ランサムウェアの現状

2020 年オーストラリア／ニュージーランド市場の業界アップデート

BlackBerry®

2020 年前半、オーストラリア／ニュージーランドの大企業の間でサイバーインシデントの報告が明らかに増加しました。これらの攻撃の大半を占めているのは、一握りのランサムウェアファミリーです。このペーパーでは、これらのランサムウェアファミリーで用いられる戦術とその有名な被害者、およびこれらの脅威に対する防御に使用する戦略を調査します。

多くの組織が侵害を報告しないのは珍しいことではありません。それどころか、侵害が起きたことにまったく気付いていないこともよくあります。ランサムウェアは、恐喝以外にもさまざまな目的で使われています。たとえば、相手の気をそらすために使用されることがあります。まず、後で使用するために認証情報を奪い、次にドライブを暗号化して IT スタッフが対応にかかりきりになるようにし、その間に攻撃者は自分の足跡を消すというものです。

最近では、攻撃者は重要なデータをダークウェブに送信したり、オークションに出品して最高入札者に販売したりといった、より悪質な目的を達成しています。

多くの組織が侵害を報告しないのは珍しいことではありません。それどころか、侵害が起きたことにまったく気付いていないこともよくあります。

Everything as a service

ハッキングスキルがほとんどまたはまったくない攻撃者でも、Ransomware as a Service（RaaS）という方法でランサムウェアを簡単に入手して使用できます。アフィリエイトパートナーのネットワークを築くことで、マルウェアの作者は自身のランサムウェアを広く拡散し、その過程で収益を劇的に増加させることができます。

多くの脅威アクターは、消費者を狙った大規模な攻撃から進化しつつあり、混乱を最大化することを目的とした、より周到に計画された標的型攻撃を選ぶようになっています。マルウェアの作者は、RaaS モデルを使用することでこのような攻撃を実行する際のハードルを大きく下げています。そのため、より多くの潜在的な犯罪者集団がこの特定のサイバー犯罪形態を利用して利益を上げることができるようになっています。

弊社のお客様の多くは、ランサムウェア攻撃の防止にきわめて効果的であるという理由から BlackBerry を選んでいます。いずれのケースでも BlackBerry は、マルウェアの被害が初めて検出された日より平均 1,000 日以上前に、アップデートなしに脅威を分析、予測、防止できました。

大きく報道された オーストラリア／ニュージーランドの事例

Toll Group はメルボルンに拠点を置くグローバルなロジスティクス企業で、2020 年 1 月に MailTo、6 月に Nefilim と 2 回のランサムウェア攻撃を受けました。また 6 月には政府機関の ServiceNSW、鉄鋼メーカーの BlueScope、金融サービス企業の MyBudget も注目度の高いサイバー攻撃を受け、大きく報道されました。

BlackBerry

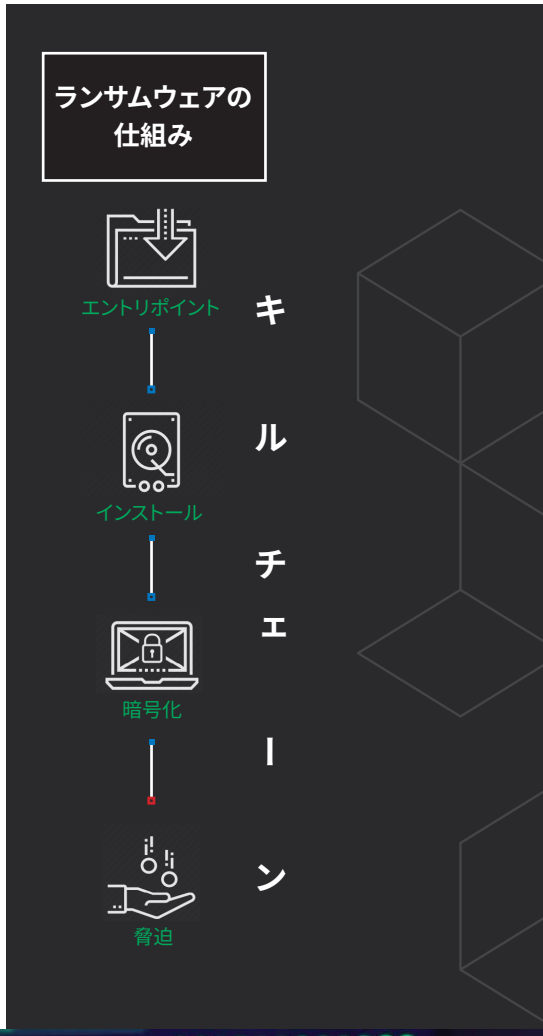
攻撃の分析 – Emotet、Trickbot、Ryuk

ランサムウェアはさまざまなベクトルを使用してコンピューターにアクセスすることができます。

最も一般的な配信システムの 1 つがフィッシングです。これは、信頼できるソースからのファイルを装ってメールの添付ファイルとして被害者に送られます。ほとんどの場合、正当なメールに見せかけるため、巧妙なソーシャルエンジニアリングが使用されます。たとえば Emotet は、メールファイルを収集し、以前にやり取りした内容を使って同僚宛のメールを巧妙に生成します。Emotet マルウェアは、TrickBot キャンペーンのローダーとして使用されるのが一般的です。TrickBot は、ロードされると、複数のモジュールを使用して被害者のシステムでさまざまな活動を実行します。TrickBot は水平移動が可能で、オペレーターがユーティリティを手動でロードできるようにします。侵入後の悪用ツールをロードしたら、ドメインコントローラー（DC）を攻撃します。DC への特権アクセスを取得すると、ボットネットオペレーターの意のままに、Ryuk などのランサムウェアをネットワーク経由で展開することができます。

公開されているもう 1 つの脆弱性はリモートデスクトッププロトコル（RDP）です。RDP はリモートアクセスを可能にするために使用されますが、そのセキュリティには以前から問題があり、ブルートフォースや悪用による攻撃につながります。恐らく最も悪名高いランサムウェアの例である WannaCry も、悪用可能なネットワークプロトコルを利用していました。

残念ながら、アンチウイルスエージェントのような従来型の防御手段は、攻撃者が簡単に無効化できるため、ランサムウェアを阻止できるとは考えられません。



BlackBerry®

真の予測防御

弊社のお客様の多くは、ランサムウェア攻撃の防止にきわめて効果的であるという理由から BlackBerry を選んでいます。次の表は、オーストラリア／ニュージーランドで最も目立つランサムウェアファミリーとの関連から、BlackBerry の優位性を示しています。いずれのケースでも BlackBerry は、マルウェアの被害が初めて検出された日より平均 1,000 日以上前に、アップデートなしに脅威を分析、予測、防止できました *。

	Phobos	Ryuk	Sodinokibi/ Sodin/Revil	Zeppelin	Ako	Mailto	Nefilim	STOP/Djvu	Maze
初検出年／月	2018 年 12 月	2018 年 8 月	2019 年 4 月	2019 年 11 月	2020 年 1 月	2019 年 8 月	2020 年 3 月	2018 年 12 月	2019 年 5 月
BlackBerry の優位性	1,229 日	1,340 日	1,343 日	1,496 日	1,000 日	1,567 日	1,448 日	1,714 日	1,464 日
前身	CrySiS/ Dharma	Hermes	GandCrab	VegaLocker/ Buran/ Jamper/ Delphi	Medusa Locker（2019 年 9 月）	Netwalker、KoKo	Nemty	新ファミリー	新ファミリー
展開手法	スパム、RDP 認証情報	スピアフィッシング、エクスプロイト	Oracle Weblogic、MSSP	MSSP	RDP エクスプロイト / 盗んだ認証情報	フィッシング、DLL インジェクション	RDP エクスプロイト	クラックおよびアドウェア	メール、RDP、エクスプロイト
標的	無差別	大企業と大規模機関	大手 MSSP とその顧客	MSSP による有名な被害者	大企業と大規模機関	大企業と大規模機関	大企業と大規模機関	無差別	大企業と大規模機関
暗号アルゴリズム	RSA1024+ AES256	RSA4096+ AES256	Curve25519+ Salsa20+ AES256	RSA4096+ AES256	RSA2048+ AES	Curve25519+ Salsa20+ ChaCha	RSA2048+ AES128	Salsa20	RSA2048+ ChaCha
拡張子	.phobos	.ryk	ランダム	ランダム	ランダム	ランダム	.nefilim	.djvu、.tro など	ランダム
支払要求額	0.1 ～ 2 BTC	15 ～ 50 BTC	5 ～ 300 BTC	不明	$3,000	不定	不定 + 流出	～ $1,000	不定 + 流出

事後対応型から防御ファースト型へセキュリティ体制を移行してランサムウェアによる侵害リスクを最小化する方法については、弊社までお問い合わせください。

* 出典：SE Labs Report。BlackBerry は 2019 年 2 月に Cylance を買収しました。SE Labs は CylancePROTECT® ソリューションで調査を実施し、このソリューションは現在、BlackBerry® Protect という名称に変更されています。

BlackBerry について

BlackBerry（NYSE：BB；TSX：BB）は、インテリジェントなセキュリティソフトウェアとサービスを世界中の企業と政府機関に提供しています。BlackBerry のソリューションは、1 億 7,500 万台の自動車をはじめ、5 億以上のエンドポイントを保護しています。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

BlackBerry Intelligent Security. Everywhere.

BlackBerry のインテリジェントなセキュリティをあらゆる場所に。

お問い合わせ

詳細については、BlackBerry.com にアクセスし、@BlackBerry をフォローしてください。