2020 年 11 月 20 日

サービス＆セキュリティ株式会社 e-Gate センター

Ryuk ランサムウェアの特徴と対策

1. 概要

国内、海外ともに、企業や公的機関のランサムウェアによる被害報告が増加しています。最近では特に、新型コロナウイルスの感染拡大に便乗して、Web サイトやメールを介して感染するケースが顕著です。その中でも海外では、病院や市の自治体などを狙った標的型攻撃ランサムウェア「Ryuk」による被害が後を絶ちません。Ryuk の登場は 2018 年と比較的古いですが、2020 年現在も増加し続けているマルウェアの 1 つです。Ryuk は海外で多く確認されている一方、国内では大規模な被害に至った事例はありません。しかしながら、主な感染経路として国内でも多く確認されているマルウェア「Emotet」を経由するため、今後国内の組織も標的となる可能性が考えられます。今回は Ryuk ランサムウェアについて、その特徴と対策を紹介します。

2. Ryuk ランサムウェアについて

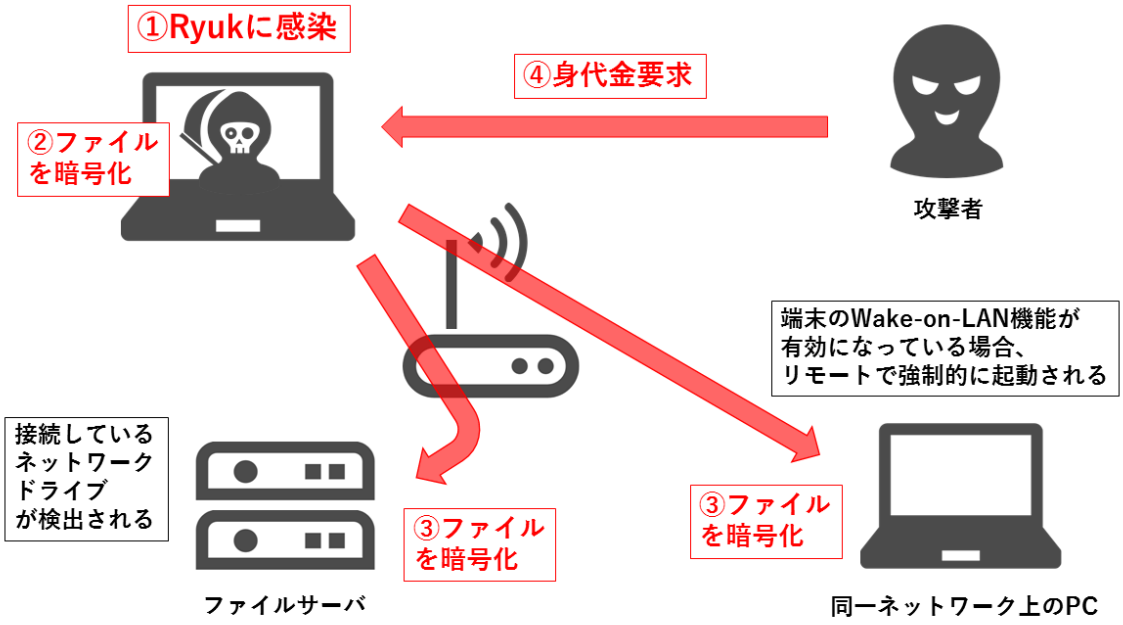
2.1. ランサムウェアとは

ランサムウェアは「身代金要求型不正プログラム」とも呼ばれるマルウェアです。感染した PC をロックしたり、ファイルを暗号化したりして使用できない状態にします。攻撃者は PC やファイルを元に戻すことと引き換えに、被害者に身代金を要求します。また、支払いを拒否すると機密情報を公開するよう脅す「二重脅迫」も増加しており、実際に身代金を支払った事例も数多くあります。

2.2. Ryuk の特徴

Ryuk は標的型攻撃（特定の組織を狙った攻撃）を行う際に用いられるランサムウェアの一種です。不特定多数の個人ではなく特定の組織を標的としており、攻撃者は他のランサムウェアと比べて高額な身代金を要求します。数百万ドルを要求されることもあります。

Ryuk はコンピュータ上のファイルを暗号化するだけでなく、接続しているネットワークドライブを検出して暗号化することができます。また、ネットワーク上の端末の電源をリモートで ON にする Wake-on-LAN と呼ばれる技術を悪用し、シャットダウンしている端末でも Ryuk により遠隔で電源を投入され暗号化の対象にされてしまいます。さらに権限昇格に成功した場合、管理者権限を悪用して Windows のシステム復元オプションを無効にすることも可能であるため、外部にバックアップがなければ回復は困難です。



【図 1】Ryuk による攻撃の流れ

2.3. Ryuk の感染経路

Ryuk は、以下の流れで PC に感染します。

[1] 主にメールの添付ファイルから、PC がマルウェア Emotet（※）に感染する。

[2] Emotet は外部と通信して、同じくマルウェアの「Trickbot」をダウンロード、実行する。

Trickbot はトロイの木馬の一種で、Emotet と同じく国内でも数多く確認されています。

[3] Trickbot は感染したコンピュータの情報を収集したのち、Ryuk を展開する。

※Emotet の詳細は以下 URL をご参照ください。

『注意喚起:進化するマルウェア「Emotet」について』

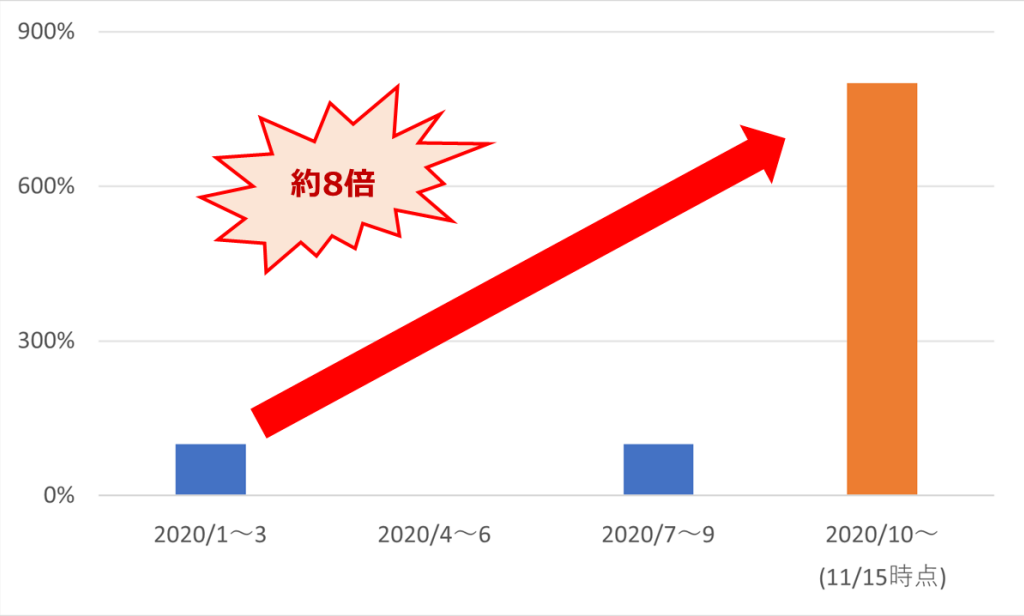
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9657

『マルウェア「Emotet」(エモテット)最新攻撃メールについて』

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10400

3. e-Gate センターにおけるランサムウェア関連の攻撃イベント

e-Gate センターでもランサムウェア関連の攻撃イベントは増加傾向にあります。今年の 8 月までと比較して、9 月から検知数が大幅に増加しています。概要でもご紹介した通り、国内企業のランサムウェア被害報告は増加しており、今後も検知数が増加する可能性が高いと考えられます。



【図 2】e-Gate センターにおけるランサムウェア関連の攻撃イベント数の推移

4. 今後に向けて

Ryuk による大規模な被害は国内では確認されていませんが、Emotet や Trickbot から感染し、被害が増加する可能性もあるため注意が必要です。国内のランサムウェアによる被害件数は世界各国と比べると比較的少ないものの、1 件あたりの被害額は高額です。

ランサムウェアにもさまざまな種類があり、2017 年には「WannaCry」、2018 年には「GandCrab」、2019 年には「Sodinokibi」などが猛威を奮いました。攻撃者が仕掛ける手口は年々巧妙化されています。今後も新たなマルウェアが登場し、情報資産が危険にさらされる可能性があります。

組織では一人一人が最新のセキュリティ事情を認識し、日ごろの業務に注意を払う仕組みづくりが重要になってきます。次章にて対策を紹介します。

5. 対策

Ryuk を始めとするランサムウェアの感染原因として、メールを介するケースや、不正サイトへのアクセスなどが主に挙げられます。以下のような対策が有効です。

・不審なメールのリンクや添付ファイルを開かない。

・不審なメールや Web サイトから、プログラムを安易にインストールしない。

・例え自身が送信したメールへの返信メールであっても、不自然な点があれば添付ファイルを開かない。（Emotet の可能性がある）

・マクロが無効化されていることを確認し、文書ファイルのマクロは有効化しない。

・メールや文書ファイルを閲覧しているとき、身に覚えのない警告ウインドウが表示された場合、警告の意味が分からない場合は操作を中断する。

・セキュリティソフトを導入し、外部の不正なサイトへのアクセスをブロックする。
・OS やアプリケーション、セキュリティソフトを常に最新の状態にする。
・重要なファイルなどはバックアップし、別のネットワークなど隔離された場所に保管する。
・組織内への注意喚起を行う。

今回のようなケースでは、感染前の不正なダウンロード通信、感染後の不正な通信などを、ファイアウォールや IPS、UTM といったセキュリティ機器により検知、防御することで、被害を最小限に抑えることができます。
日々セキュリティ機器のログを監視するアウトソーシングサービスの活用は、コストメリットのある有効な対策となります。

6. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。
また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。
監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス「e-Gate」 e-Gate
SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。
【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp