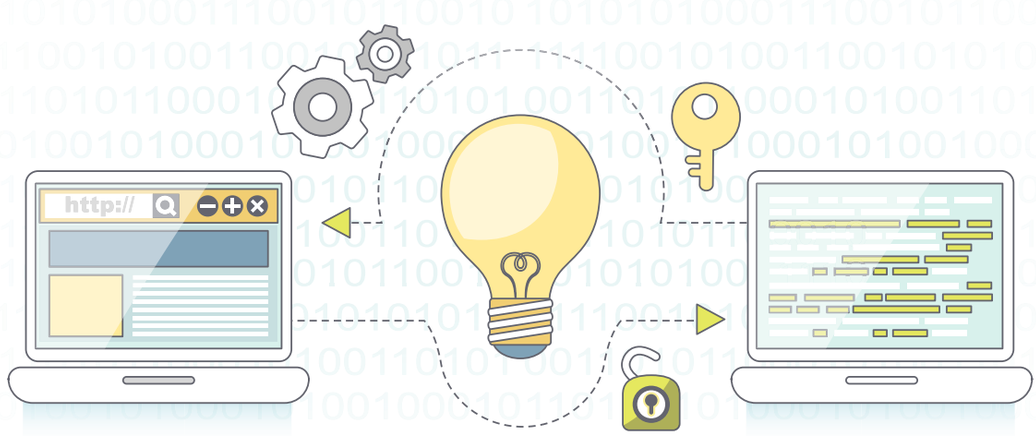
감소



2019년 상반기 사이버범죄의 양상을 살펴보면 첫 번째로, 갠드크랩 랜섬웨어가 여러 다양한 기관을 사칭하여 유포되었다. 특히, 경찰서를 사칭한 '[OO경찰서]출석요구서' 제목으로 갠드크랩 유포 이메일이 확산되었다. 최근에는 한국은행, 헌법재판소 등 국가기관을 사칭하거나, 작년에 기승을 부렸던 '입사지원서를 위장한 이메일 발송' 등 다양한 방법으로 유포되고 있어 주의 할 필요가 있다.
갠드크랩 수법의 변화는 'II. 주요 사이버범죄 유형별 분석'에서 확인할 수 있다.

두 번째로, 지인을 사칭해 송금을 요구하는 메신저피싱이 SNS와 모바일 메신저를 통해 광범위하게 발생하고 있다. 메신저피싱은 지인의 이름과 사진을 도용하고 휴대폰 고장 등을 이유로 통화를 회피하는 한편, 지연 인출을 피하기 위해 1백만 원 이하의 소액을 계좌로 송금하도록 요구한다. 특히, 최근에는 문화상품권 등의 고유번호를 받아 온라인에서 현금화하는 수법이 이용되고 있다.
메신저 피싱 수법은 'II. 주요 사이버범죄 유형별 분석'에서 확인할 수 있다.

최근 독일에서 마약, 개인정보, 악성코드 등이 거래되었던 '다크넷(Darknet)' 사이트 운영자를 체포하였다. '월 스트리트 마켓' 이라는 온라인 거래사이트로, 이용자가 115만 명, 판매처가 5천400개에 달했다.
다크넷은 IP주소가 공유되지 않은 인터넷 암시장으로 많은 범죄에 이용되고 있으며, 범죄 사례도 증가하고 있다. 경찰청 사이버안전국은 올 연말 '다크넷 불법정보 수집·추적 시스템'을 도입하여 다크넷 상에서 발생하는 범죄에 대응해 나갈 계획이다.



Ⅱ 주요 사이버범죄 유형별 분석

01 갠드크랩(GandCrab) 랜섬웨어

갠드크랩(GandCrab)은 “서비스형 랜섬웨어*(Ransomeware as a Service: RaaS)”의 한 종류로, 감염된 PC의 주요 파일을 암호화하고 확장자(‘.GDCB, .CRAB, .KRAB’ 등)를 변경한 뒤 데이터를 복구하려는 피해자에게 금전(가상통화)을 요구하는 랜섬웨어이다.

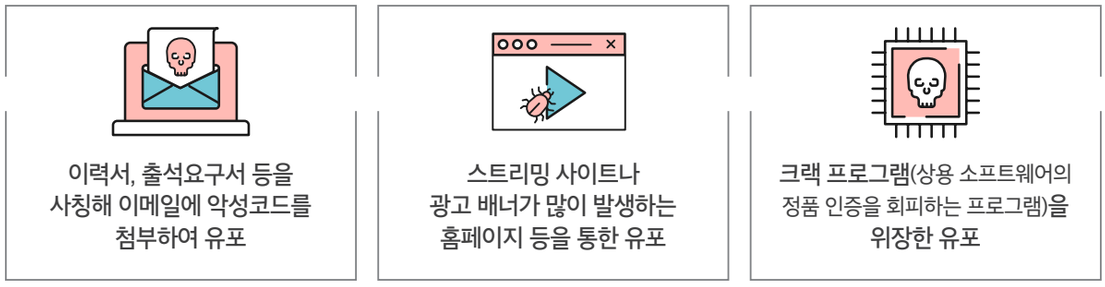
* 서비스형 랜섬웨어

제작자가 직접 공격까지 하는 일반적인 랜섬웨어와는 달리, 랜섬웨어를 제작할 기술적 역량이 없는 사람들을 위해 공격자 외 별도로 제작자가 따로 존재한다. 랜섬웨어로 벌어들이는 수익은 랜섬웨어 구매(공격)자와 제작자 간 분배하여 나눠 갖는다.

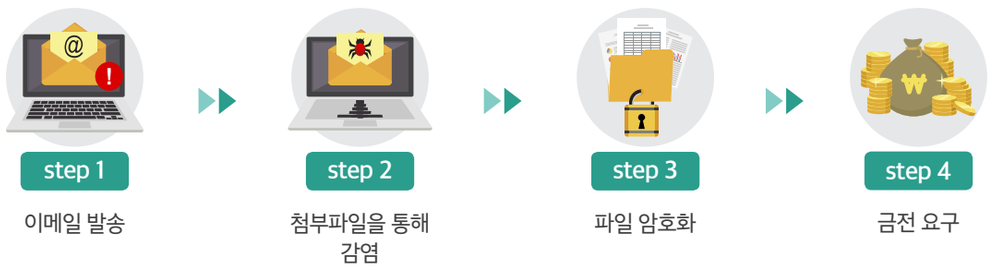
첫 번째 버전이 등장한 이후 지속적으로 발전해 왔으며, 랜섬웨어 중 가장 많은 공격 시도와 지속적인 고도화를 거듭하는 랜섬웨어로 꼽히고 있다. 갠드크랩은 “서비스형 랜섬웨어” 형태로 판매되고 있어, 다수의 공격자가 쉽게 악성코드를 구매하여 공격할 수 있는 특징이 있다.

’19. 6월 갠드크랩의 제작자는 “갠드크랩을 통해 총 20억 달러를 벌어들였으며, 앞으로는 갠드크랩 판매를 중단할 것”이라고 발표하였으나, 갠드크랩과 유사한 랜섬웨어가 지속적으로 유포되는 것으로 확인된다.

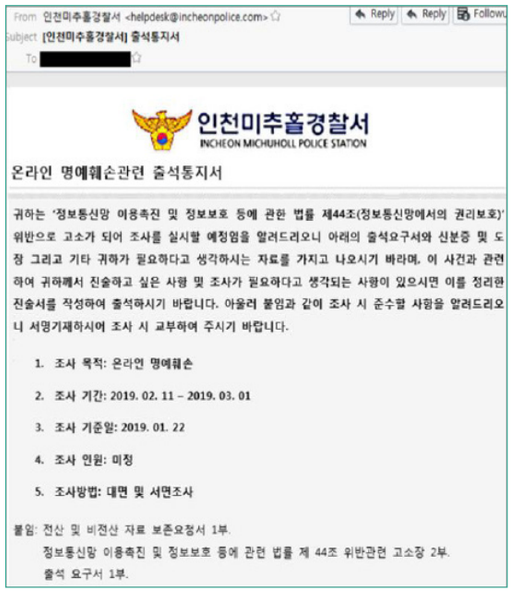
◆ 갠드크랩 랜섬웨어 유포경로 ◆

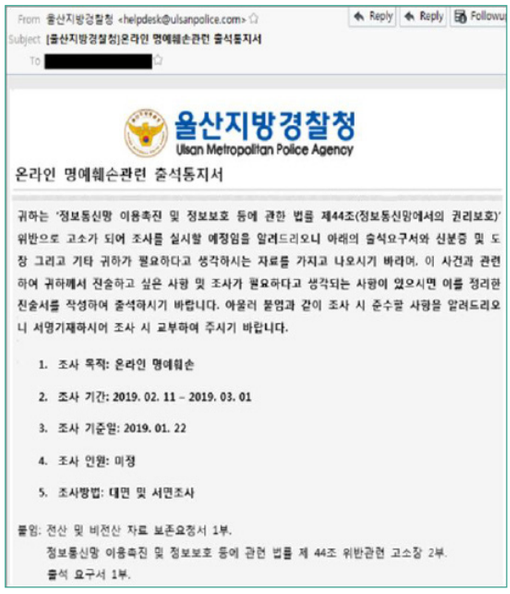


갠드크랩 감염 프로세스

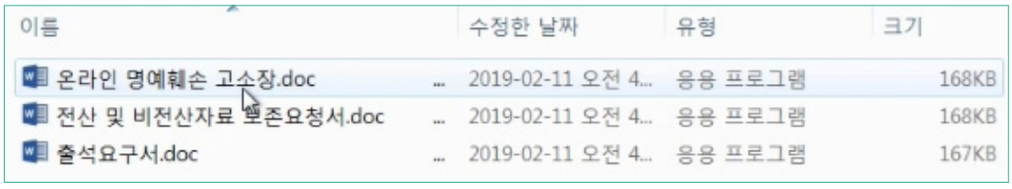


1 단계 [이메일 발송] 악성 이메일 열람

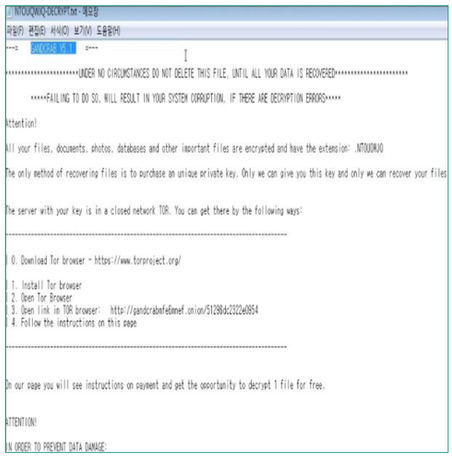




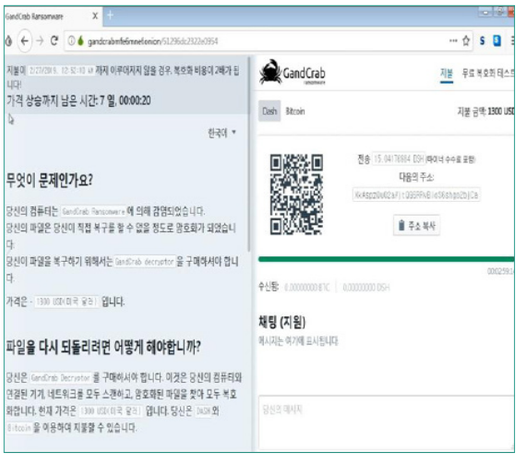
2 단계 [감염] 문서파일을 위장한 파일 실행 시



3 단계 [감염사실 고지] 다크웹에 접속하도록 유도



4 단계 [금전요구] 가상통화 입금요구



대처 방법

일부 랜섬웨어의 경우 '노모어랜섬(https://www.nomoreransom.org/ko/index.html)'을 통해 복구 가능하나, 무엇보다도 랜섬웨어를 예방하는 것이 가장 중요하다.

◆ 랜섬웨어 예방법 ◆

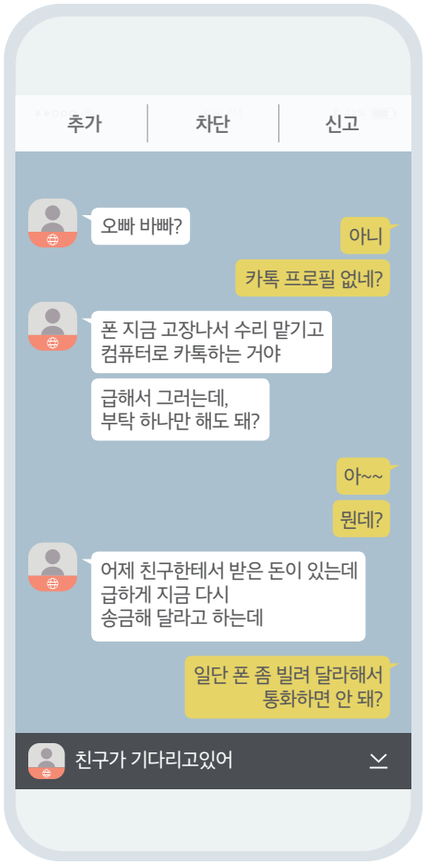
출처가 불분명한 메일의 첨부파일 및 링크 실행 금지

중요한 데이터는 별도의 외장형 장치에 반드시 백업

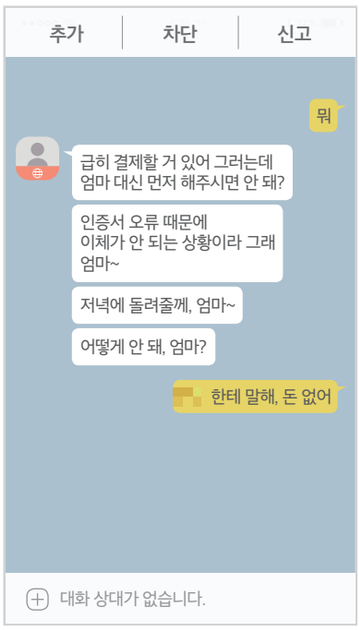
백신프로그램 및 운영체제·소프트웨어를 최신 버전으로 업데이트 유지

02 메신저피싱

이 사례는 실제 피해 사례로, 메신저피싱은 카카오톡, 네이트온 등 메신저를 이용하여 등록된 지인에게 메시지를 보내 금전을 요구하는 범죄이다.



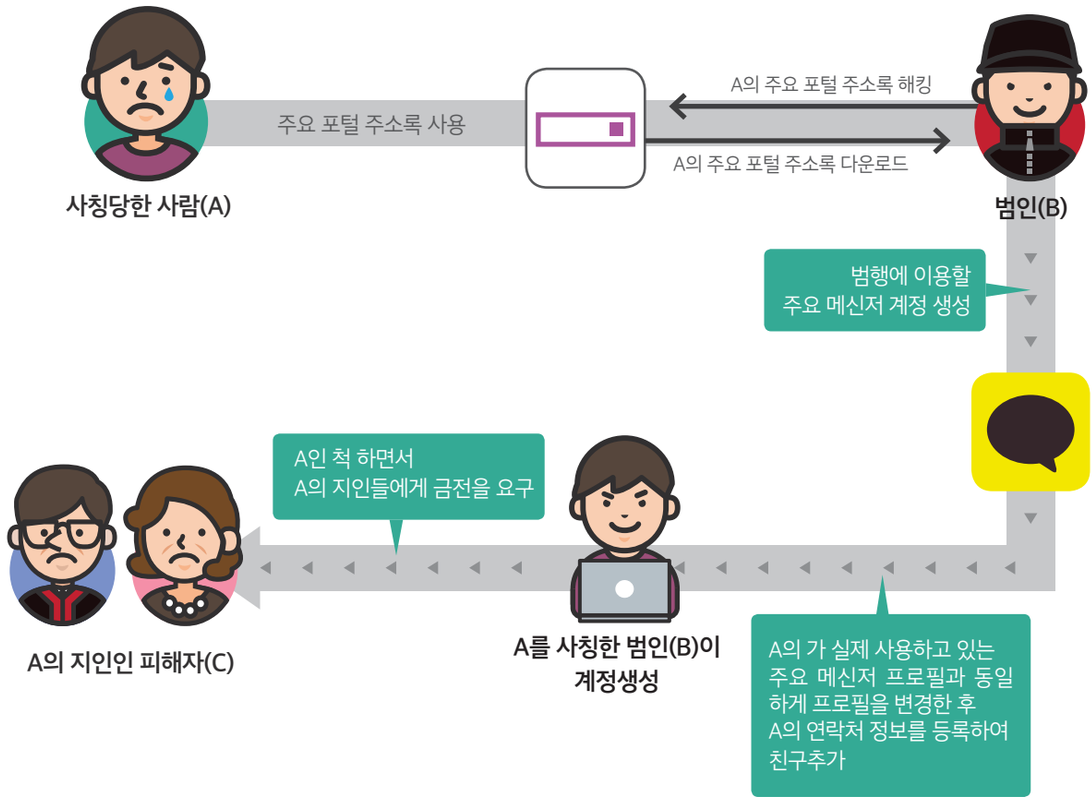
<프로필 변경에 대해 휴대폰 고장 핑계>



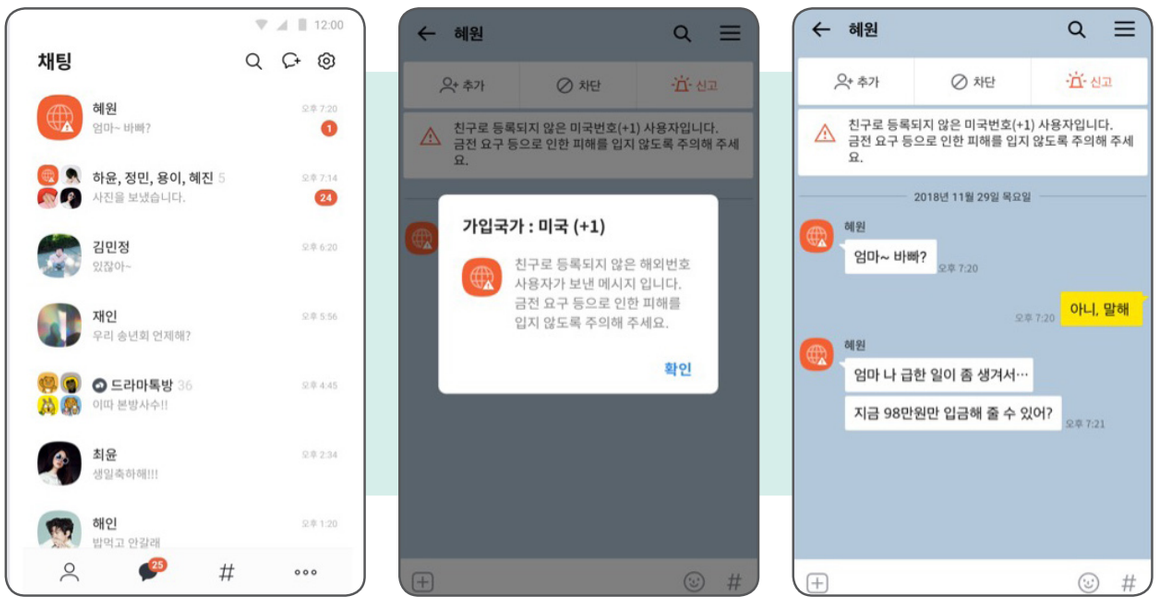
<부모, 이모, 삼촌 등 호칭을 특정>

메신저피싱 범행 수법

범인은 해킹 등을 통해 피해자의 인터넷상 주소록을 미리 확보한 후, 피해자의 메신저 프로필과 동일한 가짜 계정을 만든다. 그 후 범인은 인터넷상 주소록과 연동되어 친구 추가된 피해자의 지인에게 피해자인 척하며접근하여 긴급한 사유를 대면서 금전을 요구한다.



국내 거주자의 상당수가 K메신저를 이용하고 있기 때문에 K메신저를 이용한 메신저피싱이 많이 발생하고 있다. 이에 K메신저에서는 '19년 1월부터 해외 전화번호로 가입한 사용자에 대해서 지구본으로 표시하는 '글로벌 시그널' 기능을 제공하고 있다. K메신저 상에서 아래와 같은 지구본 모양의 상대방이 말을 걸어오는 경우, 이는 기존의 등록된 지인이 아니므로 주의해야 한다.



특히, 최근에는 범행 과정에서 피해금을 입금받는 방식으로 문화상품권의 핀번호를 받는 경우가 많다. 100만 원 이상 금액이 송금·이체된 경우, 입금 후 30분 간 자동화 기기를 통한 인출·이체가 지연되는 지연인출제도를 우회하기 위해서다.

◆ 문화상품권 이용 메신저피싱 수법 및 특징 ◆

메신저피싱 과정에서 문화상품권 대리 구매를 부탁

- 편의점 구매 직후 문화상품권 고유번호(PIN) 사진촬영 및 그 사진파일 전송 요구
- 사진으로 전달받은 상품권의 고유번호를 즉시 타인에게 재판매

대부분 50대 이상, 스마트폰·메신저사용 범죄에 취약

- 편의점은 문화상품권 판매시 금액 제한 (10~100만원)을 두고 있어, 피해자가 여러 점포를 찾아다니며 구입하고 있는 상황

메신저피싱 예방법

메신저피싱으로 인한 피해를 예방하기 위해서는 가족, 친지 등 지인이 메신저로 금전을 요구하는 경우, 반드시 전화로 본인 및 사실 여부를 확인하여야 한다. 상대방이 통화할 수 없는 상황 등을 들어가며 본인 확인을 회피하는 경우, 직접 신분을 확인할 때까지는 금전요구에 응하지 말아야 한다. 만약, 금전을 이미 송금한 경우라면 지체 없이 112(경찰청) 또는 해당 금융회사로 지급정지 신청을 하여 인출을 막아야 한다.

또한, 인터넷상 주소록과 메신저에 자체 보안 설정을 해두고, 보안 프로그램을 최신 버전으로 업데이트 해야 한다. 평소 이메일이나 휴대폰 문자메시지를 확인할 시 '출처가 불분명한 파일'은 열지 말고 즉시 삭제하여야 한다. 이와 더불어, 정기적으로 메신저 비밀번호를 변경하여 해킹 및 개인정보 유출을 예방하여야 한다.

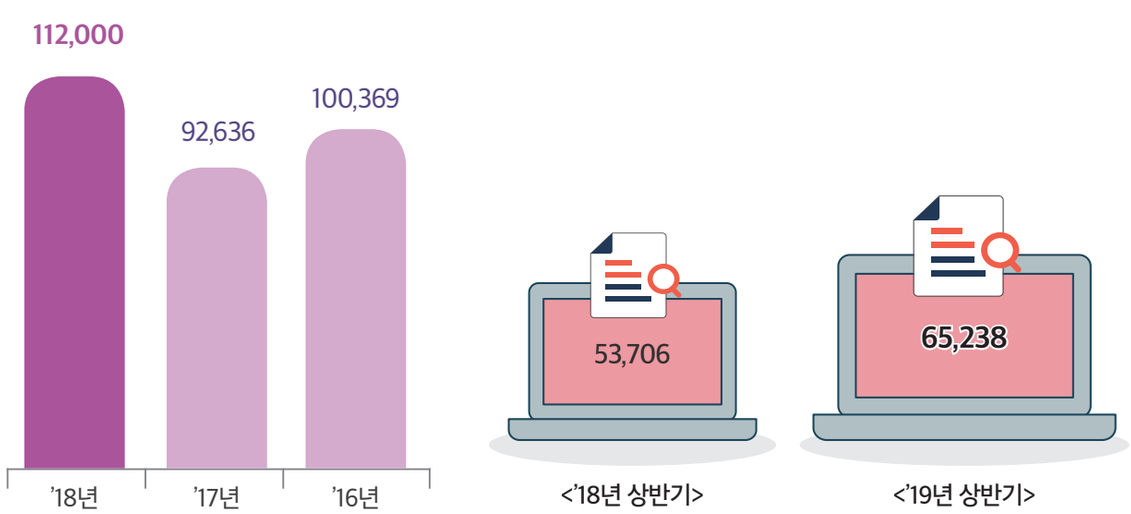
03 인터넷사기

통계 및 현황

최근 인터넷과 스마트폰을 통한 온라인 전자상거래의 활성화로 인터넷사기가 꾸준히 증가하고 있으며, '19년 6월말 기준으로 인터넷사기 발생 건수는 전체 사이버범죄의 75.9%(65,238건)로 가장 큰 비중을 차지하고 있다.

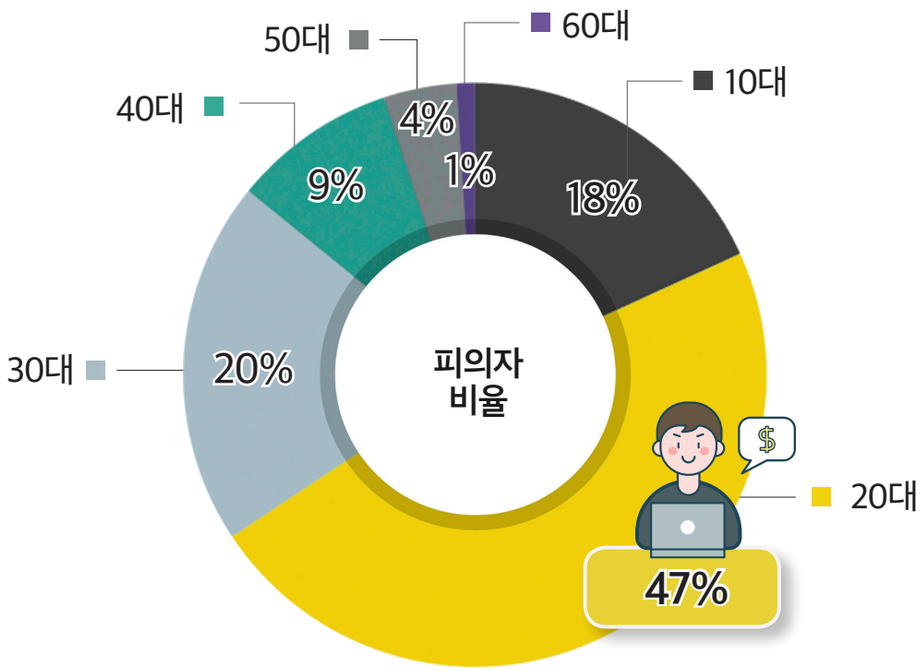
인터넷사기 발생 건수

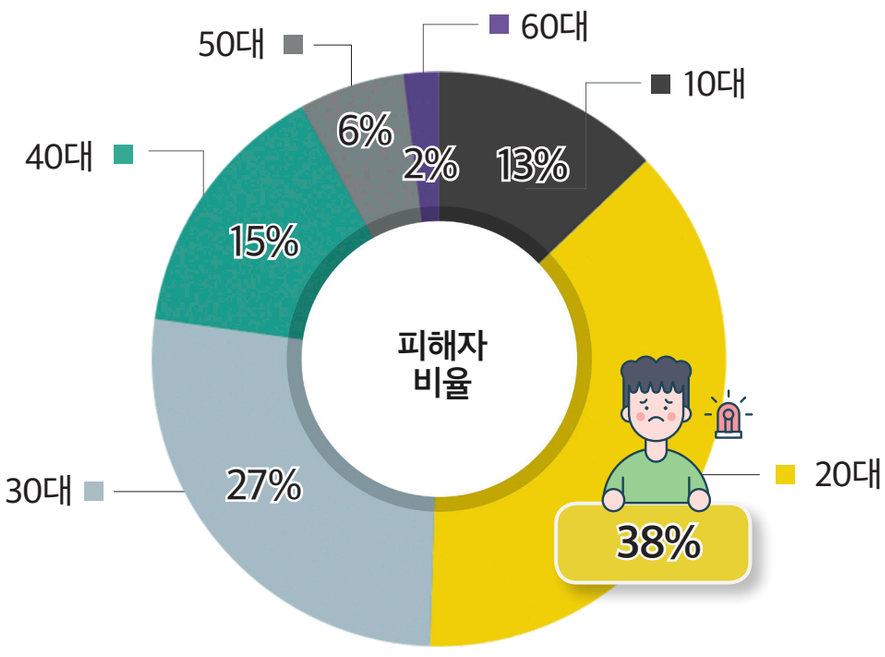
(단위 : 건)



인터넷사기 관련 전체 피의자의 67%, 피해자의 65%를 '20~30대'가 차지한다. 인터넷을 통한 재화와 용역의 거래에 익숙한 20~30대 층에서 사기 범죄 또한 가장 활발히 발생하고 있는 것으로 보인다.
('18년, 경찰청 통계자료 기준)

연령별 인터넷사기 피의자·피해자 분포

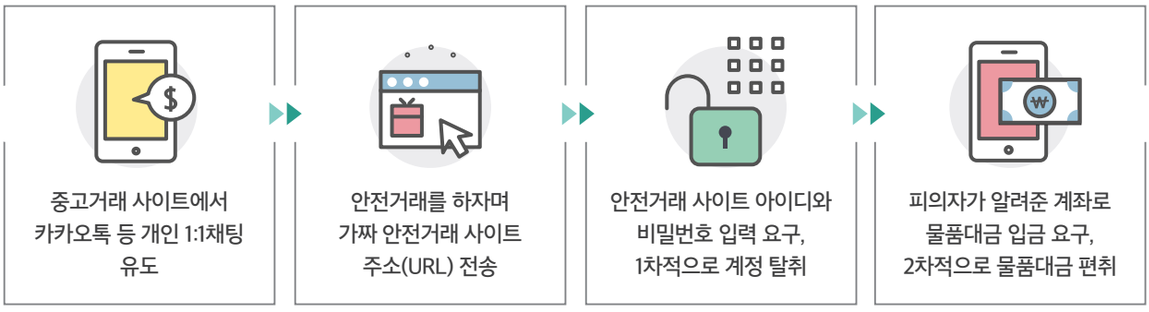




인터넷사기 유형

인터넷사기에 거래되는 물품은 전자기기, 유아용품, 콘서트 티켓, 게임 아이템, 상품권 등 매우 다양하다. 이 중에서 휴대폰, 상품권 등 고가의 물품은 주로 가짜 안전거래 사이트를 이용한 조직적·지능적 범죄 형태로 이루어진다.

◆ 가짜 안전거래 사이트 이용 범행 수법 ◆



상대방이 안전거래를 하자며 안전거래 사이트 주소(URL)를 보내올 경우 가짜 안전거래 사이트일 수도 있으니 주의해야 한다. 가짜 안전거래 사이트 주소(URL)는 육안으로 식별이 어렵기 때문에 반드시 '경찰청 사이버캅 앱'의 '가짜 안전거래 사이트 확인' 기능을 통해 확인하여야 한다.

※ 경찰청 사이버캅 앱은 구글 플레이스토어, 원스토어, 애플 앱스토어에서 무료로 다운로드 가능함.

<메인 화면>

<안전거래사이트 식별>

경찰청 사이버캅 앱에서는 국내에서 주로 사용되는 5개의 안전거래 사이트와 비교하여 가짜 안전거래 사이트인지 여부를 확인할 수 있는 기능을 제공하고 있음

◆ 가짜 안전거래 사이트 예시 ◆

진짜 사이트	가짜 사이트
• pay.naver.com	• pay.naver.pages64.com
• www.auction.co.kr	• pay.naver.com-cafejoonggonara11.ga
• www.unicro.co.kr	• auction.pige19.com
	• uniocrro-co-kr.com

※ 해당 예시에서 64, 11, 19 등의 숫자를 이용하여 변경한 가짜 안전거래 사이트가 다수 발견되고 있음

네이버페이 등 실제 안전거래 사이트의 경우에는 가입 시 등록한 주소, 전화번호 등이 거래 시 자동으로 현출되고, 계좌 예금주명이 '네이버페이' 등으로 고정되어 있다. 따라서 거래 시 주소, 전화번호 재기입을 요구하거나 계좌 예금주명이 개인 이름으로 되어 있는 경우 사기일 가능성이 높으니 주의해야 한다.

이 외에도 인터넷사기를 예방하기 위해서는 판매자와 직접 만나서 대면 거래를 하고, 부득이하게 비대면 거래 시에는 경찰청 사이버캅 앱*을 통해 상대방의 전화번호나 계좌번호에 대한 피해신고 이력을 확인해야 한다.

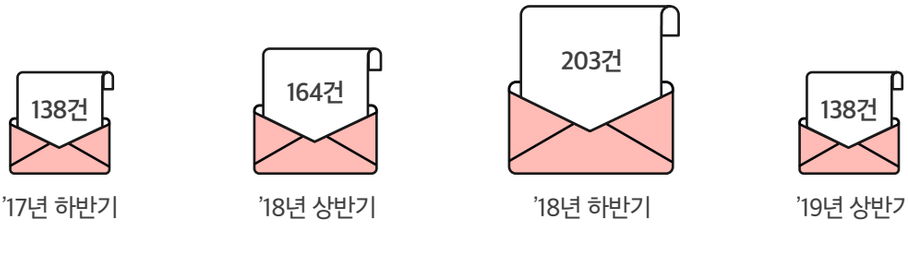
* 경찰청 사이버캅 앱
최근 3개월 간 3회 이상 인터넷사기로 피해신고 접수된 전화·계좌번호를 직접 검색할 수 있는 서비스를 제공하고 있음

04 이메일무역사기

통계 및 현황

이메일무역사기는 이메일 해킹·유사이메일 주소 이용 등의 방법을 통해 "거래계좌를 변경해 달라"는 이메일을 발송하여 물품대금을 중간에서 가로채는 범죄이다.
'18년 기준, 전체 사이버범죄 중 이메일무역사기 발생비율은 0.2%(367건)이지만, 한 건 당 피해액은 4,186만원으로 가장 많다. 발생 건수는 '17년 하반기 138건에서 '18년 상반기 164건, '18년 하반기 203건으로 증가 추세를 보이다가, '19년 상반기 138건으로 감소했다.(경찰청 KICS 통계 기준)

이메일무역사기 발생 건수



최근 세계 각국의 법집행기관, IT 기업은 나날이 증가하는 이메일무역사기에 이목을 집중하고 있다. 특히 미국 FBI는 이메일 무역사기를 '18년 핫토픽으로 선정하기도 하였다. FBI 인터넷범죄신고센터(IC3, Internet Crime Compliant Center)에 신고된 이메일무역사기는 '18년 한 해 동안 351,936건, 피해액은 27억$(US)을 넘어섰다고 한다.(FBI, 2018 인터넷 범죄 보고서)

이메일무역사기 유형 및 특징

이메일무역사기는 보통 이메일 해킹(Email hacking), 유사이메일 주소 이용(Domain Name Spoofing), 발신자 명의 변경(Display Name Deception) 등 3가지 유형으로 분류할 수 있다.

이메일 해킹은 먼저 거래상대방의 이메일 계정을 해킹해 거래내역, 절차, 문구 등을 훔쳐보는 것으로 범행을 시작한다. 해킹된 이메일을 통해 거래 과정을 지켜보다 대금 지급 시기가 되면 "세금 문제 등으로 계좌에 문제가 생겼다"고 속여 피의자의 계좌로 입금을 요구한다.

이메일 해킹에는 스피어피싱*, 스미싱, 해킹 등 다양한 방법이 이용된다.
취업을 가장한 이력서, 홍보 이메일 등의 첨부파일에 악성코드를 삽입하는 방법이 가장 많이 이용되고 있다. 최근에는 특정 웹사이트에 접속하는 것만으로도 악성 프로그램에 감염(드라이브 바이 다운로드 공격)될 수 있어 주의하여야 한다.

---

* 스피어 피싱(Spear phishing)
'작살로 물고기를 잡다'라는 뜻에서 유래되어 불특정 다수가 아닌 '특정 대상을 타켓'으로 하는 공격 기법을 말한다.

유사 이메일주소 이용 수법은 거래상대방의 이메일 주소와 유사한 이메일 주소를 만들어 속이는 방법이다. 우리나라에서 가장 많이 발생하고 있는 유형으로, 특정 문자 삽입·순서 변경, 1과 l(L) 등 혼동하기 쉬운 문자 변경 등의 수법이 있다.

◆ 유사 이메일주소 이용 수법 예시 ◆

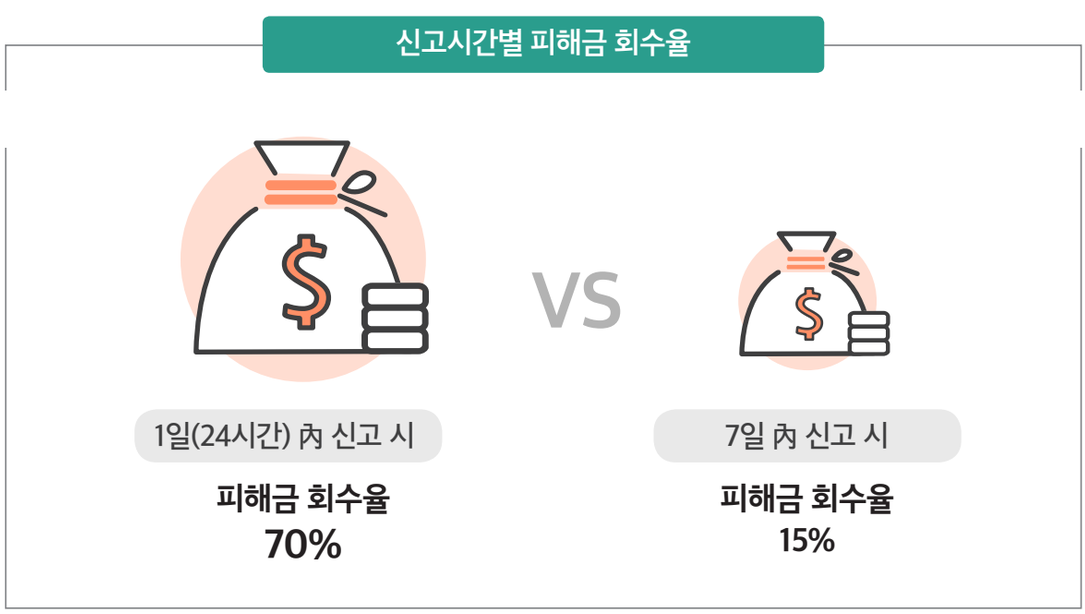
발신자 명의 변경 수법은 회사의 대표이사 등 비교적 직책이 높은 임원의 이름을 사칭하여 재무담당 직원에게 송금을 지시하는 이메일을 보내는 방법이다.
이 방법은 최근 미국에서 발생한 이메일무역사기의 63% 가량을 차지할 정도로 비중이 증가하고 있다. 향후 국내에서도 이와 유사한 범행수법이 생길 수 있으니 유의해야 한다.

이 외에도 기업의 급여 지급 목록에 침입해서 범죄자의 계좌를 추가하거나, 직원을 가장해 월급 통장을 새롭게 등록하는 등 급여 관련 이메일 피싱 수법이 새롭게 발견되고 있다.

대응 방법

이메일무역사기에 대처하기 위해서는 무엇보다 예방이 중요하다. 범죄 유형과 방법을 지속적으로 교육하여 구성원들의 경각심을 제고하여야 한다. 경찰에서는 '사이버범죄 예방교육 전문강사(전국 100여 명)'를 통해 학교·기업 등을 대상으로 사이버범죄 예방교육을 실시하고 있다.

사기 피해를 인지하면 즉시 경찰과 금융기관에 신고하여야 한다. 경찰에서는 인터폴 등 국제기구나 해외의 법집행기관과 국제공조를 통해 피해금 회복과 피의자 검거에 최선을 다하고 있다. 신속한 신고는 피해 회복에 있어 가장 중요하다. 일주일 이내에 경찰이나 금융기관에 신고하지 못하면 송금액이 인출되어 버린 경우가 많아 피해 회복이 쉽지 않을 수 있다. 미국 FINCEN(Financial Crimes Enforcement Network, 재무부 산하의 금융범죄 단속국)에 따르면 신고가 지체될수록 피해금 회수율이 급격히 낮아진다.



출처: FINCEN 보고서

마지막으로 백신을 최신 버전으로 업데이트 하고, 이메일에 첨부된 파일 실행 시 주의하여야 한다.
또한, 거래상대방이 수취계좌 변경을 요청하거나 사내 대표이사가 변경된 계좌로 입금을 지시할 때에는 반드시 재확인하여 피해를 입지 않도록 유의하여야 한다.

05 매크로 프로그램 이용 티켓구매

유명 가수의 콘서트나 주요 스포츠 경기 티켓이 오픈될 때마다 매크로 프로그램을 이용한 대량 구매에 대한 논란이 많다. 매크로를 이용해 구매한 티켓들을 웃돈을 얹어 다시 재판매하는 행위도 문제가 되고 있다.

매크로(Macro)는 마우스나 키보드 등으로 여러 번 실행하는 동작을 한 번의 명령으로 자동 실행시키는 프로그램이다. 이는 일정 시간에 해당 프로그램을 자동적이고 반복적으로 실행하게 하여 작업시간을 크게 단축시킨다.

이러한 매크로 프로그램의 매매는 각종 포털사의 카페나 개별 사이트, 트위터 등 SNS를 통해서 쉽게 이뤄진다.

<아이엠마케터 사이트 상 판매 글>

<트위터 상 매크로 판매 글>

처벌 법규

오프라인 상에서의 암표 판매행위는 경범죄처벌법(제3조) 대상이나, 매크로를 이용하여 티켓을 구매하는 행위는 처벌이 어려운 것으로 여겨져 왔으며, 이에 처벌 규정을 담은 법안(경범죄처벌법 개정안 등)이 현재 발의되어 국회에 계류 중이다.

단, 매크로를 활용해 여러 명인 것처럼 가장해 티켓을 대량 구매하는 경우(업무방해)나 예매사이트를 다수 접속해 서버 장애를 발생시킨 경우(컴퓨터장애업무방해)에는 형법상 처벌이 가능하다.

또한, 개인정보를 도용하여 아이디(ID)를 다수 생성한 경우(개인정보누설)나 티켓사이트에 불법적으로 접근한 경우(정보통신망 침해)에는 정보통신망법 위반으로 처벌받을 수 있다.

처벌 규정

			징역	벌금
형법	제314조 제1항	**(업무방해)** 허위사실을 유포하거나, 위계 또는 위력으로써 사람의 업무를 방해	5년 이하	1,500만원 이하
형법	제314조 제2항	**(컴퓨터장애업무방해)** 정보처리에 장애를 발생시킴으로써 사람의 업무를 방해	5년 이하	1,500만원 이하
정보통신망법	제28조의2 제2항	**(개인정보누설)** 영리 또는 부정한 목적으로누설된 개인정보를 제공받은 경우	5년 이하	5,000년 이하
정보통신망법	제48조 제1항	**(정보통신망침해)** 정당한 접근권한 없이 또는 접근권한을 넘어 정보통신망에 침입	5년 이하	5,000년 이하

◆ 관련 사례 ◆

타인의 인적사항으로 만든 아이디 94개로 입장권 10,186장을 예매한 행위는 혼자서 한 입장권 구매를 마치 여러 명의 구매자가 각자 하는 것처럼 가장한 행위로, 이는 1인 당 예매 제한 매수를 둔 사이트 관리자의 착오나 부지를 일으킬 목적으로 행하여진 행위로서 업무방해죄의 위계에 해당한다.
(대전지법 2017고단7, 현재 대법원 계류 中)

크롤링(자동정보수집) 프로그램을 이용해, 웹사이트 서버를 접속 중단하게 한 업체 OOO에 대하여 컴퓨터장애업무방해죄를 적용하여 현재 재판 진행 중
('19. 3. 29. 언론보도)

해외 처벌 법규

미국 연방법률인 '온라인티켓판매법'(Better Online Ticket Sales Act of 2016)은 온라인 상 불법적 프로그램을 이용한 티켓 구매행위와 재판매를 금지하며, 판매하게 될 경우 연방거래위원회(FTC : Federal Trade Commission)의 제재 대상이 되도록 규정하고 있다.

미국 뉴욕주의 '예술문화법'(Arts and Cultural Affairs Law)은 티켓 구매를 위해 불법 프로그램을 사용하거나, 이를 통해 취득한 티켓을 재판매 또는 재판매를 위해 타인에게 제공하는 경우 500달러 이상 1,500달러 이하의 벌금에 처하도록 규정되어 있다. 재판매를 통해 얻은 수익은 전액 몰수된다.

미국의 불법 프로그램을 통한 암표매매 처벌 규정

온라인티켓판매법(연방법률)

- 불법 프로그램 이용한 티켓 구매 및 재판매 금지
- 불법 취득한 티켓 재판매 시 연방거래위원회(FTC) 제재
- 주 정부는 온라인 암표 매매범에게 민사소송 제기 가능

예술문화법(뉴욕주법)

- 불법 프로그램 이용한 티켓 구매 및 재판매 시 최대 1,500달러 벌금
- 벌금형을 받고 재범을 한 경우 최대 5,000달러 벌금
- 수익 목적으로 불법 프로그램 이용 및 불법 프로그램 제작 등 관여 시 최대 금고형 선고

경찰은 관련 업체들과 협력하여 매크로 프로그램을 이용하여 티켓을 대량으로 구매한 후, 그 티켓을 암표로 판매하는 행위에 대해 지속적으로 단속할 계획이다.

III 최근 사이버위협 트렌드

01 폼재킹 증가

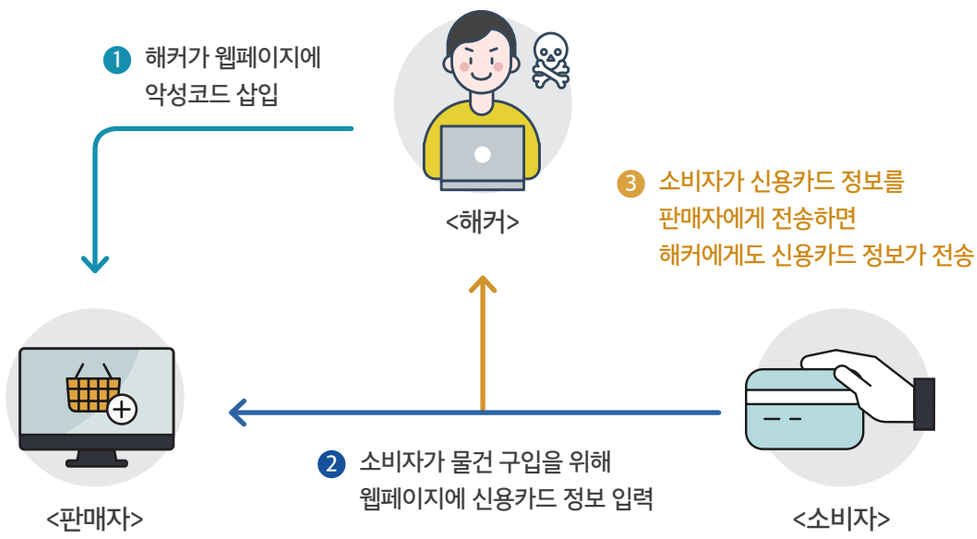
<시만텍社, 인터넷 보안 위협 보고서 vol. 23>의 내용을 발췌하여 작성하였음.

최근 온라인 쇼핑몰에서 구매자의 신용카드 등 금융정보를 탈취하는 '폼재킹*(Formjacking)'이 증가하고 있다.

* 폼재킹(Formjacking)
인터넷 쇼핑몰 등 웹사이트를 악성코드에 미리 감염시켜 사용자가 입력한 정보가 담긴 양식(Form)을 중간에서 납치(Hijacking)한다는 Form과 Hijacking의 합성어

해커는 '특정 프로그램(자바스크립트)으로 제작된 결제 웹페이지'를 사용하는 쇼핑몰을 공격 대상으로 하였고, 온라인 소매업체에서 흔히 사용하는 챗봇이나 고객 리뷰 위젯 등에 미리 악성코드를 감염시켜 폼재킹을 시도하였다.

범죄 흐름도



탈취당한 금융정보는 다크넷 등에서 45달러(약 5만 원)에 거래되고 있는데, 공격당한 웹사이트 수를 고려하면 범죄수익이 상당한 규모일 것으로 보인다.

◆ 해외 피해 사례 ◆

'18.8월 British Airways(영국항공)의 웹사이트 및 모바일 어플리케이션이 폼재킹 공격을 받아 고객의 카드 결제정보 38만여 건 유출됨

그 외 티켓마스터(美, 콘서트·뮤지컬 티켓예매 사이트)·Kitronik(英, 전자제품 소매업체)·VisionDirect(英, 컨택트렌즈 판매업체) 등에서 피해사례 다수

이와 같이 폼재킹은 보안에 취약한 중소규모 쇼핑몰에서 발생할 가능성이 높고, 해외 쇼핑몰(자바스크립트 결제방식을 사용한 사이트)에서 주로 발생하고 있어, 해외 직구 등으로 쇼핑몰을 이용하는 사용자는 신뢰할 수 있는 웹사이트인지 여부를 반드시 확인해야 하고, 신뢰할 수 없는 사이트의 경우 불필요한 정보입력을 하지 않는 등 각별한 주의가 필요하다.

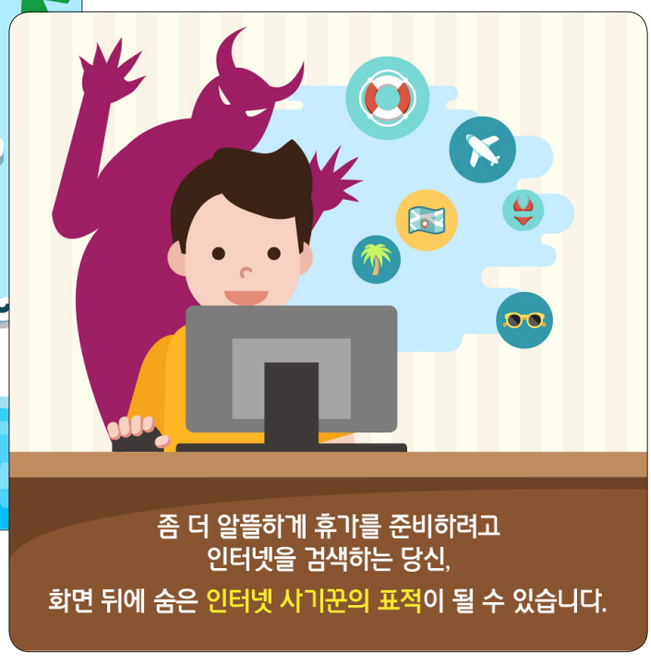
02 이메일을 매개로 한 사이버위협 증가(Cisco社, Click with Caution)

KISA 발행 「2019년 2분기 사이버위협 동향보고서」의 내용을 발췌하여 작성하였음.
(전문은 https://www.boho.or.kr/data/reportList.do를 참고하시기 바랍니다.)

'19. 4월 기준 전체 이메일 중 85%가 스팸메일이다.
악성코드 배포의 92.4%, 피싱의 94%가 공격 수단으로 이메일을 활용하고 있으며 이메일무역사기의 67%도 웹메일을 기반으로 하고 있다. 또한, 이메일에 첨부된 Microsoft Office 문서의 약 40%가 악성코드일 정도로 이메일 첨부파일을 통한 악성코드 유포는 심각한 상황이다. 이메일을 통한 사이버 범죄는 경제적 이득을 목적으로 한 경우가 대부분이다.

이메일 수신자는 이메일의 내용에 속아, 첨부파일을 실행할 가능성이 높기 때문에 피해를 당하기 쉽다. 따라서 의심스런 이메일을 받았을 때에는 첨부파일을 실행하지 않는 것이 중요하다.

[카드뉴스] 하계휴가철 인터넷사기 예방



좀 더 알뜰하게 휴가를 준비하려고
인터넷을 검색하는 당신,
화면 뒤에 숨은 인터넷 사기꾼의 표적이 될 수 있습니다.

본격적인 휴가철을 맞아 휴가용품, 여름가전과 관련한
인터넷 사기가 증가할 것으로 예상됩니다.


인터넷 사기 피해를
예방하려면?
왜 아무도
안속는거야ㅠㅠ
'사이버캅'에
상대방 전화·계좌번호 조회는 필수!
전화
의심되는 전화/계좌번호를 입력하세요
사이버캅
안전거래를 위한 번호검색
최근 3개월간
3회 이상 인터넷사기로
경찰에 신고된
전화·계좌 번호를
확인할 수 있습니다.


가급적 직접 만나 물건과 돈을 교환하기!
낮 시간에 사람들이 많은 곳에서 만나 거래하면
불필요한 분쟁이나, 위험 발생 가능성을 줄일 수 있어요
직거래가 힘들다면,
안전거래서비스를 이용하세요!
1 대금지급
3 대금지급
구매자
안전거래
서비스
판매자
2 상품배송
안전거래는 구매자가 보낸 물품 대금을 보관하고 있다가
구매자가 상품을 정상적으로 받은 것을 확인하면
판매자에게 대금을 보내주는 서비스입니다


한번 더 확인
판매자
http://www.pay□□□□/
오후 3:57
단, 상대방이 안전거래를 한다면서 가짜 URL을 보내,
물품 대금과 개인정보를 빼돌리는 경우도 있으니 주의하세요.
'사이버캅'앱을 통해 가짜 안전거래사이트 여부 확인!!!
경찰
즐겁고 행복한 휴가를 위해
거래 전 한번 더 살펴보세요.
휴가철 인터넷 사기!
간단한 원칙만 지키면,
충분히 예방할 수 있습니다!!!
인터넷 사기 피해를 당하시면,
경찰청 사이버안전국 홈페이지
cyberbureau.police.go.kr 또는
가까운 경찰서 민원실을
방문해 신고해 주세요!