サイバー攻撃と脆弱性の動向
～2019年を注意喚起と共に振り返る～

JPCERTコーディネーションセンター
早期警戒グループ 脆弱性アナリスト
平岡 佑一朗

JPCERT/CC とは

- **一般社団法人 JPCERT コーディネーションセンター**
  Japan Computer Emergency Response Team / Coordination Center
  - コンピュータセキュリティインシデントへの対応、
    国内外にセンサをおいたインターネット定点観測、
    ソフトウエアや情報システム・制御システム機器等の脆弱性への対応
    など　**我が国における「セキュリティ向上を推進する活動」**を実施
  - **サービス対象: 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）**
  - インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**我が国の窓口となる「CSIRT」**
    ※各国に同様の窓口となるCSIRTが存在する
    (例：米国のUS-CERT, CERT/CC, 中国のCNCERT/CC, 韓国のKrCERT/CC)
- 経済産業省からの委託事業として、
  サイバー攻撃等国際連携対応調整事業を実施

「JPCERT/CCをご存知ですか？」

JPCERT/CCの活動

インシデント予防　インシデントの予測と捕捉　発生したインシデントへの対応

脆弱性情報ハンドリング

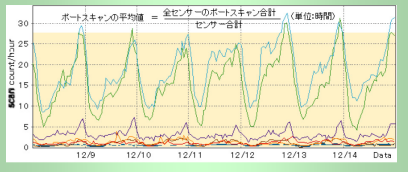
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

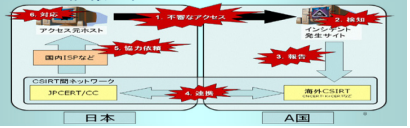
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応調整支援）

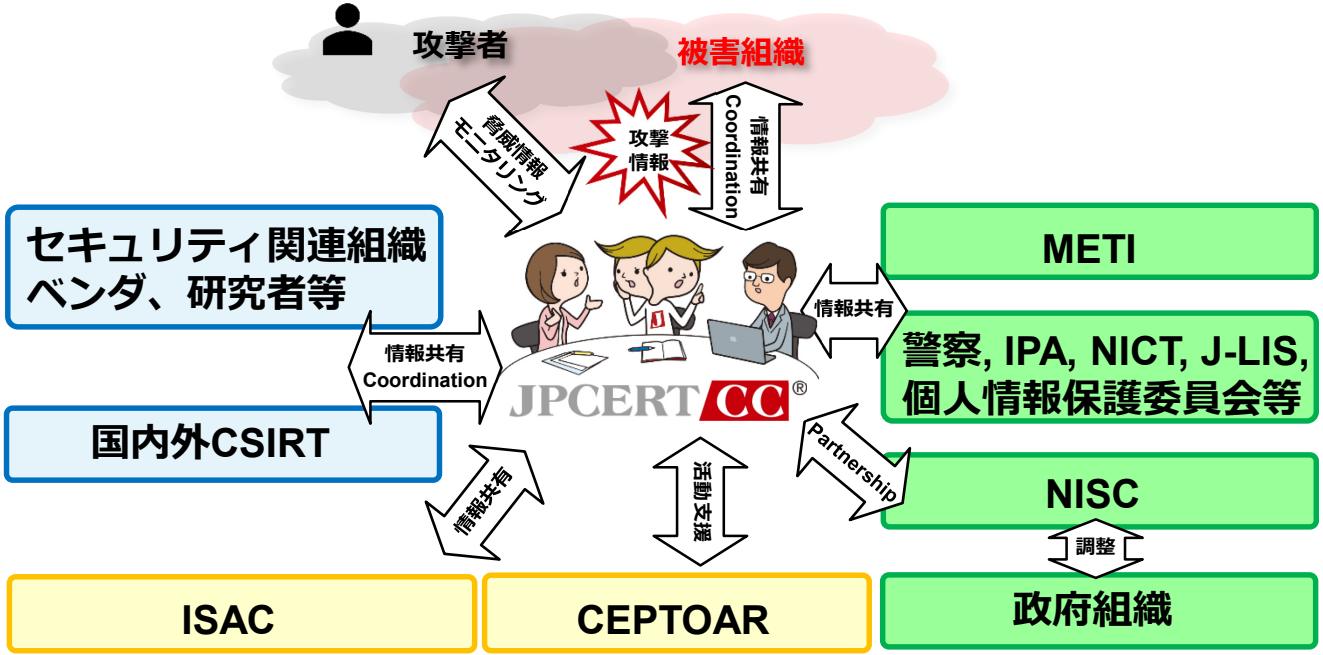
- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
脆弱性情報ハンドリング	ソフトウエア製品等の脆弱性情報に関わる開発者等との調整・公表
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
制御システムセキュリティ	制御システムに関するインシデントハンドリング/情報収集,分析発信
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

コーディネーションセンターとしての役割

■様々なパートナーとの調整



インシデントに関する調整 (coordination) 機関として、問題解決に向けて、必要な人に必要な情報を届ける業務を行っています

JPCERT/CCの活用

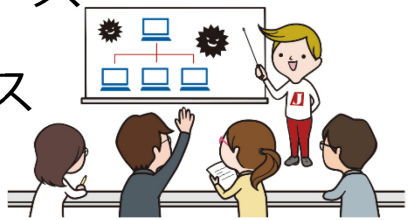
■ コーディネーションセンターの役割と活用

- インシデントレスポンス
- 脆弱性・脅威情報に関する情報流通
  - ■ 脆弱性情報 【JVN】
  - ■ 脅威情報、注意喚起、早期警戒情報他
- アーティファクト分析【検体解析など】
- 国内外 のCSIRT 連携促進、コミュニティ推進

“インシデント”に向き合った活動を展開しています

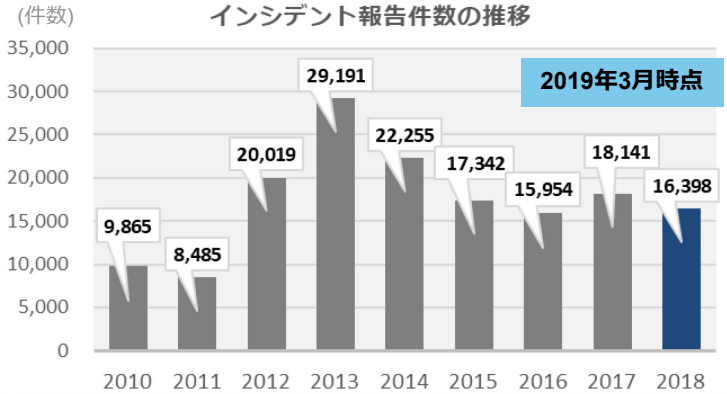
■ 例えば、こんなときにお役立てください

- **インシデントが発生し、初動対応での技術的な支援や情報が必要**となるケース
- **日々の対策を進める上で、脆弱性や脅威に関する情報が必要**となるケース
- その他、お気軽にご相談ください



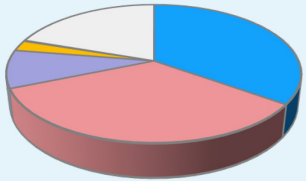
インシデント対応状況（2018年4月～2019年3月）

- JPCERT/CCへの報告
  - 全報告件数
    16,398件
  - 全インシデント件数
    16,464件
- JPCERT/CCからの連絡
  - 全調整件数
    9,835件



JPCERT/CC インシデント報告対応四半期レポートより
https://www.jpcert.or.jp/ir/report.html

インシデント件数のカテゴリ別割合



カテゴリ	割合
スキャン	38%
Web サイト改ざん	6.2%
フィッシングサイト	35.4%
マルウエアサイト	2.4%
DoS / DDoS	0.2%
標的型攻撃	0.2%
その他	17.6%

最近行われているサイバー攻撃

BEC と呼ばれる問題について

BEC とは何か？

- **Business Email Compromise (ビジネスメール詐欺)**
  - 明確な定義は難しいかもしれない
    - インターネット上にある国内外の各組織での文章を読んでも“ゆらぎ”が見られる
    - “ゆらぎ”に見られる国内の代表的な文言
      - 海外の取引先や自社の経営者層等になりすまして、偽の電子メールを送って入金を促す詐欺 (警察庁より)
      - 偽の電子メールを組織・企業に送り付け、従業員を騙して送金取引に係る資金を詐取するといった、金銭的な被害をもたらすサイバー攻撃 (IPA より※)
  - 統一した見解を立てるとしたら

    「メールを起点として組織が金銭詐欺にあうケースがある」ということ

引用: IPA ビジネスメール詐欺「BEC」に関する事例と注意喚起（続報）
https://www.ipa.go.jp/files/000068781.pdf

BEC とは何か？

- **電子メールを用いて、組織に金銭的な被害をもたらすサイバー攻撃**
  - 口座変更で入金を促す詐欺はその一つに過ぎない
  - ただし、この攻撃の過程で公開されていない取引情報が悪用されているケースがあり、情報漏えいの被害も発生していると考えられる
- **注目したい二つの文脈**
  - **金銭的利益を背景とする攻撃**
  - **電子メール等によるもの**
- **Verizon DBIR に見るインシデント背景**
  複数の組織からの報告を分析した資料
  - インシデントの背景
    - Financial と Espionage
  - **Financial のウェイトは約 7割**

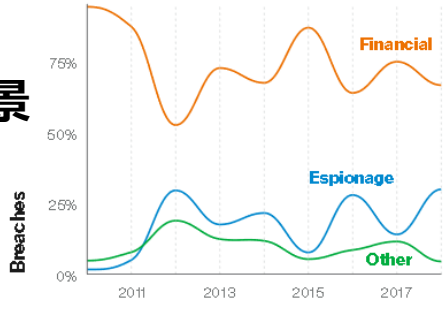


Figure 7. Threat actor motives in breaches over time

引用：verizon 2019 Data Breach Investigations Report（DBIR）
http://www.verizonenterprise.com/verizon-insights-lab/dbir/

【参考】世界の BEC から ～ FBI 編～

- **Operation WireWire (2018)**
  - International Business E-Mail Compromise Takedown
    - https://www.fbi.gov/news/stories/international-bec-takedown-061118
  - **ナイジェリア(UTC+1)** などで74人を逮捕
- **Operation reWired (2019)**
  - Worldwide Sweep Targets Business Email Compromise
    - https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019
  - **ナイジェリア(UTC+1)** など (日本含む) で281人を逮捕
    - Romance Scam と Lottery Scam が大半を占めている
- 「ふーん、そうなんだ」
  - IT側から見れば、
    「スパム？」と尋ねられれば単純にスパムの問題

偽ドメインとBECとマルウエア

- **BEC にはランサムウエアが付きまとうことも**
  - 情報窃取型、RATなど
- **SilverTerrier – 2018 Nigerian Business Email Compromise**
  https://unit42.paloaltonetworks.com/silverterrier-2018-nigerian-business-email-compromise/
  - (情報窃取)
    AgentTesla, Atmos, AzoRult, ISpySoftware, SR Stealer, KeyBase, LokiBot, Pony, PredatorPain, Zeus
  - (RAT)
    NetWire, DarkComet, NanoCore, LuminosityLink, Remcos, ImminentMonitor, NJRat, Quasar, Adwind, HWorm
- **過去には、BEC に関係して取得されたと思われる複数ドメインで LokiBot 配布が確認されたことも**

https://twitter.com/anemone_fish/status/1055030172879994880

国内での被害はあるのか？

- **邦人組織が巻き込まれるケースが複数ある**
  - 日本航空から 2017年12月に報告されたケース
    - 約 21万米ドル (日本航空米国支店 航空貨物事業所)
    - 約 325万米ドル (日本航空本社 財務担当部署)
  - 耳に届くケースを集めるだけでも複数の被害がある

- **日本国内が舞台となることも**
  - 2019年3月に日本人２名を逮捕
  - 背景にはナイジェリア人などの存在
    - ここでも**ナイジェリア (UTC+1)**


朝日新聞 DIGITAL

トップニュース　スポーツ　カルチャー　特集・連載　オピニオン

新着　天声人語　社会　政治　経済・マネー　国際　テック＆サイエンス　環境・エネルギー　地域

朝日新聞デジタル ＞ 記事　社会　事件・事故・裁判　テック＆サイエンス

ビジネスメール詐欺容疑、日本で逮捕者　マフィア関与か

有料会員限定記事

杉浦達朗　2019年3月28日15時11分

シェア　ツイート　ブックマーク　メール　印刷

国際的な詐欺事件の構図　警視庁への取材から

国際的な詐欺事件の構図

企業のメールアドレスを乗っ取ってうその振り込みを指示して約１億１千万円を詐取したとして、警視庁は東京都足立区の会社役員栗田良武（５３）と、大阪市城東区の会社役員川瀬公男（５８）の両容疑者を詐欺と組織犯罪処罰法違反（犯罪収益隠匿）の疑いで逮捕し、２８日発表した。

この手口は「ビジネスメール詐欺」と呼ばれ、世界各国で被害が出ている。警視庁は昨年からの捜査で、日本の金融機関を舞台にした一連の事件でナイジェリア人の男２人を逮捕。背後に同国の国際的犯罪組織があるとみて調べている。

引用:
朝日新聞DIGITAL
「ビジネスメール詐欺容疑、日本で逮捕者 マフィア関与か」
https://www.asahi.com/articles/ASM3W7529M3WUTIL06D.html

国内での被害はあるのか？

- J-CSIP に報告された情報より
  - 過去に取引がない新規取引先を詐称したケース
    - 口座変更ではなく、見積価格の修正を装う
    - メールヘッダやアドレスの偽装
  - 海外取引先を狙ったケース
    - 自組織と海外取引先の間に入り双方の担当を騙る
    - 双方の組織に偽のメールを送信

参考：サイバー情報共有イニシアティブ（J-CSIP）運用状況[2019年4月～6月]
https://www.ipa.go.jp/files/000076713.pdf

魅惑の UTC+1 地域

- **BEC ではたびたび UTC+1 に出くわす**
  - **「ナイジェリア」**
- そして度々逮捕者が登場するのも
  - **「ナイジェリア」**

- **BEC = ナイジェリアからの手紙**
  - といっても過言ではない

- **こうした特徴は防御する上でも貴重な情報となる**

引用:
Quara.com「Which African countries have the same time zone with Nigeria?」
https://www.quora.com/Which-African-countries-have-the-same-time-zone-with-Nigeria

BEC への組織の対応

BEC への対応

- **全銀協の注意喚起から**
  - 通常の支払手続きと異なる対応を求められた場合の対処
  - 正しい電子メールアドレスを再入力し、送信先の正当性を確認
  - セキュリティ対策や暗号化
  - **電子メールを送受信する当事者となる部門**への周知
    - 経理担当だけでなく、業務上外部とメールでやり取りをする部門

- **冒頭で挙げたこと**
  「スパム？」と問われれば「スパム」
  - IT 担当部門・CSIRT 担当部門でできることは、BEC の一つの側面に過ぎない

- **BEC の問題の本質と対応**
  - ITとして対応する問題
  - 事業部門など会社として対応する問題

この二つが不可欠

全社でのリスク対応

- **だまされる、かたられる、の両方があることを認識**
  - メールによる口座変更他、“怪しい行為”は、自組織において日常的に取り扱われていませんか？
    - “怪しい行為”であっても”怪しくなくなる“
  - 自分も怪しい行為・行動をしないこと
    - メールによる“口座変更依頼”、“別グループ関係会社宛の振り込み”、“口座の監査”などなど
      - 結局、普段のやり取りと逸脱していないので、異常に気が付けない
    - 会計部門が、異常に気が付く最後の砦

- **サプライヤも含めて考えること**
  - 現在の文脈は、１対１ (被害組織 vs 犯罪グループ) だが、今後は、関係者間でどのように責任を持つかなども議論となる可能性

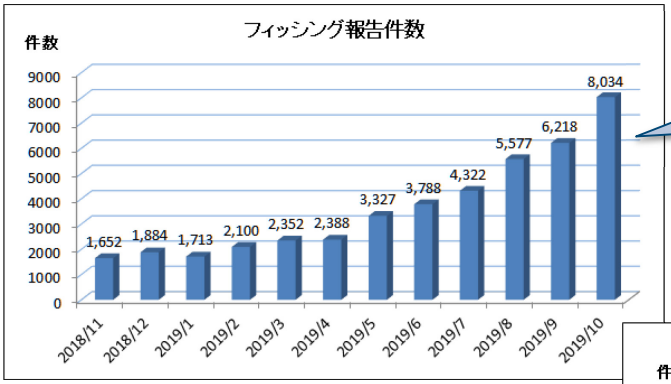
IT 部門, CSIRT 部門での対応

- **予防と事案対処の二つが不可欠**
  - **予防**
    - 不審メール、不審ドメインからのメールを、システム的に検知して担当者をサポートするしくみを導入していたり、不審メールを簡易に報告できるしくみを整備していたりする組織がある
      - 例えば、過去数カ月にわたって受信していないドメインからのメールに気を付けてみる
    - 実際に組織に届いたメールから特徴点を伝える
  - **事案対処**
    - 発覚までに時間を要する可能性
    - システムで選り分けきれなかった「何か」の特徴を見つけなければならない
      - 被害は１対１とも限らないし、自社が騙られているケースもある

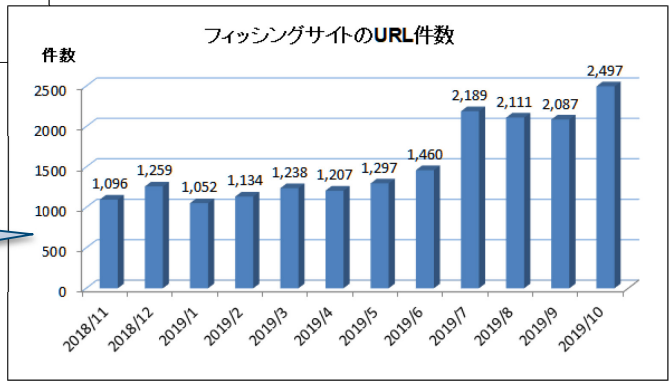
増加するフィッシングサイト

増加するフィッシングサイト

- 報告件数、URL件数ともに目に見えて増加



報告件数は約5倍



サイトのURL件数は約2.3倍

引用：フィッシング対策協議会
2019/10 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201910.html

巧妙化するフィッシング詐欺

- 国内ネットバンキングの二要素認証を狙うものが登場

引用：トレンドマイクロ セキュリティブログ
国内ネットバンキングの二要素認証を狙うフィッシングが激化
https://blog.trendmicro.co.jp/archives/22696

【参考】気象庁の報道発表を装ったメール

- 2019年11月6日 気象庁からの発表
  - 地震速報を受信できるWindows アプリを提供するという内容で気象庁の報道発表を装ったもの

フィッシングサイトを発見した際の対応

- Webサイト運営者自身で、フィッシングサイトが属するIPアドレス帯を管理する ISP に連絡してテイクダウンを行う
- 専門機関 (国内なら JPCERT/CC) にテイクダウン依頼を行う
  - テイクダウンを自ら行う場合でも、並行して専門機関に連絡しておくと、 ISP の対応がスムーズにいくことがある
- フィッシング対策協議会発行のガイドラインを参考
  - フィッシング対策ガイドライン https://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf
- JPRS が「JPドメイン名の不正登録に関する情報受付窓口」を 2019年10月に開設
  - https://jprs.jp/contact.html
  - フィッシングサイトのテイクダウンというよりは、不審なドメインの連絡をする窓口

でも・・テイクダウンは簡単ではない

- テイクダウンを行うには、フィッシングサイトを確認しにいった時点で、フィッシングサイトが稼働している必要がある

- フィッシングサイトが、第三者が運営する既存のサーバに対する不正アクセスにより作られている場合などもあり、保有組織が攻撃者か第三者か判別が難しいケースも

JPCERT/CC で取り上げた脆弱性について

JPCERT/CC が公開する脆弱性情報

- **注意喚起**
  - 国内組織において影響が大きいと判断した攻撃や脆弱性情報、セキュリティ更新などを掲載

- **CyberNewsFlash**
  - 特定の分野において影響がありそうな脆弱性、アップデートの予告など、従来の注意喚起では掲載しないセキュリティ情報を掲載

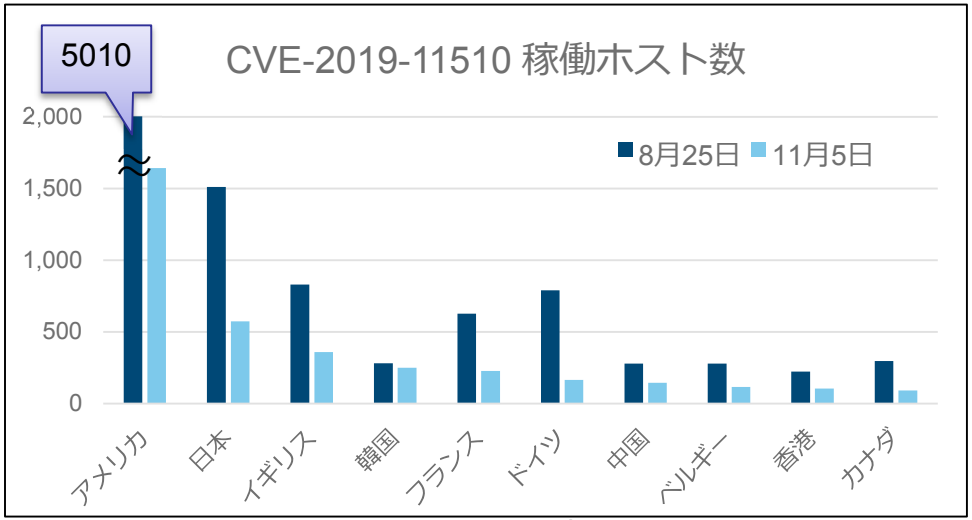
- **JVN**
  - 「情報セキュリティ早期警戒パートナーシップ」制度に基づいて報告され調整した脆弱性情報や、CERT/CC など海外の調整機関と連携した脆弱性情報を公表

2019年発行の注意喚起より

- 2019-05-15
  Intel 製品の複数の脆弱性 (INTEL-SA-00213) に関する注意喚起
- 2019-06-19
  Firefox の脆弱性 (CVE-2019-11707) に関する注意喚起
- 2019-09-02
  複数の SSL VPN 製品の脆弱性に関する注意喚起
- 2019-09-10
  ウイルスバスター コーポレートエディションの脆弱性 (CVE-2019-9489) に関する注意喚起
- 2019-09-24
  Microsoft Internet Explorer の脆弱性 (CVE-2019-1367) に関する注意喚起

複数の SSL VPN 製品の脆弱性に関する注意喚起

- Bad Packets 社が、 Pulse Secure 製の VPN 製品の脆弱性(CVE-2019-11510) を突くスキャン活動を自前のハニーポットで確認したとの情報を公開
  - Shodan 上で脆弱なバージョンを使っていることが分かるホスト数を定期的に集計している（現在も）



情報源: https://twitter.com/bad_packets

注意喚起発行までのタイムライン

- **2019/08/22:**
  - Bad Packets 社が Pulse Secure 社の VPN の脆弱性に関する大規模なスキャンを確認
  - GitHub 上に実証コードが公開される
- **2019/08/24:**
  - Bad Packets 社が専用のページを公開
- **2019/08/29:**
  - Bad Packets 社が Fortinet 社の VPN についても脆弱性を狙ったスキャンを確認
- **2019/08/30:**
  - Bad Packets 社から脆弱性があるバージョンの Pulse Secure 社 VPN が稼働している国内ホスト情報を JPCERT/CC が受け取る
- **2019/09/02:**
  - JPCERT/CC で注意喚起を公開
  - JPCERT/CC に対し外部組織から攻撃を受けた旨の情報提供
- **2019/09/06:**
  - JPCERT/CC で同製品に対する別の脆弱性の実証コードも確認
  - JPCERT/CC で情報提供の件を合わせて注意喚起を更新

そもそも各 VPN 脆弱性の修正はいつ？

- Palo Alto Networks (CVE-2019-1579)
  - **2019/07/24**
- Fortinet (CVE-2018-13379)
  - **2019/05/24**
- Pulse Secure (CVE-2019-11510)
  - **2019/04/24**

- Bad Packets 社の攻撃確認が **2019/08/23**

脆弱性が悪用される前にアップデートを実施する計画を立てるだけの時間はあった

2019年発行の CyberNewsFlash より

- 2019/05/15
  リモートデスクトップサービスにおける脆弱性
  CVE-2019-0708 について
- 2019/06/19
  リモートデスクトップサービスにおける脆弱性
  CVE-2019-0708 について(追加情報)
- 2019/10/16
  sudo コマンドの脆弱性 (CVE-2019-14287) について
- 2019/10/30
  DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メール
  について

RDS の脆弱性 CVE-2019-0708

- リモートデスクトップサービスにおける脆弱性 CVE-2019-0708 に対し、マイクロソフトが緊急の更新プログラムを公開
  - RDP を使用し、細工したリクエストを送ると任意のコードを実行する可能性がある
  - マイクロソフト公式が「Wannacry のように感染が広がる可能性がある」とブログで説明
  - のちに BlueKeep と呼ばれるようになる

- 現在ではマイニング用途でツールをインストールしたり攻撃に悪用されている

BlueKeep に関する時系列

- 2019/05/14
  - Microsoft が脆弱性を公表（この時点で悪用はなし）
- 2019/05/30
  - Microsoft がブログで更新プログラム適用を喚起
- 2019/06 上旬
  - BlueKeep をスキャンする Metasploit が見つかる
- 2019/08 下旬
  - BlueKeep を突く exploit の解説などが公開される
- 2019/09 上旬
  - Metasploit に BlueKeep を悪用できるモジュールが実装
- 2019/10 下旬
  - 海外のリサーチャーが運用する BlueKeep ハニーポットが不正アクセスによりクラッシュした報告

sudo の脆弱性 (CVE-2019-14287)

- sudoers のエントリで、root ユーザは実行できないコマンドとして定義しているにも関わらず、root 権限でコマンドが実行できてしまう脆弱性
  - ユーザ ID の検証が不十分
  - ALL キーワードで他のユーザとしてコマンド実行できる権限は設定されている必要はある

- 例

  sudoers のエントリ
  jpcert ALL=(ALL,!root) /path/to/command/aaa

  実行コマンド (実行ユーザ jpcert)
  sudo -u#-1 aaa (数値 -1 の箇所は 4294967295 も可)

DDoS 示唆し、仮想通貨を要求する脅迫メール

- メールの受信組織が管理する Web サイトや IP アドレスに対して DDoS 攻撃を行うことを予告し、仮想通貨を要求
  - 危機感を高めるために、実際に DDoS されるケースもある (最大 60Gbps の事例)
  - 観測された DDoS 攻撃の特徴
    - 攻撃手法として、一般的な DNS、NTP、CLDAP を使用した DDoS リフレクション攻撃に加え、WS Discovery や Apple Remote Management Service などを使用
    - 攻撃を受ける対象として、Web サイトだけではなく、外部から接続可能なサーバ/インフラも標的となるケース

- 攻撃者の要求に応じず、実際にDDoS攻撃が行われた場合の対応体制の確認や、対策状況の確認を推奨

まとめ

本物と見分けがつきにくい攻撃の増加

- BEC
  - 実際にやりとりのある取引相手になりすます
- フィッシングサイト
  - 実際のサイトによく似たサイトを立ち上げて誘導

- 従業員の判断で完全に回避するのが難しいケースも増えてきている
  - **システム面でのサポート**
  - **会社としての対応方針の整理**

脆弱性情報の収集と対応する体制の確認

- 各組織で利用しているサービス、機器に対する脆弱性情報の収集体制の確認
  - 自組織での OSINT
  - 外部組織に任せるところ（専門機関、ベンダ）

- 実際に脆弱性が見つかった時の対応
  - 停止しにくいシステムなどは、見つかってから対応方針を検討すると間に合わないケースもある
  - 脆弱性の影響度合いでトリアージ
    - ゼロデイか否か
    - 悪用された場合に行われること

最後に・・・

- JPCERT/CC では、注意喚起や CyberNewsFlash に掲載する情報について意見を集めています
- 掲載されている情報に関する問い合わせも含めて質問・要望がありましたらご連絡ください

— JPCERT/CC 早期警戒グループ

- ew-info@jpcert.or.jp

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

Thank you!