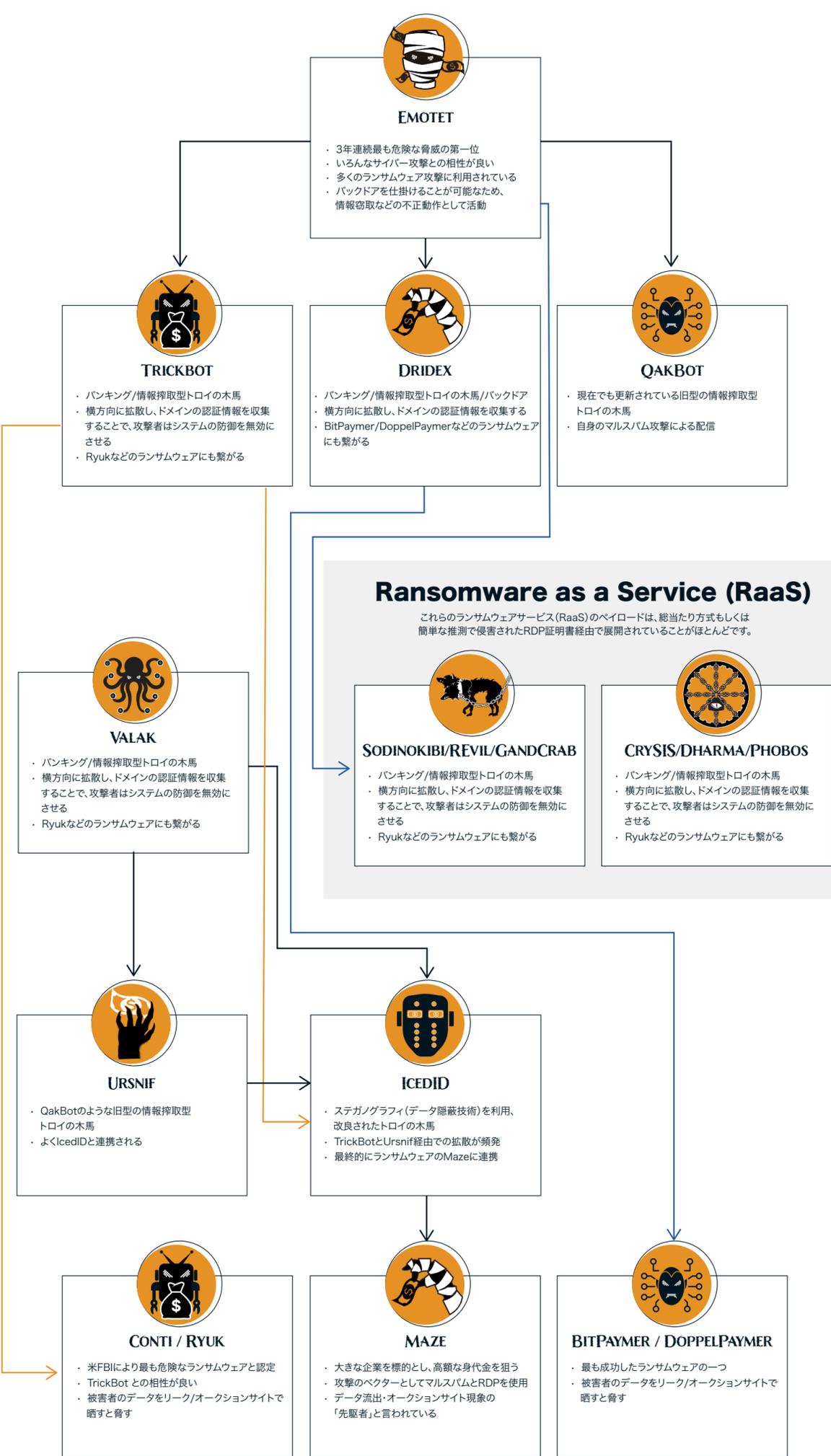


ウェブルート 最も危険なマルウェア2020

毎年、当社の脅威調査の専門家が、これまでに見た中で最も危険なマルウェアを特定するために、データを徹底的に調査しています。2020年は新型コロナウイルス感染拡大の影響でリモートワークが増し、在宅勤務者を標的としたフィッシングやRDP攻撃が主要な脅威であることがわかりました。

今年の最も危険なマルウェアや その感染の仕組み



おすすめの安全対策

現代のサイバー攻撃は複数の攻撃ベクトルと戦術を用いて確実に成功させるため、多層的な防御戦略が必要です。



企業向け

- ▶ **RDPセキュリティの強化**
データを暗号化するRDPソリューションを使用し、多要素認証を使用して、他のデバイスにリモートアクセスする際のセキュリティを向上させます。
- ▶ **フィッシングについての社内トレーニング**
多くのサイバー攻撃は、社員のフィッシングやスパムに対する意識を高めることで防ぐことができます。定期的にサイバーセキュリティ意識向上トレーニングやフィッシングシミュレーションを実施することが大事です。また、疑わしいメッセージを報告する仕組みを構築することは、感染を防止するのにとても重要です。
- ▶ **サイバーセキュリティ対策を導入**
リアルタイムで脅威インテリジェンスと機械学習を使用したツールを駆使し、数多くの異なる攻撃段階での攻撃を検知して防止するために、多層シールドによる保護できるツールをおすすめします。
- ▶ **被害に対するバックアップや復旧体制の構築**
リモートワークの増加に伴い、より強固なバックアップ・復旧体制が求められます。定期的にバックアップテストを行い、アラートを設定することで、管理者担当者は、システム障害発生時、簡単に問題を発見することができます。



個人向け

- ▶ **メッセージを疑う**
メールのリンクや添付ファイルをクリックしないことはもちろん、個人情報や要求するメール、電話、ソーシャルメディアのメッセージを疑うようにしましょう。
- ▶ **ウイルス対策とVPNでデバイスを保護**
パソコンだけでなく、スマートフォンやタブレットもセキュリティを確保することも重要です。そして、情報漏洩を防ぐために、古いデバイスを捨てる際は、データをすべて削除することを忘れないようにしましょう。
- ▶ **ウイルス対策やソフトを常に最新の状態に**
サイバー犯罪者は、古いバージョンのソフトウェアやオペレーティングシステムの脆弱性を悪用し、システムにマルウェアを侵入させ、情報を盗むことができるため、システムやソフトを常にアップデートすることをおすすめします。
- ▶ **安全なクラウドバックアップを利用**
データを暗号化して保存できるオンラインバックアップと、外付けのバックアップドライブの両方を利用することをおすすめします。使用しない際は接続を切ることが重要です。
- ▶ **強いユニークなパスワード**
パスワードマネージャーを使用し、安全なパスワードを作成して保存することができます。これを使用することで、すべてのパスワードを覚えたり、書き留めたりする必要がなくなります。
- ▶ **マクロを有効にするよう要求するファイルは使用しない**
システムのマクロの有効化を要求するファイルは、脅威コードに感染していることを示す兆候です。マクロには正当な用途があるとはいえ、通常の自宅での利用においては極めて稀です。

より詳しい情報はこちらへ
webroot.com/nastiest2020

