OneNote 에 유포된 Emotet 악성코드 분석

박보경 [1], 하소희 [2], 한성수 [3]
[1] 강원대학교 자유전공학부 학부생
[2] 영남이공대학교 사이버보안 학부생
[3] 강원대학교 자유전공학부 교수

b.gyung17@gmail.com, ihyraxi@gmail.com, sshan1@kangwon.ac.kr

Analysis of Malicious Code Emotet circulated in OneNote

Bo-Gyung Park[1], So-hee Ha[2], Seong-soo Han[3]
[1, 3]Dept. of Liberal Studies, Kangwon National University
[2]Devision of Cyber Security, Yeungnam University College

요 약

이 논문은 OneNote 악성코드의 증가 추세와 그에 따른 Emotet 악성코드의 유포 방식 및 특징을 분석하고자 하는 목적으로 작성되었다. OneNote 는 페이지 내 어디든 자유롭게 콘텐츠를 삽입할 수 있는 특징 때문에 악성코드 유포에 적극적으로 이용되고 있다. 특히, Emotet 악성코드는 OneNote 파일을 이메일 첨부 파일로 유포하고, 문서 열람 시 클라우드 연결 버튼을 클릭하면 악성 스크립트 파일이 다운로드 되어 감염이 일어난다. 이러한 악성코드 유포 방식을 방지하기 위해서는 사용자 교육과 함께 보안 솔루션 강화가 필요하다는 결론을 내리고 있다.

중심어: Emotet, Spearfishing, Malspam, OneNote, Malware, C & C

1. 서론

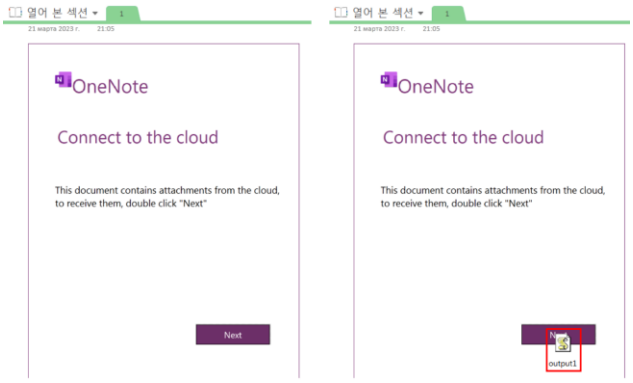
최근에 OneNote 악성코드의 유포가 점점 증가하고 있는 것으로 파악되었다. OneNote 는 파일 첨부 기능이 자유로워 악성코드 전파 수단으로 악용될 가능성이 크다. 또한, Microsoft Office 제품에 포함되어 있기 때문에 사용자 점유율이 높아 많은 사용자에게 악성코드가 무작위로 확산될 가능성이 높다는 문제점이 있다.

최근 북한 해킹 그룹 김수키가 Microsoft OneNote 를 이용해 Emotet 악성코드를 유포한 사례가 발견되었다[1]. 따라서 이러한 OneNote 악성코드의 유포 동향을 분석하고, 이와 함께 Emotet 악성코드에 대해서도 분석을 수행하여, 보다 효과적인 보안 대책 수립을 위한 연구가 필요하다.

2. Emotet 악성코드

Emotet 악성코드는 컴퓨터에 잠입하여 민감한 개인정보를 훔치려는 뱅킹 악성코드로 설계되었다. Emotet 은 주로 악성 스팸으로 전파하여, 연락처 목록에 있는 사람들에게 보낸다. 해킹된 이메일 계정에서 발송되기 때문에 수신자는 안전하다고 느껴 감염된 파일을 다운로드하는 경향이 크다[2].

지난 2023 년 03 월 21 일에 포착된 Emotet 악성코드는 '서류를 첨부했습니다.'라는 내용과 함께 Microsoft OneNote 첨부파일로 이메일을 통해 배포되었다[3]. 문서를 열람하기 위해 클라우드로 연결하는 버튼을 클릭하도록 유도하며, 버튼은 (그림 1)과 같이 output1.js 의 악성 스크립트 파일을 다운로드하게 된다.



(그림 1) OneNote 에 유포된 Emotet [3]

공격자는 스크립트 또는 바이너리를 실행하기 위해 명령 및 스크립트를 난독화 할 수 있다. (그림 2)는

output1.js 의 일부이다. 다음과 같이 output1.js 파일은 문자열 치환 방식으로 난독화 되어있다.

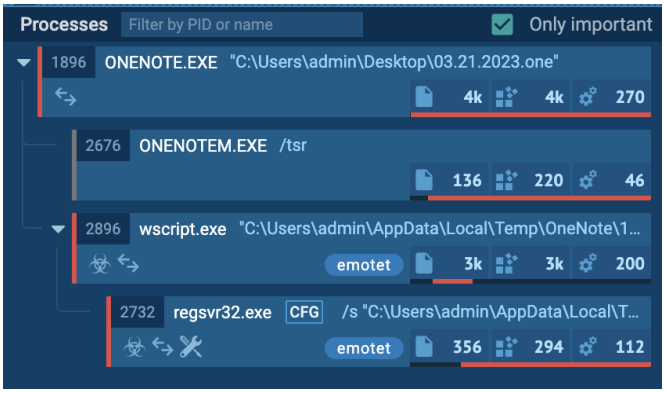
```
var xLjd9v7 = "Kqt";
var o1Oy = "%<T8S}E@;%]Ut]750HeAwzDgmHg|oW";
var uk$HdGr = 2326702;
var $3ir = "}e6rX(0[||5)7&Afmj8";
var rqckzBUe = xLjd9v7.replace("Kq", "");
function w8An(VzNB) {
var Yv = "%PQ;u#k30l+Fm/SAEX";
}
var WM4B = "0zLe{ur";
var iqrsXq5 = "dPve4Y%puVO}#<Dsg0$<f&qHFBmg0";
var Fl2x = 7005092;
var w5p = "CgU}2Xw}pMKC>b(!MYeJ+s0D&Ma";
var j = WM4B.replace("0zLe{", "");
var adN = 2950242;
var xKPDiw = "B$PeYzlCe8H1HEr[m;C9VN*NA";
var trydVPO = "-7Gw*n ";
var THXG06 = "{XCv{n=:7/Hzjw1Qw,:DrdEWe?HKogxN";
var dlS = trydVPO.replace("-7Gw*", "");
```

(그림 2) output1.js 일부

안랩 ASEC 분석팀에서 발표한 내용에 따르면, 최근 OneNote 로 유포 중인 Emotet 악성코드를 발표하였다. 스피어피싱을 기반으로 이메일을 통해 악성 스크립트 파일이 포함된 OneNote 파일을 유포하고 있다. 해당 OneNote 파일을 열람하게 되면 악성 스크립트 파일이 실행될 위험이 있고, 이 악성 스크립트 파일은 내부에 존재하는 다수의 명령제어 C&C 서버 주소로 접속을 시도하며, 접속에 성공할 경우 공격자가 추가적인 악성 행위를 수행할 수 있게 된다[3].

악성코드가 다운로드 된 후, 해당 악성코드는 (그림 3)에서 볼 수 있듯이 regsvr32.exe 프로세스를 이용하여 실행된다. 이를 ANY.RUN 대화형 악성코드 헌팅 서비스를 이용하여 확인할 수 있다[4].

Emotet 악성코드는 강력한 변종성을 가지고 있으며, 악성코드 감염 시 높은 수준의 권한을 얻을 수 있어 시스템에 대한 완전한 제어권을 획득해 통제할 수 있다.



(그림 3) ANY.RUN 을 통해 확인한 프로세스 [4]

3. 대응방안

ANY.RUN 과 같은 대화형 악성코드 헌팅 서비스를 통해 수집된 정보를 기반으로 Emotet 악성코드를 탐지하고 제거하는 대응책을 마련해야 한다. 이를 위해 시그니처와 행위 기반 탐지 기술을 적용할 수 있다.

따라서 Emotet 악성코드 감염을 사전에 예방하기 위해 이메일에서 파일 다운로드하는 것을 조심하고, 시스템 환경을 최신 버전으로 유지하는 것이 중요하다. 감염된 경우, 조직에서는 인바운드 SMB 통신을 제한하여 추가적인 감염을 방지하고, 예방 교육을 통해 미리 대비할 필요가 있다.

공격자들이 보안 솔루션 진단을 우회하기 위해 여러 방식을 사용하고 있는 상황에서, 사용자는 보안 위협에 대한 경각심을 가지고 스스로 예방하고 대처할 수 있어야 한다.

4. 결론

본 논문에서는 Emotet 악성코드 분석 및 보안 대책에 대해 소개하였다. Emotet 악성코드는 스피어피싱을 통해 시스템에 침입하고, 내부의 C&C 서버에 접속하여 시스템을 감염시키는 위험한 악성코드이다. 확산을 방지하기 위해 보안 업체는 백신 업데이트와 같은 보안 대책을 제공하여 사용자들이 신속하게 대응할 수 있도록 한다. 또한 사용자들은 개인정보 유출 등의 피해를 방지하기 위해 스피어피싱 공격에 대한 경각심을 가지고, 정기적인 보안 업데이트와 백신 업데이트를 수행하여 시스템 보안을 강화해야 한다.

참고문헌

[1] 김경애, 北 김수키 해킹그룹, '사례비 지급' 위장한 원노트 악용해 악성코드 유포, 보안뉴스

[2] Emote, alwarebytes, https://www.malwarebytes.com/emotet

[3] kwonxx, 원노트(OneNote)로 유포중인 Emotet 악성코드, ASEC, 2023.03.27

[4] ANY.RUN, https://any.run