暗号化された攻撃の現状
（2020年版）

SSLのインスペクションや脅威保護が実施されていない状況が露呈

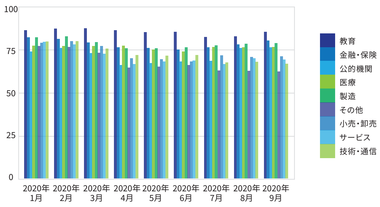
ゼットスケーラーのThreatLabzチームは、
2020年に暗号化されたインターネットトラフィック経由で到着した脅威を分析しました。

レポートを読む

SSLで暗号化されたトラフィックの増加

インターネットトラフィックの最大80%がSSLで暗号化されている

業種別の暗号化されたトラフィックの割合



260%
SSL脅威件数の増加

30%
クラウドベースのファイル共有
サービスから開始するSSLの脅威

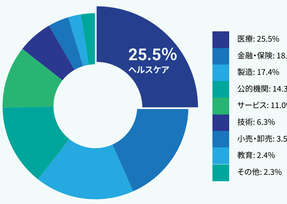
500%
SSL経由のランサムウェアの増加

> サイバー犯罪者は、COVIDのパンデミックが続く状況であっても、倫理的な例外を設けることなく医療機関を無差別に標的にし、暗号化されたチャネル経由で高度な脅威を送り込んでいます。

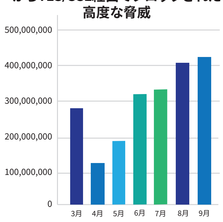
COVID-19に乗じるサイバー犯罪者

医療機関がSSLで
暗号化された脅威の標的に

業種別の暗号化されたチャネル経由でブロックされたマルウェア



代表的なクラウドストレージサービスからTLS/SSL経由でブロックされた高度な脅威

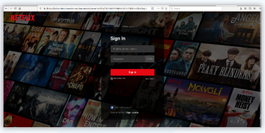


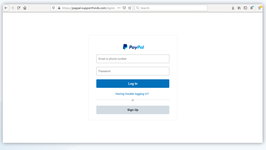
ハッカーによるファイル共有サービスの悪用

Google Drive、OneDrive、AWS、Dropbox
を標的にする攻撃の着実な増加

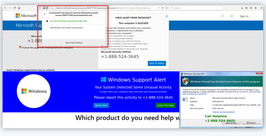
誤字・脱字に潜む脅威

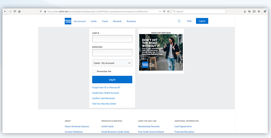
ドメインスクワッティング（ドメイン占拠）攻撃やホモグラフィック攻撃が
SSL脅威の上位を占める

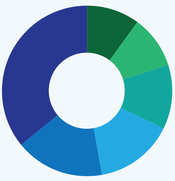




これらの画像は、正規のWebページに見せかけた不正 Webページです。
サイバー犯罪者は、人気のブランドを使って、疑いを持たないユーザを偽のWebサイトに誘導し、ログインの認証情報、PII、財務情報を不正入手し、マルウェアを実行します。







フィッシングに最も多く悪用された企業ブランド

- Microsoft: 36%
- テクニカルサポート: 17%
- PayPal: 15%
- ウェブメール: 12%
- Google: 10%
- OneDrive: 10%

ゼットスケーラーのグローバル脅威調査チームであるThreatLabZ は、
年次レポート「暗号化された攻撃の現状」で、66億件以上のセッションを分析しました。
調査結果が示すように、SSLで暗号化されたトラフィックに隠れる脅威が増加していることから、暗号化されたトラフィックが安全なトラフィックを意味するものではないことをセキュリティチームが認識することが重要です。この攻撃ベクトルがさらに拡大すれば、すべてのSSLトラフィックのインスペクションの必要性もさらに高くなります。

レポートを読む

zscaler

zscaler.jp