アンラボ・セキュリティレター

Press Ahn

2022.10　Vol.106

Lazarus グループのルートキット攻撃、企業のセキュリティシステムを無効化に

Lazarus グループ 「ルートキット」 攻撃に関する分析レポート

Lazarus グループのルートキット攻撃、企業のセキュリティシステムを無効化に

近年、北朝鮮のハッキンググループとして知られている Lazarus (ラザルス) グループの「ルートキット(Rootkit)」マルウェアが確認された。このマルウェアは、 脆弱なドライバカーネルモジュールを悪用し、企業のセキュリティシステム全体を無効化するものである。設計された攻撃の精度や、Lazarus グループによる攻撃頻度を考慮した際、各企業には格別な注意が求められている。

アンラボは、これまでの間 Lazarus グループの攻撃動向を徹底的に追跡し、今回の「ルートキット」マルウェアによる攻撃過程について、詳細な分析レポートを公開した。本記事では、レポートの主な内容を簡単に紹介していく。尚、レポート全文はアンラボのASECブログからダウンロードが可能である。

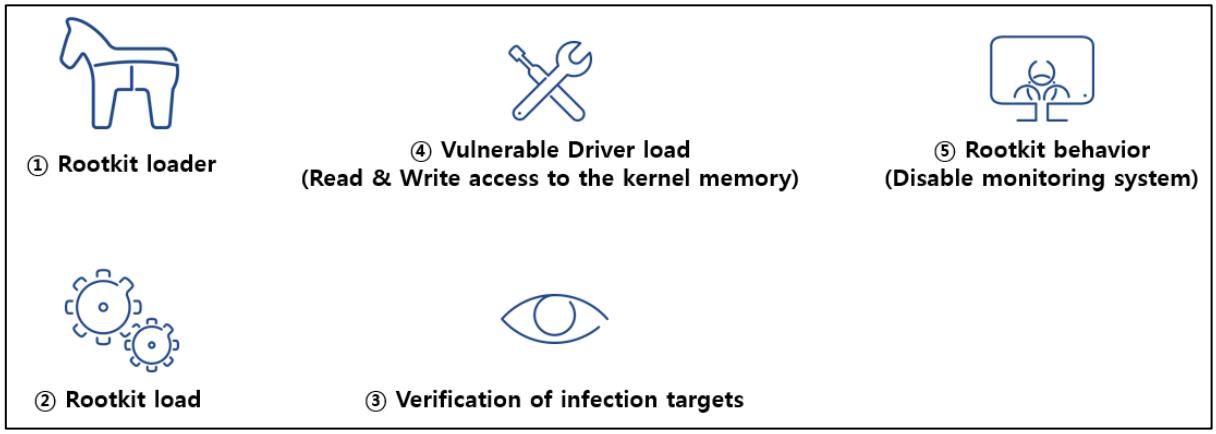
Lazarus は、韓国をはじめ、米国・アジア・ヨーロッパなどの様々な国家を対象に、2009年から攻撃を敢行しているグループである。アンラボのインフラ「ASD (AhnLab Smart Defense)」によると、Lazarus グループは 2022年上半期にも、韓国内の防衛産業・金融・メディア・製薬産業を対象に、APT (Advanced Persistent Threat) 攻撃を仕掛けている。

アンラボはこれまでの間、Lazarus グループの活動を徹底的に追跡してきた。その過程で、セキュリティ製品を無効化する攻撃展開が確認されている。アンラボの分析結果によると、Lazarus グループは INITECH 社の旧バージョンプロセスを悪用することで、企業に初期侵入を敢行後、攻撃者側のサーバーから「ルートキット (Rootkit)」マルウェアをダウンロードおよびインストールしていた。ちなみに「ルートキット」とは、攻撃者が敢行するハッキング行為を、システムユーザー側に気づかれないよう使用するツールを意味する。

製品の無効化攻撃により確認された「ルートキット」マルウェアは、 脆弱なドライバカーネルモジュールを悪用し、 カーネルメモリ領域に直接読み書きを行っていた。その結果、アンチウイルス（AV）を含むシステム内の全モニタリングシステムが無効化されるに至った。

ルートキットマルウェアの動作方式

Lazarus グループが使用するルートキットマルウェアの動作順序（①～⑤）は、[図1] の通りである。



[図1] ルートキットの動作過程（①～⑤）

ルートキットの動作過程を要約すると、まず、ローダープロセスのメモリ上に DLL 形式で作動した後、インストール時に “脆弱な” ドライバモジュール（ene.sys）をシステムドライブ経路に生成する。その後、該当ドライバをロードすることで、カーネルメモリ領域内にある特定のアドレス値を修正する仕組みだ。

脆弱なカーネルドライバによって変造されるアドレス領域は、DLL 形式で作動中のルートキット内にあるスレッドオブジェクトの PreviousMode アドレスであり、その値は 0 に変造される。ユーザー側のスレッドオブジェクトのPreviousMode 値が 0 に変更されると、ユーザー領域から “NtWriteVirtualMemory” API を介し、カーネル領域までアクセスできるようになる。

以降、攻撃者はユーザーの領域内でカーネルメモリを操作し、セキュリティシステムを無効化する。この攻撃は、AV を含め、▲ミニファイルフィルタ、▲プロセス/スレッド/モジュール検知、▲レジストリコールバック、▲オブジェクトコールバック、▲WFP ネットワークフィルタ、▲イベント追跡など、企業のセキュリティシステム全般を無効化させるほど、大きな影響力を持っていた。また、対象 OS も同様に、Windows7 から Windows Server 2022 までと広範囲に渡っていた。

ルートキット攻撃を可能にする理由

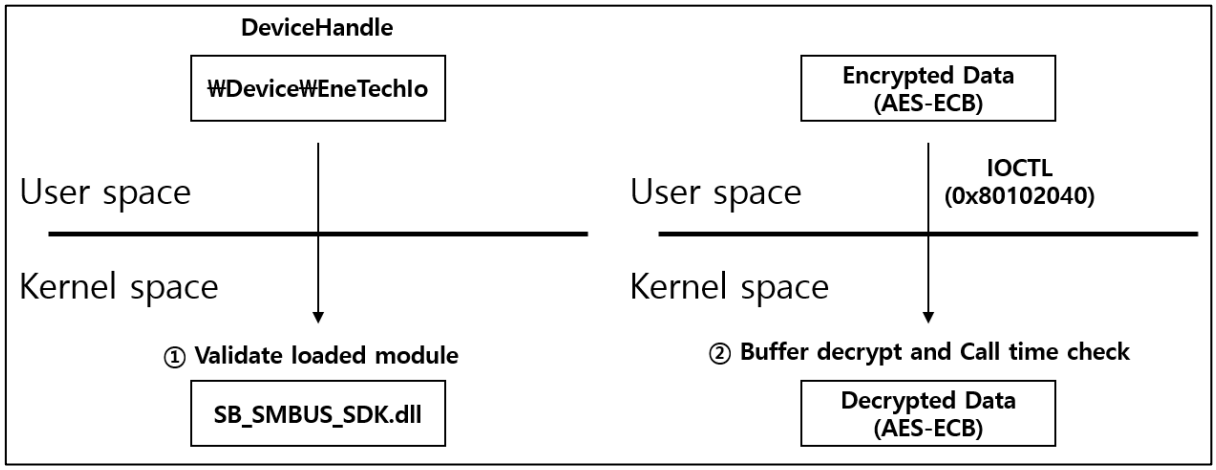
この攻撃の核心的ポイントは “脆弱な” ドライバモジュールにある。

「BYOVD (Bring Your Own Vulnerable Driver)」と呼ばれる攻撃手法は、主にハードウェアベンダーの脆弱なドライバモジュールを介して、攻撃を敢行することで知られている。最新 Windows の OS の場合、未署名のドライバをロードすることは不可能だが、攻撃者は合法的に署名された脆弱なドライバを利用することで、カーネル領域を容易に操作することができる。

今回の事例で、Lazarus グループが使用した脆弱なドライバモジュールは、前述にある「ene.sys」モジュールである。 ENE Technology 製の ene.sys モジュールは、1999年に Yariv Kaplan 氏が開発した「WinIO」オープンソースライブラリがそのまま使用されている。

ene.sys モジュールは、セキュリティ上に大きく 2つの問題点がある。1つ目は、ユーザー領域から物理メモリ領域のマッピングが可能であるという点だ。このモジュールは、カーネルの物理メモリおよび I/O (Input/Output) ポートに、ユーザー領域から直接アクセスできるようにし、ene.sys と通信するユーザープロセスは、IOCTL 通信を介してカーネル領域の物理メモリのマッピングを可能にする。これは、ユーザー領域から、任意の元カーネル内における物理メモリの操作が可能であるということを意味する。

もう 1つは、呼び出し元やデータに対する検証手順を、容易に迂回できるよう設計されているという点だ。[図2] を見ると、ene.sys は SB_SMBUS_SDK.dll モジュールのロードを検証する際、①のようにロードするモジュールが SB_SMBUS_SDK.dll であるかどうかを確認し、一致した場合、該当プロセスが信頼できるものだと判断する。この過程で、SB_SMBUS_SDK.dll をロードしたプロセスは、ene.sys ドライバや IOCTL (Input/Output Control) 通信が可能となる。



[図2] ene.sys の呼び出し元および有効データの検証手順

[図2] にある構造図 ②は、有効データの検証過程を表したものである。ene.sys は、ユーザー領域から要請された IOCTL に対する有効値を検証するため、IOCTL の呼び出し時間と、該当 IOCTL をドライバから受け取り処理した時間との差を計算する。この際、時差が 2ms 未満の場合は有効であると判断し、要請された IOCTL を処理する。

こうした検証プロセスは、簡単な迂回操作から、任意の元カーネルのメモリ領域に対する読み書きが可能となる。攻撃者も検証を迂回する手法で、ファイル・プロセス・スレッド・レジストリ・イベントフィルタなど、カーネルに関する全領域データの修正を行い、システム内の全てのモニタリングプログラムを無効化していた。

ASD インフラを介し、アンラボがドライバの流布経路を分析した結果、主にノートパソコン製造社「MSI」のRGB メモリモジュール内にある、制御モジュールに配布されていることが確認された。

攻撃の意味と予防策

ルートキット攻撃は、Windows Vista 以降適用された DSE (Driver Signature Enforcement) ポリシーによって減少したかのように見えた。しかし、本文で紹介した BYOVD (Bring Your Own Vulnerable Driver) 攻撃は、2014年からその事例が継続的に確認されている。これまでの BYOVD 攻撃は、主に権限昇格のためのものだと思われていた。だが、今回の攻撃のように、旧バージョンの Windows 7 から、最新 OS バージョンをもつ Windows Server 2022 まで、全てのシステムを無効化できる。こうした高精度なルートキット攻撃を設計したのは、Lazarus グループが初ではないかとされている。

また、マルウェアのうちの一部は、アンラボ製品によって診断されている。ASEC では同グループの活動を追跡し、マルウェアへの対応を

行った。しかし、まだ確認されていない未診断の変型が存在する可能性もある。

Microsoft では、BYOVD 攻撃への対策として、Windows 10 の HVCI モード (ハイパーバイザーで保護されたコード整合性)、および S モードの遮断ルールのもと、未許可のドライバはロードされないよう自律的に遮断している。このように、ドライバのロードを厳密に遮断することが、現時点ではルートキット攻撃を予防するための最善策とされている。

従って、企業のセキュリティ担当者は、一般ユーザーの環境下でドライバをロードすることができないよう、制御する必要がある。また、セキュリティソフトウェアのアップデートを最新状態に維持し、BYOVD を悪用した APT 攻撃を予防していかなければならない。

Lazarus グループの「ルートキット」マルウェアに関する詳細な分析内容は、下記のレポートから全文を確認することができる。

▶ 関連分析レポート

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)