radware

世界で頻発しているランサムDDoSと それを完全に防ぐRadware クラウドDDoSサービス

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

Nov.2020

Agenda

- About Radware
- Trend – Ransome DDoS
- Radware DDoS Solution
- 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

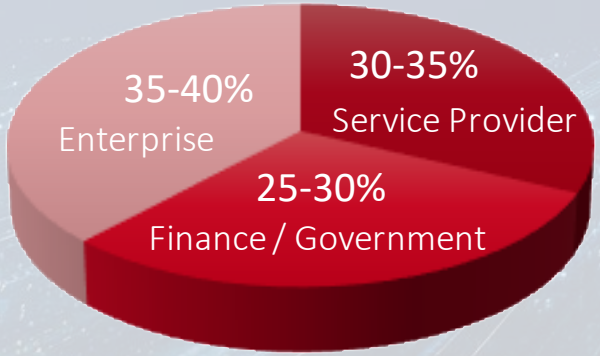
CISCO　Microsoft Azure　NOKIA

- 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

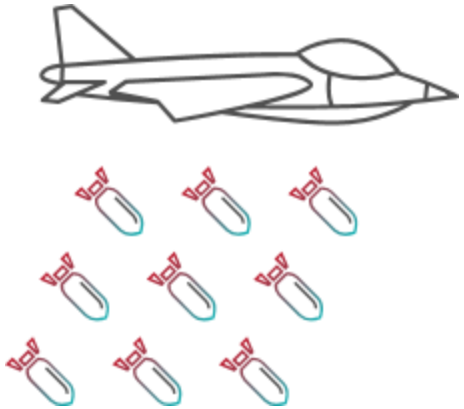
DELTA　ebay　GAP
Marriott Vacation Club　PayPal
SAMSUNG SDS　twitter　ups

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

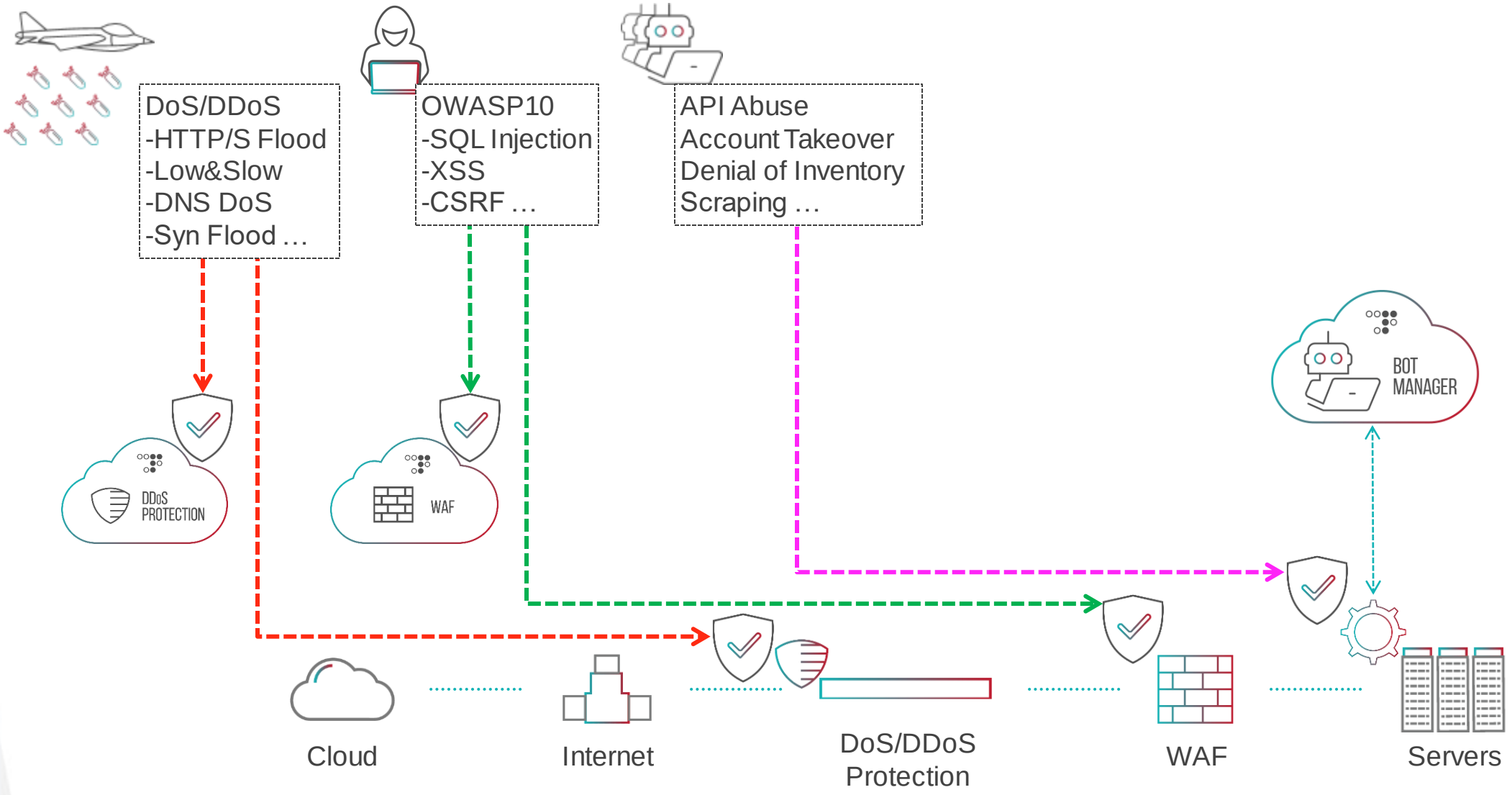


DoS/DDoS

WebApp(OWASP10)

Bot/API

Radware Solution Map (abstraction)



Trend – Ransome DDoS

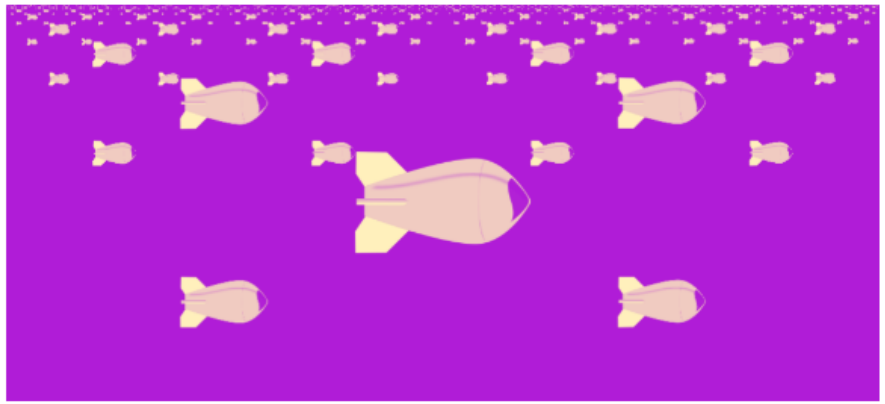
‘Carpet-Bombing’ DDoS Attack Campaign Sep/Oct 2019

'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

SA banks hit by ransom attacks

Oct 25 2019 12:57

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.

“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]

(This is not a hoax, and to prove it right now we will start a small attack on xxx.xxx.xxx.xxx and xxx.xxx.xxx.xxx that will last for 30 minutes. It will not be heavy attack, at this moment.)

What does this mean?

This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your users / customers.

How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The current fee is 1 Bitcoin (BTC). The fee will increase by 1 Bitcoins for each day after [Ransom Deadline] that has passed without payment.

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

2020現在進行系のRansomeキャンペーン

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

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: 2020-10-15

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は「DDoS 脅迫」「ransom DDoS」などとも呼ばれ、攻撃者が標的の組織に払わなければ、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 Armada Collective や Phantom Squad を名乗る攻撃者からの攻撃、2019年には Fancy B 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 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 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

** 更新: 2020年10月15日 **********

2020年10月、本攻撃による被害の報告が複数の国内組織から寄せられています。多くのケー 力を示す目的からか、標的のシステムに対して、数十Gbpsから100Gbpsほどの規模のDDoS 数の IP アドレスやシステムを対象として攻撃が行われる場合もあり、DNS コンテンツサーバ す。JPCERT/CC が確認する限り、攻撃は情報・通信系の組織に対して多く行われている傾向 下させることを目的として、攻撃および脅迫が行われている可能性があります。

Source: 日本経済新聞 https://s.nikkei.com/3lJPqvD

NZ証取にサイバー攻撃、4日連続で一時取引停止

2020/8/28 15:36

保存 共有 印刷

【シドニー=松本史】ニュージーランド（NZ）証券取引所がサイバー攻撃を受 まで4日間連続で取引を一時中断する事態に追い込まれた。サイバー攻撃で取 い込まれるのは異例だ。ロバートソン財務相は証取と協力して原因究明にあた る。

NZ証取は25日、海外から分散型サービス妨害（DDoS）と呼ばれる攻撃を受け、接続障害を起こした。ホームページの閲覧などが難しくなり、株式など現物の取引を停止した。

同証取は翌26日の午前7時すぎに「通常の取引を再開する」との通知を出したが、新たな攻撃を受けたため同11時すぎ、再度取引を停止したと発表した。25日の攻撃と類似性があるとしている。同様の取引停止は27日と28日にも起こった。

ロバートソン財務相 が証取と協力してい =AAP

「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

Cisco blog: https://gblogs.cisco.com/jp/tag/radware/

Fancy Bear: Ransom DDoS Attacks

現在進行系のランサムキャンペーン

- '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が発行されている
- 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3,000万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

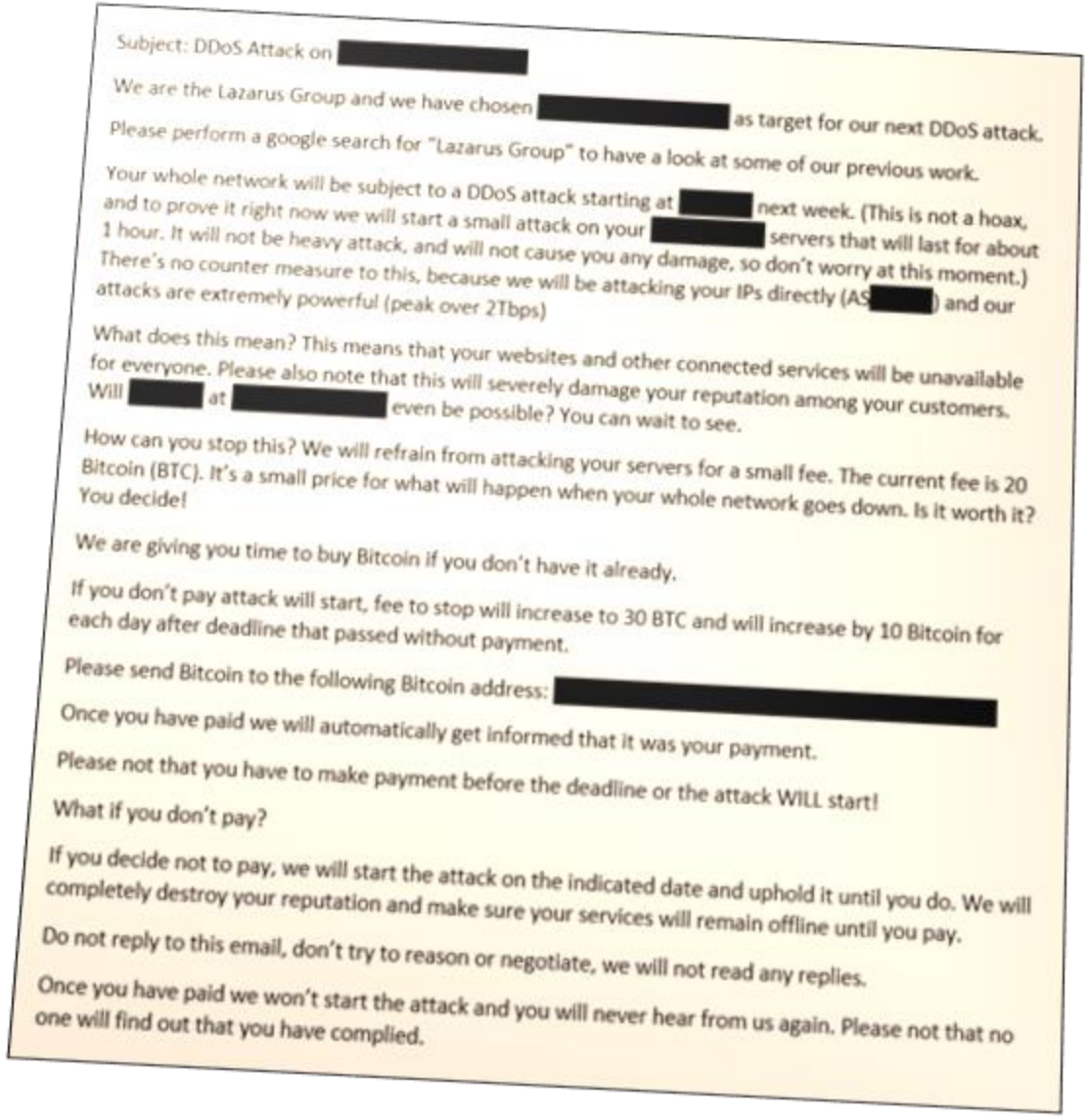
WE NEED YOUR HELP!

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

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 on [redacted]

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.

Your whole network will be subject to a DDoS attack starting at [redacted] next week. (This is not a hoax, and to prove it right now we will start a small attack on your [redacted] servers that will last for about 1 hour. 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 (AS[redacted]) and our attacks are extremely powerful (peak over 2Tbps)

What does this mean? 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. Will [redacted] at [redacted] even be possible? You can wait to see.

How can you stop this? We will refrain from attacking your servers 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.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after 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 not that you have to make payment before the deadline or the attack WILL start!

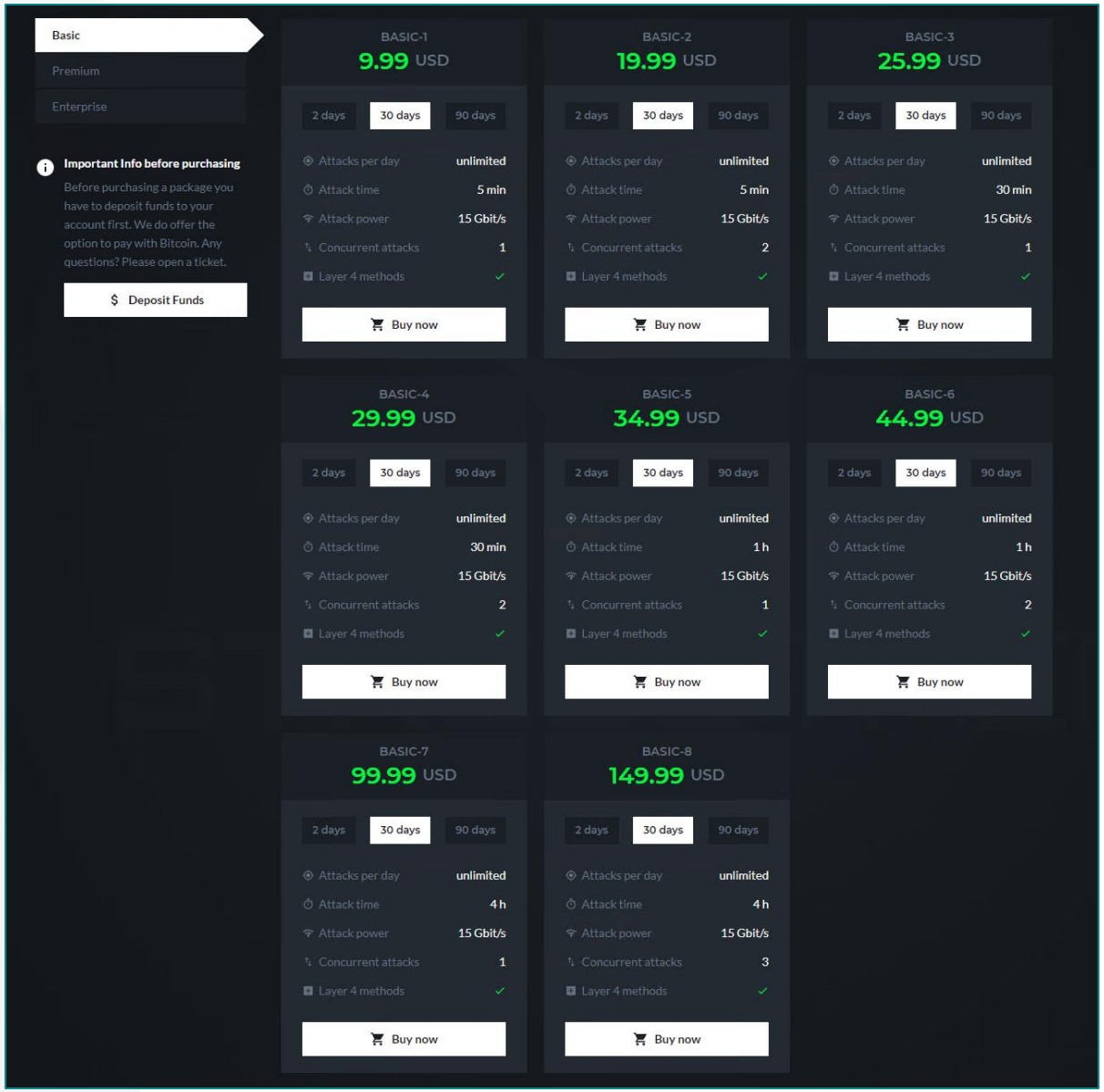
What if you don't pay?

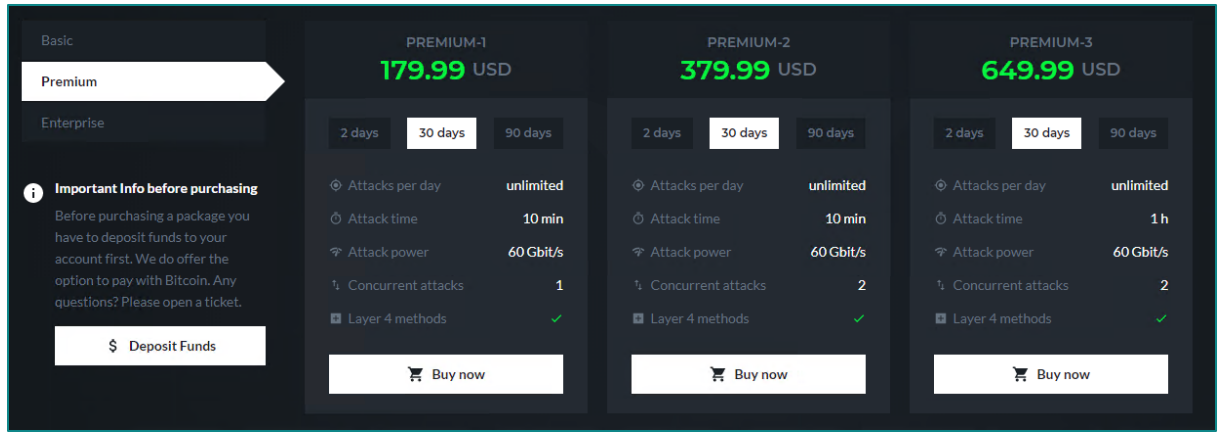
If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

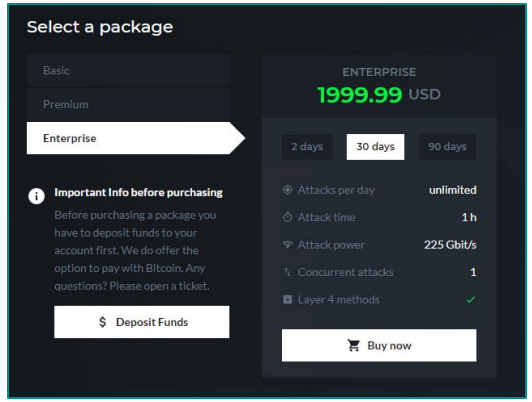
Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

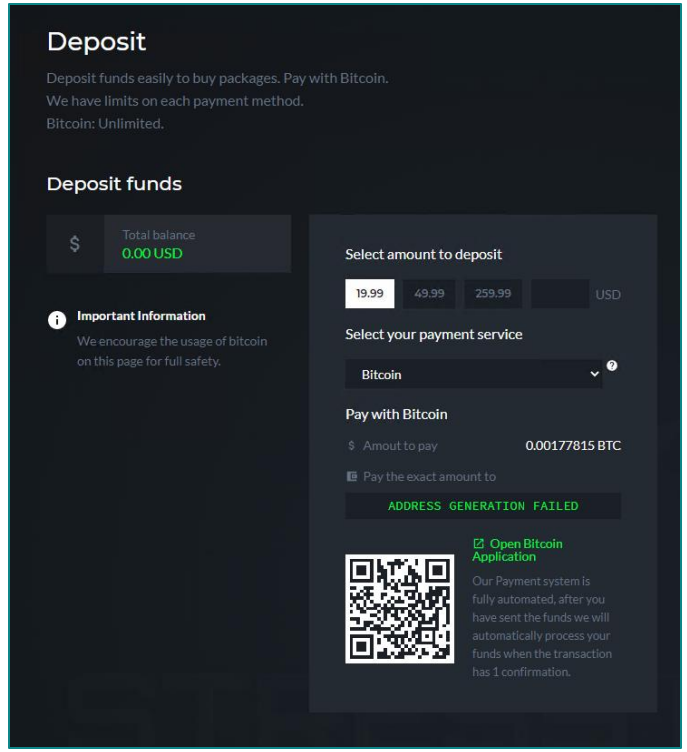
Once you have paid we won't start the attack and you will never hear from us again. Please not that no one will find out that you have complied.

DDoS as a Service



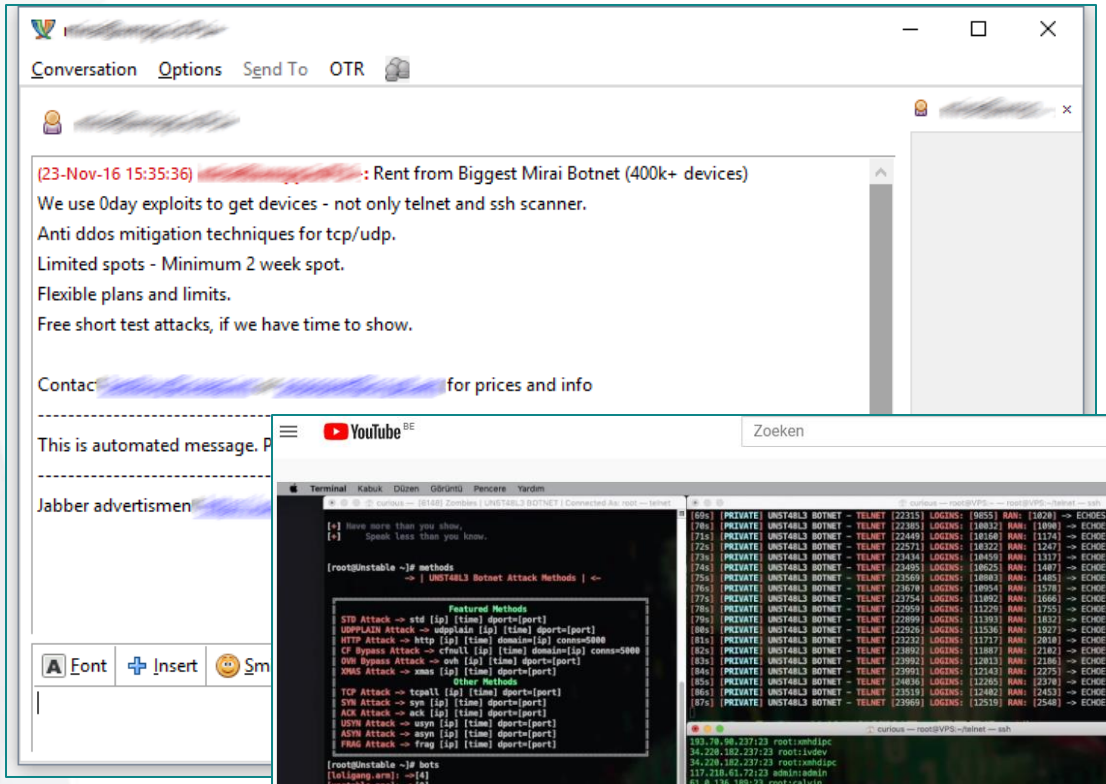




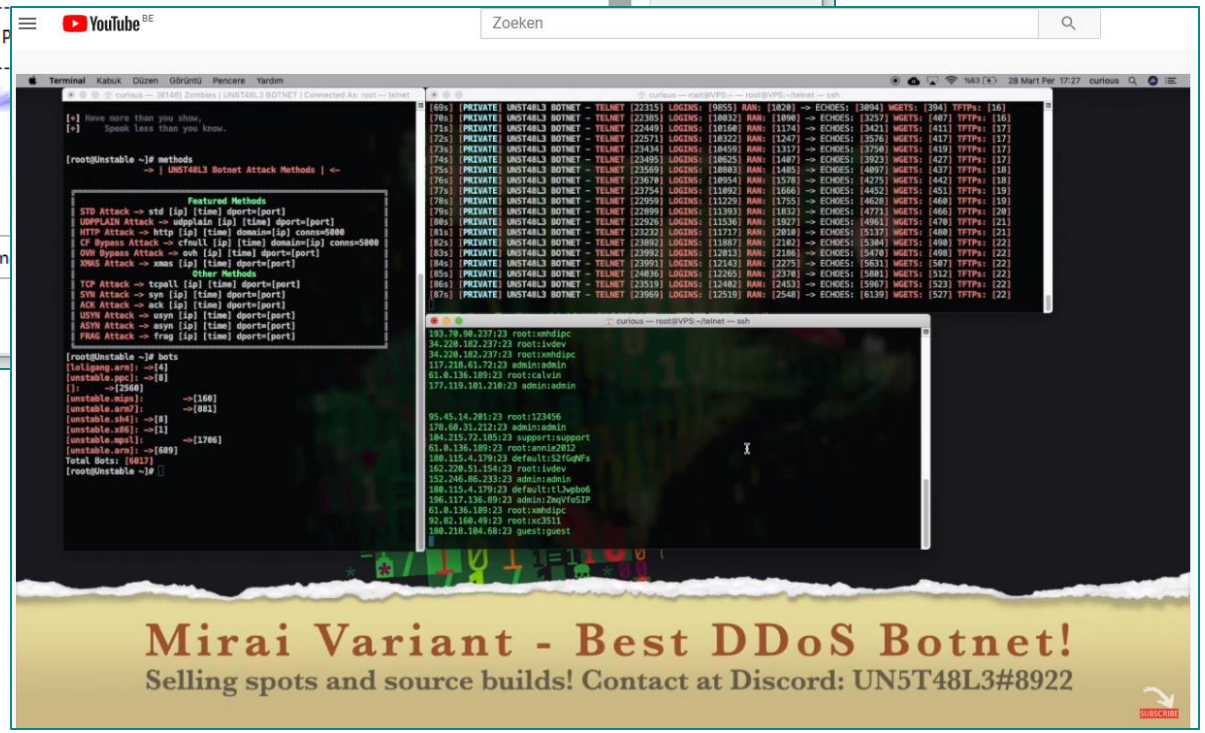


DDoS marketplace

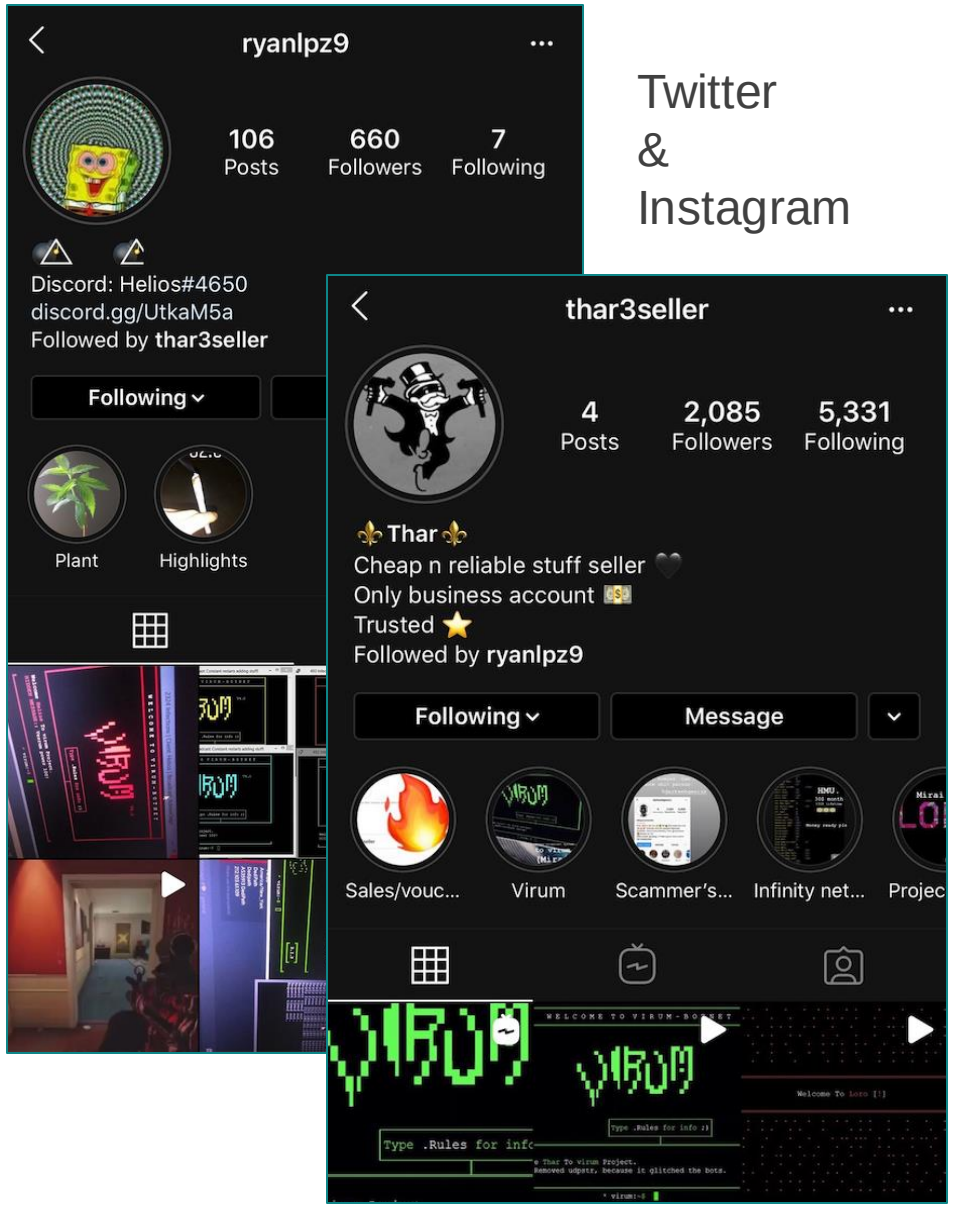
Jabber



Youtube

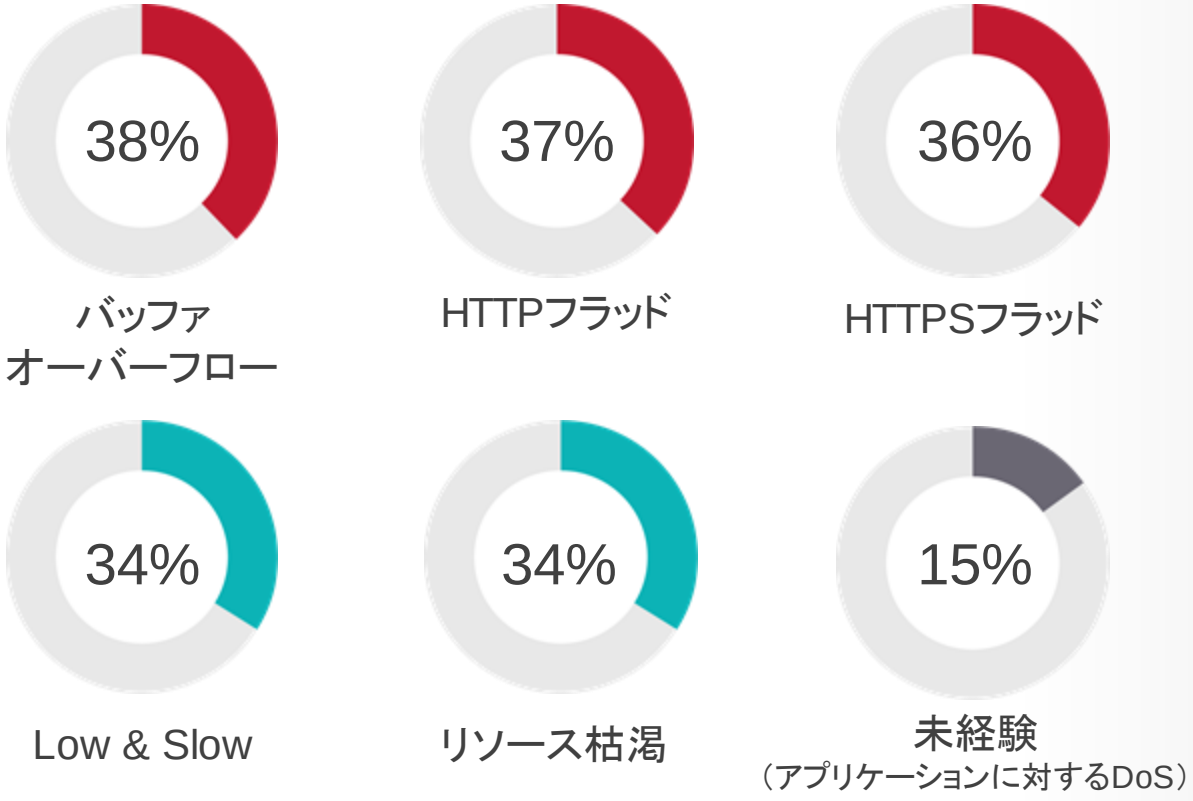


Twitter & Instagram



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



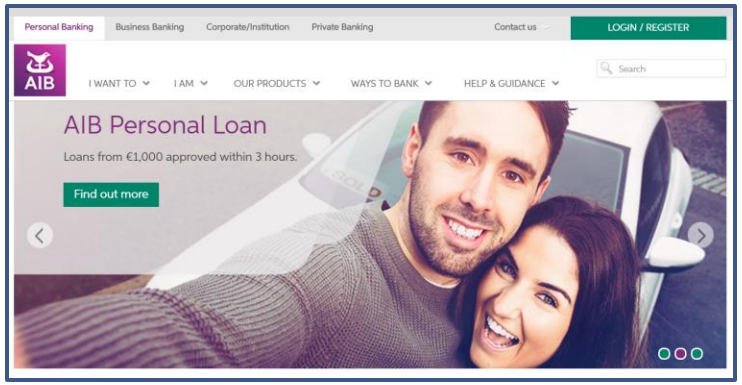
- IoTは大量にHTTP/Sトラフィックを生成
- アプリケーション層DoS攻撃は検知と軽減が困難
- アプリケーションに対する大容量型および非大容量型DoS攻撃の拡大規模は同程度

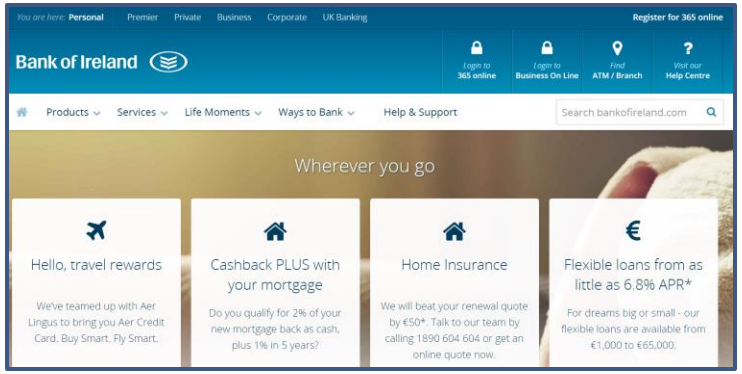
Source: Radware NETWORK AND APPLICATION SECURITY THREAT LANDSCAPE 2018-9

Encrypted DoS(SSL Flood) Attacks

- 10/12-13, 2018 週末 イギリス系銀行への大規模攻撃
- DDoSのメインはSSL Flood Attackで、同時にオンラインサービスへのブルートフォースも行われた
- 結果、全銀行がその週末、サービスダウンを余儀なくされる
- ただし、Radwareを導入していた1つの銀行は攻撃の緩和に成功し、サービスダウンしなかった

Rate-limit, Geo-location, IP Blacklistでは防げない

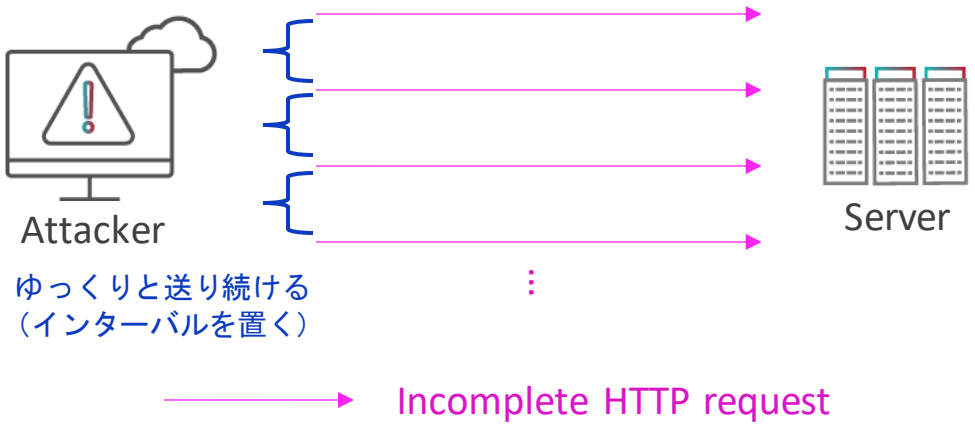




Low and Slow attack（非大容量型攻撃）

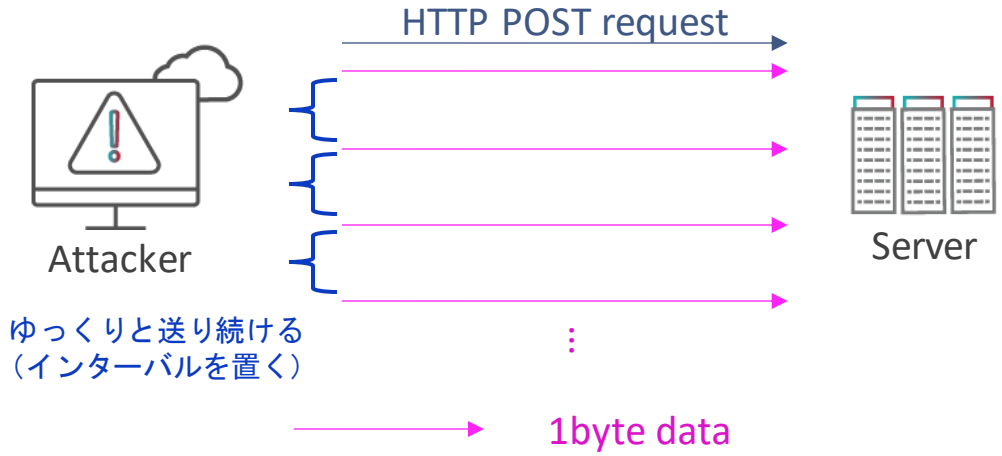
- DoS/DDoSの一種
- Application/ServerのResource枯渇を狙う攻撃
- 帯域幅をほとんど必要としない（非大容量型）のでRate-Limitで防げない
- 省リソースで攻撃を実施することができる

不完全なHTTPヘッダを時間をかけて流し続けて、
Server resourceを消費し続ける



Slowloris

少量データを時間をかけてPOSTし続けて、
Server resourceを消費し続ける



R.U.D.Y(R-U-DEAD-YET?)

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

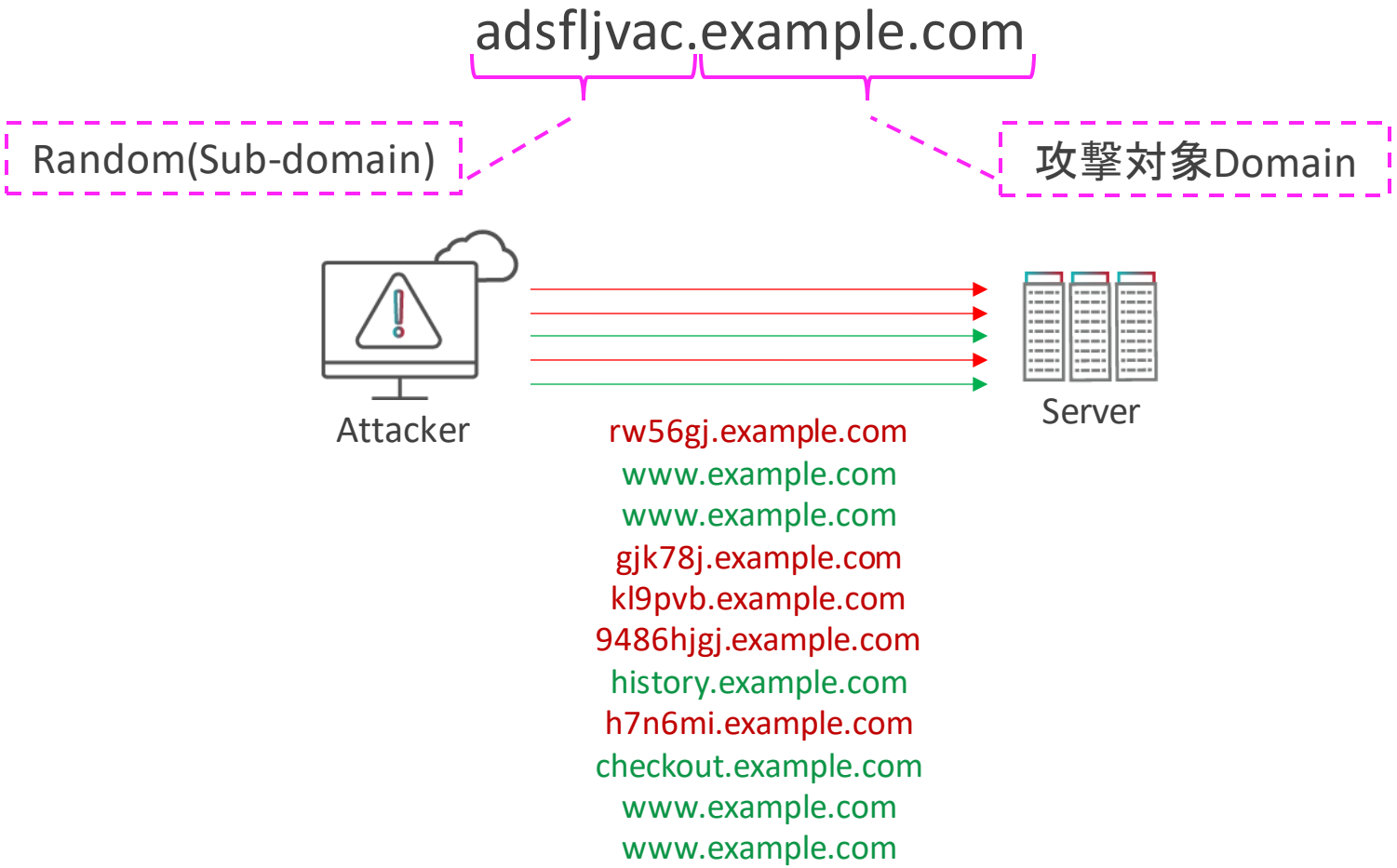
October 2016: Dyn DNS US東部リージョンがMirai botnetにより攻撃を受け、被害がTwitter, Amazon, Tumblr, Reddit, Spotify, Netflix等のサービスを数時間アクセス不可状態に

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

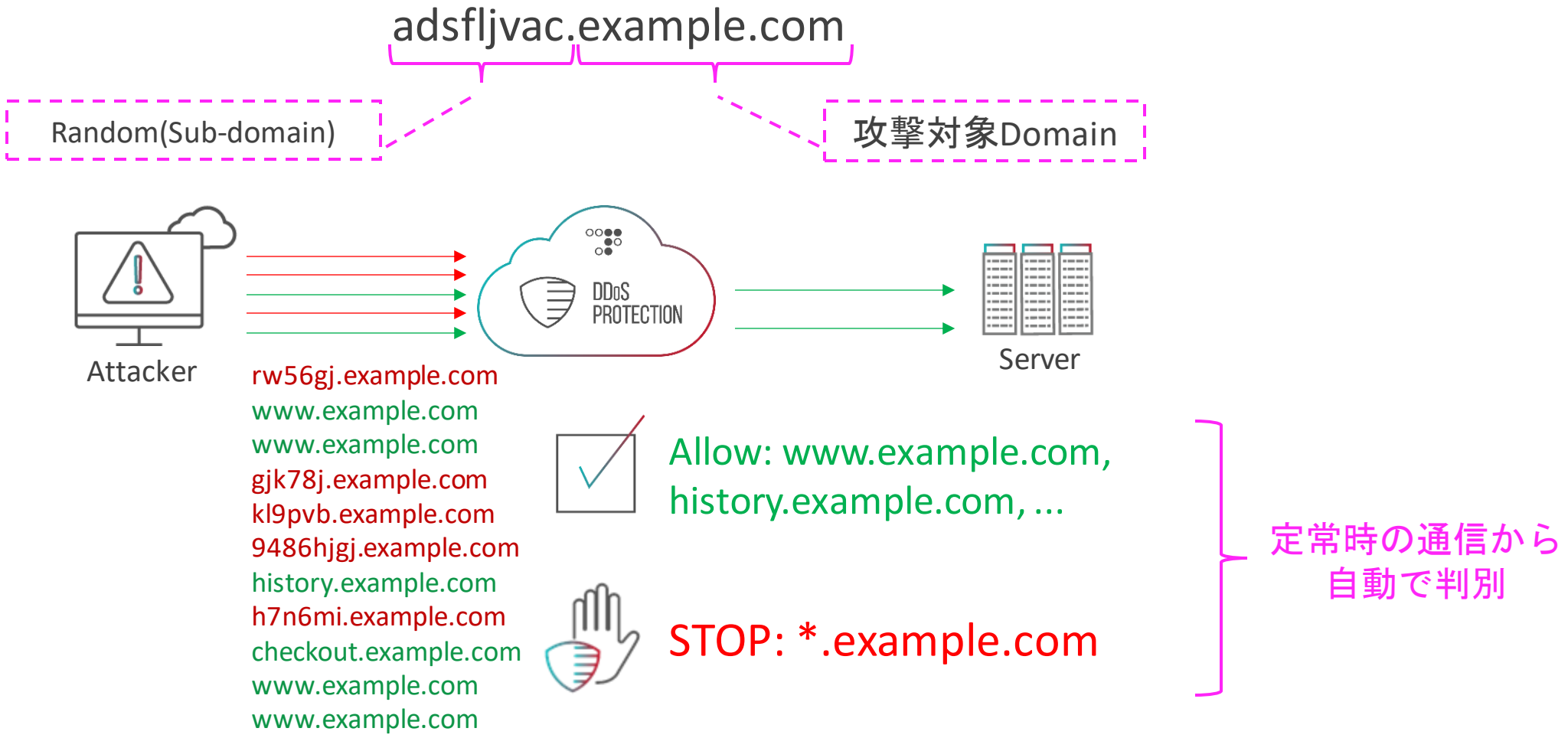
DNS Random Sub-domain attack

- DoS/DDoSの一種
- DNS QueryをRandomに生成、大量のクエリを発生させDNS ServerのResource枯渇を狙う攻撃



DNS Random Sub-domain attack

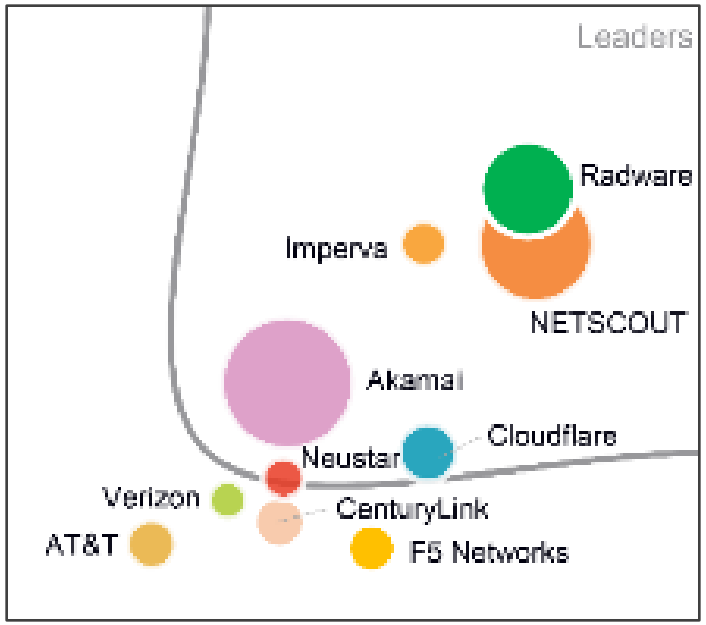
- DoS/DDoSの一種
- DNS QueryをRandomに生成、大量のクエリを発生させDNS ServerのResource枯渇を狙う攻撃



Radware DDoS Solutions

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 Flood対応
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

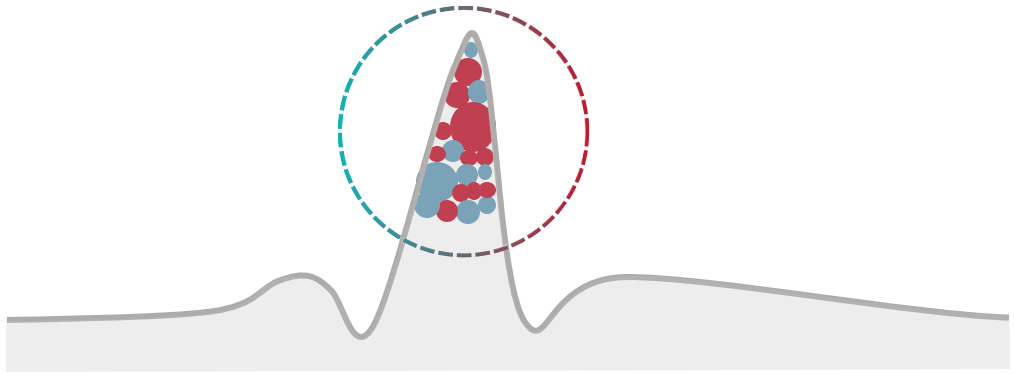
Appliance
Physical/Virtual

Managed Service
Emergency Response Team

Behavioral-Based Detection

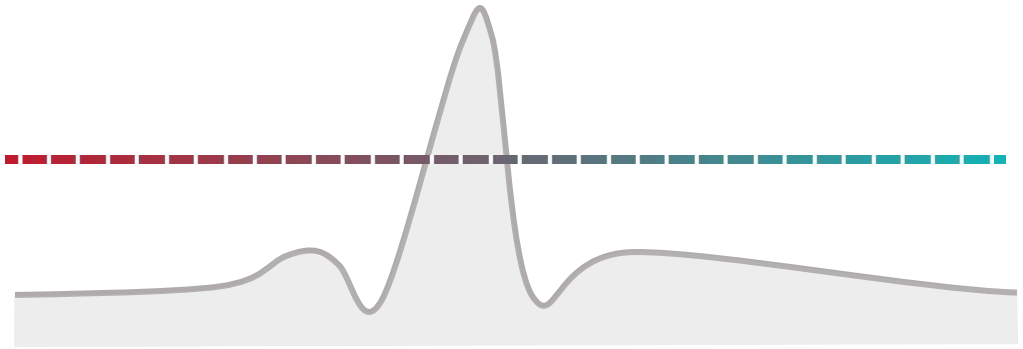
Radware

振る舞い検知



Non-Radware

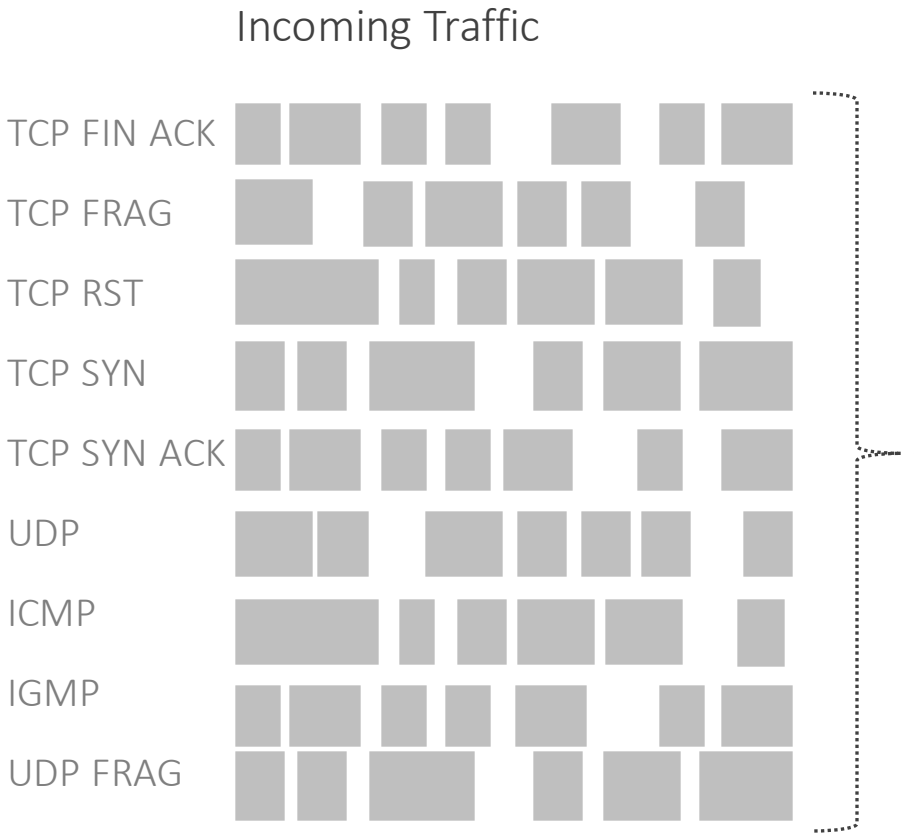
単純なレートリミット



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

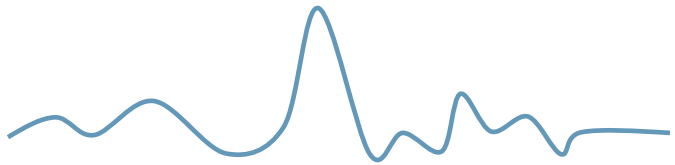
Behavioral-Based Detection



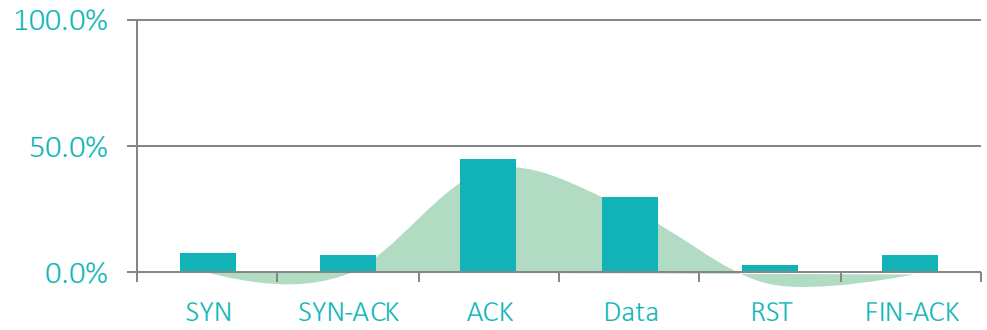
統計+比較

異常を検知

Rate Analysis(PPS)

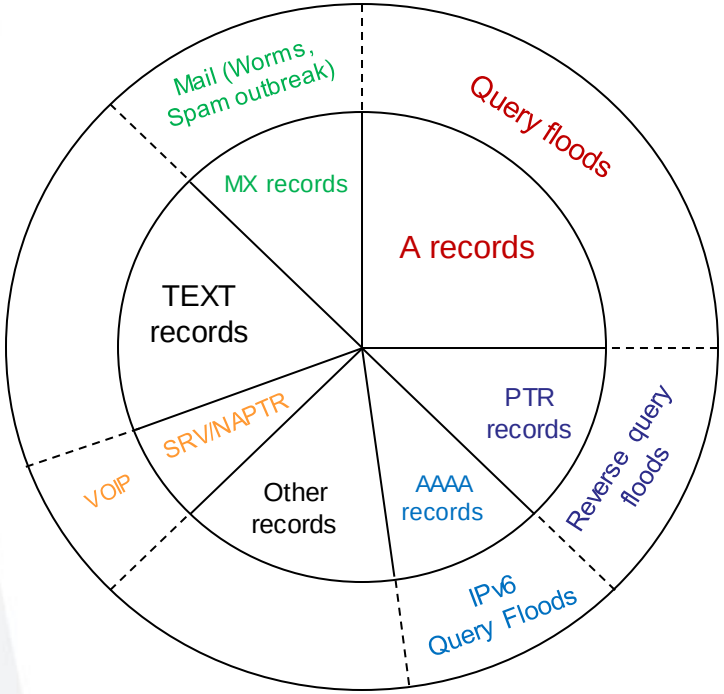


TCP Flag Distribution Analysis

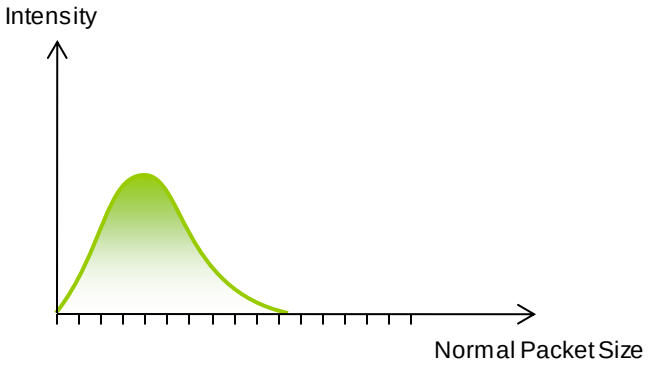


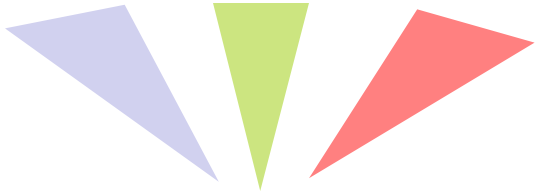
Behavioral-Based Detection

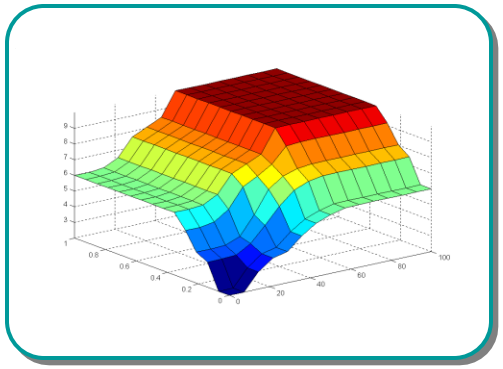
DNS Query Distribution Analysis



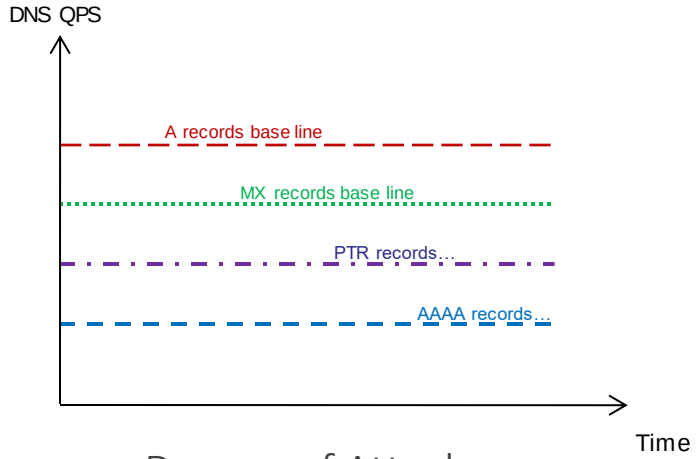
Packet Size Distribution Analysis



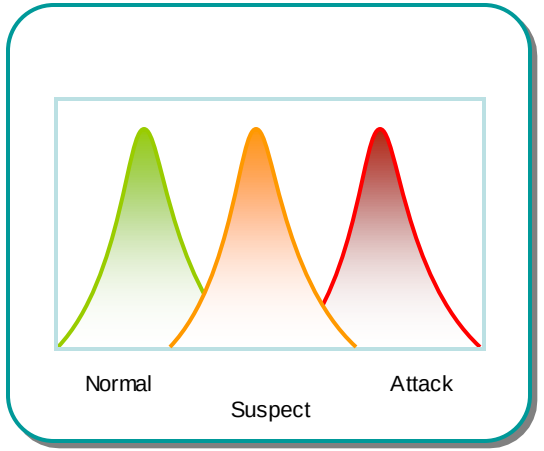




Rate Analysis(QPS)



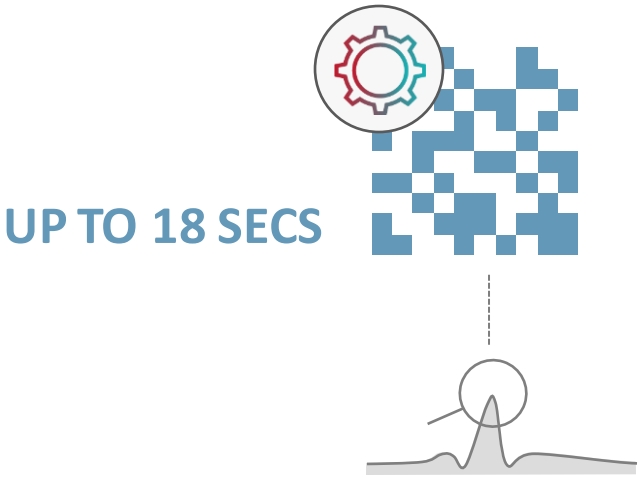
Degree of Attack per DNS Query Type



Zero-Day Detection and Quick Mitigation

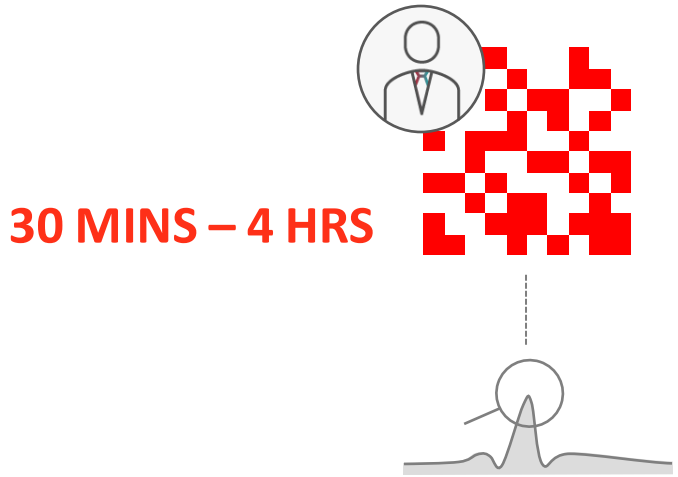
Radware

リアルタイムSignature自動生成



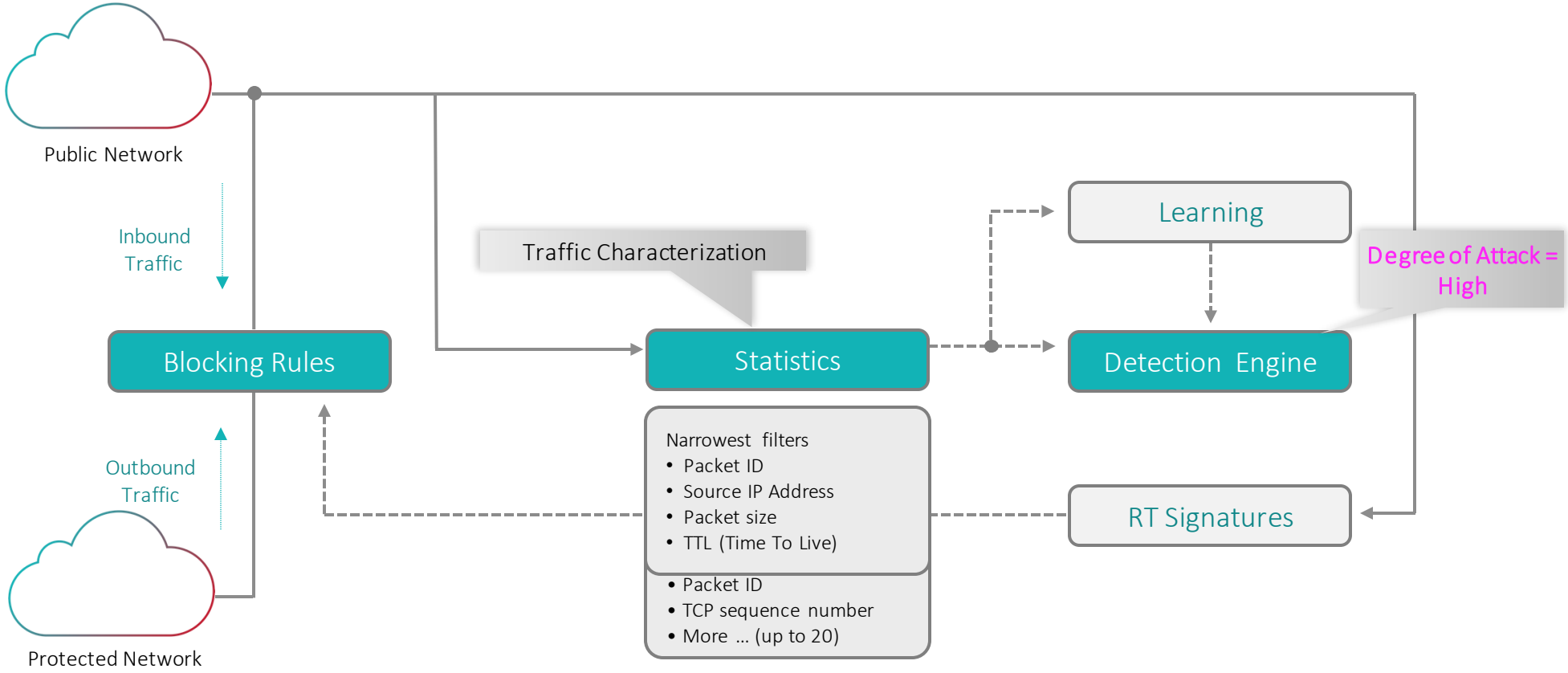
Non-Radware

マニュアルSignature作成



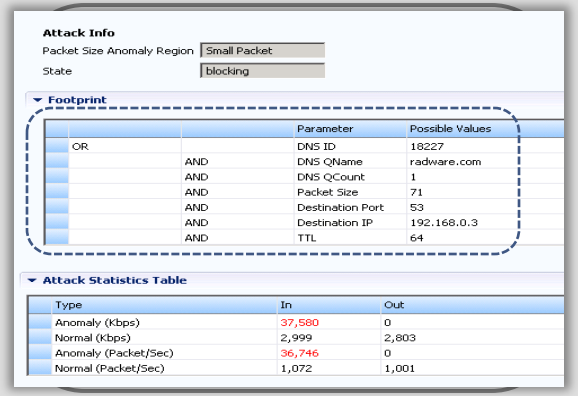
リアルタイムにSignatureを自動生成し適用、調整（SourceIP以外にも複数のパラメータを利用）
ゼロデイ攻撃に秒単位で対応可能

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

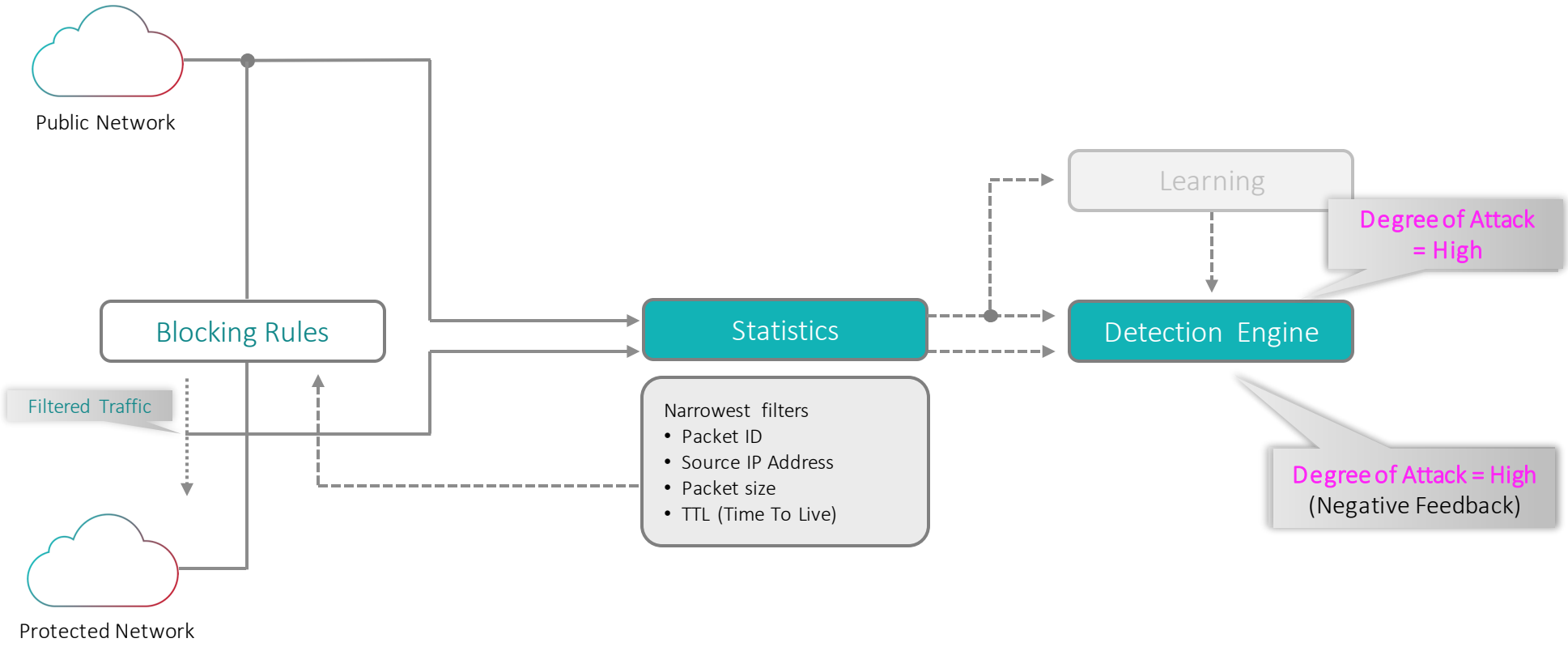
		Parameter	Possible Values
OR		DNS ID	18227
	AND	DNS QName	radware.com
	AND	DNS QCount	1
	AND	Packet Size	71
	AND	Destination Port	53
	AND	Destination IP	192.168.0.3
	AND	TTL	64

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



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

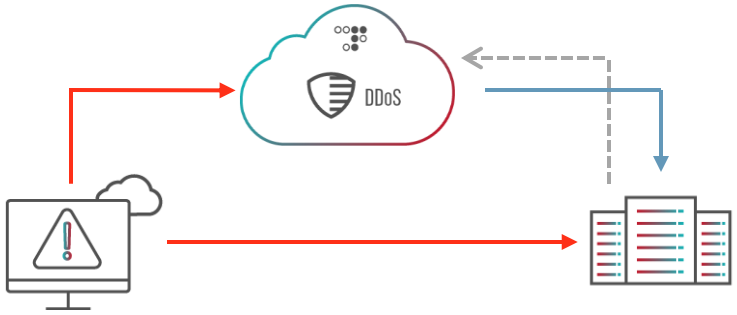
Global Cloud Security Network

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

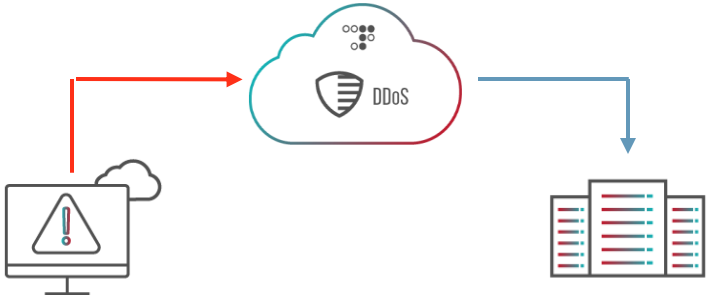
業界最大規模のバックボーン（DDoS/WAF）

Cloud DDoS Service Deployment Modes

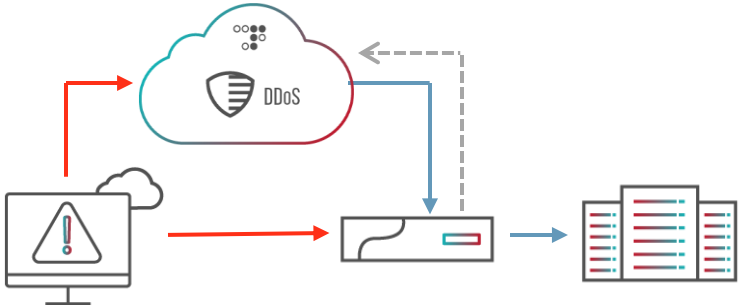
On-Demand



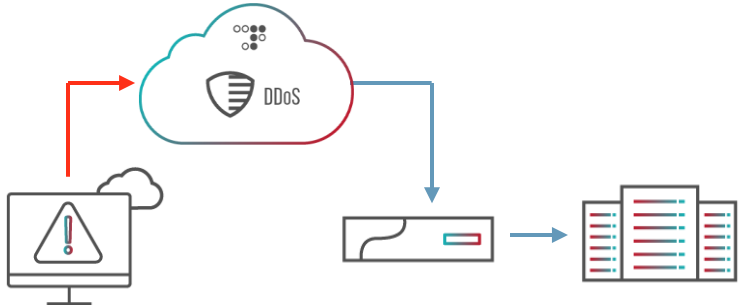
Always-On



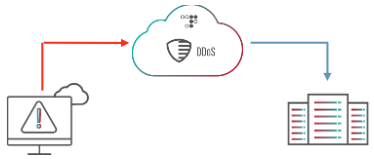
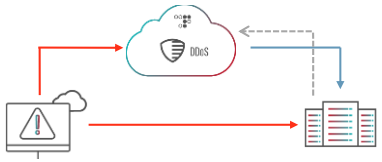
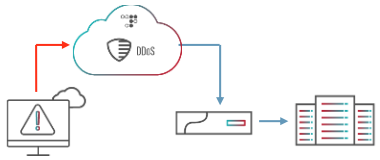
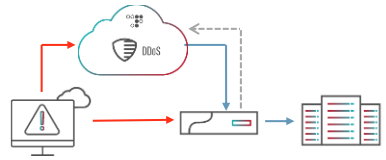
Hybrid On-Demand



Hybrid Always-On



Cloud DDoS Service Deployment Modes

	Always-on		On-demand		Hybrid Always-on		Hybrid On-demand	
通信切り替え方式	DNS	BGP	DNS	BGP	DNS	BGP	DNS	BGP
検知可能攻撃種別	大容量型＋非大容量型		大容量型のみ		大容量型＋非大容量型		大容量型＋非大容量型	
Cloudを経由する通信（検査する通信）	双方向	Inboundのみ	双方向	Inboundのみ	双方向	Inboundのみ	双方向	Inboundのみ
DNS Flood Attack	対応	対応	対応	対応	対応	対応	対応	対応
Random Subdomain Attack	対応	対応[1]	対応[2]	対応[2]	対応[3]	対応[4]	対応[4]	対応[4]
遅延	有		無		有		無	
切り替え制限（標準付与、追加可能）	NA		12回（年間）1回あたり最長48時間		NA		12回（年間）1回あたり最長48時間	
切り替え開始までの時間（SLA）	NA		自動：1分 マニュアル：15分		NA		自動：1分 マニュアル：15分	
マネージドサービス種別（標準付与、変更可能）	ERT Premium		ERT Standard		ERT Premium		ERT Standard	

1 ホワイトリストの提供が必要
2 ホワイトリストの提供が必要（非大容量型攻撃に注意）
3 クラウド/オンプレミスどちらも対応
4 クラウド対応（要ホワイトリスト提供）orオンプレミス対応

Emergency Response Team(ERT)

ERT Standard

全てのCloud DDoS Serviceに付帯

Email / 電話 対応

24/7/365稼働

オンボードサポート

ERT Premium

Always-onに付帯、On-demandは要追加費用

専任サクセスマネジャー

Forensic/Analysis 提供

Caseの優先対応

“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

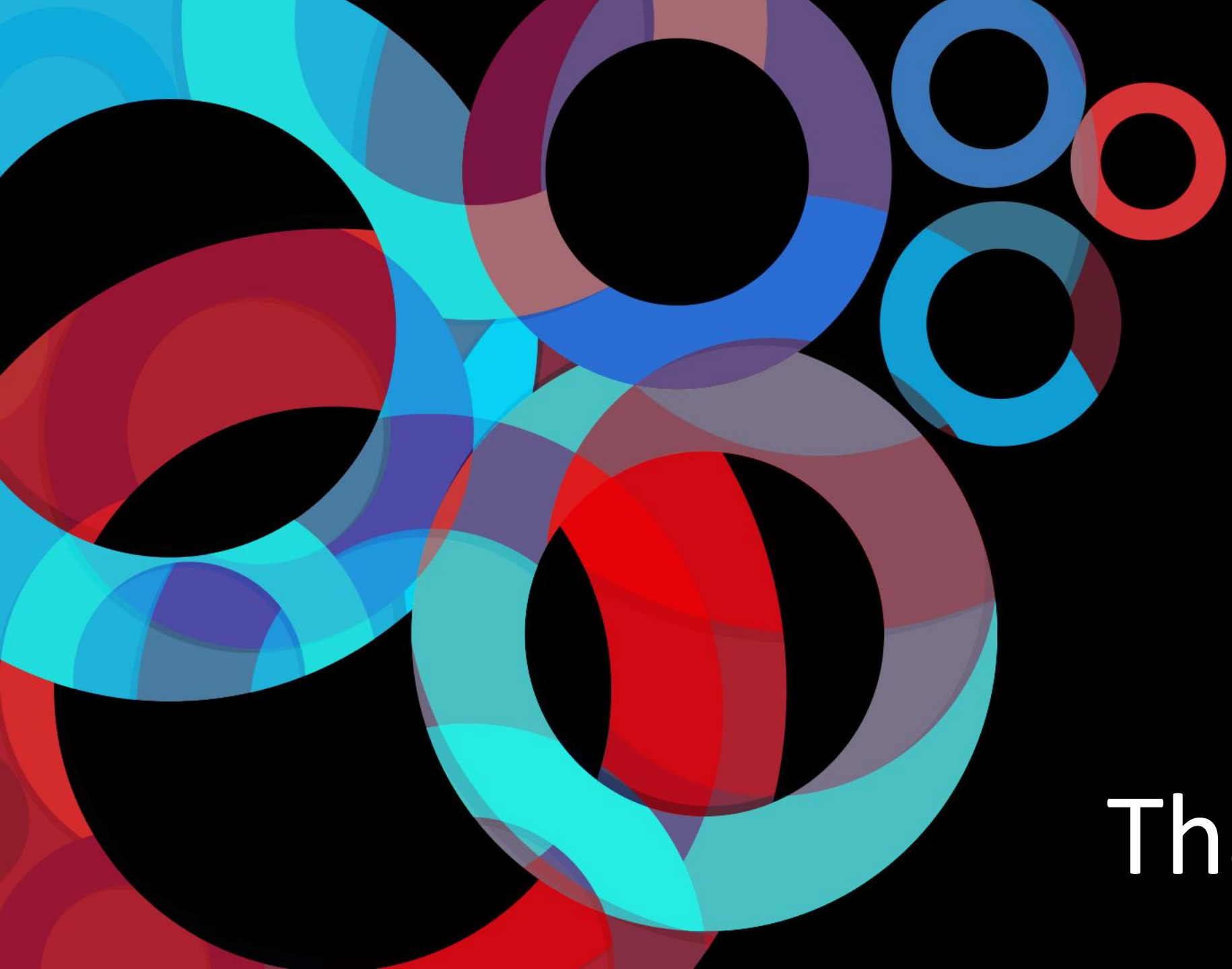
Consistency of Mitigation
緩和の一貫性

Service Availability
サービス可用性

Time to Detect SLAはRadwareの特徴

Summary

- About Radware
- Trend – Ransome DDoS
- Radware DDoS Solutions
- Emergency Response Team(ERT)



radware

Thank you