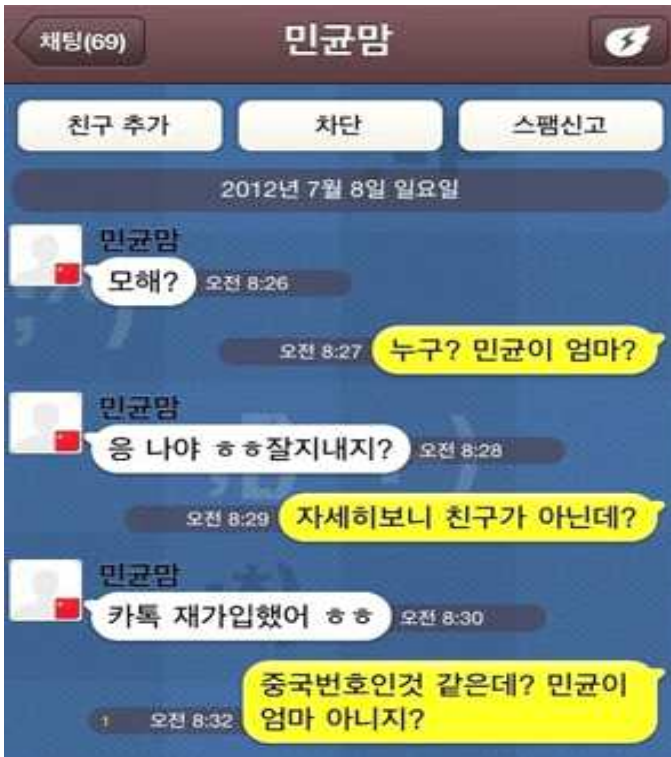


주요 정보보안 뉴스 소개

갈수록 과감해지는 피싱(Phishing)!!

: 금융기관, 공공기관 또는 지인으로 위장하여 전화, 이메일, 인터넷 팝업, 메신저 프로그램 등을 통해 개인·금융정보를 불법적으로 탈취하는 금융 사기 수법



▶ 지인으로 위장해 사용자에게 접근을 시도하는 메신저 피싱 사례

▶ 악성 애드웨어에 따른 금융감독원 피싱 사이트 (인터넷 팝업) 유도 사례

그렇다면 예방책은??

- ▶ '출처불명' 또는 금융기관 주소와 '다른 주소'로 발송된 이메일 즉시 삭제
- ▶ 컴퓨터, 이메일 등에 공인인증서, 보안카드 사진, 비밀번호 저장 금지
- ▶ 보안카드 번호 전부를 절대 입력하지 말 것
- ▶ 사이트 정상여부 확인 및 인터넷상에서 다운받은 미확인 프로그램 설치 자제
- ▶ 메신저를 통한 금전 거래 요청 시 전화를 이용하여 상대방 확인 후 거래
- ▶ 스마트폰용 보이스 피싱 차단 앱을 설치하여 피싱 사기 예방
- ▶ 백신프로그램을 최신 상태로 업데이트하고 실시간 감시상태 유지
- ▶ 인터넷뱅킹 등 전자금융 거래 시 OTP(일회성 비밀번호생성기) 사용, 공인인증서 저장 시 보안토큰(비밀정보 복사방지) 저장매체 사용

사이버침해 사고 예방 보안상식

- 국내 여성 쇼핑몰 등 여성 관련 사이트를 통한 웹캠 원격감시 악성코드 유포 주의
: 해커가 원격에서 컴퓨터나 노트북에 달린 카메라를 제어해 녹화한 영상을 탈취 할 경우
사생활 침해 등 심각한 문제를 야기 시킬 수 있음에 따라 아래와 같은 예방책을 권고

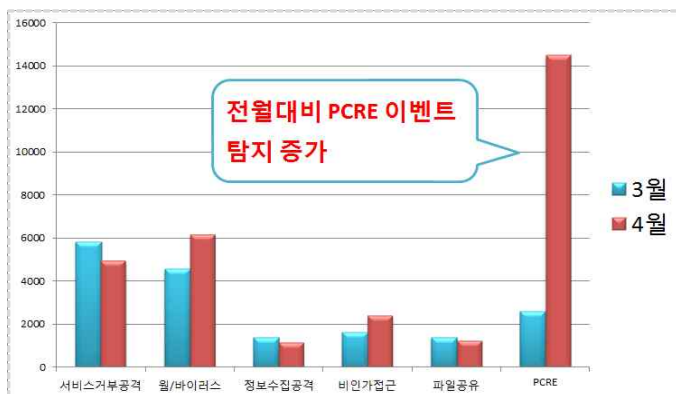


그렇다면 예방책은??

- ▶ 백신프로그램을 최신 상태로 업데이트하고 실시간 감시상태 유지
- ▶ 웹캠 미사용 시 스티커 부착
- ▶ 출처가 불분명한 링크는 클릭하지 않도록 유의
- ▶ 웹캠 원격제어 악성코드 감염여부 검사/치료 전용백신 안내
: http://boho.or.kr/kor/download/download_03_1.jsp (한국인터넷진흥원 홈페이지)

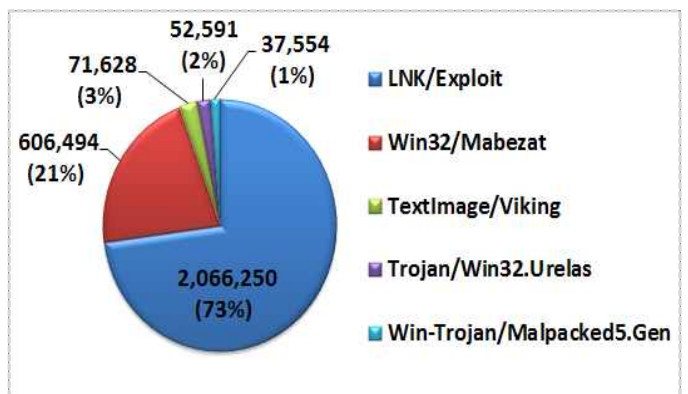
월간 사이버 침해 분석

사이버 침해 탐지 현황 [3~4월 비교]



- ▶ 전월대비 PCRE 이벤트 탐지 증가
PCRE(전산표준정규표현식) : 침입방지시스템(IPS)의 탐지 패턴을 우회한 변종 사이버 공격이며 PCRE 패턴을 이용하여 탐지/방어
예) PCRE기반에서는 '불법스팸' 이라는 공격의 변종인 '불☆법스팸' 등의 공격을 탐지할 수 있음

웬바이러스 및 악성코드 감염 현황 [4월]



- ▶ 웬바이러스 및 악성코드 감염 중 LNK/Exploit(73%), Win32/Mabezat(21%)가 높게 발생
☞ LNK 파일 취약점 및 공유폴더, USB, 스팸메일 등으로 인해 PC가 감염된 바 윈도우 상시 업데이트 시행, 이동식 저장 장치 사용 자제, 미확인 스팸메일 삭제 권고