www.police.go.kr

2018년 3분기
사이버위협 분석 보고서

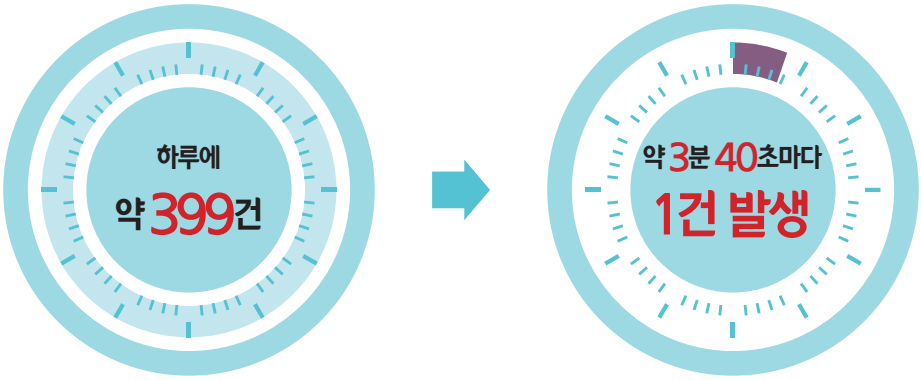
KOREAN NATIONAL POLICE AGENCY

경 찰 청
KOREAN NATIONAL POLICE AGENCY

목 차

Ⅰ. 3분기 사이버범죄 동향

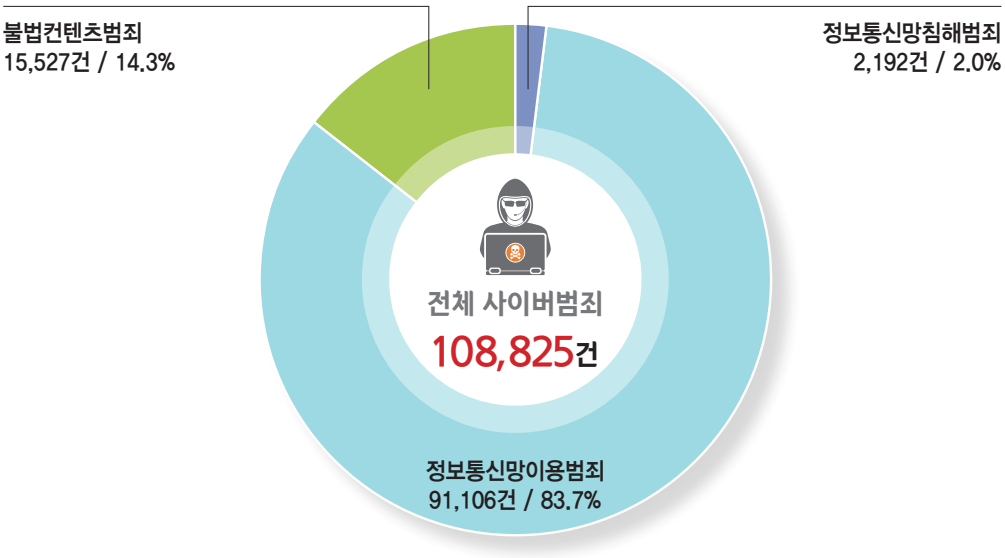
사이버범죄는 올해 3분기까지 총 108,825건이 발생하였으며, 전년도 같은 기간(101,653건)과 비교해보면 발생건수가 약 7.1% 증가하였다.



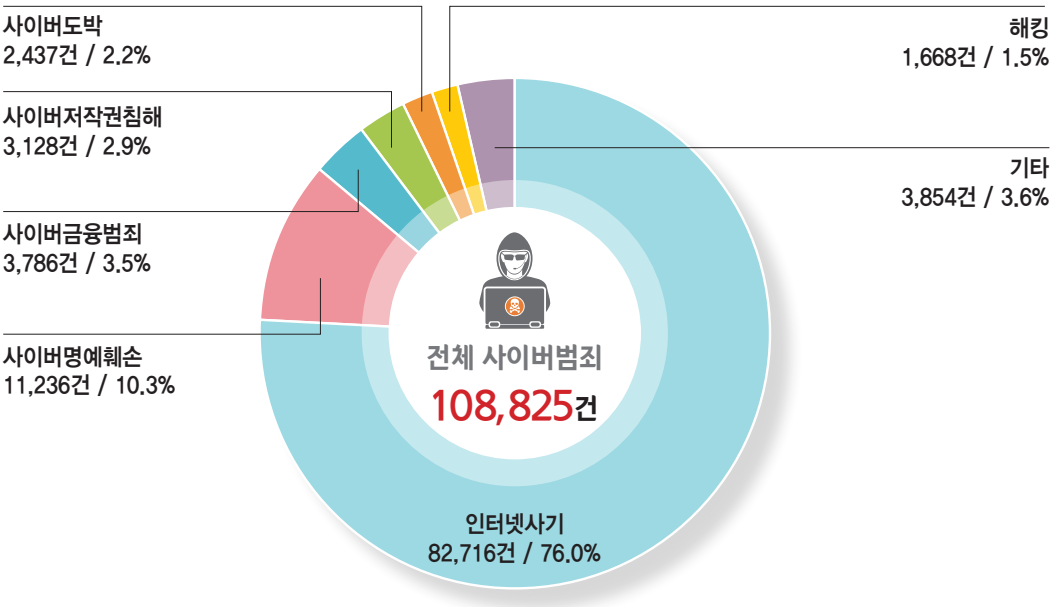
해킹, 악성프로그램 유포 등 정보통신망에 불법적으로 침입하는 방식으로 저지른 범죄(정보통신망침해범죄)는 8.6% 감소한 반면, 인터넷사기, 사이버금융범죄 등 정보통신망을 이용해 저지른 범죄(정보통신망이용범죄)는 8.9% 증가했다. 사이버음란물, 사이버도박 등 법이 금지하는 재화를 생산 · 유포하는 범죄(불법컨텐츠범죄)는 0.5% 소폭 감소하였다.

세부적으로 살펴보면, 직거래사기 · 사이버명예훼손(모욕) · 피싱 · 이메일무역사기 · 몸캠피싱의 발생건수가 증가한 반면, 사이버도박 · 사이버저작권침해 · 파밍 등의 유형이 감소하였다.

사이버범죄 유형별 발생 비율(대분류)

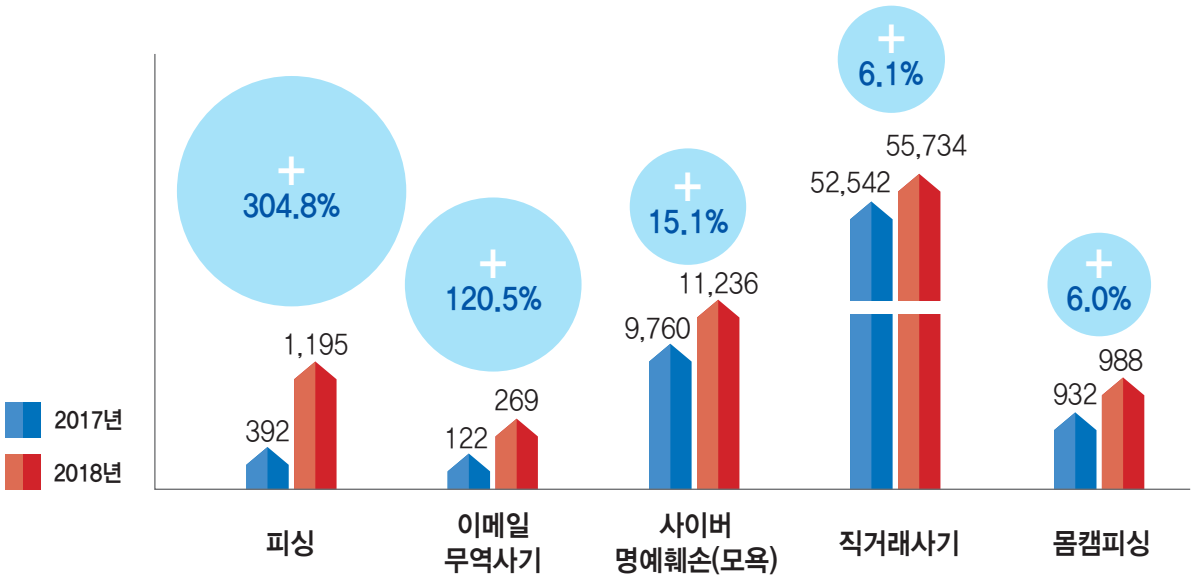


사이버범죄 유형별 발생 비율(중분류)

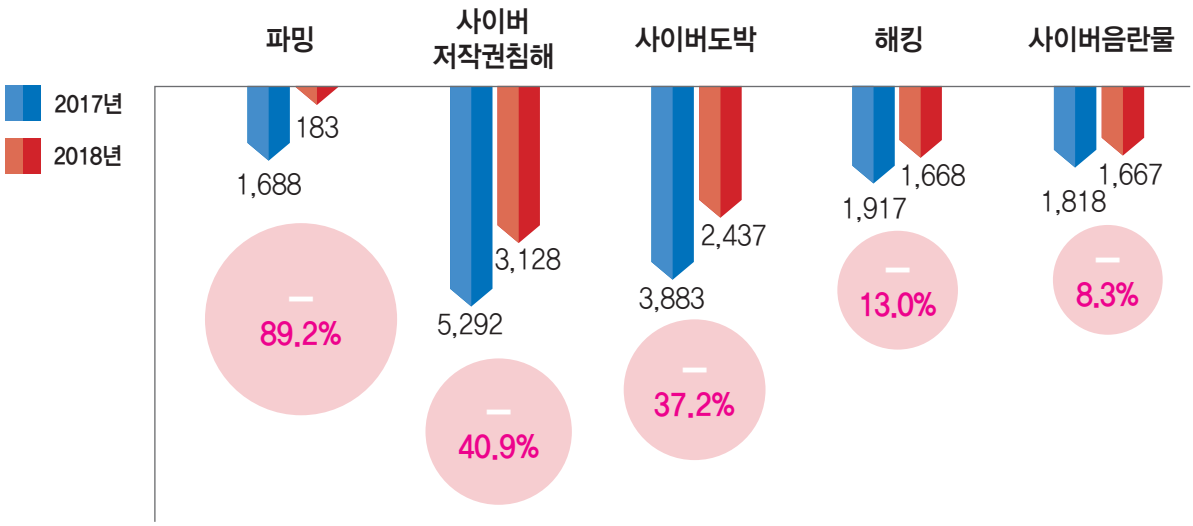


Ⅰ. 3분기 사이버범죄 동향

주요 발생 증가 유형 (단위 : 건)



주요 발생 감소 유형 (단위 : 건)

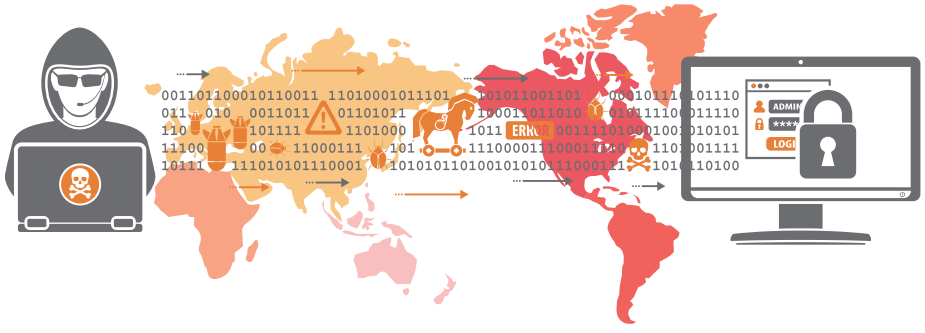


최근 사이버범죄는 크게 세 가지 양상을 보인다.

첫 번째로, 인터넷 사기는 여전히 사이버범죄의 대다수를 차지하며 발생 규모 또한 확대되고 있다. 3분기까지 인터넷 사기 발생건수는 82,716건으로 전체 사이버범죄의 76.0%를 차지했으며, 올해 11만 건에 근접할 것으로 예상된다. 특히, 허위 글을 게시하여 돈을 이체받는 인터넷 사기가 전통적인 수법이었으나, 가짜 안전거래 유도, 가짜 판매사이트 개설 등 피의자가 보다 적극적인 속임수를 사용하는 사례가 많아지고 있다. 인터넷 사기 수법의 변화는 'Ⅱ. 주요 사이버범죄 사건'에서 확인할 수 있다.

두 번째로, 신뢰를 기반으로 피해자를 속여 정보를 빼돌리는 사이버범죄가 급증했다. 이러한 범죄의 대표적인 유형은 '피싱'으로 올해 1,195건이 발생했다. 이는 작년 동기간(392건)과 비교해 볼 때 3배 이상 증가한 것이다. 특히 올해는 지인을 사칭해 송금을 요구하는 메신저 피싱이 SNS와 모바일 메신저를 통해 광범위하게 발생하고 있다. 피싱 메일 또한 점차 교묘해지고 메일수신자가 읽을 수밖에 없게끔 유인하는 형태로 유포되고 있다. 피싱 메일의 양상은 'Ⅲ. 최근 사이버위협 트렌드'에서 확인할 수 있다.

세 번째로, 범죄 수법이 지능화되고 있다. 최근 운영되는 대부분의 불법 사이트들은 해외 업체의 웹호스팅을 이용한다. 또한 IP를 우회하고, 인터넷에 널리 공개된 해킹 프로그램을 사용하여 수사기관의 추적을 피하고 있다. 또한 가상통화로 범죄자금을 세탁하는 사례도 증가하고 있다.



Ⅱ. 주요 사이버범죄 사건

사이버 성폭력 수사

경찰은 사이버성폭력을 근절하기 위해 2018년 8월 13일 사이버안전국장을 단장으로 하는 특별수사단을 설치해 집중 단속을 실시하였으며, 약 두달 반 동안 2,062명을 검거하고 88명을 구속하였다.(10. 20. 기준)

이들은 불법촬영물을 음란사이트에 게시해 광고수익을 얻거나 웹하드 사이트에 대량 업로드하고 포인트를 환전하는 방식으로 부당이득을 챙겼다. 또한 채팅 앱을 통해 알게 된 불상자와 성관계를 맺고 몰래 찍은 사진을 커뮤니티 사이트에 올리거나, 여학생을 대상으로 신체 특정 부분을 촬영하고 이를 해외 사이트에 유포하는 범행을 저질렀다.

사이버성폭력 단속 중간결과

- 해외에서 운영 중인 음란사이트 99곳을 단속해 55명을 검거하고 21명을 구속
- 특히, 불법촬영물 유통 카르텔의 주요 경로로 지목된 웹하드 업체 30개 중 20개 업체를 압수수색해 대표 6명 검거
- 이와 함께, 헤비업로더 136명 검거 및 9명을 구속하고 불법촬영자 1,298명, 음란물 유포자 774명을 붙잡아 각각 43명, 44명을 구속하고 위장형 카메라 판매자 25명을 검거

사이버 성폭력 수사

① 음란사이트 수사

경찰청에서는 음란사이트가 웹하드와 함께 음란물 유포의 핵심적인 유통플랫폼이라 판단하여 집중단속을 실시하였다.

이들은 미국 등 해외 서버를 임대하여 사이트를 개설해 수사기관의 추적을 피해왔다. 또한 스스로 음란물을 게시하지 않고 타 사이트의 음란물을 추출·복사하고 자신의 사이트에 자동적으로 재게시하는 방식을 사용하는 경우도 있었다. 또한 음성적 성매매 업소나 도박사이트 광고를 통해 수천만원에 달하는 광고 수익을 올리고 있었다.

이러한 음란사이트는 접속자의 PC에 악성코드를 설치할 수 있고, 설치된 악성코드는 해킹 등 또 다른 범죄에 악용될 수 있어 주의가 필요하다.

주요 검거 사례

- 해외(미국) 서버를 임대하여 음란사이트(ㅇㅇ닷컴) 운영을 통해 배너광고료 등으로 부당이득을 취한 운영자 2명 검거, 공범 추적 중 (9월, 인천청 사이버수사대)
- 해외(미국)서버를 임대하고 음란사이트(ㅇㅇㅇ이지, ㅇㅇ르, ㅇㅇ닷컴)를 운영하여 3,200만원의 부당이득을 취득한 운영자 1명 검거 및 구속 (9월, 전남청 사이버수사대)

② 웹하드 헤비업로더 수사

'헤비 업로더'란 저작권자의 허락을 받지 않고 웹하드에 각종 동영상, 프로그램 등 콘텐츠를 대량으로 올리고 이를 통해 얻은 웹하드 내 포인트를 환전하여 부당이득을 얻는 사람들을 말한다.

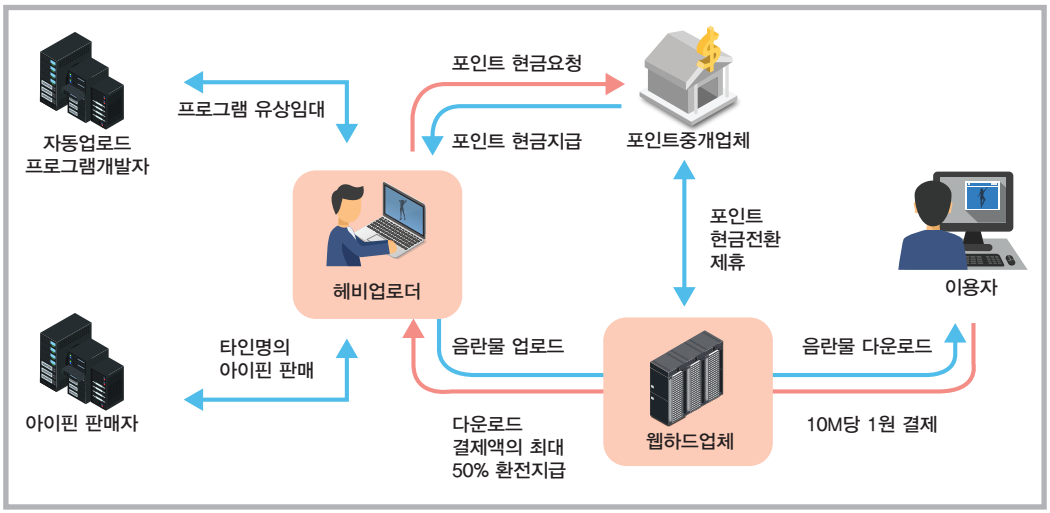
경찰청은 헤비업로더와 웹하드 운영자, 디지털장의사 등 불법촬영물 유통관련자들의 유착관계를 집중적으로 단속하고 있다.

헤비업로더는 타인 명의를 이용해 각 사이트에 계정을 생성하고 대량의 음란물을 게시해 왔다. 또한, 헤비업로더의 대량 업로드를 알고도 삭제조치를 하지 않은 웹하드 업체들에 대해서도 음란물 유포를 방조한 혐의로 수사가 진행 중이다.

Ⅱ. 주요 사이버범죄 사건

사이버 성폭력 수사

〈 범죄 흐름도 〉



주요 검거 사례

- 웹하드(ㅇ파일 등 5곳)에 음란물 7만6천여건 유포, 5천2백만원 상당 부당이득 취득한 헤비업로더 1명 검거 및 구속 (9월, 경북청 사이버수사대)
- 웹하드(ㅇㅇㅇ파일)에 음란물 3만7천여건 유포한 헤비업로더 3명 및 웹하드 운영자(방조혐의) 1명 검거 (9월, 경기북부청 사이버수사대)

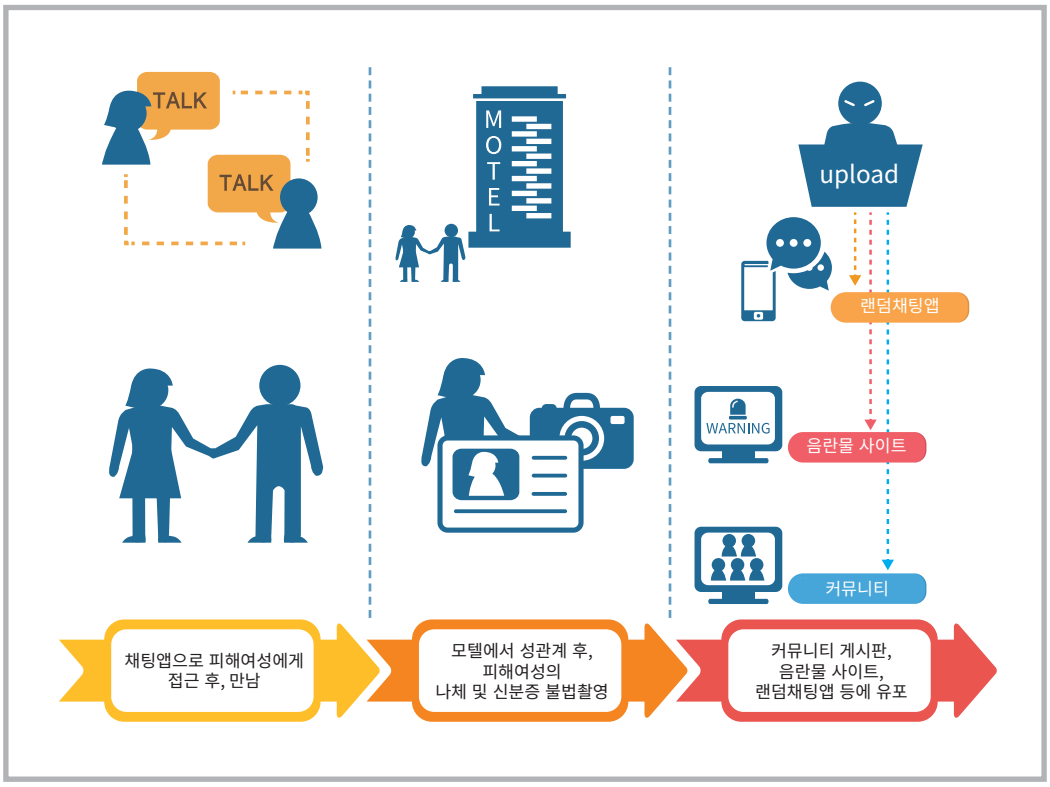
③ 커뮤니티 사이트를 통한 유포 수사

커뮤니티 사이트에는 커뮤니티 내의 입지를 높이고 자신의 지식 · 경험 등을 과시하기 위한 게시물이 올라오곤 한다. 이러한 심리가 타인의 알몸을 촬영하고 이를 유포하는 방식의 사이버 성폭력 범죄로 변질되기도 한다.

최근 채팅 앱을 통해 알게 된 이성과 성관계 후, 잠든 사이 자신의 나체모습과 신분증이 불법 촬영되어 인터넷 커뮤니티 사이트에 게시된 것을 확인하고 피해사실을 경찰에 신고한 사건이 있었고, 노년여성과의 성관계 장면을 촬영하여 게시한 자도 있었다.

사이버 성폭력 수사

〈 범죄 흐름도 〉



주요 검거 사례

- 채팅 앱을 통해 알게 된 피해자와 성관계 후, 피해자의 나체와 신분증을 함께 불법 촬영하여 커뮤니티 사이트에 유포한 피의자 검거 및 구속 (9월, 서울청 사이버수사대)
- 서울 종로의 모텔에서 노년의 피해여성과의 성관계 장면을 촬영 후 커뮤니티 사이트 등에 게시한 피의자 검거 및 구속 (8월, 충남청 사이버수사대)

④ 불법촬영물 유포 수사

카메라 등을 이용하여 성욕 또는 수치심을 유발할 수 있는 다른 사람의 신체를 동의 없이 촬영하거나, 그 촬영물을 촬영대상의 동의 없이 유포하는 것은 범죄 행위이다.

Ⅱ. 주요 사이버범죄 사건

사이버 성폭력 수사

그러나 여성을 대상으로 얼굴 · 다리 등 특정 부위를 촬영하여 텀블러 사이트 등에 게시하는 사건이 빈번하게 발생하고 있다.

일부 피의자들은 용돈 마련을 위해 불법촬영 후 이를 판매했으며, 구매자 중에서는 아동 음란물 소지 혐의로 처벌된 피의자들도 있었다. 아동 · 청소년 음란물은 현행법상 소지만으로 처벌이 되므로 누리꾼들의 각별한 경각심이 요구된다.

「아동 · 청소년의 성보호에 관한 법률」에서는 아동 · 청소년 이용 음란물임을 알면서 이를 소지한자는 1년 이하의 징역 또는 2천만원 이하의 벌금에 처하고 있다.

주요 검거 사례

- 텀블러 등에 ㅇㅇ시 소재 고등학교 여학생들의 얼굴 · 다리 등을 불법 촬영하고 촬영한 동영상을 유포 · 판매한 피의자 검거 및 구속 (8월, 경기남부청 사이버수사대)
- 학교기숙사에서 옷 갈아입는 청소년을 불법촬영한 영상물을 유포한 피의자 및 이를 다운로드 받아 소지한 혐의로 28명 검거 (8월, 경기남부청 사이버수사대)

메신저 피싱

메신저 피싱은 컴퓨터 메신저의 등장과 함께 시작된 고전적인 수법의 범죄이다. 최초 발생은 2009년으로 확인되며, 당시 많이 사용되었던 네이트온, MSN 메신저를 중심으로 메신저 피싱이 성행하였다. 기술발전 및 시대변화에 따라 컴퓨터 메신저 피싱은 카카오톡 등 모바일 메신저 피싱으로 변화하였다.

최근 수법은 피의자가 포털의 계정정보를 탈취, 계정에 연동되어 있는 주소록 등을 확보하여 피해자와의 관계를 확인하고 가짜로 만든 모바일 메신저 계정을 통해 피해자에게 접근하여 돈을 이체 받는 방식이다.

또한 지연인출을 회피하고 상대방에게 부담을 느끼지 않게 하기 위해 100만원 이하로 입금을 요구하는 경우가 많고 휴대전화가 고장났다는 사유를 들어 사칭된 실제 사람에게 전화를 하지 않도록 유도하는 사례도 확인된다.

메신저 피싱

주요 검거 사례

• 피해자의 카카오톡과 페이스북 메신저 계정을 해킹해 매형 A씨에게 "돈을 급히 송금할 것이 있는데 공인인증서가 안되서 힘들다. 괜찮으면 먼저 송금 좀 해달라."라고 속여 대포통장으로 96만원을 입금받는 등 피해자 16명으로부터 3,100만원을 편취한 피의자 검거 (4월, 일산서부경찰서)

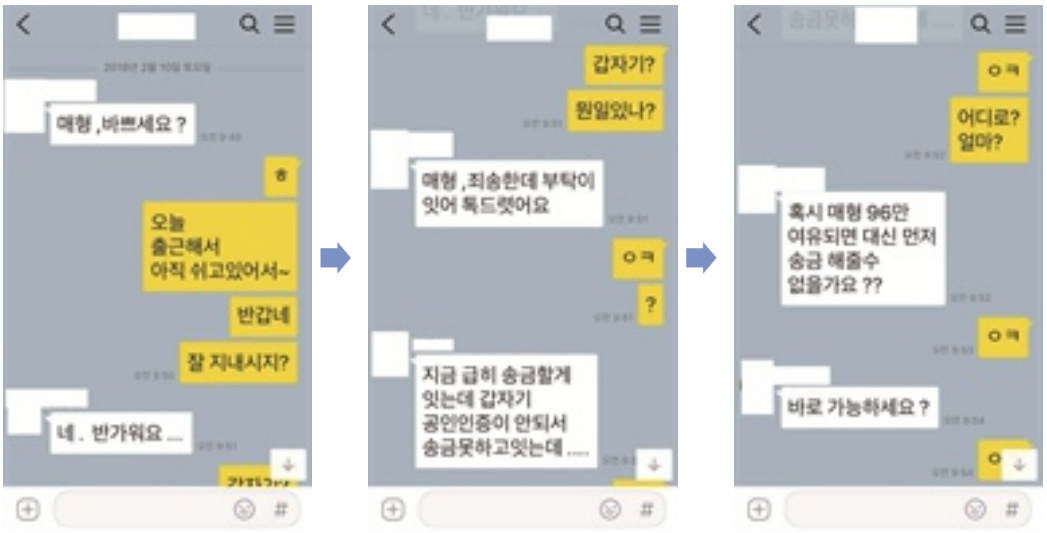
예방 방법

메신저 피싱 피해를 예방하기 위한 가장 간편한 방법은 본인에게 전화를 걸어 확인하는 방법이다. 본인에게 전화를 걸어 돈이 실제로 필요한지 여부를 확인하는 과정이 반드시 필요하다. 전화를 통해 본인임을 확인 할 수 없는 경우, 직접 신분을 확인할 때까지 돈을 이체해서는 안 된다. 또한 포털 등에 등록되어 있는 주소록을 이용해 범죄가 이루어지는 만큼, 포털사이트 계정 보안관리에 만전을 기할 필요가 있다.

Ⅱ. 주요 사이버범죄 사건

메신저 피싱

〈 실제 메신저 피싱 사례 〉



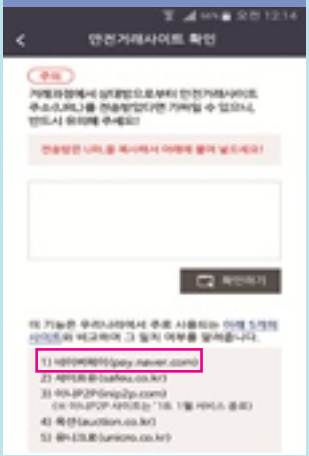
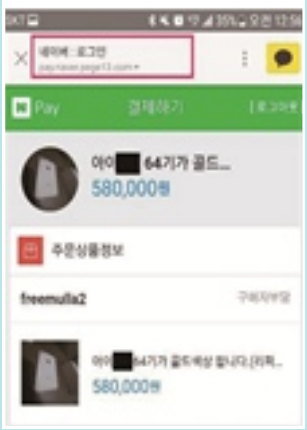
가짜 안전거래 사이트 이용 인터넷 사기

인터넷 사기가 증가함에 따라 거래상 안전을 확보하기 위해 '안전거래' 방식의 거래가 활성화되고 있다. '안전거래'란 결제대금 예치를 통한 거래를 의미한다. 즉 구매자가 거래대금을 제3자에게 맡기고 물품배송이 완료되면 제3자로부터 판매자에게 거래대금이 이체되는 구조의 거래방식이다.

통상 안전거래를 진행하면 거래의 안전성이 담보될 수 있으므로 안심하고 거래를 진행하게 되는데, 사기피의자들은 이러한 허점을 악용해 가짜 안전거래 사이트를 개설한 후 안전결제인 것처럼 가장하여 돈을 이체받는 방식으로 범행을 저지르고 있다. 판매자가 안전결제를 신청한 것처럼 속여 입금을 요청하지만 실제로는 안전거래 사이트의 가상계좌가 아닌 개인계좌로 이체를 요청한다.

가짜 안전거래 사이트는 실제 안전거래 사이트와 유사한 주소를 사용하여 피해자들을 속이고 있다. 예를 들어 '네이버페이'라는 안전거래 사이트(pay.naver.com)의 경우, 사기피의자들은 이와 비슷한 pay.naver.pege13.com이라는 가짜 피싱사이트를 개설해 피해자를 유도하는 것이다. 따라서 실제 안전거래 사이트가 아닌 다른 주소의 안전거래 사이트를 판매자가 보내준다면 그 거래는 사기라고 의심해 볼 수 있다.

안전거래 사이트(네이버페이) 피싱사이트 사례

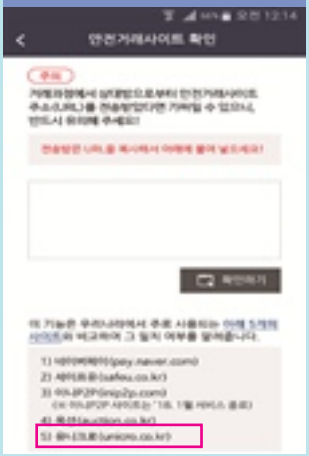
정상 사이트	피싱 사이트	피싱사이트 화면
	pay.naver.pege13.com pay-naverm.com naevevr.com naverpay.gq	

Ⅱ. 주요 사이버범죄 사건

가짜 안전거래 사이트 이용 인터넷 사기

안전거래 사이트(유니크로) 피싱사이트 사례

정상 사이트



피싱 사이트

www.unioocroo-co-kr.cc

uniocrroo-co-kr.cc

uniicroo-cr-kr.com

unicro-co-kr.org

피싱사이트 화면

주요 검거 사례

- 피의자는 네이버 중고나라 사이트에 "고가의 휴대전화를 판매하겠다."고 글을 올린 후 연락이 오는 피해자들에게 가짜 네이버 안전결제 사이트를 보내준 후 안심한 피해자에게 피의자가 지정한 개인계좌로 입금하도록 하여 33명에게 약 2억원을 받아 편취 (서울 광진경찰서)

예방 방법

이러한 사기를 예방하기 위해 경찰청에서 제작한 '사이버캅' 앱을 사용하는 것을 권장한다. 허위 안전거래 사이트로 의심되는 경우 해당 주소를 '사이버캅' 앱에 입력하면 사이트의 진위여부를 확인할 수 있다.

휴가철 인터넷 사기

하계 휴가철에는 통상 휴가를 위한 물건구입이 증가하는 시기로, 휴가물품에 대한 인터넷 사기사건도 같이 증가하고 있는 추세를 보여왔다. 특히 휴가철에는 숙박권, 여행상품, 여름가전, 캠핑용품, 워터파크 이용권 등에 대한 사기피해신고가 증가하였다.

사기범행은 주로 인터넷 쇼핑몰, 중고거래 사이트에서 발생하고 있으며 '긴급처분', '특별할인' 등의 문구를 이용해 소비자를 현혹하거나 '급하게 숙박권을 구한다'는 소비자의 글을 보고 접근하는 등 조급해지는 심리를 이용하기도 하였다.

주요 검거 사례

- 피의자는 네이버 중고나라 사이트에 "리조트 숙박권을 양도한다"는 등 거짓글을 게시하여 이를 보고 연락한 96명에게 4,370만원을 입금 받아 편취 (8월, 서울 용산경찰서)
- 피의자는 인터넷 까페 등에 '제주 한 달 살기 타운하우스를 임대해 주겠다'고 거짓글을 올려 관광객 29명에게 6,000만원을 입금 받아 편취 (8월, 제주동부경찰서)

최근 기존 인터넷 사기 수법과 구분되는 사건도 발생하고 있다. 이는 '가짜 펜션예약 사이트'의 등장인데, 다른 펜션 사진 도용, 가짜 후기, 질의응답 게시판 운영을 통해 피해자가 속을 수 밖에 없는 별도의 사기 사이트를 운영하는 사례가 최근 확인되었다.

〈 가짜 펜션사이트를 개설하고 유튜브를 통해 홍보 (현재 사이트는 폐쇄) 〉

Ⅱ. 주요 사이버범죄 사건

이메일 무역사기

이메일 무역사기는 무역업체를 대상으로 이메일을 해킹 후 '거래계좌 변경' 등 허위 이메일을 발송하여 물품대금을 중간에서 가로채는 수법이다.

국내 대기업이 피해금액 약 248억 원의 이메일 무역사기를 당해 큰 이슈가 되었던 사건이 있었다. 이메일 무역사기는 해운 · 제약회사 등 특정 기업을 가리지 않고 여러 종류의 기업에서 발생되고 있다.

이메일 무역사기의 수법은 이메일 계정을 해킹하거나, 유사 이메일 주소를 발송하여 기업을 혼란하게 하는 방식을 취하고 있다.

이메일 계정 해킹 방식은 먼저 피해자의 컴퓨터 또는 휴대폰을 악성코드로 감염시켜 메일 계정정보를 탈취한다. 이후 송수신 메일을 면밀히 관찰하다가 피해자와 유사한 이메일 주소로 다른 계좌번호를 보내 대금을 가로챈다.

유사 이메일 발송은 피싱 사이트 수법 또는 가짜 안전거래 사이트와 비슷한 방법으로, 거래처의 이메일과 유사한 가짜 이메일 주소를 생성해 물품대금을 가로채는 수법이다.

유사 이메일 주소 이용 수법

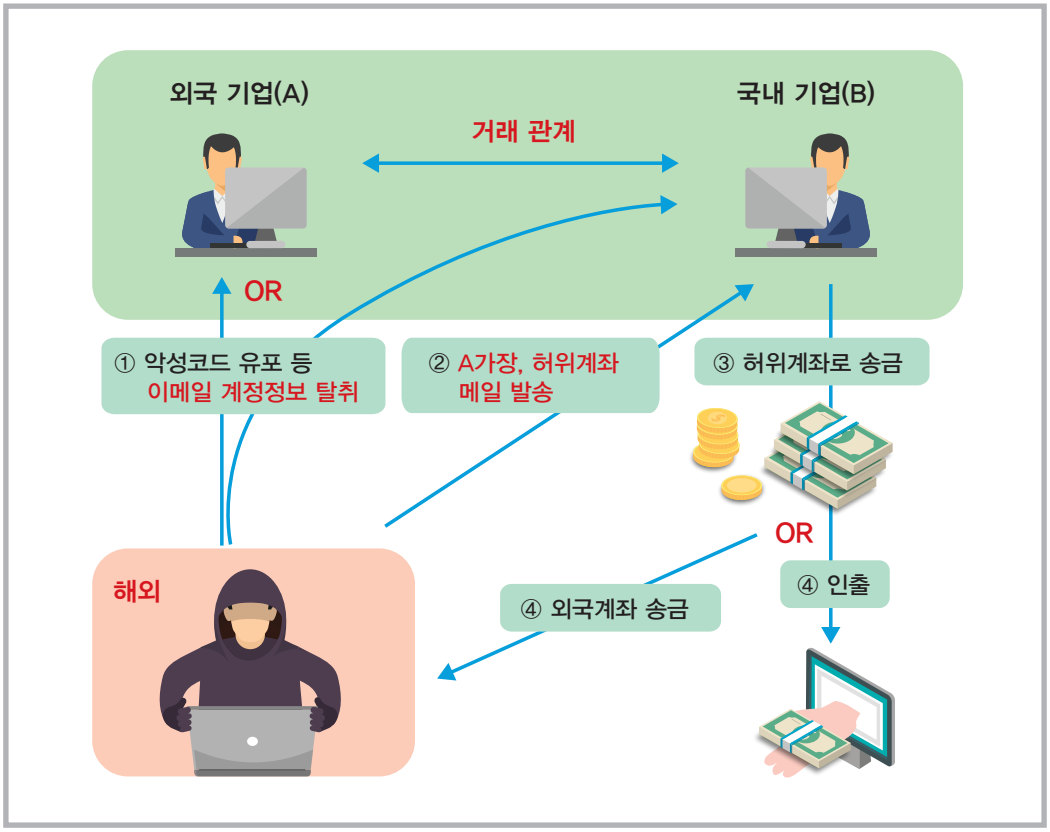
① 알파벳 추가 · 삭제 : widget**s**@freemail.com → widget@freemail.com
② 알파벳 재배치 : acme**868**@freemail.com → acme**686**@freemail.com
③ 알파벳 대체 : sales@freemail.com → sa**1**es@freemail.com
④ 이메일 네임서버(name server) 변경 : XXX@**korea**.com → XXX@**krea**.com

이메일 무역사기

이메일 무역사기 대응 사례

- 해외거주하는 피의자는 올해 3월 피해회사의 거래업체를 사칭, 300만 유로(한화 약 40억원)을 입금하라고 속여 불가리아 계좌로 입금 받음
- 경찰청은 사건 접수 즉시 금융정보분석원과 해당내용을 공유하여 수취계좌 정보파악을 진행하고, 인터폴을 통해 불가리아 경찰청과 공조하여 신속한 자금동결 및 회수를 진행하여 해당계좌 동결 및 피해금 전액을 반환 받을 수 있었음

〈이메일 해킹 무역사기 흐름도 예시 〉



Ⅱ. 주요 사이버범죄 사건

랜섬웨어 제작자 수사

랜섬웨어는 몸값(Ransom)과 소프트웨어(Software)의 합성어로 시스템을 사용 불가능한 상태로 변경하거나 피해자의 데이터를 암호화하고 복구를 원하는 피해자에게 금전을 요구하는 악성프로그램이다. 수천 종에 이르는 변종이 있으며, 최근에는 사용자 PC 내 주요 파일들을 암호화하고 일정한 비트코인을 요구하는 사례가 대부분이다.

이러한 랜섬웨어는 1989년부터 제작되어 유포되어 왔으나 국내는 2015년 한글로 돈을 요구하는 크립토락커(Cryptolocker)라는 랜섬웨어가 유포되면서 사회문제로 부각되기 시작했다.

대부분의 랜섬웨어는 윈도우즈 운영체제가 설치된 컴퓨터를 감염시키지만, 안드로이드(Android) 스마트폰이나 맥(Mac) 운영체제가 설치된 시스템에도 감염사례가 발견되기도 한다.

감염경로는 피싱 이메일의 첨부파일에 문서 · 이미지 등으로 위장된 악성코드를 첨부하여 랜섬웨어를 실행하게끔 유도하는 수법이 많이 사용된다. 이메일에 실행파일(.exe) 등이 포함된 경우, 혹은 문서파일로 보이지만 상세 확장자를 확인하면 바로가기 파일(.lnk)인 경우, 문서가 정상적으로 실행되지만 매크로 실행을 유도하는 경우는 악성코드일 가능성이 높으니 주의해야 한다. 또한 익스플로러, 플래시(Flash), 자바(Java) 등 컴퓨터에 설치되어 있는 프로그램의 보안 업데이트가 되지 않은 경우에도 공격자가 악성코드 유포지로 설정한 웹사이트에 접속하는 것만으로도 감염될 수도 있다.

주요 검거 사례

- 락스크린 랜섬웨어를 제작 및 유포하고, 피해를 복구해주는 대가로 피해자들(1,215명)에게 비트코인 5만원 상당을 요구한 피의자 검거(4월, 경찰청 사이버수사과)

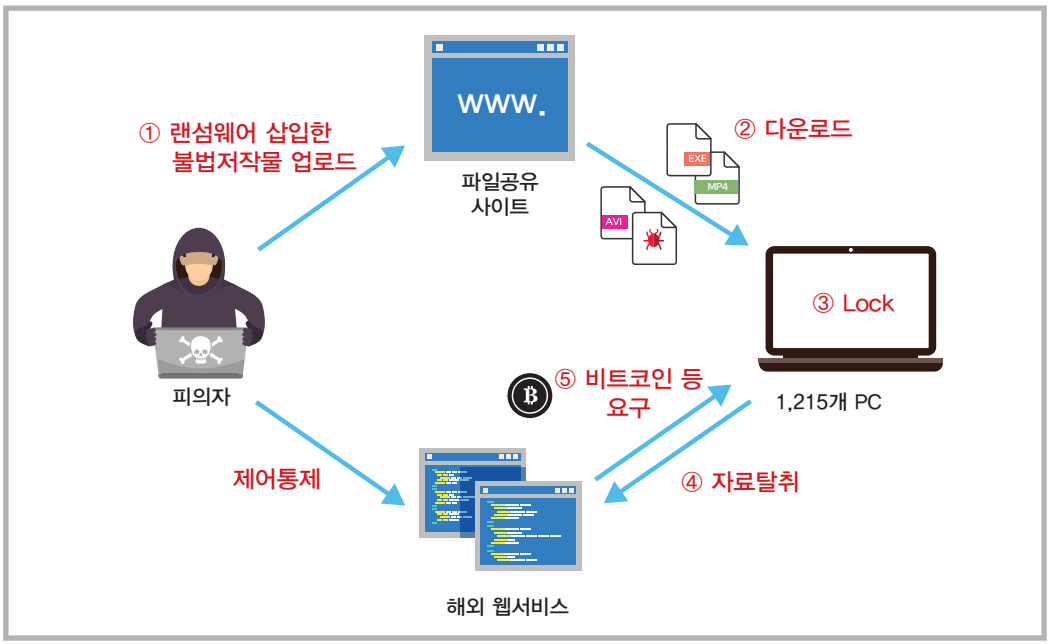
위 사건의 랜섬웨어는 문서파일을 암호화하는 일반적인 랜섬웨어와 달리 윈도우즈 초기화면을 잠근 후 피의자가 보내주는 해제키 값을 입력하지 않으면 컴퓨터를 사용하지 못하게 하는 락스크린 악성프로그램이 사용된 랜섬웨어이다.

랜섬웨어 제작자 수사

이번 랜섬웨어 유포 사건의 특이한 점은 청소년이 랜섬웨어를 제작하여 유포했다는 점인데, 해외 전문해커집단뿐만 아니라 일반인도 쉽게 랜섬웨어를 유포할 수 있다는 것을 보여준 사례이다.

이 랜섬웨어에 감염된 컴퓨터는 총 1,215대로 확인되었다. 다행히 감염된 PC 사용자들은 대부분 중요자료를 저장하지 않은 개인으로, 금전 요구에 응하지 않고 포맷을 한 것으로 확인되었다.

〈랜섬웨어 유포 및 비트코인 공갈사건 개요도 〉



예방 방법

랜섬웨어를 예방하기 위해서는 개인 및 업무용 자료는 PC와 분리된 저장소에 정기적으로 백업하는 것이 필요하며, 이메일 첨부자료는 단순 문서파일이어도 발신자로부터 내용을 확인하지 않은 이상 실행을 자제해야 한다. 또한 백신과 운영체제 및 익스플로러 등 주요 프로그램에 대해 최신 업데이트를 유지하는 것도 중요하다.

또한 '노모어랜섬'(www.nomoreransom.org) 사이트를 방문하면 일부 랜섬웨어의 복구 프로그램을 다운로드 받을 수 있다.

Ⅱ. 주요 사이버범죄 사건

게임핵 및 불법사설 서버 수사

게임핵이란 온라인 게임 캐릭터의 능력치를 향상시키거나 게임을 조작하는 악성프로그램이며, 불법사설서버란 게임회사가 제공하는 정식 게임 서버가 아닌, 개인이 제작해서 제공하는 게임서버를 말한다.

게임핵은 불법프로그램으로 게임 내에서 부정행위를 조장하고 게임의 공정성을 저해하는 범죄이며, 불법사설서버는 게임회사의 지적재산권을 침해하는 범죄이다.

주요 검거 사례

- 게임조작이 가능한 악성프로그램을 중국 해커를 통해 구매한 후 사이트를 통해 대량으로 판매, 부당이득을 취한 피의자 검거(서울 양천경찰서)
- 유명 인터넷 게임을 모방한 불법 게임 사설서버를 개설, 불특정 다수 회원들에게 게임물을 제공하여 4억 7천만원 상당의 부당이득을 취한 피의자 8명 검거(대구청 사이버수사대)

서울 양천경찰서에서 검거한 게임핵 제작자는 유명 게임회사에서 개발한 1인칭 슈팅게임의 게임핵을 개발 후 본인이 운영하는 사이트를 통해 판매하였다. 특히 벽 너머의 상대방의 모습을 확인할 수 있는 악성프로그램(일명 월핵)을 중국 해커로부터 구매한 후, 총 2,100회에 걸쳐 판매하여 1억7천만원 상당의 부당이익을 취하였다.

Ⅲ. 최근 사이버위협 트렌드

피싱메일 유포

최근 다양한 종류의 피싱 메일이 국내에 유포되고 있으며, 이들은 내용이 자연스러우며 공격 기술이 고도화된 특징을 보이고 있다.

피싱 메일은 기밀 탈취, 금전 편취 등의 목적으로 악성코드와 함께 유포된다. 특히 '갠드크랩(Gandcrab)' 랜섬웨어는 금년에만 10여회 넘게 다양한 주제로 유포 중이다.

갠드크랩 랜섬웨어 피싱메일 사례

【저작권위반경고-1월】

사용하고 있으시는 이미지들 중 제가 제작한 그림을 제작자의 동의없이 사용하시는거라 저작권법상에 문제가 되시는 걸 말씀드립니다 원본이미지랑 링크등 정리해 압축해 보내드립니다.

【이력서 사칭-5월】

최근에 '경리 및 회계업무 담당자 채용' 공지를 보았는데 그 포지션에 지원하고 싶습니다. 또한 다른 기회가 있다면 도전하고 싶습니다.
이력서를 첨부하였습니다.
감사합니다.

【소환장 사칭-6월】

-귀하는 고소를 당했습니다.-
귀하가 본 통지서를 받은 후 법원에 답변을 제출하고 다른 당사자에게 사본을 제공하거나 법원에서 법적 조치를 취할 수 있는 기간이 11일 남았습니다.

이메일에 링크를 첨부해 주요 포털과 동일한 화면의 피싱사이트로 유도하는 경우도 있다. 웹사이트를 별도 회원가입 없이 네이버 · 다음 · 페이스북 등 주요 사이트의 계정을 이용해 로그인 하는 '소셜로그인' 기능이 보편화된 상황에서 이러한 피싱 공격은 심각한 2차 피해를 유발한다.

또한 범칙금 납부고지, 정상회담 등 사회현안으로 위장한 피싱메일이 유포되는 등 공공기관도 피싱메일의 주요 사칭대상이 되고 있어 각별한 유의가 필요하다.

피싱메일 유포

최신 글로벌 사이버위협 트렌드

아래 자료는 KISA에서 발행하는 「2018년 3분기 사이버위협 동향보고서」의 내용을 요약 · 정리한 것입니다. 전문은 https://www.boho.or.kr/data/reportList.do를 참고하시기 바랍니다.

(1)가상통화 채굴 공격(트렌드마이크로社, Unseen Threat, Imminent Losse 보고서)

2017년 하반기부터 컴퓨터나 휴대전화에 채굴기를 몰래 심어놓는 '가상통화 채굴공격'이 2배 이상(144%) 증가하였다. 특히 올해 상반기에는 매달 그 수법이 변화하고 있다.

Ⅲ. 최근 사이버위협 트렌드

최신 글로벌 사이버위협 트렌드

〈2018년 상반기 가상통화 채굴공격 타임라인〉

1월	2월	3월	4월	5월	6월
구글 광고업체 악성코드 공격	크롬브라우저 확장프로그램 악성코드 주입	'ICLoader' 프로그램을 통한 배포	웹포털 'AOL' 스크립트에 채굴기 삽입	오라클 소프트웨어 취약점을 이용한 공격	봇넷 'Nercur' exploit kit

해커들은 사용자 몰래 PC나 서버에 채굴용 악성코드를 설치하고 해당기기의 자원을 무단으로 사용하여 수익을 창출한다. 또한 특정 웹사이트를 해킹하여 자바스크립트 등으로 이루어진 악성코드를 삽입하고 이에 접근하는 다른 시스템의 자원도 감염시키는 행태를 가진다. 보안업체 파이어아이社는 한국을 가상통화 채굴공격으로 피해를 많이 받은 나라 4위(8.43%)로 꼽았다.

(2) IoT 기반 사이버범죄 증가(카스퍼스키社, New Trends in world of IoT threats보고서)

2018년 1분기에 스마트 장치를 노린 악성코드 수가 2017년 전체보다 3배가 많았다. 가장 널리 공격된 형태는 기기 원격접속용 계정 해킹으로 2018년 2분기 허니팟에 대한 공격 중 75.4%를 차지하였다. 또한 IoT 기기에 다운로드된 악성코드 중 미라이 계열이 가장 선호되고 있다.

〈IoT 기기에 다운로드된 악성코드 비율〉

#	downloaded malware	% of attacks
1	Backdoor.linux.Mirai.c	15.97%
2	Trojan-Downloader.Linux.Hajime.a	5.89%
3	Trojan-Downloader.Linux.NyaDrop.b	3.34%
4	Backdoor.linux.Mirai.b	2.72%
5	Backdoor.linux.Mirai.b	1.94%

최신 글로벌 사이버위협 트렌드

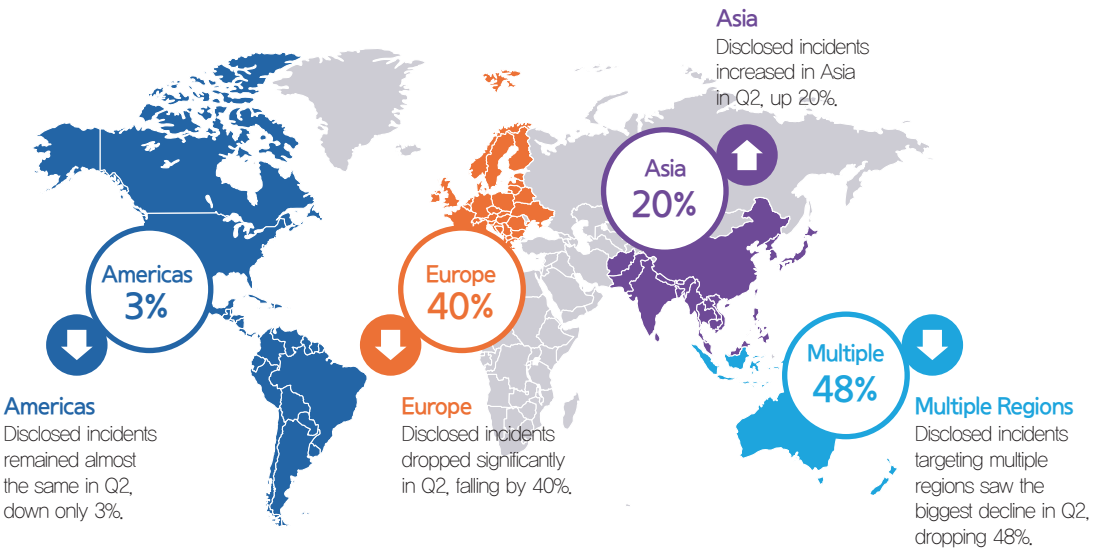
미라이 악성코드란?

2016년에 등장한 악성코드로, 리눅스 운영체계를 사용하고 있는 IoT 기기들의 취약점을 공격해 감염시킨다. 감염시킨 IoT기기는 좀비기기로 활용하여 디도스 공격을 하는데 사용된다. 미라이 악성코드는 2016. 10. 21. 미국 DNS 서비스 제공업체 다인(Dyn)에 대한 대규모 DDos 공격에 사용되었다. 그 결과 트위터, 넷플릭스, 뉴욕타임즈 등 76개 사이트가 마비되거나 서비스가 지연되는 사건이 발생하였다.

(3) 지역별 침해사고 발생변화(맥아피社, McAfee Labs Threats Report September 2018 보고서)

전 세계적으로 침해사고 발생량은 미국(3%)과 유럽(40%)는 감소한 반면, 아시아는 약 20%가 증가하였다.

〈전 세계 지역별 침해사고 발생량〉



랜섬웨어 예방 카툰


우리 오늘따라 사진빨 좀 받는데? 컴퓨터에 옮겨 놀자!
좋아! 근데 차기야~ 너무 뒤에서 찍지마~^^
찰칵
컴퓨터에 다 옮겼고~ 어_ 뭐지?
(경고) 모든 파일을 암호화했으니 찾고 싶다면 돈을 내놔라!
이게뭐야..? 내 사진! 날아가면 어떡해?! 돈을 보내야하나?!
잠깐!
현혹되면 안돼요! 복원이 확실치 않고 오히려 랜섬웨어 범죄를 조장합니다!
※랜섬웨어
몸값(ransom)과 제품(ware)의 합성어로 컴퓨터 사용을 제한하고 해제 비용을 요구하는 악성코드
네?! 그럼 제 파일들은 어떡해요?!
당황하지말고 피해 상태 그대로 신속하게 경찰에 신고하고
한국인터넷진흥원 및 전문IT보안업체에 피해복구와 악성코드 치료를 요청하세요!
중요한 자료는 정기적인 백업
백신 · 원도우 · 익스플로러 · 플래시 등 항상 최신 업데이트
이메일의 첨부 파일 클릭 주의!
"랜섬웨어" 예방 수칙 기억하기! 참 쉽죠~?