

2018年10月26日

報道関係各位

株式会社バルクホールディングス
名証セントレックス 2467

サイバージム社『Spy Chip Hack』攻撃に対する

セキュリティトレーニングを開発

サイバーセキュリティ分野における共同事業パートナーであるイスラエル CYBERGYM（サイバージム）社は、高度なフォレンジック分析と報告された攻撃シナリオの複製品を利用し、サプライチェーンとインフラストラクチャのセキュリティに関する不安を解決するトレーニングソリューションの提供を開始いたします。

このトレーニングプログラムは、某国の諜報機関が、Apple や Amazon などの世界的に重要な民間インフラストラクチャ企業や米軍や米諜報部隊において使用されているサーバーに監視チップをインストールしたというメディアの主張に応えて開発されたものです。

ハッカーによるこの攻撃は、ハードウェアサプライチェーン内のサプライヤを通して実施されたという点が重要であり、この点を考慮し、サイバージムのイスラエル R&D センターでは、複雑なハードウェアベースの攻撃に対して防御する効果的な戦略を組織に提供するトレーニングプログラムを開発いたしました。

ハードウェアまたはインフラストラクチャレベルで発生するハッキングを特定し防御するには、高度なフォレンジック分析と広範なトレーニングが必要です。

サイバージムの新開発プログラムは、メモリ、ネットワーク、PLC、オペレーティングシステムなどのフォレンジックレイヤーをすべて網羅し、組織の異常検出スキルを強化します。そのユニークな多層トレーニングは、コアメンバーに重要なフォレンジックデータ収集スキルを与えるだけでなく、組織が攻撃の被害の一部を分析、緩和、修正することを支援いたします。

サイバージムのエンジニアとホワイトハットハッカーは、実際に起こった攻撃シナリオを模倣するために、Bloomberg レポートで特定されたサーベイランスチップのバーチャルモデルを開発し、実戦的なトレーニングとしてプログラムに反映させております。

「私たちのプログラムは多層フォレンジックに基づいており、スタッフの訓練とサイバーセキュリティポリシー強化の両方を実現できるよう設計されています。」（サイバージム CEO Ofir Hason）

このトレーニングシナリオはインフラストラクチャ自体が感染してしまう可能性が高いという点に焦点を当てています。

この種の複雑な攻撃に対処するには、イベントを迅速に分析し、関連するフォレンジックを収集し、IT サプライチェーンのパートナーと協力して攻撃の拡大および進展を軽減および防止する必要があります。

す。このために、実世界で現実に起こったシナリオを即座に解析し、作成されたプログラムをもとに実戦的な訓練することが効果的となります。

この新プログラムは、日本、米国、ヨーロッパ、オーストラリアの CYBERGYM's Arena で受講することができます。

以 上

本サービスに関するお問合せ先



CYBERGYM TOKYO (Strategic Cyber Holdings LLC) <https://www.cybergym.com/ja/>

TEL : 03-6807-4312 FAX : 03-6807-4313

報道関係者様お問合せ先

株式会社バルクホールディングス <http://www.vlcholdings.com/>

経営企画室 TEL : 03-5649-2500 FAX : 03-5649-2710