FUJITSU

クイックセキュリティ診断

Infoblox DNS Firewall ～疑わしい通信を可視化できます～

ネットワークに潜む隠れたボット型マルウェア・APTによる感染状況を可視化

こんなご心配はありませんか？

1.ドライブバイダウンロード、APT攻撃などのサイバー攻撃の懸念
2.次世代ファイアウォール、アンチウィルスでは検出困難なマルウェア感染の懸念
3.自社ネットワークの隠れたマルウェア感染の懸念
4.外部サーバとの不正な通信を把握できているかの懸念
5.自社のネットワーク接続端末がボット化している懸念

診断対象の通信

・HTTP, HTTPSトラフィック
・Emailトラフィック
・ポート53番を利用したトラフィック

診断から分かる脅威

・C&Cサーバと通信が行われている脅威
・隠れたボット型マルウェア
・感染クライアントの特定

クイック診断コース

自社ネットワークに隠れたボット型マルウェアの感染端末が存在するか、**すぐ確認したいお客様**にお勧めです。

【準備物】
DNSキャッシュサーバへアクセスするパケットキャプチャー(10分間以上)
【診断レポート】
取得いただいたキャプチャーをInfobloxアナリストが解析し診断結果をご提供いたします。

※その他にも、Infoblox DNS FireWall製品を使って『じっくり』診断するコースもございます。

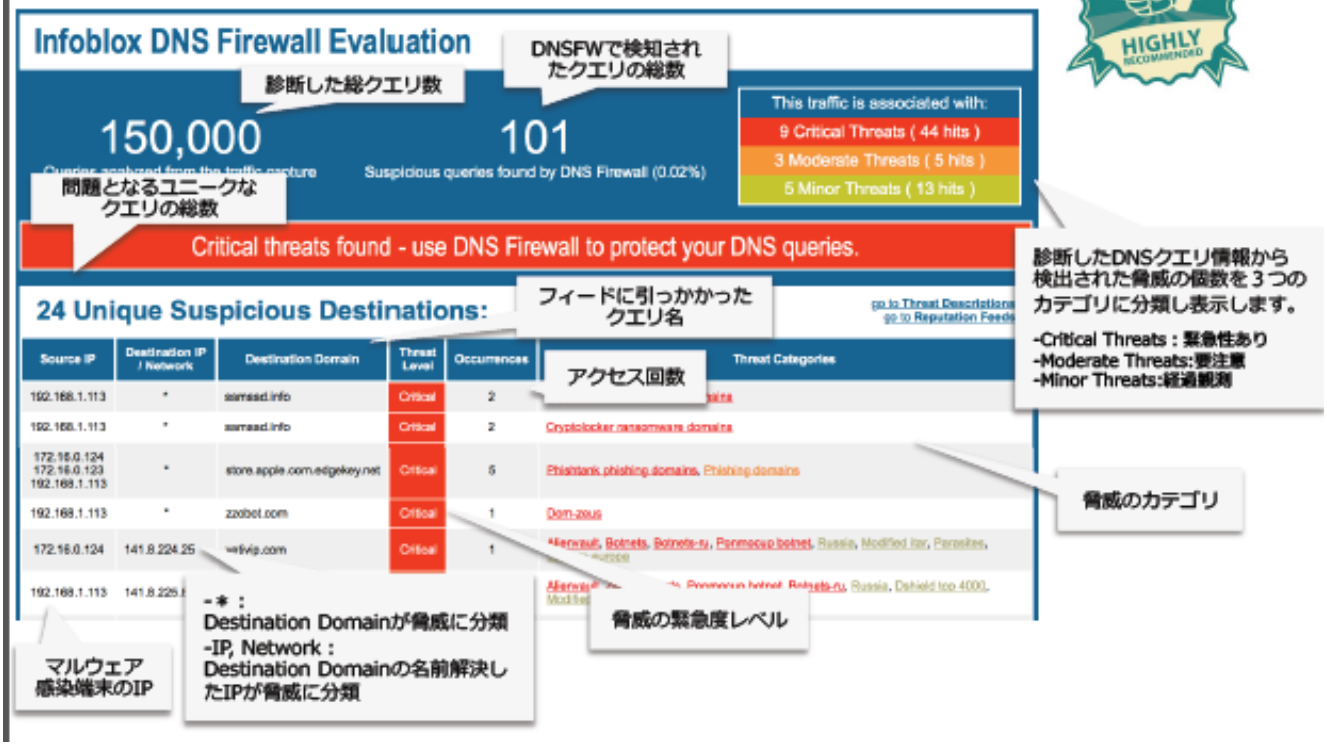
診断結果から、お客様に合った適切な「マネージド・セキュリティサービス（MSS）」をご提案いたします。

※ MSS：セキュリティ脅威のリアルタイム監視・分析を実現

■ Infoblox DNS Firewallとは？
マルウェアによるアウトバウンドのDNSベースの通信を遮断することで、ボットネットおよびC&Cサーバとの接続を防ぎます。

■Infoblox DNS Firewallの主な機能
・悪意のあるドメインへのDNSクエリの監視・遮断
・感染端末の可視化
・Fast-Fluxプロセスを利用した悪意のあるドメインのIPアドレスの急速な変化を反映した２時間毎のデータフィード自動更新
・地理的条件に基づくブロッキング（例：北朝鮮、イラン、ロシア、シリアなど）

シンプルで分かりやすい診断結果
Infoblox DNSセキュリティレポート

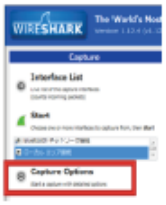


Infoblox DNSセキュリティ診断サービス
パケットキャプチャー取得方法

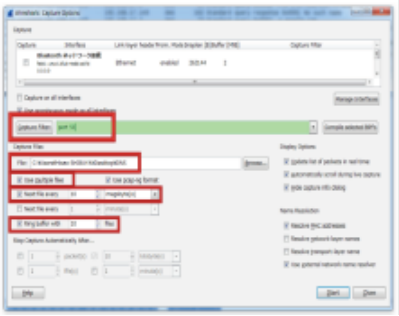
🌟 ここがポイント
Infobloxの診断サービスで必要なキャプチャーデータは、DNSクエリ情報だけでOK!!

■ Windows端末からのパケットキャプチャー取得

Wiresharkのインストール（以下URLからダウンロードしてインストール）
https://www.wireshark.org/download.html



- インターフェースの選択
  Span Portが接続されているインターフェースを選択
- Capture Options をクリック
  - Capture Filter: に"port 53"を設定
  - Capture Filesに保存場所とファイル名を設定
  - Use multiple filesをチェック
  - Next file everyを10 megabyte(s)に設定
  - Ring bugger withを10 filesに設定
- Startをクリックしキャプチャ開始
  10MB x 10ファイル取得後に自動的に終了します。



※記載の会社名、商品名は、各社の商標または登録商標です。
※記載された情報は、予告なく変更することがあります。
※記載の内容は、2015年6月現在のものです。

お問い合わせ先
株式会社富士通ソーシアルサイエンスラボラトリ（富士通SSL）

お問い合わせ総合窓口
〒211-0063 川崎市中原区小杉町1-403武蔵小杉タワープレイス
E-mail : ssl-info@cs.jp.fujitsu.com
当社ホームページ http://www.ssl.fujitsu.com