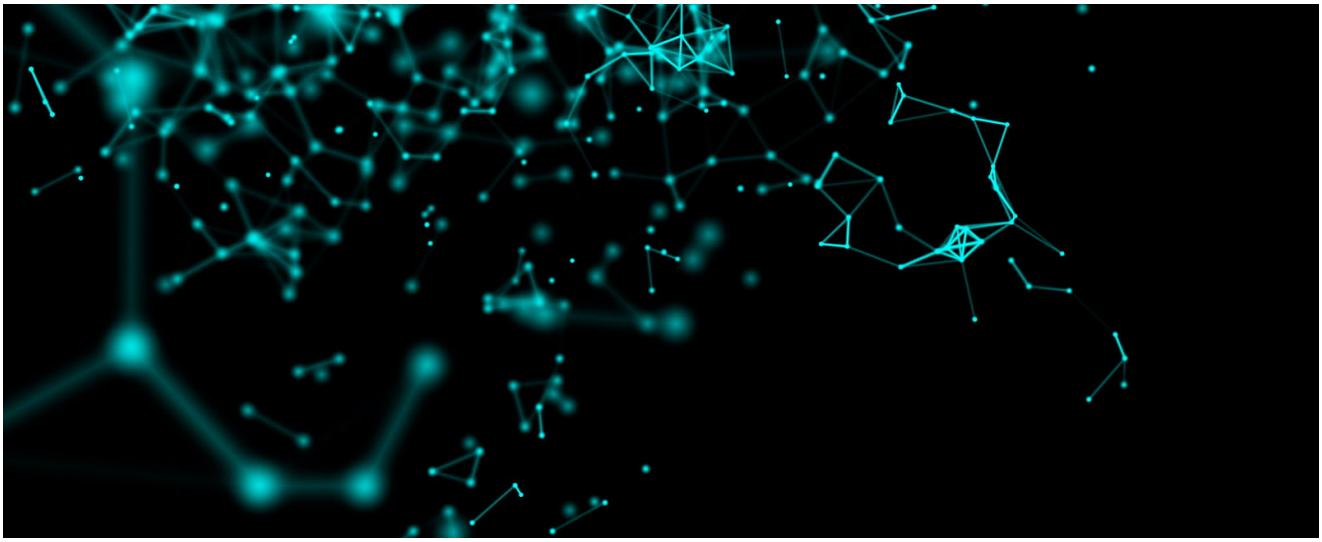
日本企業を狙う高度なサイバー攻撃の全貌 – BRONZE BUTLER



企業内システムに潜む脅威を狩り出す「標的型攻撃ハンティングサービス」を日本において実施した結果、複数の日本企業に対して同一サイバー攻撃グループによるものと思われる標的型攻撃が行われていることを観測し、深刻な被害につながっていることが確認されました。

この標的型攻撃の活動として、2015年に顕在化した日本年金機構を含む複数の国内組織が被害に遭った標的型攻撃（Emdiviマルウェアを使った攻撃）と同様に、いくつかの国内組織におけるシステムの奥深くまで侵入しているものが多く発見されています。被害に遭った企業組織の多くは、警察など第三者から通報があるまで標的型攻撃を受けていることを認識できず、気づいた時点ではすでに長期間にわたり侵入が繰り返されており、多くの知的財産情報窃取やActive Directoryの侵害といった致命的な状況も珍しくありません。

被害企業組織にとって困難な点は、標的型攻撃の手法が一般的な監視や検知の仕組みを迂回する高度なものであり、さらに時間をかけて繰り返し侵入を行うことにより、最終的に組織のネットワークシステム全体に跨る大規模な攻撃となるため、攻撃活動の根絶に多大な時間と労力を要することです。

高度かつ悪質なサイバー攻撃が攻勢をかける環境下において、打つ手のない企業組織側の状況を少しでも改善し、サイバー攻撃グループから自組織および保有する重要な情報を守るために、SecureWorks Japan は本ホワイトペーパーを作成しました。本レポートでは、近年日本企業を執拗に狙う標的型攻撃の実態を明らかにするとともに、検知困難な高度なサイバー攻撃に気づくこと、また自組織でしかるべき取り組みを行うために有益な情報を提供します。

表示する