

LNKファイルを介して実行されるマルウェアMoonPeak – IIJ Security Diary

 sect.iij.ad.jp/blog/2026/01/dprk-moonpeak-executed-via-malicious-lnk-file

Naoki Takayama

2026年1月22日

[illegible]

2026年1月、IJは韓国のユーザを標的とした攻撃で使用されたと思われる、マルウェアを実行する悪性のLNKファイルを観測しました。マルウェア解析を実施した結果、このLNKファイルは北朝鮮 (DPRK) に帰属するとされる脅威アクター¹が用いるマルウェアMoonPeak (マルウェアXenoRATの亜種) を実行するために使用されたことが判明しました。この記事では、既存のレポート等で詳細が取り上げられていない感染フローを中心に、今回観測した攻撃キャンペーンについて紹介します。

1st Stage: LNKファイル

파일명: 실전 트레이딩 핵심 비법서.pdf.lnk

(訳: 実戦トレーディングの核心秘伝書.pdf.lnk)

ファイル名から、本LNKファイルは韓国の投資家を標的とした、北朝鮮による外貨獲得のための攻撃で使用された可能性があります²。ユーザによってLNKファイルが開かれると、ファイル内にXORエンコードされた状態で埋め込まれたPDFファイル(デコイ)が開かれます。また、難読化されたPowerShellスクリプトがウィンドウ非表示状態 (`-WindowStyle Hidden`) で実行されます。このPowerShellスクリプトの役割は以下の通りです。

1. プロセス名を使用して仮想環境・マルウェア解析環境を検知

図1のPowerShellスクリプトは [hxxp://mid\[.\]great-site\[.\]net/realzan/viewpoi.txt](https://mid[.]great-site[.]net/realzan/viewpoi.txt) からPowerShellスクリプトをダウンロードして実行する機能を有しています⁵。この際、ダウンロードされたPowerShellスクリプトは一時フォルダ内に保存されますが、実行後には削除されるように実装されています。

図2のVBScriptは図1のPowerShellスクリプトをウィンドウ非表示状態、かつ、実行ポリシーをバイパスした状態で実行する機能を有しています。

図1・図2のファイルを作成したら、[wscript.exe](#) を使用して図2のVBScriptを自動実行するタスク [Selling CoinBoruhde Whistling NOprobnl{BD234234324-1243324ADVE}](#) を作成します。

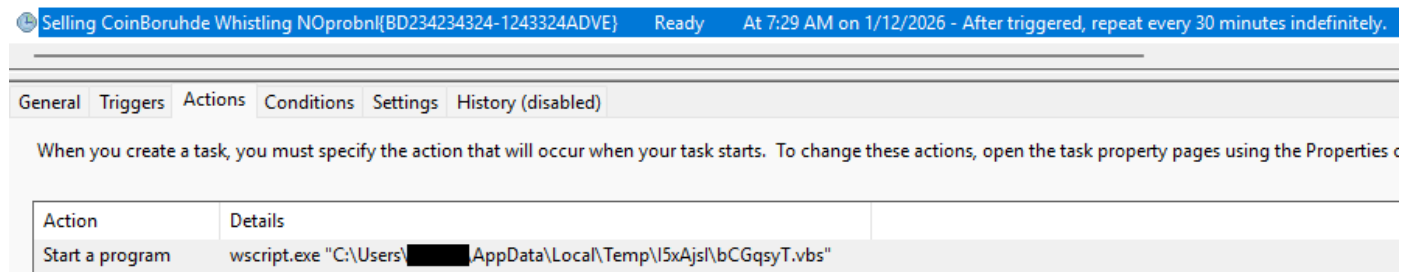


図3: 作成される自動実行用のタスク

その後、システム情報 (ホスト・ドメイン情報、OSバージョン情報、プロセス一覧など) を [hxxp://mid\[.\]great-site\[.\]net/maith.php](https://mid[.]great-site[.]net/maith.php) にPOSTリクエストで送信します。この際、PowerShellスクリプト実行時に生成されるランダムな4文字の文字列に加えて、**BEGIN** という文字列がサーバに送信されます。また、所定のデータをAES復号 ([hxxp://mid\[.\]great-site\[.\]net/aes.js](https://mid[.]great-site[.]net/aes.js) からダウンロードしたJavaScriptを使用) してパラメータに付加することも確認しています。正確な用途は不明ですが、脅威アクターに感染ホストの存在を通知するためのエンドポイントである可能性があります。

2nd Stage: PowerShellスクリプト (viewpoi.txt)

図1のPowerShellスクリプトによってダウンロード・実行される [viewpoi.txt](#) は [raw.githubusercontent.com](#) にアクセスして、GitHubリポジトリ [macsim-gun/FinalDocu](#) 内のファイル [octobor.docx](#) を取得します。当該GitHubリポジトリについては、弊社がGitHub社に通報を行い、2026年1月14日時点でテイクダウンされています。

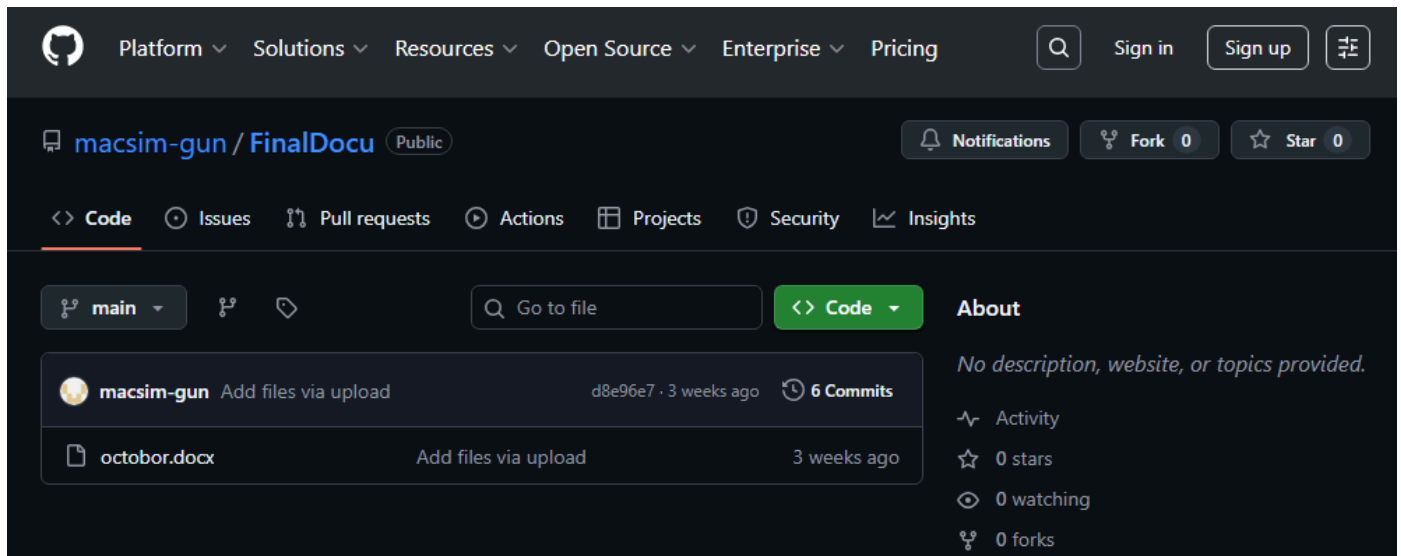


図4: 脅威アクターによって作成された悪意のあるGitHubリポジトリ

なお、コミットにはメールアドレス `sandamalmacsim@gmail[.]com` が使用されていました。GitHub上で認証済み (Verified) であったことから、当該メールアドレスも脅威アクターに関連している可能性が高いと考えられます。

```
commit d8e96e777de3234e0771e6c53b7c09a659542f12 (HEAD -> main, origin/main, origin/HEAD)
Author: macsim-gun <sandamalmacsim@gmail[.]com>
Date: Thu Dec 25 10:48:44 2025 +0900
```

```
Add files via uploadCode language: HTML, XML (xml)
```

ファイルを取得した後、`octobor.docx` の先頭7バイトを `1F 8B 08 00 00 00 00` (GZIPヘッダ) に置換して、そのままGZIP圧縮データとして解凍します。

```
$dgn43odsfgo435OSFDIg[0] = 0x1F;
$VFDsfewr32fd="FEDsrweh2345grggf
$dgn43odsfgo435OSFDIg[1] = 0x8B;
$ADSkuiygewiwuqv="dfgjkhionjdkkH
$dgn43odsfgo435OSFDIg[2] = 0x08;
$StCRdkj33ghei123="FEDsrweh2345g
$dgn43odsfgo435OSFDIg[3] = 0x00;
$SorikfCRdkjghei123="FEDsrweh234
$ASDSADSAD="FEDsrweh2345grggf(*&
$dgn43odsfgo435OSFDIg[4] = 0x00;
$ADSkuiygewiwuqv="dfgjkhionjdkkH
$dgn43odsfgo435OSFDIg[5] = 0x00;
$SCRdkljhlkhkjghei123="FEDsrweh2
$dgn43odsfgo435OSFDIg[6] = 0x00;
```

図5: ヘッダの置換

解凍後のデータは `Stella.exe` というオリジナルファイル名を持つ実行ファイルであり、PowerShellスクリプト内の `Assembly.Load` メソッドによってメモリ上で実行されます。

3rd Stage: MoonPeak (Stella.exe)

Stella.exe はConfuserExという著名な難読化ツールを使用して難読化されたマルウェア MoonPeakです。通常の.NETアセンブリは **dnSpy** や **dotPeek** といった解析ツールを使用することで、コンパイル前に近い高水準言語のソースコードを分析(デコンパイル)することができます。しかし、ConfuserExが使用されている場合、文字列やコードの暗号化によって、解析ツールが正常に動作しない場合や間違った出力が表示される場合があります。

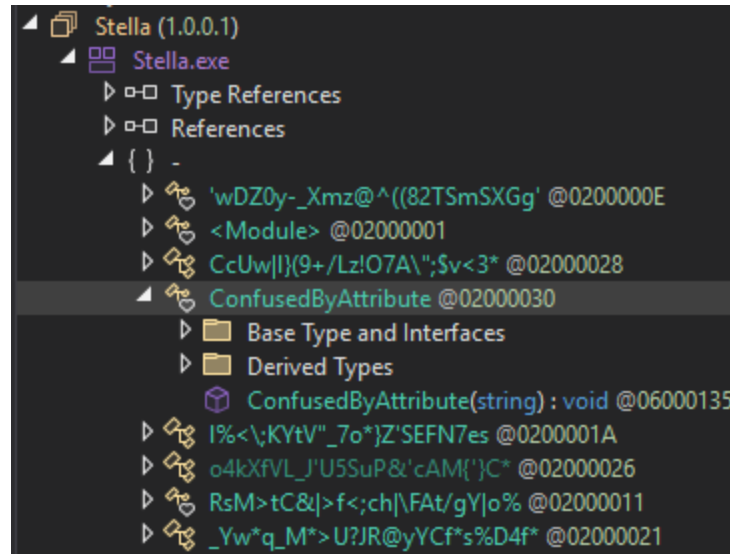


図6: ConfuserExによって難読化されている

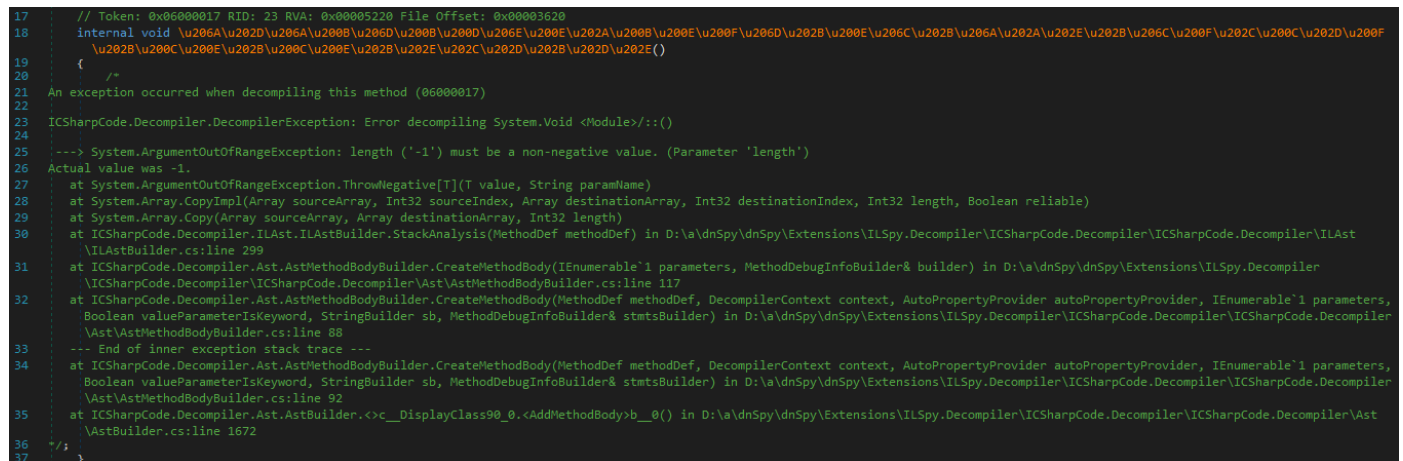


図7: デコンパイルに失敗している関数の例

これはConfuserExが有する耐タンパ機能による影響で、モジュールのコンストラクタ **<Module>.<Module>()** 内でコードを動的に復号してから実行している為です。動的解析によってコードを復号した後のモジュールをメモリ上から抽出して、更にde4dot⁷のような難読化解除ツールを適用することで、コードを静的解析することが可能です。

```
// Token: 0x0200000E RID: 14
internal class 'wDZ0y-_Xmz@^((82TSmSXGg'
{
    // Token: 0x06000047 RID: 71 RVA: 0x00007324 File Offset: 0x00005724
    [MethodImpl(MethodImplOptions.NoInlining)]
    public 'wDZ0y-_Xmz@^((82TSmSXGg'()
    {
    }
}
```

図8: DllHandlerクラスのコンストラクタ (難読化された状態)

```
// Token: 0x0200000E RID: 14
internal class Class6
{
    // Token: 0x06000046 RID: 70 RVA: 0x000095A8 File Offset: 0x000077A8
    public Class6()
    {
        for (;;)
        {
            IL_0063:
            uint num = 3901927269U;
            for (;;)
            {
                uint num2;
                switch ((num2 = num ^ 3708688073U) % 3U)
                {
                    case 0U:
                        goto IL_0063;
                    case 2U:
                        AppDomain.CurrentDomain.AssemblyResolve += Class6.smethod_0;
                        num = (num2 * 1238600071U) ^ 2698347653U;
                        continue;
                }
                return;
            }
        }
    }
}
```

図9: DllHandlerクラスのコンストラクタ (難読化を解除した状態)

解析の結果、今回観測したMoonPeakは以下のような設定情報を有していました。

- Mutex名: Dansweit_Hk65-PSAccerdle
- C2サーバ: 27.102.137[.]88:443

機能や仕様等は2025年8月に公開されたTrellixのレポート内で観測・報告されたMoonPeakから大きく変化しておらず、脅威アクターは同一手法およびマルウェアを使用し続けていると考えられます。

The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign
<https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign>

おわりに

過去に観測された攻撃キャンペーンと同様に、今回も脅威アクターはGitHubリポジトリをマルウェアのホスト元として活用していました。GitHubを含む正規サイトを攻撃で悪用する手法はLOTS (Living Off Trusted Sites) と呼ばれ、多くの脅威アクターによって使用されています。今後も悪用される可能性が高い手法であるため、警戒が必要だと言えるでしょう。



GitHub (GitHub Support)

Jan 14, 2026, 11:13AM UTC

Hello,

Our review of the account named in your report has concluded. We have determined that one or more violations of GitHub's Terms of Service have occurred and have taken appropriate action in response.

図10: 今回使用されたGitHubアカウントおよびリポジトリはテイクダウン済み

近年、北朝鮮に帰属する脅威アクターは日本を含む世界中の国々を標的とした攻撃活動を実施しており、政府機関や民間企業という主体だけでなく、インターネットユーザ(個人)にとっても重大な脅威であるといえます。我々は今後も北朝鮮に帰属する脅威アクター・攻撃活動・マルウェアの分析を続け、積極的に情報発信を行い、サイバー空間の安全に寄与していきたいと思えます。

Appendix: IoCs

ファイル

SHA256	ファイル名
1553bfac012b20a39822c5f2ef3a7bd97f52bb94ae631ac1178003b7d42e7b7f	실전 트레이딩 핵심 비법 서.pdf.lnk
aaac6eadac6c325bfc69b561d75f7cfd979ac289de1cc4430c5cc9a9a655b279	octobor.docx
8de36cb635eb87c1aa0e8219f1d8bf2bb44cad75b58ef421de77dd1aae669bf4	Stella.exe

メールアドレス

sandamalmacsim @ gmail[.]com

通信先

- ペイロード配信サーバ
mid.great-site[.]net

- `octobor.docx` 配信元

`hxxps://raw[.]githubusercontent[.]com/macsim-gun/FinalDocu/main/octobor.docx`

- MoonPeak C2サーバ
`27.102.137[.]88`

1. Cisco Talosは脅威アクターをUAT-5394としてトラッキングしています。
MoonPeak malware from North Korean actors unveils new details on attacker infrastructure
<https://blog.talosintelligence.com/moonpeak-malware-infrastructure-north-korea/> ↩
2. Trellixの研究者が2025年8月にMoonPeakを使用したサイバーエスピオナージを目的とした攻撃活動について報告しています。使用しているマルウェアや手法の類似性等から、同一の脅威アクターが関係している可能性が高いと考えられるため、今回の攻撃についてもサイバーエスピオナージが目的であった可能性は否定できません。
The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign
<https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/> ↩
3. ファイル名に近いタイトルを持つ韓国語の書籍のPDFがデコイとして使用されていました。
4. 文字列 `TARGET_PS1_PATH` は図1のPowerShellスクリプトのファイルパスに置換される。
5. 他にも `MID_LOGFOLDER_SUBPATH_PAYLOAD` を `"h6k"` で置換するコード等が含まれていましたが、我々が観測した `viewpoi.txt` 内には `MID_LOGFOLDER_SUBPATH_PAYLOAD` が存在しなかったため、未使用のコードであると考えられます。 ↩
6. 以下のレポート内で以前の攻撃キャンペーンで悪用されたメールアドレスが公開されています。
The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign
<https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/>
7. 今回の解析ではde4dotのフォーク版であるde4dot-cexを使用しました。
ViRb3/de4dot-cex – GitHub
<https://github.com/ViRb3/de4dot-cex> ↩
8. 以前の攻撃キャンペーンにおいても同じMutex名が使用されていました。
The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign
<https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/>

カテゴリー:[マルウェア解析](#)

タグ:[Targeted AttackMalware](#)