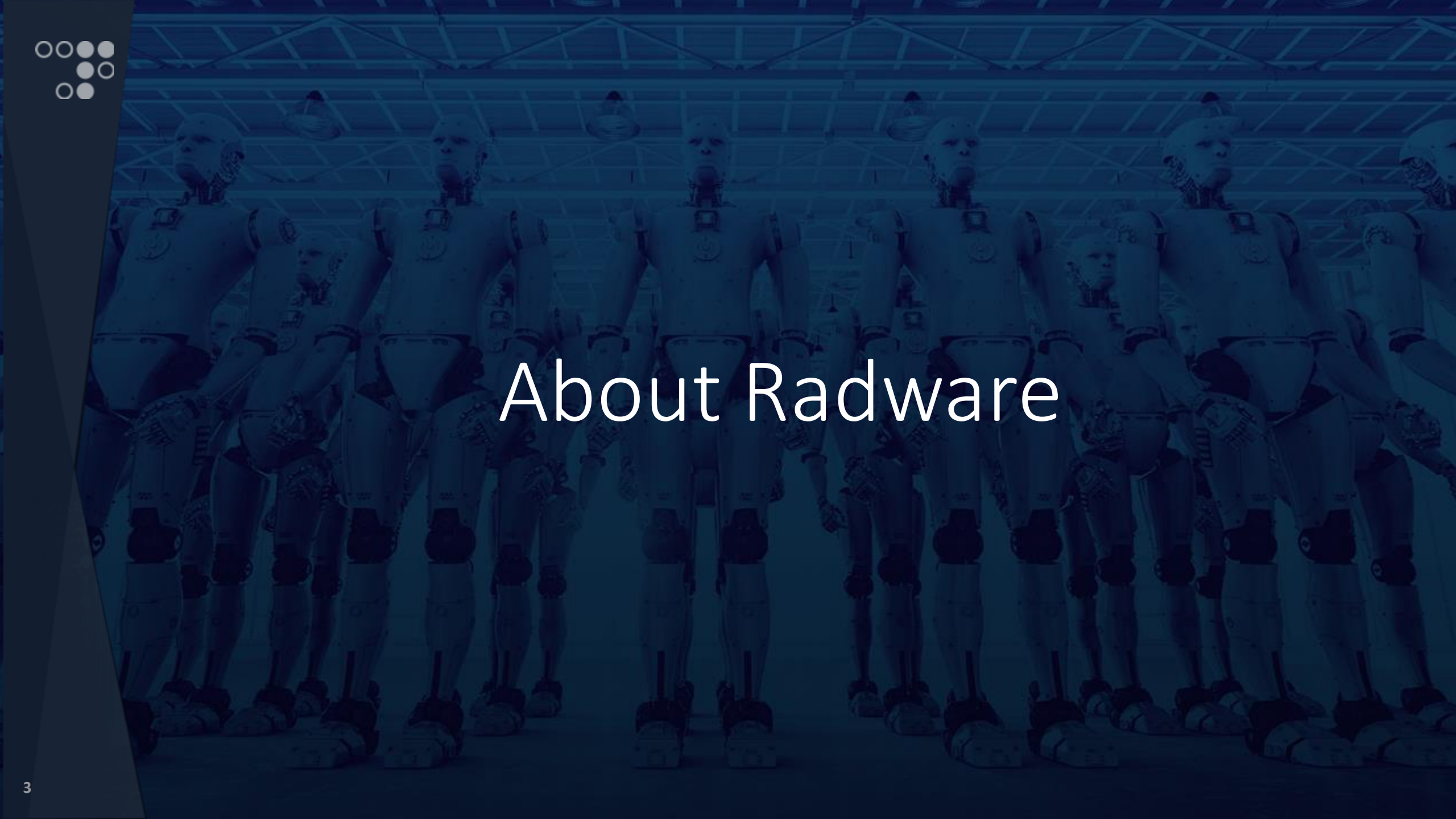
Radware Introduction

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

Sep.2020

Topics

- About Radware
- Trend - Cyber Attacks
- Radware Solutions
- 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

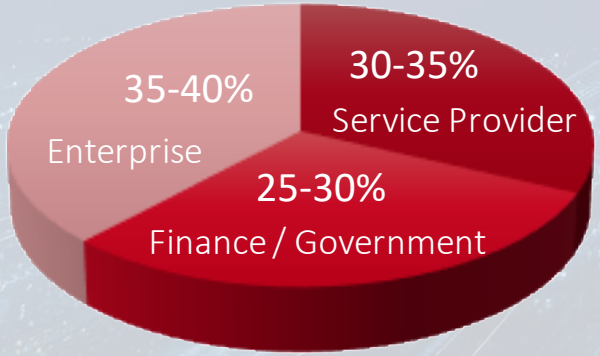
CISCO　Microsoft Azure　NOKIA

- 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

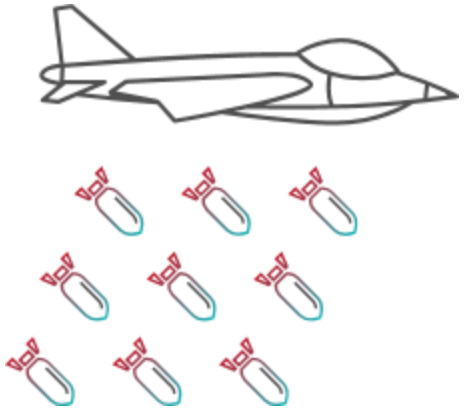
DELTA　ebay　GAP
Marriott Vacation Club　PayPal
SAMSUNG SDS　twitter　ups

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

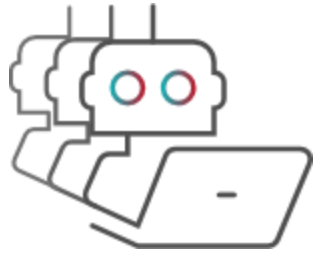
salesforce　AT&T　Cisco webex
workday　SAP
Tech Mahindra　verizon　Akamai

Radware Solutions against threats



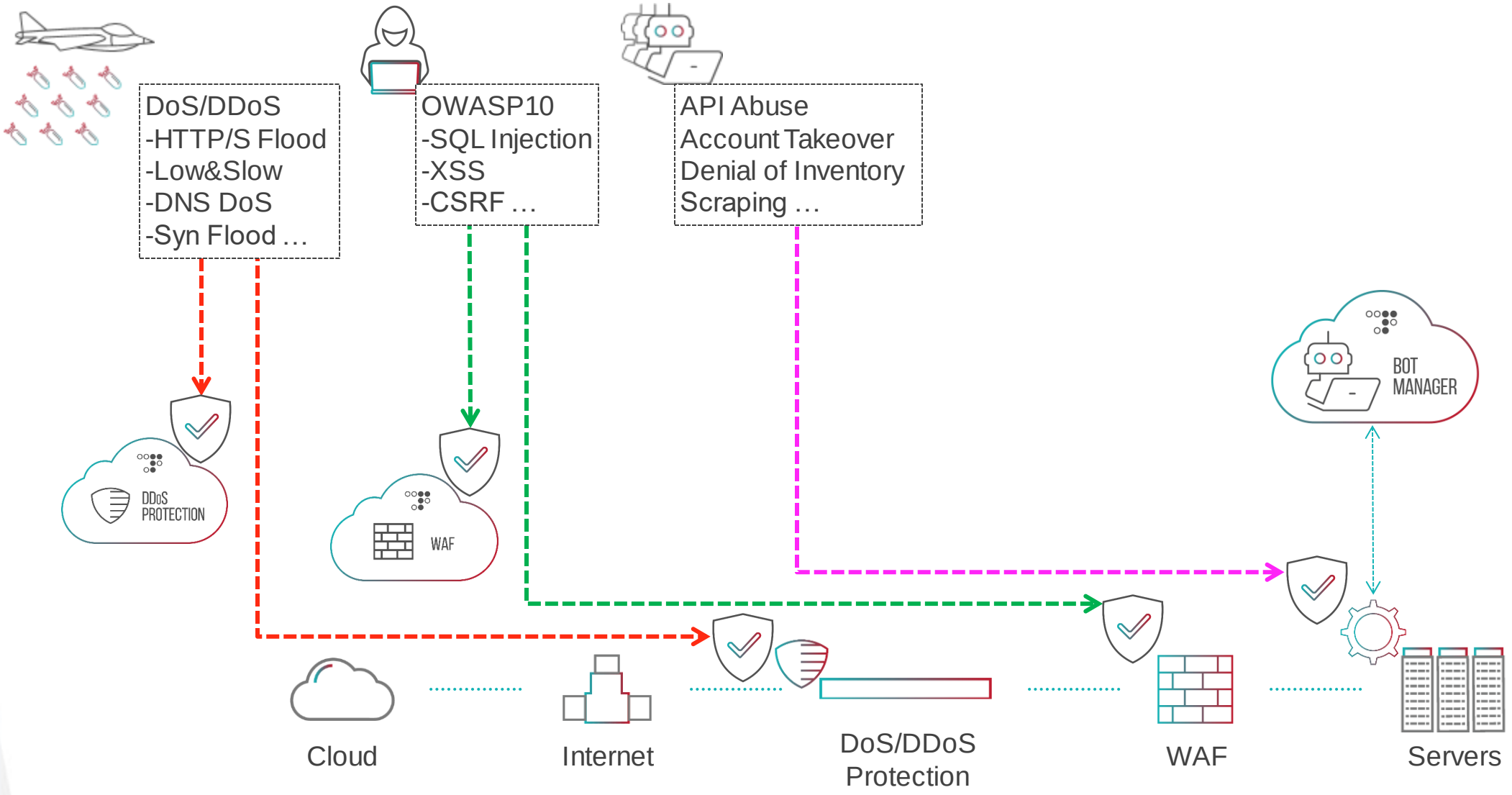
DoS/DDoS

WebApp(OWASP10)



Bot/API

Radware Solution Map (abstraction)



Recently Cyber Attacks

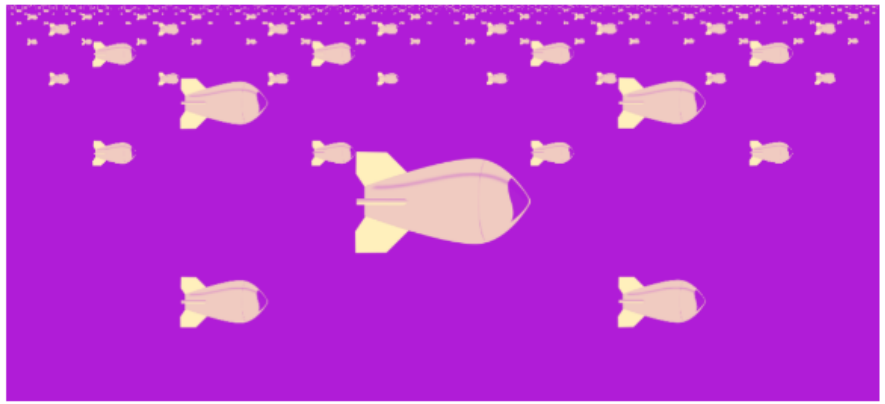
‘Carpet-Bombing’ DDoS Attack Campaign Sep/Oct 2019

'Carpet-bombing' DDoS attack takes down South African ISP for an entire day

Carpet bombing - the DDoS technique that's just perfect for attacking ISPs, cloud services, and data centers.

By Catalin Cimpanu for Zero Day | September 24, 2019 -- 19:30 GMT (20:30 BST) | Topic: Security

南アフリカのISPがDDoSにより丸一日ダウン



Mysterious attackers have taken down a South African internet service provider over the weekend using a DDoS technique called carpet bombing. *ZDNet* has learned.

The DDoS attacks took place on Saturday and Sunday, September 21 and 22, and have targeted Cool Ideas, one of South Africa's largest ISPs.

During the DDoS, attackers successfully managed to bring down Cool Ideas' external connections to other ISPs, as can be seen from open-source reporting tools.

SEE ALSO

10 dangerous app vulnerabilities to watch out for (free PDF)

Security
Chinese police arrest operators of 200,000-strong DDoS botnet

Security
Libarchive vulnerability can lead to code execution on Linux, FreeBSD, NetBSD

Security
Kamerka OSINT tool shows your country's internet-connected critical infrastructure

Security
Experts: Don't reboot your computer after you've been infected with ransomware

NEWSLETTERS

SEE ALL

RELATED STORIES

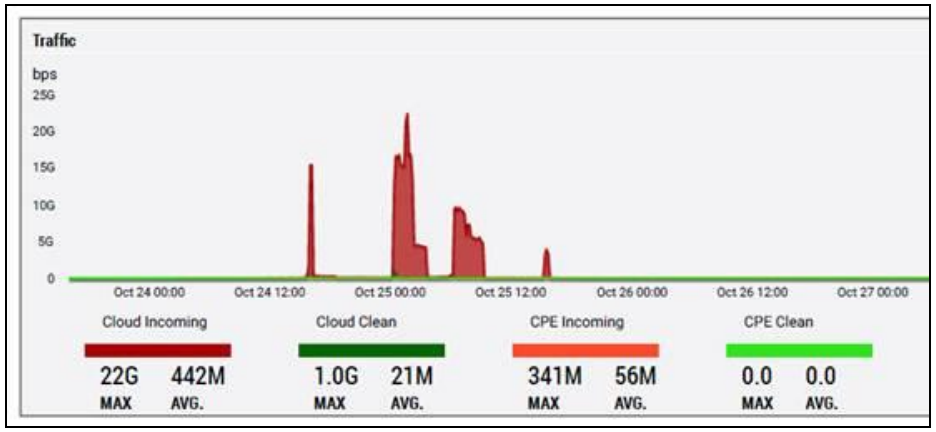
Source: ZDNet https://zd.net/38ATDMy

Fancy Bear: Ransom DDoS Attacks

金融機関を狙った世界規模のランサムキャンペーン

“Fancy Bear” というサイバー犯罪グループが実施
1ビットコイン（当時 $8k）を要求
支払わなければ毎日1ビットコインずつ増える

Radwareは南アフリカ大手銀行 3行を保護し、
アラートとブログを公開



ある攻撃は22Gbpsを記録

“Fancy Bear”からの脅迫メール

We are the Fancy Bear and we have chosen your company as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" and "Mirai Botnet" to have a look at some of our previous "work".

Your network will be subject to a DDoS attack starting at [Ransom Deadline]

x.xxx and
t.)

SA banks hit by ransom attacks

Oct 25 2019 12:57

This means that your website and other connected services will be unavailable for everyone. Please also

Australian banks targeted by DDoS extortionists

Hackers are sending emails to banks asking for large payments in Monero, and threatening DDoS a demands aren't met.

How

We a
The f
paym

Please send the bitcoin to the following Bitcoin address:

[Bitcoin Address]

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!

What if I don't pay?

If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution (Cloudflare, Incapsula and similar services are useless). 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 that Bitcoin is anonymous and no one will find out that you have complied.

Fancy Bear: Ransom DDoS Attacks

現在進行系のランサムキャンペーン

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

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
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
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、2
Armada Collective や Phantom Squad を名乗る攻撃者からの攻撃、2019年には F
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
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
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

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

Global Ransom DDoS Campaign Targeting Finance, Travel and E-Commerce

Radware is following a global ransom DDoS campaign targeting organizations in the finance, travel, and e-commerce verticals. Additionally, multiple internet service providers have been reporting DDoS attacks targetting their dns infrastructure.

Global Ransom DDoS Campaigns

Since the middle of August, Radware has been tracking several extortion requests from threat actors posing as "Fancy Bear," "Armada Collective," and "Lazarus Group." Letters are being delivered via email and typically contain victim-specific data such as Autonomous System Numbers (ASN) or IP addresses of servers or services they will target if their demands are not fulfilled. It is a global campaign with threats reported from organizations in finance, travel and e-commerce in APAC, EMEA and North America.

The ransom fee is initially set at 10 BTC, which is equivalent to $113,000 at the time of the extortion. Some fees are set as high as 20 BTC (approximately $226,000). These demands are larger versus 2019 campaigns that typically requested between 1 BTC or 2 BTC.

Ransom letters threaten cyberattacks of over 2Tbps if payment is not made. To prove the letter is not a hoax, authors indicate when they will launch a demonstration attack.

The letter indicates that if payment is not made prior to the deadline, the attack will continue and the fee will increase by 10 BTC (approximately $113,000) for each missed deadline. Each letter contains a Bitcoin wallet address for payment. The wallet address is unique for each target and allows the actor to track payments.

The ransom letters are very similar in their terms and demands. Threats and advertised capabilities follow the same indicators from earlier **reports**.

Radware is following a global ransom DDoS campaign targeting organizations in the finance, travel, and e-commerce verticals.

READ THE COMPLETE ALERT

Source:Radware Blog https://bit.ly/2R7yEJo

Attacks on DNS Infrastructure – No One Is Safe

! DNSはWebの大規模なサービスダウンを招く可能性のある、1つの重要な要素

October 2016: Dyn DNS US東部リージョンがMirai botnetにより攻撃を受け、被害がTwitter, Amazon, Tumblr, Reddit, Spotify, Netflix等のサービスを数時間アクセス不可状態に

October 2019: AWS Route 53(DNS Service)にも同様の攻撃がありAWS全体サービスへの影響が数時間あった

DNS Serverへの攻撃はWebサービスにとって非常に効果的な手法

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

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

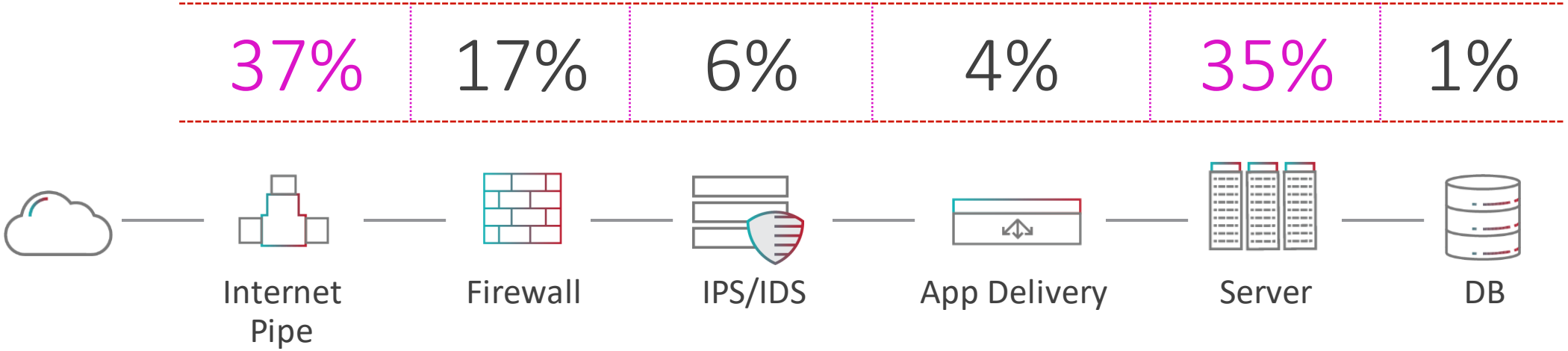
31%

情報漏えいにより
誰かが職を失う確率

Source:Radware

Failure points in the data center

- Internet でのインシデントは2016年から 50% 増
- Server が最も狙われるのは有用なデータを保持しているから
- 部分的な障害を超えた全体サービスダウンが 40% 増



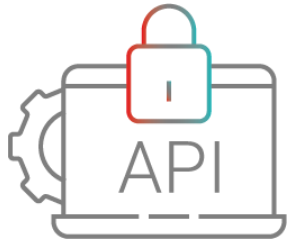
Source:Radware

OWASP* Top 10に基づくアプリケーションの保護対策

- Injections
- Unauthorized access
- Data & credential theft
- Remote scripting
- Web-scraping
- Parameter Manipulation
- Protocol attacks
- Fraud
- Session hijacking
- Cookie poisoning

DEFENSE

アプリケーションレイヤ



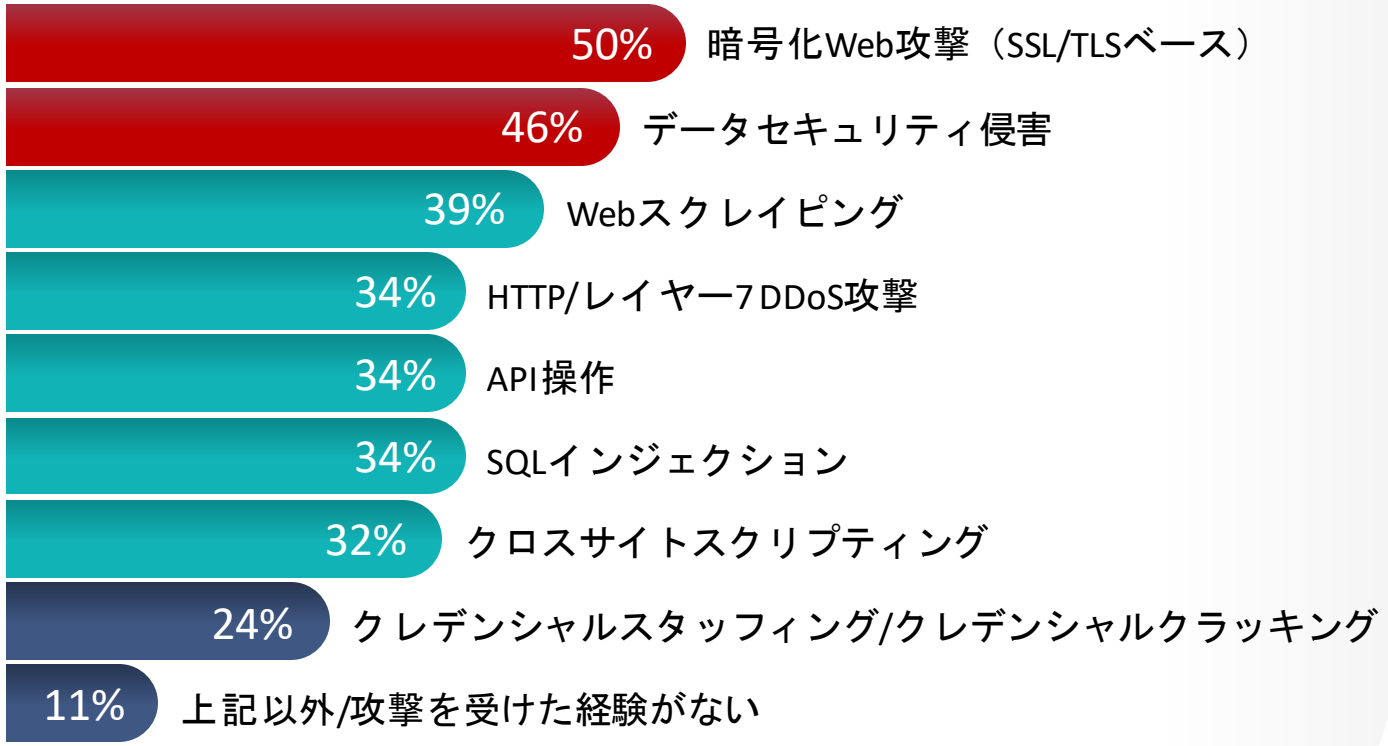
API

BoT

*Open Web Application Security Project

Application Layer Attacks

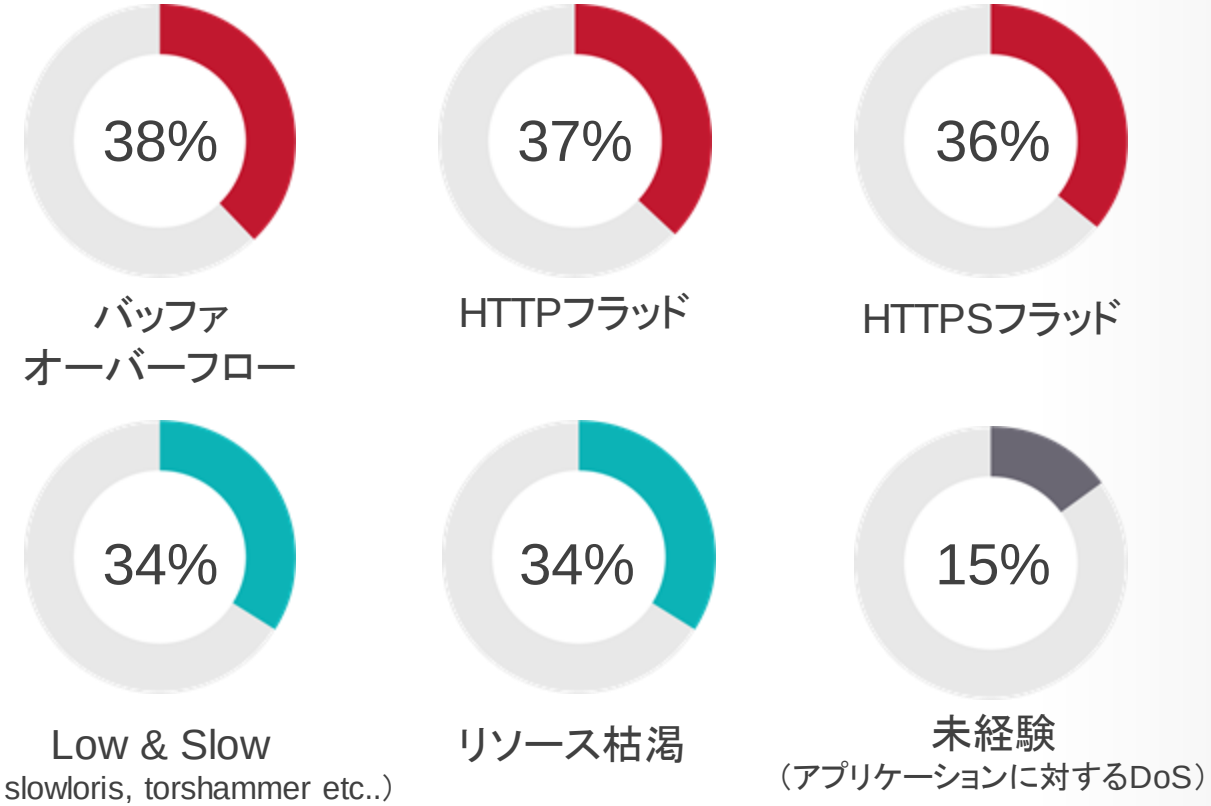
2018年 発生頻度が高かったアプリケーション攻撃



Source:Radware

アプリケーション層でのDoS攻撃

2018年で発生頻度が高かったDoS攻撃

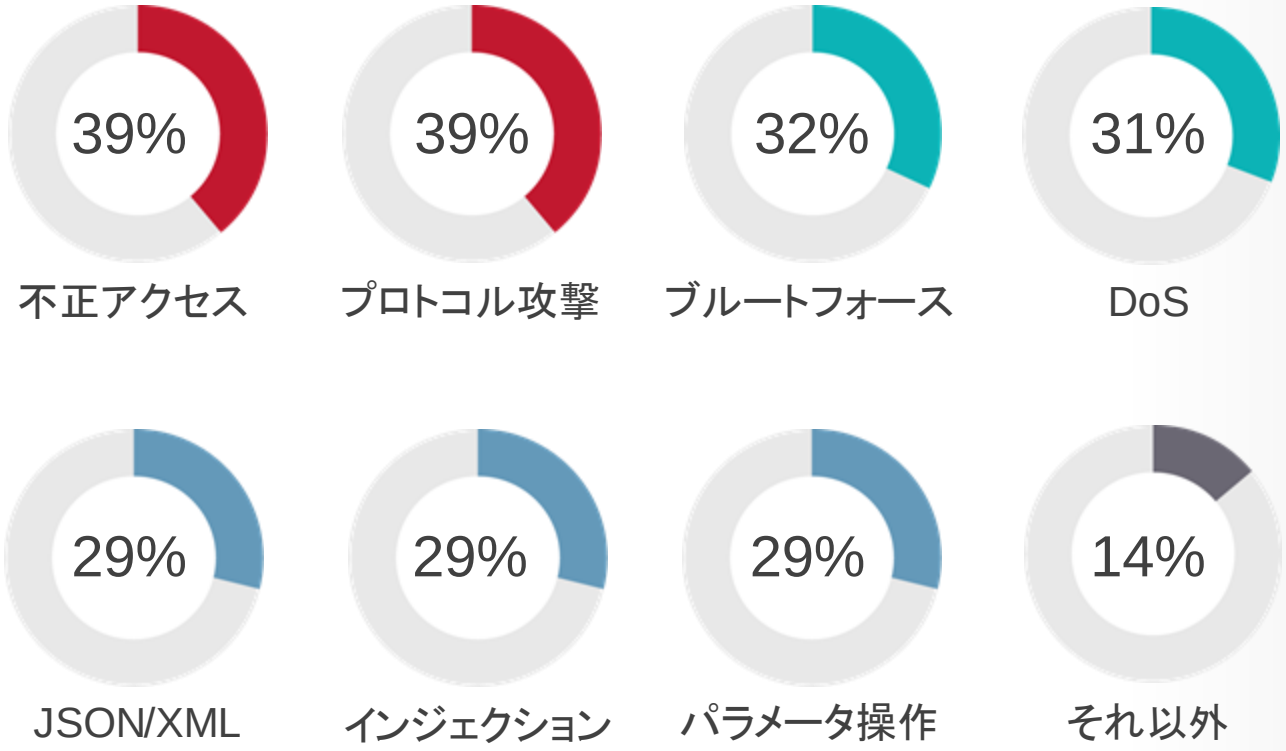


- IoTは大量にHTTP/Sトラフィックを生成
- アプリケーション層DoS攻撃は検知と軽減が困難
- アプリケーションに対する大容量型および非大容量型DoS攻撃の拡大規模は同程度

Source: Radware NETWORK AND APPLICATION SECURITY THREAT LANDSCAPE 2018-9

見落としがちなAPIセキュリティ

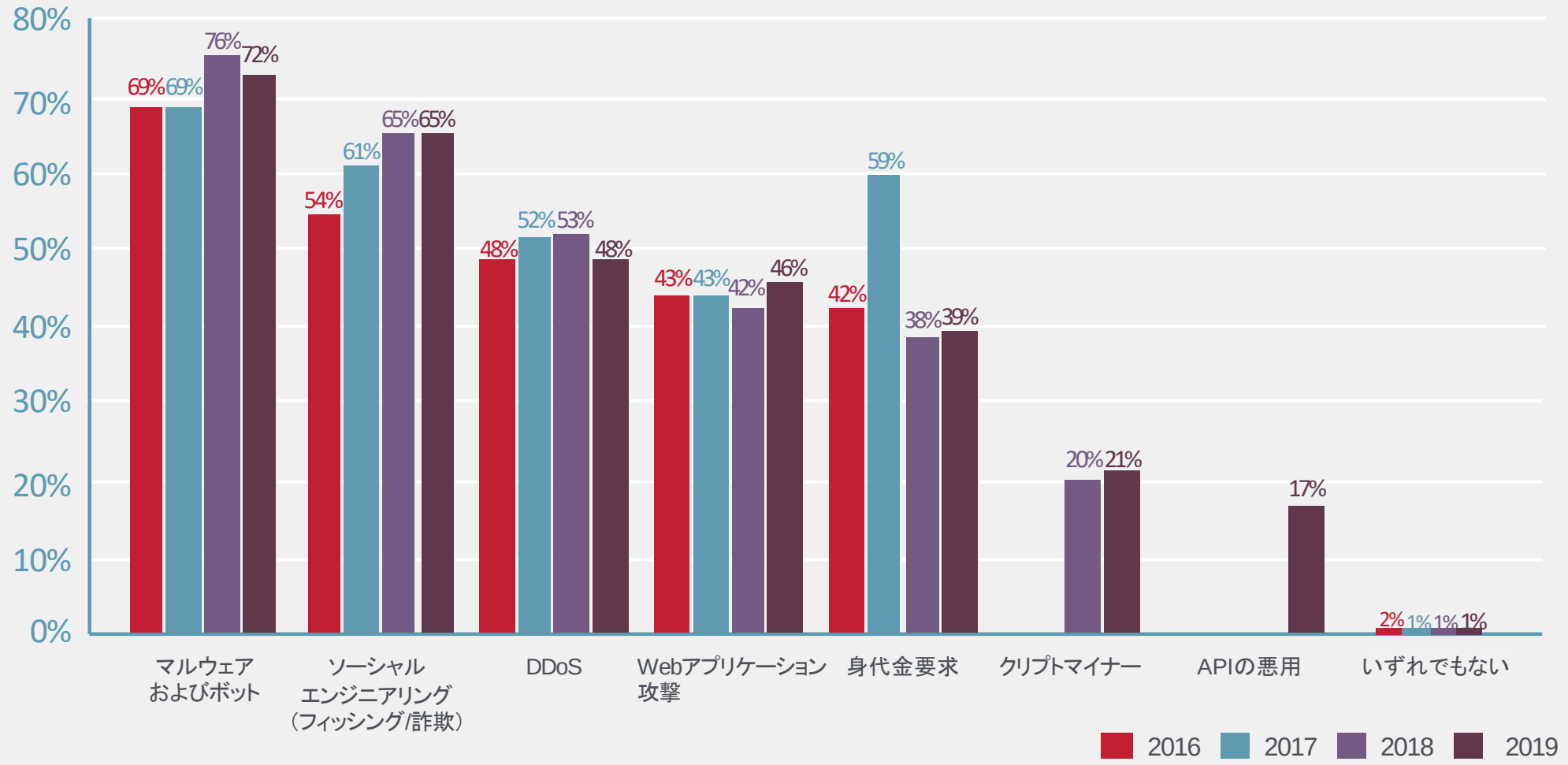
APIに対する7つの一般的な攻撃



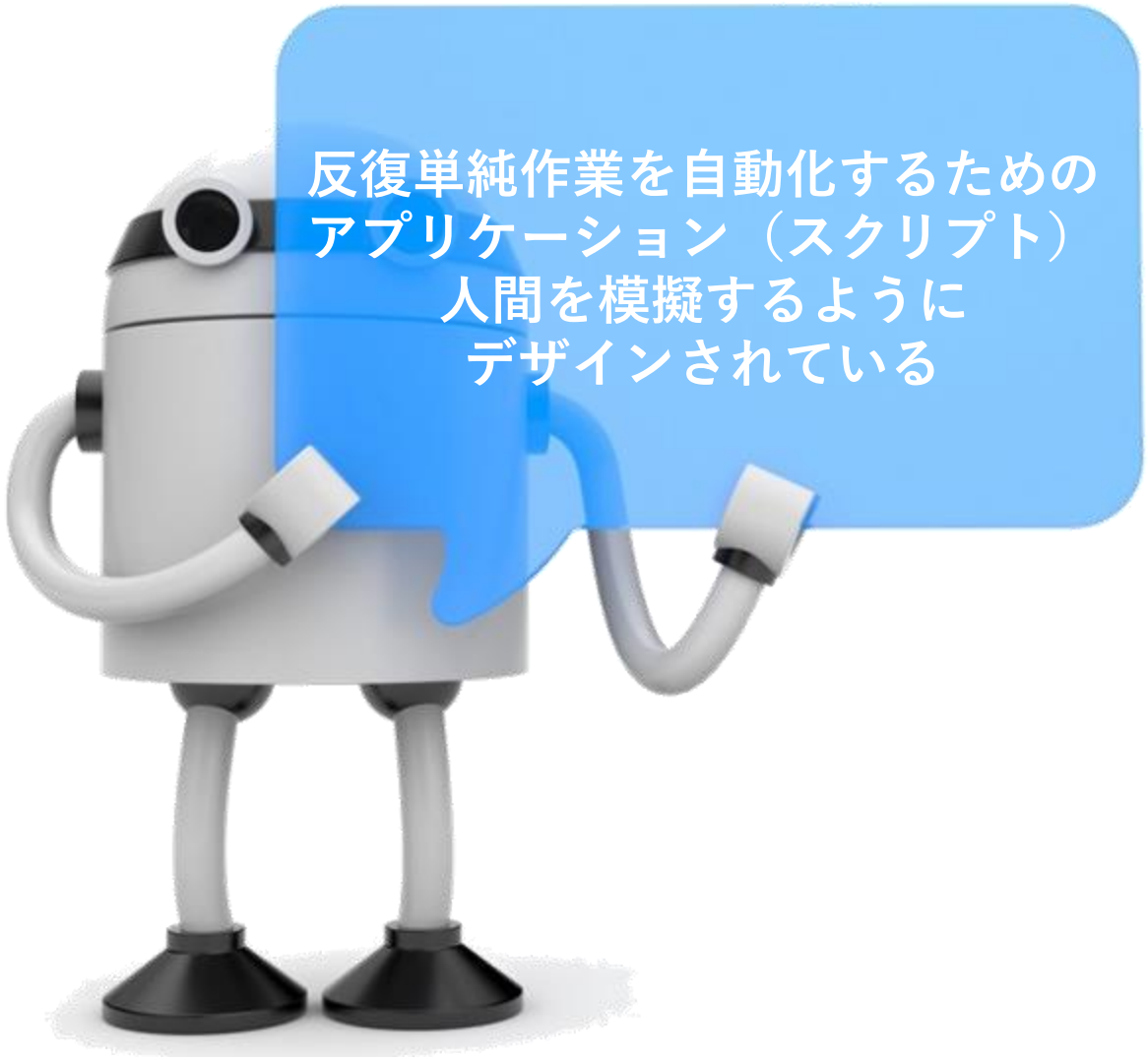
- 転送されたデータは検査や検証の対象ではない
- APIにはアプリケーションと同様の脆弱性がある
- 最も頻発している攻撃はプロトコル攻撃と違反アクセス

Source: Radware NETWORK AND APPLICATION SECURITY THREAT LANDSCAPE 2018-9

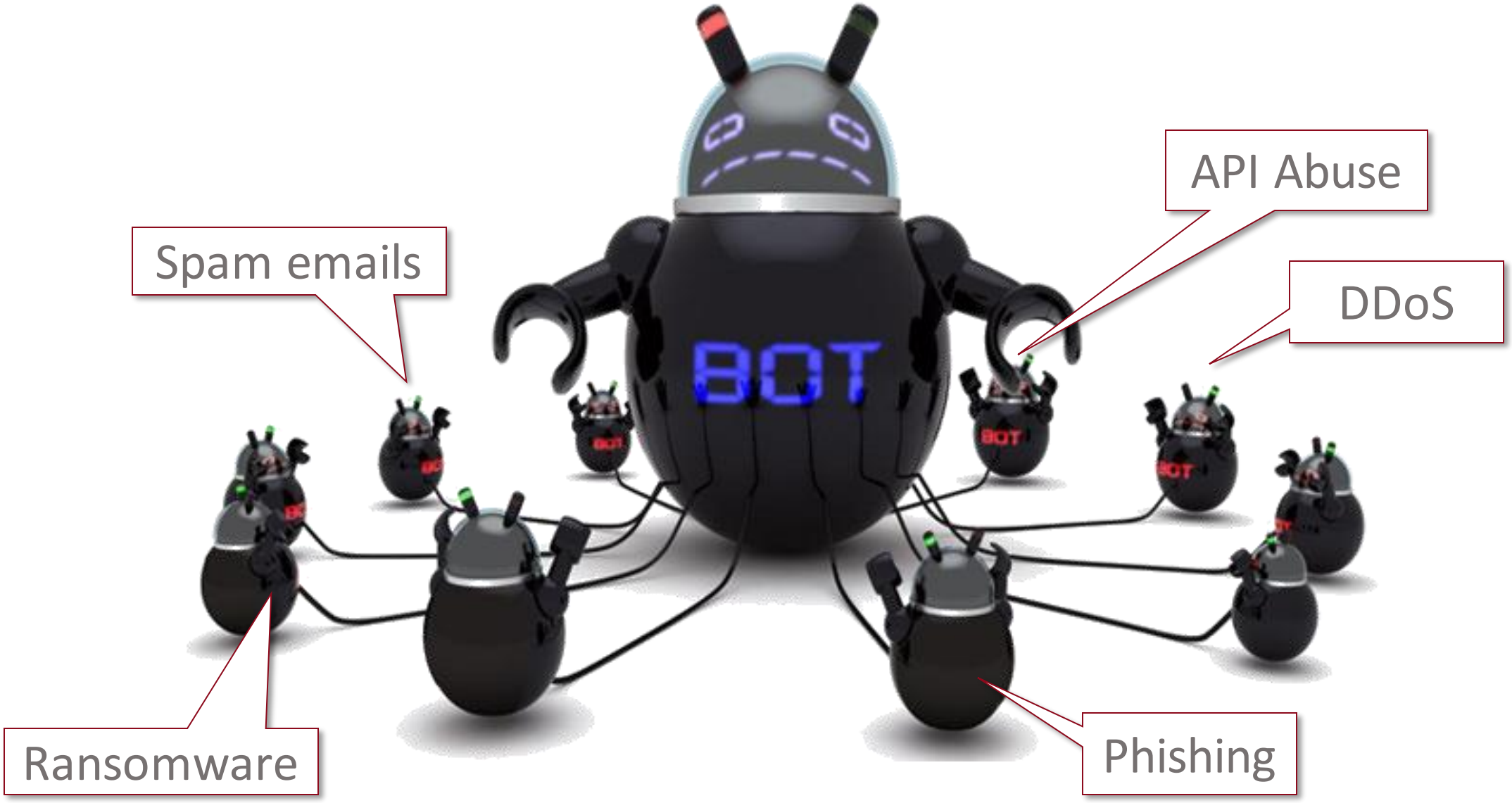
2016–2019年 企業が受けた攻撃の種類



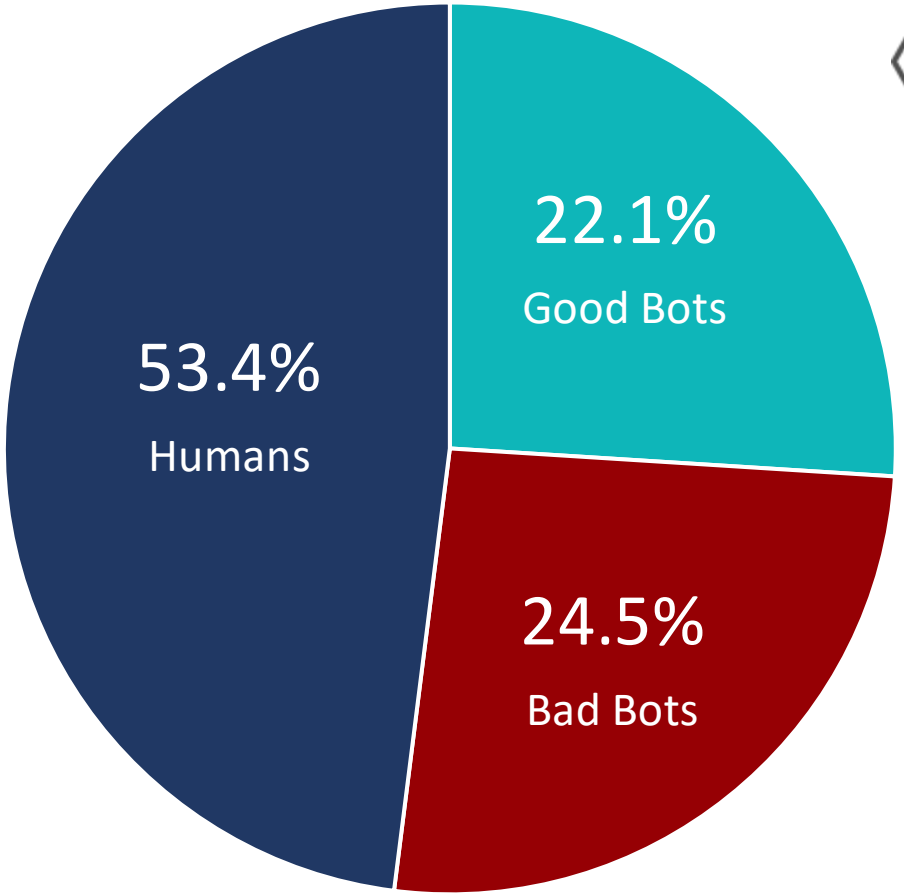
What’s Bot?

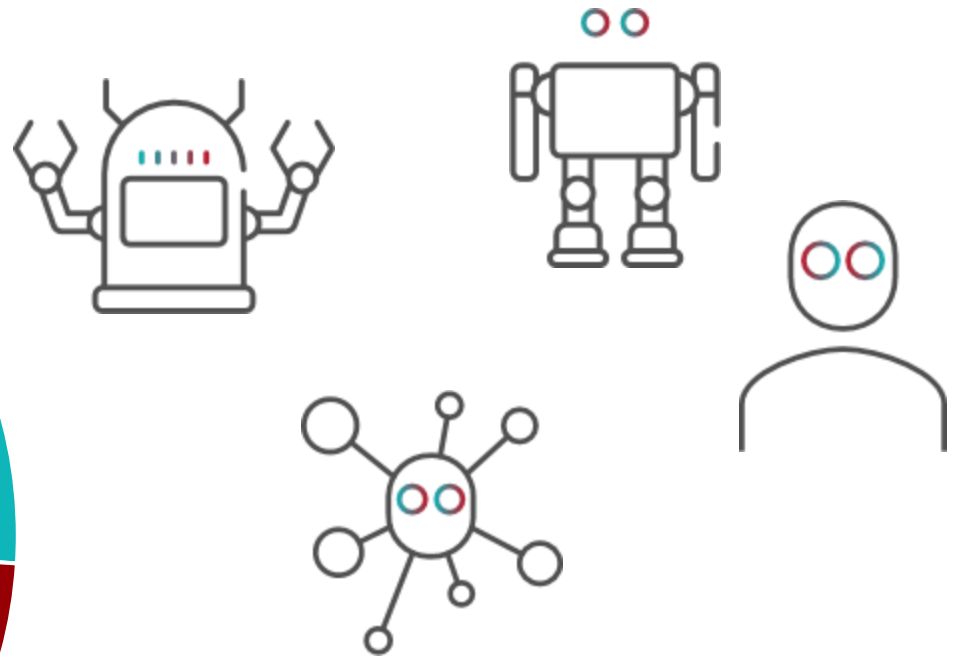


Botnet



Bots in The Internet



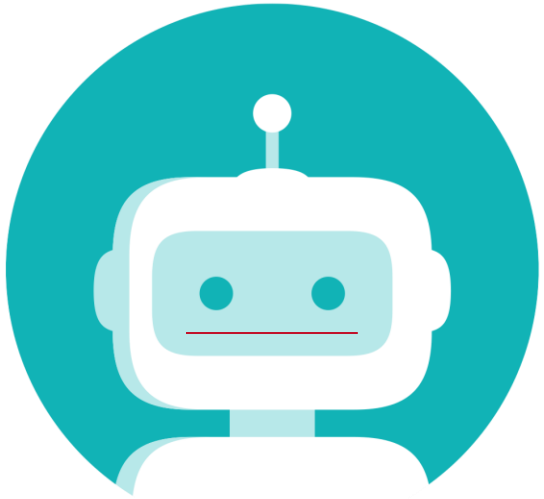


24%がBad Bots

Source: Radware The Big Bad Bot Problem 2020

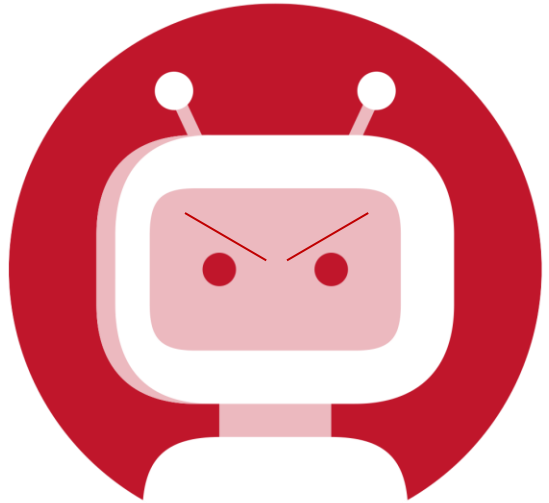
75%の組織が*Good or Bad*を判別できていない

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…）

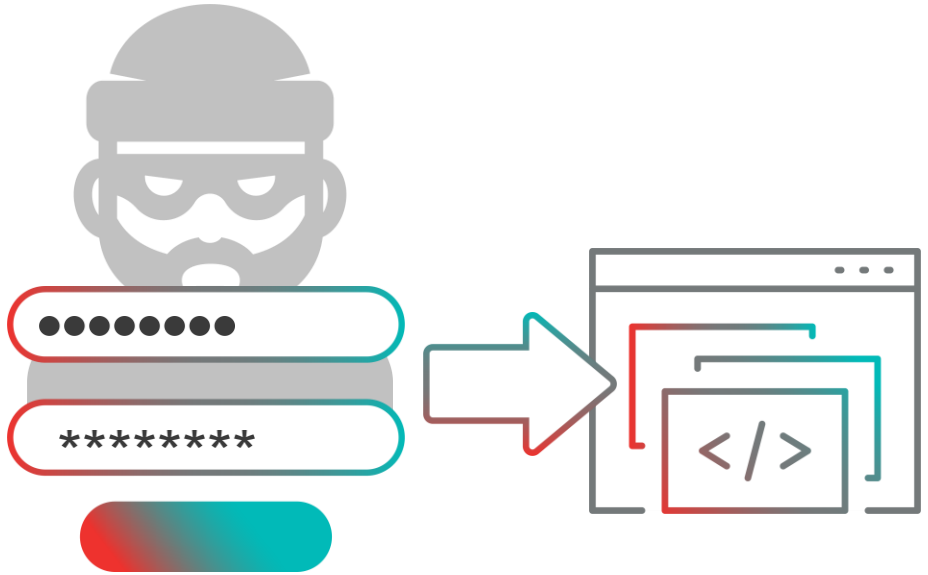


Bad Botの例

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



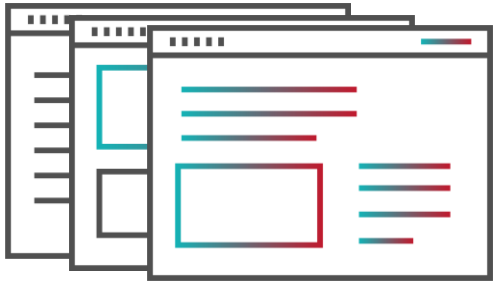
データ流出

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、公開情報収集（個人情報 等）



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

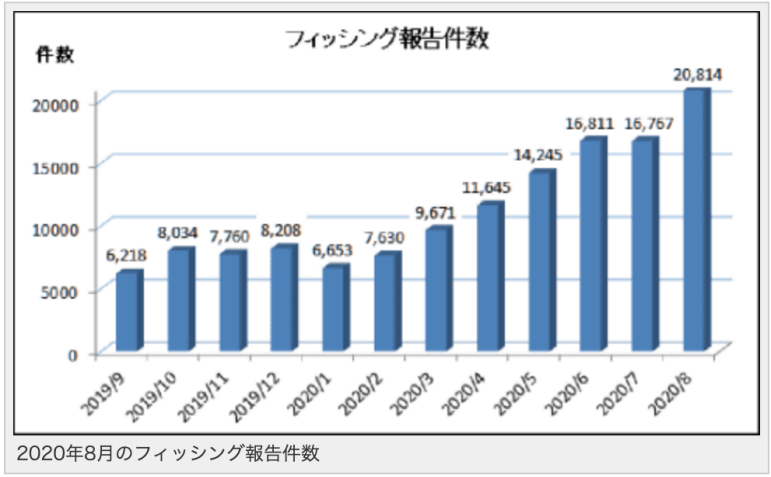
Bad bot example: Web Scraping

Amazon アカウントの 情報を更新する必要があります https://accountupdate.amazon.hyk1.com/

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グ担当者に提供する会社が、Instgram・TikTok・YouTubeのユーザーの氏名・連絡先をはじめとした個人情報、合計2億3500万人分が含まれるデータベースを誰でもアクセスできる状態で公開していたことが判明しました。データはもともと各プラットフォームからウェブスクレイピングで取得

■7万枚超の女性ユーザーの写真

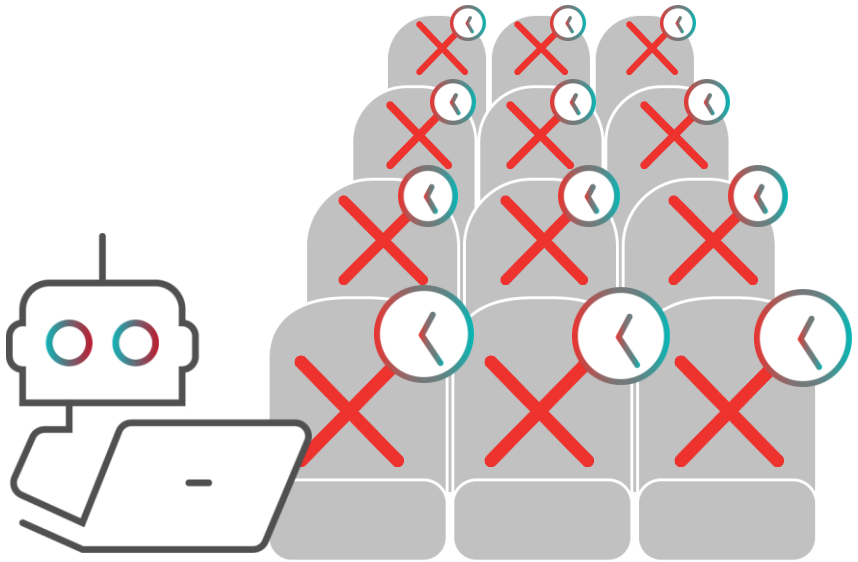
出会いを求めるアメリカの大学生の間で大流行し、4～5年ほど前から日本でも利用されるようになった「Tinder（ティンダー）」。気軽にハイスペックな男子・男性と知り合える、外国人との出会いが多い、などとも言われている。

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。

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

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

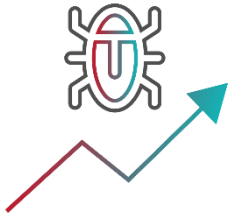
Application DDoS

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

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/

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/

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

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/

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

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

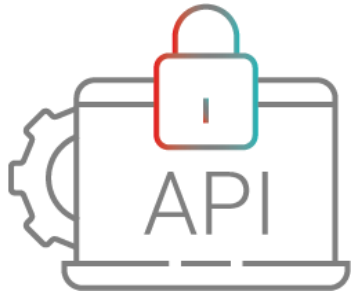
インドMcdonald のMobile Appが220万人以上のユーザ個人情報を流出　API経由の攻撃
https://www.securityweek.com/mcdonalds-app-leaks-details-22-million-customers

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

Bot Targets

WEBSITE

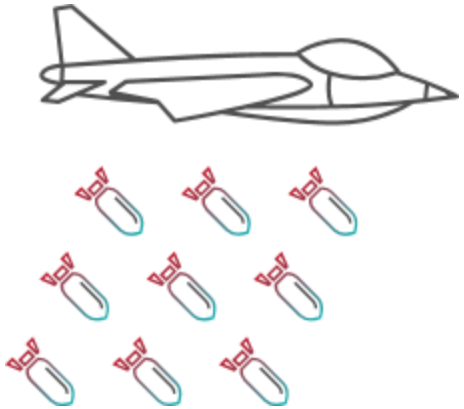
MOBILE
(WEB/APP)



API

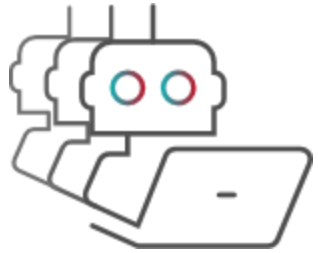
Radware Solutions

Radware Solutions against threats



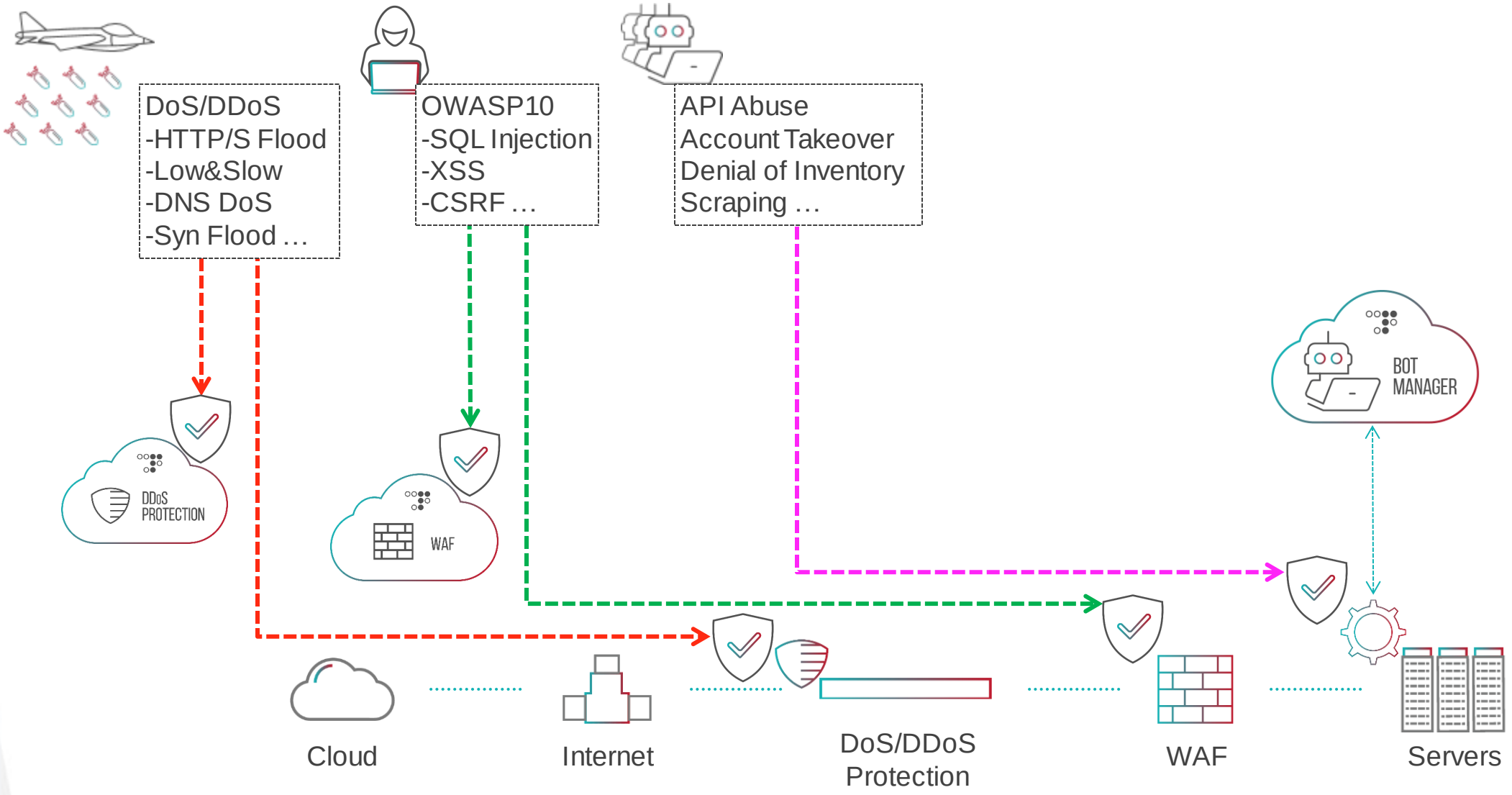
DoS/DDoS

WebApp(OWASP10)



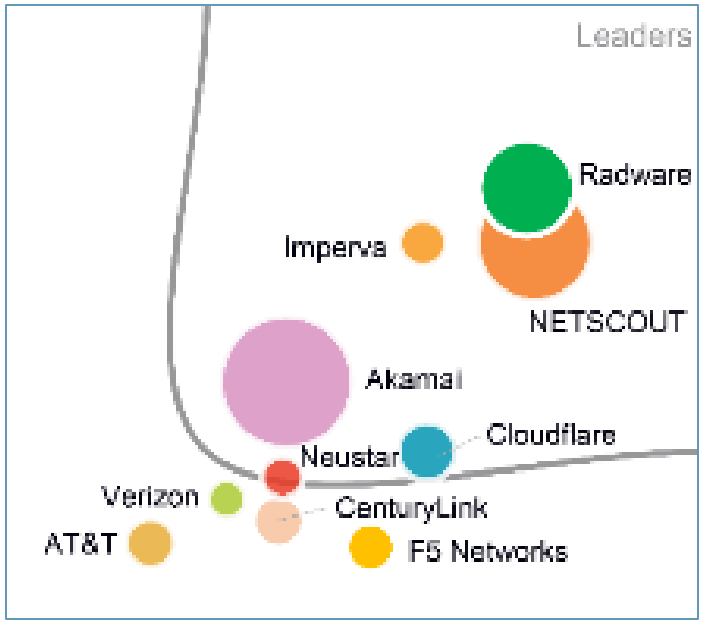
Bot/API

Radware Solution Map (abstraction)



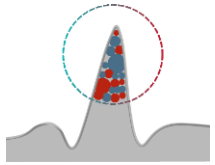
Radware DDoS Protection

テクノロジ ポジション



Source: IDC MarketScape WW DDoS Prevention Solutions 2019

高いプロテクション能力



振る舞い検知
機械学習による適切な保護

ゼロデイ検知
自動リアルタイム
シグネチャ生成

SSLキーレス検知
低遅延、独自の緩和手法

業界唯一の”6”SLA
検知時間や緩和への時間
etc…

柔軟な展開方式

Cloud Service
Always-on/On-demand

Hybrid
Cloud & Appliance

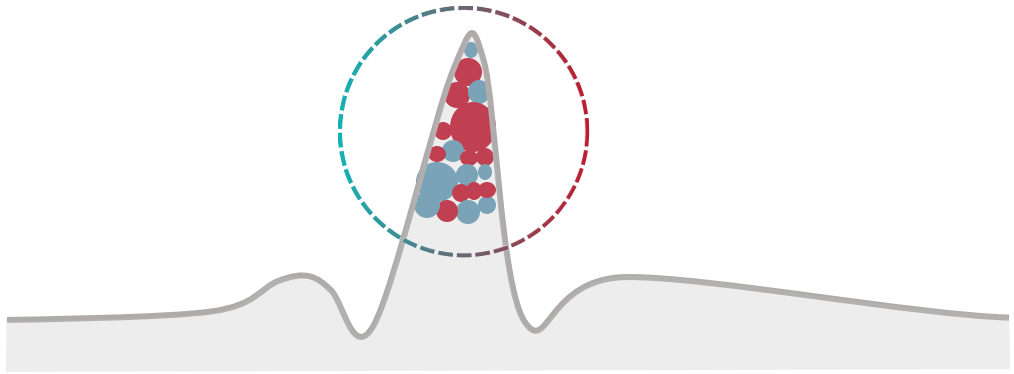
Appliance
Physical/Virtual

Managed Service
Emergency Response Team

Behavioral-Based Detection

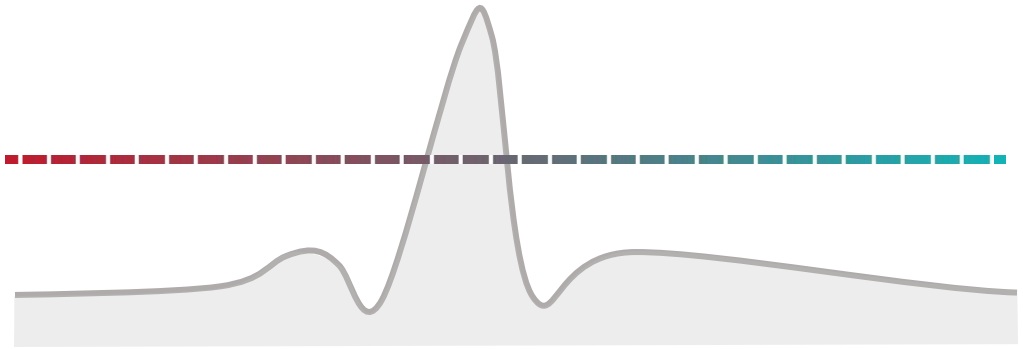
Radware

振る舞い検知



Non-Radware

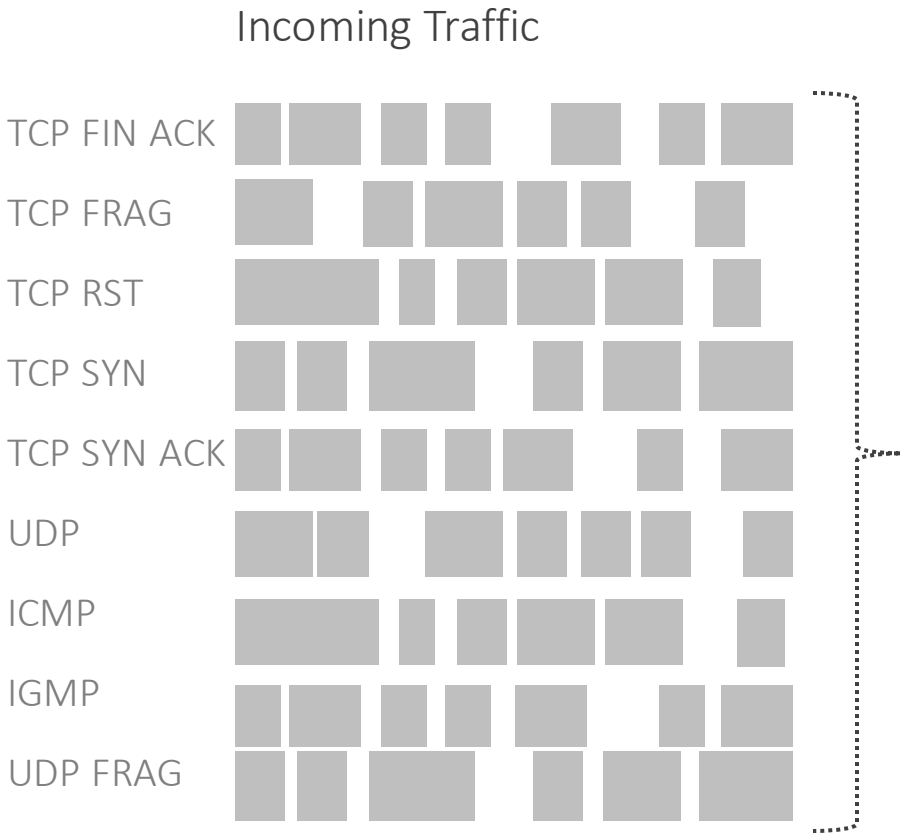
単純なレートリミット



Radware独自の機械学習アルゴリズムで攻撃トラフィックと通常トラフィックを分別

ゼロデイ攻撃検知と誤検知率低下を両立

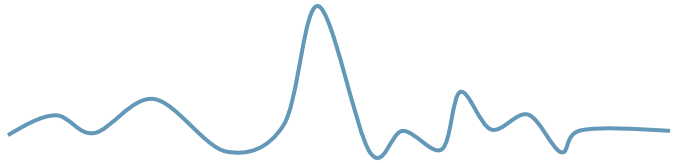
Behavioral-Based Detection

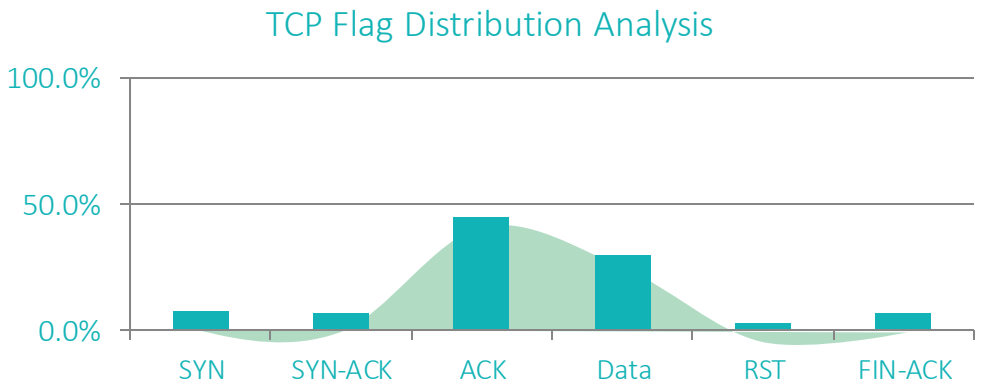


統計+比較

異常を検知

Rate Analysis(PPS)

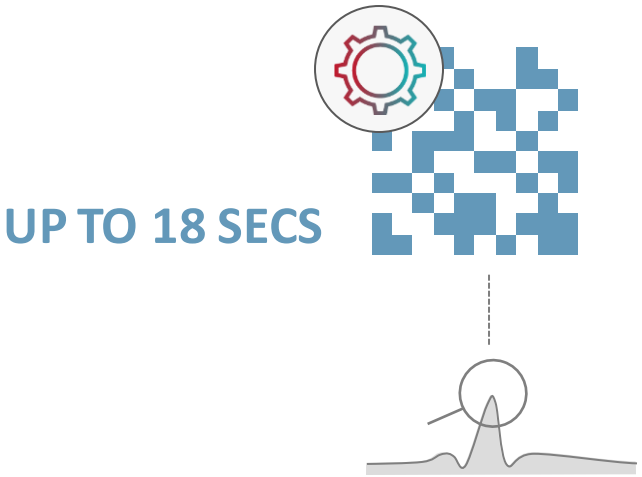




Zero-Day Detection and Quick Mitigation

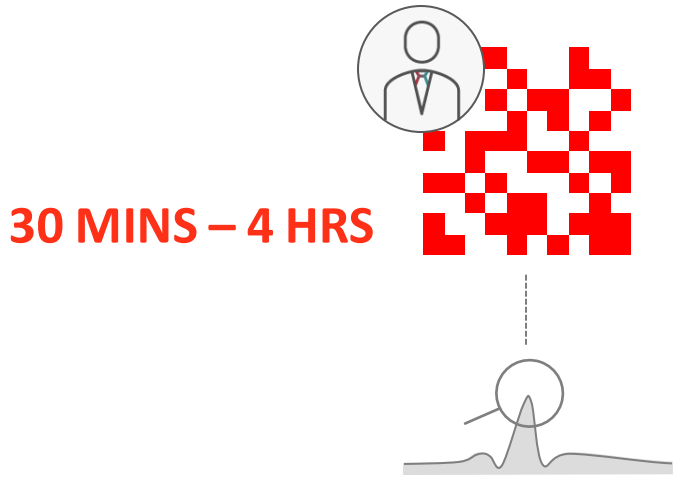
Radware

リアルタイムSignature自動生成



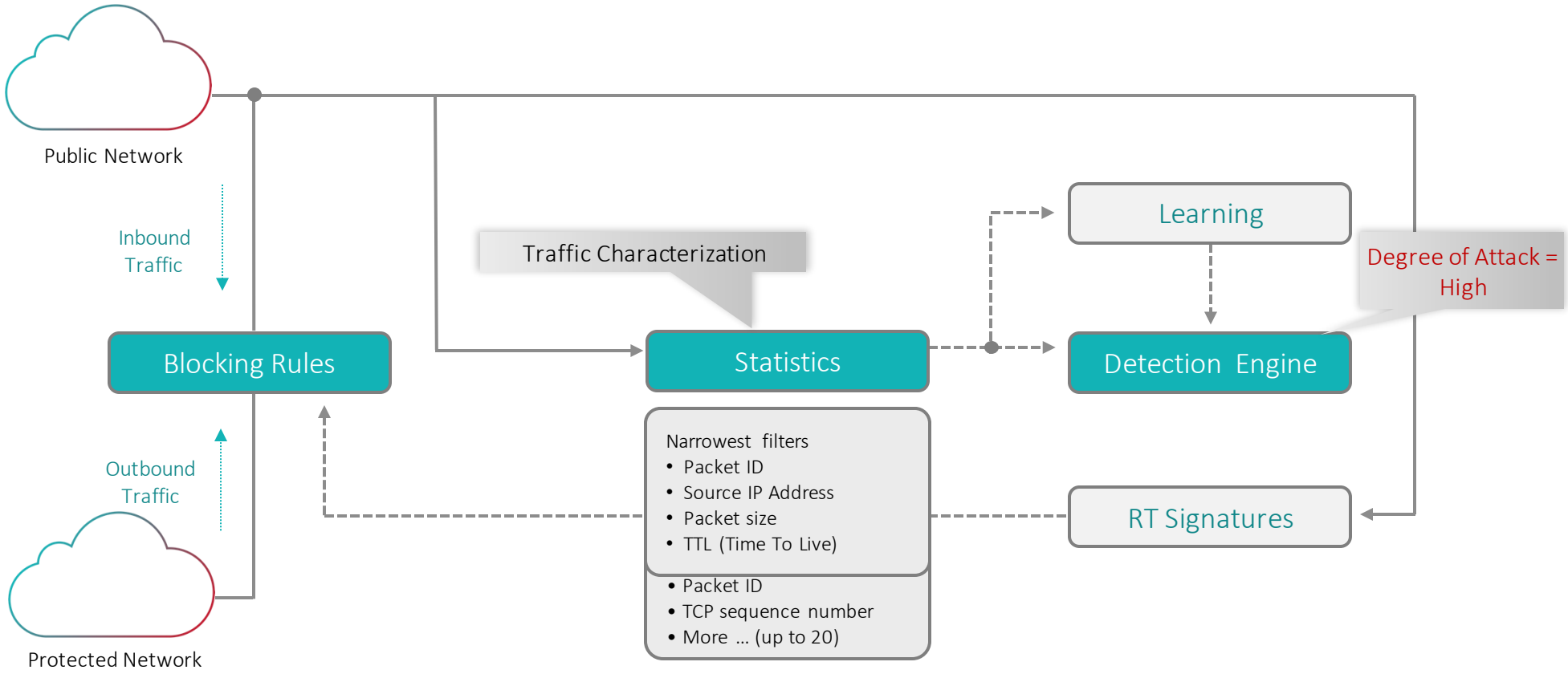
Non-Radware

マニュアルSignature作成



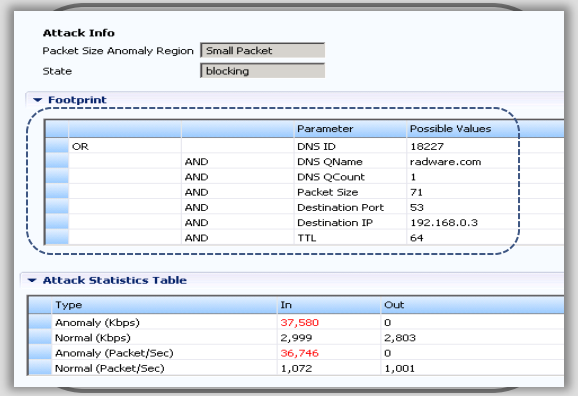
リアルタイムにSignatureを自動生成し適用、調整（SourceIP以外にも複数のパラメータを利用）
ゼロデイ攻撃に秒単位で対応可能

Behavior Analysis + Real Time Signature technology



Behavior Analysis + Real Time Signature technology

Mitigation Optimization Process



Attack Info

Packet Size Anomaly Region: Small Packet

State: blocking

Footprint

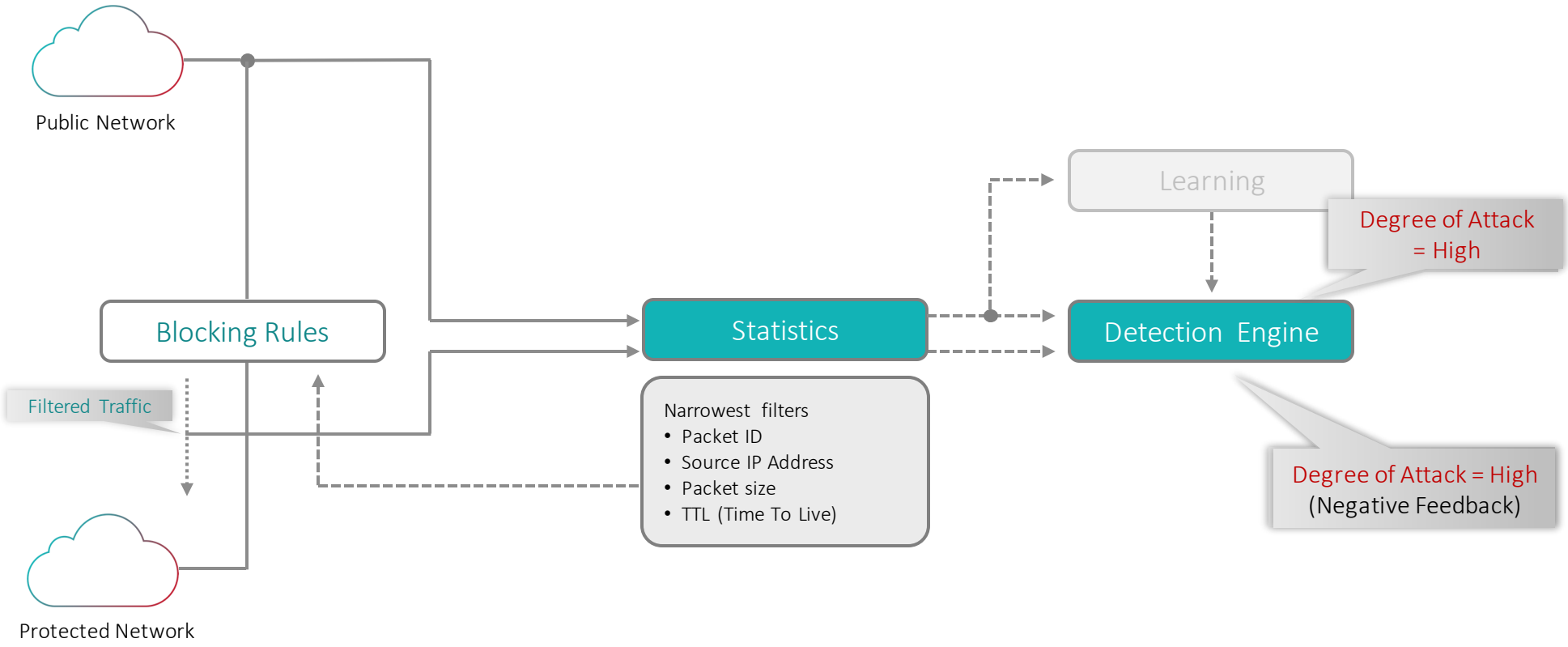
		Parameter	Possible Values
OR		DNS ID	18227
	AND	DNS QName	radware.com
	AND	DNS QCount	1
	AND	Packet Size	71
	AND	Destination Port	53
	AND	Destination IP	192.168.0.3
	AND	TTL	64

Attack Statistics Table

Type	In	Out
Anomaly (kbps)	37,580	0
Normal (kbps)	2,999	2,803
Anomaly (Packet/Sec)	36,746	0
Normal (Packet/Sec)	1,072	1,001

- Initial filter is generated: Packet ID
- Filter Optimization:
  - Packet ID AND Source IP
  - Packet ID AND Source IP AND Packet size
  - Packet ID AND Source IP AND Packet size AND TTL

Real-Time Signature



Global Cloud Security Network

11 Scrubbing Center **5TB/s** Backbone

業界最大規模のバックボーン（DDoS/WAF）

“6” Service Level Agreement(SLA)

Time to Detect
検知までの時間

Time to Alert
アラートまでの時間

Time to Diversion
切替までの時間
（on-demandの場合）

Time to Mitigate
緩和までの時間

Consistency of Mitigation
緩和の一貫性

Service Availability
サービス可用性

Time to Detect SLAはRadwareの特徴

Radware WAF Positive Security Model

Negative Security Model

大半のクラウドWAFサービスとWAFテクノロジーで標準的に採用

既知シグネチャ/ルールを用いて既知攻撃をブロックする

OWASP TOP-10に対して完全な防御は**不可能**

未知の脆弱性（ゼロデイ攻撃）は防御**不可能**

Positive Security Model

どのアクションが正規トラフィックであるか学習し定義

権限のないアクセスや未許可のアクションをブロックする

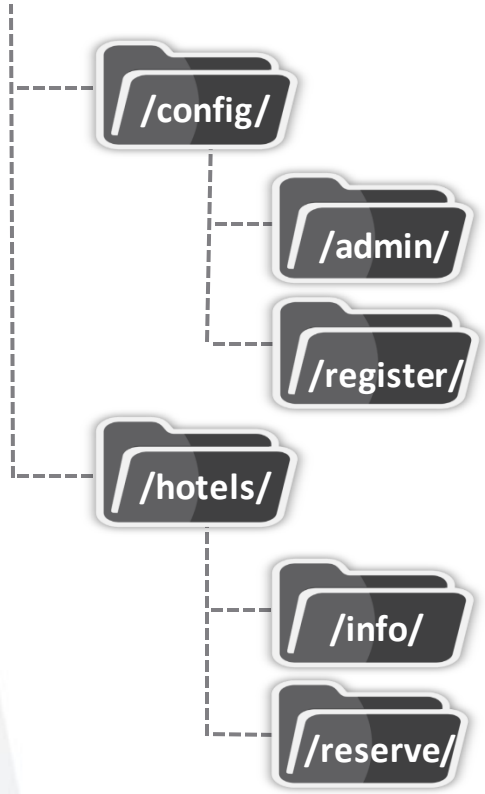
ゼロデイ攻撃や未知の脆弱性を独自の方法で防御

ハイレベル防御：OWASP TOP-10を**完全に防御、最小限の誤検知**

Radware WAF Auto Policy Generation

App Mapping

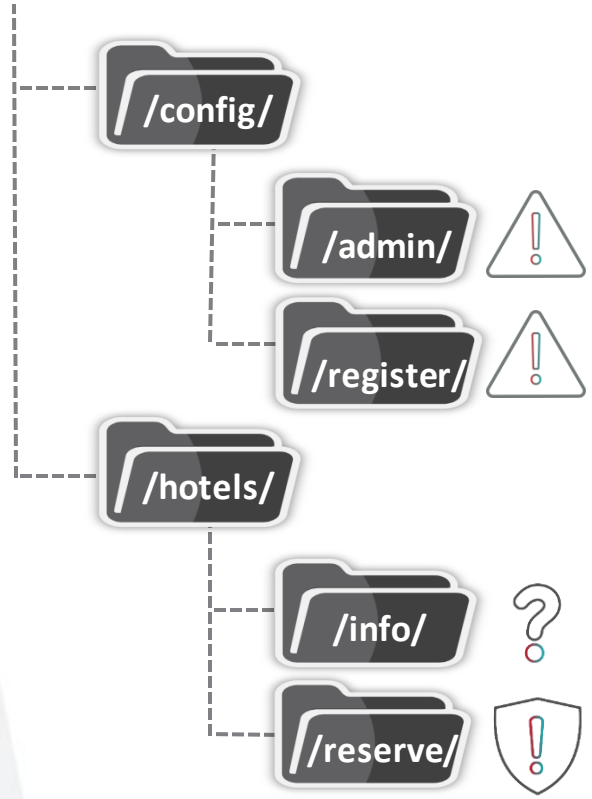
www.reservations.com



Radware WAF Auto Policy Generation

App Mapping | Threat Analysis

www.reservations.com

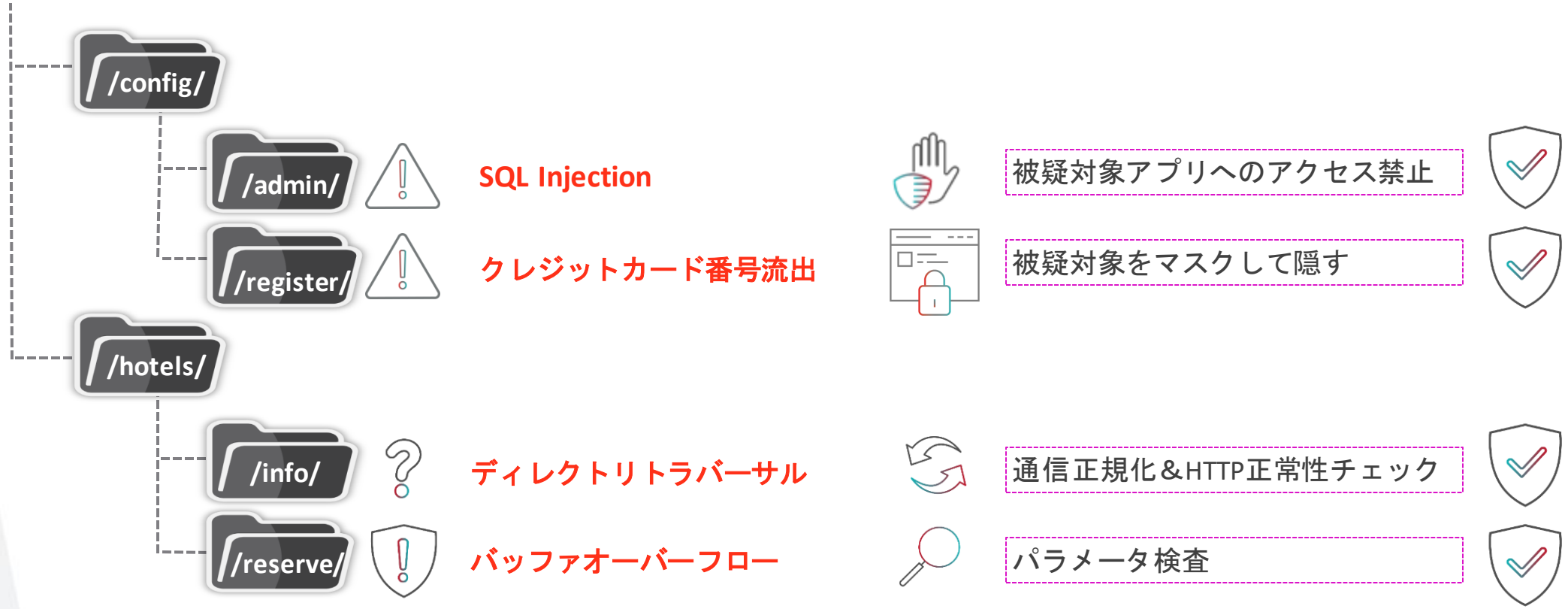


SQL Injection	なりすまし、情報漏えい、 データ改ざん
クレジットカード番号流出	情報漏えい
ディレクトリトラバーサル	ルートアクセス権奪取
バッファオーバーフロー	システムクラッシュ、 性能の著しい低下

Radware WAF Auto Policy Generation

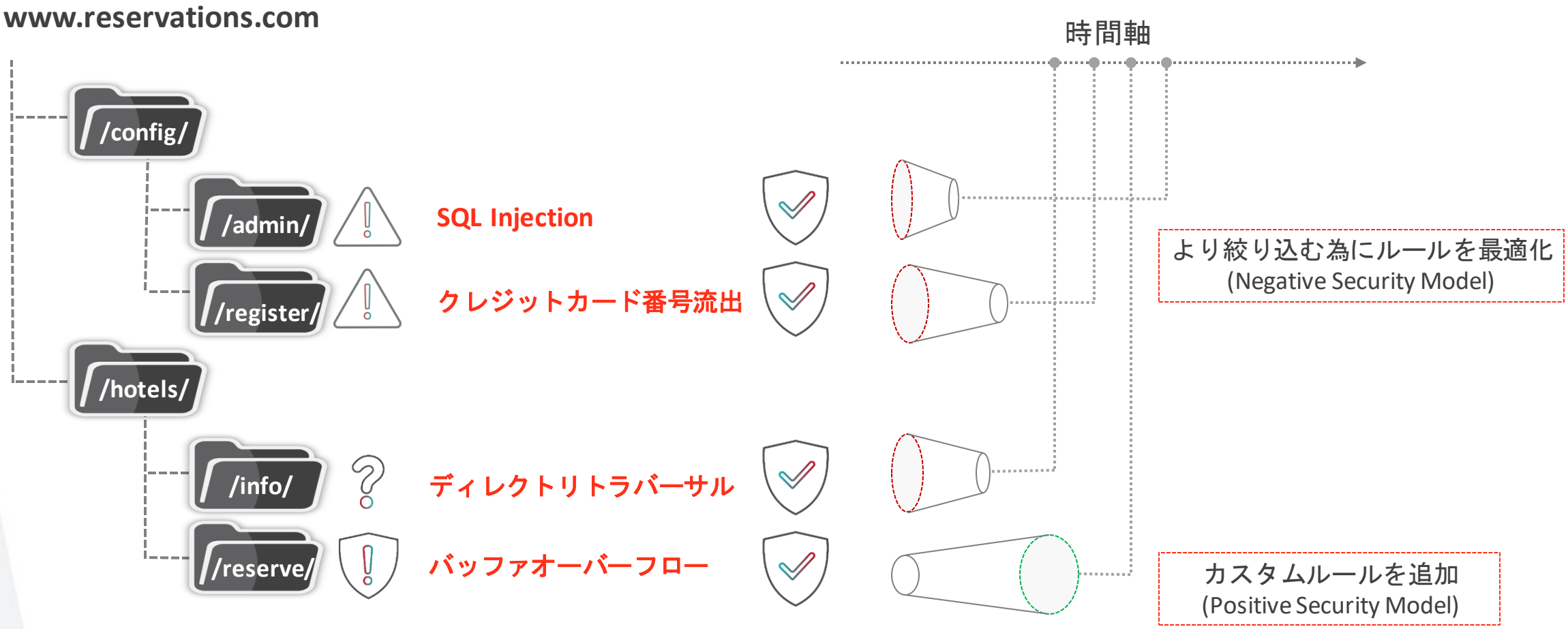
App Mapping | Threat Analysis | Policy Generation

www.reservations.com



Radware WAF Auto Policy Generation

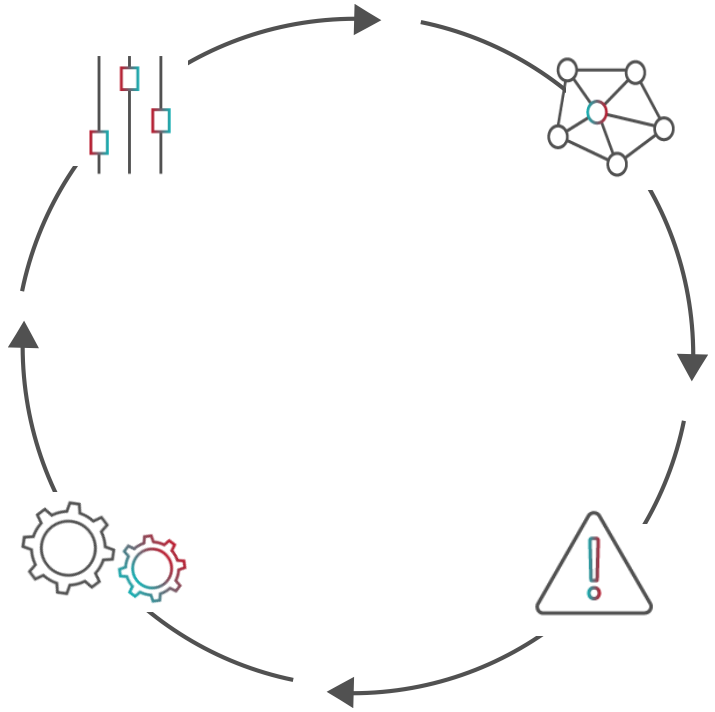
App Mapping | Threat Analysis | Policy Generation | Policy Activation



Radware WAF Auto Policy Generation

自動ポリシーアクティベーション
カスタマイズしたアプリルールを
最適化し精度向上

自動最適化によるポリシー生成
誤検知を最小化する
独創的なルール



アプリマッピング
Webアプリの新規/変更を検知

自動脅威分析
OWASP Top-10すべてと
150以上の攻撃ベクトルに対応

アプリの変化とユーザの振る舞いを継続的に監視しつつ、最適な保護環境を調整

Use Case: Cisco Webex

Challenge

30x DatacenterのWebSecurityとDDoS対策

Radware Solution

DCあたり、
1x DefensePro(DDoS)
4x AppWalls(WAF)
2x Alteon(ADC)

Why Radware

DDoS
- 攻撃手法に対するカバー範囲の広さ
- 検知率の高さ、誤検知無
- 緩和までの時間

WAF
- Auto Learning
- 導入と運用がEasy
- UIがEasy

Competition

A社:
- いくつかの攻撃が通った
- 誤検知（正規ユーザがブロック）
- 誤検知率が高かった

Points of Presence(PoP) for Cloud WAF Service

グローバルに張り巡らされたアプリケーションセキュリティネットワーク（5TB/s）

30のPoPにより対象を低遅延で保護, DDoS 1GB/s Default付与, Bot Manager Option選択可

Radware PoPとAzure DCを活用してCloud WAFを実装

Azure Native Radware Cloud WAF

独自のクラウドセキュリティネットワークに加え、RadwareのCloud WAFは、
Microsoft Azureのネットワーク内でNativeに動作する

Azureのデータセンター内からネイティブに実行できる
唯一のクラウドWAFサービス

ラドウェアのWAFテクノロジーに基づく
エンタープライズレベルの防御

マイクロソフトの光ファイバーバックボーンに基づく最小遅延時間

Emergency Response Team(ERT)

Attack時の対処等、迅速に対応可能
24時間365日稼働
セキュリティ専任チーム

Security Managed Service w/Experts

- テクニカルアカウントマネージャ
- アナリストおよび専門家
- 脅威のリサーチ
- SOCおよびクラウドの運営

Emergency Response Team(ERT)

Cloud WAF Standard

Cloud WAF 利用料金のみ＝追加料金無し

30分SLA 電話サポート

24時間365日稼働

攻撃後分析サービス
（Forensic & Advice）

Cloud WAF Premium

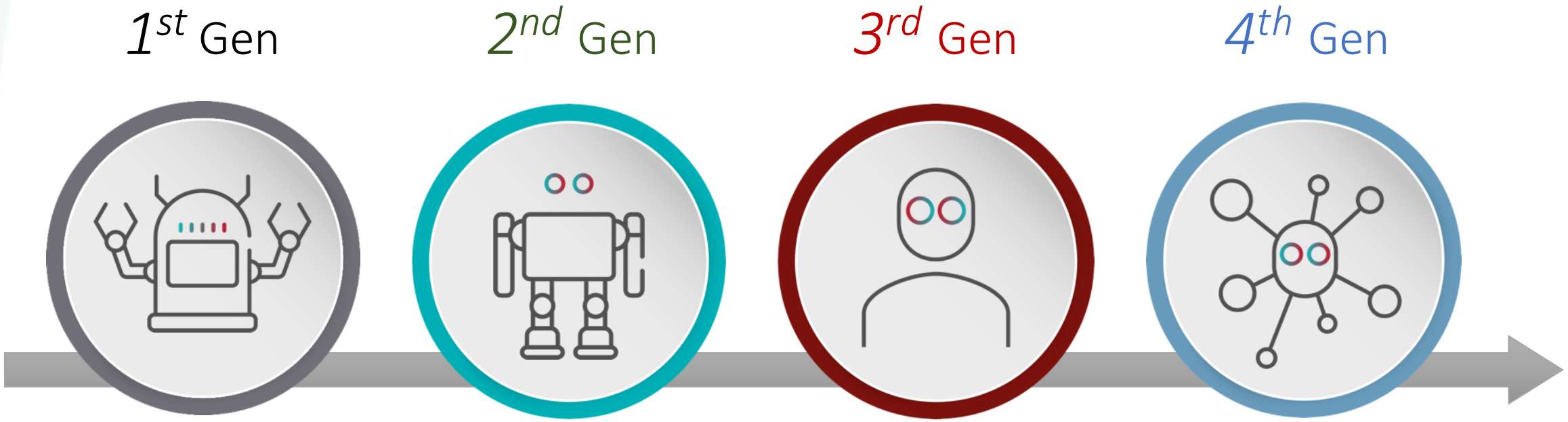
追加料金が必要

サクセスマネジャー

10分SLA ホットライン

定期レポート

Bot Generations



SCRIPT BOT

単純なスクリプト
1つ2つのIPアドレスを使用

HEADLESS BROWSER BOT

ブラウザを模擬して活動
Javascript実行
Cookie維持

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

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

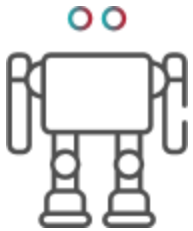
Radware Bot Manager

Radware Bot Manger

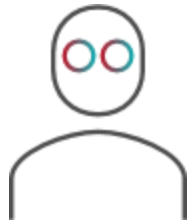
他社

Bot

Script Bots



Headless Browser Bots



Human-like Bots

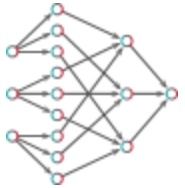
Distributed Bots

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

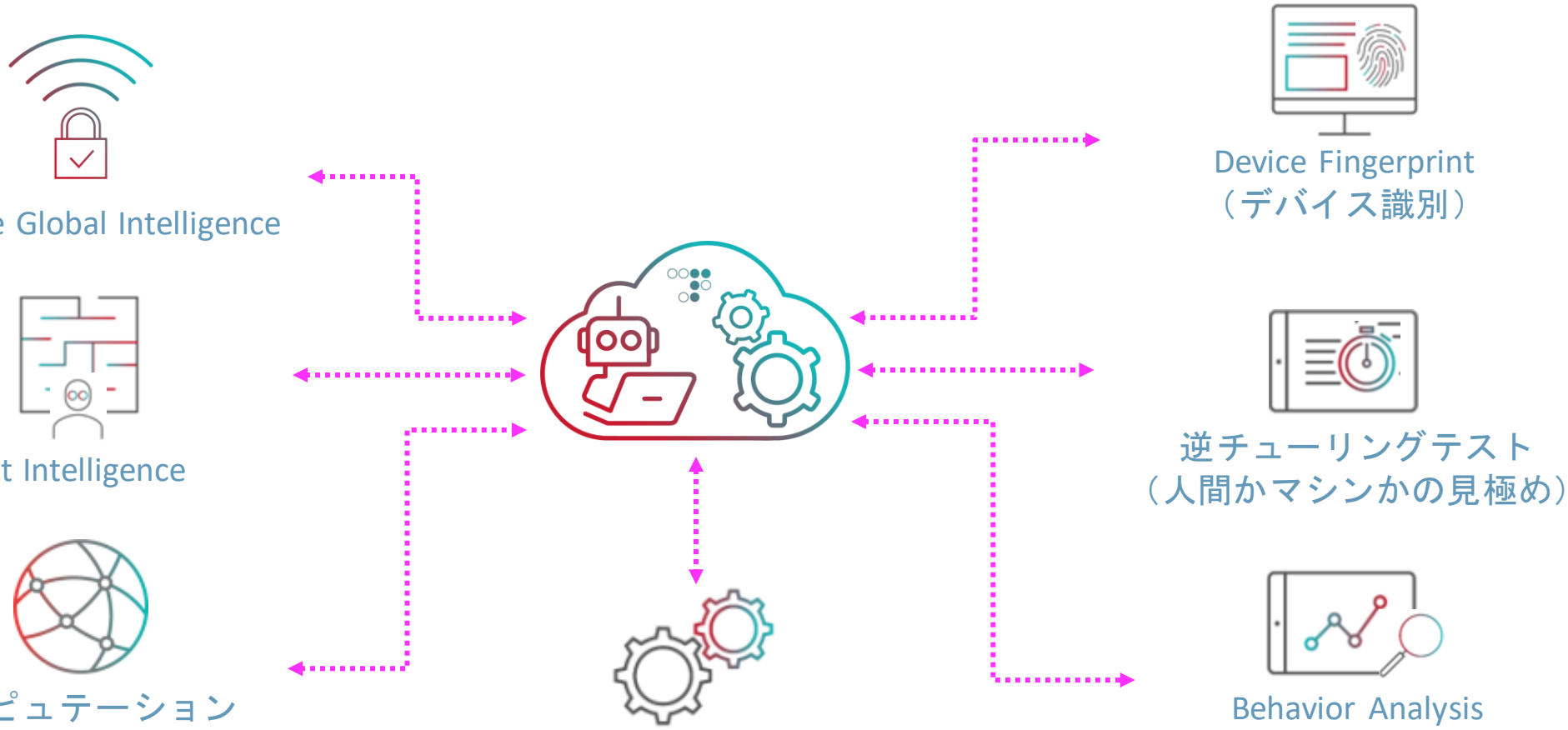
A Bad Bot Attack （ある優れたBotの例）

攻撃期間: 1day

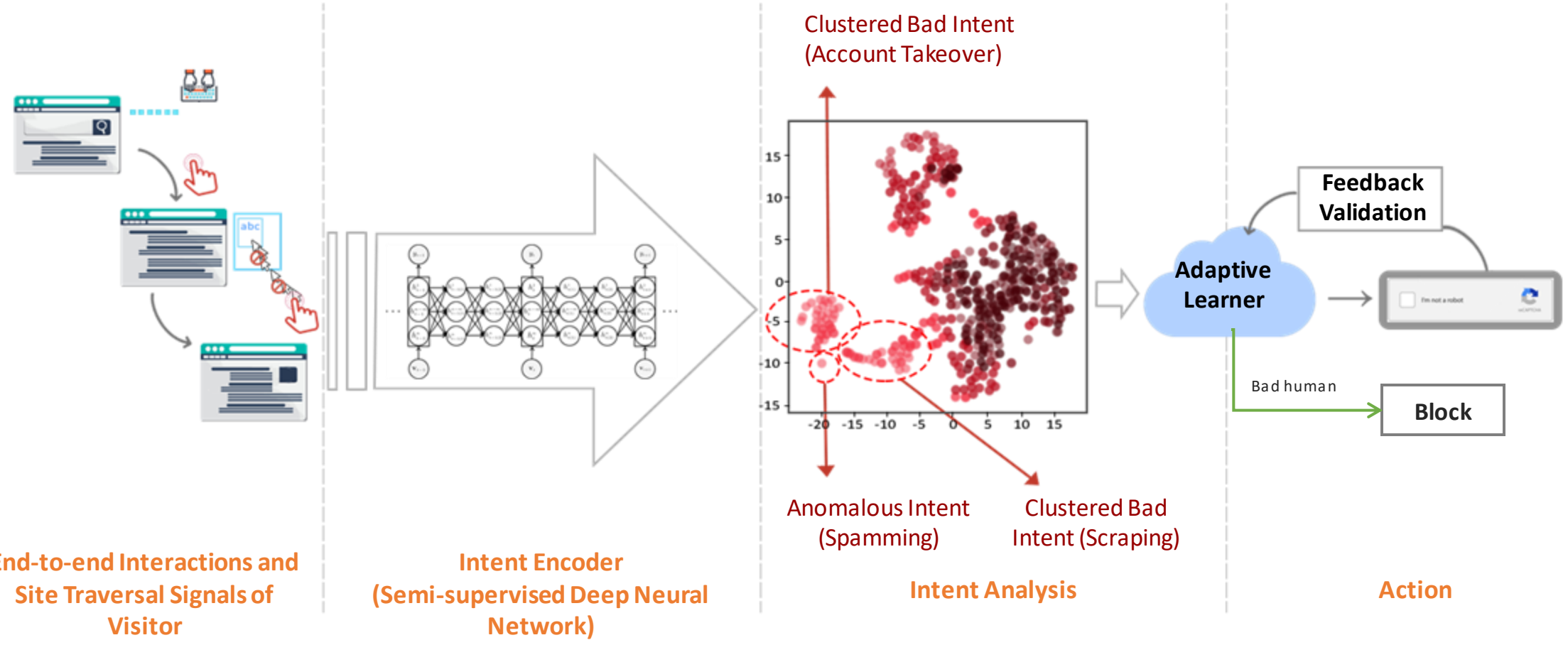
IP数	Bot Hit数	同一IPから2回以下のHit数（1時間以内）	ISP数	4時間以上ActiveだったIP数
52,278	210,723	51,658	2,802	2,847

基点となった国数: 48

BotManager Engine



Intent-based Deep Behavior Analysis

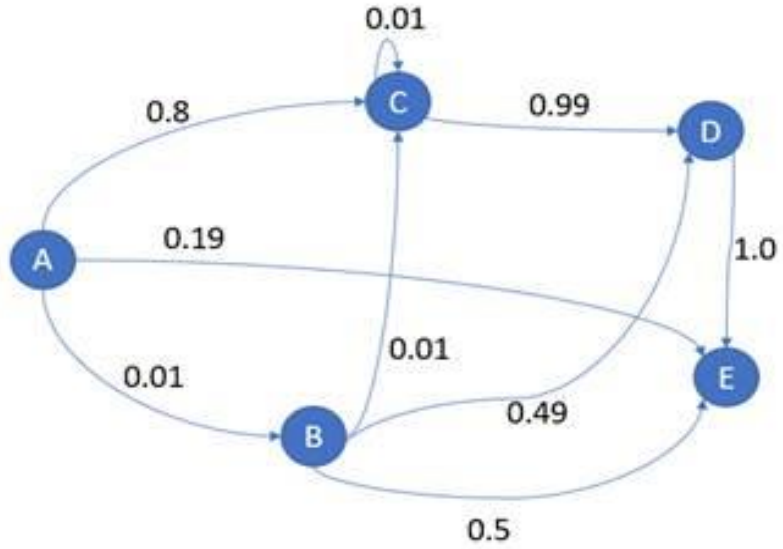


API Flow Control Module

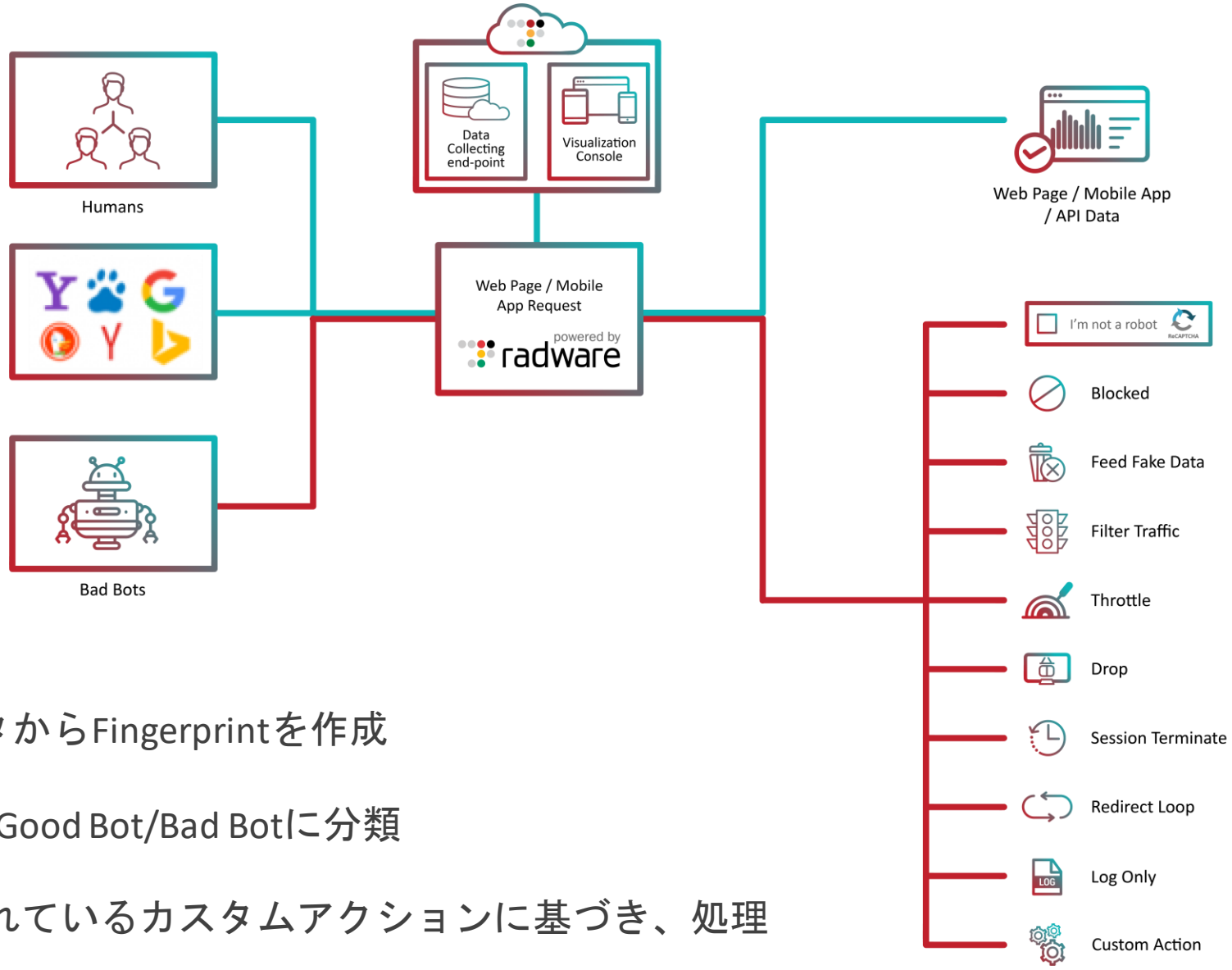
- A → B → C → C → D → E と遷移する確率＝0.00000099
- アクセスパターンを分析し、APIアクセス統計を自動作成
- APIシーケンスが悪性かどうかをチェック
- ログインや通常のページ遷移が無いDirect APIアクセスを検知

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

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)

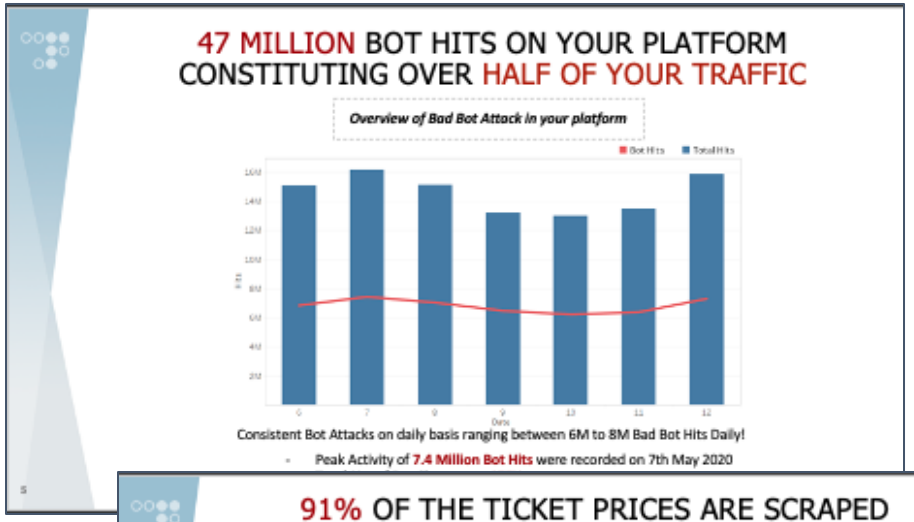
ボットトラフィックやボット攻撃検査用の無料評価ツール

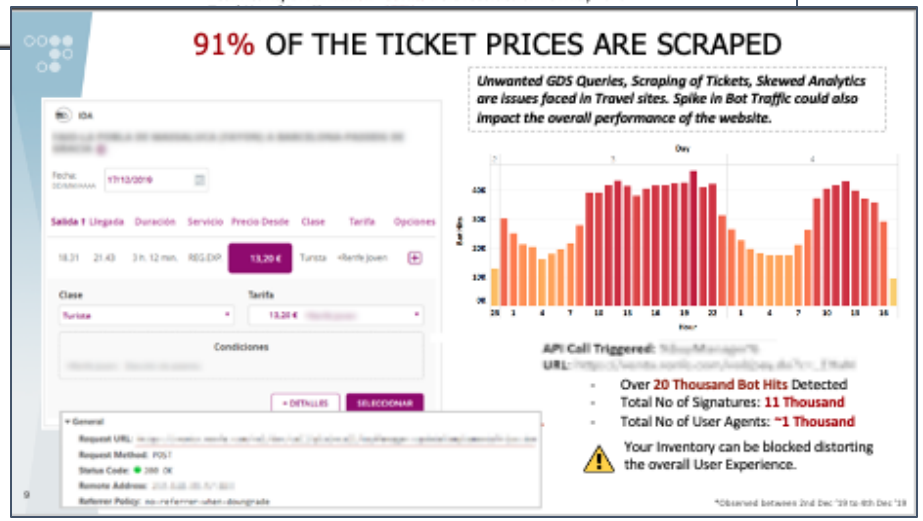
- 有害なボットトラフィックのボリュームを評価します。
- アカウントの乗っ取り試行、インベントリの偽装確保、架空請求、Webスクレイピングに対する可視性が得られます。
- あらゆるチャネルのテスト：Webサイト、モバイルアプリ、API
- 有害なボットのトラフィックを分析して巧妙度をレベル分けし、人に似た振る舞いを追跡します。
- ヒントとアドバイスが得られます。

*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

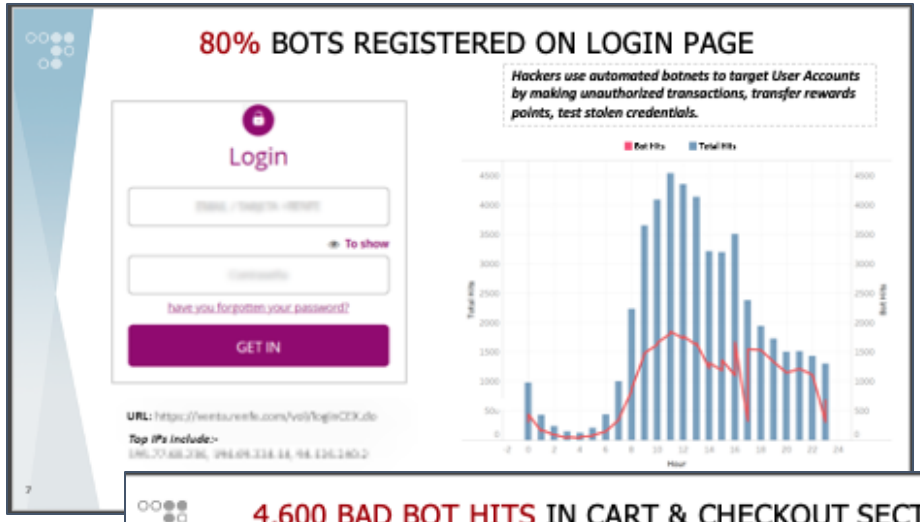
BOTがどれくらい来ているか（Good/Bad内訳）

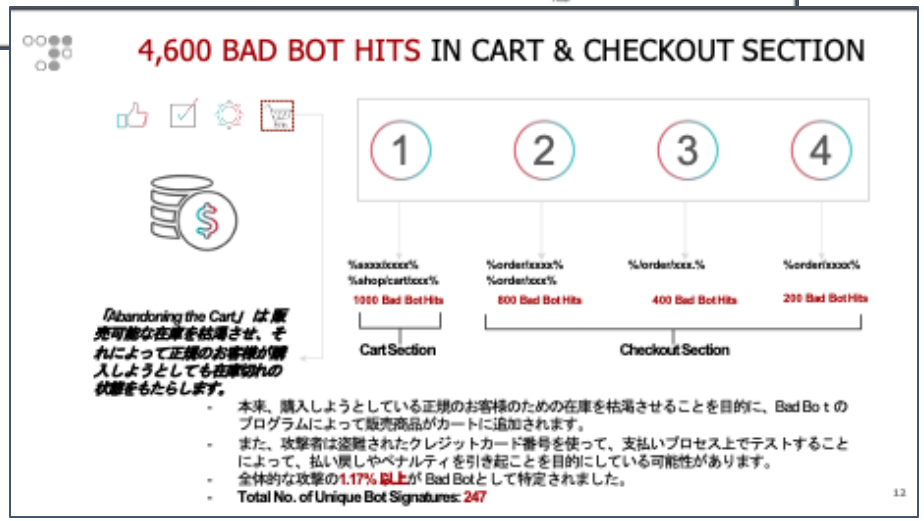




商品ページにおけるScrapingの可能性

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

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

Summary

- About Radware
- Threat Trend
- Radware Solutions
  - DDoS
  - WAF
  - BOT
  - Emergency Response Team(ERT)
- Bad Bot Analyzer(BBA)


radware
THANK YOU!