【定期レポート】CylancePROTECT Managed Service for LanScope

お客様名	株式会社〇〇〇〇
レポート対象期間	2019年5月分（2019/5/1～2019/5/31）

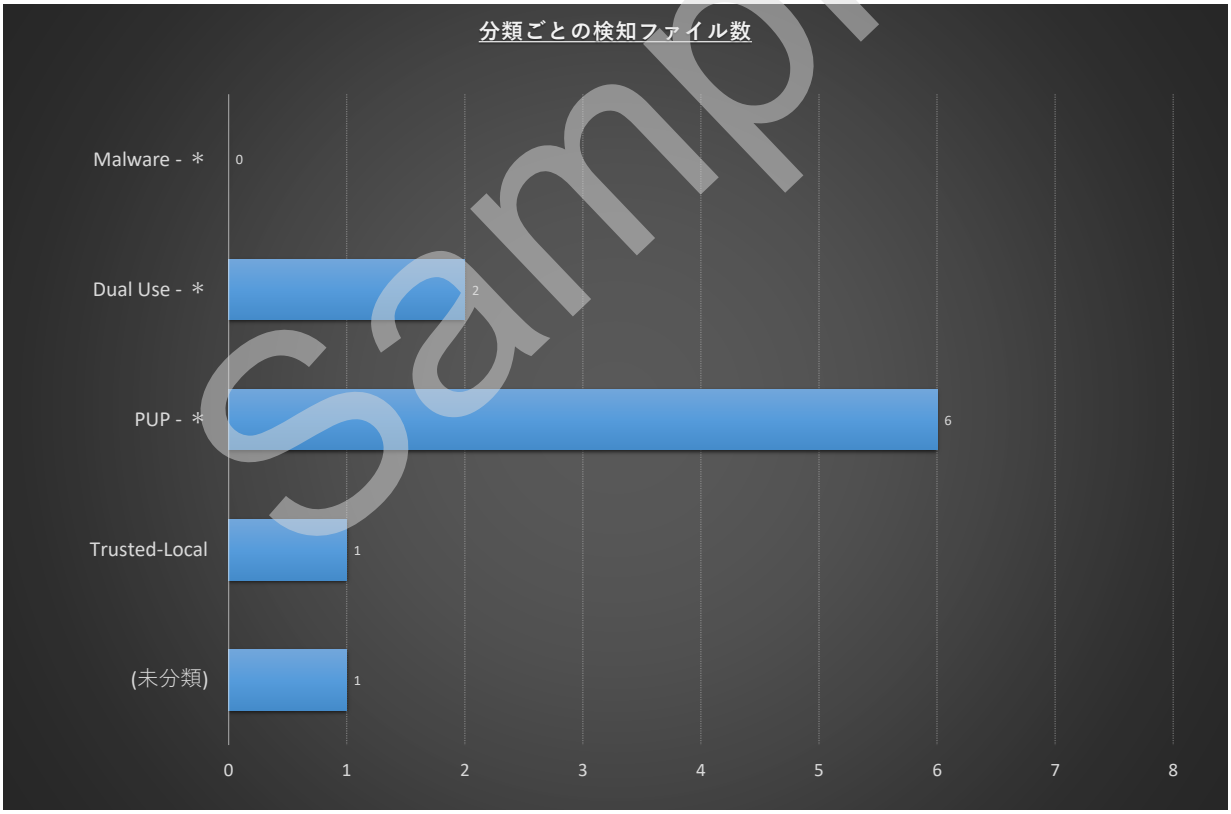
作成日：2019/06/05
エムオーテックス株式会社
ITサービス本部
セキュリティサービス部

レポートについて

上記レポート対象期間にCylancePROTECTが検知した情報をCylanceコンソールから抽出しました。
また、いくつかの検知ファイルについては弊社にて調査/解析を行いましたので、以下の通りご報告いたします。

注）
1. すでにセーフリストに登録されている、もしくは削除（クリア）されている場合はレポートに含まれません。
2. 分類が【Malware】のファイルについては全て解析を行いました。【Malware】が検知されていない場合は最大10個のファイルについて解析を行っております。
   未解析のファイルについては、お客様にて解析を行っていただきますようお願いいたします。
   （別途提供している資料や動画をご参照ください。）
3. 各ファイルの解析結果については下記表の「MOTEXコメント」や「推奨対処」欄を、詳細情報についてはCylanceコンソールをご確認ください。
4. 本レポートは、レポート作成時点において弊社の独自解析結果を基に作成しています。本レポートに記載した内容以外にも何らかの悪意のあるコードなどが
   含まれている可能性もあります。本解析結果による被害や不利益が生じた場合でも当社は一切の責任を負いません。
5. 検知台数は、本レポート対象期間も含む、これまでの累計台数です。（参考情報として記載）
6. 以下のような場合、悪意のあるファイルではありませんがマルウェアにも含まれる動作（要素）を持っているためCylancePROTECTが検知する場合があります。
   例）
   ・OSやレジストリ情報を収集して外部へデータ送信するようなPC診断ツール
   ・コンピュータの遠隔操作をするようなリモートコントロールツール
   影響が無いという判断の元に利用している場合にはセーフリストへ登録していただくことで対象のファイルを使用する（検知対象から外す）ことができます。

＜検知状況＞



＜検知ファイル一覧＞

No.	検知ファイル名	Cylance スコア	分類 ※1	検知台数 (累計)	ハッシュ値(Sha256)	初検出日時 ※2	最終検出日時 ※2	MOTEXコメント	推奨対処 ※3
1	vSnapshotServ.exe	100	Dual Use - Generic	1	6e682e5140c2b8a3710dce0094f955d1212616aff393af927bb3436dc0a67fe5	2019/5/16 21:29	2019/5/16 21:29	vSnapshotという画面キャプチャ用ソフトに関するファイルのようです。 中国製の広告表示ソフトとなりますので業務で利用しない場合は削除することを推奨	隔離推奨
2	IEDriverServer.exe	71	Dual Use - Generic	1	83e1fc1fe75ca782adc71da8c1064decc17466acba60d81b022d6253b794d9ac	2019/5/29 14:03	2019/5/29 14:03	ブラウザの操作を自動化するためのツールに関連するファイルのようです。 ファイルパスをご確認いただき、業務で利用するものであればそのまま残していただ	要確認
3	uninstaller.exe	100	PUP - Adware	1	99395af6b047fd790ba2a332f92e481c23a8bde1316ee4e750019577bc7d9cc0	2019/5/16 10:19	2019/5/16 10:19	File Openerという悪意のあるソフトウェアのようです。(インストール時に様々な不要プログラムが同時インストールされます)	隔離推奨
4	ICReinstall_zipinstall.exe	100	PUP - Adware	1	a447b57630f94800b820c9e0d91b75478b2aba0431f18c4ada653bd2c742dc20	2019/5/22 20:25	2019/5/22 20:25	ツールバーやブラウザの拡張機能を含むセットアップモジュールのようです。業務で利用しない場合は削除することを推奨します。	要確認
5	MemClCmd2.exe	100	PUP - Generic	1	ac54a176f03511455326dd65d6f051439870a2db1e21167ee8d83edea4f4deac	2019/5/26 23:21	2019/5/27 5:32	「メモリの掃除屋さん」というフリーソフトのファイルのようです。 ファイルパスをご確認いただき、業務で利用するものであればそのまま残していただ	要確認
6	FileZilla_3.43.0_win64_sponsored-setup.exe	100	PUP - Generic	1	17ffaafa6ef1ab8c1cde09587d5f06d488af62e6a0dec1afc8d61e9d7889b84f	2019/5/12 14:18	2019/5/12 14:25	FileZilla FTP Clientのセットアップに関連するファイルのようです。 ファイルパスをご確認いただき、業務で利用するものであればそのまま残していただ	要確認
7	swusrd.exe	100	PUP - Hacking Tool	1	c906a1455754d7d879f1e86d98009bccbbb22b5cc62c27f09f41b02bb26349b1	2019/5/22 23:35	2019/5/22 23:35	クオリティソフトのQNDというソフトウェアに関するファイルのようです。 ファイルパスをご確認いただき、業務で利用するものであればそのまま残していただ	要確認
8	CaspolPortal.exe	100	PUP - Scripting Tool	1	ebbe978a1dfd34489dfa243105660ebd2c7ed306a6993bfdacd56fec867838ba	2019/5/23 1:48	2019/5/23 1:48	SimSciというソフトウェアに関するファイルのようです。 ファイルパスをご確認いただき、業務で利用するものであればそのまま残していただ	要確認
9	apidsp_windows.dll	98	Trusted - Local	1	e57c267c1878909ded454e571f8b60ac41ca7a4ae248e42080f21d30c18b1441	2019/5/28 5:40	2019/5/28 5:40	―（Trusted-Localのため、セーフリスト登録を推奨）	セーフリストに追加
10	Setup.exe	98	(未分類)	1	dc513b9f3bd27b20584e904c16c3428d61f6334a2dccfb34bba7495de9e57224	2019/5/28 8:59	2019/5/28 8:59	―	―

※1：分類について

【Malware - ＊】もっとも悪性が高く、有害（危険）なファイルとなります。
【Dual Use - ＊】攻撃者と正規ユーザの両方によって使われうるもので、利用者の意図によって危険になり得るものとなります。
【PUP - ＊】潜在的に利用が望まれないプログラム（Potentially Unwanted Programs）を指し、幅広い用途で利用されるものが含まれます。
【Trusted - Local】正規のコーディングとQA手順を踏んで作成された無害（安全）なファイルとなります。
【(未分類)】Cylanceのリサーチチームによる解析がまだ実施されていないファイルとなります。（解析後に分類情報が付与されます。）

※2：初検出日時と最終検出日時について

Cylanceコンソールからエクスポートした情報はUTC時間（協定世界時）となりますが、本レポートでは、日本時間（UTC+9）に変換して記載しています。
例）最終検出日時が「2019/5/30 20:00 (UTC+0)」の場合、日本時間は「2019/6/1 5:00（UTC+9）」となるため、2019年5月分のレポートには含まれません。

※3：推奨対処について

【セーフリストに追加】検知ファイルをCylanceコンソールのセーフリストへ登録し、検知/隔離対象から除外することを推奨します。
【隔離推奨】検知されたファイルを分析した結果、危険もしくは望ましくないファイルの可能性が高いもので、隔離することを推奨しています。
隔離モードで利用している場合は、検知した時点で隔離されているため、対処不要です。
検知モードで利用している場合は、検知ファイルをCylanceコンソールの隔離リストに登録し、隔離対象としてください。
※隔離モードと検知モードについては、「CylancePROTECT-利用ガイド」のp.10やp.40をご参照ください。
【要確認】 ファイル名やファイルパスなどの情報から、業務で利用しているものかどうかを確認していただく必要があります。
検知ファイルの詳細情報は、Cylanceコンソールの[脅威保護]画面から該当ファイルのリンクをクリックすることで確認が可能です。