Case Study

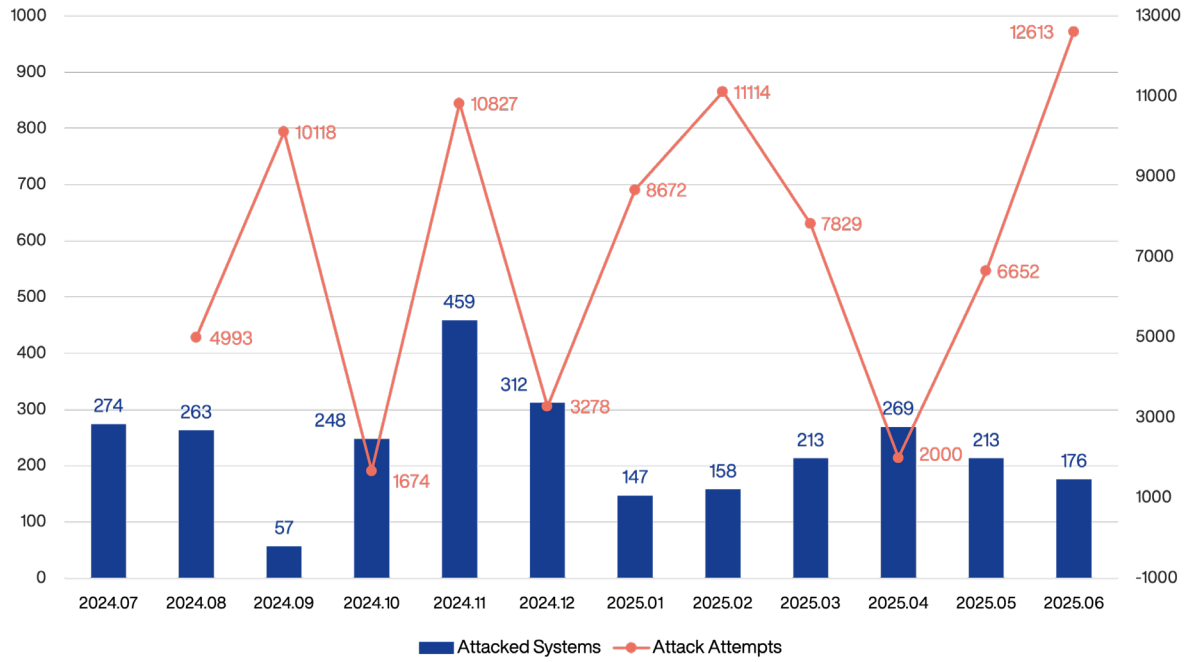
事例で見る Linux 攻撃 何から始めるべきか？

近年、Linux サーバーへの攻撃による被害が拡大している。攻撃者が Linux サーバーを狙う理由は、数多くのクライアント PC に接続されており、様々なビジネス重要データが保存されているためだ。ランサムウェアを始め、Linux ベースのシステムを狙ったマルウェアが増加することで、ビジネスの中断など深刻な被害へと繋がっている。今や企業は、自社の重要資産や顧客情報を取り扱う Linux サーバーを最優先事項に置き、セキュリティを適用する必要がある。

AhnLab は、アンチウイルス(V3 Net for Linux)、サンドボックス(AhnLab MDS)、EDR(AhnLab EDR) ソリューションを連携させたセキュリティアーキテクチャを通じて Linux を含むエンドポイント全区間に対して強力なセキュリティを提供してきている。このアーキテクチャは多くの顧客に実際に導入され、セキュリティ強化に寄与しており、構成ソリューションはグローバルセキュリティ評価で優秀な成績を収めながら卓越した技術力を証明している。

1. 統計で見る Linux サーバー攻撃

AhnLab の脅威インテリジェンス組織である ASEC(AhnLab SEcurity intelligence Center は、ハニーポットを活用して不適切に管理されている Linux SSH(Secure Shell) サーバーを対象とした総当たり(Brute Forcing)、辞書攻撃(Dictionary Attack) などを検知および分類し、統計を提供している。ここで不適切に管理されているとは、攻撃に脆弱なアカウント情報が設定されている環境を意味する。



[図1] 2025年6月基準、1年間の Linux サーバー攻撃統計

[図1] は2025年6月を基準に過去1年間、Linux サーバーを対象に感行された攻撃統計である。

各項目を見ていくと、「攻撃地(Attacked Systems)」はマルウェアまたは攻撃者によって使用されたシステムの数量であり、実際のマルウェアインストールコマンドまで実行された履歴が確認されるシステムである。もし、攻撃者が不適切に管理されているシステムに管理者アカウントでログインに成功すると、そのシステムに対する操作が可能になる。

「攻撃状況(Attack Attempts)」は、攻撃者がそのシステムを対象に攻撃を実行した回数である。Linux SSH サーバーへの攻撃はスキャニング(scanning)から始まり、総当たり戦または辞書攻撃によってアカウント情報を取得や、基本的な情報を収集する過程を経る。「攻撃状況」は、このような過程を実行したあと、実際のマルウェアインストールログが確認された事例である。

Linux サーバーの攻撃に使用されたマルウェアのタイプは、DDoS ボット(DDoS Bot)、コインマイナー(CoinMiner)、バックドア(Backdoor)、ランサムウェア(Ransomware)などで多様である。以下は、各マルウェアタイプに関する簡単な説明である。

DDoS ボット：攻撃者のコマンドに応じて感染システムを操作し、DDoS 攻撃を実行できるようにするマルウェア。追加ペイロードをインストールや、その他のコマンドを実行することができる機能を含む。

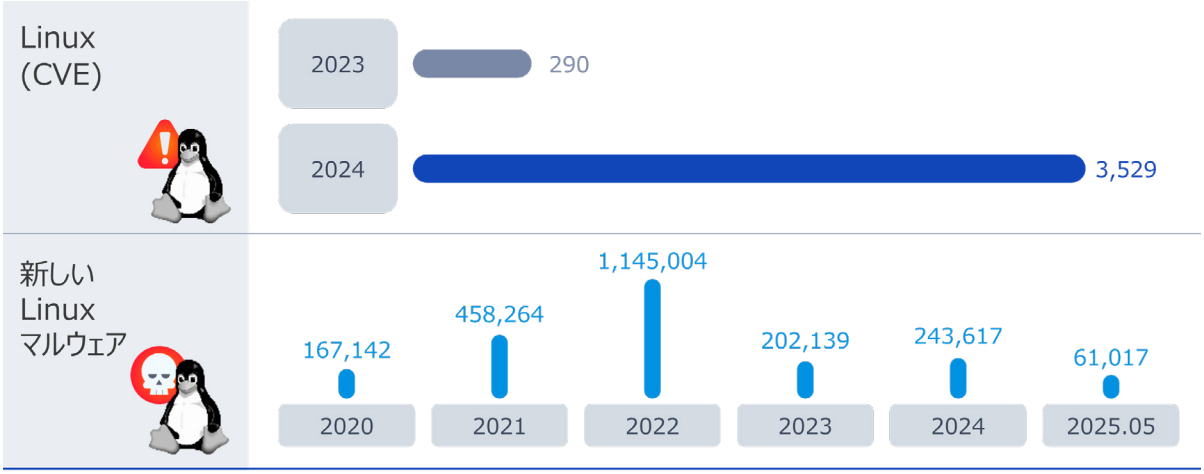
コインマイナー：感染システムのリソースを活用して仮想通貨をマイニングするマルウェア。

バックドア：攻撃者がシステムにひそかに接続し、さらなる不正な振る舞いを実行できるようにするマルウェア。

ランサムウェア：感染システム内のファイルなどを暗号化し、攻撃者が様々な形式で身代金(ransom)を要求できるようにするマルウェア。

[図1] 統計を見ると、最も 近年、6月には176個システムを対象に、なんと1万2千件以上の攻撃が実行された。過去1年間の流れを見ると、月によって差はあるが、大体的に毎月100個以上のシステムに数千件、多いものでは1万件以上の攻撃が実行された。Linux サーバーへの攻撃は、大型ハッキング事件によって関心度が高まっているが、実際は攻撃自体は長期間にわたり活発に実行されていた。

AhnLab の別の統計[図2]を見ると、その傾向をより明確に知ることができる。2023年290個だった Linux の脆弱性は、翌年である2024年には3,529個に10倍以上増加し、Linux 環境をターゲットにした新しいマルウェアは、2025年の半分も経たない5月時点で6万個以上発見された。



[図2] Linux の脆弱性と新しいマルウェアの数

Linux サーバーへの攻撃が増えている理由は簡単だ。多数のクライアント PC に接続されており、様々なビジネス重要データが保存されているためだ。ランサムウェアを始め、Linux ベースのシステムを狙ったマルウェアが増加し続けていることで、ビジネスの中断など深刻な被害に繋がっている。

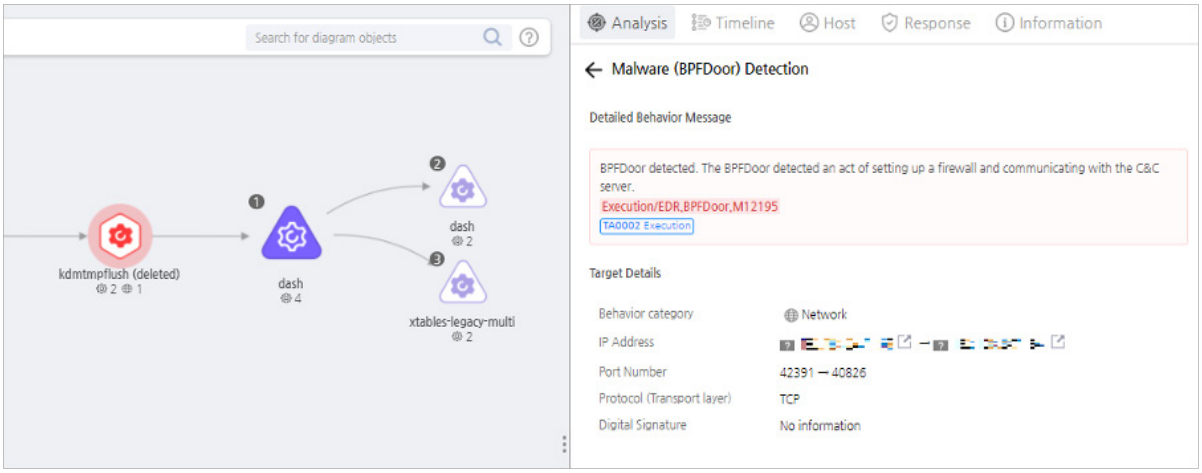
2. Linux サーバーの攻撃事例

次に、2つの実際の事例の分析を通じて Linux サーバーの攻撃について見ていこう。

事例1: BPFDoor(バックドア)を通じた情報窃取

BPF(Berkeley Packet Filter)は、ネットワークパケットフィルタリングのために開発されたメカニズムであり、カーネル領域にインストールされて外部から受け取ったパケットをユーザー領域に渡すかどうかを決定できる。BPFDoorは、この BPF のパケットフィルタリング機能を悪用する Linux バックドアマルウェアである。パケットフィルタリングルールを追加し、操作された特定のパケットである「マジックパケット」が受信されたかどうかをチェックした後、悪意のある振る舞いを実行する。

AhnLab は昨年の10月、自社のエンドポイント検知 & 対応ソリューション AhnLab EDR を活用し、BPFDoor マルウェアを検知および分析して、その内容を ASEC ブログに公開した。



[図3] 2024年10月 AhnLab EDR の BPFDoor 検知内容の一部

分析内容を確認すると、BPFDoor は最初に実行された際、特定のコマンドによって /dev/shm パスに kdmtmpflush という名前で自身をコピーしたあと、自己削除を行う。/dev/shm パスは、Linux のメモリベースファイルシステムであり、アプリケーションが一時データを保存および処理するために使用される。しかし、ディスクに記録されず、メモリ上でのみ動作する特徴があるため、攻撃者によって頻繁に悪用されることがある。

その後、[図4]の文字列のうち1つを選択して名前を変更し、正常なプロセスに偽装する。このとき、prctl() 関数が使用される。

```
char *self[] = {
        "/sbin/udevd -d",
        "/sbin/mingetty /dev/tty7",
        "/usr/sbin/console-kit-daemon --no-daemon",
        "hald-addon-acpi: listening on acpi kernel interface /proc/acpi/event",
        "dbus-daemon --system",
        "hald-runner",
        "pickup -l -t fifo -u",
        "avahi-daemon: chroot helper",
        "/sbin/auditd -n",
        "/usr/lib/systemd/systemd-journald"
};
```

[図4] 正常なプロセスの偽装に使用される文字列

そして、BPF フィルターを登録して待機する。その後、攻撃者がマジックパケットが含まれたコマンドを送ると、BPF フィルターからこれを伝達され、攻撃のための各コマンドを実行する。マジックパケットのソースコードを基準に、パスワードが justforfun の場合はマジックパケットに含まれている IP/Port に接続し、リバースシェル(Reverse Shell)を提供する。パスワードが socket の場合は、バインドシェル(Bind Shell)を提供して新しいポートをオープンし、ファイアウォールを設定して攻撃者の内部接続を確立する。最後に、パスワードにマッチしない場合は攻撃者に「1」を応答する。これにより、攻撃者はマルウェアの成功的な感染の有無を判断できるようになる。このようなプロセスを経て、攻撃者が内部環境と接続すると情報流出などの不正な振る舞いを実行することがある。

最近、通信社の攻撃と SIM カード情報流出に使用されていたマルウェアもやはり BPFDoor である。この攻撃に使用された BPFDoor は変種であり、上に説明したマルウェアと機能面でいくつかの違いがあるが、大枠では同じように動作する。これに関する詳しい内容は、AhnLab が発刊した BPFDoor ケーススタディを通して確認できる。

事例2：プロキシインストールによるシステムの無断接続

2025年2四半期には、Linux サーバーを攻撃してプロキシをインストールする事例が確認された。攻撃事例を見ると、プロキシツールの TinyProxy や Sing-box をインストールしたが、他の攻撃ログが存在しないことから、攻撃者の目的は感染システムをプロキシノードとして活用するためであると考えられる。

攻撃者は、Linux サーバーのログインに成功した後、Bash マルウェアをダウンロードしてプロキシツール TinyProxy をインストールした。その後、TinyProxy の設定ファイルである /etc/tinyproxy/tinyproxy.conf または /etc/tinyproxy.conf で Allow と Deny で始まるアクセス制御ルールを削除し、Allow 0.0.0.0/0 規則を追加した。当該規則が適用されると、外部から制限なくアクセスが可能になる。攻撃者は、TinyProxy がサービスするポート8888番にアクセスし、感染システムをプロキシとして悪用できるようになった。

```
200 #Allow 127.0.0.1
201 #Allow ::1
202 #Allow 192.168.0.0/16
203 #Allow 172.16.0.0/12
204 #Allow 10.0.0.0/8
205

325 #
326 #ReverseBaseURL "http://localhost:8888/"
327
328
329
330
331 # Added by script - WARNING: Allows all connections!
332 Allow 0.0.0.0/0
```

[図5] コメント処理および挿入された TinyProxy 設定

以下は、被害システムに Sing-box という名前のプロキシツールをインストールした事例である。Sing-box は、多目的プロキシをインストールするツールであり、vmess-argo、vless-reality、Hysteria2、TUICv5 プロトコルに対応する。Github の説明によると、このツールをインストールすることで ChatGPT および Netflix の遮断を解除できる。本事例では、攻撃者が Linux システムに無断で接続し、Sing-box をインストールした。そして、これを通じてさらなる違法行為や金銭的収益を狙ったものと推定される。

近年、Linux サーバーへの攻撃事例を見ると、プロキシ機能を担うマルウェアではなく、TinyProxy や Sing-box のように正常に使用できるツールを悪用する傾向がある。攻撃者は、感染システムをプロキシとして活用し、別の攻撃を行う際に自分を隠蔽することができる。また、このプロキシノードに対するアクセス権を販売し、違法な収益を上げることもできる。

3. Linux サーバーのセキュリティのための必須ソリューションは？

このような最新のサイバー脅威は、単一のソリューションのみを活用する断片的なアプローチでは対応が困難である。攻撃がエンドポイント、電子メールなどの様々な区間で始まり、新/変種マルウェアが頻繁に登場するためである。また、攻撃が一度で終わらず、いつでも再発する可能性がある。そのため、効果的なセキュリティのためには以下のような能力が求められる。

・脅威検知、分析および対応へと続くセキュリティ体制
・製品間の連携と連動をサポートし、複数のセキュリティ区間を保護できるアーキテクチャ
・検知および遮断を越え、脅威を追跡して再発を防止できるセキュリティ戦略

もちろん、多くのソリューションを効果的に運用できれば最良だが、現実的な余力が伴わないケースが多い。このとき、成功した Linux サーバーセキュリティを目標とする企業にとって必須のソリューションを挙げるとすれば、アンチウイルスと サンドボックス、EDR、そして MDR サービスがある。

#1. アンチウイルス：アンチウイルス(Antivirus、AV)は、シグネチャ(Signature)と振る舞い分析などの技術をベースにマルウェアの流入を事前に検知して遮断する。エンドポイントセキュリティにおいて最も基礎的でありながら必須のソリューションであると言える。AV 製品は PC とサーバー、そして Windows、MacOS、Linux など各環境に合わせて提供される。Linux サーバーのセキュリティのためには、この環境に最適化された AV ソリューションが求められる。

#2. サンドボックス：サンドボックスソリューションは、複数のセキュリティ区間でファイルを収集し、仮想環境(VM)で動的分析を実行する。例えば、仮想環境でドキュメントファイルを実行して操作し、隠れた不正な振る舞いや、未知の脅威を見つけ出すことができる。また、AV ソリューションを回避するランサムウェアも検知する。シグネチャをベースに既知のマルウェアを素早く検知する AV とは相互補完的関係を持つものと理解すればよい。

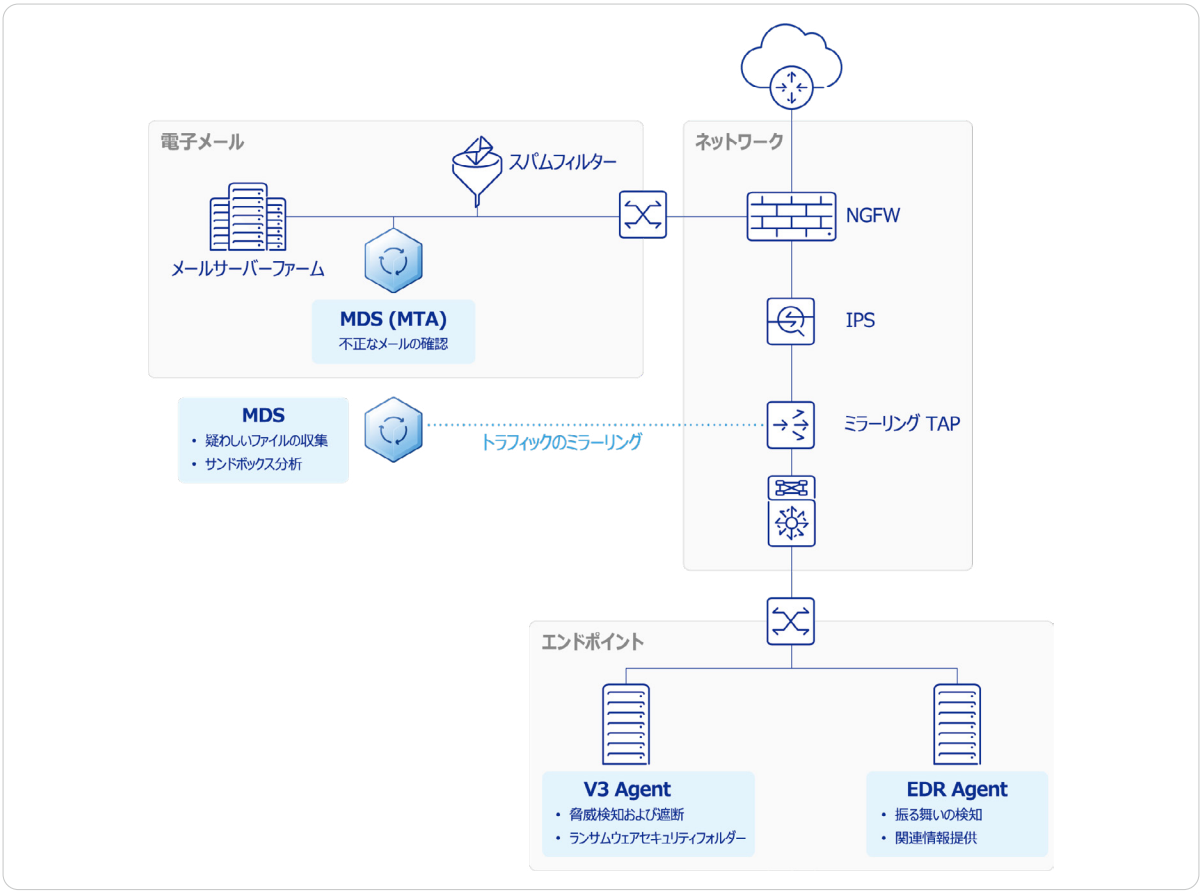
#3. EDR: EDR(Endpoint Detection & Response)は、エンドポイントで発生するすべての振る舞いとイベントを検知およびロギング(logging)し、侵害事故の調査に必要な情報を常時収集するソリューションである。収集した振る舞い情報をもとに脅威を能動的に追跡・分析し、長期的な脅威対応システムの確立に貢献する。簡単に例えると、すべてをモニタリングする CCTV のような役割を実行する。

#4. MDR サービス: MDR(Managed Detection & Response)は、セキュリティの専門家が EDR を活用した脅威の検知、分析、およびパーソナライズされた対応を提供するサービスである。これにより、企業のセキュリティ運用の負担を軽減し、検知 & 対応力を強化することができる。サイバー脅威が高度化し、EDR ベースの検知および分析には相当な専門性が要求されるため、MDR サービスへの需要と関心が高まり続けている。

このように、AV、サンドボックス、EDR を正しく運用し MDR サービスを活用すれば、様々な脅威に対する高度な対応体制を整えることができ、Linux サーバーのセキュリティに相当な効果を得ることができる。

4. AhnLab の体系的なセキュリティアーキテクチャ

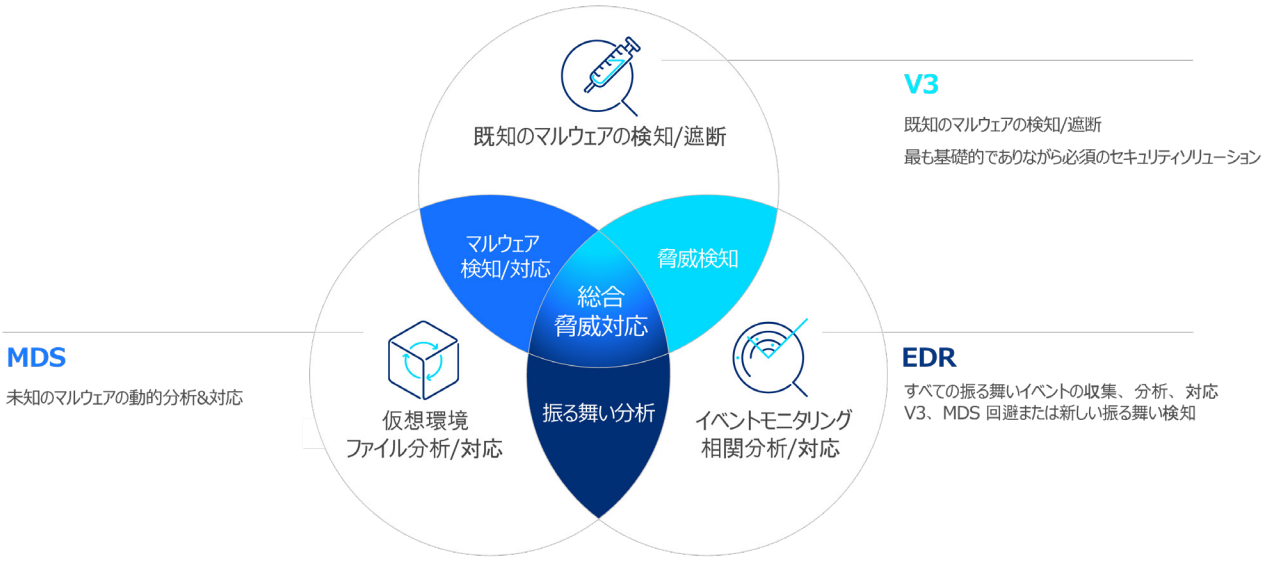
AhnLab は、エンドポイントや電子メールなど、サイバー攻撃が流入する可能性のある区間に対して最適なセキュリティ対策を提示し、顧客が強力な脅威対応システムを構築できるようにする。攻撃者が活発に使用している不正な電子メールの隔離から、ネットワークトラフィックミラーリングを通じたファイルの収集および分析、そしてエンドポイント段の様々なセキュリティ機能と脅威の追跡を通じた再発防止まで、完璧に近いセキュリティ体制を提供する。



[図6] AhnLab の Linux サーバーセキュリティアーキテクチャ

[図6]は、ランサムウェアなど主要なサイバー攻撃に対するセキュリティを提供する AhnLab の Linux サーバーセキュリティアーキテクチャである。このアーキテクチャは、各構成ソリューションが互いに柔軟に連動し、シナジーを生み出す形で運用される。アーキテクチャを構成するソリューションは、静的(Static)、評判(Reputation)、動的(Dynamic)、振る舞い(Behavior)分析など、多様な検知手法をもとに様々な脅威を隙間なく防御する。

アーキテクチャを構成するソリューションの役割を整理すると、以下の通りである。



[図7] AhnLab Linux サーバーセキュリティアーキテクチャ ソリューション別の役割

#1. AhnLab V3: 既知のマルウェアの検知 & 遮断

AhnLab V3 は、AhnLab の30年の歴史と技術力が詰まったアンチウイルスソリューションであり、数十億個のマルウェアシグネチャが保存されている自社データベースをもとに、知られているマルウェアを素早く正確に検知および遮断する。数千の不正な振る舞いパターンを活用し、知られているものだけでなく、未知のマルウェアにも対応可能である。

このほか、ランサムウェアセキュリティのための特化機能である▲デコイファイル検知 ▲アプリ隔離検査 ▲ランサムウェアセキュリティフォルダーなどを提供する。▲プロセスメモリ検知 ▲AMSI(Anti Malware Scan Interface)検知を通じて、ファイルレス形式で配布されるマルウェアも検知し、遮断することができる。

AhnLab V3 は、エンドポイントタイプや OS ごとにソリューションを提供する。Linux サーバーの場合、V3 Net for Linux が BPFDoor を始めとし、Linux 系列のマルウェアに対して最適化された検知および遮断をサポートする。また、Linux サーバーがクラウド環境でも多数使用される点を考慮し、Docker コンテナ検知などクラウドセキュリティ機能も同時にサポートし、顧客が真のハイブリッドクラウドセキュリティを実装できるようにする。

#2. AhnLab MDS : 不正な電子メールの遮断および未知のマルウェア分析

Linux セキュリティの観点から AhnLab MDS は、ネットワーク、電子メールサーバーの前段、網連携区間など、様々な領域でサンドボックスベースのファイルスキャンを実行する。

電子メール区間において AhnLab MDS の MTA(Mail Transfer Agent)は、メールのヘッダー、本文、URL、添付ファイルを総合的にチェックする。本文に含まれている URL は直接接続して異常の有無を把握し、添付ファイルはサンドボックス環境で分析する。不正な電子メールは隔離し、システムに流入しないようにする。

また、ネットワークトラフィックミラーリングを通じて疑わしいファイルを収集し、仮想 VM 環境で実行および分析して、不正であるかどうかを判別する。Linux セキュリティの観点から見ると、一般的な Linux ファイルは特定のパラメーターとともに実行されるケースが多く、AhnLab MDS はユーザーがファイルとパラメーターを直接入力して振る舞いの現象の有無を確認できるという利点がある。また、複数のファイルを仮想環境に集めて解析できるため、Linux 脅威の検知および分析に有利である。

#3. AhnLab EDR : すべてのエンドポイントイベントと振る舞い検知 & 対応

AhnLab EDR は、サーバー、PC などの複数のデバイスで発生するすべての振る舞いをモニタリングし、エンドポイントの脅威を検知 & 対応する。主要機能は、すべてのエンドポイント振る舞い情報の収集、イベントの関連関係の分析、AhnLab V3、MDS などのソリューションと連携した脅威対応などがある。エンドポイント全般の脅威管理、未知の脅威の潜伏期間の最小化と潜在的な被害および再発防止を目的とする。

AhnLab EDR は、検知した脅威に対して MITRE ATT&CK フレームワークに基づく脅威情報と流入経路、主要振る舞い、関連関係、危険度、脅威情報リンクなどに関して詳細な分析内容を提供する。分析情報を ▲ 相関図 ▲ タイムライン ▲ プロセスツリー 形式で表示し、ユーザーが全体的な攻撃フローを容易に把握できるようにする。

そして、このようにレベルの高いセキュリティ管理に最適化された専用コンソール「EDR Analyzer」を提供し、ユーザーが脅威を正確に認知して対応し、当社に最適化されたポリシーを設定できるようにサポートする。

#4. MDR サービス : EDR の活用性を最大化

EDR は、他のソリューションに比べて運用の難易度が高い。そこで、AhnLab は AhnLab EDR のソリューション運用と活用を助ける「MDR サービス」を基本で提供し、顧客の使用性を高める。AhnLab EDR の顧客は、AhnLab セキュリティ専門家のリアルタイムモニタリング、重要度の高い脅威に対する分析・対応、分析レポートと月間統計レポートなどのサービスを利用できる。より専門的なサービスを希望する顧客は、プレミアム MDR サービスが含まれた「EDR Premium」を利用できる。このサービスを利用すると、より広範囲のログ分析、組織環境とセキュリティ問題を反映したカスタマイズ型検知ルールの生成など、深層サービスを受けることができる。

5. AhnLab の Offering を選択すべき理由 3つ

AV、Sandbox、EDR すべて市場に複数のソリューションが供給されている。顧客の立場から、これらの中で AhnLab の Offering が魅力的な理由を 3つ紹介する。

#1. ソリューション間の柔軟な連携とシナジー

30年前の V3 を始まりに、アーキテクチャを構成するすべてのソリューションを自社開発した AhnLab は、ソリューション間の柔軟な連携によってシナジーを生む体系を構築した。顧客は上記のソリューションを相互補完的に使用することで、より強力なセキュリティ効果を享受できる。

[図8] AhnLab EDR と MDS 連携分析

特に、分析と対応の観点からより大きな効果を得ることができる。例えば、V3 でマルウェアとして検知された情報を基に EDR が流入経路などの詳細分析情報を提供し、今後発生する可能性のある同じ脅威を先制的に遮断することができる。また、EDR で収集された様々なプロセスとファイル情報を Sandbox で分析したい場合は MDS に深層分析をリクエストし、結果を確認して脅威に対する深層的な情報も把握することができる。

#2. 顧客事例を通して検証された優秀性

AhnLab の Linux セキュリティアーキテクチャは、長期間にわたり多くの顧客が導入して使用し、その有効性を証明している。顧客は V3 Net for Linux、AhnLab MDS、および AhnLab EDR をそれぞれ導入して活用するケースもあるが、2つまたは3つのソリューションを導入して統合セキュリティ効果を享受するケースも多い。このソリューションはそれぞれ異なる役割を実行しているが、相互補完的関係を持っているため、一緒に運用されたときに最良のシナジーを生む。

また、このソリューションは Linux だけでなく、Windows 環境まで網羅する連動ベースのセキュリティを提供し、顧客が安全なビジネス環境を構成できるようにサポートする。

#3. 卓越したグローバル公認評価成績

最後に、AhnLab のセキュリティソリューションは、全世界で公認されるセキュリティ評価で優秀な成績を収め、技術力を証明してきている。

特にAhnLab EDR は、全世界で最も公信力のあるセキュリティ製品テストの一つである「マイティアタック評価(MITRE ATT&CK Evaluation)」に、韓国のセキュリティ企業としては唯一4回連続で参加し、優秀性を証明している。マイティアタック評価は、主要脅威グループの攻撃手法を模擬実行したシナリオをベースに、参加製品の脅威検知＆対応能力を評価する。

特に、最近実施されたラウンド6では、主要ランサムウェアグループであるクローン(CL0P)とロックビット(LockBit)が Windows と Linux に渡って実行する実際の攻撃手法で構成されたシナリオのうち、95%を検知した。これは、全世界のセキュリティ企業の中でも上位に該当する成績である。さらに、検知した56個の細部段階(substep)のうち49個で最高等級である Technique を受けたが、これはユーザーが検知情報を通じて脅威の行為に対する「コンテキスト(Context)」を包括的に理解できるという証拠である。

AhnLab のマイティアタック評価ラウンド6の結果に関する詳しい内容は、結果分析報告書を通して確認できる。

6. 結びに

AhnLab は、過去 30年間にわたり蓄積してきた技術力とノウハウを基に、Linux サーバーを含むエンドポイント全領域で連携を基盤とした強力なセキュリティ能力を提供する。そして、複数の顧客導入事例を通じてソリューションの有効性を、グローバルなセキュリティ評価を通じて優れた技術力を証明してきている。

AhnLab のセキュリティアーキテクチャと共に、高度化する Linux セキュリティ脅威に効果的に対応されたい。

AhnLab の Linux セキュリティアーキテクチャ構成ソリューションに対する詳細内容は、AhnLab の公式ウェブサイトで確認できる。

- V3 Net for Linux Server
- AhnLab MDS
- AhnLab EDR
- MDR サービス

AhnLab, Japan
〒 108-0014 東京都港区芝 4丁目 13-2田町フロントビル 3階
www.ahnlab.com/jp | jp.sales@ahnlab.com