Ransomware attack using File upload vulnerability and Remediation

File upload 취약점을 활용한 Ransomware 공격 및 대응

이름:
21800213 김휘진
22000216 나보림
22100579 이진주

Abstract

본 연구는 File Upload 취약점을 악용한 Ransomware 공격에 대한 분석과 대응 방안에 대해 다루고 있다. 우선, File Upload 취약점은 웹 어플리케이션에서 사용자가 파일을 업로드할 때 발생하는 보안 결함으로, 이를 통해 악의적인 파일이 서버에 전송될 수 있다. 연구에서는 이러한 File Upload 취약점을 통해 웹 셸(Web Shell)을 서버에 업로드하는 공격 시나리오를 제시한다.

더 나아가, 웹 셸이 서버에 업로드됨으로써 공격자는 Keylogger 를 활용하여 서버 관리자의 비밀번호를 탈취할 수 있다. 이후, 서버 관리자의 비밀번호를 이용하여 Ransomware 를 서버에 실시하면서, 기업이나 개인의 중요한 데이터를 암호화하고 금전적 요구를 행하는 악성 행위가 이루어진다.

본 연구는 위 과정들을 통해 File Upload 공격의 위험성을 명시하며, 이에 대한 효과적인 대응 방안을 제시한다. 즉, 웹 어플리케이션에서의 File Upload 취약점을 식별하고, 효과적인 보안 정책과 기술적 대책을 도입하여 이러한 위협에 대비할 필요가 있다는 결론을 도출한다.

CONTENTS

List of Figures

Figure 1.

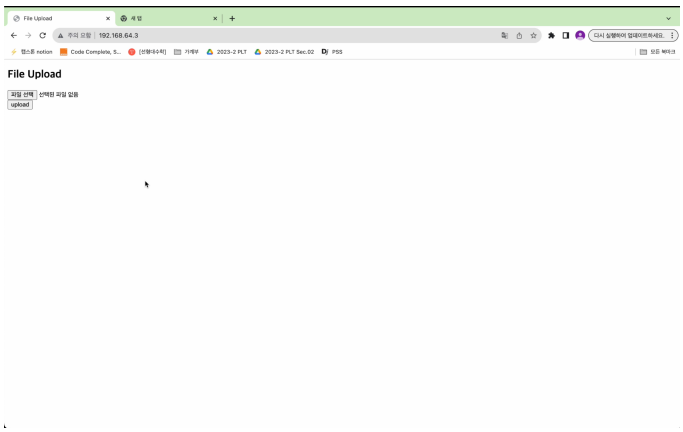


Figure 2.

Figure 3.

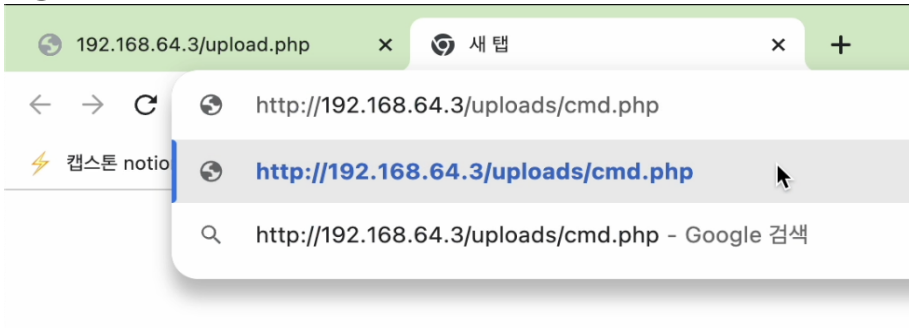


Figure 4.

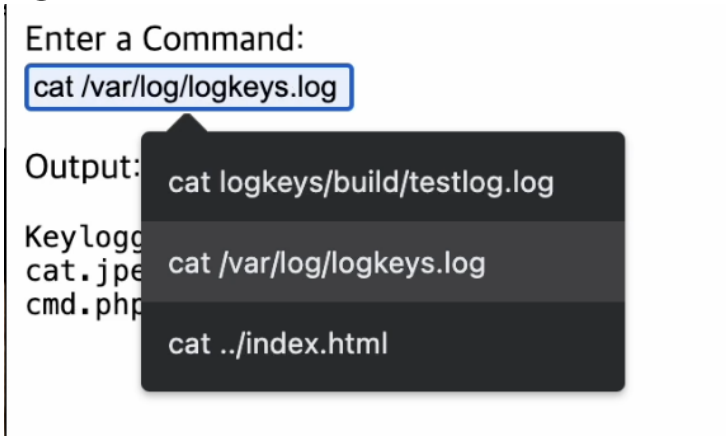


Figure 5.

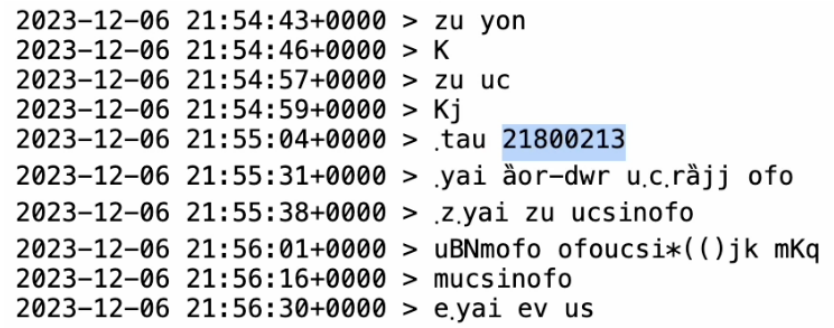


Figure 6.

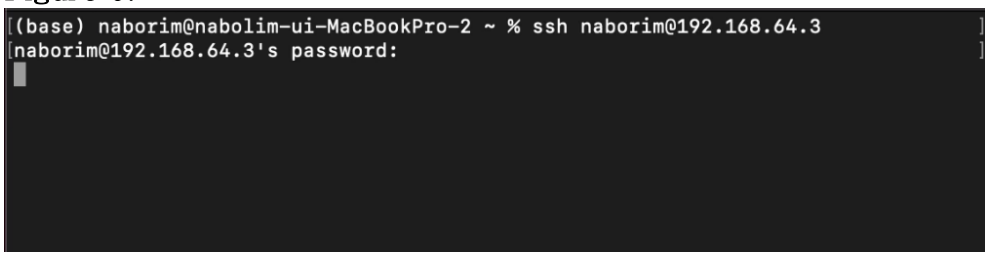
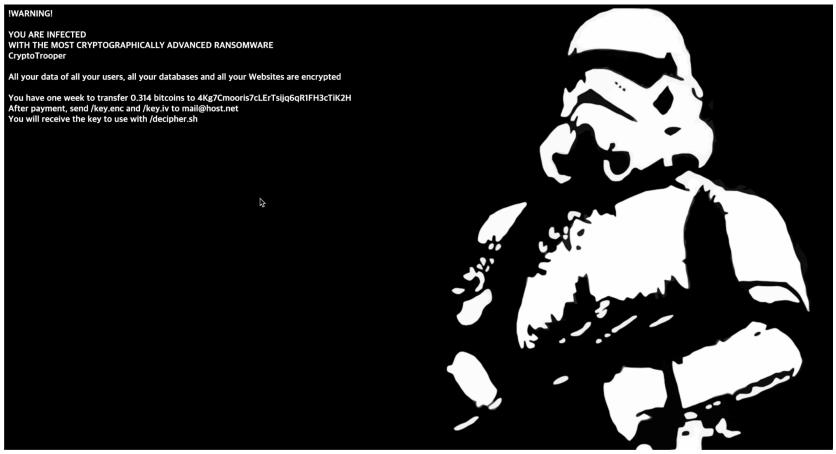


Figure 7.



I. Introduction

최근의 사이버 보안 환경에서는 다양한 공격과 위협에 대한 대비가 필수적이다. 이에 따라 보안 전문가들은 새로운 공격 기술 및 취약점에 대한 이해를 통해 조기 대응 및 방어 전략을 수립해야 한다. 본 연구에서는 특정한 해킹 시나리오를 가정하고, 해당 시나리오를 통해 시스템이 어떻게 공격당할 수 있는지에 대해 상세히 살펴보고자 한다.

본 연구에서는 시나리오에 사용되는 다양한 보안 취약점과 공격기법에 대해 설명하고, 사이버 공격자가 서버를 타깃으로 피싱 메일 및 취약점을 활용한 공격을 수행하는 시나리오를 제시한다. 공격자는 피싱 메일을 이용하여 피해 시스템에 악성 파일을 유도적으로 설치하고, 그 후에는 웹쉘을 업로드하여 시스템에 대한 외부 제어 권한을 확보한다. 이를 통해 keylogger 를 이용하여 로그를 기록하고 관리자 계정의 비밀번호를 탈취한 후, SSH 를 통해 시스템에 접근하여 랜섬웨어를 실행시킨다. 나아가 시나리오에서 사용된 취약점을 보완하기 위한 방법을 고안하고 그들 중 일부를 실제로 적용한 후속 시나리오를 시행한다..

본 연구에서의 시나리오를 통해 서버 보안의 중요성과 다양한 공격 기술을 파악함으로써, 보안 전문가 및 시스템 관리자들이 보다 강력한 방어 및 대응 전략을 수립할 수 있도록 도움을 제공하고자 한다.

II. Overview

1. File upload

File Upload 은 웹 어플리케이션에서 사용자가 클라이언트(사용자의 디바이스)에서 서버로 파일을 전송하는 기능을 나타낸다. 이 기능은 사용자들이 웹을 통해 다양한 형식의 파일을 서버에 업로드하는 주요 수단 중 하나로, 주로 이미지, 동영상, 문서 등을 업로드하는 데 활용된다. 이는 현대 웹 어플리케이션의 필수적이고 불가피한 부분으로, 사용자와 서버 간에 데이터를 주고받는 핵심 기능이다. 그러나 이러한 편리성은 동시에 보안 취약점의 발생 가능성을 내포하고 있다.

1.1 File upload vulnerability

파일 업로드 취약점은 웹 응용 프로그램에서 발생할 수 있는 보안 문제 중 하나로, 사용자가 업로드한 파일을 처리하는 부분에서 발생할 수 있다. 이 취약점은 공격자가 악성 파일을 업로드하여 웹 응용 프로그램을 공격하거나 사용자 데이터를 유출하는 데 사용될 수 있다. 아래는 파일 업로드 취약점과 관련된 주요 사항들에 대한 설명이다.

1. 파일 업로드 처리 부분 검증 부족:
   - 보통 파일 업로드 기능은 사용자가 업로드한 파일을 저장하고, 이후에 해당 파일을 다운로드하거나 특정 작업에 활용한다. 이때, 업로드된 파일에 대한 검증이 충분하지 않으면, 공격자가 악성 파일을 업로드하여 시스템에 피해를 입힐 수 있다.

2. 파일 확장자 및 MIME 타입 검증 우회:
   - 일부 웹 응용 프로그램은 업로드된 파일의 확장자나 MIME 타입을 통해 파일의 유효성을 검증한다. 그러나 이러한 검증이 충분하지 않거나 우회될 경우, 공격자는 악성 파일을 다른 확장자로 변환하거나 MIME 타입을 변경하여 검증을 우회할 수 있다.

3. 실행 가능한 파일 업로드:
   - 웹 응용 프로그램에서는 일반적으로 실행 가능한 파일(예: PHP, ASP, JSP)의 업로드를 허용하지 않아야 한다. 공격자가 실행 가능한 스크립트를 업로드하고 실행시킴으로써 시스템에 악성 코드를 삽입할 수 있다.

4. 파일 이름 충돌 공격:
   - 파일 이름 충돌은 공격자가 이미 존재하는 파일의 이름을 사용하여 악성 파일을 업로드하는 기술을 나타낸다. 웹 응용 프로그램은 이를 방지하기 위해 적절한 방어 메커니즘을 구현해야 한다.

5. 보안 헤더 및 권한 부족:
   - 웹 서버와 웹 응용 프로그램은 업로드된 파일에 대한 적절한 보안 헤더를 설정하고, 업로드된 파일에 접근할 때 권한 검사를 수행해야 한다.

취약점을 방지하기 위해 웹 응용 프로그램에서는 파일 업로드를 안전하게 처리하는 메커니즘을 구현하고, 사용자가 업로드한 파일에 대한 검증 및 제어를 강화해야 한다. 또한 보안 업데이트를 수시로 적용하여 최신 보안 취약점에 대한 방어를 강화하는 것이 중요하다.

1.2 File upload attack

파일 업로드 취약점은 웹 응용 프로그램에서 발생할 수 있는 보안 취약성 중 하나로, 사용자가 업로드한 파일을 처리하는 부분에서 발생할 수 있다. 이러한 취약점을 통해 공격자는 악성 파일을 시스템에 업로드하거나 실행하여 다양한 공격을 수행할 수 있다. 아래는 파일 업로드 공격의 실제 사례에 대한 설명이다.

1. 워드프레스 TimThumb 취약점 (2011):
   - TimThumb 은 워드프레스에서 사용되는 이미지 리사이징 스크립트 중 하나였다. 2011 년에 TimThumb 에서 발견된 취약점을 통해 공격자는 원격에서 PHP 파일을 업로드하고 실행할 수 있었다.

2. File Upload XSS 취약점 (2014):
   - 몇몇 웹 응용 프로그램에서 파일 업로드 취약점이 결합된 Cross-Site Scripting (XSS) 취약점이 발견되었다. 사용자가 업로드한 파일의 이름이나 내용을 이용하여 악성 스크립트가 실행되는 경우가 있었다.

3. 미디어위키 (MediaWiki) 취약점 (2015):
   - MediaWiki 는 위키 소프트웨어로 사용되고 있다. 2015 년에 발견된 취약점을 통해 공격자는 업로드된 파일의 MIME 타입을 변조하여 서버 측 코드 실행을 유도할 수 있었다.

4. Blue Coat 보안 기기 취약점 (2016):
   - Blue Coat 보안 기기는 업로드된 파일의 MIME 타입을 제대로 확인하지 않는 취약점이 발견되었다.

이러한 실제 사례들은 파일 업로드 취약점이 어떻게 공격자에 의해 악용될 수 있는지를 보여주고 있다. 이러한 공격으로부터 보호하기 위해서는 적절한 검증 및 보안 조치를 통해 업로드된 파일을 안전하게 처리하는 것이 중요하다. 보안 업데이트를 정기적으로 적용하여 취약점을 최소화하고, 사용자에게 신뢰할 수 있는 파일 형식만을 허용하는 등의 방어책을 마련해야 한다.

2. Keylogger

Keylogger, 다른 말로 Keystroke logger 또는 Keyboard capturing 은 사용자가 입력을 수행하는 동안 키 입력을 추적하고 기록하는 malware 또는 hardware 를 일컫는 용어이다. 해커가 피해자의 키 입력을 열람하기 위해 사용하는 가장 일반적인 방법이며, 변종에 따라서는 컴퓨터와 접촉하는 다른 장치로 확산될 가능성도 있다. 그 종류는 크게 software keylogger 와 hardware key logger 로 분류된다.

Software keylogger 의 경우 대부분 사용자의 컴퓨터에 설치할 수 있는 애플리케이션 형식으로 구성된다. 어떤 경로를 통해서라도 Software keylogger 는 한번 설치되고 작동되면 기기에서 사용중인 OS 의 거의 모든 키 입력을 모니터링하여 추적하고 기록할 수 있다. 또한 프로그램의 작성 방식에 따라 기록한 정보를 해커에게 자동으로 전송시키는 기능과 같은 부가기능을 삽입하여 스파이웨어의 한 종류로 발전시킬 수도 있다.

hardware keylogger 는 Software keylogger 와는 달리 대상 컴퓨터에 물리적으로 연결될 수 있는 장치 형식으로 구성된다. 대상 컴퓨터와 물리적 접촉이 필요하다는 점에서는 보다 설치가 까다로운 편이나, 한번 구성된 후에는 software keylogger 와 마찬가지로 동작할 수 있으며 백신 프로그램 등에도 감지되지 않기에 더욱 강력하다. 조직에서 네트워크에 액세스하는 인물과 네트워크에 연결된 하드웨어 장치 등을 주의깊게 모니터링하지 않는다면 이는 감지되지 않은 채 오래도록 취약점으로서 노출될 수 있다.

keylogger 의 동작은 사용자가 키보드에서 키를 누르는 시점과 키 입력의 정보가 모니터에 display 되는 시점 사이에서 이루어진다. 그 구현을 위한 방법은 다음과 같이 다양하다.

- 키보드와 화면을 볼 수 있는 비디오 카메라를 사용하여 키 입력을 추적하기
- 키보드-컴퓨터 간 상호작용을 촉진하는 드라이버를 키 입력을 기록하는 드라이버로 교체하여 기록된 내용을 확인
- 키보드 스택 내부의 필터 드라이버 혹은 데이터간의 유사성을 사용하는 커널 기능을 사용하기.
- 키보드 자체의 내부, 혹은 배선 내부에 하드웨어 버그를 삽입하기
- 둘 이상의 프로그램에서 사용되는 동적 연결 라이브러리(DDL)의 기능을 가로채기
- 시스템 후크를 사용하여 키를 누를 때마다 생성되는 각 알림을 가로채기

이러한 keylogger 는 사용자 본인을 위해 사용될 때도 있지만, 해커에 의한 도구로 사용되는 일이 잦은 편이다. 이럴 경우 실제 keylogger 의 사용자는 keylogger 를 이용하고자 하는 자와 상이하게 되고, keylogger 가 작동하기 위해서는 software keylogger 와 hardware keylogger 모두 사용자의 기기에 사전 설치가 필요하므로 공격자는 피해자의 기기에 keylogger 가 설치되도록 유도하여야 한다. 이를 위해서는 또한 다양한 방법이 사용되는데, 대표적인 방법은 다음과 같다.

- Spear Phishing: 합법적이고 익숙하게 느껴지는 피싱 이메일, 링크 등을 전송하거나 유포하여 피해자의 클릭을 유도한다. 친척이나 친구, 거래처 등이 보낸 것 처럼 위장하거나 안전한 것으로 보이는 이메일, 문서 등이 열릴 때 자동으로 keylogger 가 설치되도록 할 수 있다.

- Trojan Horse: 다른 안전하거나 필수적인 프로그램의 번들에 키로거를 끼워넣어 함께 다운로드되고 실행되도록 유도한다.

- Drive-by Download: keylogger 의 설치 경로를 악성 웹사이트 등에 숨겨두어 해당 사이트를 방문하면 프로그램이 자동으로 설치되도록 한다. 설치된 코드는 감지되지 않은 채 백그라운드에서 실행되며 동작한다.

- Trojan horse: keylogger 를 단일 프로그램이 아닌 여러 유용한 프로그램들의 번들로 끼워넣어 피해자의 설치를 유도한다. 피해자가 번들을 다운로드 받을 때 함께 설치된 뒤 사용자의 키 입력을 추적하여 해커가 엑세스한 장치로 정보를 전송할 수 있다.

일부 키로거는 루트킷과 함께 설치된 후 일반적인 설치 파일 혹은 백신 등으로 스스로를 위장하여 사용자 모드나 커널 모드에서 마스크 되고 자신을 숨길 수 있다. 더하여, 변종에 따라 어떤 keylogger 는 장치 자체에 추가적인 문제를 일으킬 가능성도 있다. 사용자의 key 입력을 가로채기 위한 여러 과정들 중 장치의 민감한 설정을 바꾸거나 대체할 수 있기 때문이다. 이는 감염된 장치의 유형에 따라 서로 다른 양상으로 나타나며 keylogger 로 인한 피해의 한 측면이 될 수 있다.

keylogger 는 그 자체를 활용한 정보 유출에도 문제가 있지만 탈취한 정보 중 민감한 정보나 id, password 등의 계정 정보가 통해 2 차, 3 차 공격의 기반으로 이어질 수 있다는 점에서 특히 중요성이 드러난다. 해커가 사용자의 키 입력을 분석함으로써 얻을 수 있는 수많은 정보들이 있기에 keylogger 를 이용한 공격에 당한 피해자는 또 다른 보안 시스템의 취약점을 드러낸 것이나 다름 없다. 탈취된 정보는 비밀번호, 이메일 계정, 은행 또는 투자 계좌, 또는 개인정보를 볼 수 있는 웹 사이트의 액세스 키 등이 될 수 있으며 대체로 이 인증 수단들이 사용되는 하나 이상의 공격 대상을 새로이 노출시키게 되기 때문에 각별한 주의가 필요하다.

3. Ransomware

Ransomware 는 사용자나 조직이 본인 컴퓨터의 파일에 액세스하는 것을 거부하도록 설계된 악성 코드를 일컫는 말이다. 주로 공격자가 피해자의 기기 속 모든, 혹은 주요한 파일을 암호화하고 해독 키에 대한 몸값을 요구하는 방식으로 범행이 이루어진다. 해킹을 이용한 범행 수법 중 높은 수익성을 가졌기에 첫 등장으로부터 여러 발전을 겪어오며 각기 다른 특성을 가진 수십가지 변종이 만들어졌다. 특히 COVID-19 사태로 인해 많은 조직에서 급격한 원격 근무로의 전환이 이루어지며 생긴 커다란 보안 공백을 노려 수많은 공격 사례가 발견된 바 있다. 실제로 2020 년 3 분기의 랜섬웨어 공격은 같은 해 상반기에 비해 절반가량 증가한 것으로 보고되었다. Ransomware 는 COVID-19 가 비교적 정상화된 오늘날까지도 사회에서 기업/공공 서비스의 주요한 부분을 마비시키며 다양한 조직에 심각한 피해를 입히고 있다.

Ransomware 에는 다양한 변종이 존재하는데, 그중 널리 알려진 것들은 다음과 같다.

- Ryck: 표적화된 랜섬웨어 변종의 한 예로, keylogger 와 비슷하게 spear fisging 등의 방법을 통해 전달되거나 손상된 사용자 자격 증명, RDP(Remote Desktop login Protocol)을사용해 기업 시스템에 로그인하는 방식으로 전달된다. 주요 리소스를 차지하는 특정 유형의 파일들을 암호화한 후 몸값을 요구하며, 현존하는 랜섬웨어 중 가장 비용이 많이 드는 유형으로 꼽힌다.

- maze: 최초의 랜섬웨어 변종으로 뽑히며, 암화하기 이전 피해자의 컴퓨터에서 민감한 데이터를 수집하여 몸값 요구 사항이 충족되지 않을 시 해당 데이터들을 유포하거나 입찰시키는 등의 협박이 동반된다. 이 때 몸값에는 데이터의 유출 방지에 대한 비용이 추가로 포함되게 된다.

- REvil: 대규모 조직을 표적으로 삼는 랜섬웨어 변종. 인터넷상에서 가장 잘 알려진 랜섬웨어 제품군 중 하나로, 러시아어 권의 Revil 그룹이 운영하고 있다. 파일을 암호화하는 동시에 기업으로부터 데이터를 훔치는 이중 갈취 기술을 사용하며 첫 차례의 몸값 지불 뿐만 아니라 두번째 지불을 요구하며 데이터 공개를 빌미삼아 협박하는 것이 특징이다.

Ransomware 의 공격 단계는 다음과 같다. 공격 대상지에 랜섬웨어 프로그램을 다운로드하고 실행시키거나 실행을 유도한다. 랜섬웨어 프로그램이 시스템에 엑세스하여 공격자가 시스템 파일을 암호화한다. 일부 변종은 해독 키 없이 복구하기 더 어렵게 만들기 위해 파일의 백업 및 복사본을 삭제한다. 피해자에게 돈을 요구하고 돈이 지불되면 복호화를 위한 키를 제공한다.

III. Experiment

1. Specifications

본 연구는 웹 응용 프로그램에서 발생하는 취약점 중 하나인 파일 업로드 취약점을 통한 랜섬웨어 공격을 시뮬레이션하여, 시스템 보안 취약성에 대한 분석과 취약점 보완에 대한 연구가 목적이다. 따라서, 공격 대상의 시스템이 Keylogger 파일, 웹 쉘과 랜섬웨어 파일을 통해 침해될 것으로 가정한다. 임의로 설정한 웹 사이트를 공격 대상으로 설정하였고, Ubuntu 20.04 환경에서 진행되었다.

2. Experiment method

먼저 파일 업로드의 취약점을 가지고 있는 웹 사이트의 서버에 피싱 메일을 전송하여 Keylogger[1]가 심어져 있는 파일을 설치하고 실행하도록 유도하고, 웹 사이트에 접속하여 일반적인 이미지 파일을 업로드한다.

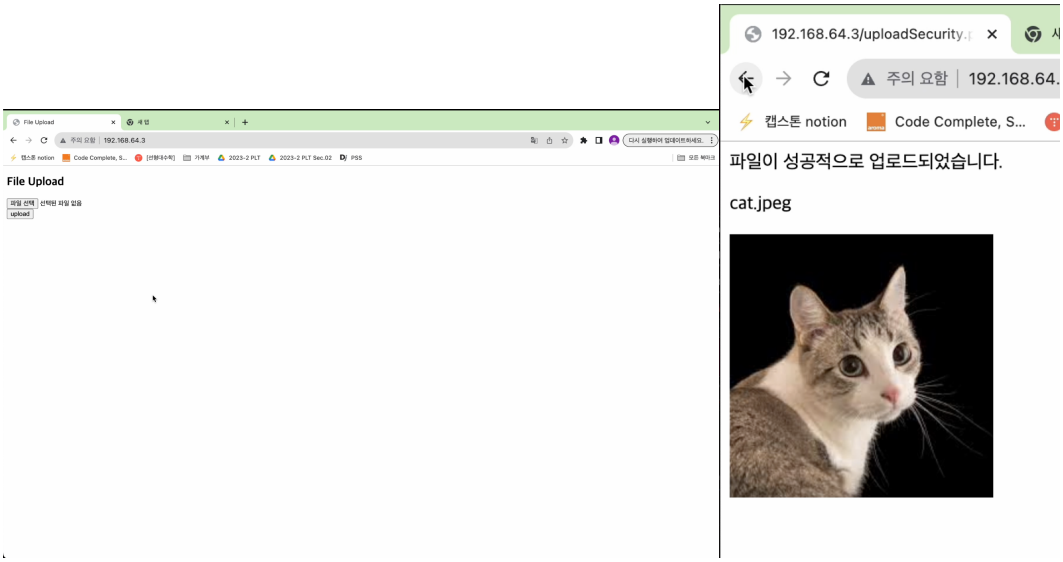


그림 1. 파일 업로드 화면

이미지 주소를 복사해서 주소창에 입력하면 업로드 한 파일이 저장되는 폴더를 알아낼 수 있다. 따라서, 웹 쉘 파일과 랜섬웨어 파일[2]을 업로드하고 이전에 알아낸 폴더를 통해 폴더 경로 + 업로드 한 웹 쉘 파일명을 입력하면 웹 쉘에 접속할 수 있다.

[1] https://github.com/kernc/logkeys.git
[2] https://github.com/jdsecurity/CryptoTrooper.git

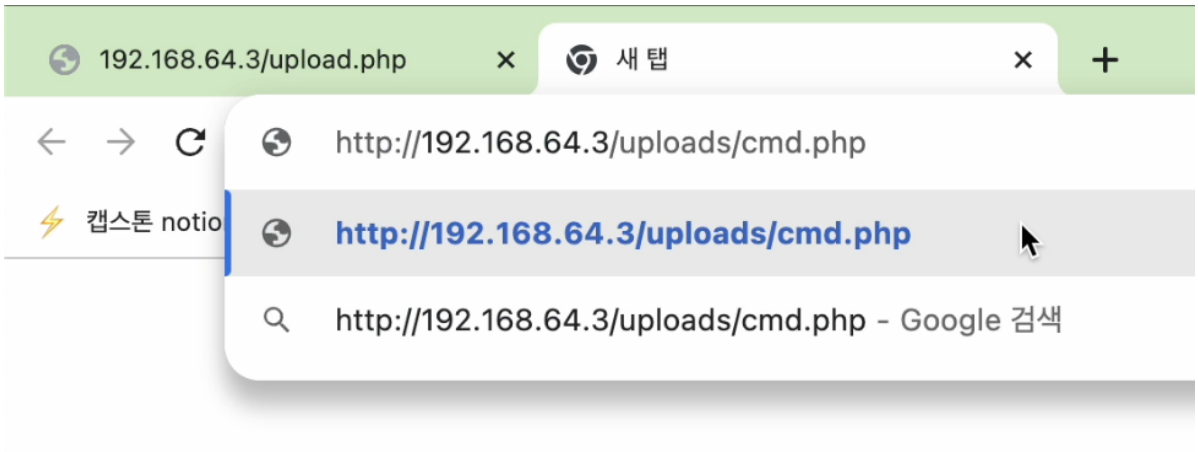


그림 2. 파일 업로드 폴더 경로 확인

시스템 관리자가 만약 시스템 명령어 및 관리자 비밀번호를 입력한 기록이 있다면 Keylogger 파일에 기록되고 있을 것이다. 웹 쉘을 통해 Keylogger 파일을 열람하여 관리자의 비밀번호를 탈취한다.

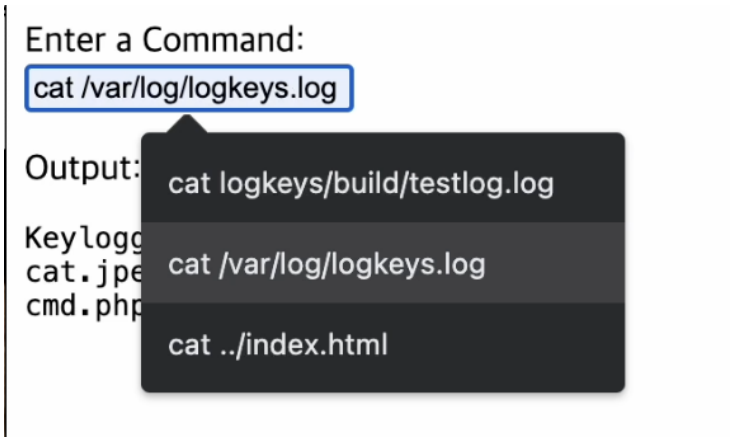


그림 3. Keylogger 파일

```
2023-12-06 21:54:43+0000 > zu yon
2023-12-06 21:54:46+0000 > K
2023-12-06 21:54:57+0000 > zu uc
2023-12-06 21:54:59+0000 > Kj
2023-12-06 21:55:04+0000 > .tau 21800213
2023-12-06 21:55:31+0000 > .yai àor-dwr u.c.rȁjj ofo
2023-12-06 21:55:38+0000 > .z.yai zu ucsinofo
2023-12-06 21:56:01+0000 > uBNmofo ofoucsi*(()jk mKq
2023-12-06 21:56:16+0000 > mucsinofo
2023-12-06 21:56:30+0000 > e.yai ev us
```

그림 4. Keylogger 를 통한 관리자 비밀번호 탈취

탈취한 비밀번호로 ssh 를 통해 관리자 계정으로 로그인 하여, sudo 권한으로 랜섬웨어 파일을 실행시켜 모든 파일을 암호화한다.

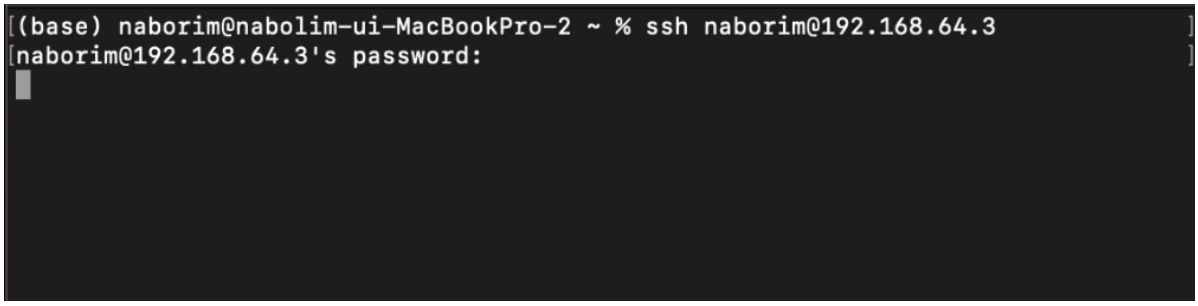


그림 5. 탈취한 관리자 비밀번호로 ssh 를 통한 접속

그림 6. 랜섬웨어로 감염된 관리자 웹 사이트

이와 같은 공격을 보완하기 위해서 파일의 확장자를 검증하여 이미지 업로드 웹사이트의 경우 이미지 확장자(jpeg, gif, png, jpg)의 파일만 업로드 할 수 있도록 설정하거나, 업로드 파일의 실행 권한을 제한하거나, 외부에서 파일을 식별할 때 파일명을 무작위로 지정하여 식별할 수 없도록 하는 방법 등을 통해 파일 업로드 공격으로 부터 시스템을 방어하고 있다.

IV. Conclusion

악성 파일 업로드 취약점을 통한 공격은 여러 가지 방법으로 보완되고 있으나, 현재까지도 계속해서 수행되고 있는 공격 방법 중 하나이다. 이러한 공격은 사용자의 개인정보 유출, 시스템 침입, 악성 코드 실행 등으로 이어질 수 있기 때문에 보안 강화가 필수적이다.

보완 강화에는 다양한 방법이 있는데 확장자 검증을 통해 블랙리스트가 아닌 허용된 화이트 리스트를 기준으로 확장자를 확인하는 방법, 파일 유효성 검증을 통해 업로드 파일의 실행 권한을 제한하는 방법, 저장되는 파일이 외부에서 식별되지 않도록 파일명을 무작위로 지정하는 방법, 다운도르 된 파일에 대한 바이러스 및 무결성 검사를 하고 통과하지 못할 경우 파일을 디렉토리에서 제거하는 방법, 파일 업로드 전처리 프레임워크를 사용하는 방법 등 다양한 방법이 제시되고 있다.

하지만 파일 업로드 공격은 지속적으로 진화하고 있으며, 이에 대한 방어 대책도 지속적으로 발전해야한다. 미래에는 머신 러닝과 인공 지능을 활용하여 신속하고 정확한 악성 파일 탐지 시스템을 개발하는 것이 중요할 것이며, 추가적인 연구와 협력을 통해 보안 취약점에 대한 지속적이고 포괄적인 대응이 이루어져야 할 것이다.

IV. References

1. 성상훈. (2014. 2. 4) 미디어위키에 심각한 보안 취약점 발견. Digital Today. https://www.digitaltoday.co.kr/news/articleView.html?idxno=43478
2. Fortinet. (n.d.). *What is Keyloggers*. https://www.fortinet.com/kr/resources/cyberglossary/what-is-keyloggers
3. Check Point Software Technologies. (n.d.). *Ransomware Threat Prevention.* https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/