RedEyes 가 유포 중인 악성코드 CHM 및 RokRAT 연구

박보경 [1], 전유부 [2], 한성수 [3*]
[1] 강원대학교 자유전공학부 학부생
[2] 동국대학교 인공지능학과 교수
[3*]강원대학교 자유전공학부 교수

b.gyung17@gmail.com, jeonyb@dgu.ac.kr, sshan1@kangwon.ac.kr

Research on the malware CHM and RokRAT being distributed by RedEyes

Bo-Gyung Park[1], You-Boo Jeon[2], Seong-Soo Han[3*]
[1, 3*] Dept. of Liberal Studies, Kangwon National University
[2] Dept. of Artificial Intelligence, Dongguk University

요 약

이 논문은 북한 해킹 그룹이 최근 유포하고 있는 악성코드 CHM 과 RokRAT 에 대해 연구하고 대응하는 목적으로 작성되었다. 악성코드 CHM 은 chm 파일 실행 시 도움말 창을 생성하여 내부 악성 스크립트가 동작하는 방식이다. 악성코드 RokRAT 은 윈도우에 기본 탑재된 lnk 파일을 pdf 아이콘으로 위장하여 사람들에게 유포하는 방식을 사용하였다. 이는 다양한 형식의 파일을 통해 유포되는 만큼 사용자가 보안 위협에 대한 경각심을 가지고 스스로 예방하고 대처할 수 있어야 한다는 결론을 내리고 있다.

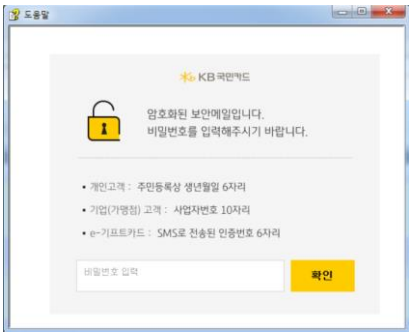
1. 서론

최근 북한 해킹 그룹 RedEyes 가 국내 금융 기업 보안 메일을 사칭한 CHM 악성코드를 유포한 사례와 링크 파일(.lnk)을 통해 RokRAT 악성코드를 유포한 사례가 발견되었다[1]. 악성코드 RokRAT 은 사용자 정보를 수집하고 추가 악성코드를 다운로드하여 문서를 통해 유포되었던 과거 방식과 달리, 정상 파일과 함께 스크립트 파일을 실행해 악성 행위를 수행한다.

따라서 RedEyes 가 유포 중인 CHM 악성코드와 RokRAT 악성코드의 유포 동향을 연구하고, 이에 대한 대응 방안을 제시하여 미리 예방하고자 한다.

2. 악성코드 CHM

악성코드 CHM 은 윈도우 도움말 파일 형식으로 이루어진 악성코드다. chm 파일은 컴파일 된 HTML Help 파일로, microsoft html help executable 프로그램을 통해 실행된다[2]. RedEyes 가 유포하는 CHM 악성코드는 chm 파일 실행 시, 국내 금융 기업의 보안 메일을 사칭한 도움말 창을 생성하고 내부에 존재하는 악성 스크립트가 동작한다.



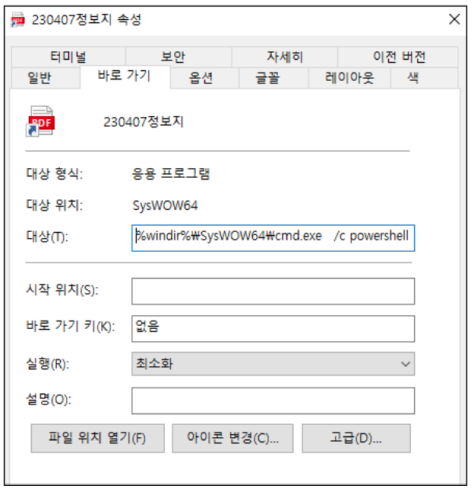
(그림 1) 금융 기업 보안 메일을 사칭한 도움말 창[3]

악성 스크립트는 바로 가기 객체를 이용하여 명령어를 실행한다. 실행 시 RUN 키 등록 및 공격자 서버로부터 명령어 수신, 명령 실행 결과 전달의 기능을 수행한다[3].

악성코드 CHM 에 감염되면 개인정보 유출, 시스템 무단 제어, 데이터 손상 등이 발생한다. 유출된 개인정보로 인해 특정 사용자로 사칭하여 2 차 피해가 일어날 수 있다. 또한 시스템을 무단 제어하여 추가 악성코드를 다운로드해 실행시켜 더 많은 문제가 발생할 수 있다.

3. 악성코드 RokRAT

RedEyes 가 유포한 악성코드 RokRAT 은 클라우드 기반 원격 접근 트로이 목마(RAT)를 사용하였다. 악성코드 RokRAT 은 사용자 정보를 수집하고 추가 악성코드를 다운로드할 수 있다. 과거 한글 문서 및 워드 문서를 통해 유포하였는데, 북한 RedEyes 는 최근 링크 파일을 통해 유포하였다. RedEyes 가 유포하는 lnk 파일은 pdf 아이콘으로 위장하고 있다. lnk 파일은 윈도우에 기본적으로 탑재된 프로그래밍 언어인 파워쉘 명령어를 내부에 포함하고 있으며, 임시 폴더 경로 (temp)에 정상 파일과 함께 스크립트 파일을 생성하고 실행하여 악성 행위를 수행한다[1].



(그림 2) lnk 파일 속성 [1]

HxD 프로그램을 통해 lnk 파일을 분석하면 더미 바이트가 존재한다. 정상 pdf 파일과 함께 실행되는 스크립트 파일에는 HEX 값으로 존재하는 악성 명령어를 실행하는 파워쉘 명령어가 존재한다. 이 명령어에서 인코딩된 데이터를 다운로드해 디코딩 후 poswershell 프로세스에 인젝션 하여 악성 행위를 수행한다. 인젝션 된 데이터는 RokRAT 악성코드로 사용자 정보 수집 및 추가 악성 파일을 다운로드할 수 있다. 수집된 정보는 클라우드 서비스를 사용하여 공격자의 클라우드 서버로 전송된다[1].

악성코드 RokRAT 에 감염되면 컴퓨터 정보, 화면 캡처 등이 공격자의 서버로 전송된다. 2 차 피해로 추가 악성코드를 다운로드하고 실행시킬 수 있다. 악성코드 RokRAT 은 스크린샷 캡처, BIOS (기본 입출력 시스템)으로 시스템 정보 수집한다. 수집한 데이터를 클라우드 서비스로 전송, 암호화된 개인정보 탈취, 파일 관리 및 암호화 복호화 관리 등을 수행한다.

4. 대응방안

악성코드 CHM 은 공격자 명령에 따라 다양한 기능을 수행하는 악성 파일이 추가로 생성될 수 있기에 실행을 자제해야 한다. 또한 특정 사용자를 대상으로 하는 파일명으로 유포될 수 있어 더욱 주의해야 한다. 악성코드 CHM 은 정상 문서 파일을 함께 유포해 사용자가 악성 파일임을 알아채기 어렵다. 사용자는 출처가 불분명한 메일 속 첨부파일 또는 url 실행을 자제하고, 로그인 시 비밀번호 외에 이중인증을 사용해야 한다.

악성코드 RokRAT 은 과거부터 꾸준히 유포되고 있으며, 다양한 형식의 파일을 통해 유포되는 만큼 사용자의 주의가 필요하다. 악성코드 RokRAT 은 악성코드 CHM 과 유사하게 정상적인 파일을 같이 실행하여 사용자는 인지하기 어렵다. 기업은 조직 내 PC ·운영체제· SW 등에 대한 보안 현황과 OS(운영체제)·SW 취약점을 상시 파악해 보안 패치를 적용해야 한다. 또한 내부 임직원 보안 교육을 실시하여 기업의 피해를 예방해야 한다. 공격자들이 보안 솔루션 진단을 우회하기 위해 여러 방식을 사용하고 있는 상황에서, 사용자는 보안 위협에 대한 경각심을 가지고 스스로 예방하고 대처할 수 있어야 한다.

5. 결론

본 논문은 북한 해킹 그룹 중 하나인 RedEyes 가 유포하는 악성코드 CHM 과 RokRAT 에 대해 연구하고 대응방안을 소개하였다. 악성코드 CHM 은 윈도우 도움말 파일 형식으로 이루어진 악성코드로, chm 파일 실행 시, 금융 기업의 보안 메일을 사칭한 도움말 창을 생성하고 내부에 존재하는 악성 스크립트가 동작하는 시스템이다. 악성코드 RokRAT 은 lnk 파일을 pdf 아이콘으로 위장하여, 사용자 정보를 수집하고 추가 악성코드를 다운로드할 수 있다. 악성코드 CHM 과 RokRAT 은 다양한 형식의 파일을 통해 유포되는 만큼 사용자가 보안 위협에 대한 경각심을 가지고 스스로 예방하고 대처할 수 있어야 한다. 또한 기업은 조직 내 PC ·운영체제· SW 등에 대한 보안 현황과 OS(운영체제)· SW 취약점을 상시 파악해 보안 패치를 적용해야 하고, 내부 임직원들의 보안 교육을 실시하여 기업 피해를 예방해야 한다.

참고문헌

[1] ye_eun, 링크 파일(*lnk)을 통해 유포되는 RokRAT 악성코드 : RedEyes(ScarCruft), ASEC, 2023.4.21.
[2] ASEC, 윈도우 도움말 파일(*.chm)로 유포되는 APT 공격, ASEC, 2022.3.17.
[3] gygy0101, 국내 금융 기업 보안 메일을 사칭한 CHM 악성코드 : RedEyes(ScarCruft), ASEC, 2023.3.3.