SecurityScorecard

SecurityScorecard社ブログ

発行日：2021年8月30日

執筆：SecurityScorecard 中村 悠
編集：SecurityScorecard 中島 朝可・橋本 詩保

脅威インテリジェンスを利用してランサムウェアの被害を“未然”に防ぐ

CryptLocker, WannaCry, BitPaymer, Maze。これまで、多くのランサムウェアが攻撃者の手によって生み出され、金銭搾取を目的とした攻撃に利用されてきました。

その攻撃の特性は時代の変遷とともに変化しているものの、その攻撃自体は現在も引き続き確認されています。
そのため、多くの組織では、その“ランサムウェア”を利用した攻撃に対応しようと、様々なセキュリティ対策を取ってきています。
「攻撃検知の製品を導入して、ランサムウェアの侵入をいち早く検知できるようにする」
「定期的に重要なサーバのバックアップを取る運用に変更し、ランサムウェアの被害にあっても、業務復旧が迅速にできるようにする」

などが挙げられるでしょうか。これらの対応がランサムウェアの被害を最小限に抑える、あるいは防ぐ有効な手段であることは間違いないです。皆様の組織ではどのような対策を取っているでしょうか。

このブログでは、こんな切り口のランサムウェアの攻撃への対策ソリューションを紹介します。
「ランサムウェアを利用した攻撃の特徴から、侵害されやすい環境かどうかを判断する」
SecurityScorecardは最近、ランサムウェアを利用した攻撃の発生の可能性を事前に示唆する機能を追加しました。
これらは、昨今、セキュリティ関連の記事でも目にし始めた「ASM（Attack Surface Management）」に着想した機能でもあります。

【Attack Surface Management】

攻撃者と組織のシステム的な接点に着目し、その接点のシステムにおいて、リスクをマネジメントしようとする動き

それらは、どのような機能でしょうか、実際の画面も例に出しながら説明をしていきます。

続きをご覧になりたい場合は

メーカーBlogへ

https://securityscorecard.com/using-threat-intelligence-to-detect-ransomeware