Trend Research

TREND MICRO

攻撃者が悪用する Windows カーネルに対する脅威の分析

はじめに

現在の大半のセキュリティ製品は、ソフトウェアスタックの高いレベルで動作する脅威に焦点を置く傾向があります。これは特にユーザモードアプリケーションに当てはまり、その結果、セキュリティ業界全体で比較的良い成果が得られています。しかし残念ながら、そのようなセキュリティ製品では、カーネル空間、ブートプロセス環境、ファームウェアなどのシステムの低いレベルにある重要な部分に対する可視性は高くありません。攻撃者がシステムに対する特権アクセスを得て、悪意のあるコンポーネントをそのレベルでインストールすると、ユーザのセキュリティ製品は脅威を検知・ブロックすることができません。これは特にルートキットなど、カーネルの低いレベルを標的とする脅威に当てはまります。ルートキットとは、感染したシステム内で気づかれずにマルウェアを実行するための環境を提供するプログラム（またはプログラムの集合）です[1, 2]。

この調査報告書では、Windows プラットフォームに影響を及ぼす、低レベルなインタフェースを狙う脅威（低レベル脅威）の現状について解説します。また、このような脅威がこの 7 年間でどのように進化し、現在のマルウェアの状況においてどのような位置付けにあるのかも示します。さらに、この分野の業界から提供された分析済みの脅威データに基づいて分類した、主要なマルウェアクラスについても紹介します。

トレンドマイクロでは、現在の脅威状況で、直接的（カーネルドライバを読み込む）または間接的に（スタックの 1 つ下のレベルで動作することによりカーネルを侵害する）Windows カーネルに影響を及ぼす 3 つの種類の低レベル脅威を特定しました。

- Windows カーネルレベルのルートキット – オペレーティングシステムが完全に初期化されると起動する脅威
- ブートキット/ブートローダ – オペレーティングシステムのブートプロセス中に起動する脅威
- ファームウェア/BIOS（Basic Input/Output System）インプラント – ブート前の環境およびファームウェアの初期化プロセス中に起動する脅威

この報告書では、これらの脅威の現在の性質を示し、2015 年以降に悪用が確認されている、60 以上の最も注目すべき低レベル脅威から構成されるトレンドマイクロのデータセットの分析に基づく調査結果について説明します。また、高度な脅威アクタが最近のシステムに導入されている最新の防御メカニズムにどのように適応し、どのようにその手法を進化させているかについても解説します。

[1] https://www.trendmicro.com/vinfo/us/security/definition/rootkit

[2] https://www.techtarget.com/searchdatacenter/definition/kernel

Windows カーネルのアーキテクチャ

Windows システムでは、カーネル（「リング 0」とも呼ばれる）は、最も強力なアクセスおよび特権機能を持ちます[3]。カーネルは、さまざまな種類のハードウェアインタフェース、およびプロセス、スレッド、ハンドル、モジュール、レジストリ、およびその他のオブジェクトなどのオペレーティングシステムにより提供される基本的なシステムコンポーネントを扱う高特権レベルです。

Windows カーネルには高いアクセスレベルが付与されているため、カーネルレベルで実行されるコードは、多様な監視やフィルタリングメカニズムの実装が可能です。重要なシステムイベントやどのようなデータフローでも、適切なカーネルレベルのコードを使用すれば傍受できます。また、登録されたカーネルコードやコールバックでフィルタリングされれば、このレベルのコードの実行により特定のイベントの発生を阻止することもできます。

カーネル空間で実行するように設計されているコアサブシステムに加え、Windows カーネルはこの特権実行レベルへのアクセスを必要とするサードパーティコンポーネントにもアクセスを拡張できます。適切な手順を実行すれば、このようなサードパーティコンポーネントをソフトウェアプラグイン（カーネルドライバとも呼ばれる）として Windows カーネルにプラグイン可能です。これらの低レベルドライバは、リング 0 で実行され、特定のハードウェアに関連する機能およびハードウェアに関連しない機能の両方を提供するように設計されています。

Windows カーネルは、複数のレイヤから構成される複合システムとしてモデル化されています。各レイヤは、そのレイヤに依存する次のレイヤにサービスを提供し、また正しく機能するには、その下にあるレイヤが信頼できることを前提としています。1 つのレイヤが侵害されると、スタック内の後続のレイヤも侵害されます。これは、後続のレイヤの信頼は、他のレイヤに対して実行環境および必要なサービスを提供している、最初に侵害されたレイヤに基づいているためです。

[3] https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/windows-kernel-mode-kernel-library

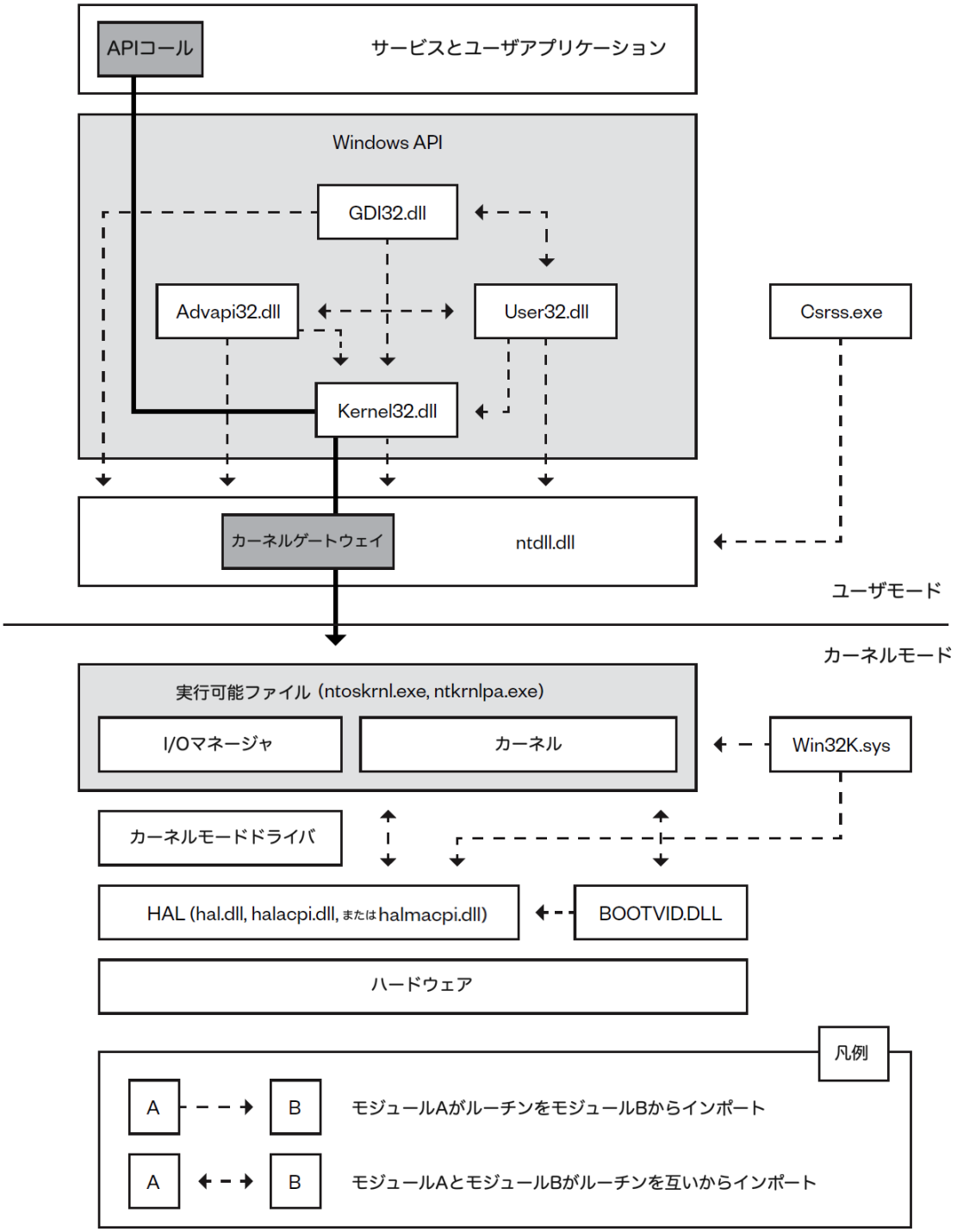


図 1：Windows カーネルサブシステムの複合モデル

出典：Windows Internals：System architecture, processes, threads, memory management, and more, Part 1（Developer Reference）7th Edition

Windows カーネルのアーキテクチャの問題

Windows カーネルには 1 つの論理アドレス空間（リング 0）しかないため、この空間内で実行されるコードは、カーネルの物理メモリ全体にアクセスできます。したがって、悪意のあるコードがカーネル内で実行され、カーネル空間が侵害されると、システム全体も侵害されることになります。従来は、カーネルコードは最高レベルの権限で実行され、通常のユーザアプリケーションのプロセスから分離されていました。カーネル空間は信頼できる領域であると見なすことが一般的でした。以前のアーキテクチャ設計では、カーネル内のさまざまなシステム操作に対するサードパーティコードを提供すれば、最高レベルの権限が与えられました。ただし、これによりカーネルの信頼モデルに大きなアタックサーフェス（攻撃対象領域）が生まれました。この信頼モデルを強化するために、Windows カーネルアーキテクチャ全体でカーネルコンポーネント自体に新たな境界を追加することが必要になりました。これについては、仮想化ベースのセキュリティメカニズムのセクションで詳しく解説します。

この後のセクションで紹介する、トレンドマイクロのテレメトリデータおよびその他のサードパーティのリポジトリデータによると、毎日何万個もの固有のカーネルドライバモジュールが確認されています。図 2 は、サードパーティのマルウェアリポジトリに提出された、署名が失効した固有のカーネルドライバモジュールの数が、2015 年から 2021 年までの間に急激に増加したことを示しています。攻撃者がカーネル内に侵入するために使用するその他の方法に加えて、これらの各カーネルドライバモジュールは、前提となる、信頼および保護されているカーネル空間で多様な脆弱性を引き起こす可能性があります。これらの脆弱性についても、以降のセクションで紹介します。

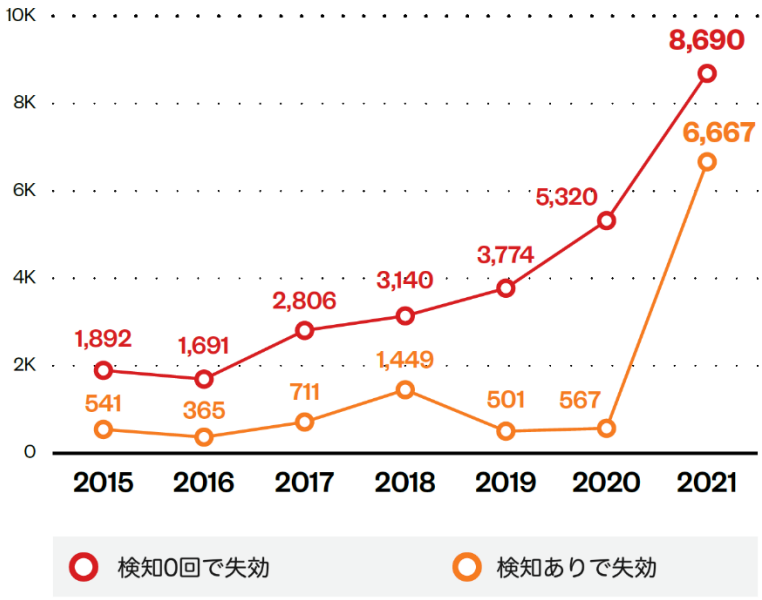


図 2：2015 年から 2021 年までの間にサードパーティのマルウェアリポジトリに提出された、署名が失効したカーネルドライバモジュールの数

このデータに基づくと、あらゆるユーザモードアプリケーションの改ざんの試みから完全に隔離された、十分に保護された小さなカーネル空間領域という概念を使用する信頼モデルはまったく現実的とは言えません。カーネル境界を追加したとしても、カーネル内に読み込まれている悪意のあるコード、またはユーザモードアプリケーションの完全な初期化が実行される前に実行環境の 1 つ下のレイヤで実行するように設定されている悪意のあるコードにより無効化される可能性があります。これ以降のセクションでは、この従来の信頼モデルを悪用した、最近確認されたカーネルに対する脅威をまとめています。

もう一つの Windows カーネルの問題が、オペレーティングシステムのすべてのコンポーネントに対して最小限の可視性しかないこと、またシステム全体がどのように構築されているかに関する機密性です。長い間、Windows カーネルでは、セキュリティ維持のために不明瞭さによるセキュリティ（STO）[4]の設計パターンを採用してきました。しかし、攻撃者の方が公開されていないインタフェースやコマンドを悪用して自身の悪意のあるコードを起動するために費やせる時間やリソースが多い傾向にあることから、このプロセスは防御する側よりも攻撃者にとってより利益があることが実証されています。

また攻撃者は、Windows カーネルにおけるセキュリティ上の欠陥を見つけるため、システムコンポーネントのリバースエンジニアリングを行う手段も持っています。一方、防御側は通常、正式な公開されているインタフェースに従って防御メカニズムを配置します。

このパターンの最近の例が、Conti ランサムウェアファミリのオペレータから流出した会話によって明らかになっています[5]。これらの会話は、Conti グループが精力的にリバースエンジニアリングやファジング手法を使用して、Intel マネジメントエンジンのファームウェアに侵入し、システムのソフトウェアスタックに深い足掛かりを得ていたことを示しています。このインシデントは、今でもサイバー犯罪者が STO 設計パターンを自分たちのアドバンテージとして悪用していることを示しています。

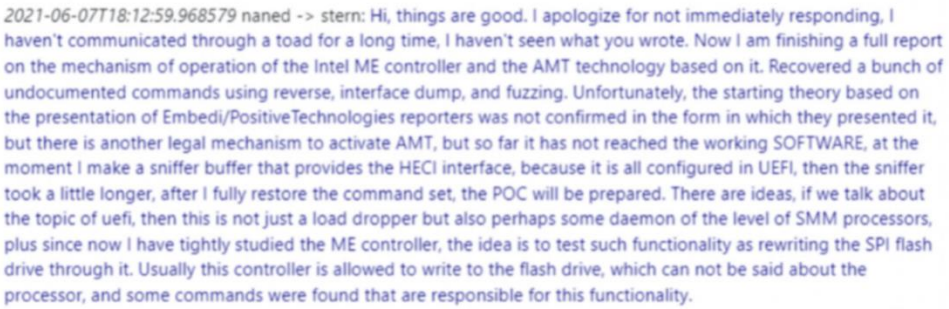

2021-06-07T18:12:59.968579 naned -> stern: Hi, things are good. I apologize for not immediately responding, I haven't communicated through a toad for a long time, I haven't seen what you wrote. Now I am finishing a full report on the mechanism of operation of the Intel ME controller and the AMT technology based on it. Recovered a bunch of undocumented commands using reverse, interface dump, and fuzzing. Unfortunately, the starting theory based on the presentation of Embedi/PositiveTechnologies reporters was not confirmed in the form in which they presented it, but there is another legal mechanism to activate AMT, but so far it has not reached the working SOFTWARE, at the moment I make a sniffer buffer that provides the HECI interface, because it is all configured in UEFI, then the sniffer took a little longer, after I fully restore the command set, the POC will be prepared. There are ideas, if we talk about the topic of uefi, then this is not just a load dropper but also perhaps some daemon of the level of SMM processors, plus since now I have tightly studied the ME controller, the idea is to test such functionality as rewriting the SPI flash drive through it. Usually this controller is allowed to write to the flash drive, which can not be said about the processor, and some commands were found that are responsible for this functionality.

図 3：概念実証（PoC）の開発に関するチャットの翻訳
出典：Eclypsium.com

[4] https://www.techopedia.com/definition/21985/security-through-obscurity-sto
[5] https://eclypsium.com/research/conti-targets-critical-firmware/

調査の範囲

本調査では、Windows カーネルの信頼モデルに影響を及ぼしている低レベル脅威の現状と、これらの脅威がこの 7 年間でどのように進化してきたかに焦点を置いています。本報告書では、ライフサイクル（PoC からその後の実際の脅威アクタ間での拡散まで）や、高度な標的型攻撃（APT）グループの感染チェーンの一部としての使用など、低レベル脅威の特性についても解説します。

低レベル脅威に関しては、オペレーティングシステムにより提供される現在の防御メカニズムが脅威動向に影響を与えます。新しい CPU の仮想化拡張機能を利用する最新の革新的な防御は、これらの脅威の作成と実行方法を大きく変えています。新たな防御メカニズムが導入されるたびに、マルウェアアクタは別の抽象化レイヤに適応し、ファームウェアおよびハードウェアレイヤにより近づくために、カーネルとブートプロセス間に焦点を移すことを余儀なくされています。したがって、これらの脅威の歴史、セキュリティに関してセキュリティコミュニティでは現在何が起きているのか、また Windows システムの最新のバージョンに搭載される防御システムが絶えず進化していくにつれ、この種の脅威が今後どのような方向に進んでいくのかについて論じることが重要です。

本調査では、Windows カーネルに関連する 60 以上の低レベル脅威について解説しています。トレンドマイクロは分析したサンプルを、さまざまな脅威の種類での主なパターンを特定し、このカーネルレベルの機能を追求している攻撃者の傾向を見つけ、このような特権アクセスレベルを求める理由を判断し、推定される開発コストに関する洞察を獲得し、カーネルレベルの機能をサイバー犯罪者のマルウェア武器庫に追加することのトレードオフの可能性を明らかにするために、いくつかのクラスタに分類しました。

また、最近見つかったルートキットのサンプルで現在確認されている機能を紹介し、トレンドマイクロのテレメトリに基づき、これらのモジュールの現在の検知率の統計分析も提供します。最後に、攻撃者が Windows カーネルを悪用するために利用する可能性のあるアンダーグラウンド市場のサービスなどについても詳しく説明します。この調査では、カーネル空間またはその下で主に実行される脅威、または Windows カーネルで実行されるコンポーネントを 1 つ以上持つ脅威に焦点を置いています。

攻撃者がカーネルレベルのアクセスを追求する理由

標的とするシステムのカーネルレベルでコードを実行できるようになると、被害システムのセキュリティ防御を無効化して検知されないようにするなど、攻撃者は多くの利点を得ることができます。特にルートキットは、攻撃者のツールが長期間潜伏することを可能にします。

本セクションでは、低レベルの実行環境を保護するとされる新たな防御メカニズムが登場しているにもかかわらず、攻撃者がなぜこのような低レベルの機能を未だに追求しているのかについて解説します。この機能を持つことが攻撃者の攻撃シナリオや目的にとって最適であるとしても、それは簡単な手段ではないはずです。最後に、カーネルレベルのマルウェアファミリを開発する際にかかるコストについても検討します。

メリット

カーネルレベルのルートキットおよびその他の低レベル攻撃の高い開発コストを正当化する最も明白なユースケースは以下のとおりです。

- システムリソースへの高特権アクセスを得ることができる
- デバイス上の不正な活動を隠ぺいすることにより検知や対処を困難にする
- システム上のフィルタリングプロセスにより、攻撃者の生成ファイルやツールなどが排除されることを回避できる
- 検知を長期間回避することが可能なステルス攻撃を実行できる
- ウイルス対策製品からの信頼を得ることができる
- 複数のアプリケーション（ユーザモード）に影響を及ぼすコアサービスのデータフローを改ざんすることができる
- 攻撃を妨げるセキュリティ製品を改ざんすることができる
- 検知率が非常に低くなる（最新のルートキットの多くは長期間にわたって検知されないままの状態）

このような脅威の検知が困難であるのは、カーネル境界内で動作するほとんどのカーネルモジュールにより実行される操作に対して、セキュリティ製品ではその可視性が制限されているためです。

これらの不正なカーネルドライバはセキュリティ製品のドライバと同じ権限レベルを持つため、多くの場合見逃されます。不正なカーネルドライバはユーザモードアプリケーションよりも多くの信頼を継承しているため、カーネルルートキットはセキュリティコントロールやツールを回避できます。さらに、独立したカーネルコンポーネントとして導入されているマルウェアの種類を対象とする軽減手法の数は多くありません。図 4 は、登録された

PreProcessThread コールバック内のカーネルドライバに対し、エンドポイントセキュリティソリューションが暗黙的な信頼を付与する例を示しています。

- Exclude (PID < 8 and OperationInformation.KernelHandle == 1).
- Include (! OperationInformation.KernelHandle == 1 and ExGetPreviousMode()).

```
int __stdcall OnPreOpenProcess(int a1, _OB_PRE_OPERATION_INFORMATION *a2)
{
  char v3[4]; // [esp+4h] [ebp-10h]
  HANDLE v4; // [esp+8h] [ebp-Ch]
  PEPROCESS Process; // [esp+Ch] [ebp-8h]
  BOOL Is_System_Process; // [esp+10h] [ebp-4h]

  Is_System_Process = (unsigned int)PsGetCurrentProcessId() < 8;
  if ( Is_System_Process & a2->KernelHandle & 1 )
    return 0;                           // Return OB_PREOP_SUCCESS if operation is coming from the Kernel
  Process = (PEPROCESS)a2->Object;
```

図 4：ウイルス対策ソリューションはユーザモードアプリケーションと比べてカーネルドライバをより信頼する傾向がある

デメリット

カーネルルートキットの使用には、以下のようなデメリットもあります。

- カーネルルートキットの開発および実装は、他のアプリケーション（ユーザモード）のマルウェアと比較して困難であり、必ずしも理想的な脅威とはならない。
    - カーネルルートキットの開発には、対象となるオペレーティングシステムの内部コンポーネントを理解し、システムコンポーネントのリバースエンジニアリングに関して十分な知識や能力を持つ技術者が必要となる。
    - カーネルルートキットはエラーに敏感なため、カーネルモジュールのコードバグによりシステムがクラッシュし、BSOD が発生した場合、不正操作の全体像が判明してしまう可能性がある。カーネルモードルートキットのソースコードのエラーは、修復不能な変更を引き起こし、必然的にシステムの安定性に影響を及ぼす。
- 被害システムのセキュリティメカニズムが有効でない場合や、より容易な手法でダウンさせることができる場合、カーネルモードコンポーネントの導入は、かえって攻撃を複雑化させてしまう恐れがある。標的とするシステムの侵入ポイントや脆弱な境界防御、重要なセキュリティシステムの欠陥を発見した場合、カーネルレベルのルートキットを使用することは非合理的である。
    - カーネルレベルのルートキットの開発とテストには多くの時間がかかる。カーネルレベルのルートキットは、新たに発見されたエクスプロイトを悪用し、すぐに使えるツールで被害者のネットワークに侵入する傾向のあるサイバー犯罪者ではなく、標的型攻撃（APT）の実行者により適したマルウェアである。

トレードオフ

攻撃者はカーネルルートキットの構築やカーネルの初期化前の低レベルレイヤでの不正ツールの導入などの高度な手法を選択する前に、まず要件を評価します。どの設計を選択するかは、特定の手法を検知する手段が公開されている数、その手法がどれだけ有用であるかの理解、その手法に対する検知の導入コストなどのいくつかのパラメータによって左右されます。攻撃者は常に、公開されていない、低コストで検知が難しく、安定した攻撃手法を探しています。

攻撃者は、仮想化ベースのセキュリティ（VBS）やハイパーバイザーで保護されたコード整合性（HVCI）[6]などの新たな防御メカニズムの現在の導入率に応じて、さまざまな抽象化レイヤやシステム境界間で攻撃手段を切り替えています。現在のプラットフォームのセキュリティメカニズムにより、攻撃機能の安定性と有用性に影響を及ぼすことなく攻撃者が活動できる最も適切な実行レベルが決まります。トレードオフの例として、システムの安定性を損ねるカーネルモードコード署名（KMCS）の回避か、Windows システムの全バージョンでは有用ではない手段の利用などが挙げられます。

図 5 は、最新の脅威で初期の感染ポイントがどのように変化しているかを示しています。また、一部の脅威が、各レイヤのメリットとデメリットおよび各レイヤで導入されている防御に基づき、1 つのレイヤでの活動から別のレイヤへと移っていることも示しています。新たな保護が導入されると、攻撃者は最も抵抗の少ない経路を選択し、ソフトウェアスタックの次のレイヤを選びます。たとえばトレンドマイクロで分析した過去のデータでは、Moriya ルートキット[7]の背後にいる攻撃者が、ユーザモード実行レベル（IISpy）での活動からカーネルモードコンポーネントへと移行していることが確認されています。同じ攻撃者が、ステルス性と KMCS を回避するリソースが必要なことから、より強力な機能を求めてカーネルモードコンポーネントを使用しています。また、TDL3 ルートキットもカーネルレベルから進化し、次のレイヤで活動するブートキット（TDL4）として登場しています。最後に、ZeroAccess ルートキット[8]はコモディティマルウェアとして普及し、KMCS の導入時にカーネルモードからユーザモードへと移行しています。

[6] https://learn.microsoft.com/en-us/windows-hardware/drivers/bringup/device-guard-and-credential-guard

[7] https://www.zdnet.com/article/new-moriya-rootkit-stealthily-backdoors-windows-systems/

[8] https://nakedsecurity.sophos.com/2012/06/06/zeroaccess-rootkit-usermode/

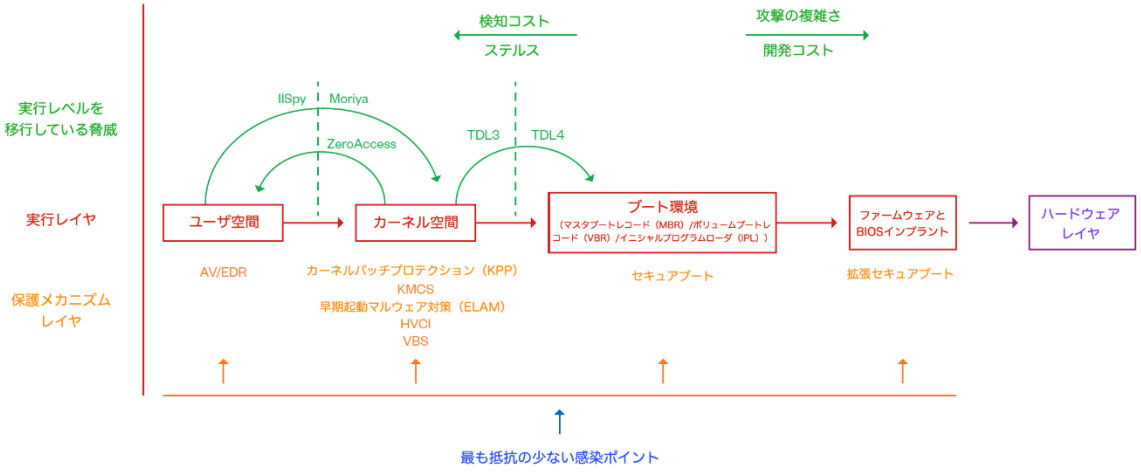


図 5：現在のプラットフォームセキュリティメカニズムの影響を受けた初期の感染ポイントの動向

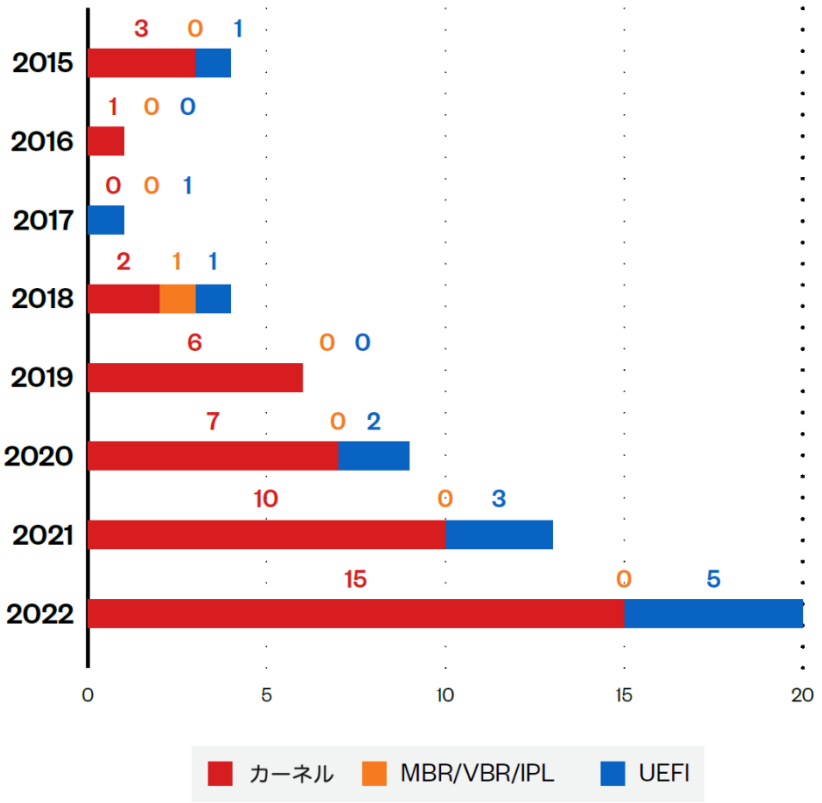


図 6：UEFI（Unified Extensible Firmware Interface）を初期感染ポイントとして使用したカーネルレベルの攻撃数

Windows カーネルに対する脅威の変遷

ここ数年、Microsoft はカーネルの根幹信頼性を含む全般的なセキュリティ体制を強化するために複数のセキュリティメカニズムを追加することに重点を置いてきました。これは、カーネルの信頼が侵害されると、システム全体の安定性と機密性に大きな影響を及ぼすことを認識していたためです。このセクションでは、Windows カーネルの信頼モデルに影響したイベントやそのイベントを実行した脅威、各セキュリティメカニズムの背景、および攻撃者がどのようにカーネルレベルのマルウェアを作り出し、新しい Windows バージョンで導入されたセキュリティ防御に適応したかについて振り返ります。

KMCS 以前の時代（Windows Vista 64 ビットより前）

この時代は、大半の攻撃者は、その動機や技術的能力にかかわらず、攻撃チェーンの一部として簡単にカーネルモードモジュールをコンパイルしてロードすることができました。これは、カーネルレベルの実行能力を得るために必要なコストがかなり低かったためです。カーネル空間の境界は、Windows カーネルドライバを作成できれば誰でも越えられました。これにより、攻撃者はカーネル内で深い足掛かりを維持し、システムサービスの破壊と操作、あらゆる種類の重要なカーネルオブジェクトのフック、サードパーティのウイルス対策エンジンの妨害、システムディスパッチテーブルの破壊など、あらゆる不正行為を実行することができました。保護エンジンと同じレベルで実行されるコードを保護することは困難または不可能でさえあったため、サードパーティソリューションがこの競争で負けていることは明白でした。

一部の Windows カーネル開発者により作成された未テストで質の低いカーネルコードが原因で、この時代のカーネルセキュリティ体制は無秩序な状態でした。コードから、クラッシュダンプを引き起こした問題のあるコードを作成した元のエンティティをたどる方法はありませんでした。また、あらゆる侵入時にカーネルルートキットが埋め込まれていました。セキュリティ業界は、複雑なヒューリスティックスキャン機能、あいまいなカーネルデータ構造の分析機能、および損傷の検知時に復元を試みる機能を備えたいくつかのルートキット対策ソフトウェアの作成で対抗しました。その結果、システム全体が非常に不安定になり、BSOD（Blue Screen of Death）が頻繁に発生していました。この時点では、カーネルの不安定性の根本原因は、カーネルドライバの構成における未検証のカーネルレベルのコードでした。

KMCS の時代およびそれ以降（Windows Vista 64 ビット以降）

Microsoft はカーネルコードモジュールの品質の管理、各コードの作成者の確認、および昇格されたアクセス権で実行されるコードに対する制限の追加の必要性を 2006 年に認識しました。Windows の開発者がルートキットおよびその他の低レベルのマルウェアの種類によ

る被害およびその普及の範囲を評価した後、Microsoft は Windows Vista 64 ビットバージョンシステムに KMCS を搭載することを発表しました。この期間にリリースされた Windows Vista システムには、KMCS とともに、いくつかのコアカーネルオブジェクトやディスパッチテーブルの整合性を維持し、悪意のあるコードによる改ざんを阻止する、Microsoft KPP や PatchGuard などの強化されたカーネルパッチ保護メカニズムも含まれました。

Microsoft によるこの動きは、中級レベルの攻撃者に対し、カーネルモジュール、特にコモディティマルウェアに主に依存するカーネルドライバを含む攻撃の設計コストを引き上げました。また、Microsoft PatchGuard のセキュリティ機能は、DKOM（Direct Kernel Object Manipulation）やコアシステムサービステーブルに対するインラインフックなど、ルートキットの作成者により使用されていた多くの手法にも影響しました。これにより、一連の攻撃が使用不能になり、Windows カーネルへのコードの導入がすでに成功していたとしても、ルートキットの作成者の活動を効果的に制限することができました。

これらの機能強化は、カーネル空間のアドレス空間内で実行されるコードの品質を管理するために、カーネルドライバにデジタル署名を付加することをハードウェアおよびソフトウェアのベンダに義務付けました。つまり、ドライバを読み込むには、マルウェアの作成者にも有効な署名が必要になりました。

以下の理由から、ルートキット脅威の状況は、この時代に劇的に変化しました。

- カーネルルートキットを読み込めるようにするには、より高い開発コストがかかるようになった
- マルウェアにカーネルルートキットを含めるための技術力を持つ攻撃者はさほど多くなかった
- Microsoft が新しい Windows バージョンに追加したセキュリティ防御を回避するためには、攻撃者には新たな手法が必要であった

図 7 に、KMCS の導入以前と、カーネル信頼モデルを改善するためのセキュリティ強化機能の初期バージョンの導入以降のカーネル脅威の状況を示します。

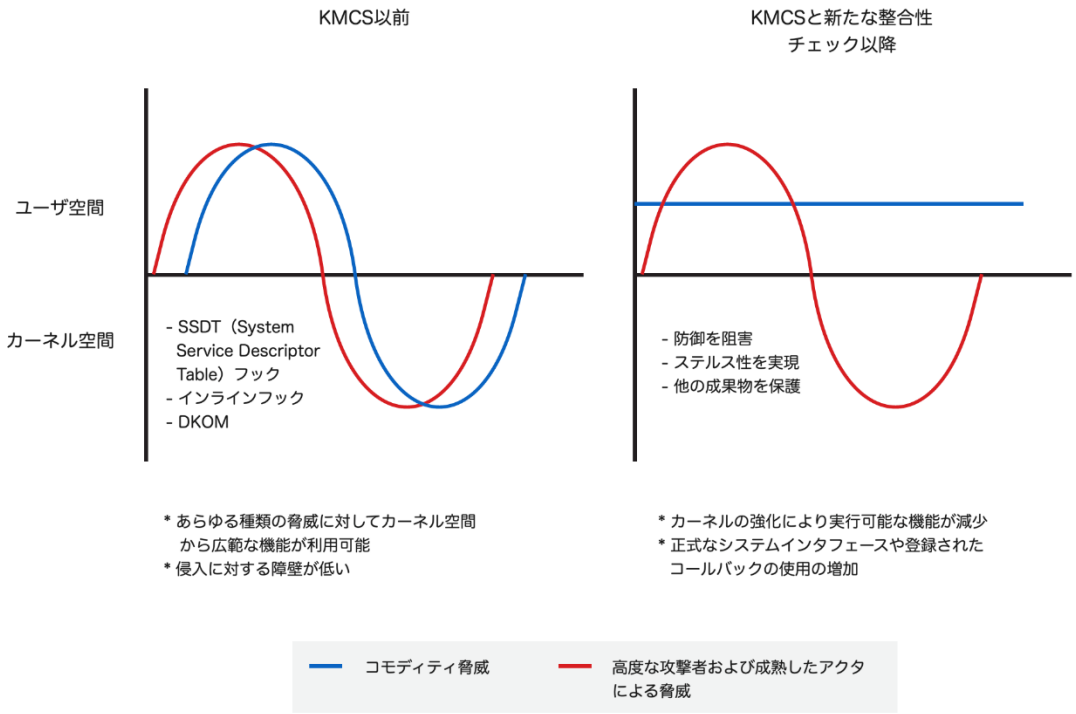


図 7：KMCS の導入以降の Windows カーネルセキュリティの強化

成熟した攻撃者が KMCS に適応した方法

Microsoft が新しいバージョンにいくつかのセキュリティメカニズムを導入した後、カーネルルートキットはマルウェアの世界からは一掃され、この種類の脅威はユーザ空間に完全に移行し、この攻撃ベクタ全体が最終的には消えるものと考えられていました。調査コミュニティも、導入されたセキュリティメカニズムに対して考えられる回避手法の理解へと焦点を移していました。しかし、KMCS はカーネルルートキットの量を減らし、悪意のあるコードから作成者をたどることには役立ちましたが、攻撃者がカーネルレベルのアクセスを攻撃に積極的に追加することを阻止する決め手とはなりませんでした。

KMCS 適用モジュールが Windows システムに完全に読み込まれると、攻撃者は署名されていないコードをカーネルに読み込むことはできなくなりました。これにより、KMCS の整合性チェックを回避するその他の方法を探さざるを得なくなりました。以下のリストでは、2015 年 4 月から 2022 年 10 月の間に発見された低レベル脅威で確認可能な手法を、3 つの主なクラスタに分類しています。分析された各脅威には、キルチェーン内でカーネル空間のアクセス制限を回避するカーネルレベルのモジュールが 1 つ以上含まれます。

1. KMCS を回避する脅威
    - 正規のビルトインツールを使用して KMCS を無効にする脅威
    - 脆弱なドライバを悪用する脅威（BYOVD: Bring Your Own Vulnerable Driver）攻撃）

- デュアルユースドライバを悪用する脅威
- レガシーシステムを標的とする脅威

2. 正規のドライバ自己作成技術を使用する、KMCS に準拠する脅威
   - 盗んだ有効なコード署名証明書を使用する脅威
   - 取得または購入したコード署名証明書を使用する脅威
3. より低い抽象化レイヤに移行した脅威
   - ブートキット
   - ファームウェアレベルの攻撃
   - BIOS インプラント

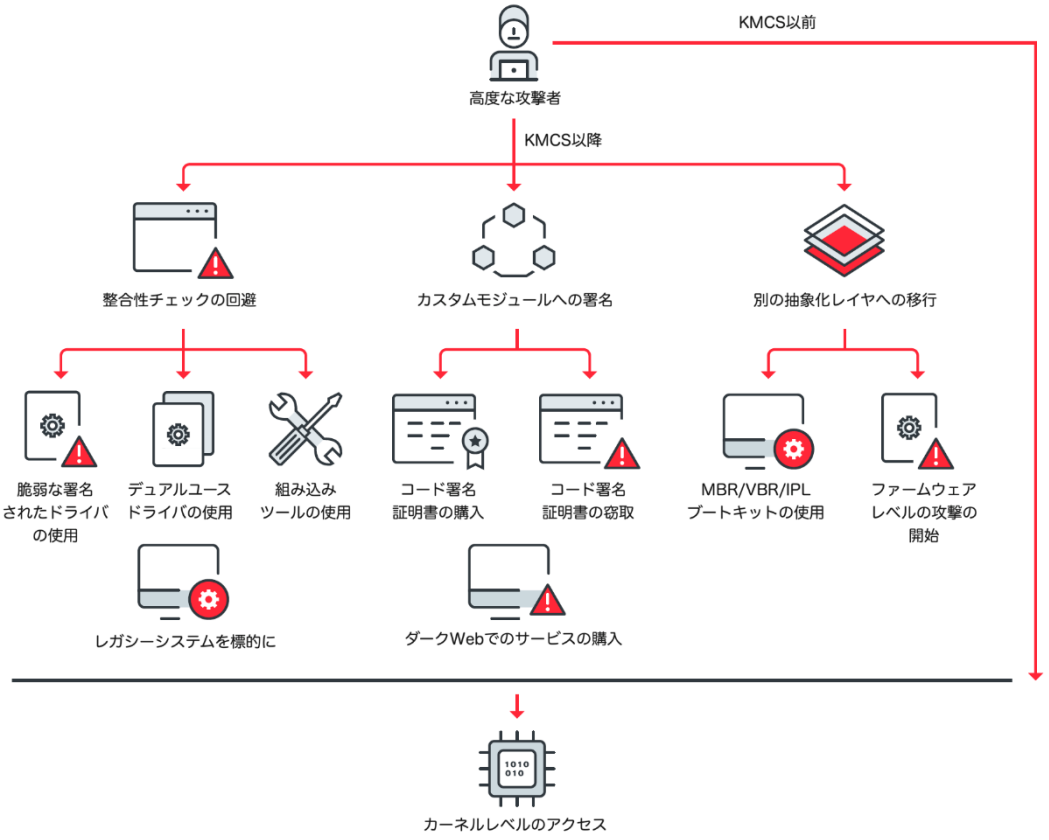


図 8：KMCS の導入以降の各クラスタのカーネルレベルの脅威の増加を示す図

分析したカーネルレベルの各脅威は、この 3 つの主なクラスタのいずれかに属していました。第 1 クラスタは、次のようなさまざまな手段で署名の制限を回避することに直接依存しています。正規の管理ツールを使用して KMCS を無効にする、正規のベンダにより署名された脆弱なコードを侵害する、基本的なカーネルレベルの操作を実行するために適切な認証を必要としないユーザ空間アプリケーションの露呈された汎用インタフェースを持つデュアルユースカーネルドライバを使用する。

第 1 クラスタの 1 つ目の手法では、主にデバッグとテストのために KMCS を明示的に無効にする正規の組み込みツールを利用します。このようなツールは、ドライバの検証を一時的に無効にし、ドライバのデジタル署名の検証のためにテスト署名を有効にするインタフェースを提供します。これらのツールは意図せずに、監視システムによる検知を回避していました。

BYOVD として広く知られている、第 1 クラスタの 2 つ目の手法では、Windows システムのカーネルドライバまたはサードパーティのカーネルドライバのいずれでも、カーネルに正当に読み込み可能な脆弱なドライバを利用して、意図したカーネルコードに組み込みます。この手法の最近の例は、ランサムウェアアクタがウイルス対策プロセスおよびサービスを無効にするために、ロールプレイングゲームの「原神」に対する脆弱なチート対策ドライバを悪用したケースです[9]。

脆弱なドライバの定義には、ユーザ空間のコンポーネントに対する広範なカーネル機能をサポートする、汎用入出力制御（IOCTL）インタフェースを持つ、デュアルユースカーネルドライバも含まれます。このようなドライバには正当な用途がありますが、攻撃者により KMCS を回避するために使用されることもあります。また、コードの整合性モジュール（CI.dll）を使用して KMCS を完全に無効にするために使用できるため、攻撃者にとって有用です。このようなモジュールは、KMCS の状態を制御する、カーネル空間の 1 つの特定の変数を使用してオンとオフを切り替えることができます。メモリの読み取り/書き込みプリミティブを含む脆弱なドライバを使用してこの変数を操作することにより、整合性チェックロジック全体を停止できます。その後、Microsoft は、どの単一の変数もコードの整合性ステータスを制御できないように、セキュリティをさらに強化しました。

第 2 クラスタの脅威は異なるアプローチを使用します。このクラスタの脅威は Microsoft の署名要件に準拠しているため、非常に限定的なタスク用に構築された、カスタマイズされたカーネルドライバを柔軟に作成して署名することができます。このために、攻撃者は正規の組織を偽装して有効なコード署名証明書を取得し、Microsoft の証明書のクロス署名プロセスに従うか（Microsoft でカーネルモードコードのクロス署名がまだ許可されていたため）、他人の証明書を盗む必要がありました。この第 2 クラスタの手法を使用する攻撃の例としては、攻撃者が Windows ハードウェア互換性プログラム（WHCP）ポータルを悪用し、Microsoft により署名されるように悪意のあるドライバを提出したケース[10]が挙げられます。2021 年 6 月に発生したこの攻撃は、ゲーミング環境を標的としていました。その他の手法と比べ、この攻撃で使用されていた手法には比較的コストがかかっており、主に国家支援の APT アクタによって使用されていると考えられます。2022 年 12 月、Microsoft Windows ハードウェア開発者プログラムを通して認定されたカーネルドライバが、ランサムウェア攻撃

[9] https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html

[10] https://msrc.microsoft.com/blog/2021/06/investigating-and-mitigating-malicious-drivers/

などの悪意のあるキャンペーンで使用された後、Microsoft はこのプログラムのいくつかのアカウントを停止しました[11]。

第 3 クラスタでは、より複雑な一方で効果的な戦略を使用します。この戦略では、図 8 に示すように、ソフトウェアスタックの下位レベルのレイヤに完全に移行し、新たな抽象化レイヤで動作します。これにより、コード署名ポリシーを適用する完全なカーネルとコアコンポーネントが初期化される前に、悪意のあるカーネルコードを読み込めるようになります。ブートキット感染手法の人気が再燃し、さまざまな攻撃者が実際の攻撃で使用したマルウェアファミリでのこの手法の利用が確認されています。このクラスタの手法はこの後、従来の BIOS ベースのブートプロセス内の MBR/VBR/IPL エントリの感染から、ハードウェアにさらに 1 つ近いレイヤに存在するファームウェアの脆弱性の悪用へと進化しています。このクラスタの進化は主に、次のセクションで解説する、より多くのブートプロセスのセキュリティ機能が導入されたことによるものです。

カーネル防御メカニズムの新たなバージョン

攻撃者が戦術を進化させ、KMCS の制限に適応したため、Microsoft の開発者は戦略を再度見直し、攻撃者がカーネルに戻る既存の回避策を使用するすべての脅威に対するハードルを上げることが必要になりました。Microsoft は、カーネル境界の全般的なセキュリティをさらに強化するために、新しい Windows バージョンに、一連の新たな防御機能を搭載しました。

この機能の 1 つが早期起動マルウェア対策（ELAM）検知メカニズムであり、これは他のサードパーティドライバが読み込まれる前にブートプロセスの非常に早い段階で確実に実行されるカーネルモードドライバをサードパーティのウイルス対策ソフトウェアが登録することを可能にします[12]。2012 年 8 月に Windows Server 2012 に最初に導入された ELAM は、サードパーティのウイルス対策ソフトウェアに、特に第 1 と第 2 クラスタに属す既知の不正なカーネルドライバに対する優位性を与えます。ELAM により、カーネルコンポーネントが完全に初期化された後、システムにすでに登録されている可能性があるその他の悪意のあるコードが読み込まれる前に、ウイルス対策カーネルドライバが読み込まれることが保証されます。ただし、オペレーティングシステムカーネルが読み込まれる前に投下されるその他の脅威（つまり第 3 クラスタの脅威）には効果はありません。ELAM はブートプロセスの低いレベルの抽象化レイヤを保護するために設計されたものではなく、正当に読み込まれたドライバのみを監視できます。大半のブートキット、および公開されていないオペレーティングシステム機能を使用してカーネルモードドライバを読み込む UEFI レベルのルートキットは監

[11] https://msrc.microsoft.com/update-guide/vulnerability/ADV220005

[12] https://learn.microsoft.com/en-us/windows-hardware/drivers/install/early-launch-antimalware

視できません。つまり、このような脅威はこのセキュリティ機能を回避し、カーネルアドレス空間にコードを注入することができます。

新たな Windows システムに ELAM が搭載される前にも、セキュアブートと呼ばれる新たなセキュリティ標準の採用が増えたことがありました。セキュアブートは、カーネルの初期化直前に、ブートプロセスで使用されるコンポーネントの整合性を確認するために設計されました[13]。このセキュリティ標準は、Windows のブートプロセスを標的とする、第 3 クラスタの脅威の一掃に役立ちました。また、ブートキットの作成者に対してもハードルを引き上げました。この結果、作成者は攻撃をスタックの 1 つ下のレイヤに移行し、実際のファームウェアを標的とするようになりました。セキュアブートの企業システムでの導入率が上がれば、第 3 クラスタの脅威は方向を転換し、手法を変えざるを得ないと考えられます。ブートプロセスの代わりに、システムのファームウェアの脆弱性が、標的とされるソフトウェアスタックの次の感染ポイントとなります。

Windows 10 では、仮想化ベースのセキュリティである仮想保護モード（VSM）機能が登場しました。この機能は、最新の CPU の仮想化拡張機能を使用して、メモリ内のデータに対する追加のセキュリティを提供します[14]。この機能ではより堅牢な防御メカニズムがサポートされ、Windows システムの整合性チェックロジックをまったく新しいレベルに引き上げます。この機能は、カーネルの侵害後に整合性チェックを無効にするための経路を見つけることに依存している、一部の脅威クラスタの一掃につながりました（第 1 クラスタの脅威は、脆弱なドライバまたはデュアルユースドライバを通して整合性を無効にします）。このような整合性チェックの中核にあるのが、カーネルイメージから分離された独立した仮想環境で実行する機能です。このため、侵害されても、ハイパーバイザーは分離されたコード整合性およびその他のセキュリティメカニズムに対する別の境界を適用することができます。

HVCI は、その中でカーネルモードのコード整合性を実行し、システムの侵害に使用される可能性があるカーネルメモリの割り当てを制限することにより、この仮想環境を保護して強化する重要なコンポーネントです。HVCI のトラストレットおよび VBS のどちらも、Windows カーネル信頼モデルを改善し、さまざまなエクスプロイトを使用して Windows カーネルを標的とする最新のマルウェアに対する強力な保護を提供しています。

この設計がより一般的になり、導入率が上がれば、Microsoft が適切なインタフェースを公開し、必要な最新の PC ハードウェアがより簡単に入手可能になった時点で、サードパーティのセキュリティソリューションも独自のハイパーバイザーをカスタマイズし始める可能性もあります。これは、あらゆるオペレーティングシステムのコア防御の未来形となる可能性

[13] https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot

[14] https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/tlfs/vsm

があります。しかし、このような高度なセキュリティメカニズムが登場しても、Windows カーネルの最も堅固な領域を標的とした脅威が未だに見られます[15]。

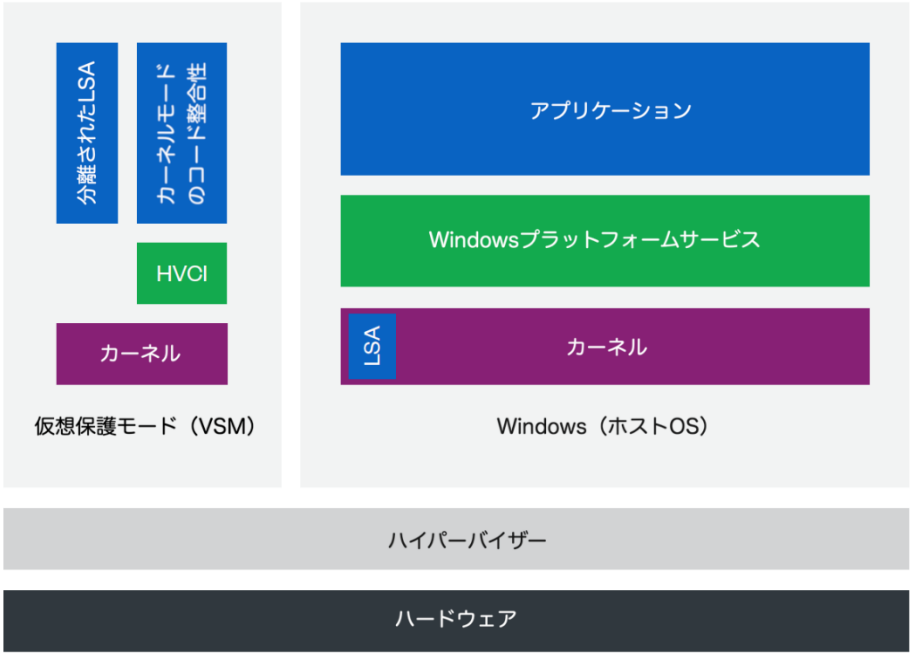


図 9：Windows 10 のユーザモードとカーネルモードレベル
出典：Windows Internals, Part 2, 7th Edition

脅威が未だに存在する理由

脅威アクタは、主要な目的を加速させ、サポートする高いアクセスレベルを獲得するために、常に最も抵抗の少ない経路をたどろうとします。

早期のブートプロセス、ハイパーバイザーレイヤにより保護される、完全に読み込まれ、初期化されるカーネル、新しいバージョンの Windows に搭載されているすべて組み込みのセキュリティメカニズムやハードウェアレベルのサポートなど、ソフトウェアスタック全体が防御機能により適切に保護されているように見えても、以下の理由から、Windows カーネルレベルの脅威は未だに存在し、当分は完全に消滅することはありません。

- ほとんどの企業ネットワークにはレガシーシステムが未だに存在している。
- 最新の革新的な仮想化ベースのメカニズムおよびセキュアブートメカニズムを導入するには、高いハードウェア要件を満たす必要がある。
- パフォーマンスへの影響および下位互換性の問題から、新しいカーネル防御メカニズムの導入率が低い。

[15] https://arstechnica.com/information-technology/2022/10/how-a-microsoft-blunder-opened-millions-of-pcs-to-potent-malware-attacks/

- 新たな防御も完璧ではない。いずれかのレイヤの保護メカニズムが回避されると、それ以降のレイヤも侵害される[16]。

トレンドマイクロでは今も、標的のネットワーク上で多様な目的のために展開されている、新たなカーネルレベルの脅威を確認しています。Windows システムにセキュリティメカニズムが導入されても、攻撃者はソフトウェアスタック内の感染ポイントを変えて適応します。

[16] https://arstechnica.com/information-technology/2022/10/how-a-microsoft-blunder-opened-millions-of-pcs-to-potent-malware-attacks/

Windows カーネル脅威の時系列での分析

脅威データの分析結果

このセクションでは、カーネルドライバコンポーネントに完全に依存しているか、カーネル空間で実行されるモジュールがチェーン内に 1 つ以上含まれる脅威を分析し、時系列で示します。分析されたデータには、悪用が確認されている脅威のみが含まれ、PoC は含まれていません。以下の図は、この 7 年間でサイバーコミュニティにより報告された、注目すべき脅威およびその他の主要なイベントの数を示しています。ここ 5 年で、数値は顕著な傾向を示しています。

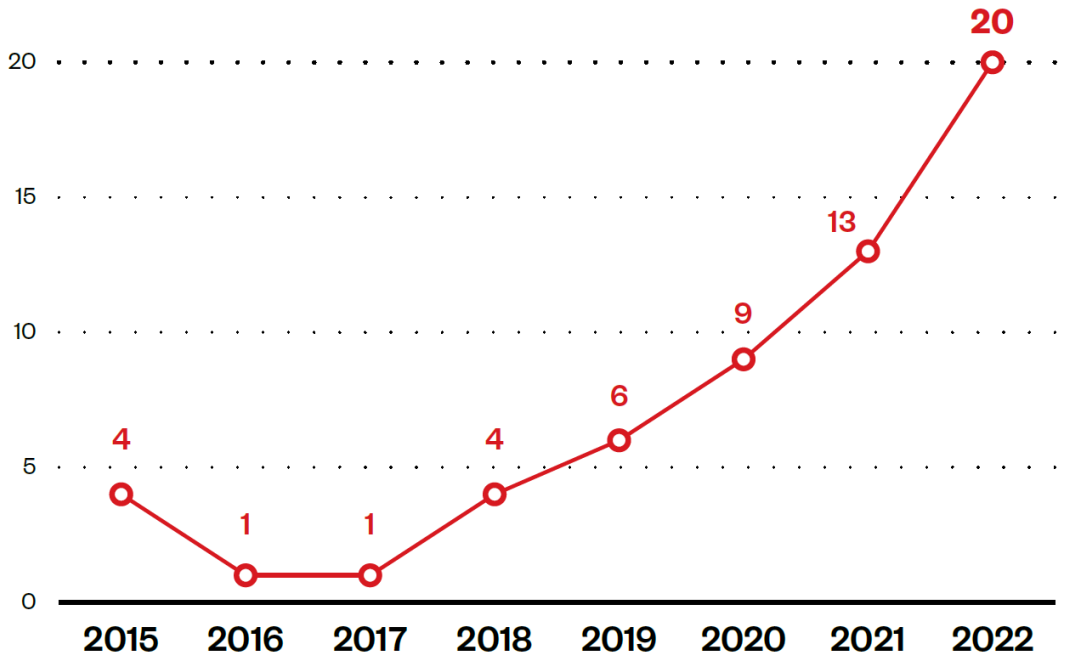


図 10：2015 年 4 月から 2022 年 10 月までのカーネルレベルの脅威を含んでいた、公開されたインテリジェンスレポートの数

図 11 は、第 3 クラスタの脅威の数が最も少なかったことを示しています。図 12 は、この 7 年間で各クラスタがどのように進化したかを示しています。ここ 3 年で、第 3 クラスタの脅威の数が顕著に増えていることがわかります。

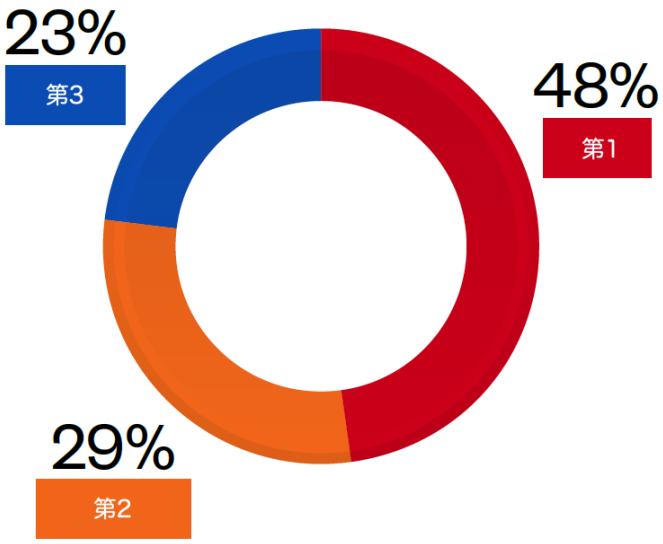


図 11：2015 年 4 月から 2022 年 10 月までのカーネルレベルの脅威の 3 つのクラスタの割合

図 11 を見ると、さまざまな脅威アクタ間で、依然として第 1 クラスタの脅威が最も人気であることは明らかです。現時点では、第 1 クラスタの脅威が、Windows カーネルに影響する脅威の大半を占めています。このクラスタの脅威の数は、Windows 10 で導入された新たなハイパーバイザーを基にした防御策が普及するまで増加し、その防御策の導入率が高まると、これらの脅威の数は大幅に減少すると予想されています。Microsoft がカーネルドライバに対するクロス署名プロセスを、ポータル内でカーネルドライバを検証、テスト、署名するためのより厳格な手順で置き換えると、第 1 クラスタの脅威により悪用されている脆弱なカーネルドライバの数は減少するでしょう。

第 2 クラスタの脅威は、このような攻撃の開発には高いコストがかかるため、第 1 クラスタの脅威ほど検知は多くありません。ただし図 12 を見ると、第 2 クラスタの脅威の数は 2018 年以降増加していますが、Windows 10 および 11 のカーネルコード署名ポリシーの影響により今後は減少し、最終的には脅威が消滅すると予想されています。これ以降のセクションでは、これらの署名ポリシーについて、またこれらのポリシーがカーネルレベルの脅威にどのように影響するかについて詳しく解説します。

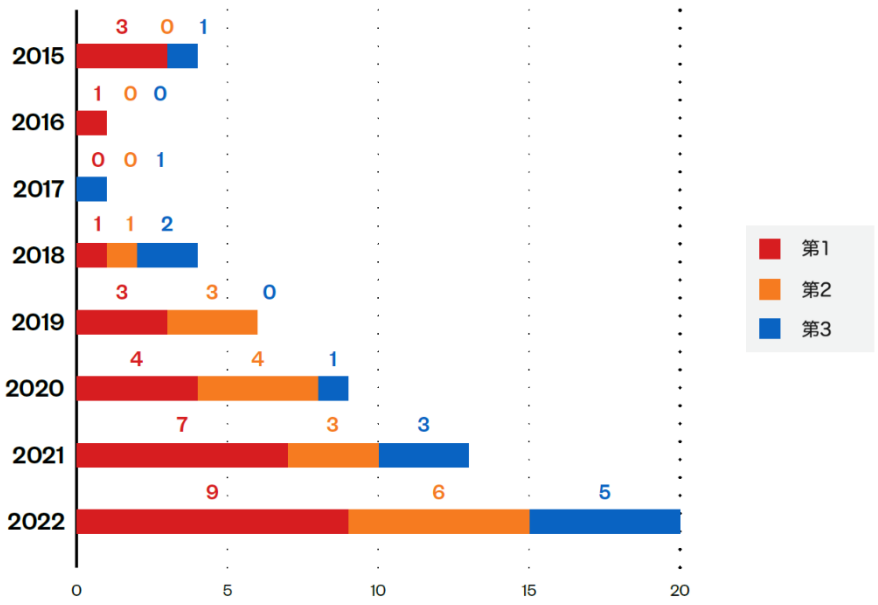


図 12：2015 年 4 月から 2022 年 10 月までのクラスタごとに分類された
カーネルレベルの脅威

最後に、第 3 クラスタの脅威は、その複雑な設計および非常に高度で成熟したアクタによってのみ使用されていることから、最も検知数が少なくなっています。今後数年間は第 3 クラスタの脅威が徐々に増加すると考えられます。これは、攻撃者が前述の最新のセキュリティメカニズムを回避するために、最初の感染ポイントをプロセスのより早い段階にシフトするためです。前述のとおり、これらの脅威の開発は複雑であることから、急速には増加しないでしょう。

また、この調査のために分析したデータを基に、カーネルレベルのアクセスを使用する脅威の種類を、図 13 に示すように分類できました。

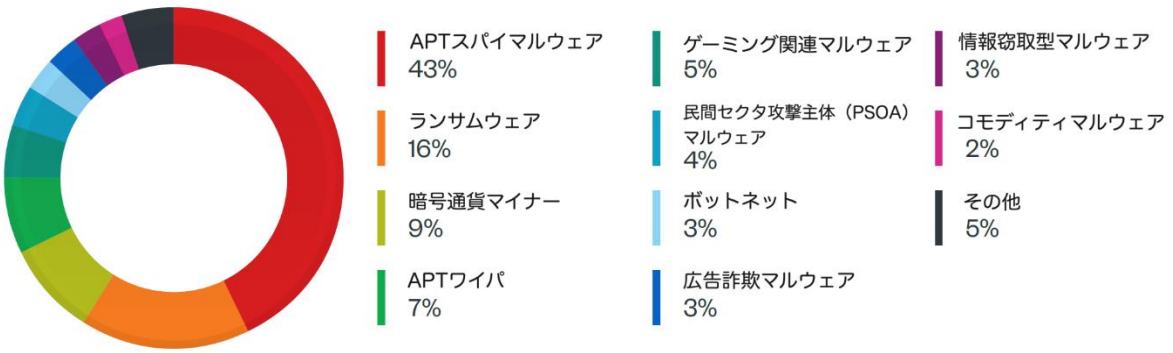


図 13：2015 年 4 月から 2022 年 10 月までのカーネルレベルのマルウェアを利用した脅威
の種類

図 13 は、APT スパイマルウェアが、低レベルのコンポーネントを攻撃で最も使用していたことを示しています。これは、APT スパイグループの活動には、カーネルルートキットや

低レベルのインプラントなどのステルスコンポーネントの使用が適しており、またカーネルルートキットを開発し、攻撃で使用するための能力とリソースを持っているためです。ほとんどのルートキットのインスタンスは、高度なアクタにより開始された注目度の高い標的型攻撃に関連するため、このような脅威の検知と根絶は容易ではありません。

ランサムウェアアクタおよびその攻撃参加者も、攻撃で使用するランサムウェアファミリに対して特権レベルのアクセスを得ることに高い関心を示していました。最終的なペイロードの投下時にセキュリティ製品による検知を回避するために、低レベルコンポーネントを組み込んでいるランサムウェアファミリを使用しています。クリプトマイニング脅威もカーネルに足掛かりを持っていることが確認されています。これらの脅威の主な目的は、違法なクリプトマイニングプロセスを保護し、さまざまなコンポーネントを隠し、影響するシステムでクリプトマイナーにより引き起こされるパフォーマンスの低下を隠ぺいすることです。

これらのカーネルレベルの脅威の各キルチェーンをマッピングすることにより、図 14 に示すように、ほとんどのカーネル関連のペイロードは通常、防御回避フェーズで使用されていることがわかりました。これは、攻撃者がカーネルレベルのアクセスを取得すると獲得できる特権アクセスの典型的な用途であると考えられます。

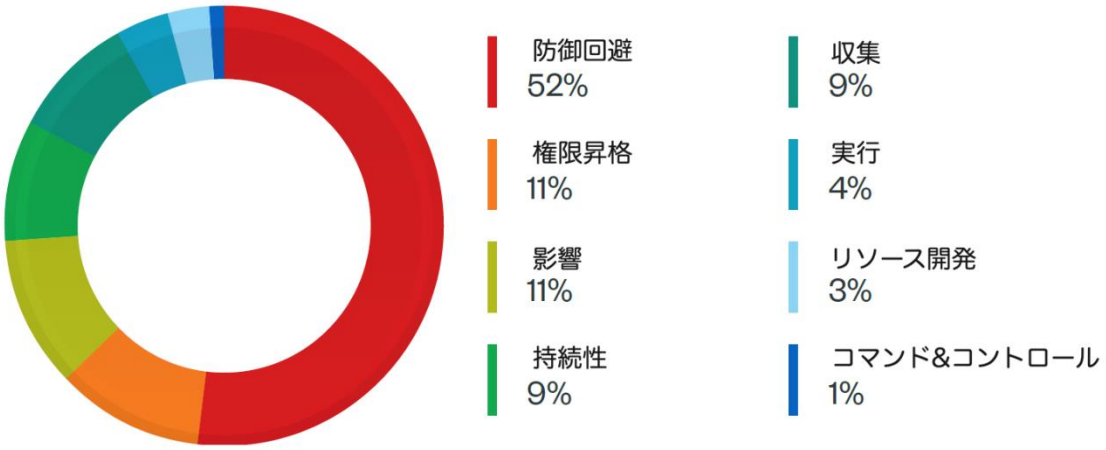


図 14：カーネルレベルの脅威が使用されているキルチェーンフェーズの特定

キルチェーンの収集フェーズでは、攻撃者は重要なデータの収集を試みますが、これをカーネル空間から行うことにより、検知されずに保護されたリソースに自由にアクセスすることが可能になります。一方、リソース開発フェーズでは、高度な攻撃者は、カスタムドライバを読み込むためのコード署名証明書の取得など、カーネルレベルのアクセスを取得するための多様な機能を獲得しようと試みます。通常、これは実際の侵入の前に計画されます。

図 15 に、この調査で分析したカーネルレベルの脅威に、最も使用されている MITRE ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）の手法をどのようにマッピングしたかを示します。

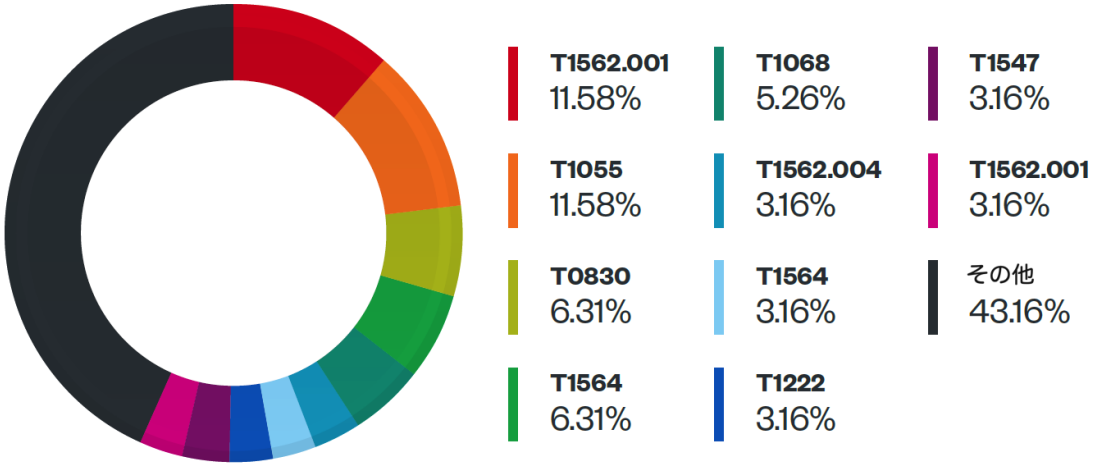


図 15：カーネル脅威の MITRE ATT&CK の手法へのマッピング

トレンドマイクロのデータに基づくと、カーネルレベルの脅威の 11%は、防御を阻害するために（Impair Defenses：Disable or Modify Tools、T1562.001）、カーネルレベルのアクセスの取得を試みています。攻撃者は、マルウェアペイロード、ツール、および活動の検知を回避するために、セキュリティツールの改ざんや無効化を試みます。ユーザのデスクトップまたはサーバでのエンドポイント保護プラットフォーム（EPP）やエンドポイントでの検知と対応（EDR）テクノロジにより、ユーザ空間プロセスの保護が強化されていることから、この用途は当然といえます。このように保護レイヤが追加されていることから、攻撃者は最も抵抗の少ない経路を選択し、セキュリティソリューションを妨害するためにコードの一部をカーネルレベルで実行しています。

VirusTotal の統計情報

トレンドマイクロでは、a）署名されたドライバが失効しているか、また b）VirusTotal のマルウェアリポジトリなどのマルウェア検索エンジンで 1 回以上検知されているかに基づいて、Windows カーネルドライバのサンプルを評価しました。2015 年 1 月から 2022 年 5 月までに収集した脅威サンプルをどのように分類したかを以下に示します。

サンプルセット	説明
セット1	検知数が0回で、失効されていない署名されたドライバ
セット2	複数のエンジンでの1回以上の検知数で、失効されていない署名されたドライバ
セット3	検知数が0回で、失効されている署名されたドライバ
セット4	複数のエンジンでの1回以上の検知数で、失効されている署名されたドライバ

分析したカーネルレベルの脅威の大半は、複数のエンジンでの 1 回以上の検知数で、失効されていない署名されたドライバを持ち、検知数が 0 回で、失効されていない署名されたドライバを持つ脅威の割合がそれに続いています。

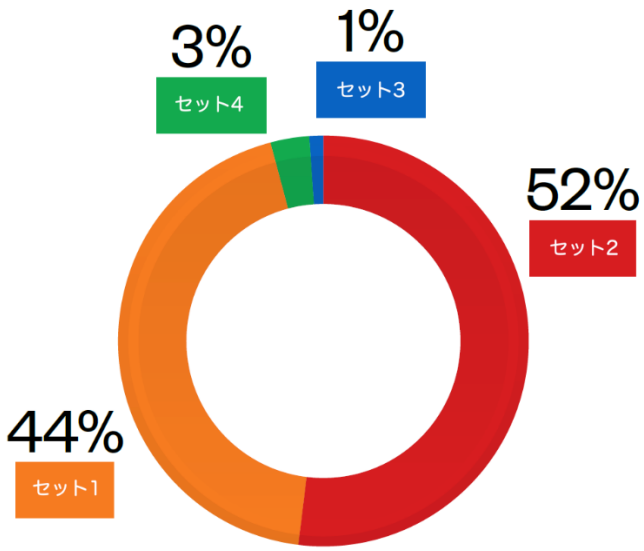
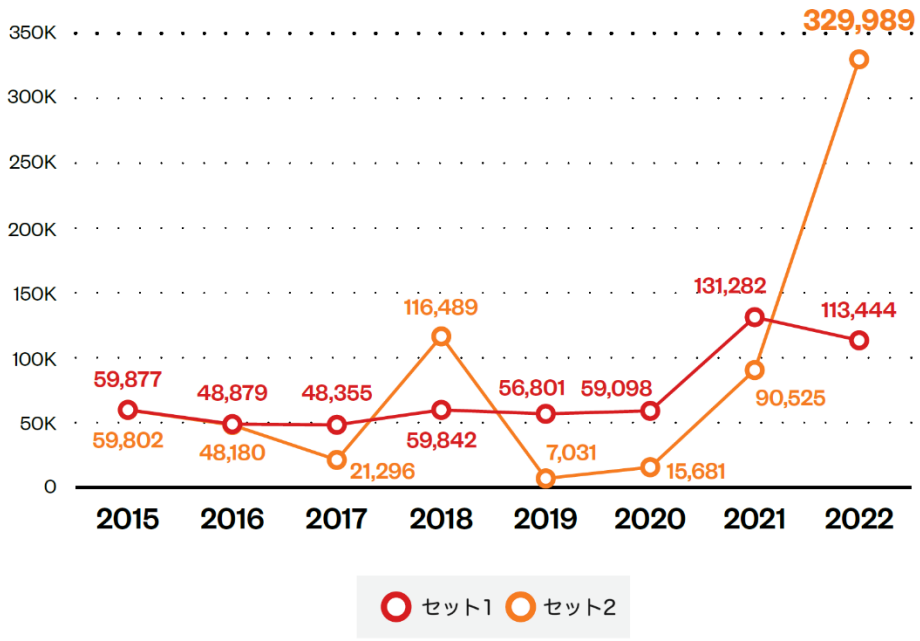


図 16：a）署名されたドライバが失効されているかどうか、また b）1 回以上検知されているかどうかに基づく、Windows カーネルドライバのサンプルの内訳

トレンドマイクロのデータは、2020 年から 2022 年 5 月にかけて、4 つのサンプルセットのうちの 3 つ（セット 2、3、4）の脅威が増加したことを示しています。



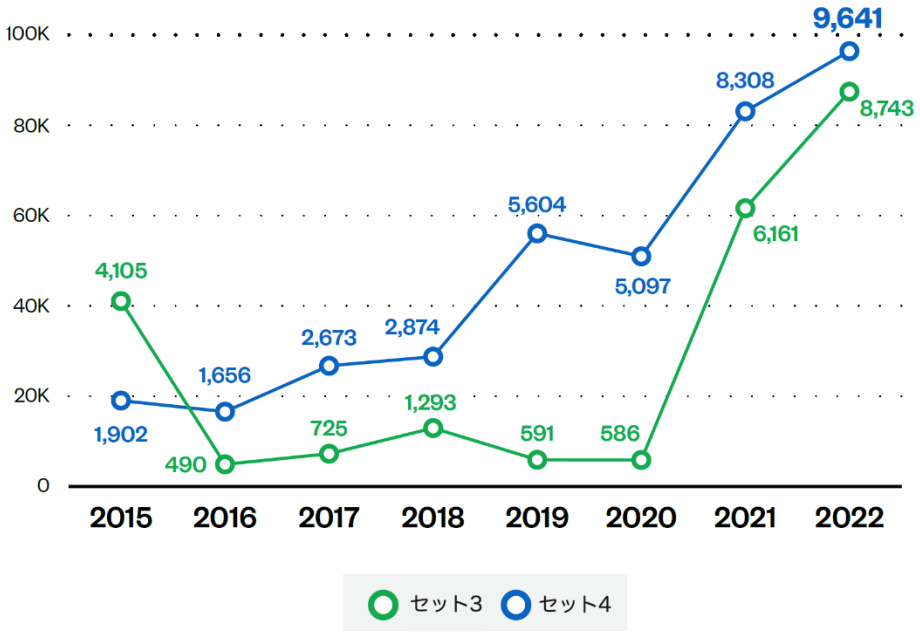


図 17：2020 年から 2022 年 5 月にかけて、サンプルセット 2、3、4 のカーネルドライバの提出数が増加

注目すべきイベント

このセクションでは、2015 年 4 月から 2022 年 10 月の間に、Windows カーネルに影響を及ぼした、一般に公開されている注目すべきイベントを紹介します。図 18 に、各脅威クラスタに対する主要なイベントのタイムラインを示します。またそれ以降の表には、攻撃者の攻撃目標を達成するためにどのように使用されたか、また Windows カーネルの信頼モデルにどのように影響したかなど、各脅威についての詳細を示します。表 1、2、3 は、各脅威クラスタからのサンプルを示しています。PoC およびこの調査との関連性を確認するための一般公開されたサンプルのない攻撃は含まれていません。

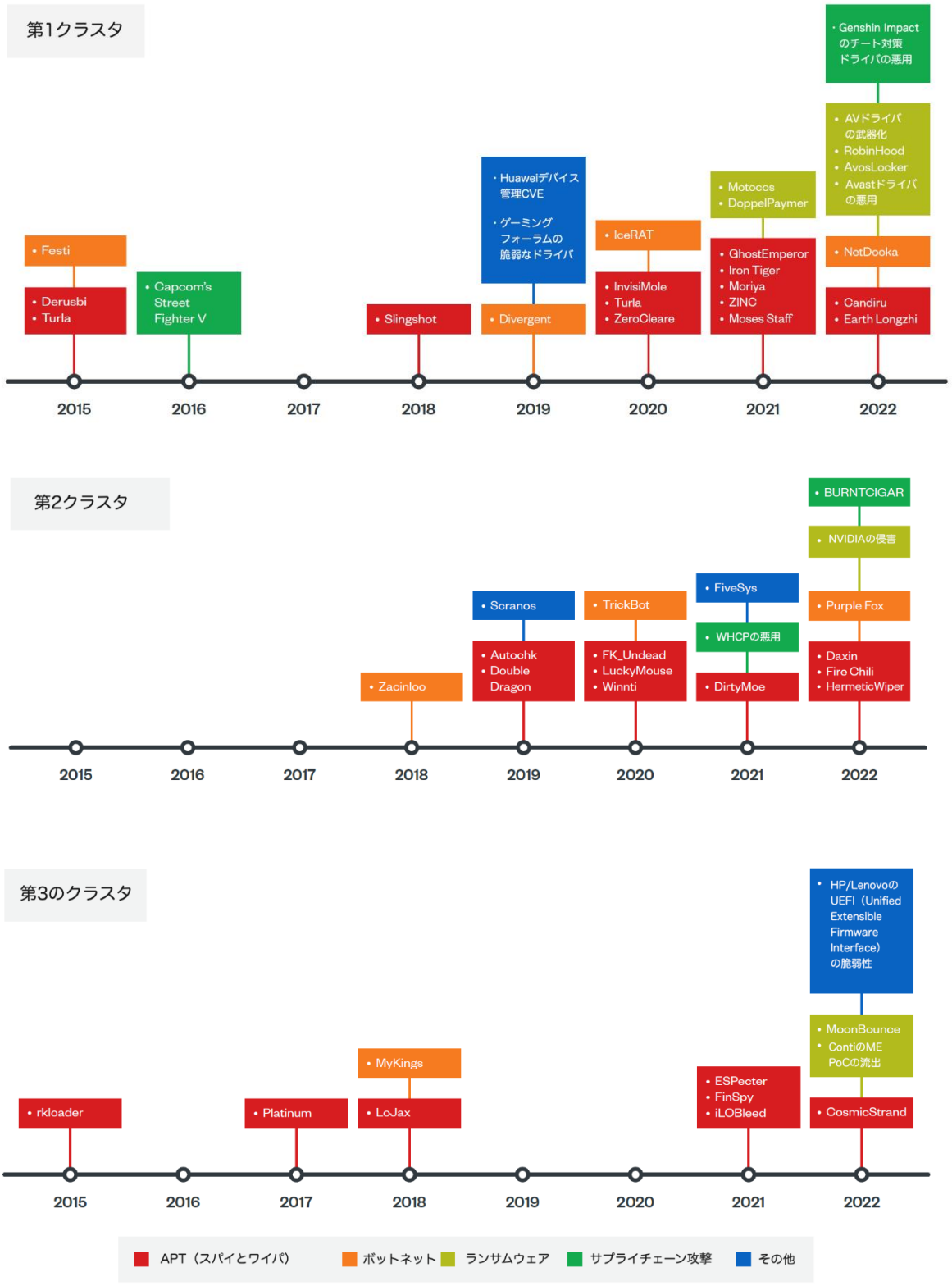


図 18：2015 年 4 月から 2022 年 10 月の間に Windows カーネルに影響を及ぼした注目すべきイベント

脅威名	脅威プロファイル
Earth Longzhi（2022）[17]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**カスタマイズしたCobalt Strikeローダを使用して複数の地域を標的とするキャンペーン。このAPTグループは、台湾、中国、タイ、マレーシア、インドネシア、パキスタン、およびウクライナの防衛、航空、保険、および都市開発産業の知名度の高い企業を標的としています。 **カーネルドライバの動作：**脆弱なドライバ（RTCore64.sys）は、認証されたユーザがカーネル空間を含む任意のアドレスを読み取る/書き込むことを可能にします。ウイルス対策製品を終了させるために使用されます。
Genshin Impactのチート対策ドライバの悪用（2022）[18]	**脅威の種類：**ランサムウェア **手法：**脆弱なドライバ **脅威の詳細：**チート対策機能を提供する脆弱なドライバを悪用することにより、被害者のデバイス内にランサムウェアを導入する脅威アクタ。 **カーネルドライバの動作：**このドライバは現在、ランサムウェアを一括導入する目的でウイルス対策プロセスやサービスをキルするためにランサムウェアアクタにより悪用されています。
Candiru（2022）[19, 20, 21]	**脅威の種類：**PSOA **手法：**署名されたドライバ **脅威の詳細：**Candiruは、サービスとしてのハッキング（Hacking-as-a-Service）パッケージとしてサイバー兵器を政府に販売している民間企業です。同社が販売している兵器の1つが、Google Chromeに対するゼロデイエクスプロイトを使用した水飲み場攻撃によって、レバノン、トルコ、イエメン、およびパレスチナのユーザを標的とするスパイウェアです。 **カーネルドライバの動作：**physmem.sysと呼ばれる署名されたドライバを使用します。このドライバの説明は「物理メモリアクセスドライバ」であり、「仕様により」カーネルの読み取り/書き込みが可能です。このドライバが、他のプロセスから一部のAPIコールが見えないようにするなど、検知を阻止するためにカーネルを使用して特定のAPIコールをプロキシするように悪用されました。

[17] https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html

[18] https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html

[19] https://www.microsoft.com/en-us/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

[20] https://decoded.avast.io/janvojtesek/the-return-of-candiru-zero-days-in-the-middle-east/

[21] https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

脅威名	脅威プロファイル
ウイルス対策ドライバの武器化（2022）[22]	**脅威の種類：**ランサムウェア **手法：**デュアルユースドライバ **脅威の詳細：**Avastアンチルートキットカーネルドライバの機能を悪用して、一般的なAVおよびEDRプロセスを終了させるランサムウェアキャンペーン。 **カーネルドライバの動作：**エンドポイントセキュリティ製品に属すプロセスやファイルをキルします。
Avastドライバ（2022）[23]	**脅威の種類：**ランサムウェア **手法：**脆弱なドライバ **脅威の詳細：**これらの脆弱性は、検知されずにセキュリティ製品を無効化し、システムコンポーネントを上書きし、その他の悪意のある操作を実行するための昇格した権限を攻撃者が得ることを可能にします。 **カーネルドライバの動作：**攻撃者は、*aswArPot.sys*カーネルドライバ内のソケット接続ハンドラで、CVE-2022-26522およびCVE-2022-26523をトリガします。
NetDooka（2022）[24]	**脅威の種類：**コモディティマルウェア **手法：**組み込みツール **脅威の詳細：**ローダ、ドロッパ、保護ドライバ、および独自のネットワーク通信プロトコルを実装するフル機能のRATを含む高度なマルウェア。攻撃はPPI（Pay-per-Install）サービスによって拡散されます。 **カーネルドライバの動作：**このドライバの主な機能は、ユーザモードコンポーネントを保護して隠すことです。
AvosLocker（2022）[25]	**脅威の種類：**ランサムウェア **手法：**デュアルユースドライバ **脅威の詳細：**正規のAvastアンチルートキットドライバ（*asWarPot.sys*）からエクスポートした機能を使用して、セキュリティ関連のプロセスを終了させるラン

[22] https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/

[23] https://www.sentinelone.com/labs/vulnerabilities-in-avast-and-avg-put-millions-at-risk/

[24] https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html

[25] https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html

	サムウェアキャンペーン。 **カーネルドライバの動作：**ランサムウェアペイロードを中断および検知されずに実行できるようにセキュリティ関連のプロセスを終了させるために、正規のドライバが使用されます。
RobbinHood（2022）[26]	**脅威の種類：**ランサムウェア **手法：**脆弱なドライバ **脅威の詳細：**脆弱なドライバを使用して、署名ポリシーを無効にし、署名されていないドライバを読み込むランサムウェアキャンペーン。 **カーネルドライバの動作：**ランサムウェアペイロードを中断および検知されずに実行できるように、署名されていないドライバが、エンドポイントセキュリティ製品に属すプロセスやファイルをキルし、改ざん防止機能を回避します。

脅威名	脅威プロファイル
DoppelPaymer（2021）[27]	**脅威の種類：**ランサムウェア **手法：**脆弱なドライバ **脅威の詳細：**Process Hackerツールを使用して、セキュリティ関連のサービスやプロセス、メールサーバ、データベースソフトウェアを終了させるランサムウェアキャンペーン。 **カーネルドライバの動作：**Process Hackerツールのユーザモードプロセス内のDLLサイドローディングの脆弱性を利用して、Process Hackerドライバと通信し、プロセスを終了させます。
MosesStaff（2021）[28]	**脅威の種類：**APTワイパ **手法：**サードパーティドライバの悪用 **脅威の詳細：**イスラエルの組織を標的とし、機密情報を盗み、被害者のネットワークを暗号化し、身代金の要求なしに盗んだデータを漏洩させたキャンペーン。 **カーネルドライバの動作：**この脅威はDiskCryptorオープンライブラリを使用して被害者のマシンを暗号化してから、カスタマイズしたブートローダをインストールして被害者のマシンをロックします。

[26] https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/

[27] https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html

[28] https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

GhostEmperor（2021）[29, 30]	**脅威の種類：**APTスパイ **手法：**デュアルユースドライバ **脅威の詳細：**被害者のサーバの遠隔操作を可能にすることを目的とした、高度なマルチステージマルウェアフレームワーク。 **カーネルドライバの動作：**このカーネルドライバは、ファイル、レジストリ、TCP接続、実行中のサービスなどのユーザモードの成果物を隠します。
Motocos（2021）[31]	**脅威の種類：**ランサムウェア **手法：**脆弱なドライバ **脅威の詳細：**MotocosランサムウェアはTelegramを使用して被害者とやり取りします。またこのランサムウェアは、被害者のマシンを感染させた後、身代金の額を毎日引き上げます。 **カーネルドライバの動作：**Motocosランサムウェアは、RobinHoodランサムウェアと似たドライバ構造を持ちます。
Moriya（2021）[32]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**アジアおよびアフリカの複数の著名な組織を標的とし、公開されているサーバに受動的なバックドアを導入するキャンペーン。 **カーネルドライバの動作：**このドライバはネットワークパケットの検査を実行するため、攻撃者はネットワークスタックにより処理される前に対象のパケットを投下し、セキュリティソリューションにより検知されないようにすることができます。Moriyaの開発者に関連する可能性がある、AVプロセスをキルするその他のドライバもあります。

[29] https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/

[30] https://usa.kaspersky.com/about/press-releases/2021_ghostemperor-apt-targets-high-profile-victims-using-unknown-rootkit

[31] https://twitter.com/TrendMicroRSRCH/status/1398270334068011016

[32] https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/

脅威名	脅威プロファイル
Iron Tiger（2021）[33]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**東南アジアのギャンブルおよび賭博会社を標的とし、バックドアをインストールするキャンペーン。*dlpumgr32.exe*に存在する、サイドロードされる注入手法を利用し、既知の脆弱性を悪用してDSEを無効化し、署名されていないドライバを読み込みます。 **カーネルドライバの動作：**このカーネルドライバは、定義済みのトークンで受信トラフィックをフィルタリングし、 「*lsass.exe*」プロセス内にコードを注入します。
ZINC（2021）[34]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：***Browse.vc.db*と呼ばれる悪意のあるDLLを始めとする構築済みのバイナリを含む悪意のあるVisual Studioプロジェクトを送信することにより、脅威研究者を標的とするキャンペーン。 **カーネルドライバの動作：***Viraglt64.sys*内のCVE-2017-16238の悪用を試みます。ただしこのコードにはバグが多いようで、脆弱性の悪用には失敗します。
InvisiMole（2020）[35]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**被害者のWebカメラやマイクを録画または録音し、位置情報をトラッキングし、最近アクセスしたドキュメントを収集するなど、広範なスパイ機能を提供するバックドア。 **カーネルドライバの動作：**正規のユーザモードプロセスへのコードの注入に使用される脆弱なドライバ。

[33] https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

[34] https://www.microsoft.com/en-us/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

[35] https://web-assets.esetstatic.com/wls/2020/06/ESET_InvisiMole.pdf

AcidBox（2020）[36]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**持続性とlsassプロセスへのDLLの注入およびVirtualBoxを悪用した署名されていないドライバの読み込みのために、Windowsセキュリティサポートプロバイダ（SSP）を悪用します。 **カーネルドライバの動作：**1つ以上のコンポーネントからのコマンドを待機します。これらのコマンドの目的は、ドライバによるカーネル空間からの追加のレジストリペイロードの読み込みや、新たなSSP DLLのインストールなどです。
ZeroCleare（2020）[37]	**脅威の種類：**APTワイパ **手法：**脆弱なドライバ **脅威の詳細：**Windowsベースのマシンのマスタブートレコード（MBR）およびディスクパーティションの上書きを目的とする破壊的な攻撃です。脆弱なドライバを悪用してDSEを無効化し、ElRawDiskドライバを読み込んで生ハードディスクデータにアクセスします。 **カーネルドライバの動作：**ハードディスクへのアクセスを可能にする署名されていないドライバです。

脅威名	脅威プロファイル
Divergent（2019）[38, 39]	**脅威の種類：**広告詐欺 **手法：**サードパーティドライバの悪用 **脅威の詳細：**NodeJSおよびWinDivertと呼ばれる正規のオープンソースユーティリティを利用する、新しいマルウェアローダ。攻撃者はこのマルウェアを使用して企業ネットワークを標的とすることができます。主にクリック詐欺を実行するように設計されているようです。 **カーネルドライバの動作：**このマルウェアは、WinDivertライブラリを使用してAVトラフィックをブロックし、感染したホストが試みるすべての外部接続に対する、3ウェイTCP（Transmission Control Protocol）ハンドシェイクの最初のSYN（同期）パケットを傍受して書き換えます。SYNパケットに加えられる変更は、*divergent.exe*と*mdivergent.exe*のどちらの実行可能ファイルが使用されたかにより異なります。

[36] https://unit42.paloaltonetworks.com/acidbox-rare-malware/

[37] https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/

[38] https://blog.talosintelligence.com/divergent-analysis/

[39] https://repnz.github.io/posts/abusing-signed-drivers/

ドライバの脆弱性（2019）[40]	**脅威の種類：**その他 **手法：**脆弱なドライバ **脅威の詳細：**Huaweiドライバの脆弱性の悪用。攻撃者がカーネル空間からWindowsの非同期プロシージャ呼び出し（APC）を使用して他のユーザモードプロセス内にコードを注入することを可能にします。これにより、ローカル権限の昇格を実行できます。 **カーネルドライバの動作：**権限のないプロセスが他のプロセス内にコードを注入することを可能にする、Huaweiドライバの脆弱性。
SlingShot（2018）[41]	**脅威の種類：**APTスパイ **手法：** **脅威の詳細：**ローダSlingshotがシステムDLL「scesrv.dll」を独自のDLLで置き換えます（SYSTEM権限でServices.exeにより読み込まれます）。持続性と権限昇格のために、不正なDLLは脆弱なドライバを悪用し、DSE（Driver Signature Enforcement）を無効にし、独自の署名されていないドライバを読み込みます。 **カーネルドライバの動作：**このカーネルモードコンポーネントは次の操作を実行します。ユーザモードプロセスにペイロードを注入し、ネットワークトラフィックを隠し/傍受し、デバッグ対策手法のための関数をフックし、カーネルレベルで実行するためのコードを受信し、イベント関連のプロセスについてユーザモードプロセスに通知します。
CapcomのStreet Fighter V（2016）[42]	**脅威の種類：**ゲーミング関連 **手法：**脆弱なサプライチェーン **脅威の詳細：**影響するコンピュータ上にインストールされているアプリケーションにカーネルレベルの権限を付与するルートキットをインストールするアップデート。 **カーネルドライバの動作：**このルートキットは、オペレーティングシステムのSMEP（Supervisor Mode Execution Protection）機能を無効にして、悪意のあるコードを実行します。その後、SMEPを再度有効にします。

[40] https://www.microsoft.com/en-us/security/blog/2019/03/25/from-alert-to-driver-vulnerability-microsoft-defender-atp-investigation-unearths-privilege-escalation-flaw/

[41] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf

[42] https://www.theregister.com/2016/09/23/capcom_street_fighter_v

脅威名	脅威プロファイル
DERUSBI（2015）[43]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**非常に平凡なリモートアクセス型のトロイの木馬（RAT）を含む、Derusbiサーバの亜種です。ファイル管理（アップロードとダウンロード）、ネットワークトンネリング、リモートコマンドシェルなどの基本的なRAT機能をサポートしています。 **カーネルドライバの動作：**このドライバは、Windows XP以前のバージョンに含まれる、公開されていないWindowsファイアウォールのフック手法を使用するか、Windows Vista以降のバージョンに含まれる、公開されているWindowsフィルタリングプラットフォームを使用して、Windowsファイアウォールにフックします。クライアントとサーバの亜種間で特定のハンドシェイクが発生すると、確立済みのセッションの残りの通信セッションはリダイレクトされます。 これにより、攻撃者は1つのIPから発生するネットワークセッションのクラスタ内に自身の通信を隠せます。
Festi（2015）[44]	**脅威の種類：**ボットネット **手法：**レガシーシステム **脅威の詳細：**非常に強力なサービス拒否（DoS）エンジンを実装し、スパムメッセージを送信するボット。主にPPI（Pay-per-Install）方式で拡散されます。 **カーネルドライバの動作：**攻撃のメインモジュールが、コマンドアンドコントロール（C&C）サーバからの設定データを更新し、実行する追加の専用カーネルプラグイン（これらがすべてのDDOSおよびスパム攻撃を実行する）をダウンロードします。
Turla（2015）[45]	**脅威の種類：**APTスパイ **手法：**脆弱なドライバ **脅威の詳細：**高機能なルートキットを含む高度なマルウェア。サイバースパイ活動や認証情報の窃取などの多様な目的で使用できる分散C&Cアーキテクチャに基づいています。 **カーネルドライバの動作：**このカーネルコンポーネントの主な機能は、メモリでntoskrnl.exeおよびndis.sysを編集し、新しいIDTエントリを作成することによって、そのユーザモードコンポーネントを隠す/保護することです。

表 1：第 1 クラスタの脅威の一覧

[43] https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Derusbi_Server_Analysis-Final.pdf

[44] https://www.welivesecurity.com/2012/05/11/king-of-spam-festi-botnet-analysis/

[45] https://www.eset.com/us/about/newsroom/press-releases/cyber-espionage-group-turla-and-its-latest-malware-under-the-microscope-1/

脅威名	コンテキスト
BURNTCIGAR（2022）[46]	**脅威の種類：**ランサムウェア **手法：**署名されたドライバ **脅威の詳細：**複数のセキュリティ製品を回避するために、Microsoft署名の不正なドライバを利用する攻撃者。 **カーネルドライバの動作：**さまざまなエンドポイントセキュリティ製品ベンダにより使用されているプロセスやサービスを終了させます。

脅威名	コンテキスト
NVIDIAの侵害（2022）[47, 48]	**脅威の種類：**ランサムウェア **手法：**流出した証明書 **脅威の詳細：**サイバー犯罪グループのLapsus$がNVIDIAを侵害し、データおよびデジタル署名証明書を窃取しました。 **カーネルドライバの動作：**認証情報、ソースコード、および期限の切れた2つのコード署名デジタル証明書が公開されました。
Fire-Chili（2022）[49]	**脅威の種類：**APTスパイ **手法：**署名されたコード **脅威の詳細：**主に金融、教育、化粧品、および旅行業界を標的とするキャンペーン。漏洩されたGh0st RATコードに基づくバックドアを導入し、感染したマシン上で盗んだデジタル証明書を使用します。 **カーネルドライバの動作：**このドライバは、ゲーム開発会社から盗まれた証明書でデジタル署名されています。DKOM（Direct Kernel Object Modification）を使用して、ユーザモードコンポーネントからの不正な成果物を隠して保護します。

[46] https://news.sophos.com/en-us/2022/12/13/signed-driver-malware-moves-up-the-software-trust-chain/

[47] https://www.techrepublic.com/article/nvidias-breach-might-help-cybercriminals-run-malware-campaigns/

[48] https://www.youtube.com/watch?v=1H9tEfkjFXs&t=320s&ab_channel=DEFCONConference

[49] https://www.welivesecurity.com/2012/05/11/king-of-spam-festi-botnet-analysis/

HermaticWiperの実行可能ファイル（2022）[50, 51, 52]	**脅威の種類：**APTワイパ **手法：**CS証明書の取得 **脅威の詳細：**ウクライナの組織を標的とするワイパ攻撃。 **カーネルドライバの動作：**このドライバは、ユーザモードコンポーネントが生ディスクの特定のセクタに書き込むことを可能にするプロキシとして機能します。
Daxin（2022）[53]	**脅威の種類：**APTスパイ **手法：**署名されたコード **脅威の詳細：**特定の政府およびその他の標的とする重要なインフラストラクチャに対する長期のスパイ活動で使用されているバックドア。攻撃者が感染したコンピュータ上でさまざまな通信およびデータ収集操作を実行することを可能にします。 **カーネルドライバの動作：**このドライバは、正規のTCP/IP接続を乗っ取り、任意のファイルを読み取り/書き込み、任意のプロセスを開始します。
PurpleFox（2022）[54, 55]	**脅威の種類：**クリプトマイニング **手法：**署名されたコード **脅威の詳細：**暗号通貨マイナーにより、感染したマシンのリソースを利用する攻撃。 **カーネルドライバの動作：**このドライバは、セキュリティ製品のミニフィルタドライバを停止し、ファイルをコピーして削除し、サービスをインストールし、プロセスをキルします。

[50] https://www.reuters.com/world/europe/cyprus-games-writer-denies-links-malware-found-before-russian-invasion-2022-02-24/

[51] https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/

[52] https://www.malwarebytes.com/blog/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine

[53] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage

[54] https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html

[55] https://minerva-labs.com/blog/malicious-telegram-installer-drops-purple-fox-rootkit/

脅威名	コンテキスト
FiveSys（2021）[56, 57]	**脅威の種類：**情報窃取型マルウェア **手法：**WHCP署名されたコード **脅威の詳細：**認証の窃取とゲーム内購入の乗っ取りを主な目的とした、オンラインゲームを標的とする攻撃。 **カーネルドライバの動作：**このドライバは、攻撃者が関心を持つインターネットアドレスへのトラフィックのプロキシ、ユーザモードコンポーネントの保護、および他のマルウェアドライバの感染した環境への読み込みの阻止のために使用されます。
DirtyMOE（2021）[58, 59]	**脅威の種類：**クリプトマイニング **手法：**署名されたコード **脅威の詳細：**このキャンペーンの主な目的は、クリプトジャッキングを実行し、感染したマシン上でDDoS攻撃を開始することです。 **カーネルドライバの動作：**このドライバはユーザモードの悪意のある活動やサービスを隠します。ファイルシステムやレジストリへの書き込み、プロセスのキル、標的プロセスへの任意のDLLの注入など、ユーザモードから受信したコマンドも実行します。
WHCPの悪用（2021）[60]	**脅威の種類：**ゲーミング関連 **手法：**正規に署名されたドライバ **脅威の詳細：**中国のゲーミング環境を標的とするキャンペーン。 **カーネルドライバの動作：**サイバー犯罪者の位置情報を偽装してシステムをだまし、どこからでもゲームをプレイできるように、不正なドライバが使用されます。
IceRat（2020）[61, 62]	**脅威の種類：**暗号通貨マイニング **手法：**署名されたドライバ

[56] https://www.bitdefender.com/blog/labs/digitally-signed-rootkitsare-back-a-look-atfivesys-and-companions/

[57] https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf

[58] https://decoded.avast.io/martinchlumecky/dirtymoe-rootkit-driver/

[59] https://decoded.avast.io/martinchlumecky/dirtymoe-3/

[60] https://msrc.microsoft.com/blog/2021/06/investigating-and-mitigating-malicious-drivers/

[61] https://www.gdatasoftware.com/blog/icerat-evades-antivirus-by-using-jphp

[62] https://isc.sans.edu/diary/Example+of+how+attackers+are+trying+to+push+crypto+miners+via+Log4Shell/28172

	脅威の詳細：被害者のマシン上での違法な暗号通貨マイニング活動を可能にするバックドアです。 **カーネルドライバの動作：**メモリの読み取り/書き込みとCPUのMSR（Model-Specific Register）へのアクセスのためのカーネル空間へのアクセスを可能にする、WinRing0x64ドライバを使用します。
TrickBot（2020）[63]	**脅威の種類：**ボットネット **手法：**署名されたドライバ **脅威の詳細：**よく知られた脆弱性を悪用することによりトリガされる、ファームウェアレベルの脅威。攻撃者はファームウェアに悪意のあるコードを埋め込むことにより、感染したマシンでそのコードが最初に実行されるようにすることができます。 **カーネルドライバの動作：**REWEverythingドライバを使用してハードウェアインタフェースに直接アクセスし、ファームウェアレベルでよく知られた脆弱性を探し、ファームウェアにパッチを適用し、マシン上で持続性を保ちます。

脅威名	コンテキスト
LuckyMouse（2020）[64]	**脅威の種類：**APTスパイ **手法：**署名されたコード **脅威の詳細：**接続先のC&Cサーバを受動的に待機するバックドア。ポート3389と443の2つの通信チャネルが可能。 **カーネルドライバの動作：**このドライバはペイロードを復号してメモリに注入します。また、RDP（Remote Desktop Protocol）ポート3389を通るトラフィックをフィルタリングし、トロイの木馬のC2通信を挿入します。
FK_Undead（2020）[65, 66]	**脅威の種類：**APTスパイ **手法：**署名されたコード **脅威の詳細：**少なくとも3種類のルートキットモジュールを含む、マルチステージスパイウェア脅威。 **カーネルドライバの動作：**このドライバはすべてのネットワークトラフィックを監視し（Webページにスクリプトを注入し）、ブラウザにプロキシを追加し、他のマルウ

[63] https://eclypsium.com/research/trickbot-now-offers-trickboot-persist-brick-profit/

[64] https://securelist.com/luckymouse-ndisproxy-driver/87914/

[65] https://lab52.io/blog/recent-fk-undead-rootkit-samples-found-in-the-wild/

[66] https://www.avertium.com/blog/fk_undead-malware-modules

	ェアドライバの読み込みを阻止し、そのレジストリを保護し、HOSTSファイルへのすべてのアクセスを監視して、svchost.exeがアクセスしようとするたびに悪意のあるバージョンのファイルを提供します。
Winnti（2020）[67]	**脅威の種類：**APTスパイ **手法：**署名されたコード **脅威の詳細：**iodineソースコードのカスタム実装を通したDNSトンネリング通信チャネルに依存し、盗んだデジタル証明書を使用してドライバをデジタル署名するバックドア。 **カーネルドライバの動作：**このドライバはネットワークに未加工のパケットを注入し、フォーマットされた特別なパケットを受け取ることができます。
Autochk（2019）[68]	**脅威の種類：**APTスパイ **手法：**署名されたドライバ **脅威の詳細：**外国大使館を標的とし、政府、防衛、およびテクノロジ分野のデータを収集する、中国を拠点とする脅威アクタ。 **カーネルドライバの動作：**このドライバは、正常なファイルをポイントするようにマルウェアファイルをリダイレクトします（セキュリティソリューションを回避するために）。また、C&Cサーバへのネットワーク接続も隠します。
Double Dragon（2019）[69, 70]	**脅威の種類：**APTスパイ **手法：**署名されたコード **脅威の詳細：**ゲーミング、医療、ハイテク、高等教育、電気通信、旅行サービスなどの業界を標的とする脅威アクタ。エクスプロイトを使用して被害者のマシンにアクセスし、侵害したシステムにバックドアをインストールします。 **カーネルドライバの動作：**このドライバはネットワークトラフィックを隠し、C&Cサーバと通信します。

[67] https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/

[68] https://repnz.github.io/posts/autochk-rootkit-analysis/

[69] https://content.fireeye.com/apt-41/rpt-apt41

[70] https://www.mandiant.com/resources/blog/game-over-detecting-and-stopping-an-apt41-operation

脅威名	コンテキスト
Scranos（2019）[71]	**脅威の種類：**情報窃取型マルウェア **手法：**署名されたコード **脅威の詳細：**ブラウザおよびユーザの決済アカウントからのログイン認証情報の窃取、ブラウザの履歴の持ち出し、Internet ExplorerへのJavaScript広告ウェアの注入などを目的とするスパイウェアキャンペーン。 この活動は、盗まれた可能性がある証明書でデジタル署名されたルートキットドライバを中心として行われています。 **カーネルドライバの動作：**このドライバはユーザモードプロセス内に不正なペイロードを注入します。また、DSEとPatchGuardを回避するために、感染したマシンにその他のコンポーネントもインストールします。
Zacinlo（2018）[72]	**脅威の種類：**広告詐欺 **手法：**署名されたコード **脅威の詳細：**オペレータに対して収益を生み出し、被害者のプライバシーを侵害する高度な広告ウェア。 **カーネルドライバの動作：**このカーネルドライバはそのユーザモードコンポーネントを保護します。また、その動作に影響する他のプロセスを停止する機能を持ち、SSL通信を傍受して復号し、悪意のあるスクリプトを注入するためのマンインザブラウザ機能をインストールします。

表 2：第 2 クラスタの脅威の一覧

[71] https://www.bitdefender.com/blog/labs/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/

[72] https://www.bitdefender.com/blog/labs/six-years-and-counting-inside-the-complex-zacinlo-ad-fraud-operation/

脅威名	コンテキスト
CosmicStrand（2022）[73]	**脅威の種類：**その他 **手法：**UEFI **脅威の詳細：**中国語を話す攻撃者によるものと考えられているUEFIファームウェアルートキット。その長い実行チェーンにより、悪意のあるコンポーネントがダウンロードされ、Windows内に導入されます。 **ブートドライバの動作：**このルートキットは、GigabyteまたはASUSマザーボードのファームウェアイメージに含まれます。C&Cサーバと通信するドライバを読み込むために、Windowsのブートマネージャにフックします。
MoonBounce（2022）[74, 75]	**脅威の種類：**APTスパイ **手法：**UEFI **脅威の詳細：**中東の政府機関内で発見された脅威活動。独自のUEFIブートキットを使用してそのドライバを読み込みます。このドライバはユーザモードプロセス内にペイロードを注入し、マルウェアのその他のステージをダウンロードします。 **ブートドライバの動作：**このUEFIファームウェアは、マルウェアの持続性と、オペレーティングシステムの読み込み後に実行される悪意のあるコードの導入のために使用されます。

脅威名	コンテキスト
HPファームウェアのシステムマネジメントモード（SMM）の脆弱性（2022）[76]	**脅威の種類：**その他 **手法：**UEFI **脅威の詳細：**これらのUEFIファームウェアの重度の脆弱性は、HPのノートPCおよびデスクトップに影響します。 **ブートドライバの動作：**これらのUEFIファームウェアの脆弱性を悪用することにより、ローカル権限をSMM権限に昇格させることができます。

[73] https://securelist.com/cosmicstrand-uefi-firmware-rootkit/106973/

[74] https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/

[75] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf

[76] https://www.sentinelone.com/labs/another-brick-in-the-wall-uncovering-smm-vulnerabilities-in-hp-firmware/

Lenovo UEFIファームウェアの脆弱性（2022）[77, 78]	**脅威の種類：**その他 **手法：**UEFI **脅威の詳細：**これらのLenovo UEFIファームウェアのバッファオーバーフローの脆弱性を悪用して、感染したシステムで権限を昇格させることができます。 **ブートドライバの動作：**これらの脆弱性は、セキュリティ関連の機能を無効にし、オペレーティングシステムの実行フローを乗っ取るための、任意のコードの実行を可能にします。
iLOBleed（2021）[79]	**脅威の種類：**APTワイパ **手法：**UEFI **脅威の詳細：**ファームウェアモジュールを改ざんし、感染したシステムから完全にデータを消去します。 **ブートドライバの動作：**この悪意のあるファームウェアは、DSEを無効にしてから署名されていないドライバを読み込みます。 このドライバはペイロードをユーザモードプロセスに注入します。
ESPecter（2021）[80]	**脅威の種類：**APTスパイ **手法：**UEFI **脅威の詳細：**このキャンペーンはDSEを回避して、不正な署名されていないドライバを読み込み、スパイ活動を実行します。 **ブートドライバの動作：**この悪意のあるファームウェアはWindowsブートマネージャにパッチを適用して、DSEを無効にし、署名されていないドライバを読み込みます。
FinSpy（2021）[81]	**脅威の種類：**APTスパイ **手法：**UEFI **脅威の詳細：**監視目的で使用されるスパイウェア。シングルステージインストーラを使用して拡散されます。 **ブートドライバの動作：**この悪意のあるUEFIは、メモリ内で元のUEFIを読み込み、パッチを適用します。パッチが適用されたUEFIは「PsCreateSystemThread」をフックし、次のステージを復号し、実行します。

[77] https://www.welivesecurity.com/2022/04/19/when-secure-isnt-secure-uefi-vulnerabilities-lenovo-consumer-laptops/

[78] https://thehackernews.com/2022/07/new-uefi-firmware-vulnerabilities.html

[79] https://threats.amnpardaz.com/en/2021/12/28/implant-arm-ilobleed-a/

[80] https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

[81] https://securelist.com/finspy-unseen-findings/104322/

脅威名	コンテキスト
MosaicRegressor（2020）[82]	**脅威の種類：**APTスパイ **手法：**UEFI **脅威の詳細：**このキャンペーンは、アフリカ、アジア、およびヨーロッパの外交官やNGOメンバーを標的としています。その目的はスパイ活動とデータ収集です。 **ブートドライバの動作：**このUEFIファームウェアは、持続性と、オペレーティングシステムの読み込み後に実行される悪意のあるコードの導入のために使用されます。
Lojax（2018）[83]	**脅威の種類：**APTスパイ **手法：**UEFI **脅威の詳細：**バックドアを使用して、バルカン半島および中欧と東欧の政府機関を標的とするキャンペーン。 **ブートドライバの動作：**この悪意のあるUEFI/BIOSは、正規のファイル*autochk.exe*のコピーを作成してから、悪意のあるユーザモードコンポーネントで置き換えます。
MyKings（2018）[84, 85]	**脅威の種類：**クリプトマイニング **手法：**MBR/VBR/IPL **脅威の詳細：**通常はクリプトマイナーやRATを配信するボットネットです。 **ブートドライバの動作：**このブートキットは検知を回避し、削除または軽減が難しい持続性を確立するために使用されます。これは、割り込み15hをフックし、そのシェルコードのためのスレッドをカーネル内に作成することにより行われます。このシェルコードは、何百ものウイルス対策製品で使用されているデバイス名を作成し、これらの読み込みを阻止します。
Platinum（2017）[86]	**脅威の種類：**APTスパイ **手法：**UEFI（Unified Extensible Firmware Interface） **脅威の詳細：**このキャンペーンは南アジアと東南アジアの被害者を標的とし、機密性の高い知的財産を盗むために、攻撃内でマルチステージマルウェアインフラストラクチャを使用します。

[82] https://securelist.com/mosaicregressor/98849/

[83] https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

[84] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-uncut-mykings-report.pdf

[85] https://www.zscaler.com/blogs/security-research/darkcloud-bootkit

[86] https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/?sort-by=newest-oldest&date=any

	ブートドライバの動作：Intel® AMT（Active Management Technology）のSOL（Serial-over-LAN）チャネルを通信に使用する、ファイル転送ツールを利用します。
rkloader（2015）[87]	**脅威の種類：**APTスパイ **手法：**UEFI **脅威の詳細：**この攻撃者はUEFI BIOSルートキットを使用して、ハードドライブのフォーマットやWindowsオペレーティングシステムの再インストールが実行されても、RCS（Remote Control System）エージェントが感染したシステムにとどまれるようにします。 **ブートドライバの動作：**このUEFI BIOSルートキットは持続性のために使用されます。

表 3：第 3 クラスタの脅威の一覧

[87] https://www.zdnet.com/article/hacking-team-stealthy-spyware-rootkit-stays-entrenched-through-hard-disk-removal/

第 1 クラスタの脅威はまだ存在するのか

歴史的には、第 1 クラスタの脅威が数では最も優勢でした。ソフトウェアスタック全体のあらゆる種類のサードパーティ Windows カーネルドライバで攻撃者が新たな脆弱性を見つけることが可能なため、BYOVD が一般的に使用されています。このクラスタは、カスタムの悪意のあるコードを Windows カーネルにピギーバックするため、またはセキュリティ機能を無効にし、KMCS により他のモジュールがカーネルに読み込まれることを阻止するために使用できます。

Microsoft は、毎月同社のテレメトリで約 100 万件のドライバハッシュを確認していると述べています。これらのドライバには脆弱性がいくつでも含まれる可能性があります。またそれ以外にも、攻撃者はこれらのドライバに悪意のあるカーネルモードコードを埋め込むことができます。OEM（Original Equipment Manufacturer）およびサードパーティドライバでは、最小限のリバースエンジニアリング作業でゼロデイ脆弱性を簡単に見つけることができます。Microsoft、Intel、NVIDIA などの最大手のソフトウェアベンダからのカーネルドライバモジュールでも脆弱性が見つかっています。

攻撃者の観点から見たこのクラスタのメリットは、少数のプリミティブだけで権限を昇格できるという点です。被害者側から見ると、脆弱なドライバに対する下位互換性が必要なため、第 1 クラスタの脅威の防止と検知は困難なことがあります。このようなドライバをブロックすると、システムのブートプロセスに影響する脆弱なブートドライバが悪用されている場合、システムの起動に影響する可能性があります。ただし、これらの脅威は代償も伴います。見つかったプリミティブによっては、異なるオペレーティングシステムバージョンで互換性や安定性の問題があることがわかっています。

Microsoft のドキュメントによると、カーネルの管理者、またはカーネルへのアクセスを取得するために管理者権限を必要とするカーネルドライバの悪用は、セキュリティ境界ではありません[88]。つまり Microsoft の観点では、カーネル境界は、カーネル空間から分離された非管理者プロセスと定義されます。脆弱なカーネルドライバを悪用することにより、非管理者ユーザプロセスがこの境界を侵害することが可能になります。

また、脆弱なドライバにより、デバイスインタフェースがシステムや管理者ユーザアカウントに対して制限されながら、汎用インタフェースが露呈されている場合もあります。つまり、この脆弱なドライバにより、管理者はそのドライバのインタフェースとのみ通信することが可能になります。

Microsoft および相当数のベンダは、このこと自体を脆弱性とは見ていませんが、攻撃者はこの機能を悪用し、保護されているセキュリティエージェントを改ざんして防御を阻害する、

[88] https://www.microsoft.com/en-us/msrc/windows-security-servicing-criteria

悪意のあるカーネルモジュールを読み込むことができます。これにより、セキュリティソリューションは重要なカーネルコードがこの経路で悪意のあるコードによって操作されないように、改ざん防止手法に頼らざるを得なくなります。

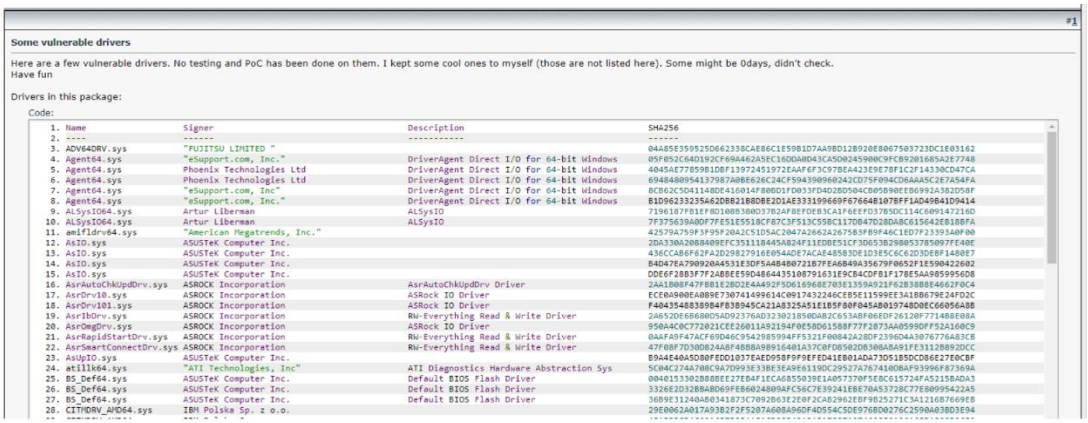
ランサムウェアオペレータが露呈されている汎用インタフェースを悪用している例として、DoppelPaymer での AV サービスをキルするための Process Hacker カーネルドライバの使用が挙げられます。DoppelPaymer の例は、この種のカーネルドライバを使用して AV/EDR 機能を無効化するという大きなトレンドの一部です[89]。

Microsoft はこのクラスタの脅威の増加に反応し、脆弱なドライバのブロックリストを維持することで軽減を図っています[90]。このブロックリストは、VBS ベースのテクノロジである HCVI トラストレットを使用している新しい Windows のバージョンで、コアコンポーネントにより適用されます。これにより脆弱なドライバの寿命が劇的に短縮され、HCVI により適用されるブロックリストの迂回が非常に困難になります。

図 19：Microsoft が HVCI VBS テクノロジを使用して脆弱なカーネルドライバのブロックリストを適用

トレンドマイクロのソリューションでは、攻撃者による使用が確認されているすべての脆弱なドライバ、およびサイバーセキュリティコミュニティにより公開されているドライバを積極的に監視しています。図 20 は、一部のゲームハッキングフォーラムで共有されている一般的な脆弱なドライバの例を示しています。このような脆弱なドライバは、脅威アクタがカーネルに足掛かりを得るために攻撃内で悪用するため、セキュリティリスクとなり得ます。

[89] https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/
[90] https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules



Some vulnerable drivers

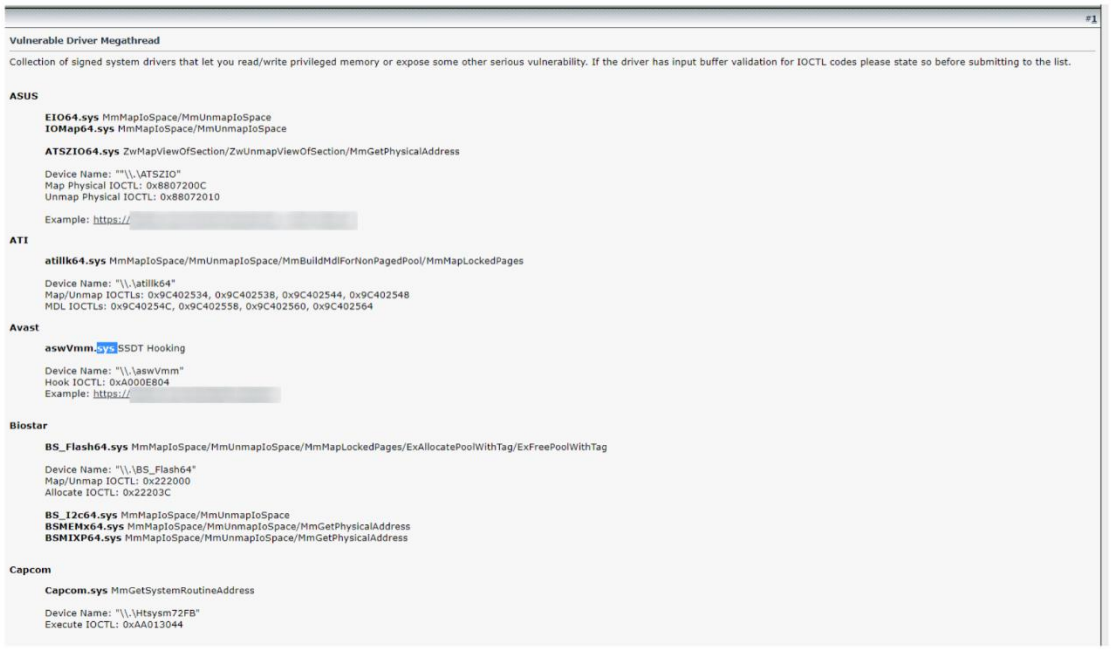
Here are a few vulnerable drivers. No testing and PoC has been done on them. I kept some cool ones to myself (those are not listed here). Some might be 0days, didn't check.
Have fun

Drivers in this package:

Code:

Name	Signer	Description	SHA256
ADV64DRV.sys	"FUJITSU LIMITED "		04A85E359525D66233BCAE86C1E59B1D7AA9BD12B920E8067503723DC1E03162
Agent64.sys	"eSupport.com, Inc."	DriverAgent Direct I/O for 64-bit Windows	05F852C64D192CF69A462A5EC1BDDA0D43CA5D0245900C9FCB9201685A2E7748
Agent64.sys	Phoenix Technologies Ltd	DriverAgent Direct I/O for 64-bit Windows	4045AE77859B1DBF13972451972EAAF6F3C97BEA423E9E78F1C2F14330CD47CA
Agent64.sys	Phoenix Technologies Ltd	DriverAgent Direct I/O for 64-bit Windows	6948480954137987A0BE626C24CF59439096024 2CD75F094CD6AAA5C2E7A54FA
Agent64.sys	"eSupport.com, Inc"	DriverAgent Direct I/O for 64-bit Windows	8CB62C5D41148DE416014F80DD1FD033FD4D2BD504CB0589 0EEB6992A382D58F
Agent64.sys	"eSupport.com, Inc."	DriverAgent Direct I/O for 64-bit Windows	B1D9623323 5A62DB2188DBE2D1AE3331996 9F67664B107BFF1AD4964 1D9414
ALSysIO64.sys	Artur Liberman	ALSysIO	7196187FB1EF8D1088 38D37B2AF8EFDEB3CA1F6EEFD37B5DC114C6091472 16D
ALSysIO64.sys	Artur Liberman	ALSysIO	7F375639A0DF7FE51E5518CF87C3F513C55BC117DB47D28DA8C615642EB188FA
amifldrv64.sys	"American Megatrends, Inc."		42579A759F3F95F20A2C51D5AC2047A2662A2675B3FB9F46C1ED7F23393A0F00
AsIO.sys	ASUSTeK Computer Inc.		2DA330A208B409EFC351118445AB24F11EDBE51CF3D653B29B053785097FE40E
AsIO.sys	ASUSTeK Computer Inc.		436CCA86F62FA2D29827916E054ADE7ACAE485B3DE1D3E5C6C62D3DE8F1480E7
AsIO.sys	ASUSTeK Computer Inc.		B4D47EA790920A4531E3DF5A4B4B0721B7FEA6B49A35679F0652F1E590422602
AsIO.sys	ASUSTeK Computer Inc.		DDE6F28B3F7F2ABBEE59D4864435108791631E9CB4CDFB1F178E5AA9859956DB
AsrAutoChkUpdDrv.sys	ASROCK Incorporation	AsrAutoChkUpdDrv Driver	2AA1B08F47FBB1E2BD2E4A492F5D6169685E703E13594921F628388E4662F0C4
AsrDrv10.sys	ASROCK Incorporation	ASRock IO Driver	ECE0A900EA0B9E73074149961 4C0917432246CEB5E11599EE3A1BB679E24FD2C
AsrDrv101.sys	ASROCK Incorporation	ASRock IO Driver	F4043546B3B9B4FB3B945CA21A8325451E1B5F80F045AB01974BD0EC66056A8B
AsrIbDrv.sys	ASROCK Incorporation	RW-Everything Read & Write Driver	2A652DE6B6B0C5AD92376AD323021850DAB2C653ABF06E0F26120F7714B8E08A
AsrOmgDrv.sys	ASROCK Incorporation	ASRock IO Driver	950A4C0C772021CEE26013A82194F0E5BD6158BF77F2873AA05990FF52A160C9
AsrRapidStartDrv.sys	ASROCK Incorporation	RW-Everything Read & Write Driver	0AAFA9F47ACF69D46C954298599 4FF5321F00842A28DF2396D4A3076776A83CB
AsrSmartConnectDrv.sys	ASROCK Incorporation	RW-Everything Read & Write Driver	47F08F7D30D824A8F4B88A9B916401A37C0FDB502DB308ABA91FE31128B92DCC
AsUpIO.sys	ASUSTeK Computer Inc.		B9A4E40A5D80FE0D1037EAED958F9F0EFED411E801ADA73D5185DCD86627E0CBF
atillk64.sys	"ATI Technologies, Inc"	ATI Diagnostics Hardware Abstraction Sys	5C04C274A708C9A7D993E338E3EA9E6190C29527A767410BAF93996F873694
BS_Def64.sys	ASUSTeK Computer Inc.	Default BIOS Flash Driver	0040153302B88BEE27EB4F1ECA6855039E1A057370F5E8C615724FA5215BADA3
BS_Def64.sys	ASUSTeK Computer Inc.	Default BIOS Flash Driver	3326E2D328BABD69FEB6024809AFC56C7E39241EBE70A53728C77E8099542245
BS_Def64.sys	ASUSTeK Computer Inc.	Default BIOS Flash Driver	3689E31240AB0341873C7092B63E2E0F2CAB2962E8F9B25271C3A1216B7669E8
CITHDRV_AMD64.sys	IBM Polska Sp. z o.o.		29E0062A017A938 2F2F5207460A960F4D554C5DE976B0D276C2590A03BD3E94

図 20：ゲームハッキングフォーラムで公開されている脆弱なカーネルドライバの情報



Vulnerable Driver Megathread

Collection of signed system drivers that let you read/write privileged memory or expose some other serious vulnerability. If the driver has input buffer validation for IOCTL codes please state so before submitting to the list.

ASUS

EIO64.sys MmMapIoSpace/MmUnmapIoSpace
IOMap64.sys MmMapIoSpace/MmUnmapIoSpace

ATSZIO64.sys ZwMapViewOfSection/ZwUnmapViewOfSection/MmGetPhysicalAddress

Device Name: "\\.\ATSZIO"
Map Physical IOCTL: 0x8807200C
Unmap Physical IOCTL: 0x88072010

Example: https://

ATI

atillk64.sys MmMapIoSpace/MmUnmapIoSpace/MmBuildMdlForNonPagedPool/MmMapLockedPages

Device Name: "\\.\atillk64"
Map/Unmap IOCTLs: 0x9C402534, 0x9C402538, 0x9C402544, 0x9C402548
MDL IOCTLs: 0x9C40254C, 0x9C402558, 0x9C402560, 0x9C402564

Avast

aswVmm.sys SSDT Hooking

Device Name: "\\.\aswVmm"
Hook IOCTL: 0xA000E804
Example: https://

Biostar

BS_Flash64.sys MmMapIoSpace/MmUnmapIoSpace/MmMapLockedPages/ExAllocatePoolWithTag/ExFreePoolWithTag

Device Name: "\\.\BS_Flash64"
Map/Unmap IOCTL: 0x222000
Allocate IOCTL: 0x22203C

BS_I2c64.sys MmMapIoSpace/MmUnmapIoSpace
BSMEMx64.sys MmMapIoSpace/MmUnmapIoSpace/MmGetPhysicalAddress
BSMIXP64.sys MmMapIoSpace/MmUnmapIoSpace/MmGetPhysicalAddress

Capcom

Capcom.sys MmGetSystemRoutineAddress

Device Name: "\\.\Htsysm72FB"
Execute IOCTL: 0xAA013044

図 21：ベンダごとの脆弱なカーネルドライバのリスト

前述のように、脆弱なカーネルドライバを利用する複数のエクスプロイト手法を軽減可能な仮想化ベースのセキュリティ（VBS）機能の導入の増加により、このクラスタは時間とともに減少すると予想されます[91]。また、カーネルドライバの開発プロセスでの VBS テクノロジに対応した厳格なルールの実施によっても、特定のバグクラスを排除できます。サードパーティのセキュリティベンダが、VBS で使用されている Microsoft のネイティブのハイパーバイザーに似た、独自のカスタムハイパーバイザーを導入する場合もあります。これにより、第 1 クラスタの脅威に対してより適切な保護を提供するようにセキュリティソリューションを強化できます。

[91] https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

第 2 クラスタの APT のケーススタディ

「成熟した攻撃者が KMCS に適応した方法」セクションで解説したように、第 2 クラスタの攻撃は、Microsoft のコード署名要件に準拠しています。これにより、攻撃者は特定のタスク用に設計されたカーネルモジュールを作成し、現在の Microsoft のカーネルモジュールの署名ルールに基づいて、カスタマイズしたドライバで署名するという柔軟性が得られます。このクラスタでは、攻撃者は以下のいずれかのアプローチを使用できます。

1. 流出した、侵害された環境から盗まれた、またはアンダーグラウンド市場で購入したコード署名証明書を使用する。
2. 正規の組織を偽装して新しい有効なコード署名証明書を取得し、Microsoft のクロス署名証明書を取得するプロセスに従い（Microsoft でカーネルモードコードのクロス署名がまだ許可されていた時代）、署名されたカーネルモジュールを発行する Microsoft のポータルを悪用し、実際のアイデンティティに結び付いている有効なコード署名証明書や EV（Extended Validation）証明書をアンダーグラウンド市場で購入する。

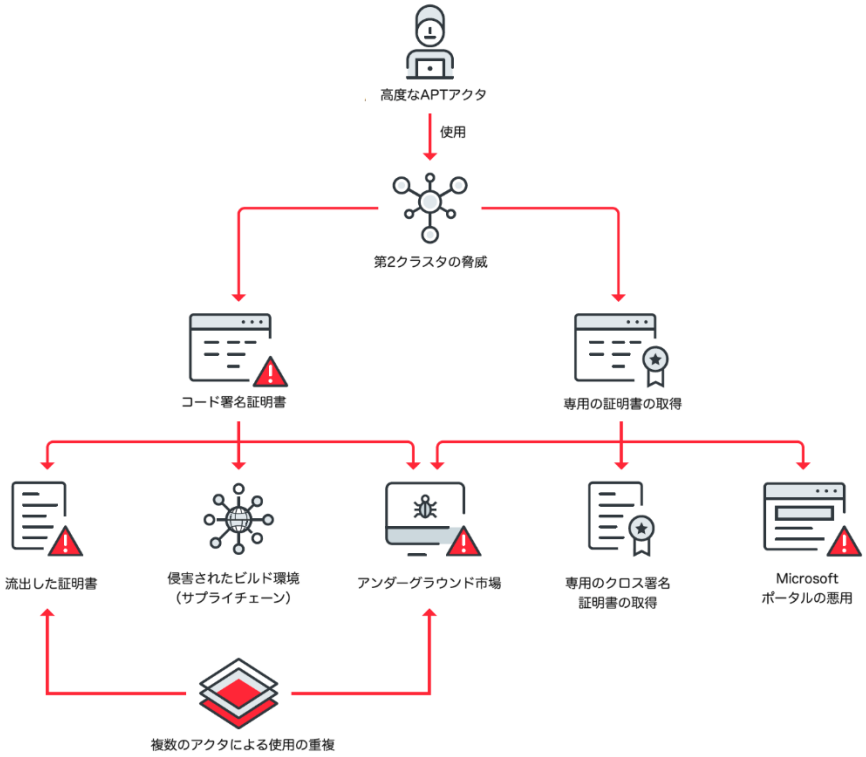


図 22：第 2 クラスタの脅威の起動時に攻撃者が使用できる 2 つのアプローチを示す図

コード署名証明書を使用する APT

過去のデータとインテリジェンスフィードのトレンドマイクロでの分析に基づくと、Earth Baku または APT41 は、キャンペーンで使用しているマルウェアに署名するためにコード署

名証明書を日常的に使用しているアクタの 1 つです。このアクタが使用しているデジタル署名の大半は、ゲーム開発スタジオから盗まれた、失効していない有効なデジタル証明書でした。アンダーグラウンド市場に投稿された広告によると、有効なデジタル証明書でファイルを署名すると、ペイロードのインストールの成功率は 50%向上します。トレンドマイクロは、ユーザ空間またはカーネル空間でマルウェア武器庫を署名することを Earth Baku が選択した理由として、以下の目的を把握しています。

- KMCS を使用している環境にカーネルモジュールを読み込む
- 標的とするシステムとの親和性を確保し、検知を回避する
- 不正なペイロードが検知される可能性を大幅に減らし、検知された場合でも極力疑われないようにする
- 自動スキャンを実行するセキュリティソリューションを回避し、署名されていないコードを制限する Windows のグループポリシーを迂回する

盗まれたコード署名証明書

第 2 クラスタの最初のアプローチでは、新たな証明書の購入が不要であり、匿名性が向上するという 2 つのメリットが得られます。攻撃者は自分でコード署名証明書を購入する代わりに、他人のコード署名証明書を使用します。また、以前の調査から、期限が切れたか失効された証明書でカーネルドライバが署名されていても、Windows カーネルドライバローダで読み込まれることがわかっています。このような証明書のいくつかが、特にゲーミングフォーラムなどですでに公開されています。さらに、GrayhatWarfare などのオンラインスキャナサービスを使用して、.pfx や.p12 などの特定のファイル拡張子を持つ秘密鍵の有無をスキャン可能な、いくつかの露呈された Amazon S3（Simple Storage Service）バケットも確認しました[92]。これもいずれは悪用される可能性があります。

高度な脅威アクタは、コード署名機能を獲得するために、以下の 2 つのアプローチを使用している可能性が非常に高いでしょう。

- ソフトウェアベンダを直接標的とする
    - 実際の証明書を盗むことなく、悪意のあるコードが署名されるように、ビルドシステムを標的とする（サプライチェーン侵害）
- ビルドシステムからコード署名証明書を盗む
    - アンダーグラウンド市場のサービスや公開されている流出した証明書を使用する

サプライチェーン攻撃中に、攻撃者はソフトウェアベンダのビルド環境を侵害して、コンパイルされる前に署名された悪意のあるコードを注入できます。

[92] https://buckets.grayhatwarfare.com/

トレンドマイクロの調査では、このアプローチを使用して署名されたユーザモードアプリケーションのみが見つかっています。また、高度なサイバー犯罪グループ APT41 が、不正なアップデートを正規の証明書で署名していることも確認しています。この場合、侵害された組織により、すべてのアップデートが署名されることが求められていました。つまり、APT41 はコード署名証明書を使用してアップデートメカニズムを無効にする必要がありました。トレンドマイクロの分析により、APT41 が悪意のあるコードをコンパイル前にパッケージに注入して、コード署名証明書を盗む必要性を回避し、その後パッケージを自身でコンパイルしたことが明らかになっています。

土台となるビルド環境が侵害されていれば、この同じアプローチをカーネルモードのコードの署名に使用することも理論的に可能ですが、トレンドマイクロの分析ではカーネルモジュールは見つかりませんでした。

2018 年のビデオゲーム業界を標的とした APT41 の攻撃では、このグループは同じアプローチを使用し、制作環境にアクセスして、正規のビデオゲームファイルに悪意のあるコードを注入することによって、マルウェアを拡散させました。これらのファイルは有効なコード署名証明書で署名され、エンドユーザに広く配布されました。これは、APT41 が被害者の制作環境にアクセスできたことを示している可能性が高く、これによりサプライチェーン侵害および侵害された同じ組織からの正規のデジタル証明書を使用した悪意のあるファイルの署名が促進されました。このグループによるサプライチェーン侵害の独特の使用法および侵害されたコード署名証明書の一貫した使用は、この脅威アクタがどれだけ創造的で十分なリソースを備えているかを示しています。

APT41 は、ビデオゲームスタジオから盗んだデジタル証明書を使用して、不正なカーネルドライバを含むマルウェアコンポーネントを署名していることが知られています。このグループは、少なくとも 19 の盗まれたコード署名証明書を悪用したことが以前報告されています。

盗まれた正規のコード署名証明書を使用した脅威を軽減する際の問題は、流出したか盗まれたコード署名証明書で署名されたすべての実行可能ファイルを完全にブロックすることは難しいという点です。これは、このような証明書は何年も前に公開され、その有効期間の間に複数の正規のモジュールを署名するために使用されている可能性が高いためです。

盗まれた証明書を全面的にブロックする戦略は実用的な解決策ではないため、流出した証明書で署名されている不正なドライバの大半は、ほとんどのウイルス対策ソリューションでは扱われていません。また、侵害されたデジタル証明書を失効させる責任は証明機関にあります。このため、対応時間は場合によって異なり、悪用されたことが最初に特定されてから長期間経っても、デジタル証明書が悪用され続けていることもあります。これらのコード署名証明書の期限が切れるか失効されても、引き続きカーネルモジュールの署名活動では使用可能です。

盗まれた証明書の重複した使用

ソフトウェアベンダと証明機関との間の信頼関係を悪用することで、攻撃者は組織のインフラストラクチャを侵害して、コード署名証明書にアクセスして盗むことにより、秘密鍵を窃取できます。

たとえば、APT41 はあるゲームパブリッシャからのコード署名証明書を、別のゲーミング業界の企業に対して使用しています。侵害された同じ組織からの別のデジタル証明書が、中国を拠点とするサイバースパイグループなどの複数の他の APT オペレータによって使用されています。

これは、盗まれた証明書が重複して使用されており、さまざまな脅威アクタが互いに証明書を共有していることを示しています。

暗号通貨マイナーを配布するさまざまなサイバー犯罪グループで使用されている、盗まれたコード署名証明書に関連する別のパターンも確認しています。FiveSys ルートキットや Purple Fox マルウェアの背後にいる攻撃者が、盗んだ署名情報を使用して、互いを特定してブロックしています[93]。

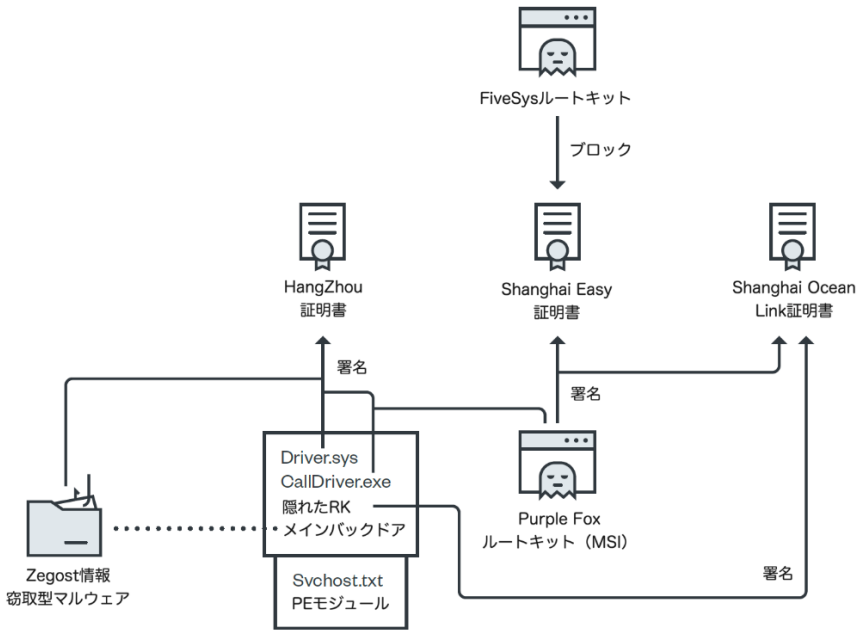


図 23：FiveSys のオペレータが Purple Fox のオペレータにより使用されている盗まれたコード署名証明書をブロック

出典：Trend Micro Research, News, and Perspectives[94]

[93] https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf

[94] https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html

図 24：FiveSys のルートキットのブロックリストには Purple Fox のオペレータにより使用されている Shanghai easy kradar のコード署名証明書が含まれている
出典：Trend Micro Research, News, and Perspectives[95]

新しいコード署名証明書または有効な署名の取得

このクラスタの 2 つ目のアプローチでは、攻撃者がリソース開発フェーズの一環としてコード署名証明書を自ら取得します（T1587.002）。一般的にキャンペーンでこのアプローチを使用しているのは、この複雑なプロセスを利用する資金がある国家支援の脅威アクタです。

この 2 つ目のアプローチの例として、2021 年に攻撃者が Windows ハードウェア互換性プログラム（WHCP）ポータルを介して認定を受けるために不正なサードパーティ製のドライバを提出したケースが挙げられます[96]。2022 年 12 月には、攻撃者がどのように WHCP を悪用して不正なドライバに署名し、エンドポイント上の EDR エージェントをキルしたかに関するレポートを Mandiant が公開しています[97]。

このアプローチは、他の手法と比べて比較的高いコストを伴います。専用のコード署名証明書の購入は、標的型攻撃やレッドチーム演習では良い選択肢となります。しかし、証明書は証明機関（CA）により完全に失効されることがあり、また購入者は自身の身元を明かす必要があるため、コード署名証明書の購入は絶対安全な手段ではありません。

図 25 は、カーネルモジュールを署名して読み込むための、Microsoft による要件の進化を示しています。オペレーティングシステムのマイルストーンとなったのが Windows 10 のリリ

[95] https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html
[96] https://msrc.microsoft.com/blog/2021/06/investigating-and-mitigating-malicious-drivers/
[97] https://www.mandiant.com/m-trends

ースです。このバージョンからクロス署名証明書の使用が廃止され、このような証明書を低レベル攻撃に使用してきた攻撃者に大きな影響が及びました。取得した証明書は Microsoft が信頼している CA によりクロス署名されているため、攻撃者がカーネルコードを改ざんすることはできなくなり、また Microsoft は提出された身元を信用することができます。

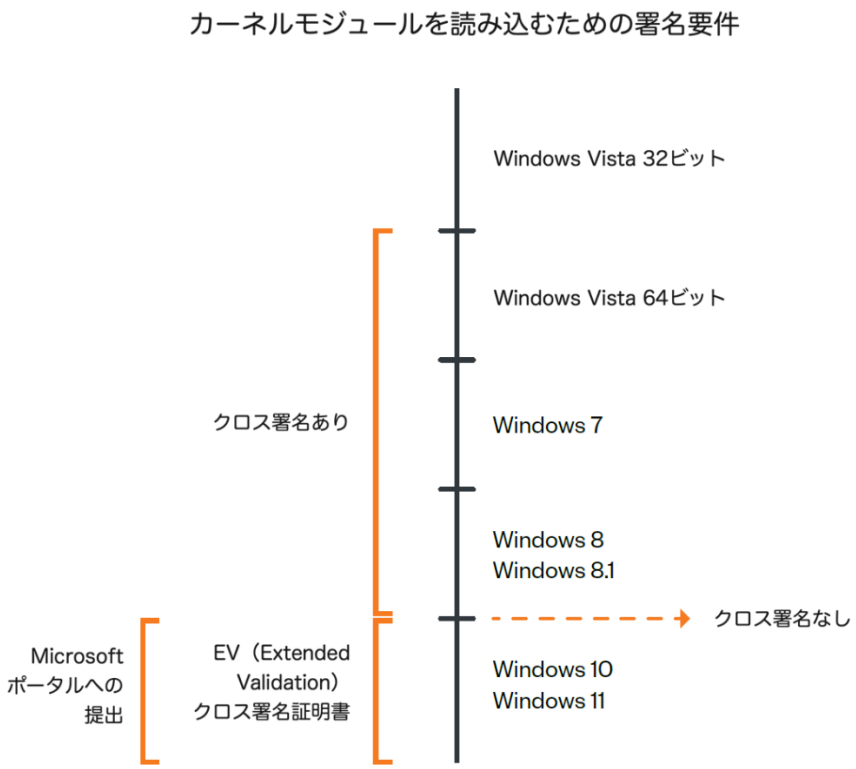


図 25：Microsoft によるカーネルコードの署名要件

オペレーティングシステム	署名要件
Windows XP	なし
Windows Vista 32ビット	なし
Windows Vista 64ビット	MCVR（Microsoft Code Verification Root）証明書とSHA-1
Windows 7	MCVRと（SHA 1またはKB3033929）とSHA-2
Windows 8、8.1	MCVRとSHA-256
Windows 10、11	MCVR、SHA-256、ポータル

表 4：Windows のカーネルコード署名条件

要件	説明
MCVR	上の表では、MCVRは、カーネルモジュールの署名の信頼のチェーンが、Microsoft Code Verification Root証明書またはカーネルが信頼するその他の証明書につながっている必要があることを意味します。**WHQL**プロセスを経由している署名は、この要件をすでに満たしています。これは、カーネルが信頼されたルート証明機関のリストにはアクセスできないことを意味します。**この要件を満たすには、通常はクロス署名証明書が必要です。**
ポータル	Microsoftは2015年4月1日に、すべての新しいWindows 10のカーネルモードドライバは、**Windowsハードウェアデベロッパーセンターダッシュボードポータル**に提出してデジタル署名を受ける必要があることを発表しました。下位互換性のために、Windows 10では、特定の条件下では古い証明書からの署名でカーネルモードドライバを引き続き使用できますが、これには古い証明書が必要であるため、実用的ではありません。**このポータルでは、すでにEV証明書で署名されているドライバの提出のみを受け付けます。**EV証明書は一般的に通常の証明書よりも高価です。
SHA-1	署名が存在する必要があり、SHA-256を使用していてはなりません。これはカーネルドライバ自体の署名、および証明書に対する信頼のチェーンを保護する署名にも当てはまります。
SHA-256	SHA-1は、いずれはWindowsで信頼されるハッシュではなくなります。Windowsでは、ファイルダイジェスト、メインの証明書、タイムスタンプダイジェスト、タイムスタンプ証明書など、すべてにSHA-256（またはそれ以降）が使用されるようになります。

表 5：各カーネルコード署名要件の説明

すべてのカーネルドライバモジュールをポータルに提出することを求めることにより、Microsoft はカーネルに読み込まれるコードの品質を保証しようとしていることを証明しています。すべての要件が満たされている場合にのみ、署名が追加されます。この目的で、ポータルへの提出のために、追加の EV コード署名証明書が必要になります。EV コード署名証明書は高価であり、コピーするのが難しい USB ハードウェアトークンが付属しているため、このプロセスを悪用しようとしている攻撃者にとって、プロセスを複雑にします。

アンダーグラウンド市場（サービスとしての証明書：Certificate-as-a-Service）

EV 証明書は特に、攻撃者が最近の Windows リリースに不正なカーネルモジュールを読み込み、大半のセキュリティソリューションを回避するために使用できるため、アンダーグラウンド市場で人気のある商品となっています。これにより、脅威アクタは正規に署名されたカーネルモジュールを含む、より大規模な攻撃の実行が可能になります。

このセクションでは、アンダーグラウンド市場での EV 証明書の販売を専門とする犯罪者の例を紹介します。この犯罪者は、デジタルセキュリティ企業の DigiCert および Sectigo により発行された EV コード署名証明書を販売しており、カスタムのパブリッシャ名で発行された証明書もさらに高い価格で販売できるとしています。この報告書の執筆時点では、この犯罪者はアンダーグラウンドフォーラムで複数の肯定的なレビューを含む良い評価を得ています。この犯罪者は証明機関から証明書を取得するために、偽の会社情報または実際の会社から盗んだ情報を使用した可能性が高いでしょう。

HermeticWiper は、コード署名証明書を取得するために正規の会社データの使用が確認されている最近の脅威の例です[98, 99]。このマルウェアは、ビデオゲーム設計を専門とする小規模ビジネスである Hermetica Digital のデジタル証明書を使用して署名されています。同社は、この攻撃には無関係であり、デジタル証明書を申請したこともなく、証明書が発行されていたことも知らなかったと報告しています。

この犯罪者は、EV 証明書を USB トークンにコピーして顧客に発送するとしています。一部の犯罪者の主張によると、カスタムの会社名で発行されたコード署名証明書の価格は 15,000 米ドルです。犯罪者は、これらの証明書の有効期間は使用方法によって異なるとも主張しています。証明書によっては 1 週間から 1 年有効なものまであります。


We are selling EV code-signing certificates available in stock or have them issued to order.
EV Code Signing Certificate for sale.
Here's a Telegram channel where we will publish information on available certificates. Join it.
Created a channel where information on the sale of certificates will be published. Follow.
https:/
Item and cost
EV Code Signing certificate: USD 4,000 and up (it takes 2 to 4 weeks to get one issued)
EV Code Signing Certificate - from $ 4000 (production time 2-4 weeks)
Having the certificate put on our USB Token and delivered within Russia costs USD 350.
* Get a USD 50 discount for a review.
* EV certificates require a physical USB token.
* 50 $ discount per review
* EV certificates require a physical USB token.
Tokens that are suitable for EV certificates:
USB tokens for EV certificate:
SafeNet eToken 5100
SafeNet eToken 5105
SafeNet eToken 5110
SafeNet eToken 5200
SafeNet eToken 5205
SafeNet eToken PRO 72K
SafeNet eToken Pro Anywhere
iKey 4000
A certificate can be issued in a specific company name. The conditions are negotiated on a case-by-case basis.
Registration of code signing certificates for a specific company name is possible, conditions are discussed individually.
Contact details
Telegram: @
(Add a message with the username to your 'Favorites' and follow the link. Thus, you will be able to avoid fake accounts.)
Jabber: provided on request
Contact us; we'll be glad to cooperate with you!
We will be glad to cooperation!
What is a certificate for?
EV Code Signing certificates are specialized digital certificates that can be used to sign software, various scripts, applications, macros, etc in order to avoid copyright issues.
- [The certificates are used] for executable x86/x64 files (.exe, .cab, .dll, .msi)
- for drivers, including the ones for Windows 10
- for VBA macros and JavaScript scripts

図 26：EV 証明書を販売するアンダーグラウンド市場の投稿

[98] https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/

[99] https://www.reuters.com/world/europe/cyprus-games-writer-denies-links-malware-found-before-russian-invasion-2022-02-24/

アンダーグラウンド市場から EV 証明書を購入する以外にも、攻撃者は保護されていないハードウェアトークンを悪用して EV 証明書を取得し、会社のアイデンティティを偽装し、その証明書を攻撃で使用しています。

アンダーグラウンドフォーラムおよびチャネルで販売されている関連サービスを分析することにより、

一般的な大半のサービスはコード署名証明書および EV 証明書を販売していることがわかりました。

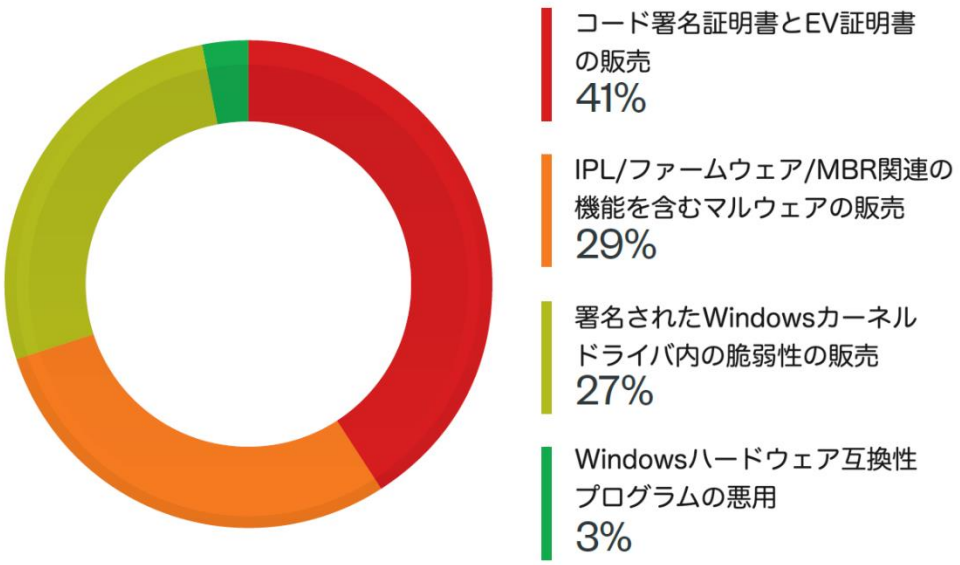


図 27：アンダーグラウンドフォーラムおよびチャネルで販売されている関連サービスの分析

まとめと今後の予測

この 7 年間にわたり Windows カーネルの信頼モデルに影響を及ぼしてきた主要な脅威の分析から、低レベルのコンポーネントを使用する脅威が完全に消滅するのではなく、進化していることが明らかになりました。このような脅威の変容は、最新の Windows カーネルに組み込まれた、新しい革新的なセキュリティメカニズムにより主に誘発されています。このようなテクノロジの進歩にもかかわらず、トレンドマイクロの分析によると、未だに何かが 1 つ回避されるだけで、ソフトウェアスタック全体が侵害されます。したがって、オペレーティングシステムとともに常に進化している新しい脅威の検知と阻止に関して、これらの組み込みテクノロジは完ぺきではないことを理解することが重要です。

成熟した高度な脅威アクタは、今も Windows オペレーティングシステムへの高特権アクセスを精力的に追求しています。またこれらの攻撃者は、ユーザのデスクトップまたはサーバでのエンドポイント保護プラットフォーム（EPP）やエンドポイントでの検知と対応（EDR）テクノロジによるユーザ空間プロセスの保護の強化に対抗するための手法を使用しています。このように保護レイヤが追加されていることから、攻撃者は最も抵抗の少ない経路を選択する傾向があり、カーネルレベルまたはさらに下のレベルから悪意のあるコードを実行しています。このため、トレンドマイクロでは、このような脅威は当分、脅威アクタのツールキットから消えることはないと考えています。

公開されているカーネル脅威を 3 つの主なクラスタに分類して分析した結果、特定のクラスタは将来的には廃れる可能性が高いことがわかりました。一方、攻撃者はセキュリティ機能を回避するために最初の感染ポイントを防御メカニズムの 1 つ下のソフトウェアスタックへと移行しているため、その他のクラスタはやがて増加すると考えられます。

攻撃者は、セキュリティツールから悪意のあるコードを隠し、セキュリティ防御を阻害し、長期間検知を回避するために、ルートキットを使用し続けるでしょう。ルートキットは主に、低レベルシステムのコンポーネントをリバースエンジニアリングするスキル、およびこのようなツールを開発するために必要なリソースを備えた、高い技能を備えたグループにより主に使用され続けると予想されます。このようなグループは、ダーク Web でルートキットを購入するか、ルートキットを構築するためのコード署名証明書を購入するために十分な資金を持っています。つまり、このような種類のルートキットを使用する攻撃の主な危険は、キルチェーンの早い段階で使用される、複雑な標的型攻撃を隠せる能力にあります。これにより、被害者の環境で実際のペイロードが起動する前に、防御機能が阻害されます。

TREND MICRO

〒151-0053

東京都渋谷区代々木 2-1-1　新宿マインズタワー

大代表 TEL：03-5334-3600 FAX：03-5334-4008

http://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。