ZLoader 악성코드, 사업 정지 경고로 위장해 유포중

By 알약(Alyac)

Published: 2020-10-21 · Archived: 2026-04-05 23:11:50 UTC

안녕하세요? 이스트 시큐리티 ESRC(시큐리티대응센터)입니다.

금일 ZLoader 악성코드가 국내에서 이메일을 통해 유포됨을 확인하였습니다. 이메일은 “당신의 사업이 조만간 정지될 것이다”의 내용으로 첨부된 URL을 실행하도록 유도합니다.

[그림 1] 사업 정지 내용의 악성 메일 화면

이용자가 문서 확인을 위해 이메일 내 링크를 클릭하게 되면은 구글 문서가 열립니다. 그리고, ‘Click here to download the document’를 한차례 더 누를 경우, ‘https://donwloadfiles[.]top/download.php’에서 ‘details1910p.xls’ 엑셀 파일이 다운로드됩니다.

[그림 2] 연결된 구글 드라이브 화면

문서 실행 시 아래와 같이 매크로 실행을 유도하는 화면이 나옵니다.

[그림 3] ‘details1910p.xls’ 실행 화면

만일 매크로를 실행하게 되는 경우, ‘MS Excel 4.0 Macro’ 매크로가 있는 엑셀 파일 내 시트 ‘Y’에서의 셀에서 다운로더 기능을 수행하는 코드를 실행합니다.

[그림 4] Y 시트의 매크로 코드

현재 공격자 서버인 ’https://donwloadfiles[.]top/dllD2x22a3df/xlsp.c1’에서 추가 파일이 유포 중이며 동일한 기능의 파일이지만 다른 해시를 가지는 파일을 지속적으로 바꾸고 있습니다.

다운로드된 파일은 dll 파일이며 경로 ‘C:\MChqqpu\RYfKXWm\’하위 ‘YTvxeyE.dll’로 생성 됩니다.

[그림 5] 매크로에서 사용하는 C&C 주소 화면

다운로드된 파일은 정상 프로세스 ‘rundll32.exe’에 ‘DllRegisterServer’ 파라미터로 로드되어 실행됩니다. 이 파일은 ‘msiexec.exe’와 ‘rundll32.exe’에 페이로드를 인젝션하여 실행됩니다.

[그림 6] ZLoader 실행 화면

이 코드는 ‘fqnceas[.]su/gate.php’에서 추가 파일 다운로드 시도합니다. 이는 악명 높은 Zeus 뱅킹 트로이목마의 변종으로써 해당 코드는 사용자의 금융 정보뿐 아니라 사용자의 브라우저의 패스워드, 쿠키 등도 수집하는 것으로 알려져 있습니다.

[그림 7] C&C 연결 화면

따라서 악성코드 감염을 예방하기 위해, 출처가 불분명한 메일을 확인할 경우, 특히 첨부파일을 열어볼 경우에는 신중을 기해야 하며 백신 업데이트 최신화와 정기 검사를 습관화하여야 합니다.

현재 알약에서는 ‘**Trojan.Downloader.XLS.gen**’, ‘**Trojan.Agent.ZLoader**’으로 탐지 중입니다.