aruba
a Hewlett Packard Enterprise company

HPE Aruba リーナ通信

vol. 35

WannaCryの対策がワカラナイ…
HPE Aruba的ランサムウェア対策のススメ

皆様
日本ヒューレット・パッカードの重村リーナです。
本メルマガをご覧頂きありがとうございます。

朝晩はひんやりしていることもありますが、日中はかなり暑い日が続いています。
営業って本当に体力勝負だと実感する毎日です。

いやはや、本当に暑い…

皆様、熱中症対策も含めてしっかりケアしていただければと思います。

私も何か暑さ対策を講じねば、と考えていたところ、
ゴールデンウィークに開催されたとあるイベントに参加したことを思い出しました。

暑さ対策になるイベントというか、背筋がぞくぞくするという感じのイベントなんですけど…

そう、それは“ゾンビ”に追いかけまわされるというイベントです。

鹿島アントラーズが開催した参加者体験型イベントで、いわゆる謎解きをしながら
ミッションをクリアしていくという“リアル脱出ゲーム”のようなもの。
サッカースタジアム内で徘徊しているゾンビから逃げつつ、謎を解いていくイベントです。

ファンイベントの一環として、OBで元日本代表の中田浩二さんなどもいらっしゃると聞いて、
ぜひ参加してみようと思った次第です。

謎解きと事前に聞いていたのですが、開始直後からスタジアム内のあちこちで悲鳴が響き、
気付いたら真後ろにゾンビが迫ってくる状況に。な、謎って！？

でも、しっかり押さえておきましたよ、記念の一枚を。

元日本代表の名良橋晃さんです！！

な、名良橋さん、ゲストって聞いていましたけど“ゾンビ”枠で参加していたとは…

逃げ回っている最中に偶然お見掛けし、強引に写真を1枚。

生まれて初めてです、ゾンビに写真をお願いするの。

背筋がゾゾっとする割には、走り回った挙句に疲れ果ててしまい
ひんやりするような涼を感じるイベントとはならなかったようで…

でも、とっても楽しいイベントでした！！

今回は、猛威を振るうランサムウェア「WannaCry」について、その特徴を学びながら有効な対策についてご紹介。実際には大輔PCがランサムウェアに感染して大騒ぎ！そんな中で、新キャラ「ディーン」が登場し、有効なマルウェア対策の極意を披露します。ぜひお楽しみに！

WannaCryの対策がワカラナイ…
HPE Aruba的ランサムウェア対策のススメ

大輔の自宅PCが、今猛威を振るっているランサムウェアに感染、
すべてのファイルが暗号化されてしまった！
助けを求める大輔に、新たなメンバー、ディーンが新たに登場して
その解決策を伝授！
自業自得の大輔、またしても残念な結果になってしまうのか！？

大輔（だいすけ）

A市役所のIT推進室から転職して、現在は世界的なお菓子メーカーであるD&W社の情報子会社に転職。ネットワーク統括部のメンバーとしてグローバルなIT基盤の運用管理を担う。実際にはITの知識があまりなく、いつも周囲に頼ってばかりいる。

美咲（みさき）

大輔と同じくA市役所職員から転職した、もと大輔の部下。大輔が所属する情報子会社の親会社にあたる、グローバル本社のD&W社システム企画部に所属。社会人歴はわずか3年ほどだが、平成生まれのデジタルネイティブ世代として、ITの知識は豊富。

ディーン

D&W社のシステム部門に在籍する留学生・インドネシア人。ネットワークやセキュリティのスペシャリストながら、日本の文化に傾倒、大輔や美咲よりも日本のカルチャーに詳しい。

た、大変だぁ！！

なんか遠くから叫び声が聞こえるな。あの声は…あ、やっぱり大輔さんですね。

おお、美咲くん、大変だよぅー。PCが、完全にロックされてしまった！

何です、藪から棒に。ロックされたとはどういうことです？

自宅で動画編集用に古いPCを使ってたんだけど、なんか急に暗号化されちゃって。解除するなら金払えって表示が出たまま何もできなくなっちゃったんだよぅ。何が起こっているんだろう？

ああ、今話題のやつですよね。「WannaCry」に感染したんですね、きっと。

ワカラナイ？何それ。

WannaCry（ワナクライ）ですよ。ランサムウェアの一種です。
結構厄介なマルウェアのようで、ちょうどいろんなところで注意喚起されていましたね。結構被害が広がっているようですね。

ハンサムウェアって素敵な男子だけが感染するやつでしょ？
そうかー、IT業界にもハンサムなのがばれちゃったか。

ハンサムはスルーしますよ。でも、何でパッチを当ててなかったんですか。

だって家のPCってWindows XPだし。
そんな古いOSのパッチなんて、もう出てないでしょ？

このWannaCryについては、問題の大きさを考慮してか、マイクロソフトも緊急のパッチを出しています。結構ニュースになっていたのに。

えー！？そうなのか。どうしたらいいんだろう。

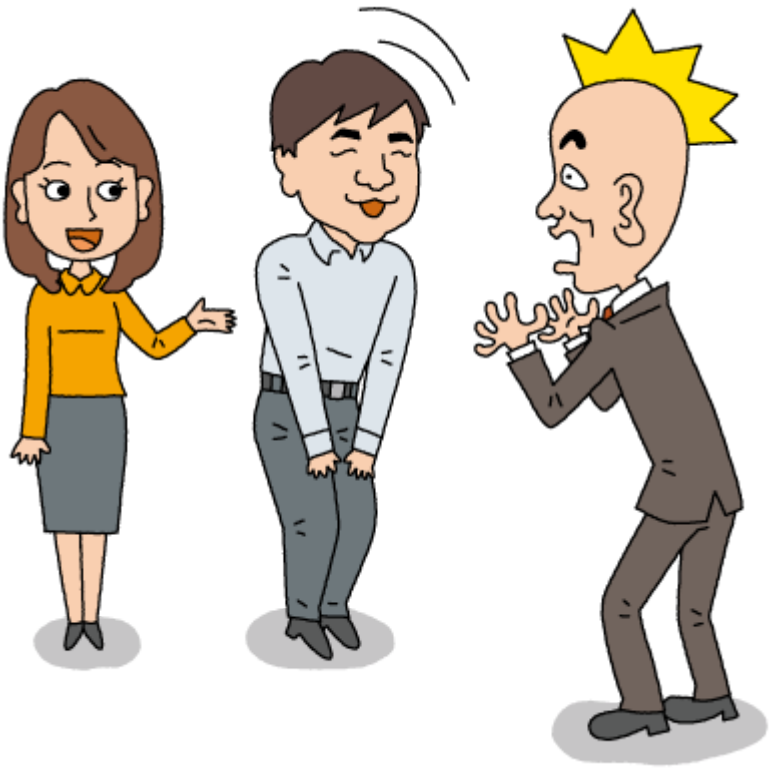
今のところ復旧ツールは出ていないようですし、クリーンインストールするしかないんじゃないですか？まさか攻撃者にお金を払うわけにもいかないし。

そうかぁ。トホホ…

まあ大輔さんは個人の被害ですけど、企業の中で感染してしまうと大事です。
どうやら暗号化してお金を要求するだけでなく、DOUBLEPULSAというバックドアも同時に仕掛けられ、別のマルウェアに感染させられたりするようですよ。
感染しないようにパッチはしっかり適用するとして、感染した場合に備えてその対策を練っておく必要がありますね。

でも、どうしたらいいんだろう。

そのことで、ちょうどディーンと話をしていたんですよ。ね、ディーン。



はじめまシテ。ディーンと言いマス。

ど、どうも。美咲くん、どなた？まさか美咲くんの、こ、こ、こ、こ（恋人）…

にわとりじゃないんだから。
彼は、先月入社したばかりの新人で、インドネシアから来た留学生です。

あ、そうなんだ。でも、なんかほっとしたよ。

なんで大輔さんが、ほっとするんですか。

いや、まあ、美咲くんは僕にとって娘みたいなもんだからさ。
でWannaCryの対策ってどうするの。

万一感染した場合、ネットワーク上でどうやって遮断するとかでしょうか。
何か個別の仕組みを用意するしかないのかなと思っていたんです。

そこで、先ホド美咲先輩に今の会社のインフラ構成を教わっていたのデス。
いい方法がありまスヨ、この構成であレバ。

いい方法？僕のPCも救ってくれる？

それは難しいと思いますケド。いずれ、これから対策するナラ、ClearPassと振る舞い検知のソリューションを組み合わせるこトデ、ネットワークの遮断ができまスシ、問題があれば、検疫サイトに誘導してパッチを適用させるといったこともできるようになりマス。

あ、そうか！ClearPassでやればいいのか。

そうなりまスネ。

でもどうやって検知するの？ClearPassに検知する機能なんてあったっけ？

実はいいソリューションがあるんデス。NIARA ANALYZERってご存知でスカ？
最近HPEが買収したソリューションで、ClearPassと連携することでマルウェアの拡大を防ぐことができるんデス。

NIARA ANALYZERって初めて聞いたな。

いわゆるUEBA（User and Entity Behavior Analytics：ユーザー／エンティティ挙動分析）ソフトウェアと呼ばれるジャンルのものデ、社内のトラフィックを監視、検知する仕組みです。ある意味ネットワークを理解するSIEM（Security Information Event Management）のような存在だと言えます。

シーム？
お菓子や食材を真空パックするときに空気を抜く“シーラー”なら知ってるけど。

逆に、それは知らないです…
SIEMはサーバーやネットワーク機器からの膨大なログを収集管理し、不正を検知する仕組みですよ。ネットワークのトラフィックをモニタリングして分析し、そこから問題のあるトラフィックを検知するってやつです。

さすが、美咲先輩。理解が早イ。
特にNIARA ANALYZER強いノハ、ビッグデータから機械学習を通じてそのパターンを認識シ、わかりやすい形で解析結果を表示してくれるというところデス。

でも今回のランサムウェアって初めてのものじゃないの？
まだ解析できるほど学べてないのでは？

通常のトラフィックとは異なり、大量のDNSエラーや不明なサイトへのアクセスが頻発するタメ、異常はすぐに検知できるはずデス。過去のデータもNIARA ANALYZERのほうでパターン化できますシ、トレーニングなしでもランサムウェアのモジュール側で対応できるようになっていマス。

検知した後はどうするの？

ClearPassと連携し、感染したと思われる端末の通信を遮断できマス。今回のWannaCryはSMB v1のホールを探し、他の端末にも感染しようと試みマス。通信を遮断するコトで被害の拡大を最小限に防ぐことができるようになるのデス。

でも、新しいソリューションだと連携とか大変だし、運用もバラバラのメーカーだとやりにくそうですね。
できれば提供してくれるところは統一しておきたいところですね。

それは好都合デス。ちょうどこの前買収されたようですヨ、HPEに。

NIARA ANALYZERが？それは都合がいい！でも、その前にすべての端末にパッチが当たっているかどうか、全部チェックしておかないと。

ClearPassが入っていレバ、ClearPass Onguardでパッチが当たっているかどうか確認できますヨ。当たってないものがあレバ、強制的に検疫サイトへ隔離し、パッチを適用するように警告すればいいわけデス。

万一感染したらNIARA ANALYZERが検知してくれて、ClearPassと連携して遮断してくれると。

おっしゃる通りデス。

うちの会社の対策としてもよさそう。すでに導入済みのClaerPassと連携してランサムウェア対策できるなんて。大輔さん、どう思います？

いいと思うんだけどね。でも、僕のPCはどうしようもないわけでしょ。

それは大輔さんの自業自得…

ジゴウジトク！？どういう意味でスカ。

身から出た錆というか…

おぅ、体から錆が出るのでスカ。なかなか不思議な表現ですネ、日本語って。

いや、日本語について“感心”しないで、僕のPCに“関心”持ってよ。

いやー、自分の身に起こると思うト“寒心（かんしん：ぞっとすること）”ですネ。

おあとがよろしいようで…ってよろしくないよ！！誰か助けてよー…

バックナンバー

- vol.34「クラウドWi-Fiをコストから比較する！最適選びの勘所」
- vol.33「見えない現場の管理、障害対応はどうする？クラウドWi-Fiあるある」
- vol.32「安易に手を出すと後悔する！？クラウドWi-Fi選び」
- vol.31「オンプレなのに過剰な投資なくスモールスタート、それホント？」
- vol.30「それってリースじゃないの？フレキシブルキャパシティの秘密」
- vol.29「新サービス“フレキシブルキャパシティ”何がすごいの？」
- vol.28「端末を離さない“スティッキー対策”の有効打」
- vol.27「目に見えない無線LAN、音声品質を的確に把握する方法とは？」
- vol.26「ワークスタイル変革に最適な無線LANの心得」
- vol.25「また手作業？端末証明書の“セルフサービス化計画”を発動」
- vol.24「妨害電波を出すAPが登場！テザリングを無効化する技」
- vol.23「ClearPassが内部情報漏洩対策に？アクセス制御の極意を学ぶ！」
- vol.22「新シリーズ「ClearPassによる安全対策のイロハ」スタート！」
- vol.21「WAN回線の障害で認証できない… IAPならできる、そのワケ」
- vol.20「無駄にならないIAPという選択肢」
- vol.19「卓上APで工事費ゼロ、の衝撃」
- vol.18「計算し忘れたAP工事費の後始末〜前編〜」
- vol.17「SSIDを増やしてゲストに開放！遠隔地のAP設定に便利なツールとは？」
- vol.16「トラブル発生でも大丈夫！原因究明に役立つAirWaveログの実力」
- vol.15「他拠点への展開、遠隔地のAP管理もお手軽簡単に“見える化”」
- vol.14「失念していた予備APのバージョンアップ、その対処法は？」
- vol.13「30台のAP、LANにつなげるだけで自動設定できるスゴ技」
- vol.12「天井設置が要らないAP！？無線LAN工事のすごワザ」
- vol.11「コントローラ内蔵APが現場を救う！ 無線LAN導入のススメ」
- vol.10「予知できるから安心！無線LANトラブルの回避 トリガー設定編(4/4)」
- vol.9「予知できるから安心！無線LANトラブルの回避 トリガー設定編(3/4)」
- vol.8「大量通信の容疑者は誰だ！？無線可視化でわかること」
- vol.7「無線LANアラートの閾値設定の方法、教えます！」
- vol.6「マップから異常なAP、見つけた！！無線LAN障害の対処法」
- vol.5「チャネル使用率から原因を絞ってみると… 無線LANトラブル解析」
- vol.4「クライアントのヘルス値が下がった要因とは？無線LANの健康状態を探る」

- vol.3「無線LANがおかしい、21:30に何が起こっていたのか？」
- vol.2「見えるから解決！ 無線LANトラブル トラブル1 うまくつながらない！(2/2)」
- vol.1「見えるから解決！ 無線LANトラブル トラブル1 うまくつながらない！(1/2)」