악성코드 상세 분석 보고서

Secure Drive 인증으로 위장한 악성코드 유포 피싱 메일
(고위 공직자 신분을 위장한 악성 메일)

(Document No : DT-20260120-001)

HAURI

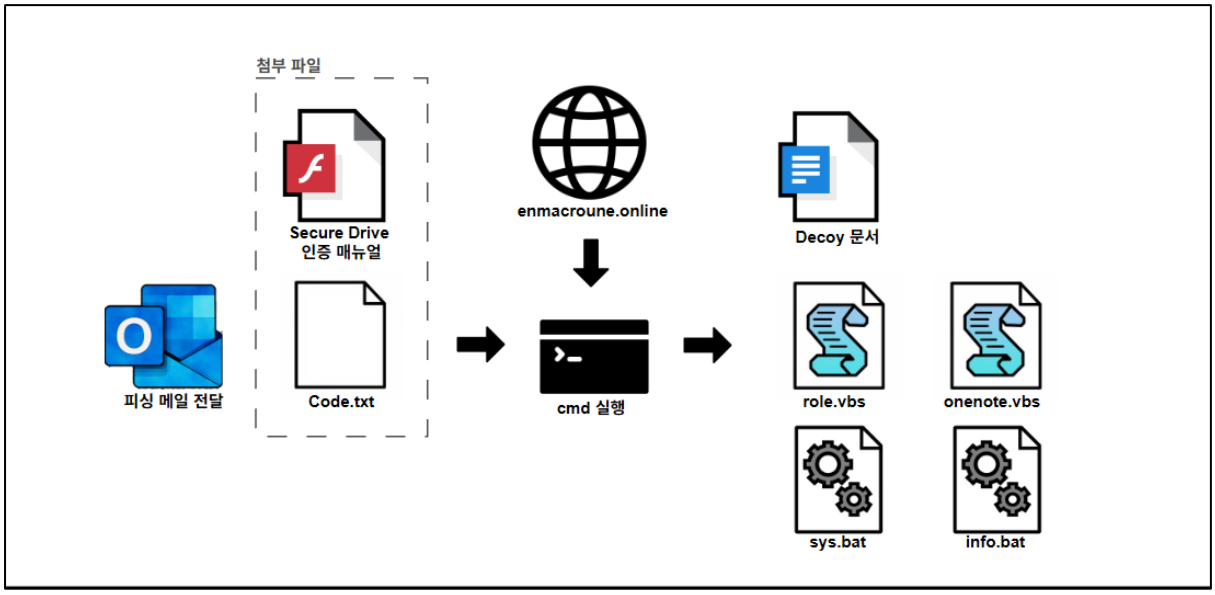
www.hauri.co.kr

∘ 분석 개요

Secure Drive 인증을 가장하여 사용자가 직접 악성코드를 실행하도록 유도하는 악성코드가 확인되었다. 해당 악성코드는 고위 공직자 신분을 사칭한 피싱 메일 첨부로 유포되었으며, 보안에 각별한 주의가 요구되는 지위를 악용한 신뢰 기반 사회공학 기법이 사용되었다.

해당 악성코드는 사용자 기만 전술과 난독화를 통한 보안 장비 탐지 회피, 사용자 직접 실행을 유도하는 로컬 보안 우회 기법을 통해 실행되도록 설계되었다.

악성코드는 실행 후 C&C로부터 추가 페이로드를 다운로드하여 실행하나, 분석 시점에는 페이로드가 삭제되어 확인이 어려웠다. 해당 C&C는 장기간 운영되며 다양한 대상을 상대로 악성 행위에 활용된 정황이 확인되어, 본 유형의 공격에 대한 각별한 주의가 필요할 것으로 보인다.



[공격 도식도]

1. Code.txt

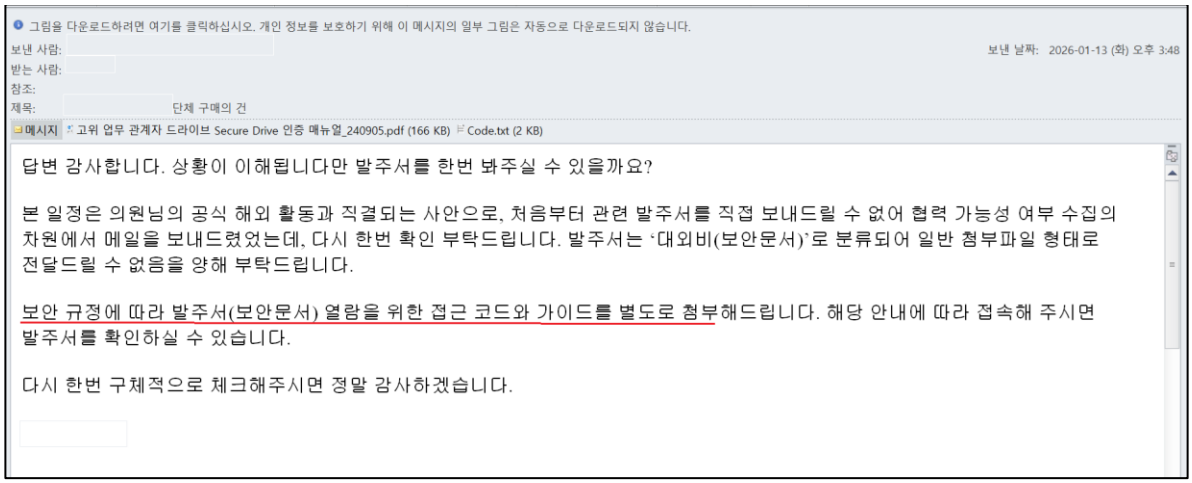
(MD5 : 75B4C33AF33D8C1BB6F9FEA9285DC541, SIZE : 2,370)

개요 : 추가 페이로드를 다운로드하여 실행한다.

ViRobot	BAT.S.Downloader.2370

상세분석 :

(1) 공격자는 고위 공직자 신분으로 위장하여 신뢰를 형성한 뒤, "보안 규정"이라는 명분으로 Secure Drive 인증이 필요한 상황을 조성하여 사용자가 매뉴얼을 통해 의심없이 악성코드를 직접 실행하도록 설계하였다.


그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

보낸 사람:

받는 사람:

참조:

제목: 단체 구매의 건

보낸 날짜: 2026-01-13 (화) 오후 3:48

메시지 고위 업무 관계자 드라이브 Secure Drive 인증 매뉴얼_240905.pdf (166 KB) Code.txt (2 KB)

답변 감사합니다. 상황이 이해됩니다만 발주서를 한번 봐주실 수 있을까요?

본 일정은 의원님의 공식 해외 활동과 직결되는 사안으로, 처음부터 관련 발주서를 직접 보내드릴 수 없어 협력 가능성 여부 수집의 차원에서 메일을 보내드렸었는데, 다시 한번 확인 부탁드립니다. 발주서는 '대외비(보안문서)'로 분류되어 일반 첨부파일 형태로 전달드릴 수 없음을 양해 부탁드립니다.

보안 규정에 따라 발주서(보안문서) 열람을 위한 접근 코드와 가이드를 별도로 첨부해드립니다. 해당 안내에 따라 접속해 주시면 발주서를 확인하실 수 있습니다.

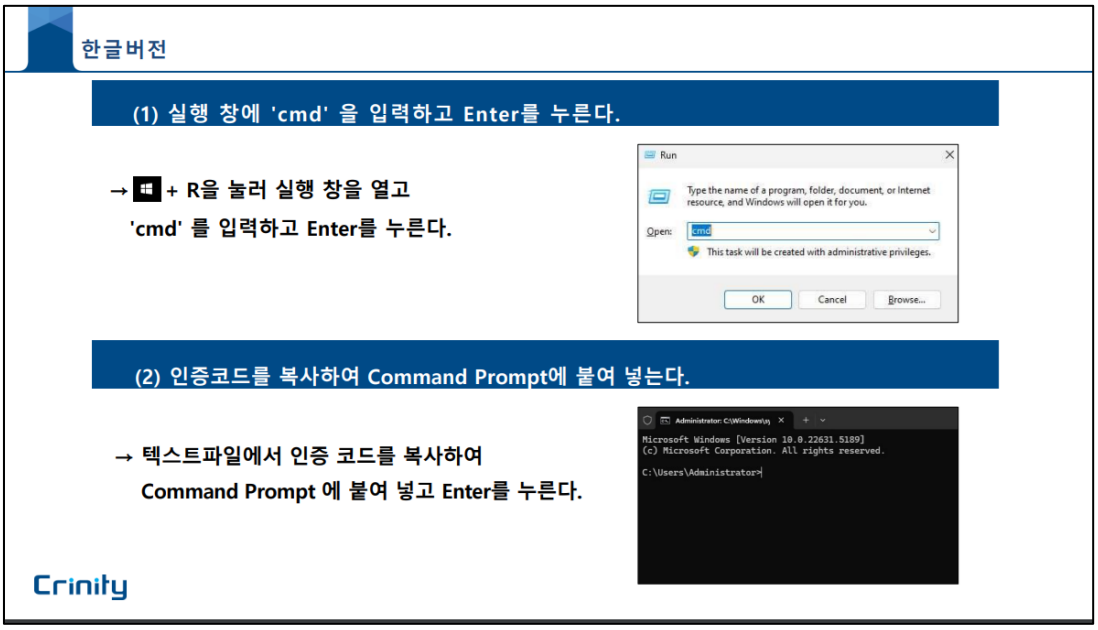
다시 한번 구체적으로 체크해주시면 정말 감사하겠습니다.

[그림 1] 사회 공학 피싱 메일

(2) 메일에 첨부된 PDF 에는 공직자 통합 메일 시스템인 Crinity 와 국회의 로고가 사용되어 문서의 신뢰도를 높였다. 해당 문서가 실제 인증에 사용되는 공식 매뉴얼인지는 확인되지 않았으나, 이후 안내되는 인증 방식은 상당히 비정상적인 특징을 보인다.

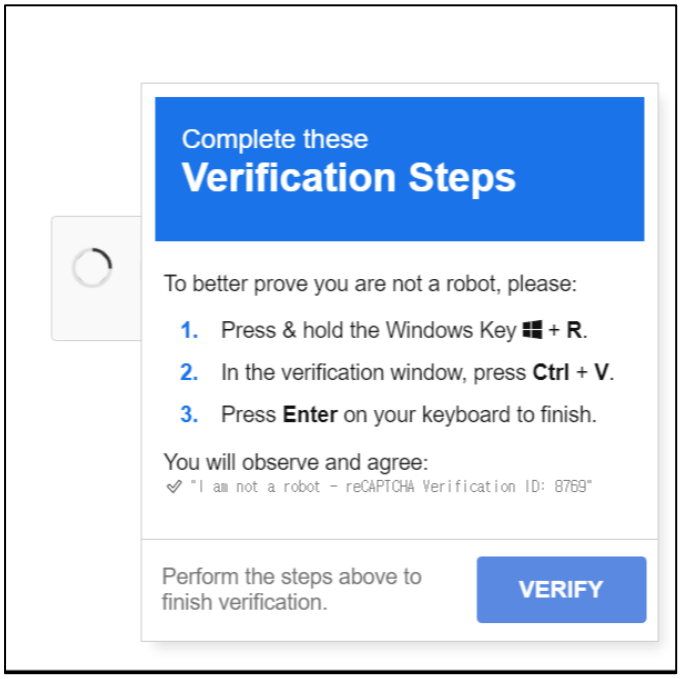
[그림 2] 피싱 메일에 첨부된 Secure Drive 인증 매뉴얼 -1

(3) Secure Drive 인증 과정에서 사용자가 명령 프롬프트(CMD)에 인증 코드를 직접 붙여넣어 실행하도록 유도한다. 사용자의 로컬 환경에서 명령을 직접 실행하도록 요구하는 이러한 방식은, CAPTCHA 인증으로 위장하여 악성 명령 실행을 유도하는 Click-Fix 공격과 높은 유사성을 보이며, 인증 메뉴얼을 가장한 악성코드 실행 메뉴얼이다.



[그림 3] 피싱 메일에 첨부된 Secure Drive 인증 매뉴얼 -2

(4) Click-Fix 공격과 같이, 인증을 명목으로 사용자가 로컬에서 명령을 직접 실행하도록 요구하는 방식은 정상적인 인증 절차로 보기 어렵다.



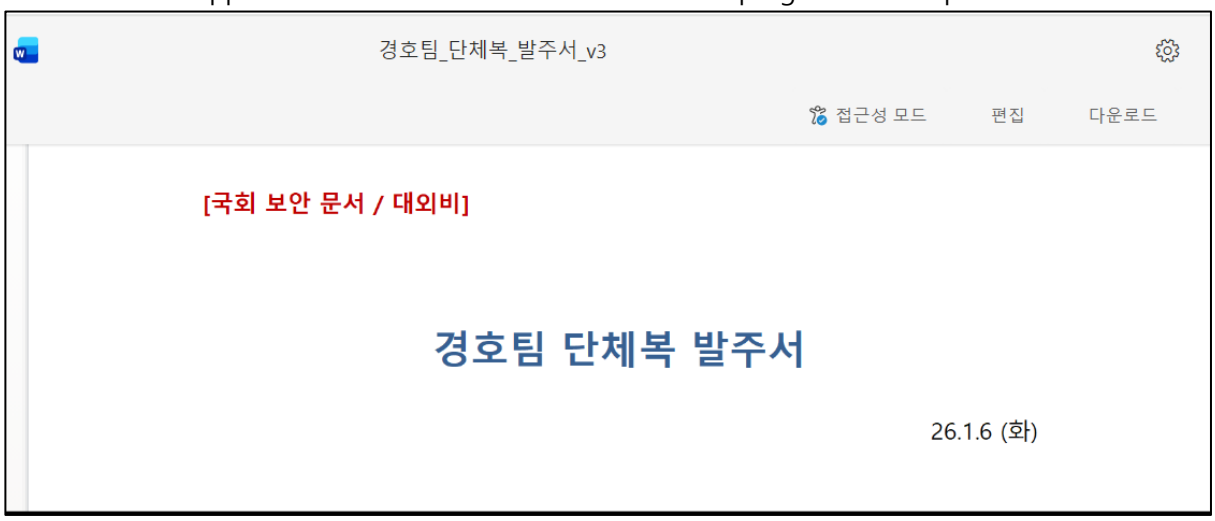
[그림 4] Click-Fix 공격

(5) Code.txt 는 난독화로 인해 실제 동작을 식별하기 어려워 일반 사용자가 인증 코드로 오인하기 쉽고, 보안 장비 탐지 회피를 통해 악성 코드 실행 가능성을 높인다.

[그림 5] Code.txt 입력 화면

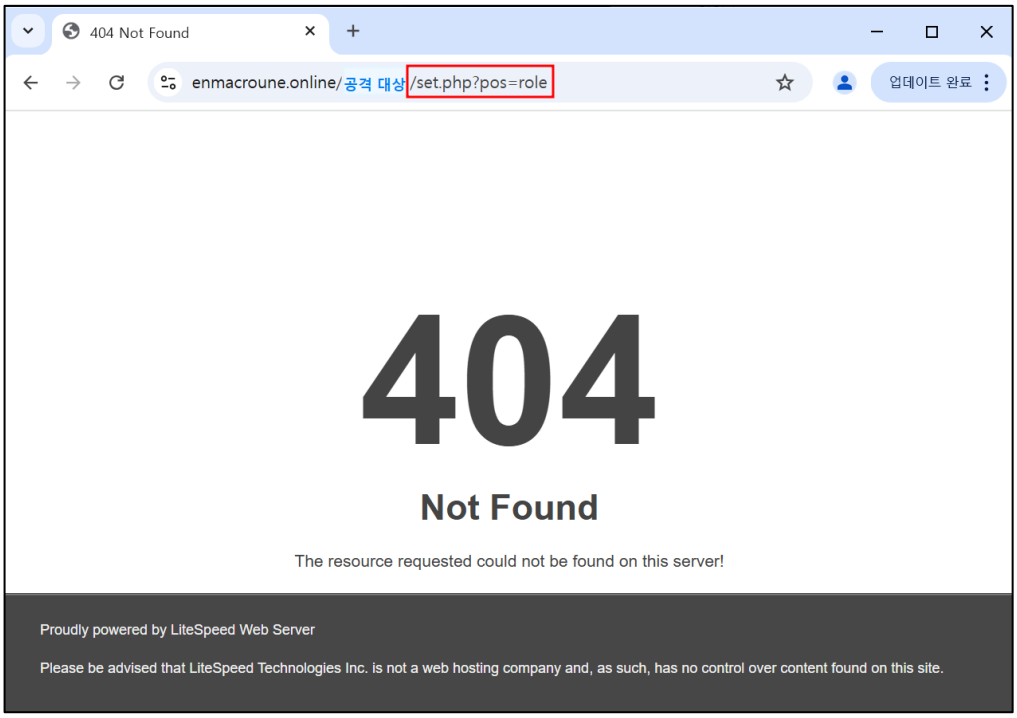
(6) Enter 입력 시 사용자에게는 원드라이브 디코이 문서가 출력되어 정상 동작으로 인식되도록 하며, 일정 시간 지연 후 백그라운드에서 C&C 로부터 추가 페이로드를 다운로드하여 지정된 경로에 저장 및 실행한다.

- C&C: hxxps://enmacroune[.]online
- 파일 경로
  - c:₩sysinfo₩role.vbs
  - c:₩sysinfo₩bsys.vbs
  - c:₩sysinfo₩binfo.vbs
  - c:₩%appdata%₩microsoft₩windows₩startmenu₩programs₩startup₩onenote.vbs



[그림 6] 디코이 문서

(7) 분석 당시 C&C 의 페이로드는 삭제되어 확인이 불가하였다. 이는 공격자가 인프라를 장기간 유지하기 위해 페이로드를 제거하는 방식의 회피 기법을 사용한 것으로 판단된다. 해당 도메인은 2025년 7월 이후 다양한 분야의 대상을 상대로 지속적인 공격에 활용한 정확이 확인되었다.



[그림 7] C&C 접속 화면

(8) 해당 도메인이 사용된 URL 파라미터 구조를 분석한 결과, PHP 기반 페이지에서 Kimsuky 공격 캠페인과 유사한 파라미터 패턴이 확인되었다. 또한 피싱 메일을 통한 초기 침투, LOLBin 기반 실행 방식, 스크립트 난독화, C&C 인프라 운영 및 페이로드 삭제를 통한 분석 회피 전술 등 복수의 전술·기법이 김수키 공격 사례와 유사한 점이 관찰되었다.

```
https://enmacroune.online/[redacted]/css.php?na=py
https://enmacroune.online/[redacted]/inc.php?bbs=util

https://enmacroune.online/[redacted]/board.php?pos=cache
https://enmacroune.online/[redacted]/board.php?pos=tmp
https://enmacroune.online/[redacted]/board.php?pos=temp

https://enmacroune.online/[redacted]/set.php?pos=role
https://enmacroune.online/[redacted]/set.php?pos=onenote
https://enmacroune.online/[redacted]/set.php?pos=bsys
https://enmacroune.online/[redacted]/set.php?pos=binfo

https://enmacroune.online/[redacted]/board.php?pos=temp
https://enmacroune.online/[redacted]/board.php?pos=log
https://enmacroune.online/[redacted]/board.php?pos=cache
https://enmacroune.online/[redacted]/board.php?pos=btemp
https://enmacroune.online/[redacted]/board.php?pos=blog
```

[그림 8] 공격에 사용된 URL

IOC

***C&C**

enmacroune.online

***MD5**

75B4C33AF33D8C1BB6F9FEA9285DC541

3C216462CB51A3AA86DCD46246D08885