radware

不正ログイン/不正送金/情報漏洩の裏に潜む悪性BotやAPI脆弱性

Kazutoshi Wada
セールスエンジニアリング本部 本部長
kazw@radware.com | PMP#160930 | CCIE#27778

Oct.2020

Agenda

- About Radware
- 悪性Botとその被害
- Radware Bot Manager
- Summary



About Radware



About Radware

- 日本法人設立：2000年
  （HQ＝イスラエル：1997年）
- 株式上場：1999年（NASDAQ）
- 売上：2億5,200万ドル（2019年度）
- 従業員数：約1,100名（2020年）
- 拠点数：世界35ヵ所

- パートナー

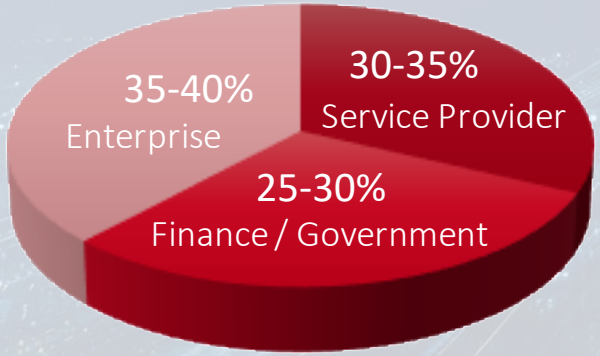
CISCO　Microsoft Azure　NOKIA　Check Point SOFTWARE TECHNOLOGIES LTD.

- サイバーセキュリティ+ADC

Gartner
ADC MQ Leader + WAF MQ Visionary

FORRESTER
DDoS Wave Leader

顧客数: 12,500社以上



金融

世界Top 12為替取引所、8社
世界Top 20銀行、10社

Bank of America　Bloomberg　Capital One　HSBC　Deutsche Bank　ING　ADP　SBI

リテール、オンラインビジネス

世界Top 10リテール企業、5社

DELTA　ebay　GAP　Marriott VACATION CLUB　PayPal　SAMSUNG SAMSUNG SDS　twitter　ups

通信キャリア、SaaSプロバイダー

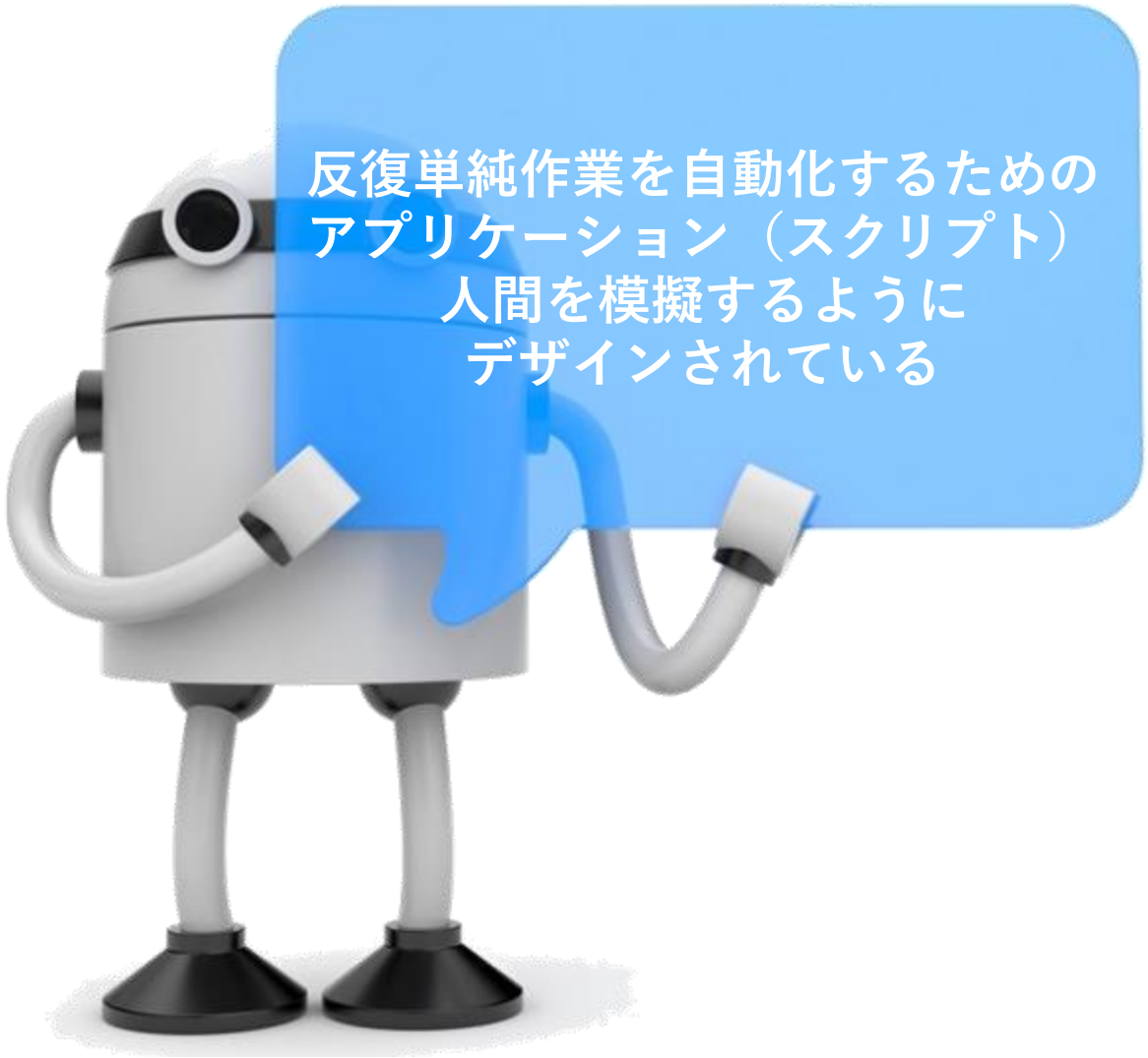
世界Top 10通信キャリア、10社
世界Top 10SaaSプロバイダー、5社

salesforce　AT&T　Cisco webex　workday　SAP　Tech Mahindra　verizon　Akamai

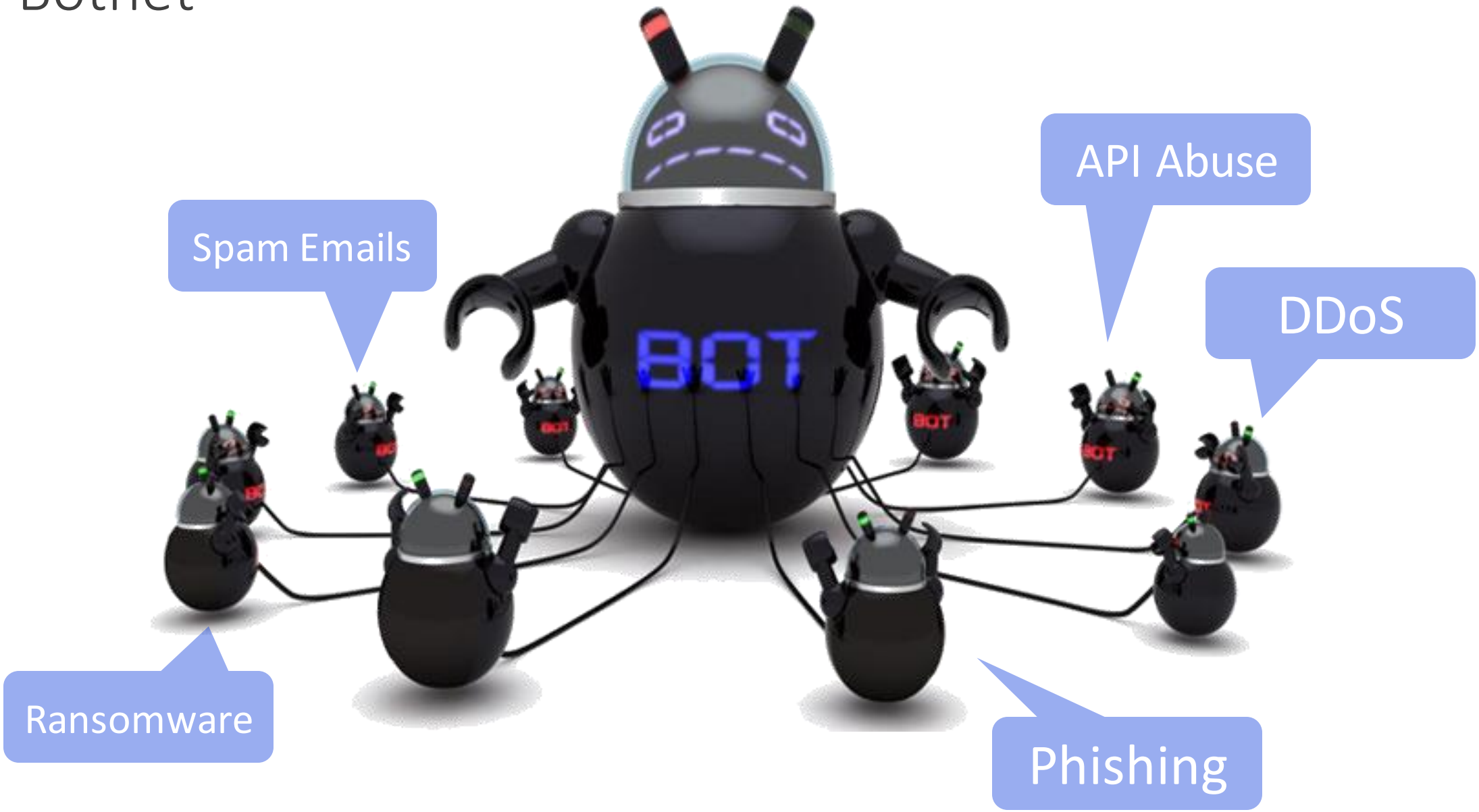
悪性Botとその被害



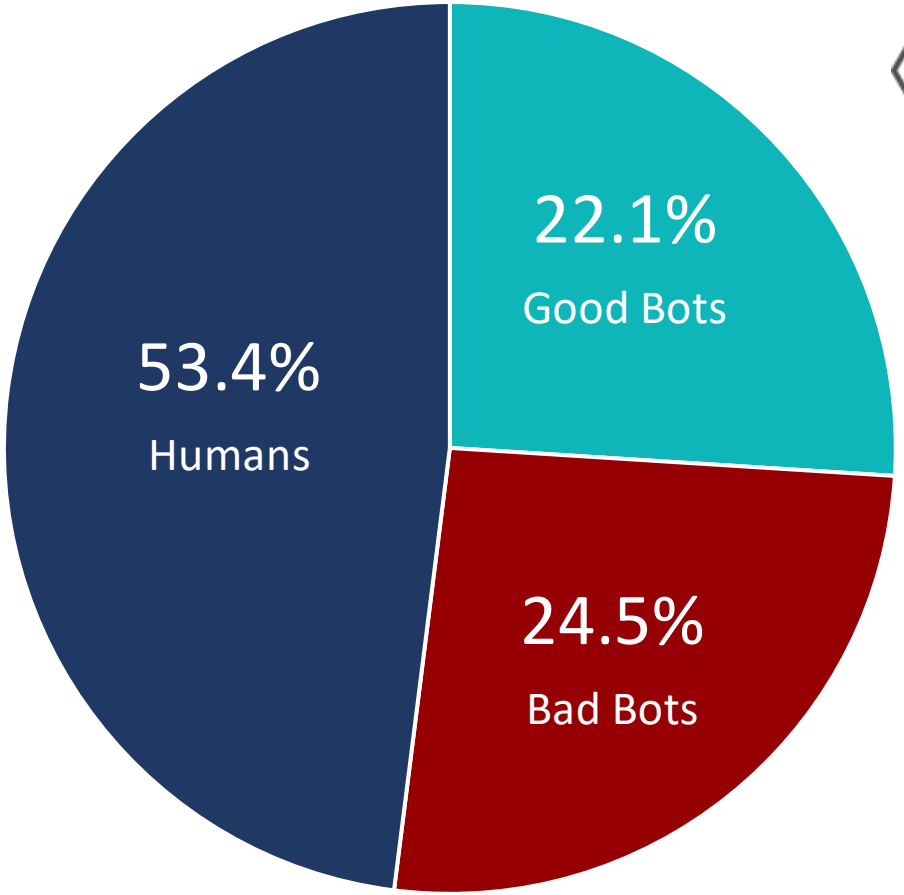
What’s Bot?

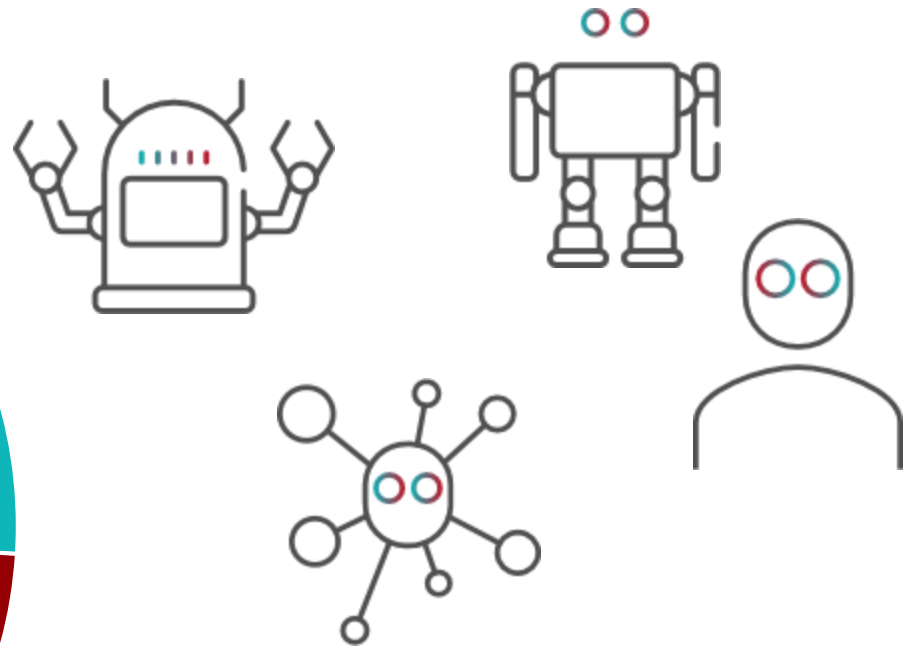


Botnet



Bots in The Internet



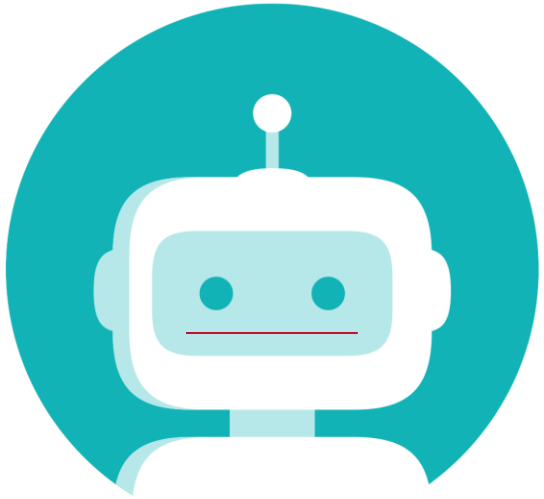


24%がBad Bots

Source: Radware The Big Bad Bot Problem 2020

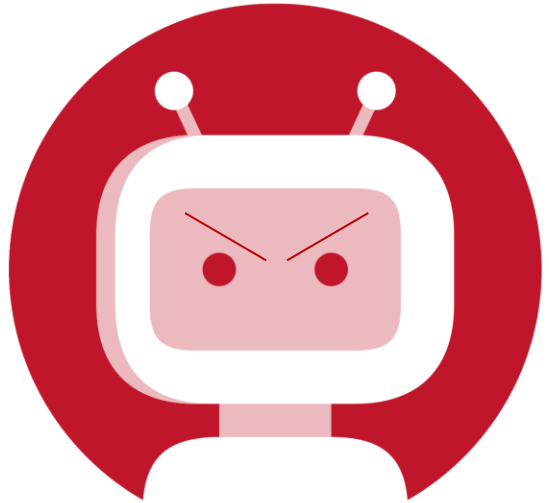
75%の組織が*Good or Bad*を判別できていない

Good or Bad?



Good Botの例

検索エンジン
チャットロボット
クローラー（スパイダー）
メディアボット
監視ボット（著作権 etc…）

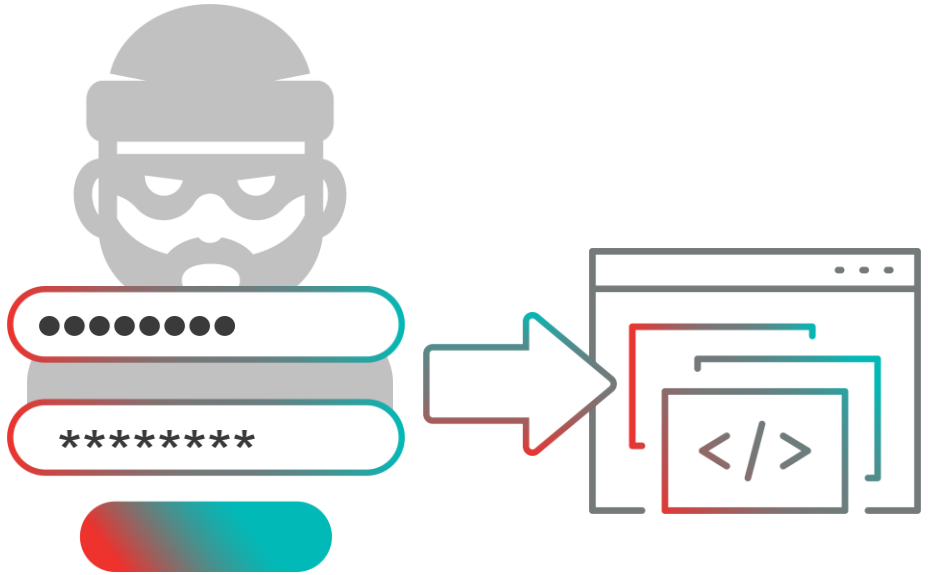


Bad Botの例

スクレーパー（複製）
アドフラウド
クリックボット
ダウンロードボット
スパイボット
ゾンビボット

Bad bot example: Account Takeover(ATO)

アカウント盗用から、製品やサービス情報を抜き出す



データ流出

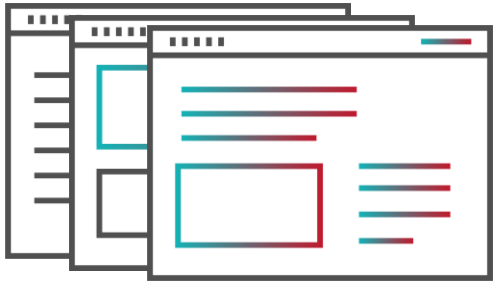
企業評価下落

経済損失

Bad bot example: Web Scraping



ウェブサイトの情報を盗み出す
フィッシングや偽サイト、SEOへの影響



87%

Scrapingは重大な脅威



40%

Scraping被害割合（週次）



データ損失



収益低下

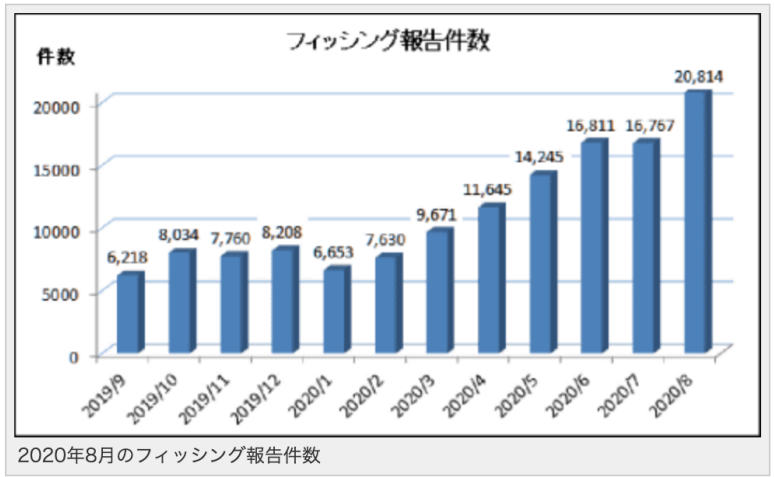
*ソース: Radware Research: Web Application Security in a Digitally Connected World, Nov 2017

Bad bot example: Web Scraping

8月のフィッシング報告は2万814件に、7月から4047件急増

Amazon関連のフィッシング詐欺が全体の7割近くに

岩本 理夢　2020年9月8日 14:58



2020年8月のフィッシング報告件数

フィッシング詐欺に関する報告が8月は2万814件に上り、7月（1万6767件）から4047件急増したことをフィッシング対策協議会が明らかにした。また、フィッシングサイトのURL件数は4953件で前月から583件減少し、フィッシング詐欺に悪用されたブランドは55件だった。

Source: Internet Watch
https://internet.watch.impress.co.jp/docs/news/1274848.html

Source: GIGAZINE
https://gigazine.net/news/20200820-instagram-tiktok-youtube-user-data-expose/

2020年08月20日 12時05分　セキュリティ

Instagram・TikTok・YouTubeのユーザー情報2億3500万人分をデータ販売会社が無断公開していたことが判明

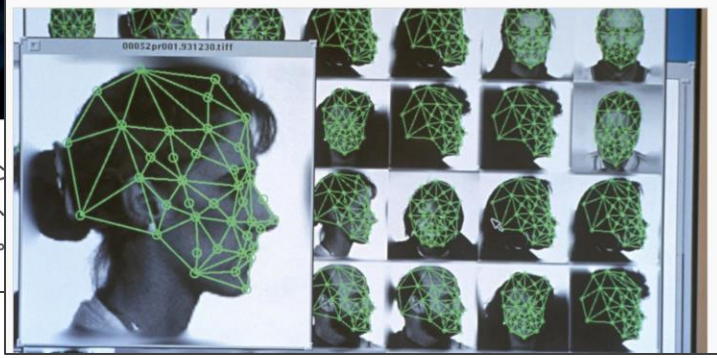


インフルエンサーの情報をマーケティン
氏名・連絡先をはじめとした個人情報、
態で公開していたことが判明しました。
されたものとみられます。

顔認識スタートアップのClearview AIがイリノイ州法違反で集団訴訟に発展

2020年2月17日 by Devin Coldewey

Source: TechChurch https://tcrn.ch/3cJP1po



■7万枚超の女性ユーザーの写真

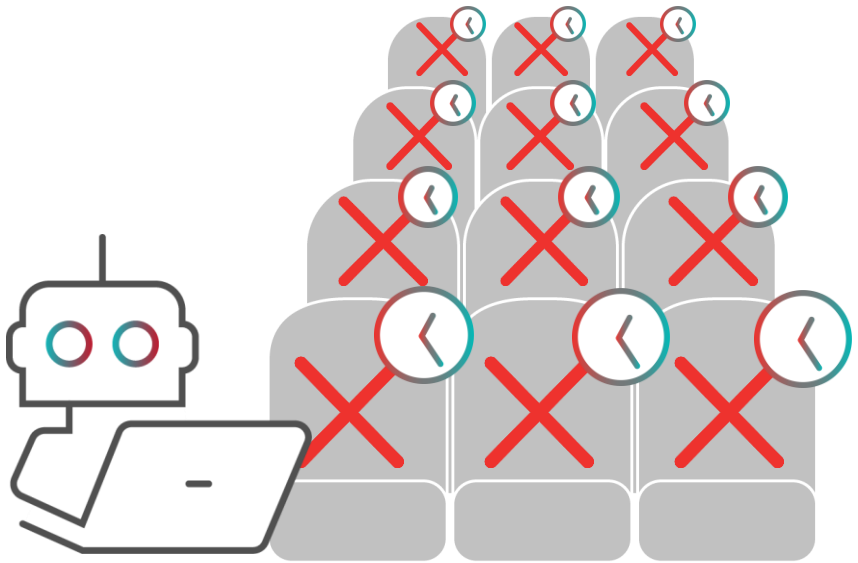
Source: SIRABEE
https://sirabee.com/2020/01/21/20162239660/

出会いを求めるアメリカの大学生の間で大流行し、4～5年ほど前から日本でも利用されるようになった「Tinder（ティンダー）」。気軽にハイスペックな男子・男性と知り合える、外国人との出会いが多い、などとも言われている。

そのTinderについて海外大手メディアがここのところ、「少なくとも7万枚を超える女性ユーザーの写真、16,000名のユーザーIDおよびテキスト・ファイルが流出した」と伝え、波紋を広げている。

Bad bot example: Deniel of Inventory

実際に購入することなく、買い物かごや予約枠を埋め尽くす



45% 品薄を経験

32% 実際に枯渇を経験

顧客損失

企業評価下落

経済損失

*Source: Radware Research: Web Application Security in a Digitally Connected World, Nov 2017

Use Case

Challenge

BotによるDeniel of Inventoryを受ける
IPが動的に変わる攻撃だった

Radware Solution

22 xWAF

Why Radware

WAFのアンチBotプロテクト
（Fingerprintingによる動的IP攻撃からの防御）
自動ポリシー作成
SSL攻撃防御の優位性

Competition

F社　　パフォーマンスで脱落
A社　　検知率で脱落

Delta Airlines Project Architect – 予約サイトは一番の収益源であり、ダウンタイムがあってはならない。Radware WAFのFingerprinting技術と自動ポリシー作成は何か問題が起きたときにすぐルールを作成し実装できるので、Radwareに決めました。

Other Bad bot examples



Account Takeover



Fake Account Creation



Carding



Gift Card Cracking



Application DDoS



Denial of Inventory



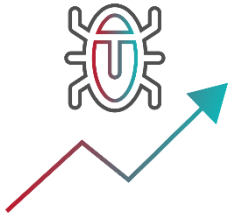
Ad Fraud



API Abuse



Price and Content Scraping



Ticket Scalping



Skewed Analytics



Form Spam

BOT Events

source: Radware Ultimate guide to BOT MANAGEMENT

2019 APR

映画 Avengers:Endgame 、イギリスの歌手 Ed Sheeran のライブチケット　Scalping被害（転売）
https://www.asiaone.com/singapore/scalpers-selling-tickets-avengers-endgame-888-carousell
https://theindustryobserver.thebrag.com/ed-sheeran-cancels-tickets-fight-scalpers/

2019 FEB

航空会社Ryanair(アイルランド) が不正なScrapingをされたとして、Expedia を米国で提訴
U.S. Computer Fraud and Abuse Act(CFAA)に違反、Ryanairに対して風評被害、ウェブサイトへの過剰負荷があったと主張
https://skift.com/2018/02/25/ryanair-files-u-s-lawsuit-against-expedia-over-screen-scraping/

2018 NOV

FBI, 国土安全保障省, Google, その他民間セキュリティ会社が大規模な詐欺広告ネットワーク（Botnet）を排除
70万台以上の感染PC + 6万アカウントで構成されていた　https://digitalguardian.com/blog/all-about-3ve

2018 SEP

British Airwaysが38万人に及ぶ可能性のある情報漏えい被害（決済システム）に遭う
これはMegacart（犯罪グループ）と連携していて、Megacartは AdMaxim, CloudCMS, Picreel10 といった企業の情報を詐取している
同様の手口でAWS S3上（設定に不備のある）に保存されているJavaScriptファイルに悪意のあるコードを追加し、
多数の企業から不正に情報を抜き取ることに成功している
https://www.riskiq.com/blog/labs/magecart-british-airways-breach/ https://www.riskiq.com/blog/labs/cloudcms-picreel-magecart/ https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets/
https://japan.zdnet.com/article/35139832/

2018 APR

panerabread.com が8ヶ月間に渡り、顧客情報を平文で流出、700万人に影響した可能性
API 上の脆弱性をつかれ、顧客方法を抜き出された
https://www.csoonline.com/article/3268025/panera-bread-blew-off-breach-report-for-8-months-leaked-millions-of-customer-records.html

2017 JUN

タイ警察の摘発により500台ものスマートフォンを利用したクリック詐欺ファームが明らかに
https://www.vice.com/en_us/article/43yqdd/look-at-this-massive-click-fraud-farm-that-was-just-busted-in-thailand

2017 MAR

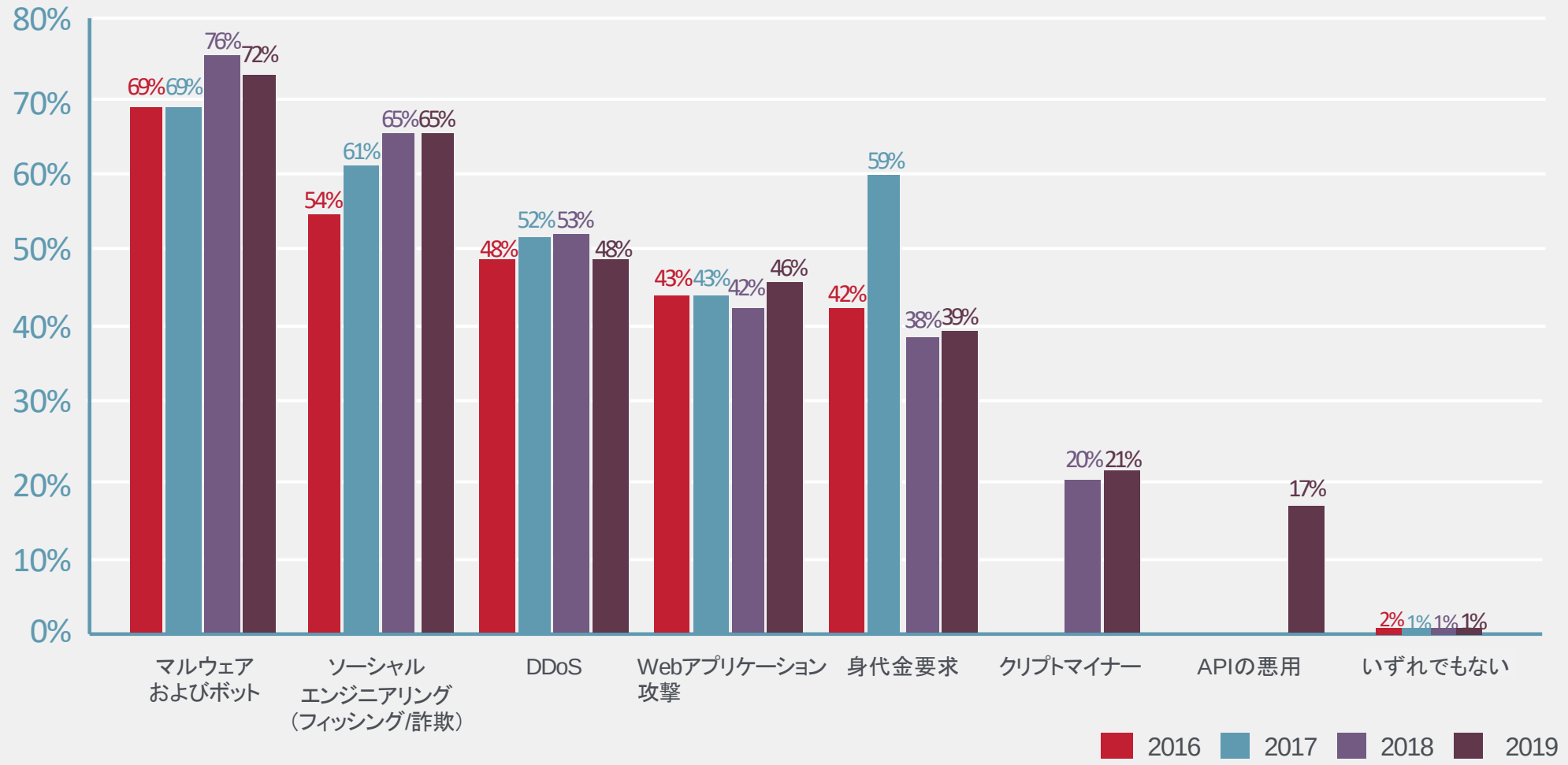
インドMcdonald のMobile Appが220万人以上のユーザ個人情報を流出　API経由の攻撃
https://www.securityweek.com/mcdonalds-app-leaks-details-22-million-customers

2016 MAY

選挙コンサルタント Cambridge Analytica がFacebookから米8700万人の個人情報をScraping
取得した個人情報を選挙活動に利用しようと試みた
https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie



2016–2019年 企業が受けた攻撃の種類



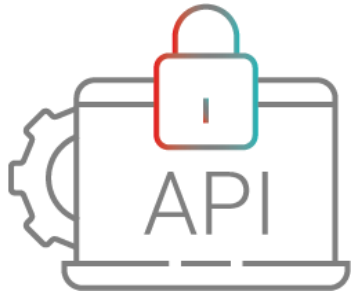
Bot Targets



WEBSITE



MOBILE
(WEB/APP)



API

情報漏えい被害

13億

流出レコード数, 2018

$150

1レコードあたり, 2019

$3.29 M

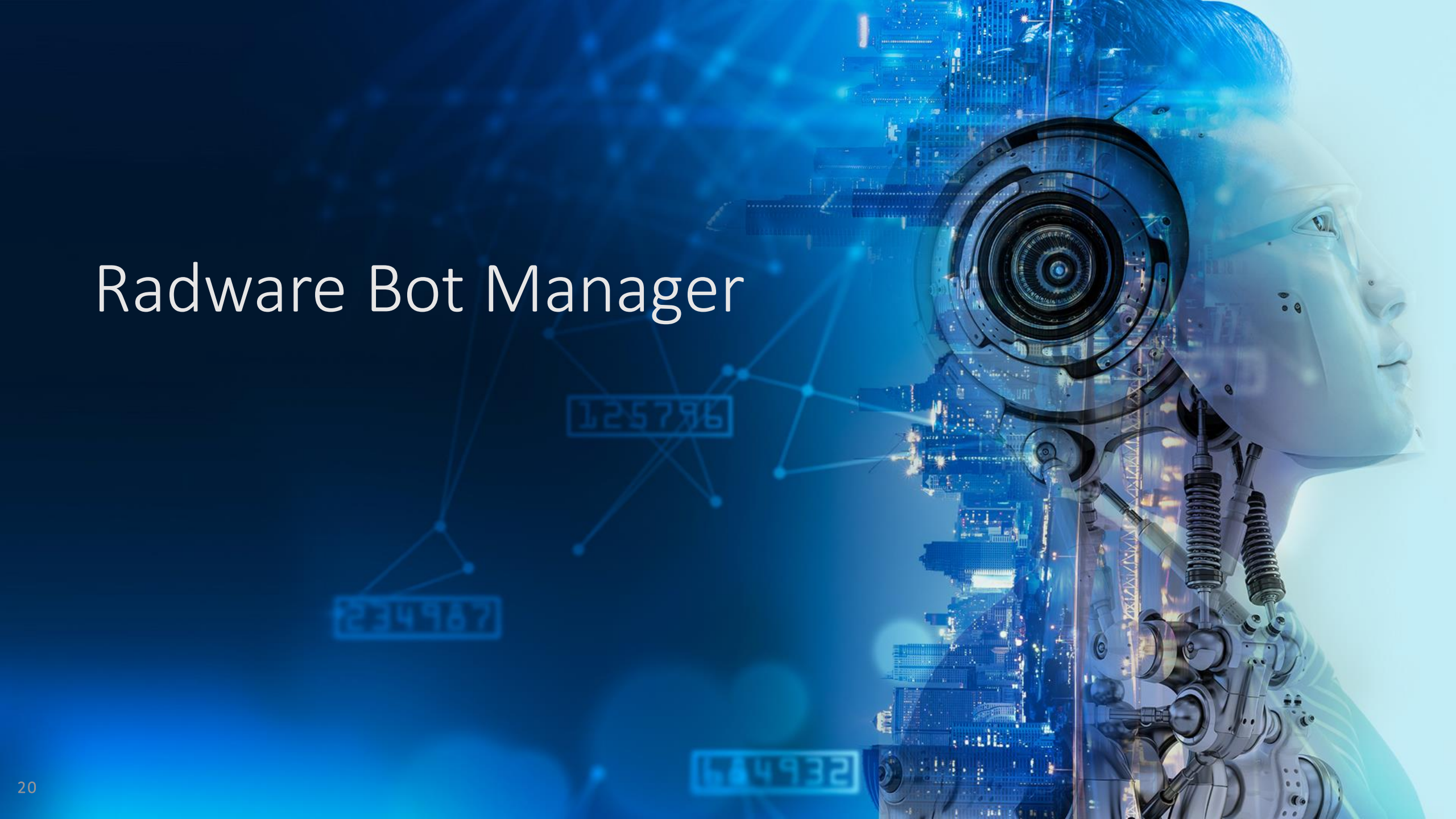
情報漏えいの
平均被害コスト, 2019

31%

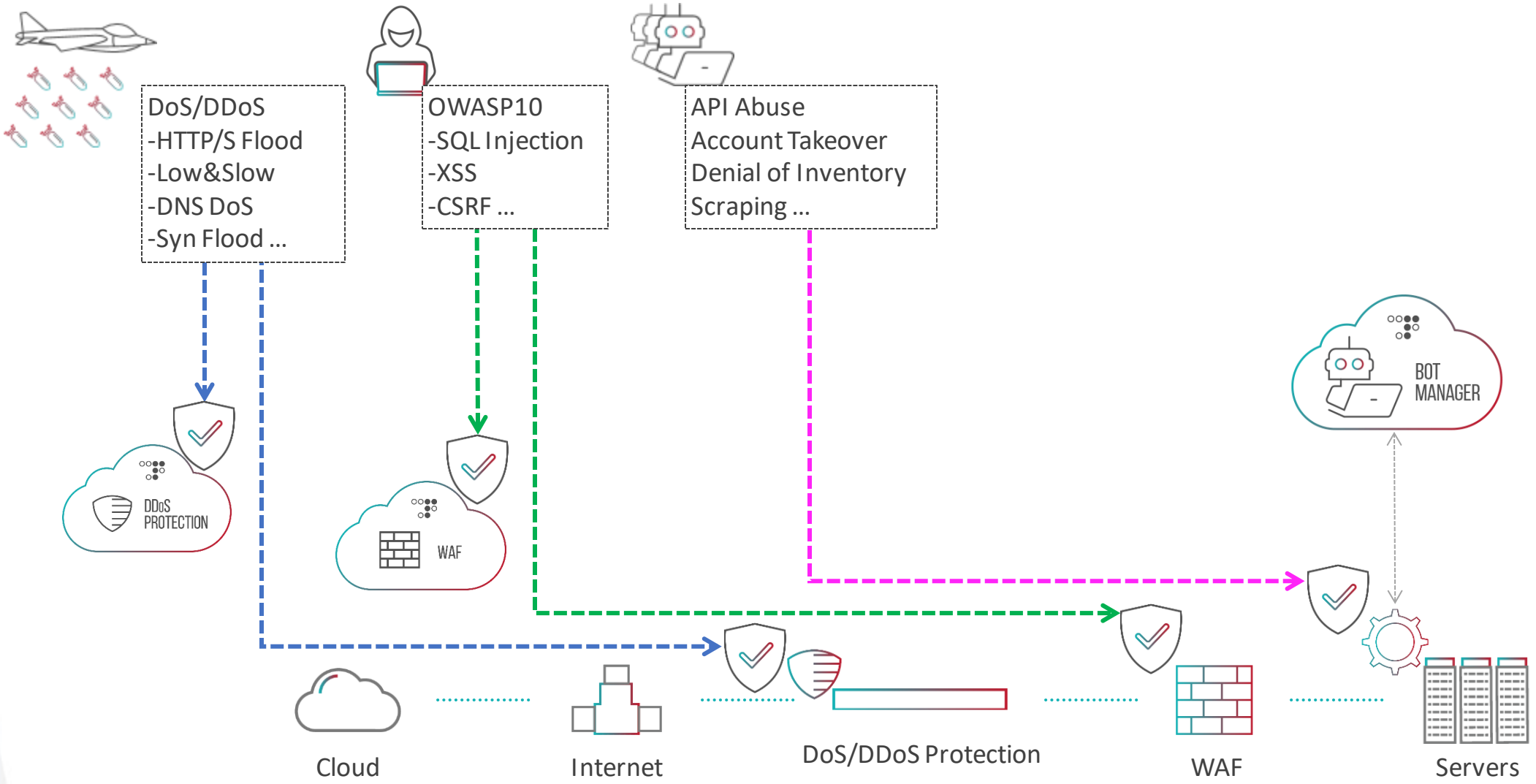
情報漏えいにより
誰かが職を失う確率

Source:Radware

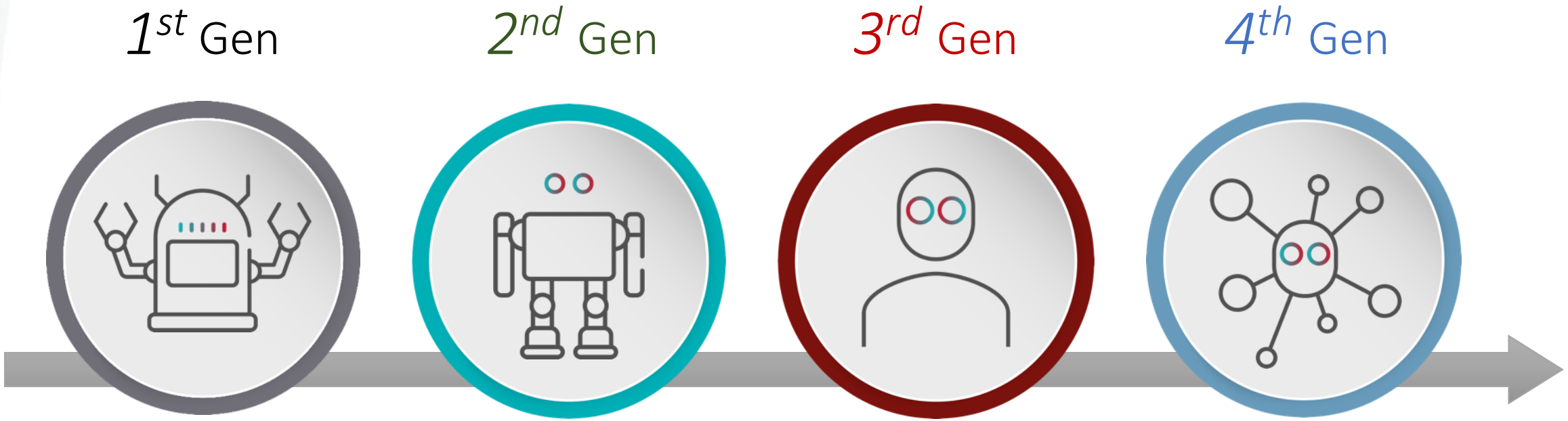
Radware Bot Manager



Radware Solution Map (abstraction)



Bot Generations



1st Gen

SCRIPT BOT

単純なスクリプト

固定された
IPアドレスを使用

2nd Gen

HEADLESS BROWSER BOT

ブラウザを模擬して活動

JavaScript実行

Cookie維持

3rd Gen

HUMAN-LIKE BOT

ブラウザを利用
「人っぽく」振る舞う

マウス動作＋クリック

CAPTHA等に対応できない

4th Gen

DISTRIBUTED BOT

より「人に近い」動作
（直線ではなくランダム）

大量のIP/UAを使い回す

モバイルアプリ複製

Radware Bot Manager

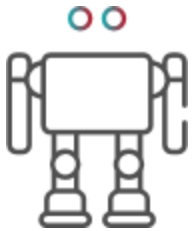
Radware Bot Manger

他社

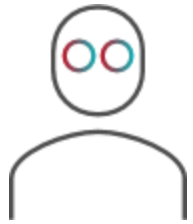
Bot



Script Bots



Headless Browser Bots



Human-like Bots



Distributed Bots

Technology



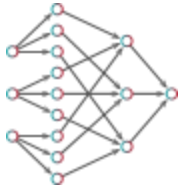
IP, User Agent



デバイス＋ブラウザ
フィンガープリント



ふるまい検知



ビッグデータ
相関解析、機械学習

A Bad Bot Attack （ある優れたBotの例）

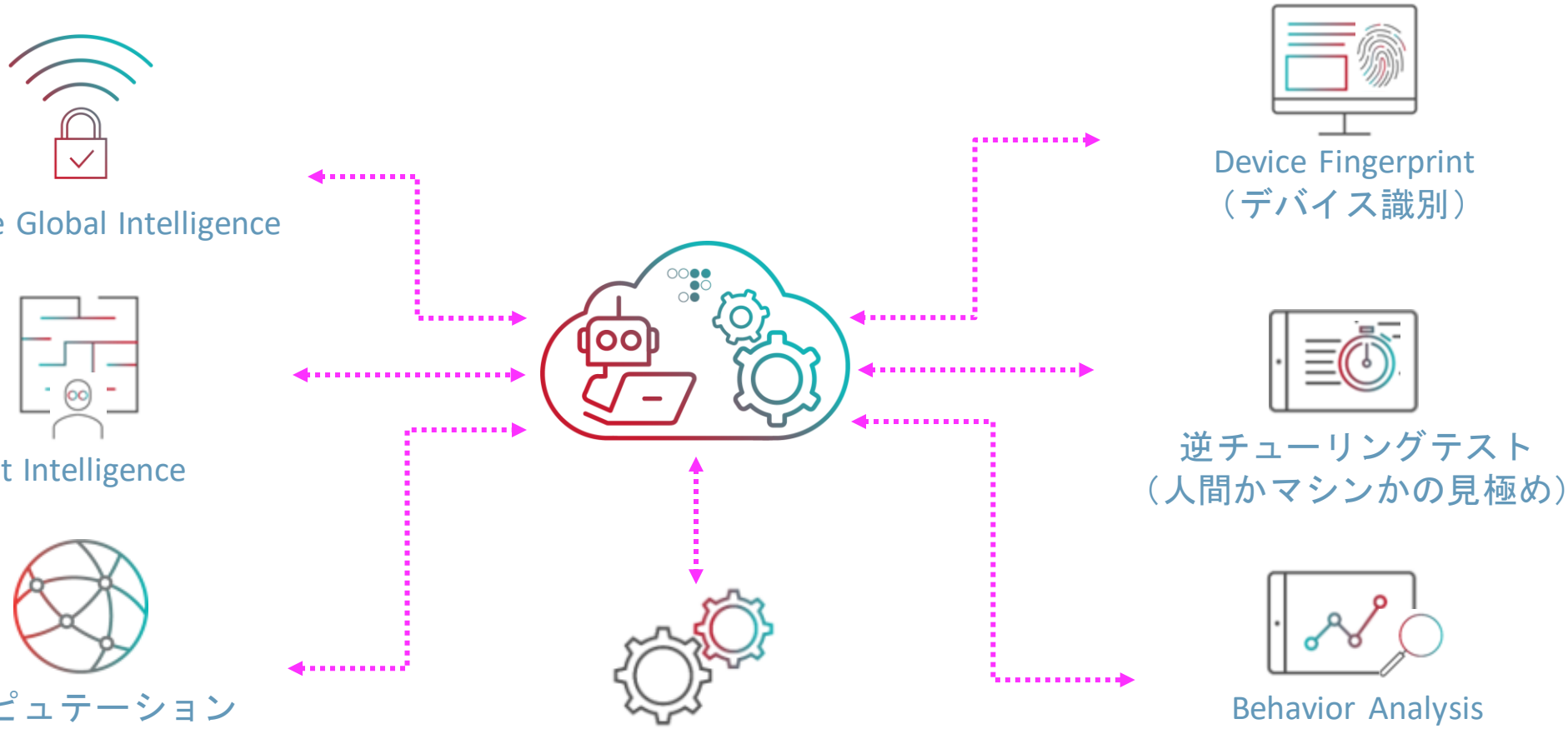
攻撃期間: 1day

IP数	Bot Hit数	同一IPから2回以下のHit数（1時間以内）	ISP数	4時間以上ActiveだったIP数
52,278	210,723	51,658	2,802	2,847

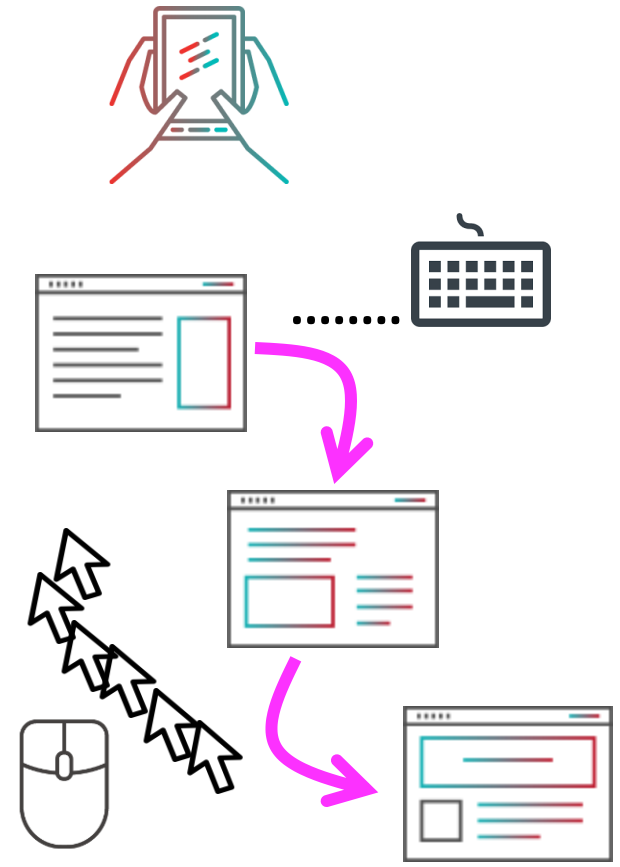
基点となった国数: 48



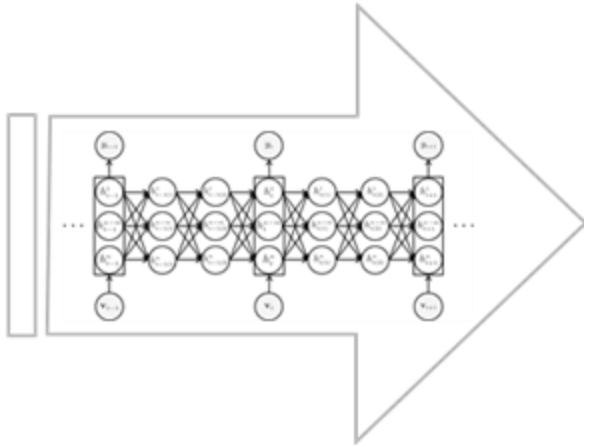
Bot Manager Engine



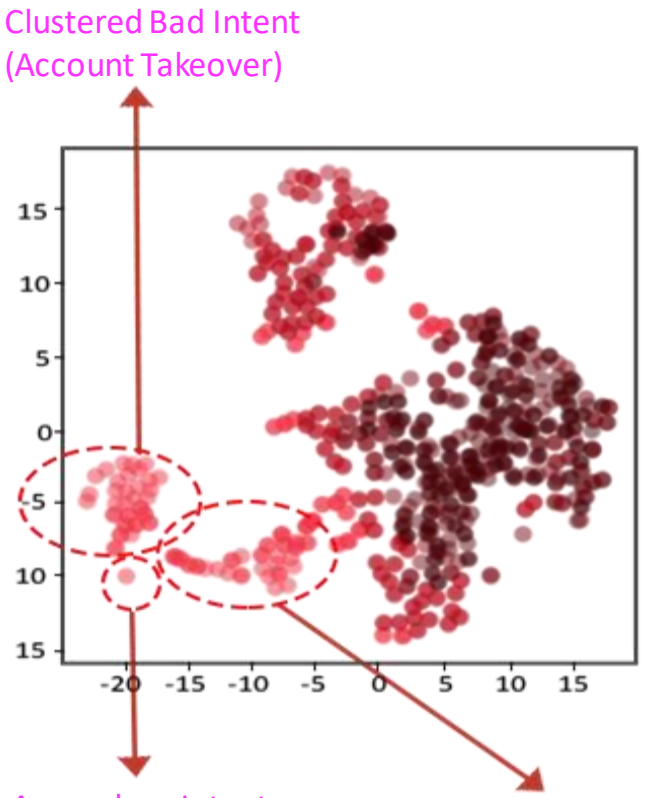
Intent-based Deep Behavior Analysis



End-to-Endインタラクションとサイト遷移



Intent Encoder
(Semi-Supervised Neural Network)



API Flow Control Module

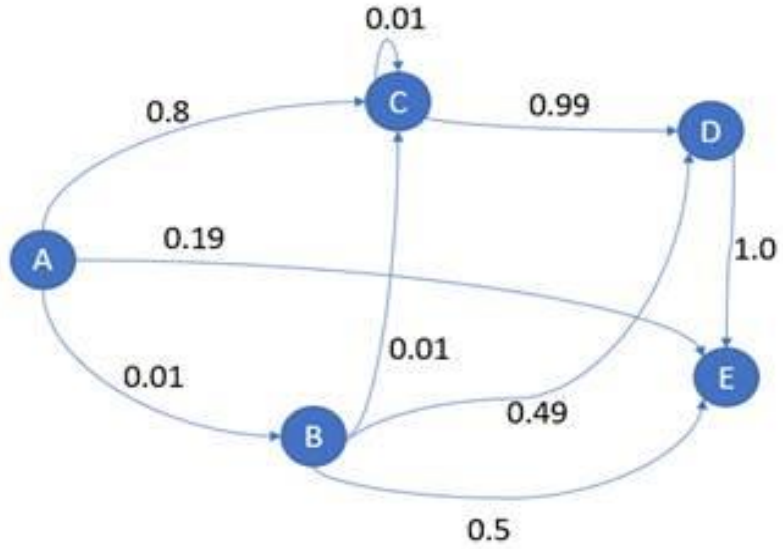
- アクセスパターンを分析し、APIアクセス統計を自動作成
- APIシーケンスが悪性かどうかをチェック
- A → B → C → C → D → E と遷移する確率＝0.00000099
- ログインや通常のページ遷移が無いDirect APIアクセスを検知



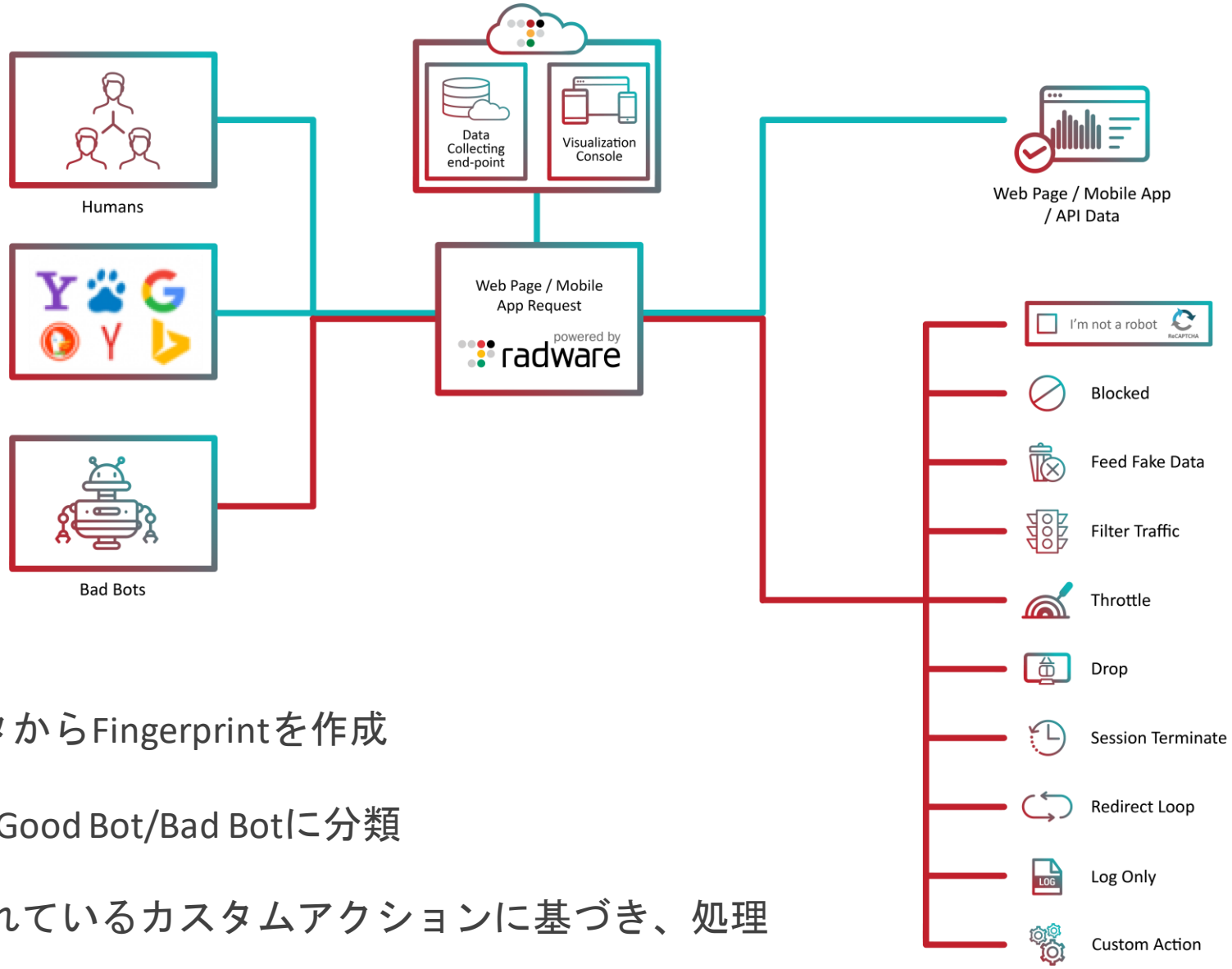
Monitoring Flow



Blocking Bad Flow

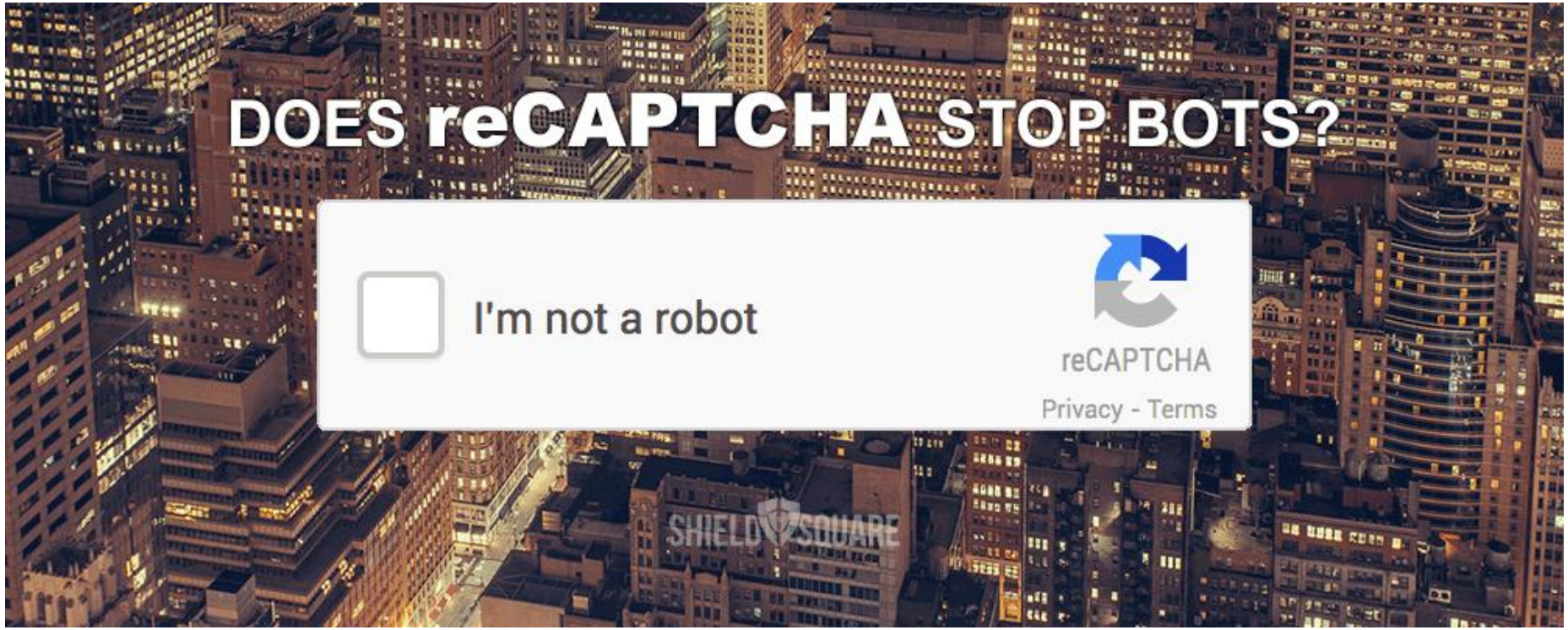


How to Defending



1. トラフィックパラメータからFingerprintを作成
2. CloudのEngineでHuman/Good Bot/Bad Botに分類
3. Bad Botに対して設定されているカスタムアクションに基づき、処理

How to Defending - reCAPTCHA



Global of PoPs



Oregon, USA
Los Angeles, USA
S Carolina, USA
IOWA, USA
N Virginia, USA

Montreal, CN
London, UK
Netherlands, GR
Belgium, GR
Frankfurt, GR

Finland, GR
Zurich, SWISS
Sydney, AUS
São Paulo, BR
Mumbai, IN

Taiwan, CHN
Hong Kong, CHN
Tokyo, JP
Singapore

Bad Bot Analyzer(BBA)

ボットトラフィックやボット攻撃検査用の無料評価ツール

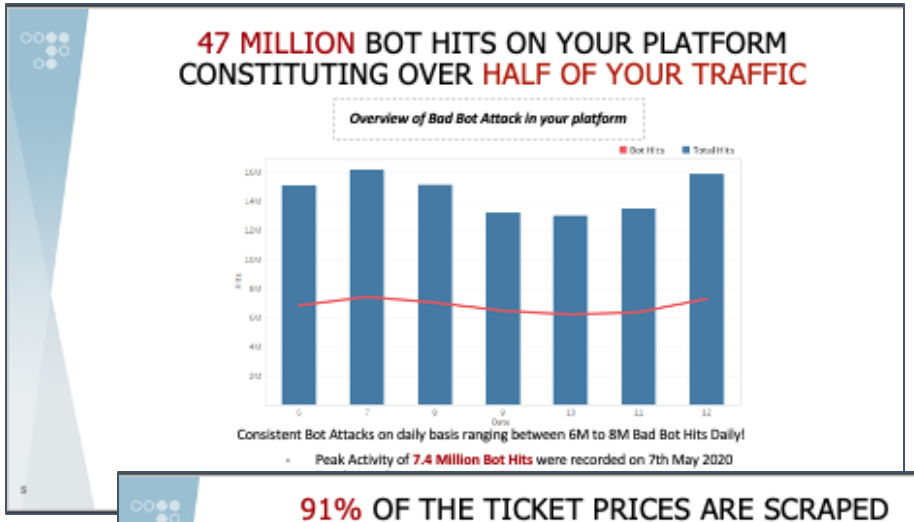
- 有害なボットトラフィックのボリュームを評価します。
- アカウントの乗っ取り試行、インベントリの偽装確保、架空請求、Webスクレイピングに対する可視性が得られます。
- あらゆるチャネルのテスト：Webサイト、モバイルアプリ、API
- 有害なボットのトラフィックを分析して巧妙度をレベル分けし、人に似た振る舞いを追跡します。
- ヒントとアドバイスが得られます。

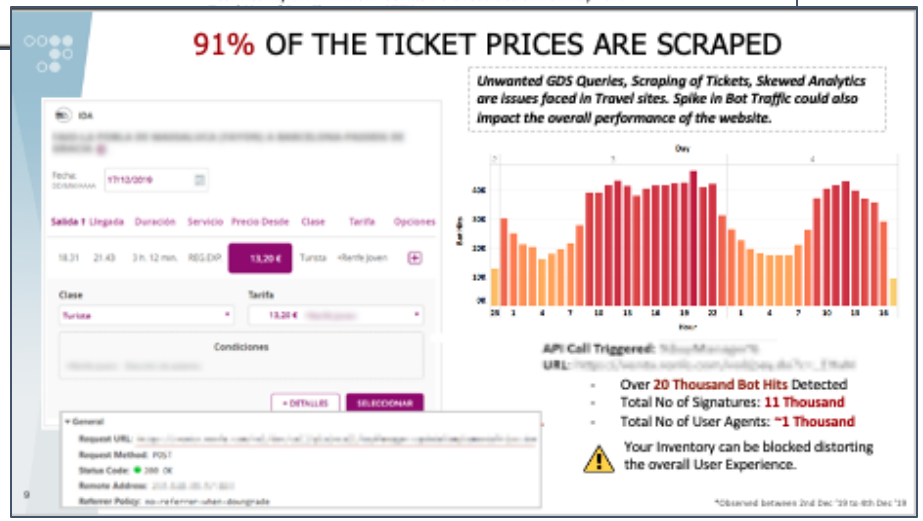
*顧客は、サーバー、CDN、またはWAFのアクセスログを共有する必要があります。



Bad Bot Analyzer report example

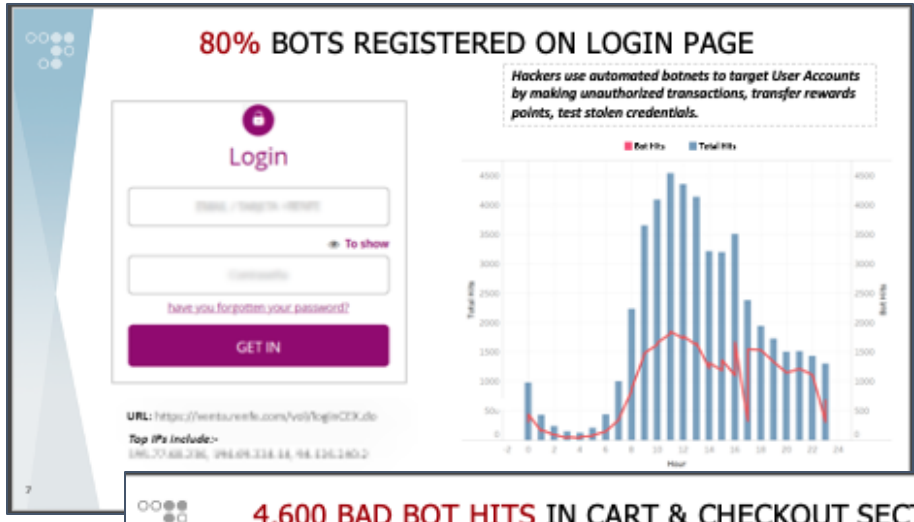
Botがどれくらい来ているか（Good/Bad内訳）

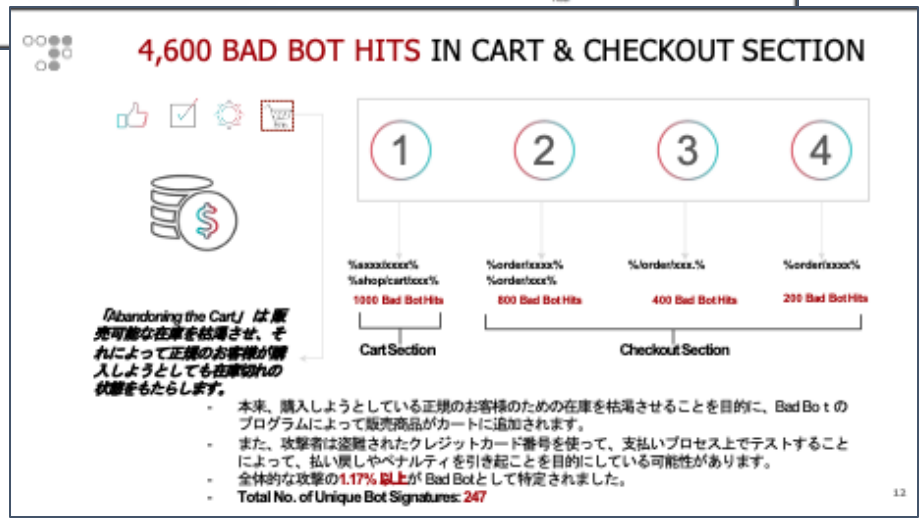




商品ページにおけるScrapingの可能性

ログインページにおけるアカウント乗っ取りの可能性





決済ページにおける不正決済の可能性

Summary

- About Radware
- Bot Threat Trend
- Radware BotManager
  - Bot Generations
  - API Flow Control Module
  - Semi-Supervised Machine Learning
- Bad Bot Analyzer(BBA)



Ransome DDoS（サイバー攻撃と脅迫行為）

- DDoS（サービス妨害、停止攻撃）を利用した犯罪グループによる脅迫活動
- 金銭（仮想通貨）を要求する
- 毎年のように実施され、今年は日本もターゲットエリアに指定されている

DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について

最終更新: 2020-09-07

ツイート　メール

CyberNewsFlash一覧

I. 概要

JPCERT/CC は、2020年8月以降、DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為に関する情報を複数確認しています。こうした脅迫行為は「DDoS 脅迫」「ransom DDoS」などとも呼ばれ、攻撃者が標的の組織宛にメールを送り、指定する期間内に仮想通貨を支払わなければ、DDoS 攻撃を実行すると脅迫します。過去には類似する攻撃として、2015年に DD4BC グループによる攻撃、2017年には Armada Collective や Phantom Squad を名乗る攻撃者からの攻撃、2019年には Fancy Bear Group を名乗る攻撃者からの攻撃等が確認されています。

JPCERT/CC は、国内の組織を標的とした攻撃に関する情報も確認しており、国内の組織においても引き続き警戒が必要な状況です。2020年8月以降に確認されている攻撃について、公開情報等から攻撃の流れ、手法や特徴を以下に整理いたしました。攻撃を検知および防御するための対策の検討や、攻撃を検知あるいは認知した場合の対応手順や体制を確認する場合の参考情報としてご活用ください。

Source:JPCERT https://www.jpcert.or.jp/newsflash/2020090701.html

「ランサムDDoS」を国内で観測 - 支払有無で結果変わらず

JPCERTコーディネーションセンターは、8月以降にDDoS攻撃を行うと脅し、金銭を要求する攻撃が発生しているとして注意喚起を行った。攻撃と見られるパケットについても観測しているという。

攻撃対象の組織に対し、指定期間以内に仮想通貨を支払うようメールを送り付け、応じない場合は「DDoS攻撃を行う」として金銭を支払うよう脅迫する「ランサムDDoS（DDoS脅迫）」攻撃が確認されているもの。

過去にも同様の攻撃が発生しており、目新しい攻撃ではないが、ふたたび8月中旬ごろよりグローバルに攻撃が展開されている。

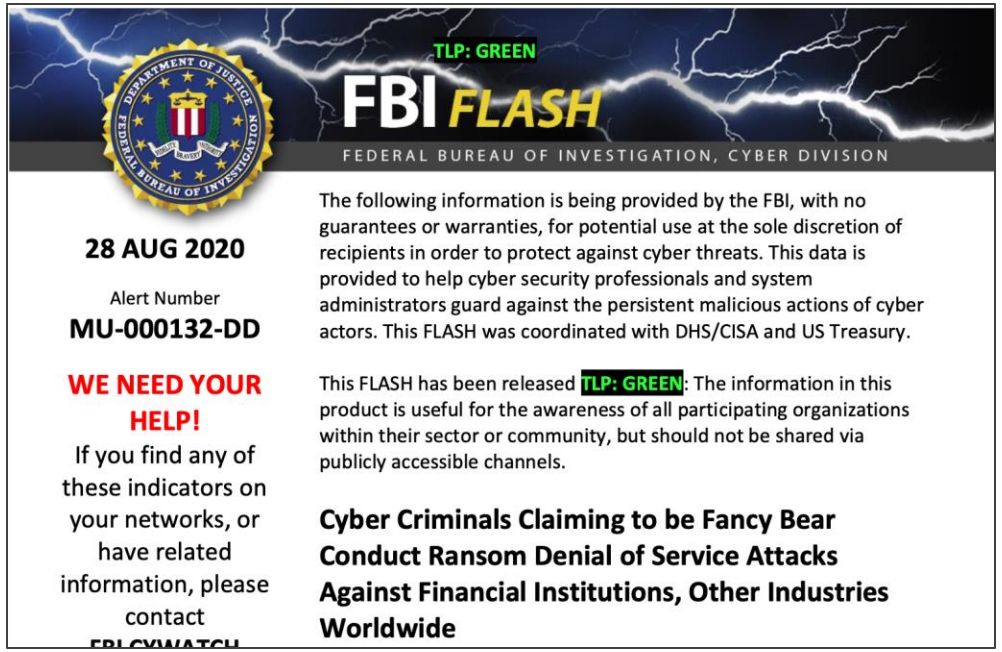
DDoS攻撃対策を提供する複数のベンダーが観測しているほか、標的型のDDoS攻撃が展開されているとして、米国やニュージーランドなど、各国のセキュリティ機関が注意喚起を行った。

地方銀行、証券取引所、オンライン決済サービス事業者など金融関連サービスをはじめ、旅行代理店、eコマースなどが標的となっており、サービスが停止することでビジネスに大きな影響が及ぶ事業者を狙っている。

Source: Security Next https://www.security-next.com/118189

2020進行中のRansome DDoS

- ‘Fancy Bear’, ‘Armada Collective’, ‘Lazarus Group’　といったサイバー犯罪グループが主導
- Interpol, FBI等からAlertが上がっている
- 金融、トラベル、Eコマースが主なターゲット
- 200–300Gに及ぶ大規模攻撃（デモも実施する）
- およそ2,000万相当の仮想通貨を要求



TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

28 AUG 2020

Alert Number
MU-000132-DD

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA and US Treasury.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Criminals Claiming to be Fancy Bear Conduct Ransom Denial of Service Attacks Against Financial Institutions, Other Industries Worldwide

Subject: DDoS Attack

We are the Lazarus Group and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search for " Lazarus Group" to have a look at some of our previous work. Also, perform a search for "[redacted]" or "[redacted]" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting [redacted] next week. (This is not a hoax, and to prove it right now we will start a small attack on a few of your IPs from AS[redacted] block that will last for about 60 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.

Worst of all for you, you will lose Internet access in your offices too!

We will refrain from attacking your network for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already. And hopefully for this message to reach somebody who can handle it properly.

If you don't pay the attack will start and fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

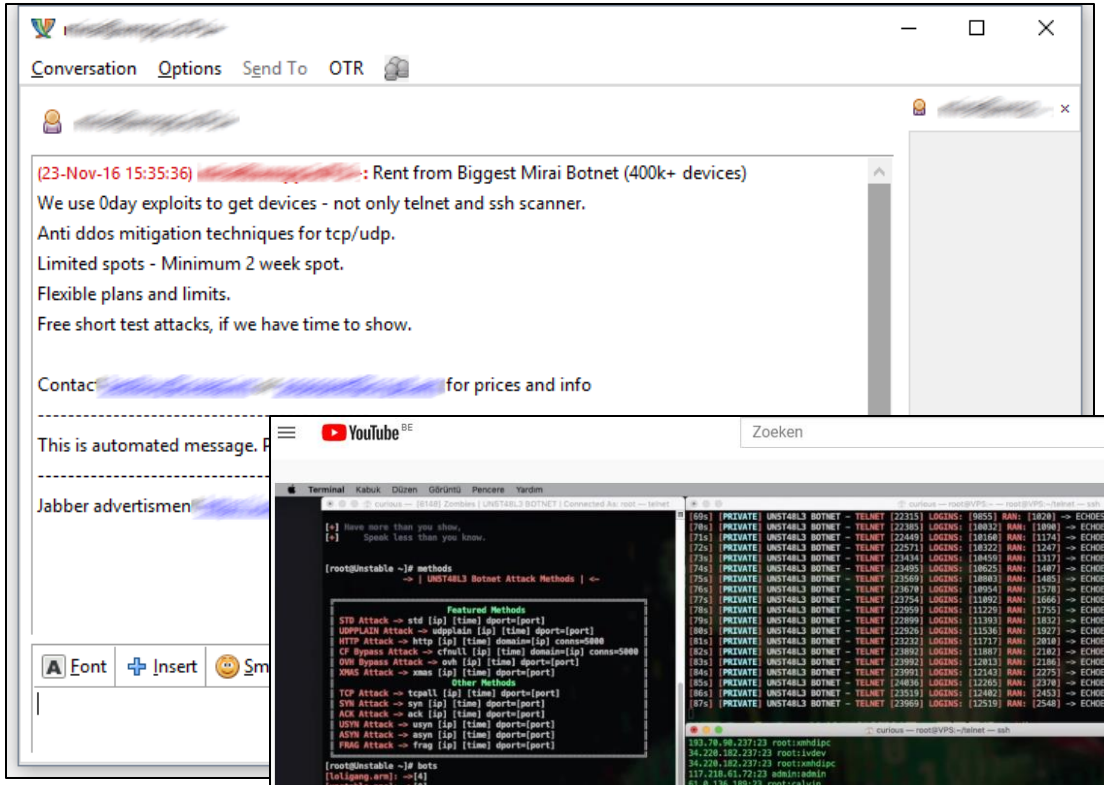
Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

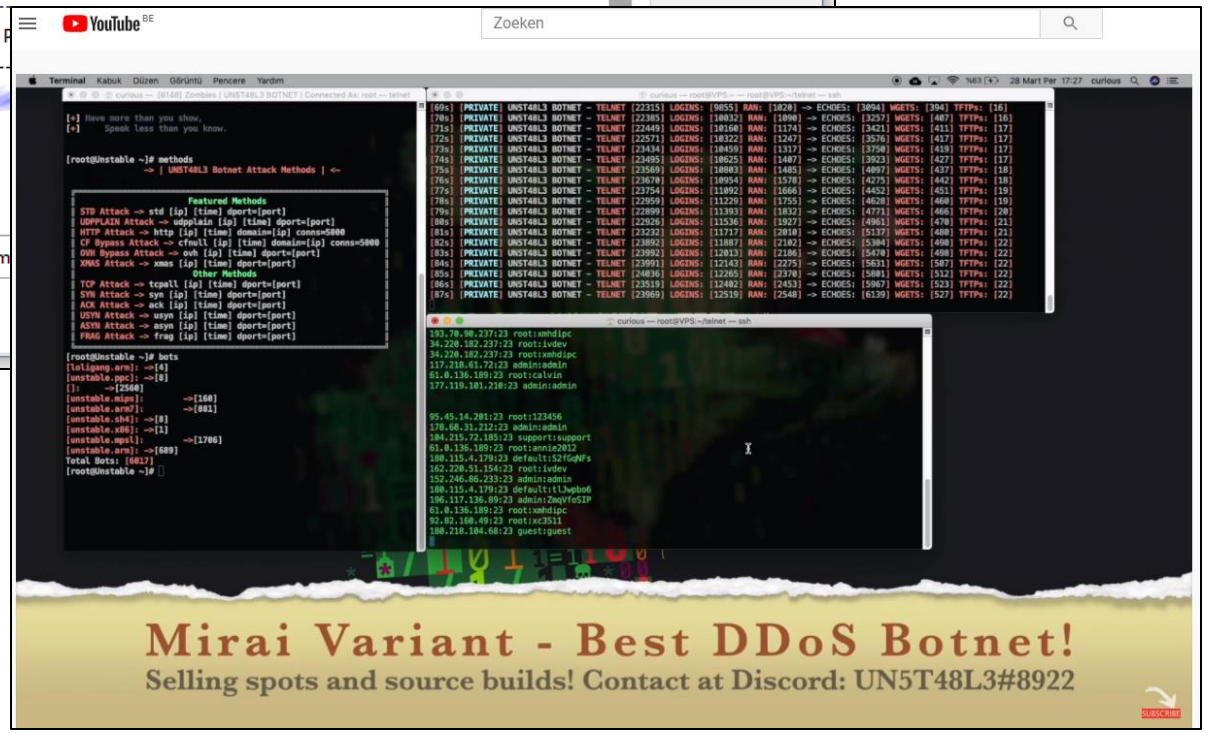
Please note we will respect your privacy and reputation, so no one will find out that you have complied.

DDoS Market Place

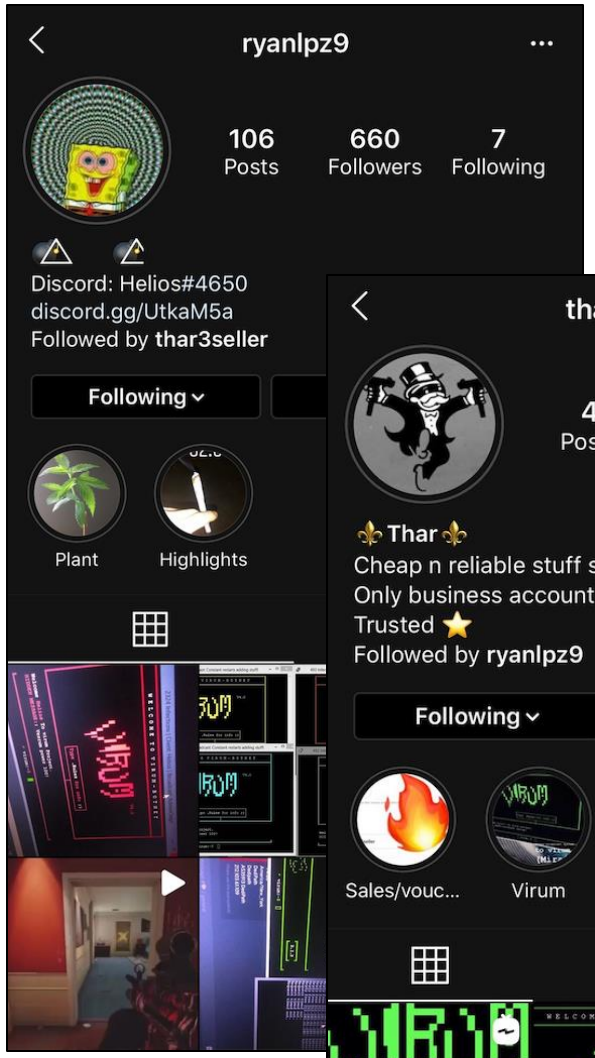
Jabber

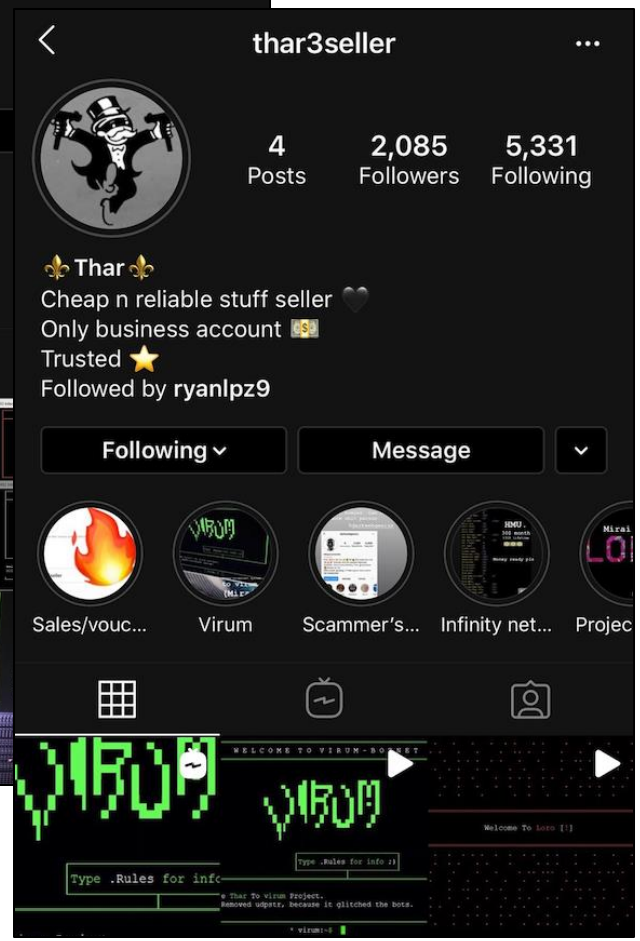


Youtube

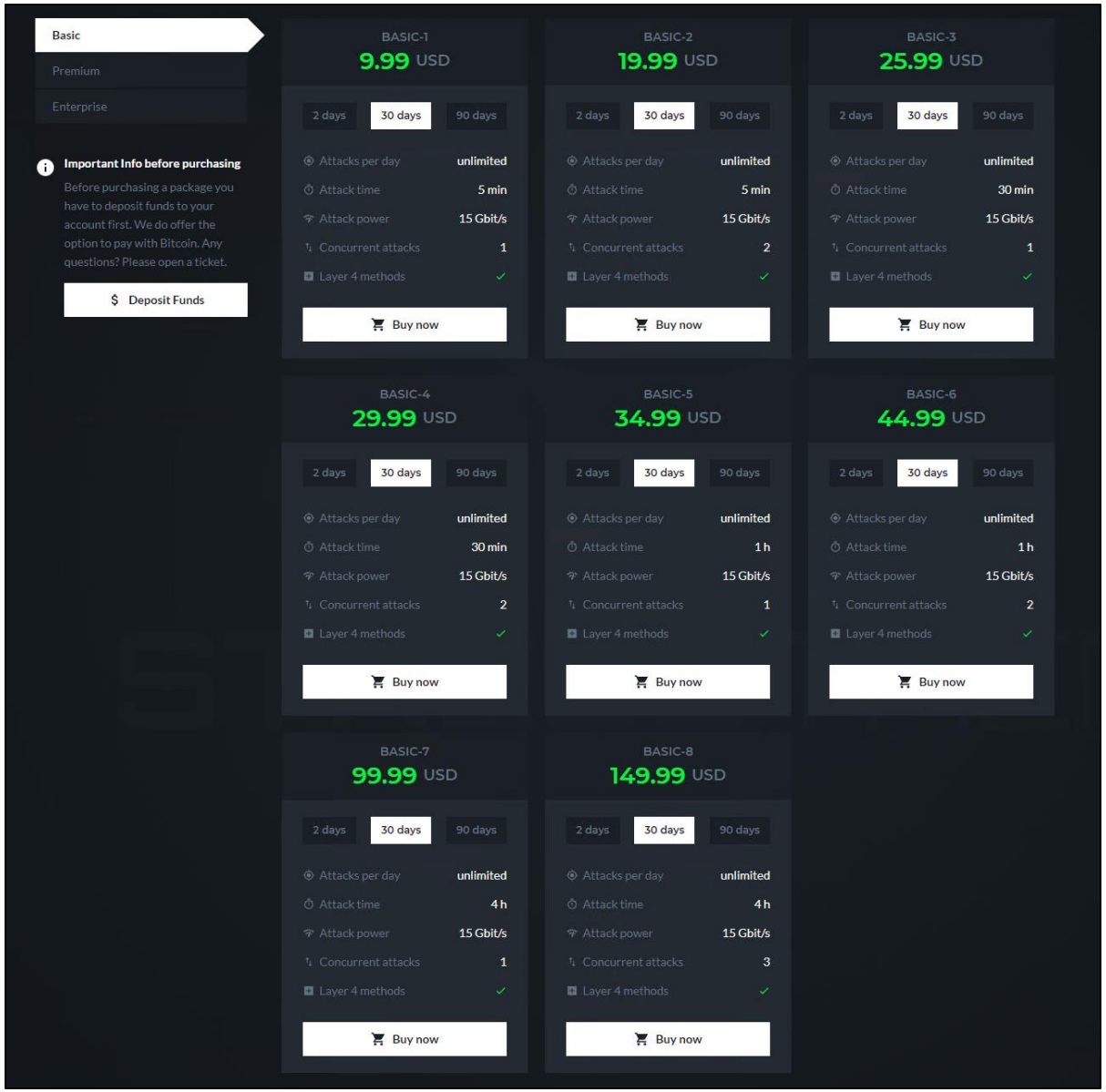


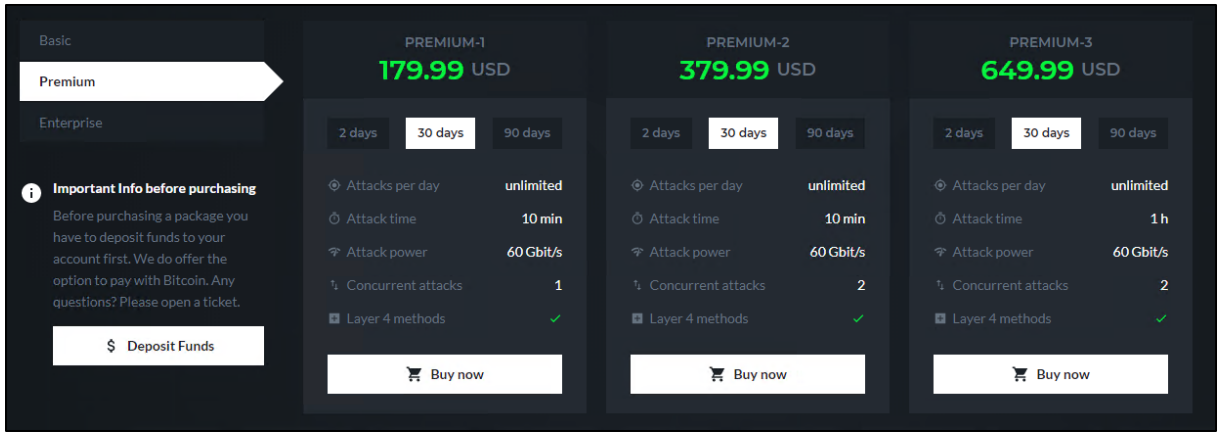
Twitter
&
Instagram

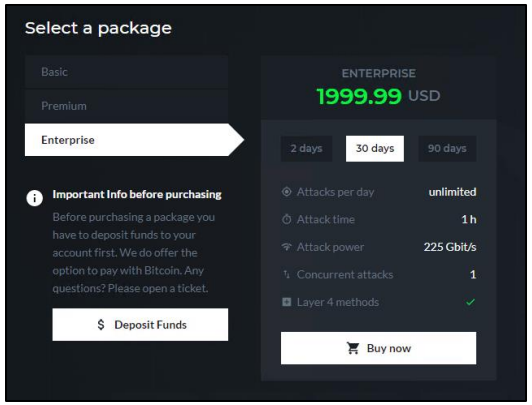


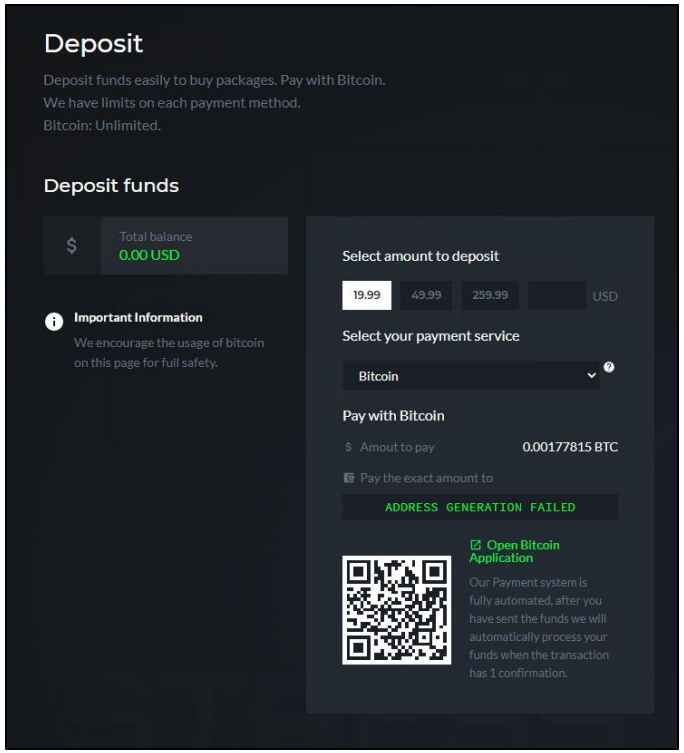


DDoS as a Service









Summary

- About Radware
- Bot Threat Trend
- Radware BotManager
  - Bot Generations
  - API Flow Control Module
  - Semi-Supervised Machine Learning
- Bad Bot Analyzer(BBA)
- Ransome DDoS



radware

THANK YOU!

