proofpoint

ET INTELLIGENCE

ハイライト

- 常に最新の状態にアップデートされるインテリジェンスを使い、ダイナミックに変化する脅威環境に追随
- 攻撃が組織に到達する前に遮断
- シンプルで活用しやすいデータセットにより、既存のセキュリティインフラのROIを向上
- 現実のインテリジェンスに基づいたプロアクティブなセキュリティ対策を適用
- 侵害後の活動の兆候を探し、予防デバイスがきちんと機能しているかを検証
- 疑わしいIPアドレスやドメインに関する情報を使って既存のログデータを強化
- 組織にとって重要なレピュテーションカテゴリ、スコア及びしきい値を基にカスタムのセキュリティポリシーを適用

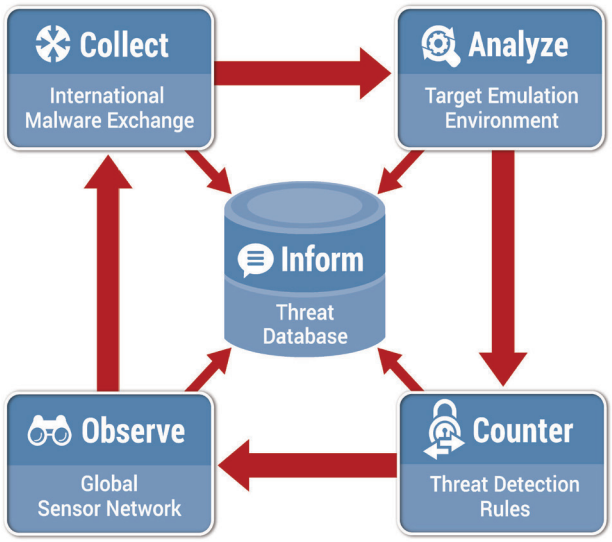
Proofpoint ET Intelligenceは、業界で最も正確でタイムリーな脅威インテリジェンスの情報ソースです。ET Intelligenceは、すぐに活用できる(actionableな)最新のIP及びDomainのレピュテーション情報と、世界中で観測された脅威とマルウェアの解析データベースを組み合わせており、マリシャスな攻撃を予防し、調査に必要なコンテキストを提供してセキュリティプロフェッショナルを助けます。

Proofpoint ET Intelligenceが必要な理由

現代の先進的サイバー攻撃は、金銭的利益の追求やスパイ目的など幅広い動機を持ち、様々な経路から高頻度の攻撃を仕掛けてきます。

これらの攻撃で使われる基本的なツールは共通の部品から作られており、ほとんどが20個ほどのよく知られたエクスプロイトキットを基にしているとはいえ、個々の攻撃は別々のボットネット、プロキシ、攻撃経路、コマンド&コントロールシステムなどを使っています。これらの攻撃の本質はダイナミズムであり、激しく変化する脅威環境に個々の企業が追随していくことは、ほぼ不可能です。

そこで、Proofpointの出番です。



Proofpoint ETラボの専任の脅威研究者のチームと解析システムが解析を行いますから、お客様が手を煩わせる必要はありません。ETラボは直接的な観測による100%オリジナルの情報ソースを元に、IPアドレス、ドメイン、マルウェアサンプル、エクスプロイトキットに関連する脅威インテリジェンスを提供します。世界最大級のマルウェア交換所を持ち、膨大な規模での被害者エミュレーション、オリジナルの検知技術、そして世界規模のセンサーネットワークを有効に活用する独自のプロセスを構築しています。Proofpoint ET Intelligenceはリアルタイムにアップデートされ、様々な組織へ向けて、現代の先進的脅威と戦うためのすぐに活用できるインテリジェンスを提供します。

Proofpoint ET Intelligenceには、ドメイン及びIPアドレスのレピュテーション情報と世界的な脅威データベースが含まれていますから、行動に結びつく脅威インテリジェンスと共にインシデントと脅威の調査に役立つ有用なコンテキストを提供します。

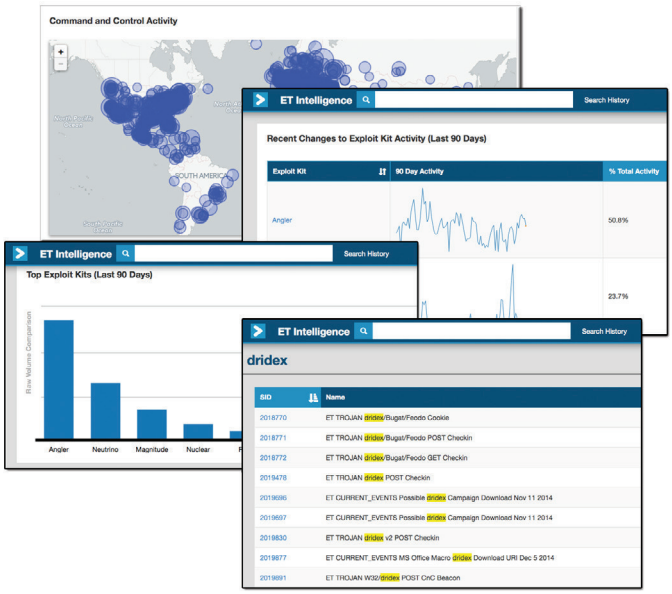
動的IP及びドメインレピュテーション

ET Intelligenceは、ファイアウォール、侵入検知/防御システム (IDS/IPS)、ログ/イベント管理システム (SIEM)、認証システムなどに、すぐに活用できる脅威インテリジェンスを提供します。

これらの動的な情報を使って、ProofpointのETラボで直接観測された疑わしい、あるいはマリシャスな行動に関連するIP及びドメインを特定します。この機能には以下が含まれます:

IPアドレスとドメインの個別のリスト

- 40種類以上のカテゴリに分類され、カテゴリ毎に信頼性スコア(0から127まで)を付与されたIP及びドメイン
- 直近の活動レベルとアグレッシブエージングを反映したスコア
- アグレッシブエージングされたリストとスコアを1時間毎にアップデート
- TXT、CSV、JSON及び圧縮ファイルなど複数のファイルフォーマットをサポート



Proofpoint ET Intelligence
世界規模の脅威データベース

世界規模の脅威データベース

現代の環境では、どのようなタイプの脅威が存在するかということだけを知っていても十分ではありません。攻撃を予防し、リスクを減らすためには、その脅威がどこで作られたか、誰が作ったのか、いつ攻撃を受けたのか、どのような方法を使ったのか、なぜ攻撃をしたのかなど、過去のコンテキストを知ることが重要です。Proofpoint ET Intelligenceを使えば、インシデントの調査を進め脅威の研究を行うために、IPやドメインその他関連する脅威インテリジェンスについての現在及び過去のメタデータにオンデマンドでアクセスできます。

以下の機能を含みます:

- 現在及び過去の脅威インテリジェンスへのオンデマンドのアクセスを可能にします。IPアドレス、ドメイン、マルウェアMD5、ETシグネチャID、メッセージテキストなどで検索可能です。
- 検索結果はピボットやドリルダウンにより、さらなる検討が可能です。インシデント調査を効率化するためのフォレンジックデータ痕も提供します。
- 5年間に及ぶ脅威アクティビティの観測結果を提供します。
- データは継続的にアップデートされます。
- コマンド&コントロール、活発なエクスプロイトキットについての世界規模の脅威環境をリアルタイムにダッシュボードに表示します。
- WebインターフェースまたはAPI経由で利用可能です。

Proofpointのレイヤードセキュリティ

個々のセキュリティシステムは、特定のタイプの脅威から組織を防御するためには効果がありますが、全ての脅威を完全にカバーできるわけではないため、最終的には侵害されてしまいます。

- ET Intelligenceを使って、先進的脅威を検知するためのすぐに活用できるリアルタイムなインテリジェンスとコンテキストを手に入れます。
- Targeted Attack Protection と Proofpoint Enterprise Protection で、メールベースの攻撃を調査します。
- URL Defense Service と Attachment Defense Serviceからのレポートで、より深い先進的脅威のフォレンジックを実現します。
- Threat Responseを使って遮断した脅威を調査します。
- Proofpoint Enterprise Privacyを使って重要かつ機密なデータを守る能力を高めるために、インテリジェンスを活用します。

既存のデータとツールを強化

現代のネットワークセキュリティインフラには、ファイアウォール、次世代ファイアウォール(NGFW)、統合脅威管理(UTM)アプライアンス、セキュリティインシデントイベント管理(SIEM)プラットフォーム及び認証システムなどが含まれています。これらにタイムリーな脅威インテリジェンスを供給することによって、より効果的に運用することができます。

レピュテーションデータの利用:

- ファイアウォール、NGFW、IPS/IDS、UTMなどでリスクの高いIPアドレスとの接続を遮断することにより、これらのデバイスの有効性を高めます。
- リスクベースの認証システム内で、疑わしいIPアドレスにチャレンジを送ります。
- SIEMプラットフォームのイベント及びログデータの強化を行います。
- プレディクティブな解析システムにデータを供給します。
- 侵害された資産を特定し、内部の感染範囲を調べます。

グローバル脅威データベースの利用:

- インシデントの調査を行います。
- 特定の攻撃を利用可能な数十億の侵害指標に関連づけます。
- 世界中で活動している攻撃と攻撃者を検索し、表示します。
- マルウェアのサンプルが実行された際に生成されるネットワークトラフィックを可視化してマルウェアを研究します。
- 調査のための追加のコンテキストのためにSIEMと統合します。

今すぐProofpointにご相談下さい

現代の脅威環境は非対称な闘いを強いられています。攻撃者は狙いをひとつ見つければよいところを、攻撃される側は多くの側面を守らなければなりません。現在の防御は、それがどれだけ洗練されていたとしても、効果的では無いのです。すぐに活用できる脅威インテリジェンスがプロアクティブに提供され、それがコンテキストを伴っていれば、大規模な流出を軽微な侵害に変えることができます。