elastic security labs

2023年版グローバル脅威レポートでCISOが押さえるべき10のポイント

脅威に関するインサイトを提供するために始動したElasticのグローバル脅威レポートは今年で2年目に突入しました。何か月にもわたって10億超のデータポイントから収集されたプライベートテレメトリーや公開テレメトリーに基づく主な調査結果をご紹介します。Elastic Security Labsでは、これらのインサイトを3つに分類しました。展望予測、攻撃者の戦略、そしてシステムです。

展望予測

1.オープンソースツールがさらに浸透
脅威アクターは無料のオープンソースツールを活用して、簡単にサイバー犯罪に手を染めるようになります。Elasticでは、グローバル脅威レポートやそれ以前の分析において、r77 rootkitやJOKERSPYといったオープンソースのマルウェアツールをいくつか観測しています。

2.新規参入の脅威アクター向けのサービスとしてのマルウェア（MaaS）が増加
攻撃者は知識や製品についてのギャップを埋めるためにサービス形態（AaS）のモデルを活用します。これはサービスとしてのランサムウェア（RaaS）の隆盛と同様の状況です。悪意のあるAaSを提供する企業は、ポートフォリオをさらに拡充し、購入者のニーズに沿おうとします。攻撃者はMaaSを通じて難読化やなりすましの技術を利用します。

3.攻撃者は身を潜めずに環境を改変
環境が攻撃耐性を高める中、攻撃者は以前よりもセキュリティセンサーを無効化したり、改変したりしようとすることが増えました。グローバル脅威レポートの分析以外でも、ElasticではOSの設計上の瑕疵を突いた攻撃の増加を観測しています。たとえば、Bring Your Own Vulnerable Driver（BYOVD、脆弱性を有したドライバーの持ち込み）により、悪用可能な脆弱性が1つ以上あるドライバーをデプロイさせるなどです。

攻撃者の戦略

4.ランサムウェアの拡大と多様化が進行中
ランサムウェアは、注目を集めているWannaCryやNotPetyaだけに限らず、年々脅威度を増しています。サービスとしてのランサムウェア（RaaS）は、観測されたランサムウェア全体の81%を占めており、新規攻撃者と古参の攻撃者の両方にとって、参入障壁が低くなっていると考えられます。今後、脅威アクターはこのサービスを利用しながら革新を続けていくと考えられます。

5. 攻撃者はシステムについて熟知している
観測されたエンドポイントの振る舞いのうちほぼ半数（43.89%）が、防御回避に該当していました。この割合の高さから、攻撃者が防御回避に慣れており、簡単にセキュリティシステムを回避できていることがわかります。

6. 組み込みのOSユーティリティを通じて悪意のあるコードを実行
Elasticが観測した、エンドポイント上で実行された防御回避技術の48%が、システムバイナリプロキシ実行で占められていました。脅威アクターはこの技術を使用して悪意のあるコードをネイティブなOSプログラム内で実行することができます。この種のアラートは分析に時間がかかるため、この技術は非常に人気があります。

7. 攻撃者はクラウド環境で認証情報アクセス技術を利用
Elasticの観測では認証情報アクセスのシグナルが11%増加しており、クラウドに侵入するプロセスにおいて認証情報が重要な要素になっていることがうかがい知れます。認証情報の収集が簡単になっていることや、環境が十分に可視化されておらず有効な認証情報が不正に使用されたことを特定しきれていないなどの状況が考えられます。

システム

8.Windowsでの観測が増え、Azureの人気を示している
ElasticのWindows環境の可視化能力は今年さらに高まり、Microsoft 365での観測も含めると、昨年の分析と比べて422%の増加が見られました。クラウドサービスプロバイダーに関する分析によれば、Azureでのアクティビティが昨年の13.14%から36%に増えています。AWSがまだ大部分を占めていますが、AWS環境からのシグナルはおよそ10%減少しました。

9. Windowsがエンドポイントシグナルの大半を占めているが、macOSとLinuxのシグナルの増加も目立つ
エンドポイントの振る舞いのアラートの94%がWindowsを対象としていましたが、その一部の要因は、Windowsに注目したテレメトリーにあります。Elasticの観測では、Windows、Linux、macOSで全体的にシグナルが大きく増加しています。macOSでの118%もの増加を受け、革新担当チームがRUSTBUCKETというマルウェアを新発見したこともありました。

10.マルウェア感染が最も多く観測されているのはLinuxシステム
Elasticのあらゆるシステムへの観測能力が強化されたにもかかわらず、Linuxは今も感染事例の91.2%を占めています。これらの攻撃のほとんどは人の手による介入が一切なく、自動的に、場合によっては無差別に攻撃を実行しているのが特徴です。

脅威の展望を知る

これらを含むさまざまな脅威の進化に備えましょう。Elastic Security Labsのエキスパートの提案を2023年版Elasticグローバル脅威レポートでご覧ください。X（旧Twitter）でElastic Security Labs（@ElasticSecLabs）をフォローして、脅威の進歩や研究等に関する最新の記事を確認しましょう。

