

직원 성과 보고서로 위장하여 유포 중인 Guloader 악성코드

A asec.ahnlab.com/ko/91798

ATCP

December 31, 2025



최근 AhnLab SEcurity intelligence Center(ASEC)에서는 직원 성과 보고서로 위장하여 피싱 메일로 유포되는 Guloader 악성코드를 확인했다. 이메일 본문은 2025년 10월 직원 성과 보고서를 안내하는 내용으로 가장하고 있으며, 일부 직원의 해고 예정 사실을 언급하여 첨부 파일 확인을 유도한다.



[그림 1] 피싱 메일 본문

첨부된 파일은 RAR 형식의 압축 파일이며, 내부에는 “staff record pdf.exe”라는 이름의 NSIS 실행 파일이 포함되어 있다. 확장자가 표시되지 않을 경우 PDF 문서로 오인하여 실행할 위험이 있으므로 주의가 필요하다.



[그림 2] 첨부된 압축 파일 내부

staff record pdf.exe 파일은 Guloader 악성코드로, 실행하게 되면 아래 C2에 존재하는 셸코드를 메모리에 로드하여 실행한다.

URL : <https://drive.google.com/uc?export=download&id=1bzvByYrIH24oMCIX7Cv41gP9ZY3pRsgv>



[그림 3] 다운로드되는 셸코드

최종적으로 실행되는 악성코드는 Remcos RAT이며, 공격자의 명령에 따라 키로깅, 스크린샷 캡처, 웹캠 및 마이크 제어뿐만 아니라 설치된 시스템에 존재하는 웹 브라우저의 히스토리 및 비밀번호 추출 기능과 같은 악의적인 원격 제어가 가능하다.

Remcos RAT C2 : 196.251.116[.]219:2404,5000



[그림 4] Remcos RAT의 C2 정보

출처가 불분명한 메일 열람은 사용자의 각별한 주의가 요구된다. 2차 피해를 예방하기 위해 주기적인 패스워드 변경이 필요하다. 또한, 공격자의 주소나 침해당한 주소로 정보를 유출하는 유형과 달리 정상 플랫폼을 C2로 활용하는 사례가 계속 증가하고 있으므로 사용자는 각별한 주의가 필요하다.

MD5

c95f2a7556902302f352c97b7eed4159

AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

