한국인터넷진흥원 C-TAS에서 보안공지 합니다.

신종 악성코드 유포 주의 보안권고

□ 개요

O 최근 기업을 대상으로 신종 악성코드(백도어 기능)를 유포하여 피해 기업‧기관 전산망에 침투하는 침해사고 확인

O 이와 관련, 위협정보를 공유하오니 각 기업‧기관에서는 백신 업데이트 및 전산망 점검 등 관련 보안조치 필요

□ 신종 악성코드명

O Netplwiz.dll

O oci.dll

O msectc.ax

□ 신종 악성코드 백신 진단명

O 안랩 V3 : Trojan/Win.Loader.C5648600 등 3종

O 하우리 : Trojan.Win.S.Agent.135736362 등 3종

O 이스트시큐리티 : Trojan.Agent.135736362 등 3종

□ 보안권고 사항

O 각 기업‧기관 자체 점검 후, 이상징후가 탐지될 경우 한국인터넷진흥원 인터넷침해대응센터 종합상황실로 통보 요청

□ 상세 내용

O C-TAS 홈페이지 실시간 상황전파 참고(https://ctas.krcert.or.kr/)

침해사고 신고 : 한국인터넷진흥원 인터넷침해대응센터 종합상황실(02-405-4911~5, [certgen@krcert.or.kr](mailto:certgen@krcert.or.kr))

2024년 전체 기간으로 조회한 결과

행내 혹은 dmz 구간에서 동일 파일 이름 / 진단명으로 확인된 건은 없습니다.

해당 진단이 v3 어느 엔진 버전부터 포함되었는지는 추가 확인해보겠습니다.

확인 결과 총 3개의 진단명 중 2건은 7월 10일자 엔진에 반영되어 현재 행내 v3에 적용 완료되었습니다.

다른 1건은 오늘자(버전 2024.07.12.00) 부터 반영되어 전체 단말에는 15일 월요일 적용 예정입니다.