전 세계 약 5억 명이 사용하는 압축 프로그램에서 취약점 발견
CVSS(공통 취약점 등급 시스템) 위험도 최고점 10점 중 7.8점 평가

WinRAR 원격코드 실행 취약점

요약

1. WinRAR는 전세계 사용자 약 5억명을 확보한 압축 프로그램으로
   1995년 출시 이후 꾸준히 버전업 지원 중
2. 사용자가 많고 공격 재현이 쉬운 탓에 2022년 9월 처음 발견됐으나
   지속적으로 악용될 가능성있음
3. CVSS 위험도 7.8점은 고위험군에 속하는 점수이며
   해당 취약점이 악용될 경우 큰 피해가 발생할 수 있음
4. WinRAR는 취약점 발견 즉시 보안패치를 릴리즈했으나
   모든 사용자에게 적용되기까지 상당 시간 소요되어 피해발생이 지속될 것으로 예상
5. WinRAR 원격코드 실행 과정
   1) 조작된 압축파일을 타깃에게 유포
   2) 취약한 버전의 WinRAR로 파일을 실행하여 '미끼파일' 클릭 시 악성코드 실행

대응 방안

1. WinRAR 사용자는 프로그램을 최신 형상으로 유지
2. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
3. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션
4. PC 취약점을 주기적으로 점검, 보완
5. 신뢰할 수 없는 메일의 첨부파일 실행 금지
6. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결 차단
7. OS나 어플리케이션은 최신 형상 유지

목차

1. 개요

1.1 배경

1.2 파일 정보

2. 분석

2.1 악성 압축 파일 유포

2.2 임시 압축 해제

2.3 악성 파일 실행

2.4 결론

3. Privacy-i EDR 탐지 정보

4. 대응

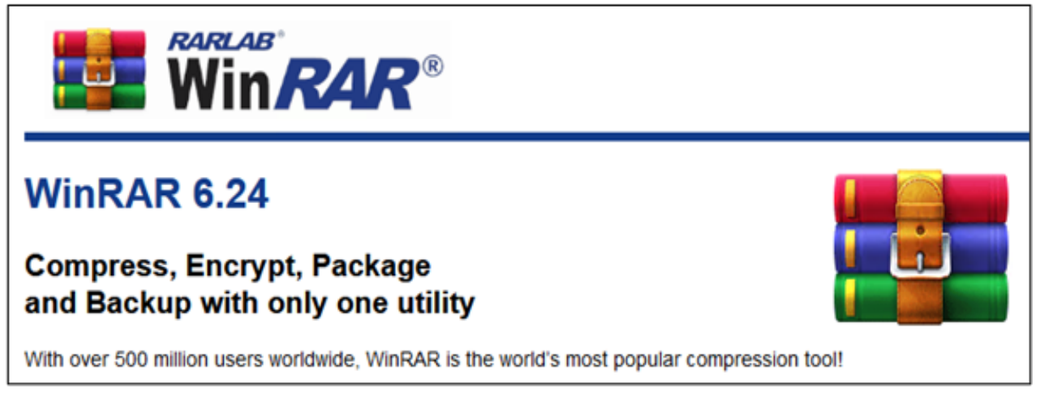
5. 참고자료

5.1 국내 피해 현황

5.2 국제 피해 현황

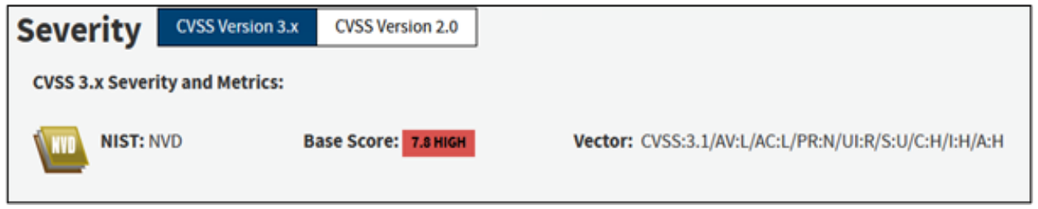
1. 개요

1.1 배경



[그림 1] WinRAR 공식 홈페이지

2023년 8월, WinRAR 6.22 버전 이하의 모든 제품에서
원격 코드 실행이 가능한 취약점 CVE-2023-38831이 공개되었다.
WinRAR은 1995년에 출시된 상용 압축 프로그램으로 약 30년 동안 지속적으로 업데이트를 지원하고 있다.
해당 제품은 사용자가 많고 공격의 재현이 쉽기에 현재까지 공격이 활발히 이어지고 있다.
이에 WinRAR 사용자는 주의가 필요하다. WinRAR은 Windows, Linux, macOS, Android 등
다양한 운영체제를 지원하지만, 본 보고서에서 다룰 취약점은 Windows에서 동작하는
WinRAR에서 발생하므로 Windows 환경을 기반으로 작성했다.

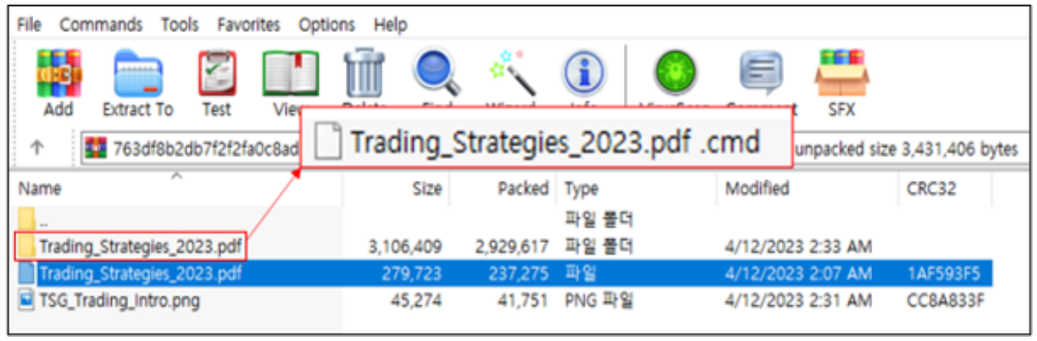


[그림 2] CVE-2023-38831 취약점 CVSS 평가 결과

평가지표	결과
Attack Vector (공격 지점)	Local
Attack Complexity (공격 복잡도)	Low
Privilege Required (필요 권한)	None
User Interaction (상호작용 필요 여부)	Required
Scope (영향 범위)	Unchanged
Confidentiality (기밀성 침해 정도)	High
Integrity (무결성 침해 정도)	High
Availability (가용성 침해 정도)	High

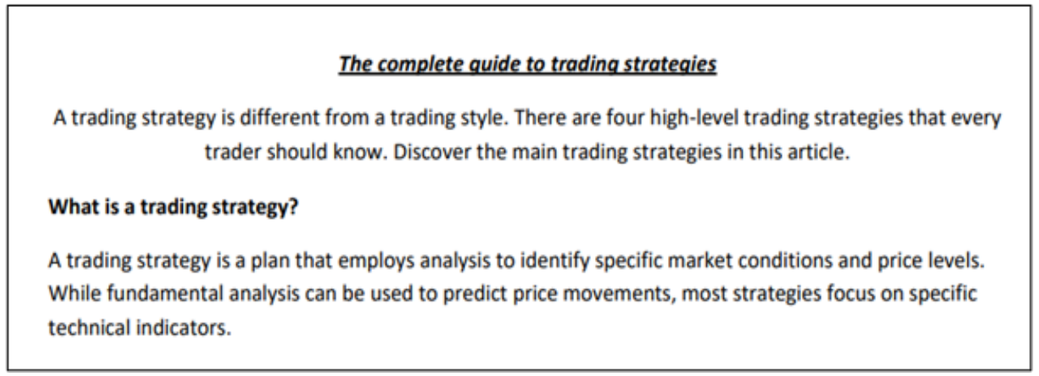
[표 1] CVE-2023-38831 취약점 CVSS 평가 결과

CVE-2023-38831은 CVSS(Common Vulnerability Scoring System) 평가에서
7.8점을 받아 높은 위험도의 취약점으로 분류되었다.
원격 코드 실행이 가능하므로 기밀성, 무결성, 가용성 침해 측면에서 높은 점수를 받았고,
공격 복잡도가 낮아 재현이 쉽다는 점 또한 영향을 미쳤다.
해당 취약점이 성공적으로 발현되려면 피해자와의 상호작용이 필요하다.
따라서 공격자는 피싱 메일을 유포하거나 피싱 페이지의 첨부 파일을 이용하는 등의 방식으로
피해자의 상호작용을 유도한다.



[그림 3] WinRAR 압축 파일 미리보기 화면

[그림 3]은 WinRAR로 압축 파일을 열었을 때의 미리보기 화면이다.
눈에 띄는 점은 파일명과 폴더명이 동일하다는 것인데,
이는 취약점을 발현시키기 위해 제작된 압축 파일에서 공통적으로 보이는 특징이다.
피해자는 미끼 파일을 실행하여 상호작용을 수행한다.
미끼 파일의 확장자는 무엇을 사용하든 상관이 없지만,
공격의 성공률을 높이기 위해서 이미지나 PDF 등의 파일 형태가 주로 사용되고 있다.
압축 프로그램에서 파일을 열어 내용을 간단히 확인하는 경우가 많기 때문이다.
미끼 파일을 실행하면 취약점이 발현되고 동일한 이름의 폴더 내에 포함 되어있던 악성코드가 실행된다.



The complete guide to trading strategies

A trading strategy is different from a trading style. There are four high-level trading strategies that every trader should know. Discover the main trading strategies in this article.

What is a trading strategy?

A trading strategy is a plan that employs analysis to identify specific market conditions and price levels. While fundamental analysis can be used to predict price movements, most strategies focus on specific technical indicators.

[그림 4] 공격자의 스크립트로 실행된 미끼 파일

피해자의 PC 화면에는 일반적으로 [그림 4]와 같은 미끼 파일이 표시된다.
그러나 이는 미끼 파일이 최초로 실행된 것이 아니며 악성코드가 피해자를 속이기 위해
의도적으로 표시한 것이다. 따라서 이미 악성 행위가 수행되고 있다.

b. Critical Bug: CVE-2023-38831. A vulnerability was discovered in the processing of ZIP format. Attackers could utilize affected archives to distribute malware. User interaction is required to exploit this vulnerability.

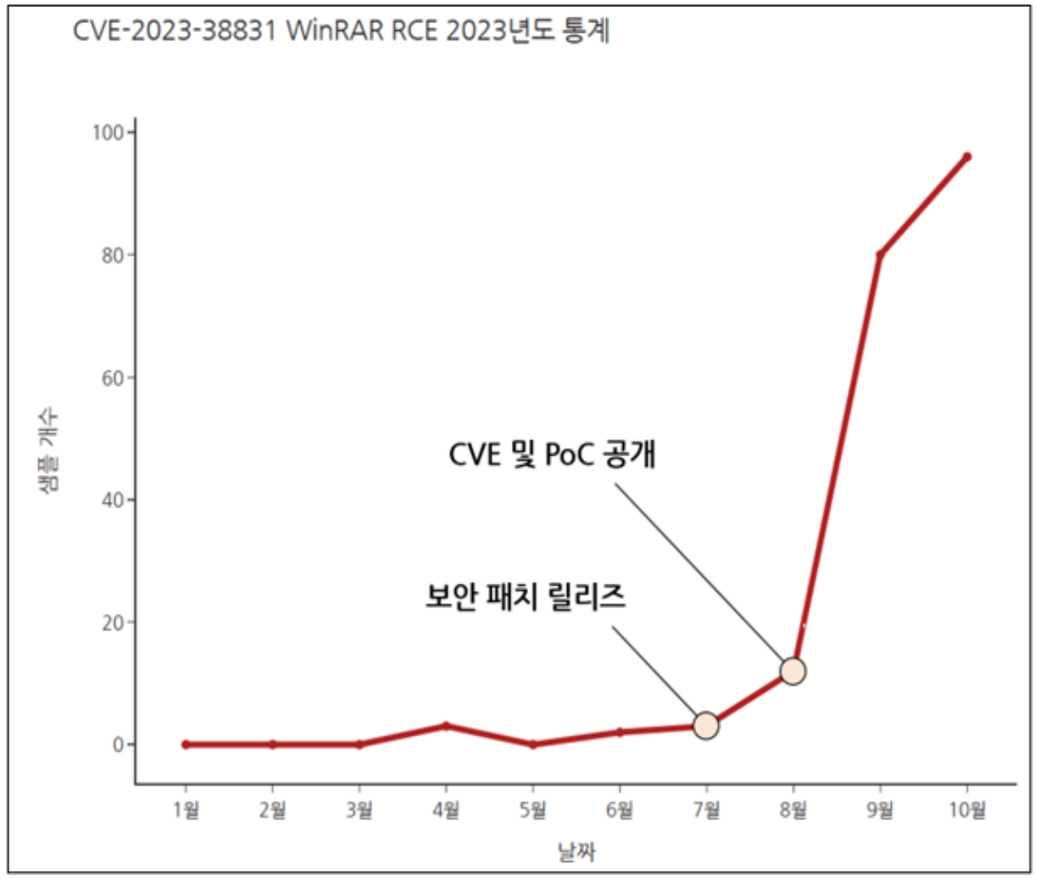
We would like to thank Andrey Polovinkin of Group-IB Threat Intelligence for reporting this bug.
www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/

Bug reported: July 2023
Fixed in 6.23 Beta Version, released: 20.07.2023
Full Version 6.23 release: 02.08.2023

[그림 5] WinRAR 6.23 버전 패치 내역

WinRAR은 2023년 7월 해당 취약점을 인지한 이후,
발 빠르게 대응하여 보안 패치가 적용된 6.23 베타 버전을 출시했고
다음 달인 8월에 6.23 정식 버전을 출시하였다. 현재는 6.24 버전까지 출시됐지만,
모든 사용자들이 보안 패치가 적용된 버전으로 업데이트하기까지는 시간이 필요해 보인다.

취약점 정보와 PoC가 공개된 후 조작된 압축 파일의 유포량은 가파르게 상승했다.
모든 사용자가 업데이트하기까지 시간이 걸린다는 점과 공격 재현이 쉽다는 점 등을 고려했을 때
동일한 상승세를 유지하거나 비슷한 수준을 이어나갈 것으로 전망된다.



[그림 6] CVE-2023-38831 샘플 유포 동향 그래프

CVE-2023-38831은 취약점 정보가 공개되기 이전인 4월부터 공격자에 의해 활용됐다.
악성코드 파일을 유포한 것으로 추정되는 조직은 2022년 9월에 최초로 식별된 Evilnum이다.[01]
취약점이 이 조직에 의해 최초로 발견됐는지는 확인 불가능하다.
본 취약점을 제보한 Group-IB 사의 위협인텔리전스 팀 또한 해당 공격 활동을 통해 취약점을 발견했다.[02]
취약점에 노출된 WinRAR을 사용하는 경우, 일괄적으로 6.23 버전 이상으로 업데이트하거나
Privacy-i EDR과 같은 보안 제품을 사용해 대책을 마련하는 것이 바람직하다.

01 Operation DarkCasino: In-Depth Analysis of Attacks by APT Group Evilnum (Part 1)

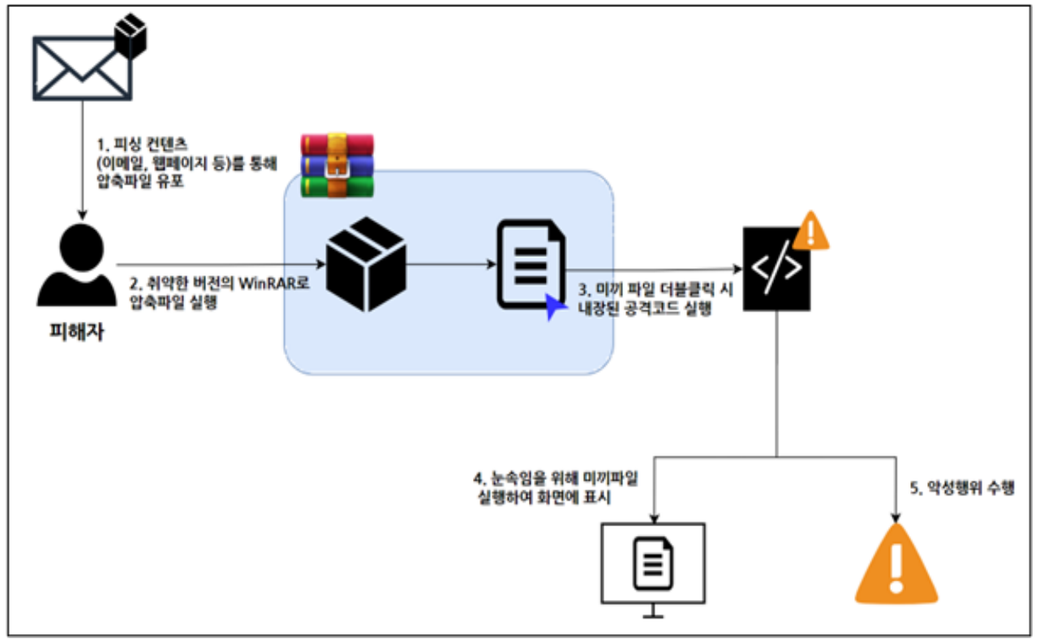
02 Traders' Dollars in Danger: CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders

1.2 파일 정보

Name	New order_jpg.r10
Type	Compressed File
SHA-256	dc4dc6829ccc4a2ef99d620ffc000220d45b113b21d7f6143908e40e338a065e
Description	Malicious Compressed File via CVE-2023-38831

[표 2] Malicious Word Document File

2. 분석



[그림 7] CVE-2023-38831 취약점 공격 순서도

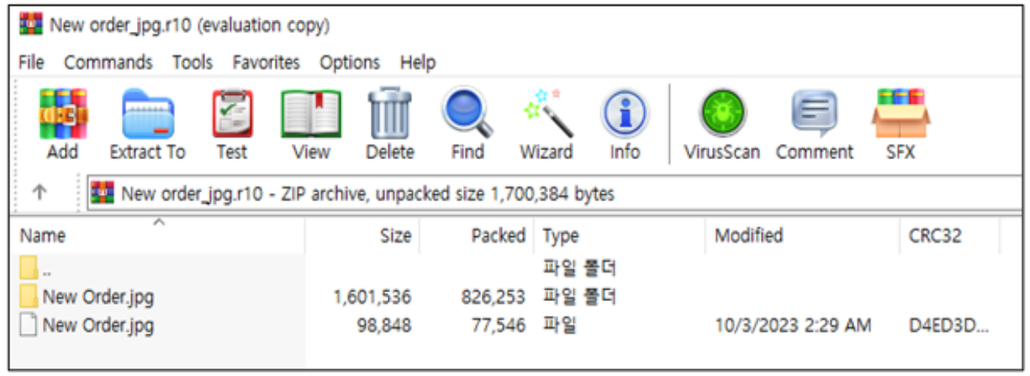
CVE-2023-38831 취약점의 공격 과정은 [그림 7]과 같다.
공격자는 취약점이 발현되도록 조작된 압축 파일을 유포한다.
압축 파일은 피싱 메일이나 웹 페이지에 첨부하여 유포하는 것이 일반적이다.
피해자가 취약한 WinRAR 버전에서 미끼 파일을 실행한다면 공격자가 유포한 악성 파일이 실행된다.

2.1 악성 압축 파일 유포

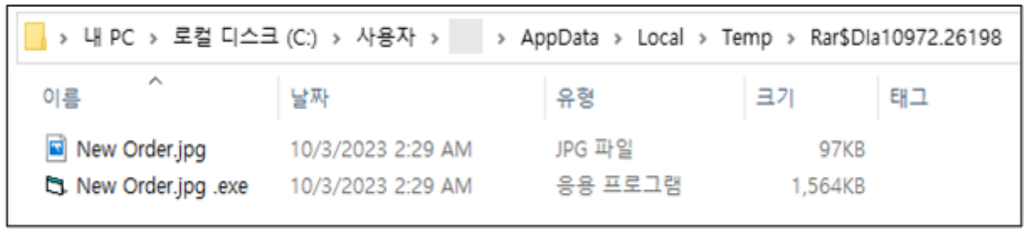
[그림 8] 피싱 메일에 첨부된 악성 압축 파일

분석에 사용된 샘플은 피싱 메일로 유포되었다.
첨부 파일은 r10이라는 생소한 확장자를 가지고 있는데,
이는 구버전의 WinRAR에서 분할 압축을 했을 때 나타나는 확장자이다.
분할 압축 파일 확장자인 .r00부터 .r29까지는 그 외 다른 압축 프로그램에 등록되어 있지 않아서
피해자의 PC에 WinRAR 이외에 또다른 압축 프로그램이 설치되어 있다고 하더라도
오직 WinRAR를 통해서만 열리도록 만들 수 있다. 즉, 공격의 성공률을 높일 수 있게 된다.

2.2 임시 압축 해제



[그림 9] WinRAR 압축 파일 미리보기 화면



[그림 10] 임시로 압축이 해제된 파일들

미끼 파일을 실행하면 WinRAR은 %TEMP% 경로에 임의 폴더를 생성하여 압축을 해제한다.
이 때 미끼 파일과 동일한 이름을 가진 폴더 내의 파일들도 동일한 경로에 함께 압축 해제된다.
압축 해제 후 WinRAR은 사용자가 선택한 미끼 파일을 실행하기 위해
파일의 경로를 인자로 삼아 ShellExecuteExW 함수를 호출한다.

2.3 악성 파일 실행

```
while ( 1 )
{
  letter = *cur;
  if ( !*cur )
    break;
  if ( letter <= 0x5Cu )
  {
    if ( letter == '.' )
    {
      p_ext = cur;                          // 가장 최근의 확장자(.*) 위치를 저장
    }
    else if ( letter == '\\' || letter == ' ' )
    {
      p_ext = 0i64;                         // 백슬래시 또는 공백을 만날 경우,
                                            // 이전 확장자 위치 삭제
    }
  }
  if ( ++cur >= extended_max_path )
    return (LPWSTR)&path[lstrlenW(path)];
}
if ( p_ext )
  return p_ext;                             // 확장자 위치 반환
return cur;
```

[그림 11] kernelbase!PathFindExtensionW 함수 의사코드

ShellExecuteExW 함수 내부에서는 PathFindExtensionW 함수를 호출해
실행할 파일의 확장자가 무엇인지 확인한다.
PathFindExtensionW 함수는 Windows의 확장 경로에서 허용하는
최대 글자 수[03] 32,767 자를 초과하지 않는 이상, 항상 경로 문자열의 마지막 문자까지 탐색한다.
경로에서 마지막에 위치한 점(.) 위치를 찾아 확장자 위치를 반환하는데,
이 때 확장자명에 공백이 있으면 파일 확장자를 찾지 못한 것으로 간주한다.

03 Maximum Path Length Limitation


```
FirstFileW = FindFirstFileW(lpFileName, &ffd);
if ( FirstFileW == -1i64 )
  goto LABEL_35;
v14 = 4i64;
do
{
  cnt_0 = 63;
  cnt_1 = 0;
  p_ext = &c_aDefExtList;
  do
  {
    if ( ((cnt_0 & 1) != 0 || cnt_1 == 6) && !StrCmpIW(&ffd.cFileName[p_basename], *p_ext) )
      break;
    ++cnt_1;
    cnt_0 >>= 1;
    ++p_ext;
  }
  while ( cnt_1 < 7 );
```

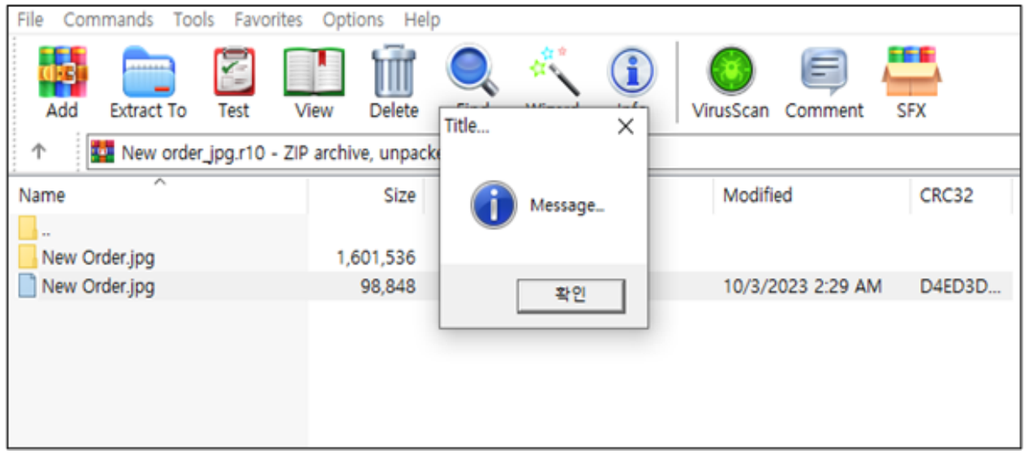
```
".pif"
".com"
".exe"
".bat"
".lnk"
".cmd"
```

[그림 12] shell32!ApplyDefaultExts 함수 의사코드

우선순위	확장자명	설명
1	.pif	DOS 바로가기 파일
2	.com	DOS 실행 파일
3	.exe	실행 파일
4	.bat	배치 스크립트 파일
5	.lnk	바로가기 파일
6	.cmd	배치 스크립트 파일

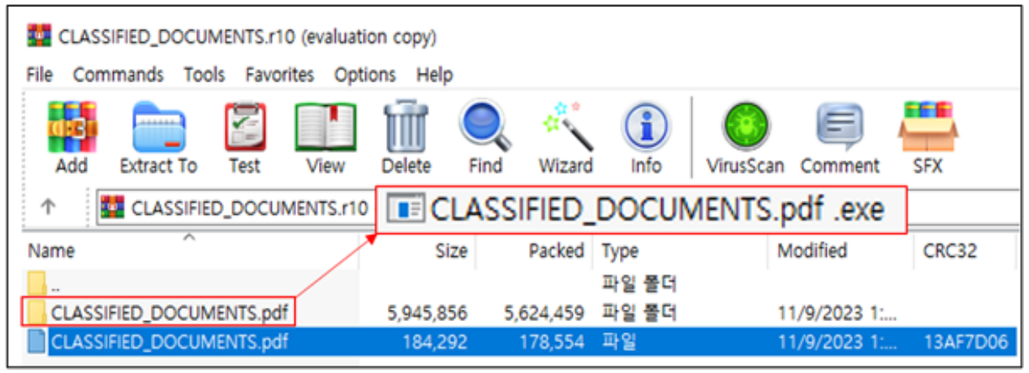
[표 3] shell32.dll에 존재하는 기본 확장자 목록

PathFindExtensionW 함수에서 파일 확장자를 찾지 못했다면
“New_Order.jpg_.*”(밑줄은 공백을 말함)와 같이 경로의 끝에 확장자를 찾기 위한
와일드카드(.*)를 삽입하여 해당 경로로 시작하는 파일이 존재하는지 검색한다.
이 때, 검색은 shell32.dll 안에 위치한 6개의 기본 확장자 중 일치하는 파일만을 대상으로 하며
이들 사이의 우선순위는 [표 3]와 같다. 일치하는 파일을 찾았다면 해당 파일을 대신 실행하게 된다.
따라서 미끼 파일 대신에 실행되는 악성 파일의 확장자는 항상 [표 3]의 확장자 중 하나를 가진다.

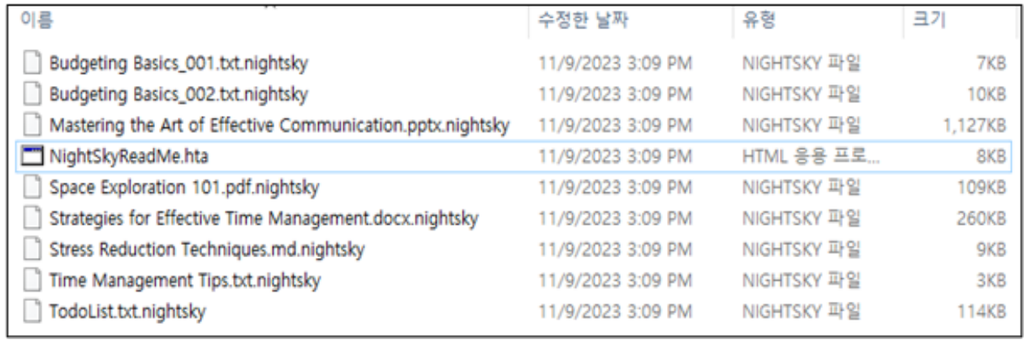


[그림 13] 미끼 파일 대신 실행된 악성코드

악성 파일 “New_Order.jpg_.exe”가 기본 확장자 목록에 대응되면서 피해자가 실행하고자 했던 미끼 파일 “New_Order.jpg_” 대신에 악성 파일이 실행되게 된다.



[그림 14] 랜섬웨어가 포함된 악성 압축 파일



[그림 15] 미끼 파일 실행 후 랜섬웨어에 감염된 모습

소만사 악성코드 분석 센터는 해당 취약점의 위험성을 확인하기 위해
압축 파일에 랜섬웨어를 포함시켜 테스트를 진행하였다. 미리 보기 화면에서 미끼 파일을 실행한 결과,
랜섬웨어가 성공적으로 실행되었고 시스템이 [그림 15]와 같이 감염되었다.

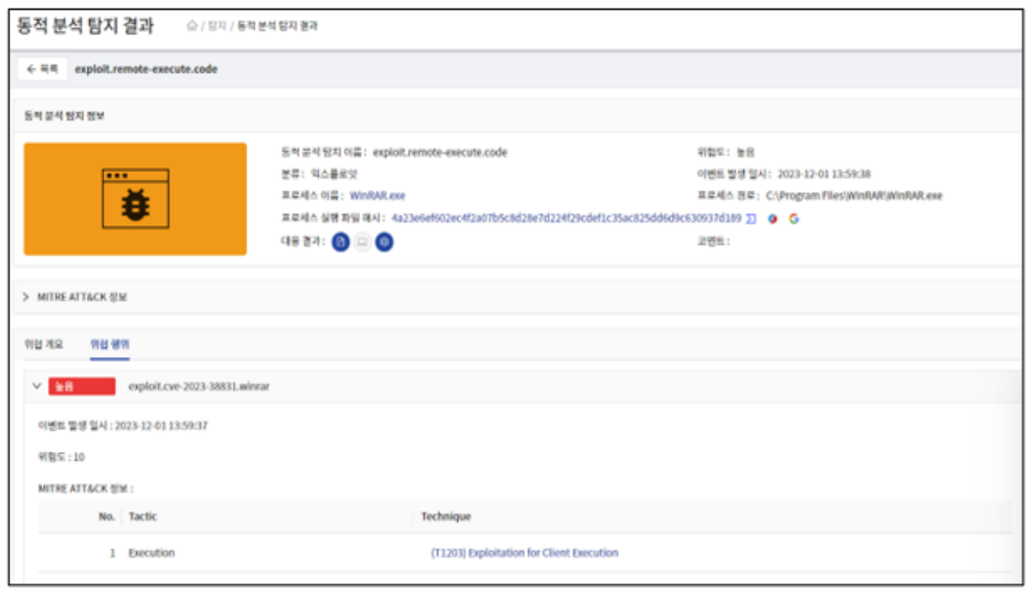
2.3 악성 파일 실행

CVE-2023-38831 WinRAR 원격 코드 실행 취약점은 공격을 성공시키기 위해
피해자의 반응을 이끌어내야 하므로 대체적으로 피싱의 성격을 띈다.
본 취약점을 통해 실행 가능한 악성 파일은 shell32.dll에 등록된 기본 확장자만 가능하다는 제약이 있지만
EXE, BAT, CMD 등 악성코드를 작성하기 용이한 확장자들이 사용 가능하여 영향을 주지 않는다.

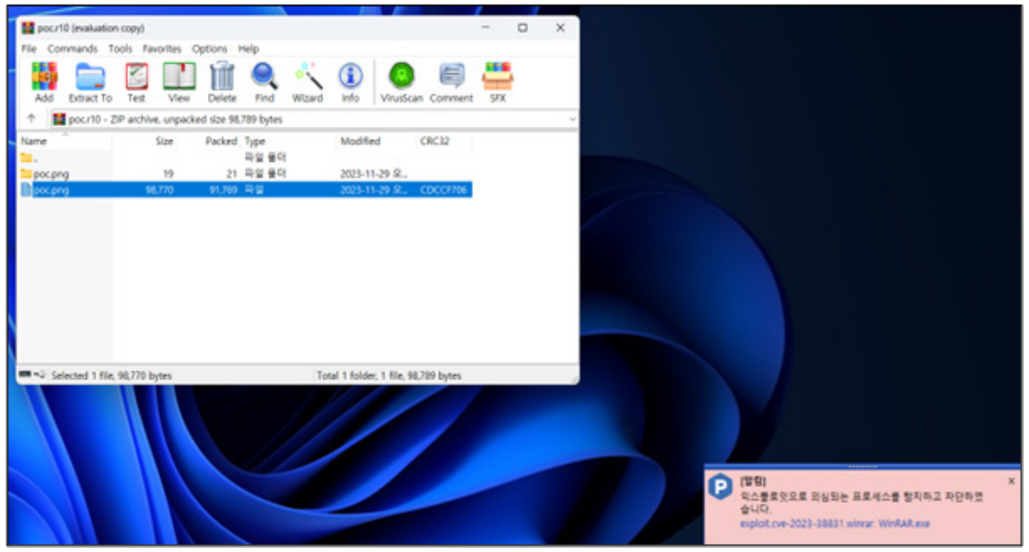
공격의 재현이 쉬운만큼 WinRAR 제품을 사용하는 조직은 빠른 대응이 필요하다.
이 취약점에 대응하기 위한 방법은 **[4. 대응]** 절을 참고하기 바란다.

3. Privacy-i EDR 탐지 정보

3.1. CVE-2023-38831 익스플로잇 행위 탐지



[그림 16] Privacy-i EDR 행위 엔진 탐지 정보



[그림 17] CVE-2023-38831 익스플로잇 시도 차단

Privacy-i EDR은 공격자의 CVE-2023-38831 익스플로잇 시도를 [그림 17]과 같이 탐지 후 차단하였다. 행위 엔진으로 공격을 선제적 차단하여 설령 피해자가 미끼 파일을 살행했더라도 악성코드를 차단할 수 있다.

4. 대응

1. WinRAR 사용자는 프로그램을 최신 형상으로 유지한다.
2. WinRAR을 최신 형상으로 변경할 수 없는 경우
   설정 화면의 Security 탭에서 “File types to exclude from extracting” 항목에 체크한 뒤,
   해당 목록에 [표 3]의 기본 확장자들을 기입한다.
   단, 이 항목을 체크하면 기본 확장자를 가진 정상 파일 또한 압축 해제가 불가하다.
3. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단한다
4. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션을 최신 형상으로 유지한다.
5. PC 취약점을 주기적으로 점검, 보완한다.
6. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지한다.
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단한다.
8. OS나 어플리케이션은 최신 형상을 유지한다.

5. 참고자료

5.1 국내 피해 현황

기업명	설명
-	식별된 피해 사례 없음

[표 4] 국내 기업 피해 현황

5.2 국제 피해 현황

기업명	설명
-	식별된 피해 사례 없음

[표 5] 국제 기업 피해 현황

본 자료의 전체 혹은 일부를 소만사의 허락을 받지 않고, 무단게재, 복사, 배포는 엄격히 금합니다.
만일 이를 어길 시에는 민형사상의 손해배상에 처해질 수 있습니다.
본 자료는 악성코드 분석을 위한 참조 자료로 활용 되어야 하며,
악성코드 제작 등의 용도로 악용되어서는 안됩니다.
㈜ 소만사는 이러한 오남용에 대한 책임을 지지 않습니다.
Copyright(c) 2024 ㈜ 소만사 All rights reserved.

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오