日立ソリューションズ

HITACHI
Inspire the Next

導入事例

株式会社 KVK 様

CylancePROTECT®

ランサムウェア感染をきっかけに AIベースの製品で 未知のマルウェア対策を強化

十分なセキュリティ対策をしていたつもりが、
ランサムウェアに感染してファイルを暗号化されてしまった――。
この苦い体験を教訓に、株式会社 KVKは
未知のマルウェアを実行される前に検知できる
「CylancePROTECT」を全社に導入。
既存のマルウェア対策ツールと併用して、
高度化・深刻化するセキュリティ脅威への対策を強化しました。

BlackBerry CYLANCE × KVK

課題

- 未知のマルウェアによる被害を防ぎたかった
- 仮想環境もマルウェアから守りたかった

効果

- ランサムウェアによるファイルの暗号化など、マルウェアによる被害を防止できるようになり、少ない工数での運用管理も実現
- 仮想環境にもスムーズに導入でき、またマルウェアからの防御も実現

従来からの課題

セキュリティ対策をすり抜けた 未知のランサムウェアに感染

株式会社ＫＶＫは、1939年創業の水栓金具の専業トップメーカーで、岐阜県に本社を置き、浴室、キッチン、洗面化粧室向けの製品を、国内および中国、フィリピンの工場で製造しています。

「当時、当社のセキュリティ対策は、ゲートウェイ、ファイアウォール、スパムメール対策アプライアンス、マルウェア対策ツールなどを複合的に組み合わせた構成になっていました。マルウェア検知用のパターンファイルはサーバーで一括管理されており、事務所や工場のPCについては、起動時にローカル側のパターンファイル更新とスキャンを自動的にかけるという設定でした」(川出氏)

セキュリティ対策が甘かったわけではないＫＶＫが対策の見直しに迫られたのは、2016年のことでした。

同年11月にメールの添付ファイルとして送られてきたランサムウェアが、パターンファイルに載っていない“未知のマルウェア”だったため、マルウェア検知の仕組みをすり抜けてしまいました。その結果、メールの添付ファイル開封時に仮想環境につながっている1台のPCが感染。そのPCがアクセスしていた共有フォルダ内のファイルが暗号化されてしまうという問題が発生しました。

「幸い、基幹系システムの停止によって業務が止まってしまうといった深刻な事態は避けられました。しかし、定期バックアップの対象になっていなかったファイルは使えなくなってしまいました」(川出氏)

導入の経緯

AIベースの検出エンジンを評価 無償トライアルを利用して検証

このままでは、また未知のマルウェアが入ってきたときに被害を防げない――。ＫＶＫの情報システム部は、PCや仮想環境において、パターンファイルに基づく従来の検知方式では防げない未知のマルウェアも的確に検知できるソリューションの導入が必要だと考え始めました。

「そのときに、ふと思い出したのが、半年前に日立ソリューションズの営業から紹介を受けていた『CylancePROTECT』というマルウェア対策製品でした。AI(人工知能)ベースの検出エンジンが特長でしたので、まだパターンファイルに載っていない新種のマルウェアや亜種にも対応できるのではないかと考えたのです」(川出氏)

ＫＶＫから依頼を受けた日立ソリューションズは、早速、未知のマルウェア対策ソリューションの提案書を作成して情報システム部を訪問。「CylancePROTECT」やバックアップ、サンドボックスなどを組み合わせたソリューションの効果を日立ソリューションズのセキュリティエンジニアが提案しました。

この提案を受けて、ＫＶＫはまず「CylancePROTECT」の無償トライアル制度を利用し、ＫＶＫの社内ネットワークがどのような脅威にさらされているかを確かめてみました。

「試用アカウントを用意していただき、情報システム部のセキュリティ担当者を管理者として登録。

Interview

株式会社 KVK
情報システム部
情報システム課
課長
川出　淳二 氏

情報システム部内のPCにインストールしました。当社の場合は11月の感染の影響が残っていることも考えられましたので、既存ファイルも含めてスキャンするように設定。以前にマルウェア対策ツールで検知・隔離していたマルウェアの標本も流してみて、きちんと検出できるかを確認しました」(川出氏)

導入時の取り組み

国内外の約750台のPCに社内ネット経由で自動的にインストール

試用期間の終了後、その期間中のログファイルを日立ソリューションズに送り、どのようなマルウェアを検知できたのかを調べました。

「2017年2月にはログファイルの調査結果を当社に報告していただきました。11月の感染の際に使われた、Tor通信(経路秘匿通信)を行うマルウェアが再び送られてきていることを、きちんと検知できていました。社内の他システムや仮想環境に悪影響を及ぼさないことも確認。試用期間中に発見された未知のマルウェアについて、それがどのようなマルウェアか、どの程度の危険性を持つものなのか、といった詳しい説明もありました。これなら間違いなく使える、と判断し、同月に導入を決定。外部とのやり取りが多い部署から段階的にインストールしていくことにしました」(川出氏)

最初のインストール先としたのは、全国の営業所とカスタマーサービスの部署に設置されているPC約250台です。展開は、日立製作所の統合システム運用管理ツール「JP1」の資産・配布管理機能を利用。自動的にインストールを実行する"サイレントインストール"方式で行いました。インストール時の設定は、試用時と同様、既存ファイルもスキャンさせるやり方にしました。この方法だとその都度、多くの検知メッセージが管理者に送られてくるため、30台程度を1回の単位として、何日かかけて段階的に展開していきました。

その後、同社は500ライセンスを追加で導入し、社内ネットワークに接続されているすべてのPC(工場の生産ラインなどを含む)と海外拠点にも「CylancePROTECT」を組み込んでいきました。

導入の効果

感染被害がないことが最大の効果 作業量や工数を低く抑えた 運用管理も実現

すべてのインストールが完了したのは、2017年11月です。

「当社にとって最も重要な導入効果は、PCや仮想環境が未知のマルウェアに感染したり、ランサムウェア感染によるファイル暗号化の被害に遭ったりしていないこと。また、パターンファイル方式のマルウェア対策ツールでは見つけられなかった『望ましくない動きをするソフトウェア』(ツールバーを勝手に組み込むなど)も検出できるようになりました。まさに、これまで守れなかったところも防御できるようになった、という感じです」(川出氏)

各部署のPCへの展開はサイレントインストール方式で自動化しましたので、エンドユーザー向けの説明会を開いたり、展開時に情報システム部の担当者が立ち会ったりする必要はありませんでした。「CylancePROTECT」が何かを検知したときは情報システム部の担当者にメールが自動的に送られますから、エンドユーザー側での対処は不要です。

「情報システム部のセキュリティ担当者は、実質的に1人。『CylancePROTECT』から検知メールが送られてきたら管理コンソールで詳細を確認するという対応でうまく回っており、セキュリティの運用管理に要する作業量と工数も低く抑えられています。展開当初は検知メールが数多く来ましたが、今では1週間に1〜2回程度です。検知後はすぐに自動的に隔離されます。まったく手間はかかりません」(川出氏)

今後の展望

その他のセキュリティ対策も強化 複合的な対策も構想

未知のマルウェアへの感染対策の完了を受けて、KVKはその他のセキュリティ対策についても強化に向けた見直しを始めています。

「日立ソリューションズから提案されたサンドボックスについては、十分な費用対効果が見込めれば、他のセキュリティ機器を更新する際に併せて活用したいですね。また、各部署に設置されているファイルサーバー用のネットワーク接続ストレージ(NAS)を全社のファイルサーバーに統合しようという構想も検討していきます」(川出氏)

「顧客の状況を理解したうえで最適な提案をしてくれるITベンダー」というのが、日立ソリューションズに対するKVKの評価です。セキュリティの脅威がますます高度化・深刻化する今、日立ソリューションズは費用対効果が高い確かなセキュリティソリューションを提供していきます。

流し台用シングルレバー式シャワー付混合栓
(KM6101EC)

Company Profile

〈富加工場〉

株式会社 KVK(ケーブイケー)

本社所在地	岐阜県岐阜市黒野308番地
設立	1949年1月25日(創業は1939年)
従業員数	1,253人(連結、2017年3月31日時点)
事業内容	水栓金具、継手、排水金具、水栓部品の開発・製造・販売

http://www.kvk.co.jp

※本事例の内容は取材時点(2018年2月)の情報です。※本文中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記しておりません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本文中の情報は、事例作成時点のものです。

本事例のwebページはこちら
www.hitachi-solutions.co.jp/cylance/case08/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/cylance/

J18K-03-05　2023.07