㉾04373 서울시 용산구 청파로 40 삼구빌딩 [http://www.kma.org]/전화(02)6350-6517/전송(02)797-8176
총무학술국 국장 문지환[6510]/ 팀장 송창섭[6522]/ 담당 김지은[6517]/E-mail:myelle3@kma.org

문서번호 대의협 제191-1호

시행일자 2020. 4. 16.

수 신 수신처 참조

참 조

제 목 보건복지부 「코로나19 관련 신종 악성코드, 랜섬웨어 및 정보보안 강화 수칙 준수」관련 안내의 건

1. 귀 회의 무궁한 발전을 기원합니다.

2. 관련 근거 : 보건복지부 정보화담당관-2807(2020. 4. 7.)

3. 상기 호로 보건복지부로부터 코로나19와 관련하여 등장한 신종 악성코드, 랜섬웨어 및 정보보안 강화 수칙을 준수하여 줄 것을 다음과 같이 요청해 온 바, 이를 안내드리오니 귀 회 소속 회원에게 널리 안내하여 주시기 바랍니다.

- 다 음 -

가. 신종악성코드 주요 내용 및 정보보안 강화 수칙

○ 신종악성코드(“코로나바이러스”) 주요 내용

- 해당 악성코드는 MBR 디스크(부팅영역) 덮어쓰기 등을 통해 컴퓨터를 복구하지 못하게 하는 삭제형 악성S/W로, 피해자의 컴퓨터에서 작동하면 가장 먼저 coronavirus.bat이 실행되어 컴퓨터 내에 COVID-19라는 숨김 폴더를 만들고, ‘윈도우 작업 관리자’와 ‘사용자 접근 제어’를 비활성화 시키며, 바탕화면 또한 변경함
- 이와 동시에 MBR 디스크 덮어쓰기로 컴퓨터를 사용하지 못하게 하고 있음

○ 정보보안 강화 수칙

- 의심스러운 외부메일 열람하지 않고 삭제

- 백신프로그램 설치하고 바이러스 검사하기
- 운영체제 및 소프트웨어는 자동 업데이트 설정
- 신뢰할 수 없는 웹사이트 방문 및 파일 다운로드 자제

○ 의료법 제23조의3에 따라 진료정보 침해사고 발생 시 진료정보침해대응센터로 신고

➜ [문의] 진료정보침해대응센터 상황실(02-6360-6500) / [신고] cert@khcert.co.kr

나. 악성 랜섬웨어 주요 수법 및 예방 방안

○ 주요 수법

- 랜섬웨어 공격은 주로 3가지 방법(①악성 이메일 및 첨부파일, ②사용자 권한 장애 유발, ③이전 시스템 취약점 이용)을 통해 이루어지며 시스템 침투 후 모든 서류들을 암호화하거나 삭제하고 사용자에게 금전 요구
- 협박을 받은 피해자가 실제로 금원을 지불하는지 여부와 무관하게 대부분의 피해자들은 기존 파일을 회수하거나 시스템 복구를 하는 것이 어려움

○ 예방 방안

- 주기적인 파일 백업
- 안티바이러스 관련 시스템 업데이트
- 스팸메일 차단 등 주의
- 시스템 계정 관련 보안 강화
- 민감 정보 노출 최소화를 위한 네트워크 분리 및 데이터 카테고리화
- 제3자 침입방지 등

붙임 자료 : 보건복지부 코로나19 관련 정보보안 강화 협조 공문 - 1부. 끝.

대 한 의 사 협 회 장

"국민의 건강과 행복, 의협이 함께 합니다"

수신처 : 16개 시도의사회장, 각과개원의협의회장, 대한개원의협의회장, 대한공공의학회장, 대한공중보건의사협의회장, 대한군진의학회장, 대한병원의사협의회장, 대한의학회장(26개 전문과목학회장), 대한전공의협의회장, 한국여자의사회장