THE NEW VALUE FRONTIER

KYOCERA

SecureOWL

Darktrace「Enterprise Immune System」

内部ネットワーク見える化診断サービス

標的型攻撃や内部犯行など、既存の対策では検知できない
未知の脅威をDarktraceの内部ネットワーク可視化により検知

https://www.kccs.co.jp/secureowl/solution/internal/darktrace/

サービス概要

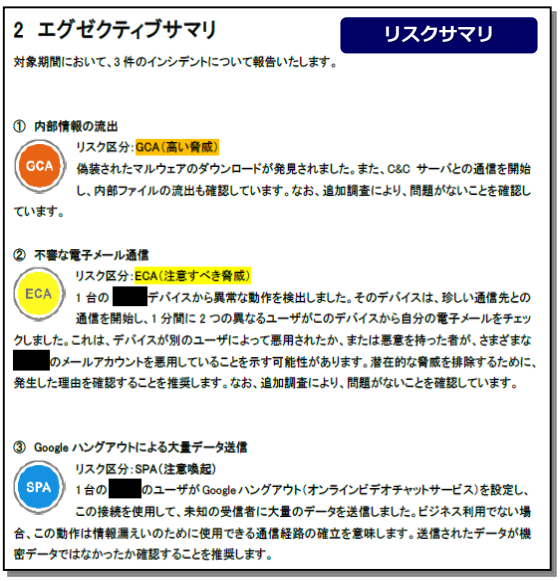
ネットワークの状況を把握し未知の脅威を検知するDarktraceをお客様環境へ設置。
Darktraceの検知内容を当社エンジニアが分析し、レポートを提供します。


サンプル株式会社　御中

Darktrace 脅威情報レポート
【サンプル】

2017年2月14日
京セラコミュニケーションシステム株式会社
セキュリティ事業部

No:　KCCS-xxx-xxxx-xx-xx

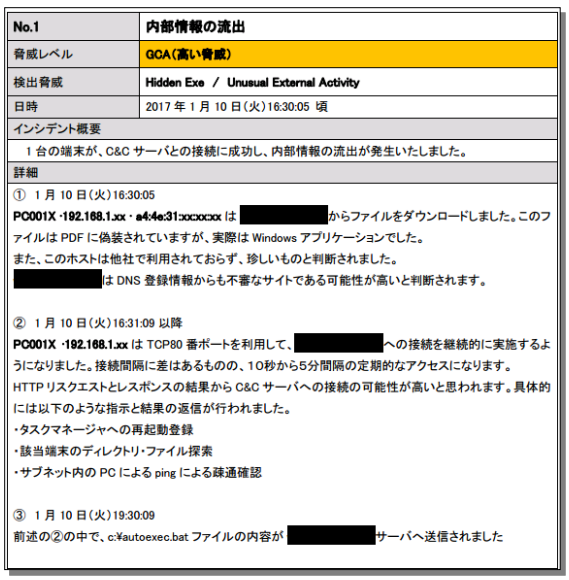

2　エグゼクティブサマリ　リスクサマリ

対象期間において、3 件のインシデントについて報告いたします。

① 内部情報の流出
リスク区分：GCA（高い脅威）
GCA　偽装されたマルウェアのダウンロードが発見されました。また、C&C サーバとの通信を開始し、内部ファイルの流出も確認しています。なお、追加調査により、問題がないことを確認しています。

② 不審な電子メール通信
リスク区分：ECA（注意すべき脅威）
ECA　1 台の [redacted] デバイスから異常な動作を検出しました。そのデバイスは、珍しい通信先との通信を開始し、1 分間に 2 つの異なるユーザがこのデバイスから自分の電子メールをチェックしました。これは、デバイスが別のユーザによって悪用されたか、または悪意を持った者が、さまざまな [redacted] のメールアカウントを悪用していることを示す可能性があります。潜在的な脅威を排除するために、発生した理由を確認することを推奨します。なお、追加調査により、問題がないことを確認しています。

③ Google ハングアウトによる大量データ送信
リスク区分：SPA（注意喚起）
SPA　1 台の [redacted] のユーザが Google ハングアウト（オンラインビデオチャットサービス）を設定し、この接続を使用して、未知の受信者に大量のデータを送信しました。ビジネス利用でない場合、この動作は情報漏えいのために使用できる通信経路の確立を意味します。送信されたデータが機密データではなかったか確認することを推奨します。



No.1	内部情報の流出
脅威レベル	GCA（高い脅威）
検出脅威	Hidden Exe / Unusual External Activity
日時	2017 年 1 月 10 日（火）16:30:05 頃
インシデント概要	
1 台の端末が、C&C サーバとの接続に成功し、内部情報の流出が発生いたしました。	
詳細	
① 1 月 10 日（火）16:30:05 PC001X -192.168.1.xx - e4:4e:31:xx:xx:xx は [redacted] からファイルをダウンロードしました。このファイルは PDF に偽装されていますが、実際は Windows アプリケーションでした。 また、このホストは他社で利用されておらず、珍しいものと判断されました。 [redacted] は DNS 登録情報からも不審なサイトである可能性が高いと判断されます。 ② 1 月 10 日（火）16:31:09 以降 PC001X -192.168.1.xx は TCP80 番ポートを利用して、[redacted] への接続を継続的に実施するようになりました。接続間隔に差はあるものの、10 秒から 5 分間隔の定期的なアクセスになります。 HTTP リクエストとレスポンスの結果から C&C サーバへの接続の可能性が高いと思われます。具体的には以下のような指示と結果の返信が行われました。 ・タスクマネージャへの再起動登録 ・該当端末のディレクトリ・ファイル探索 ・サブネット内の PC による ping による疎通確認 ③ 1 月 10 日（火）19:30:09 前述の②の中で、c:¥autoexec.bat ファイルの内容が [redacted] サーバへ送信されました	

DARKTRACE

内部ネットワーク見える化診断サービス

内部ネットワークにおけるセキュリティリスクをレポート！

発見したセキュリティリスクをまとめたレポートを提供。
お客様環境におけるセキュリティリスク改善にご活用いただけます。
（Darktrace導入から分析、レポート納品まで、約1.5か月を想定）

短時間で診断準備が可能！

お申し込み後、必要な情報をお伺いするヒアリングシートにご回答いただき、
当社にて初期設定を行います。
導入作業はタップもしくはミラーポート※への接続などを含め、
約1～2時間で完了します。※事前にご準備いただく必要があります。

■ サービス利用料：¥1,000,000/回・台

KYOCERA

京セラ コミュニケーションシステム株式会社
KCCSカスタマーサポートセンター
フリーコール　0120-911-901
携帯電話・PHS・IP電話など　050-2018-1827
受付時間　平日9:00 ～ 17:00
（17:00以降のお問い合わせは自動応答になります。）
KCCSホームページ　https://www.kccs.co.jp/
E-mail：kccs-support@kccs.co.jp

2017年2月現在