Dell SecureWorks
標的型攻撃兆候解析サービス

ネットワークセキュリティの分野においては日々新たな脅威の発見や、企業に対する攻撃等が報道されております。 また、攻撃を行う者も、これまでのような無差別に攻撃を行う愉快犯から、特定の企業等を標的として営利目的において攻撃を行う犯罪者や組織へと変貌しております。

特に、昨今話題となっている標的型攻撃は組織の重要なIT資産を盗み出すことを主な目的としており、企業や組織に対して非常に大きなリスクとなっています。

問題は、このような攻撃を受けている現状が可視化し難いというところにもあります。情報の漏えいが開始されてから、検出されるまで数か月も状況を把握できないケースも見受けられます。

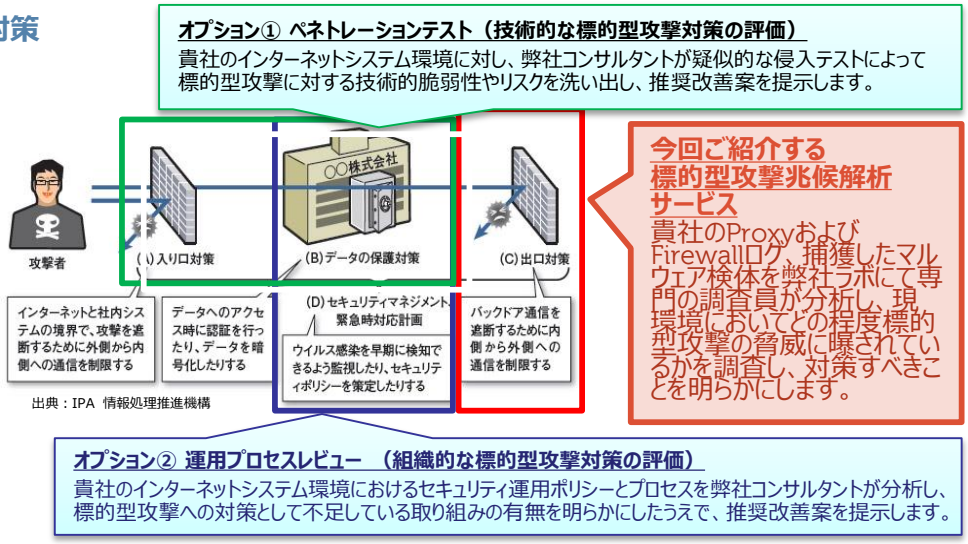
本サービスでは、お客様のProxyおよびFirewallログを弊社ラボにて専門の調査員が分析し、現環境においてどの程度標的型攻撃の脅威に曝されているかを調査し、対策すべきことを明らかにします。これにより、セキュアなIT活用の実現、確かな費用対効果、意思決定の迅速化を実現することができます。

標的型攻撃兆候解析サービスの特長

- 短期間のアセスメントで、今後お客様がすべきセキュリティ対策を明らかに
- 3,800社以上へのセキュリティ対策の豊富な実績と信頼、高い技能、迅速な対応により、確実な成果をご提供
- 全世界8か所のSOC及び専門の解析部門による全世界のセキュリティ状況を、お客様向けのサービスに反映し、今有効な対策をご提供

■ 標的型攻撃への包括的な対策

デル SecureWorks では、包括的なセキュリティ対策サービスをご提供しております。今回ご紹介する標的型攻撃兆候解析サービスだけでなく、模擬テストの実施や、運用プロセスのレビュー、さらにはセキュリティ運用監視まで、様々なサービスをご提供させていただきます。



■ デル SecureWorks が提案する「標的型攻撃兆候解析サービス」の内容

「標的型攻撃兆候解析サービス」 はお客様のインターネット接続部に設置されているファイアウォール、プロキシから出力されるログや、マルウェア検知システムによって捕獲された検体をお預かりし、弊社ラボのセキュリティエンジニアが解析し、結果報告を行います。

解析方法

- 3,800社の顧客に提供中のマネージドセキュリティサービスから検知したC&Cサーバのリストと、貴社のセキュリティログを比較分析し、ATP攻撃を受け感染したPCが初期動作時に接続を行う通信が発生していないか確認を行います。

解析対象

- お客様のグローバルネットワークにおける全てのインターネット出口を対象とできます。
- 日本からの出口のみとすると、お客様のネットワークが閉域網として後ろでつながっていますと、他の出口にRouteされて出てしまっていることが考えられる為、必ずしも問題が発見されない恐れがあります。

サービス要件

- 解析対象期間：1か月
- 分析、報告期間：ログおよび検体取得後、1か月～1.5か月（要調整）
- 納品物：標的型攻撃検知サービス報告書
- 報告会：1～1.5時間程度