elastic security labs

2022年版グローバル脅威レポート

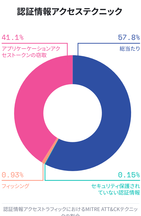
インフォグラフィック

脅威の発生源はどこかご存知ですか？

Elastic Security Labsは2022年版のグローバル脅威レポートでは、ソリューションのテレメトリに基づき、脅威の現象、トレンド、推奨事項を明らかにしています。これらの情報は組織が将来に備えるために役立ちます。調査結果には次の内容が含まれています。

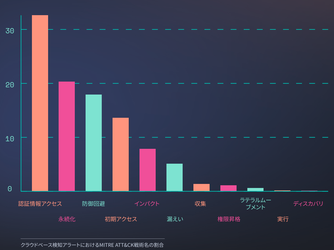
クラウドの運用は、セキュリティのデフォルト設定にさらに追加してセキュリティ制御を行うことで安全になる

認証情報アクセスアラートの41%は、アプリケーションアクセストークンの窃盗の試みにより発生している。



認証情報アクセストラフィックにおけるMITRE ATT&CKテクニックの割合

一旦侵入した攻撃者が主に狙うのは認証情報アクセス



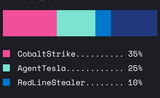
クラウドベース検知アラートにおけるMITRE ATT&CK戦術名の割合

商用ソフトウェアが武器化されている

レッドチームのために設計されたマルウェアが組織に対して使用されている。

Windowsエンドポイントを標的とする悪意のあるバイナリやペイロードの中で最も多く見られたのがCobaltStrikeであり、続いてAgentTeslaと、そしてRedLineStealer。

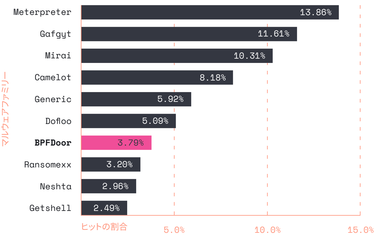
すべての検知



- CobaltStrike..... 35%
- AgentTesla..... 25%
- RedLineStealer..... 10%

オープンソフトウェアは、思っているほど安全ではない

Linuxの マルウェア/ペイロードトップ10

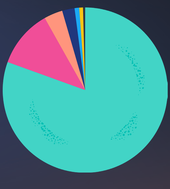


Linuxにおけるマルウェアおよびペイロードのトップ10 (BPFDoorアクティビティの増加が顕著)

成果物を兵器化する方法として引き続き好まれているのはトロイの木馬

カテゴリー別のマルウェア

- トロイの木馬 80.5%
- クリプトマイナー 11.3%
- ランサムウェア 3.7%
- パッカー..... 2.4%
- バックドア 0.9%
- プロキシ 0.7%
- その他 0.5%



良いニュース - エンドポイントセキュリティは機能している

エンドポイント攻撃者による防御回避の手口が多様化している。今年は、失敗したエンドポイント侵入手法を50件観察した。

テクニック	シグナルの割合
なりすまし	44.29%
システムバイナリのプロキシ実行	30.00%
アクセストークンの操作	12.32%
プロセスインジェクション	7.62%
BITSジョブ	4.74%
信頼される開発者ユーティリティのプロキシ実行	0.90%
XSLスクリプト処理	0.66%
防御の弱体化	0.65%
防御回避のための悪用	0.64%
システムスクリプトのプロキシ実行	0.13%
レジストリの変更	0.03%
ホスト上のインジケーターの削除	0.01%

2022年版グローバル脅威レポートをダウンロードして、Elastic Security Labsのリサーチャーによる調査結果の全文をご確認ください