ランサムウェアが「人質」を取る仕組み

ランサムウェア攻撃およびそれらが
配布される方法を理解する

SONICWALL™

はじめに

ランサムウェアはマルウェアの一種です。被害者がサイバー犯罪者に身代金を支払うまで、被害者がデータやシステムにアクセスできないようにします。ランサムウェアは数年前から存在していましたが、近年、より一般的になり、被害額も増加しています。CryptoLocker、CryptoWall、RSA4096 などは、広く知られているランサムウェアの例です。

FBI によれば、米国で 2016 年第 1 四半期に支払われた身代金の額は 既に 2 億 9 百万ドルを超えている[1] とのことで、これは前年度のランサムウェア被害合計額の 2,500 万ドルを大きく上回ります。

[1] http://sd18.senate.ca.gov/news/4122016-bill-outlawing-ransomware-passes-senate-committee

SONICWALL™

ランサムウェアの仕組み

ランサムウェアは、さまざまな方法で被害者に悪意のあるアプリケーションをダウンロード、インストールさせることによってシステムに侵入します。デバイスへの侵入に成功したら、このアプリケーションはシステム全体に広がり、ハードドライブのファイルを暗号化したり、単純にシステムそのものをロックしたりします。画像やメッセージをデバイスの画面に表示してシステムへのアクセスをブロックする場合もあります。こうして、ファイルやシステムを解放するために必要な暗号鍵と引き換えにマルウェアの運用者に対して身代金を支払うようにユーザーに要求します。

デジタル通貨は追跡が困難なことから、ビットコインは、ランサムウェアの身代金の支払い方法として一般的に使用される方法の 1 つです。

フィッシングメール

ランサムウェアを配布する最も一般的な方法はフィッシングメールです。これらの電子メールは、受取人に電子メールを開けさせて、Web サイトのリンクをクリックするように誘導します。誘導先のサイトは、機密情報の入力を求めたり、ランサムウェアなどのマルウェアが含まれていたりします。ここからランサムウェアが被害者のシステムにダウンロードされます。

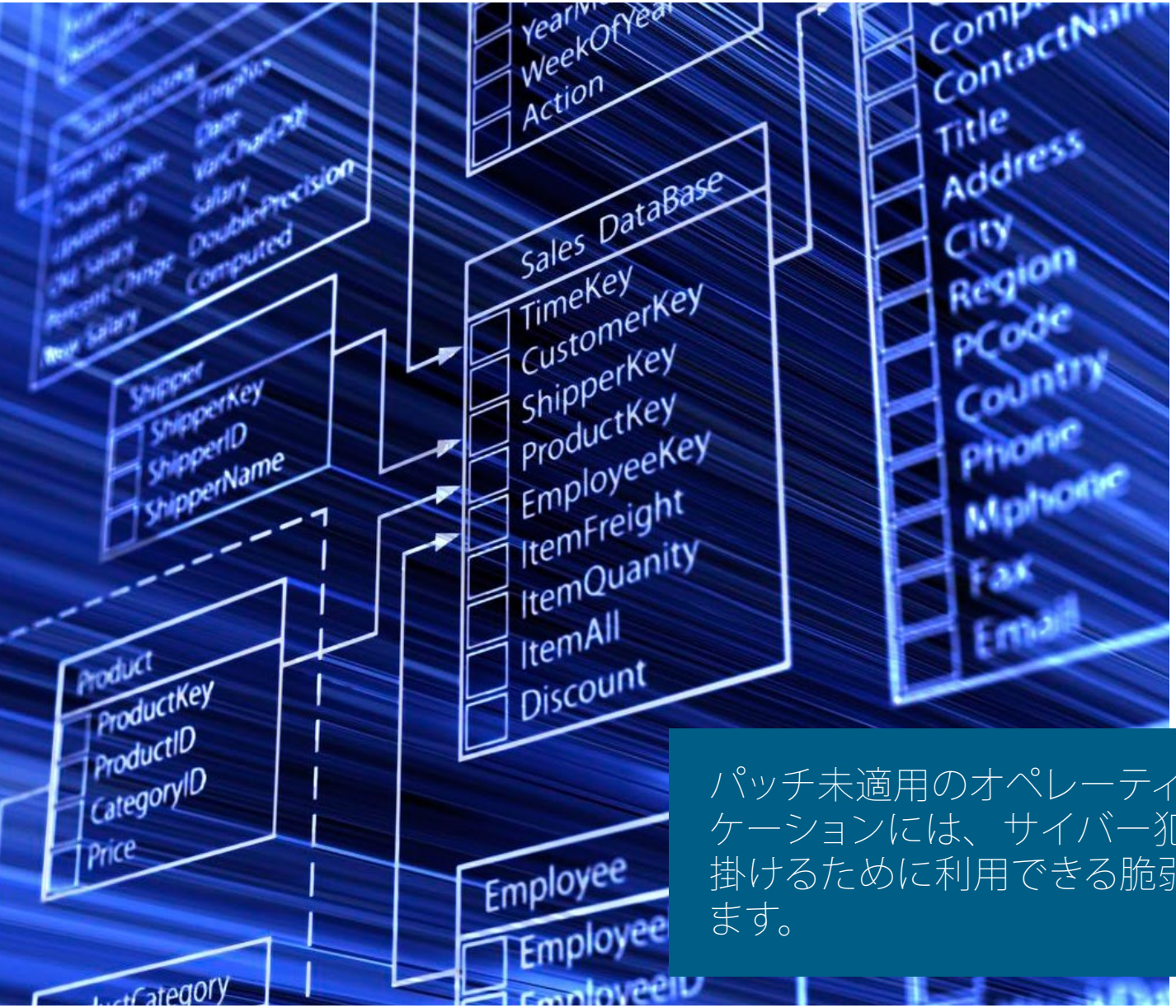
フィッシングメールの受取人の 23% がメールを開封し、11% が添付ファイルをクリックしています。[2]

[2] ベライゾン社の2015年度データ漏洩/侵害調査報告書

不正広告

ランサムウェアを配布するもう 1 つの一般的な方法は「不正広告」です。これはオンライン広告を利用してランサムウェアを拡散する悪意のある広告手法です。攻撃者は、広告用ネットワークに侵入し、場合によっては偽物の広告や代理店を掲示し、マルウェアが含まれた広告を合法的な Web サイトに挿入します。悪意に気づかずサイトにアクセスしたユーザーのシステムは、この宣伝をクリックするまでもなく、感染してしまいます。

ランサムウェアを起動するだけでなく、「不正広告」は、顧客のクレジットカード番号、社会保障番号、その他の機密情報を盗み出すために使用されます。



パッチ未適用のシステムおよびアプリケーションの悪用

多くの攻撃者はオペレーティングシステム、ブラウザ、一般的なアプリケーションの既知の脆弱性を悪用します。サイバー犯罪者は、これらの脆弱性を悪用して、最新のソフトウェアパッチが適用されていないシステムに対してランサムウェア攻撃を仕掛けます。

パッチ未適用のオペレーティングシステム、ブラウザ、アプリケーションには、サイバー犯罪者がランサムウェア攻撃を仕掛けるために利用できる脆弱性が含まれている可能性があります。

外部デバイス

USB ドライブなどの外部デバイスは、ファイルの格納や転送に使用されます。これらは、複数のシステムにわたってランサムウェアを拡散する手段として格好の標的です。これらのファイルには、マクロなどの高度な機能も含まれており、ハッカーはファイルが開かれるとランサムウェアが実行されるように悪用します。

Microsoft 社 は、Office 2016 でこの脅威に対抗するべくセキュリティを強化したもの の、Microsoft Word、Excel、PowerPoint は、 サイバー犯罪者にとって主要な標的になっています。

従来の手法ではランサムウェア攻撃を防ぐことができない理由

多くの従来型セキュリティ制御ではランサムウェアを検出できません。普段と異なる動作や侵害の標準的な兆候を発見するのが精一杯です。システムに一度インストールされてしまえば、ランサムウェアはセキュリティアプリケーションと同じように動作して、他のシステムやプログラムへのアクセスをブロックできます。通常は、その配下にあるファイルやシステムには感染せず、インターフェースへのアクセスを制限するだけです。

ランサムウェアは、ソーシャルエンジニアリングと組み合わせることで、極めて効果的な攻撃になります。

隠されたランサムウェア

ランサムウェアはファイアウォールで検出されません。ファイアウォールはSSL 暗号化された Web トラフィックを復号して検査することができないためです。従来のネットワーク セキュリティ ソリューションでは通常、SSL/TLS 暗号化されたトラフィックを検査できません。できたとしても、検査を実施するとパフォーマンスが大幅に低下するため実用的ではありません。こうした背景から、マルウェアを暗号化されたトラフィックに隠す術を熟知したサイバー犯罪者が増えているのです。

Secure Sockets Layer/Transport Layer Security (SSL/TLS) 暗号化が急速に普及しており、その結果として、検出されないハッキングが増えて、2015 年度には少なくとも 9 億人のユーザーが影響を受けました。[3]

[3] 2016 デルのセキュリティ脅威に関する年次レポート

結論

SonicWall は、あらゆるパケットを検査し、あらゆる ID を管理することによって、組織全体の保護を強化できます。その結果、データの場所を問わず、保護することが可能になり、インテリジェンスを共有して、ランサムウェアを含めた多様な脅威から守ることが可能になります。

SonicWall ネットワークセキュリティ製品の Web ページをご覧ください。

当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、E メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com

Ebook-NS-Ransomware-US-KJ-29223 -D1

SONICWALL™