2019
TOKYO / OSAKA / NAGOYA

LanScope Cat × CYLANCE PROTECT

Protect Cat Users Conference

MOTEX
Secure Productivity

プロテクトキャットユーザー会について

ランサムウェアだけでなく、標的型攻撃やBEC（ビジネスメール詐欺）など、企業をターゲットとしたサイバー攻撃は日々巧妙さを増しています。もはやビジネスのひとつと化したサイバー攻撃は、今後も増加の一途をたどり、減少する見込みはありません。
従来のアンチウイルスソフトだけの対策では不十分であることは周知の事実で、新たな対策を検討することは今や当たり前となっています。

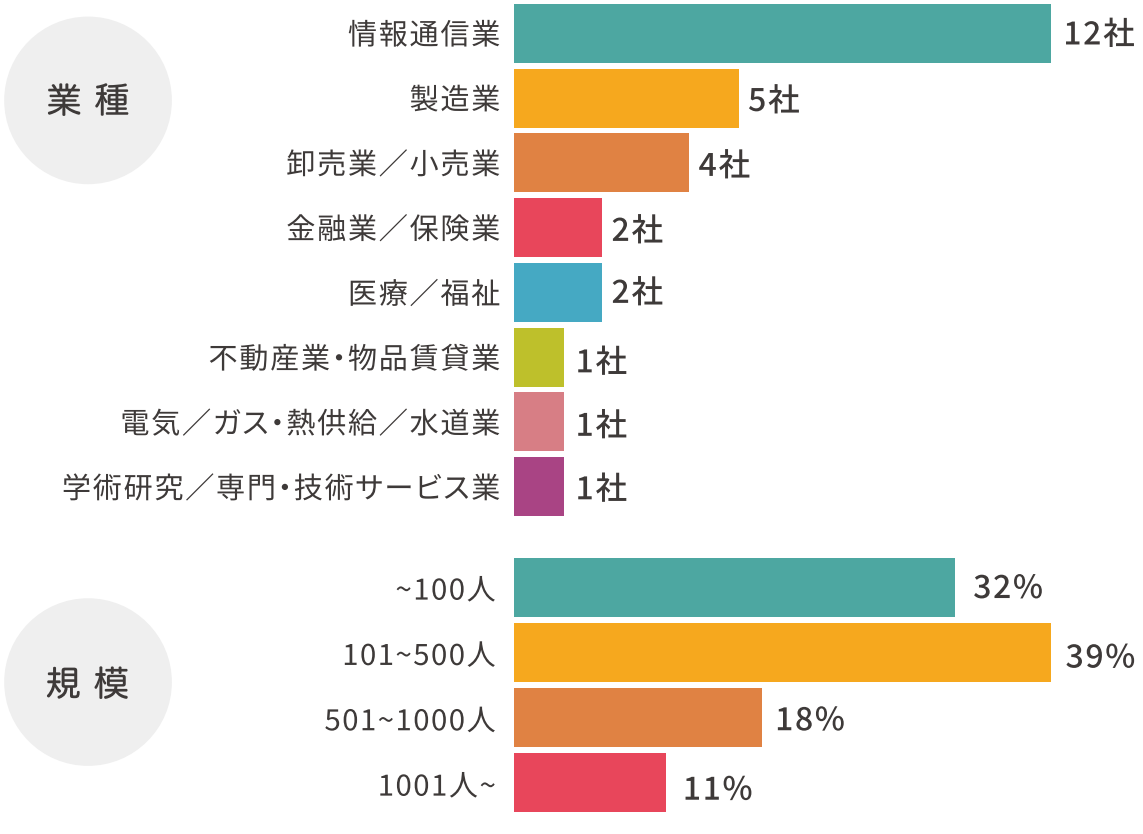
MOTEXはマルウェア検知率99%※を誇る次世代アンチウイルスCylancePROTECTを、LanScope Catのオプション「プロテクトキャット」として2016年7月にリリースしました。
リリースから3年が経ち、300社を超える企業様にご導入いただいております。

※2018 NSS Labs Advanced Endpoint Protection Test結果より

今回は、導入検討中を含む28社33名のユーザー様にお集まりいただき、3年目となる「プロテクトキャットユーザー会」を東京・名古屋・大阪の3拠点で開催いたしました。

当日は、BlackBerry Cylanceの基調講演をはじめ、CylancePROTECTユーザーである弊社MOTEXもユーザーの立場から実際に行った導入前の検証から、現在の運用に至るまでをお伝えさせていただきました。
また後半には、ユーザー様同士が交流し普段から抱えている悩みや課題、プロテクトキャットの運用ノウハウなどを共有する情報交換会を実施しました。
チャタムハウスルールのもと、大変活発な意見交換が行われました。

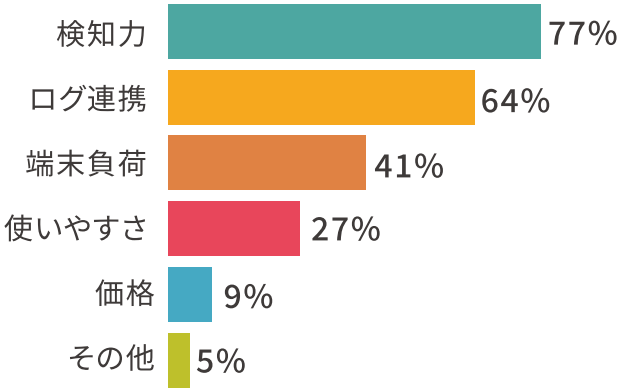
参加ユーザー様属性【28社】



事前アンケートサマリー

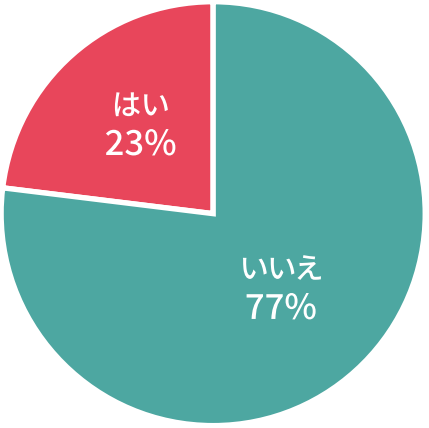
Q プロテクトキャット導入の決め手について ※複数回答可 (n=22)

約8割が「検知力」が決め手に



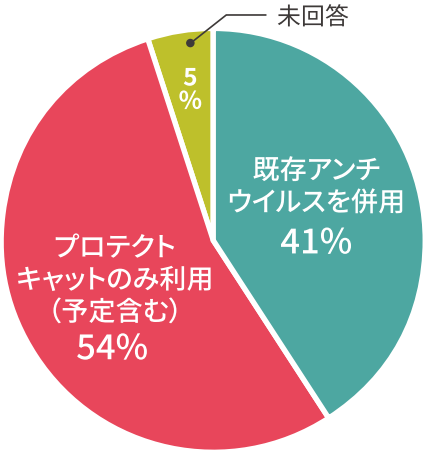
Q プロテクトキャット導入後に追加導入した外部脅威対策製品がある (n=22)

4社に3社が追加導入なし



Q プロテクトキャット導入後の既存アンチウイルスについて

2社に1社がプロテクトキャットのみ利用 (予定含む) (n=22)



Q 現在抱えているセキュリティ全般の課題

(自由回答)

- ●標的型訓練メールを開けてしまう社員が後を絶たない。
- ●業務のしやすさが優先されて、情報の取り扱い方法が守られていない。
- ●セキュリティ対策に対する社内の意識がなく、知識も薄い。
- ●セキュリティ対策にどのくらい費用をかけるべきか悩んでいる。
- ●新しい製品を導入しようとすると、これまでの費用とのギャップが説明しきれない。どのように上層部を説得すればよいか困っている。

チャタムハウスルール

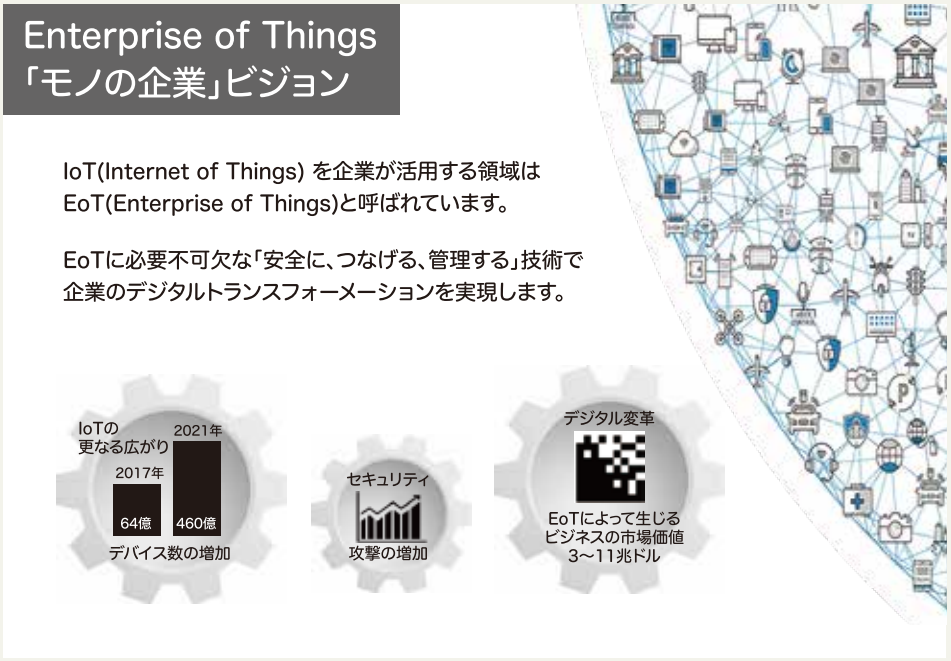
会議の参加者に遵守が求められることがあるルールの一つ。チャタムハウスルールの下では、参加者は会議中に得た情報を外部で自由に引用・公開することができるが、その発言者を特定する情報は伏せなければならない。チャタムハウスルールには、会議参加者が自身の立場や役職に縛られることなく、自由な意見を述べることができる利点があるとされている。

脅威のトレンドと最新ロードマップ

BlackBerry Cylance 最高技術責任者 乙部 幸一朗

BlackBerryとの買収統合

元々スマートフォンのメーカーとして知られているBlackBerry社は、そのビジネス形態を大きく変貌させ、現在では世界最大規模のセキュリティソフトウェア会社となっています。今後IoTがより多くの企業で使われ、EoT（Enterprise of Things）実現を目指す中、その基盤を支える安全で高信頼なプラットフォームを提供するという戦略のもと、最近では多くの新興ソフトウェア企業を買収しています。今回その戦略を担う大きな柱としてCylanceの買収が発表され、2月に正式に会社が統合されました。今後もBlackBerry傘下の独立事業部門として製品の開発・販売・サポートは引き続き変わらず提供されますが、それに加えてCylanceが持っているAI、そしてサイバーセキュリティの技術がBlackBerryの提供するEoTソリューションに組み込まれていくことになります。



脅威のトレンド

Cylanceが提供する「2019脅威レポート※」によると、2018年の傾向としてはグローバルでマルウェアの数は10%増加の微増となっていますが、身代金要求型のマルウェアであるランサムウェアの数は26%減少しており減少傾向にあります。その代わりに、コインマイナーと呼ばれる暗号通貨のマイニングを行うマルウェアが47%増加しており、この傾向は今後も続くものと思われます。

代表的なマルウェアとしてGandCrabというランサムウェアがあります。これはRaaS（Ransomware-as-a-Service）と呼ばれる闇サイト上で提供されるサービスで作成可能なランサムウェアの一種です。エクスプロイトキットを使ってWeb経由で感染しますが、頻繁なアップデートを行ったり支払い通貨でDASHという匿名暗号通貨を使ったりするなどの特徴があります。また、もう1つ紹介するのが情報搾取系マルウェアであるEmotetです。これはバンキングトロージャンと呼ばれるオンラインバンキングを狙ったトロイの木馬型ウイルスがベースとなっていますが、最近ではネットワーク経由で広がるワーム感染機能やボット機能、メッセージ収集機能などをモジュール化して次々と追加し、飛躍的な進化を遂げています。

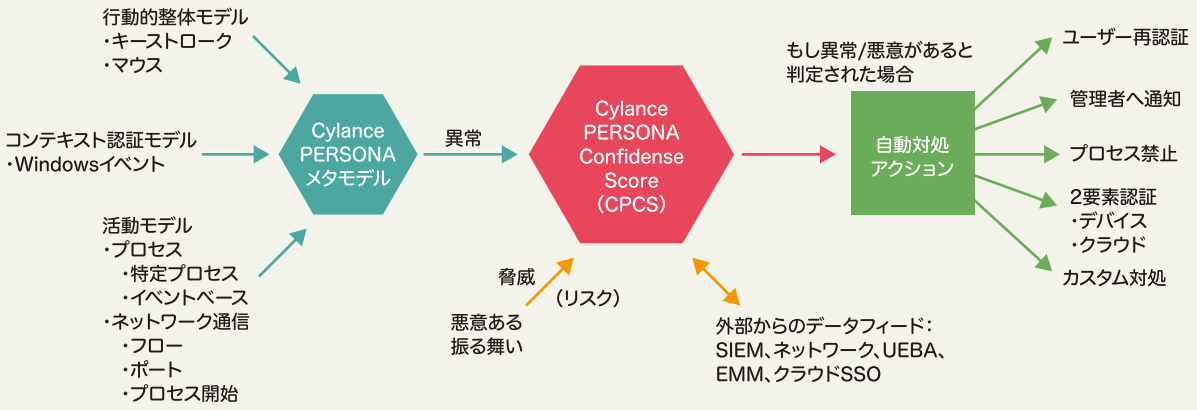
標的型攻撃と呼ばれる高度な脅威の領域においては、従来のように攻撃グループが独自で開発したマルウェアやツールだけではなく、商用ツールやオープンソースコードの流用が数多くみられるようになっています。これは、ツール開発などのコストを削減したり開発期間を短縮したりするというメリットとともに、痕跡を消すことで攻撃グループの身元をわかりにくくするという目的があると考えられます。

2018年全体の傾向

- 10% 増加 — マルウェアの全体数
- 26% 減少 — ランサムウェアの感染企業数
- 47% 増加 — 暗号通貨マイニングの感染企業数

※ https://www.cylance.com/ja_jp/company/newspress/jp the blackberry cylance 2019 threatreport.html

CylancePERSONA の仕組み



最新ロードマップ

今後も、従来製品の機能強化や新しい製品など、数多くのリリースが予定されています。まずは、一般家庭向け製品であるCylance Smart Antivirusです。既に米国をはじめとする他の地域では先行してリリースされており、今年の後半には日本国内でもリリースを予定しています。既存の企業向け製品であるCylancePROTECTとCylanceOPTICSに加えて、家庭向けにはこのCylance Smart Antivirusを提供することで、企業そして一般家庭においても包括的なエンドポイントセキュリティを実現していきます。

次にリリースが予定されているのが、新型エージェントです。Cylanceの企業向けのエンドポイント製品としては現在CylancePROTECTとCylanceOPTICSという2種類が提供されていますが、新型エージェントではこれらを統合してEPPおよびEDRの両方の機能が1つのエージェントで提供される予定です。このEPPとEDRの完全な統合は、管理面やリソース面のみならず、エンドポイントにおける効果的なセキュリティの実現に寄与することになり、今後エンドポイントセキュリティ業界の主流になっていくものと考えています。

そして最後に紹介するのがCylance-PERSONAです。CylancePERSONAはAIと行動的生体認証を組み合わせた新しい認証の製品で、最近注目されているUEBA（User and Entity Behavior Analytics）と呼ばれるユーザーの行動分析のアプローチにAIによる予測モデル技術を活用することで、パソコン端末上で行うユーザーの行動を学習し、なりすましや異常行動を検知するという新しいタイプの認証ソリューションです。

CylancePERSONAは主にユーザーがパソコン上で行う生体的行動（マウスやキータイプなどの動き）と、実際の活動（どのようなアプリケーションを使うか、どのようなサイトにアクセスするかなど）を学習し、そこからPERSONAモデルと呼ばれるユーザーごとの人格モデルを作成します。その後、作成されたモデルを使って今度はユーザーの行動を監視することで、いつもと異なるキータイプやアプリケーションの使用が行われるとリアルタイムで検知し、強制的に再認証を行ったり、管理者へアラートを通知したりできます。これによって盗難されたIDやパスワードを起点とする外部からの脅威に対応するだけでなく、内部犯行などの内部からの脅威にも対応できるようになると考えます。

このようにCylanceが持つAIによる予測モデル技術というアプローチは、今後様々な形でBlackBerryが提供するソリューションに組み込まれていくことになるでしょう。

Emotet

・2014年に登場したバンキングトロージャン
・主にメールに添付されたワードファイル（マクロダウンローダー）によって感染
・モジュール化され多くの機能が追加
  ・マルウェア配信
  ・スパム配信
  ・パスワード盗難
  ・ネットワークワーム機能
  ・メールメッセージの収集

CylancePROTECT選定の理由と導入効果

エムオーテックス株式会社 MOTEX-CSIRT 丸山 悠介

MOTEXではCylance社の日本法人ができる半年前、2015年12月に米国法人との直接取引によりCylancePROTECTを導入しました。

MOTEXで導入前に実際に行ったCylancePROTECTの検証（2015年11月実施）

〇検証の概要

・検証に利用したウイルスの準備

1.マルウェア情報サイトVirusTotalより直近で登録されたマルウェアを100個入手（既知のマルウェア100個）

2.入手した100個のマルウェアを難読化（未知のマルウェア100個作成）

3.実際に親会社（KCCS）とMOTEXにメールで届いたマルウェア18個を用意

合計218個のマルウェア検体を元に検証を実施 ※1

※1 マルウェアの入手から検証までに3～5日経過

■検証実施製品：計7製品

・従来型シグネチャAVS：5製品

・国産ふるまい検知型AVS：1製品（WindowsDefender併用）

・CylancePROTECT ※2

※2 Cylanceのみ未知のマルウェア検知の有効性を確認する為、半年前のバージョンを使用

■検証環境

Windows 7 Professional 32bit もしくは 64bitのPC7台。

それぞれアンチウイルスソフト（以下：AVS）をインストール（最新のWindows Updateを適用済み）※3

※3 AVSは2015年11月時点の最新のシグネチャで検証

〇検証結果

VirusTotalに登録後3～5日が経過したマルウェア検体は、どの製品も 90%以上の検知ができました。しかし、難読化した未知のマルウェアに対する検知率には歴然とした差がありました。従来型AVSでは、高いものでも30%程度の検知率に留まり、多くのマルウェアはすり抜けてしまったのです。当時導入検討していたふるまい検知型のソリューションは、未知のマルウェアに対して90%以上の検知率だったものの、従来型AVSと併用しなければ既知のマルウェアを検知できず、過検知も多いという結果でした。そんな中、CylancePROTECTに関しては既知のマルウェア、未知のマルウェアともに半年前のバージョンで100%の検知率をたたき出しました。

■検証結果

製品名	ウィルス検知率	難読化ウィルス
製品A	95.8%(113/118)	15.0%(15/100)
製品B	96.6%(114/118)	6.0%(6/100)
製品C	97.5%(115/118)	7.0%(7/100)
製品D	100.0%(118/118)	11.0%(11/100)
製品E※（Windows Defender併用）	93.2%/11.9%(110/118)	96.0%/95%(96/100)
製品F	97.5%(115/118)	33.0%(33/100)
CylancePROTECT※	100.0%(118/118)	100.0%(100/100)

※ CylancePROTECTのみ半年前のバージョンを使用

この検証結果のインパクトは非常に大きく、様々な手法でエンドポイントに着弾したとしてもゼロデイのマルウェア感染リスクを最大限減らせると判断し、数ある対策の中から最優先でCylance-PROTECTの導入を決めました。

CylancePROTECT導入後の効果

CylancePROTECT導入から約3年が経過しましたが、MOTEXでは導入から今までマルウェア感染による大きなインシデントは発生していません。当初狙っていた導入効果が実現できているだけでなく、運用する中で良かったと感じた点があります。

1：報告業務の工数軽減

例えば、攻撃に使われたマルウェアの検体情報が公開された際に、シグネチャを用いた従来型AVSで対応を行う場合、以下のサイクルを回すことが多いのではないでしょうか。

1:検体情報の入手
2:対応したシグネチャの確認・入手
3:エンドポイント全台のシグネチャアップデートの確認（オフラインPCも多数あり工数大）

これらのステップで初めて安全確認ができますが、工数負担が大きくなります。また、亜種が作り出される度に、①～③のサイクルを回し続ける必要があります。

MOTEXではCylancePROTECT導入後、話題となる事件を確認した際に、以下の対応を行っています。

1:VirusTotalなどで該当のマルウェア検体入手
2:Cylanceの古いバージョン（運用環境よりも古いバージョン使用）での検知確認

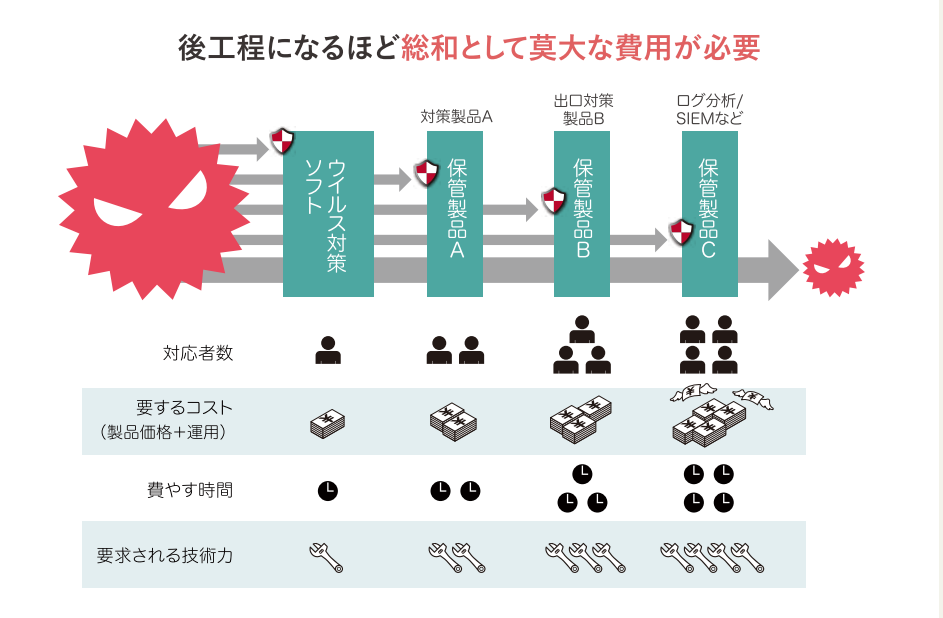
この2ステップで、「仮にMOTEXに着弾

してもブロックできます」と安全宣言ができるようになりました。
近ごろよく使われている著名企業を騙ったばら撒き型攻撃メールにおいても、半年間分49個のマルウェア検体を収集し、過去のバージョンで検証したところ、2年前のバージョンでも48検体を検知・隔離できることが確認でき、CylancePROTECTの予測検知の効果を実感できています。

2：PC負荷の軽減

2017年の7月にそれまで併用していた従来型AVSをアンインストールし、CylancePROTECTに一本化しました。すると社員から、当初想定していなかった「PCの動作が軽くなった」といった声が多数上がりました。CylancePROTECTは日々パターンファイルを更新し、シグネチャとマッチングさせる仕組みではなく、インストール時のフルスキャン以降は新しく端末に入ってきたファイルに対してのみ、数理モデルでマルウェアの特徴点を計算して判断する仕組みのため、PCに与える負荷を軽減し、端末作業者の生産性向上にも寄与しています。

■インシデント対応とコスト



3：インシデント対応時のコストパフォーマンス

MOTEXでは「感染してから早急に対処」ではなく、マルウェア攻撃に対して「CylancePROTECTで検知・隔離を行い、LanScope CatのPC操作ログから流入原因をつかみ、経路をふさぐ」という運用をしています。上流で対処することで最小限のマンパワーとスキルで効率よく対処する環境づくりができています。

最後に

昨今のサイバーセキュリティ対策市場は「防御重視のセキュリティの限界、感染後の対応を迅速に」というメッセージが一般的になり、EDR製品をはじめとした感染後対応型のソリューションやサービスが流行しています。しかしながら、スキルのある人間が職人技で使いこなせば効果が出るものの、一般的な企業のセキュリティ担当者には荷が重すぎる製品も多く、想定した効果が発揮できないというケースが多いのではないでしょうか。
サイバー攻撃はROIの観点からも、減ることは期待できず、今後増えていくことは間違いありません。検知後の対応はもちろん重要ですが、高度なスキルとある程度の工数が必要であり、ここをいくら効率化したとしてもインシデントの発生量が増え続ければ、いつかは限界が訪れます。
「防御を意識する」と中々言いづらい市場の雰囲気となっています。検知後の対応を強化する前に防御力の強化を常に検討し、優先順位を考慮しながらインシデント発生頻度を減らしていくこと、これこそがもっとも重要だと我々は考えています。

■社内調査した検体（古い数理モデルでブロック確認済み）

CylancePROTECTの過去のバージョンでブロックを確認したマルウェアの一部

2015年　　：TeslaCrypt (VVV) ウイルス
　　Emdivi
2016年　5月：Locky
2016年　6月：バングラディッシュ銀行アタック
2016年　6月：某旅行サービス業への攻撃（PlugX）
2016年　6月：新型ランサム Bart
2016年　7月：新型ランサム Zept
2016年10月：不正送金マルウェア「Gozi」　別名 Ursnif
　　ランサムウェア「PETYA」
　　不正送金マルウェア「URLZone」　別名 Shiotob
2017年　5月：WannaCry
2017年12月：Spider
2017年12月～2018年5月：ばら撒きメール マルウェア 49個
2019年　4月：「Emotet」
　　ランサムウェア「Robinhood」

情報交換会

INFORMATION SHARE MEETING

＊プロテクトキャットはCylancePROTECTのOEM製品であり、同等のマルウェア検知機能を有します。

Q プロテクトキャット導入のきっかけは何ですか？

・元々導入していたAVSの更新期限が来たため製品を変更しようと、NGAV+EDRで検討し複数製品を評価しました。CylancePROTECTの比較対象だった製品は、使いにくい（わかりにくい）という声が他メンバーから上がったため**操作性の良いプロテクトキャットの採用を決めました。**

・従来のAVSで検出されなかったウイルスによる通信がFWでブロックされたことがありました。同じウイルスがPOCで検出され、CylancePROTECTの検知率の高さを実感しました。

・外部から組織内のネットワークに侵入させないよう、境界防御の対策（入口対策）に力を入れていました。ですが、**標的型攻撃などの巧妙な攻撃の増加に伴い、「侵入されても重大な情報を社外に漏らさない」こと（出口対策）に重点を置いた強化対策を行うことが必要不可欠**になったと考え、導入検討を始めました。

・これまで利用していた従来型AVSは、機能強化に伴いライセンス料の値上げや、端末への負荷増加が発生したため、リプレイス検討のきっかけとなりました。

・セキュリティ商材を提案する中で、自社もお客様と同じ環境であることに気が付きました。もし感染してしまったときに、セキュリティを提案しているベンダーとして言い訳が出来ないと思い、導入を決めました。

・ITリテラシーの低い社員は、既存AVSのシグネチャーを最新にしてもらえない課題がありました。**EDRとも迷ったものの、EDRは検知だけで止めてくれるわけではないので防御力強化の観点からCylancePROTECTに決めました。**

Q POCの結果、また現在はどのように運用をしていますか？

・自動隔離設定後は、**検知時には利用者側にポップアップを出しています。利用者から連絡がなければそのまま隔離していますが、隔離設定1~2か月後以降はほとんど連絡がくることはありません。**

・ホワイトリストは業務に必要かどうかで都度判断しますが、利用者からの申告がない限り許可登録はしません。

・Excelマクロの利用率が高いことと、ウイルスバスターとのバッティングがあること、また、開発端末で検知しすぎるため、スクリプト制御、メモリ防御はマクロ以外をONに設定しています。

・Unsafeは隔離、Abnormalは放置で運用していますが、そこそこ検知している感覚です。Trusted Localは許可、など検知したファイルの分類ごとに対応を変えています。

Q プロテクトキャット導入でどのような効果がありましたか？

・負荷が軽くてきちんと検知をしてくれています。PCのスペックがやや低めでも動作に問題無いだけでなく、パターンファイルが最新かどうかを気にしなくてよくなり安心です。

・なぜそのファイルが引っかかったのか分かるので助かります。引っかかっている＝隔離してくれている、と判断できるので工数削減に繋がりました。

・マルウェアに感染したことがある端末にCylancePROTECTをインストールすると、従来型AVSで見つからなかったファイルを見つけてくれます。
従来型AVSで5個見つかるとしたら、CylancePROTECTなら20個くらいは見つかる感覚です。

・既存PCのスペックがかなり低い（メモリ4GB、CPUも低い）のですが、特に業務に問題はなく、CylancePROTECTだからこそだと実感しています。

・パターンファイルの更新をやらないといけなかったのですが、実際はできていませんでした。（更新により問題が発生することを懸念したため）Cylance-PROTECTの導入によって更新の必要がなくなったので、工数削減にはなっていないものの、ルールが守られるようになりました

Q セキュリティ全般の課題は何ですか？

・規定が裏目に出て、部門長が事象、インシデントの判断をするため、報告が上がって来なくなった。お客様への守秘義務をつかって報告しないということも。

・CSIRTは監督官庁から指導があったため専任でなく兼務でとりあえず作った、という感じになってしまっています。

・セキュリティ研修を年2回やって、順守度チェックも実施しています。ですが、それでも浸透していないと感じており、セキュリティレベルの向上がなかなか見込めません。

・ビジネスメール詐欺に引っかかりそうになったことがあります。実在する取引先のメールアドレスで送られていましたが、やり取りの途中で気付くことができました。

Q セキュリティ教育・啓蒙活動における課題は何ですか？

・メール訓練を実施しており、引っかかった人は補習を受けてもらうようにしていますが、実際には補習を受けてくれない人が多く課題に感じています。

・**訓練ツールを作ったものの形骸化してしまいました。**毎年同じことを行っているため、意味があるのか疑問に感じてきてしまっています。

・**e-ラーニングを導入**しましたが、受講率が低く活用できていません。

・いろいろと啓蒙は試みていますが、浸透しません。

Protect Cat Users Conference

今回でプロテクトキャットユーザー会も3年目となり、東名阪3拠点開催で合計9回、84社95名のユーザー様に参加いただきました。ユーザー様同士の情報共有の場であるだけでなく、プロテクトキャットに関わらずセキュリティ全般についてユーザー様と情報共有・相談できる場は、弊社にとっても大変貴重な場として捉えています。

1年目は、まだ市場に浸透していないAIアンチウィルスソフトであるプロテクトキャットを先行して導入されたアーリーアダプターのユーザー様にお集まりいただきました。新しい概念のAI製品を導入するに至るまで、どのように上層部へ説明したのか？などアーリーアダプターならではの苦労されたエピソードが多くありました。また、AI製品の宿命である過検知対応についてもたびたび話題になりました。

それから2年が経ち、今年も様々な議論が行われましたが、「プロテクトキャット導入後にマルウェア感染被害を受けた」という事例は1社もありませんでした。

VOICE
参加ユーザー様の声

短い時間で多くの
情報交換ができて
良かったです。

他社の利用実態
（負荷や過検知状況など）を
聞けて参考になりました。

有意義な時間を
過ごさせていただきました。

ハイレベルな会で
おどろきました。
とても勉強になり、今後もっと
自社のセキュリティを
何とかしていきたいと
思いました。

他社の事例が聞けて
とても面白かったです。
ぜひ今後とも良い製品を
作っていってください。

他社の意見がきけて、
大変参考になりました。

さらに、プロテクトキャット導入後に新たなセキュリティ投資を行っている企業様が少なかったことも投資対効果の面で効果的なソリューションであると実感しています。
サイバーセキュリティの市場は、常に最新の技術を使った製品が参入を続けており、日々様々な情報が飛び交う中で、「ベンダーのセールストーク」ではなく「実際に導入したユーザーが価値を感じているか？」が最も重要であり必要とされる情報ではないでしょうか。

今後もMOTEXでは、ベンダー発信の情報だけではなく、ユーザー様同士が交流し、情報共有出来る場の構築を目指し、継続して取り組んでまいります。

最後になりましたが、本イベントにご協力いただきました皆様に心よりお礼申し上げます。

■今回の参加企業（一部抜粋）

社会福祉法人静岡市社会福祉協議会
三重精機株式会社
株式会社名古屋リース
株式会社システムトラスト
熊本信用金庫
株式会社オプテージ
ティーメックス株式会社
アイテック阪急阪神株式会社
住友セメントシステム開発株式会社
システムズ・デザイン株式会社
大明化学工業株式会社
池上通信機株式会社
コグニビジョン株式会社
三井E&Sシステム技研株式会社

※上記含めて合計【28社／33名】にご参加いただきました。
※プロテクトキャットを導入検討中のユーザー様にもご参加いただいてます。

MOTEX
Secure Productivity

エムオーテックス株式会社

本　　社：〒532-0011　大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル　TEL:06-6308-8980
東京本部：〒108-0075　東京都港区港南1-2-70 品川シーズンテラス5F　TEL:03-5460-1371
名古屋支店：〒460-0003　名古屋市中区錦1-11-11　名古屋インターシティ3F　TEL:052-253-7364
九州営業所：〒812-0011　福岡市博多区博多駅前1-15-20　NMF博多駅前ビル2F　TEL:092-419-2390

TEL:0120-968995 受付時間 9:30 - 12:00、13:00 - 17:30（下記休業日を除く）
（休業日：土・日・祝祭日および弊社の定める休日）

E-mail：sales@motex.co.jp　　URL：www.motex.co.jp

●お問い合わせは当社へ