ご参考資料（ブログ）
報道関係者各位

2018 年 9 月 11 日
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

台頭するファイルレス・マルウェアも検出可能な Check Point SandBlast Agent

新機能「Behavioral Guard」を使い、不正なふるまいを検出

米カルフォルニア州 サン カルロス - 2018 年 8 月 23 日

攻撃の際にファイルを使用しない「ファイルレス・マルウェア」が増加しています。この高度な攻撃手法では、攻撃者が標的のマシンを攻撃する際、マルウェアをインストールする必要がありません。そのため、（シグネチャーベースの）従来型のアンチウイルス・ソリューションでは検出することができません。ファイルレス・マルウェアは、標的のマシンに存在する既存の脆弱性を悪用し、Windows Management Instrumentation（WMI）や PowerShell などの一般的なシステム管理ツールを用いて、通常は安全であると信頼されているプロセスに不正なコードを挿入します。

増加の一途を辿るこのファイルレス・マルウェアを非常に効果的に検出できるのが、先ごろチェック・ポイントがリリースした SandBlast Agent の新機能、Behavioral Guard です。Behavioral Guard は、簡単に言えば、あらゆる不正なふるまいを検出して対処する振る舞い検出エンジンです。独自のフォレンジック技術を活用して未知のマルウェアのふるまいを効果的に検出し、そのマルウェア・ファミリーを正確に特定します。この高度な検出技術は、マルウェアの継続的な進化に適応する柔軟性を備えており、正規のスクリプト・ツールの悪用など、次々出現する新しい攻撃手法にも対応することが可能です。

Behavioral Guard の投入依頼、チェック・ポイントは、従来型の技術では検出困難なファイルレス攻撃を数多く発見しています。最近、お客様環境の PC で見つかった攻撃の 1 つでは、ファイルレスのペイロードが WMI のファイル・システムの奥深くに隠されており、システムの起動時など特定のイベント時にのみ、Windows システムによってバックグラウンドで密かに実行されていました。

この攻撃では、PowerShell を実行する永続的な WMI イベント・コンシューマ・オブジェクトを作成し、インラインのスクリプトで Windows の認証情報を収集、パブリック・クラウド・サービス上のサーバにアップロードしていました。PowerShell は、現行のすべての Windows オペレーティング・システムに標準搭載されている、Microsoft による署名付きの信頼されたプロセスです。シグネチャで検出できる一般的なマルウェア攻撃と異なり、この攻撃は、ディスクにファイルを書き込んだり、オペレーティング・システム上で不正なプロセスを実行したりすることなく、システムの奥深くで進行します。しかし、チェック・ポイントの Behavioral Guard は、スクリプトが難読化されたこのファイルレス攻撃の検出に成功しています。

スクリプト型のマルウェアは、本格的なファイル・ベースのマルウェアよりも短時間で簡単に作成できることから、攻撃者の間ではスクリプト型に移行する動きが広がっています。また、攻撃におけるスクリプトの使用は、ファイルとは違う課題をセキュリティ・ベンダーに突きつけています。スクリプト型マルウェアの詳細については、こちらのレポートをご覧ください。

ファイルレス攻撃の観測数は、増加する一方です。防御側の組織は、この攻撃の特徴や、従来型のアンチウイルス・ソリューションでは検出困難であるという事実を理解しておく必要があります。一般的なエンドポイント・セキュリティ対策は、高度なファイルレス攻撃に対してまったくの無力であり、いわゆる次世代アンチウイルス（NGAV）ソリューションでもこれらの攻撃を検出することはできません。しかし上で述べたように、SandBlast Agent の Behavioral Guard 技術は、ファイルレス攻撃に対して有効に機能することが実証されています。既知の攻撃だけでなく、まだ見ぬ未知の攻撃に対しても、同様の効果が期待できます。

本ブログは、米国時間 8 月 23 日に配信されたものの抄訳です。
米ブログ本文はこちらをご確認ください。
https://blog.checkpoint.com/2018/08/23/file-less-malware-no-match-for-sandblast-agent/
日本のブログ本文はこちらをご確認ください。
https://www.checkpoint.co.jp/threat-cloud/2018/09/file-less-malware-no-match-for-sandblast-agent.html

■チェック･ポイントについて

チェック・ポイント・ソフトウェア・テクノロジーズ（www.checkpoint.com）は、世界各国の政府機関や企業など、あらゆる組織に対応するサイバー・セキュリティ・ソリューションを提供する大手プロバイダーです。業界随一の検出率を誇る先進のソリューションにより、お客様のネットワークを、マルウェアやランサムウェアなどの多岐にわたる第 5 世代のサイバー攻撃から保護します。企業のクラウドやネットワークのほかモバイル・デバイスに保存されている情報を、今日の第 5 世代のサイバー攻撃を含めてあらゆる脅威から保護するため、第 5 世代の脅威に対応するマルチレベルのセキュリティ・アーキテクチャを備え、直感的で操作性に優れた総合的かつ一元的なセキュリティ管理システムを展開しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社　広報代行　共同ピーアール株式会社

担当　マーケティング　横山

Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: marketing_jp@checkpoint.com

担当　上瀧・花岡

Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

