Lead Initiative 2019 (2019/10/23)

最近のサイバー攻撃動向

根岸 征史 (@MasafumiNegishi)

IIJグループの CSIRT 所属 (IIJ-SECT, 2001年結成)

https://sect.iij.ad.jp/

SANS JAPAN 公式インストラクター (2007年〜)
OWASP Japan アドバイザリーボード (2012年〜)
WASForum Hardening Project 実行委員 (2012年〜)
CODE BLUE レビューボード (2015年〜)
ポッドキャスト「セキュリティのアレ」 (2017年〜)

IIJ-SECT
IIJ Group Security Coordination Team

IIJ
Internet Initiative Japan

- HOME
- IIJ-SECTについて
- IIJセキュリティ情報統括室について
- MITFについて
- Security Diary
- リンク
  - IIJ
  - Internet Infrastructure Review (定期発行技術レポート)
- お問い合わせ
- 個人情報保護ポリシー
- Twitter @IIJSECT
- RSS

Security Diary

HOME > Security Diary > Wikipedia, Twitch, Blizzard への DDoS 攻撃

Diary | 2019年09月17日 Masafumi Negishi |

Wikipedia, Twitch, Blizzard への DDoS 攻撃

今月 9/7 から 9/9 にかけて、Wikipedia, Twitch, Blizzard の各サーバに対して連続
発生しました。この一連の攻撃は Mirai 亜種によるボットネットによって引き起こされたこ
よりわかりました。本記事では IIJ のマルウェア活動観測プロジェクト MITF のハニーポッ
ら、この攻撃で利用されたボットネットの特徴と DDoS 攻撃の発生状況について紹介しま

DDoS 攻撃の概要

一連の攻撃は日本時間の 9/7 2:40 頃から始まり、最初に被害を受けたのは Wikipe
後、攻撃対象は Twitch から Blizzard へと変わりました。

- Malicious attack on Wikipedia—What we know, and what we're doing – W
  Foundation
- Recent DDoS Attacks Impacting Game Service - Community / General Di
  World of Warcraft Forums

各サイトへの攻撃発生時刻はおよそ以下のとおりです。Twitch と Blizzard に対しては
続的に攻撃が発生しています。IIJ では該当時間帯のボットネットの活動を監視しており
データは C2 サーバからの攻撃指令の内容に基づいています。

サイト	攻撃時刻 (日本時間)	主な攻撃対象アドレス
Wikipedia	9/7 2:40 - 12:00頃	91.198.174.192, 208.80.1 208.80.154.224

カテゴリー
- 脆弱性 (15)
- セキュリティ事件 (33)
- 技術解説 (8)

https://sect.iij.ad.jp/

https://wizsafe.iij.ad.jp/

安全をあたりまえに wizSafe by IIJ

wizSafe Security Signal

安心・安全への道標

HOME | お知らせ | 観測レポート | 注意喚起

English | RSS

タグ Exploit Kit

2019.10.01 観測レポート

Servers.comを狙ったDDoS攻撃の観測

執筆者：セキュリティオペレーションセンター 守田 瞬

はじめに 2019年8月18日から8月20日において、ホスティングサービスを提供しているServers.comに対してDDoS攻撃があったことが公表されました[1]。本攻撃ではUDPを用いたDDoS攻…

Read More >

2019.09.30 観測レポート

wizSafe Security Signal 2019年8月 観測レポート

サイト内を検索

関連サイト
- セキュリティブランド「wizSafe（ウィズセーフ）」
- IIJ SECTブログ

新着記事
- Servers.comを狙ったDDoS攻撃の観測
- wizSafe Security Signal 2019年8月 観測レポート
- wizSafe Security Signal 2019年7月 観測レポート

技術レポート「Internet Infrastructure Review（IIR）」

RSS

「Internet Infrastructure Review」は、インターネットの基盤技術に関する最新の技術動向や、セキュリティ情報を積極的に発信する季刊の技術レポートです。IIJがインシデント観測の仕組みで収集した各種攻撃の傾向と対策に関する情報や、インターネットバックボーンの運用を通して蓄積した技術的知見を掲載しています。
冊子の定期的な発送をご希望の方は、下記よりお申し込みください。

* Internet Infrastructure Review（IIR）は、IIJ.news(IIJグループ広報誌)との同梱でお届けします。

> IIJ.news、IIRの送付をご希望の方はこちらから

2019年

> Vol.44 (2019年9月26日)

IIJの技術
> 研究開発お知らせ
> IIJ Technical Seminar
> セキュリティ・技術レポート
– 技術レポート「Internet Infrastructure Review（IIR）」
– IIJ-SECT ブログ
– WizSafe Security Signal
> エンジニア講演・寄稿情報
> 会場提供

https://www.iij.ad.jp/dev/report/iir/

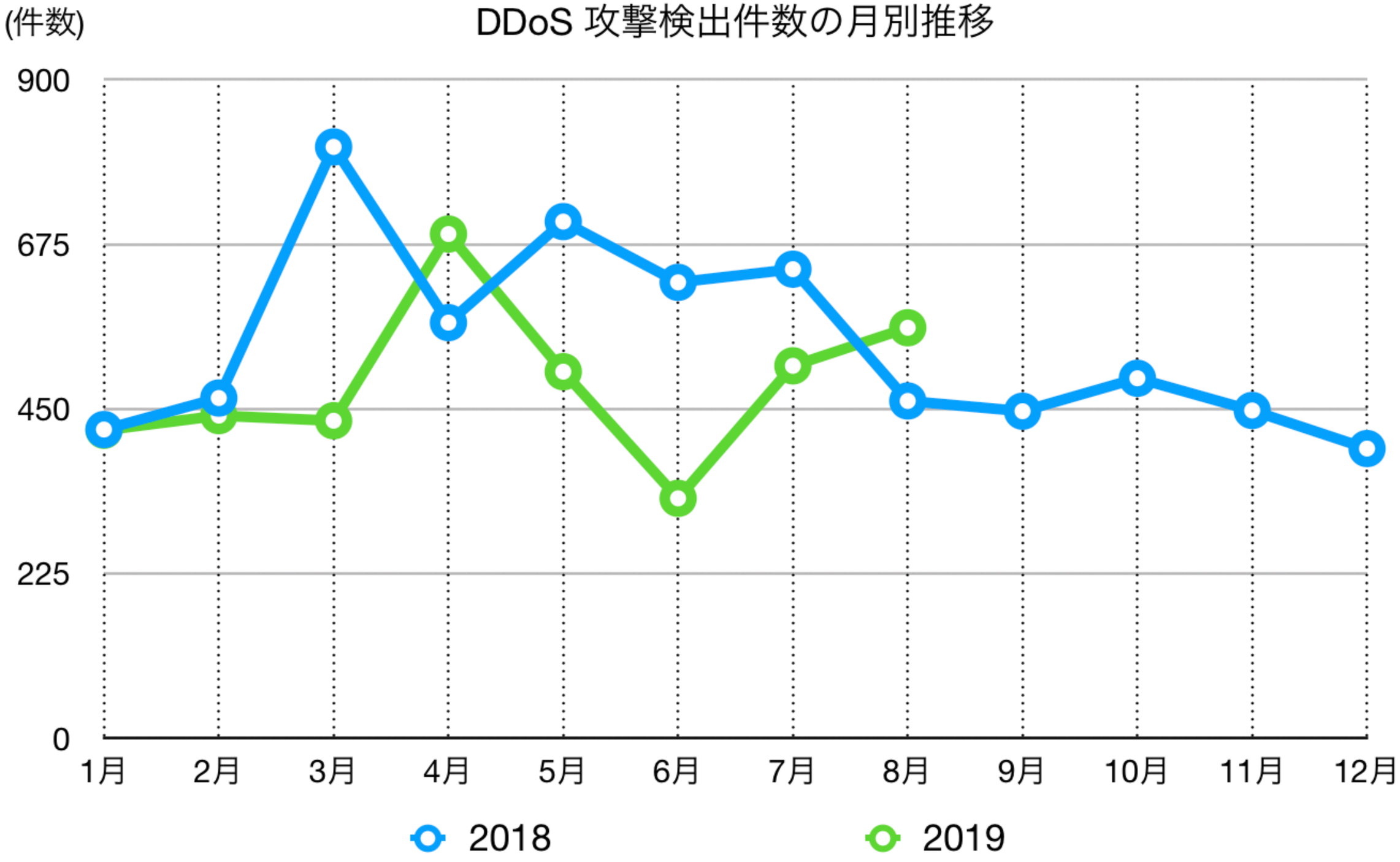
本日のトピック

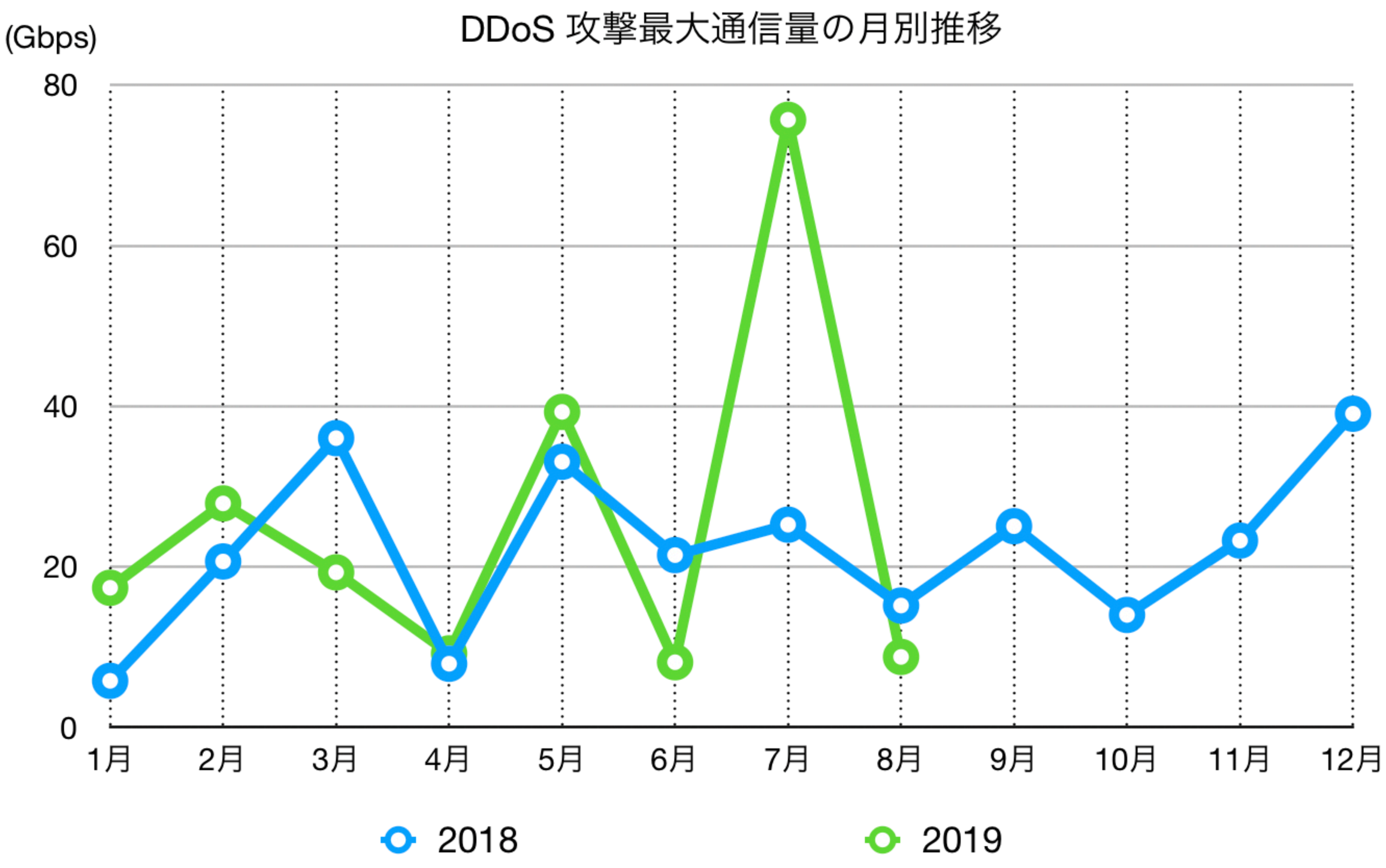
DDoS 攻撃

標的型ランサムウェア

DDoS 攻撃の最近の傾向

- カジュアル化 ← Booter / Stresser サービス、SNS
- 攻撃手段の多様化 ← 攻撃インフラの整備
- 攻撃件数、攻撃規模、ともに横ばい ← 観測情報


(件数)
DDoS 攻撃検出件数の月別推移
900
675
450
225
0
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
2018
2019


DDoS 攻撃最大通信量の月別推移
(Gbps)
80
60
40
20
0
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
2018
2019

DDoS 攻撃の目的、動機

- ハクティビズム (政治的あるいは社会的な主義や主張)
  少数の確信犯による執拗な攻撃 (⇔ 多数の匿名参加者による攻撃)
  政治、外交、スポーツイベント
  日本および周辺諸国における活動
  - 歴史的特異日 (9/18 など)
  - 反捕鯨、小型クジラ漁反対 (#OpKillingBay 2013年〜)
  - 香港デモ (2019年 6月 Telegram, 2019年 8月 LIHKG)
  - 日韓関係 (2019年 10月)

- 金銭、怨恨、娯楽、ほか

Booter / Stresser (DDoS-as-a-Service, DDoS-for-Hire)

- 誰でも手軽に安く DDoS 攻撃が実施できるサービスの普及

Carpet Bombing (絨毯爆撃)

- 単一の IP アドレスを狙うのではなく、サブネット (CIDR) 単位で攻撃する
- UDP アンプ攻撃や TCP SYN/ACK リフレクション攻撃との併用
- IP アドレス単位での攻撃検知を回避
- 2018年頃から急増

DDoS 攻撃の主な攻撃手法

- UDP アンプ 攻撃
  DNS, NTP, CLDAP, SSDP
  Apple Remote Desktop (3283/udp), WS-Discovery (3702/udp)
- TCP SYN/ACK リフレクション攻撃
  2018年頃から急増, 2019年 8月 Servers.com への攻撃事例 (UDP + TCP)
- IoT ボットネットによる攻撃
  TCP / UDP / HTTP Flood
  多数の小規模ボットネット (数百 IP 程度) と一部の大規模ボットネット (数万 IP 程度)
  2019年 9月 Wikipedia, Twitch, Blizzard への攻撃事例 (moobot)

2019.10.01　**執筆者 ：** セキュリティオペレーションセンター 守田 瞬

Servers.comを狙ったDDoS攻撃の観測

はじめに

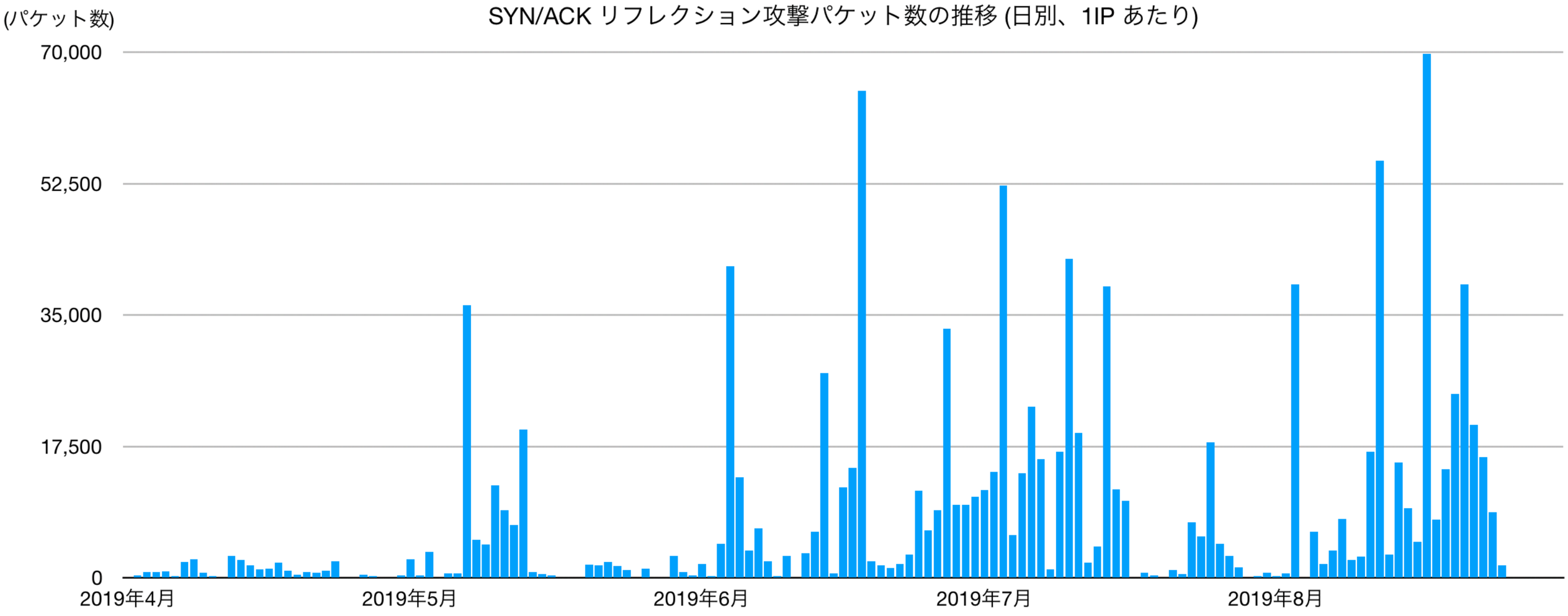
2019年8月18日から8月20日において、ホスティングサービスを提供しているServers.comに対してDDoS攻撃があったことが公表されました[1]。本攻撃ではUDPを用いたDDoS攻撃の他にTCPを利用したSYN/ACK リフレクション攻撃を複合的に利用した攻撃であることが[1]で示されています。

一方で、SOCでは2019年7月の観測レポート[2]に引き続き、2019年8月においてもSYN/ACKリフレクション攻撃と考えられる攻撃を多数観測しています。2019年8月に観測しているSYN/ACKリフレクション攻撃のうち、Servers.comを対象とした攻撃を観測しており、本記事では被害者であるSevers.comの視点で分析された詳細なレポート[1]を元に、攻撃で利用されたリフレクタ側の視点からSYN/ACKリフレクション攻撃を分析した結果を共有します。尚、SYN/ACKリフレクション攻撃の原理についての詳しい説明は、2018年9月の観測レポート[3]をご参照ください。

SYN/ACKリフレクション攻撃は、送信元を攻撃対象に偽装することで実現されます。したがって、今回取り上げる攻撃において、偽装された送信元はServers.comが利用しているIPアドレスになります。偽装された送信元におけるSYNパケットは、実際にはパケットに記録された送信元とは異なる送信元から送信されます。また、そのSYNパケットを受け取ったリフレクタは、偽装された送信元に対して応答としてSYN/ACKパケットを返送します。これはTCPにおけるthree-way handshakeのコネクションを確立する仕組みを悪用した攻撃になります。

https://wizsafe.iij.ad.jp/2019/10/764/

IIJ ハニーポットにおける攻撃観測



Diary | 2019年09月17日 Masafumi Negishi |

Wikipedia, Twitch, Blizzard への DDoS 攻撃

今月 9/7 から 9/9 にかけて、Wikipedia, Twitch, Blizzard の各サーバに対して連続して DDoS 攻撃が発生しました。この一連の攻撃は Mirai 亜種によるボットネットによって引き起こされたことが IIJ の調査によりわかりました。本記事では IIJ のマルウェア活動観測プロジェクト MITF のハニーポットの観測結果から、この攻撃で利用されたボットネットの特徴と DDoS 攻撃の発生状況について紹介します。

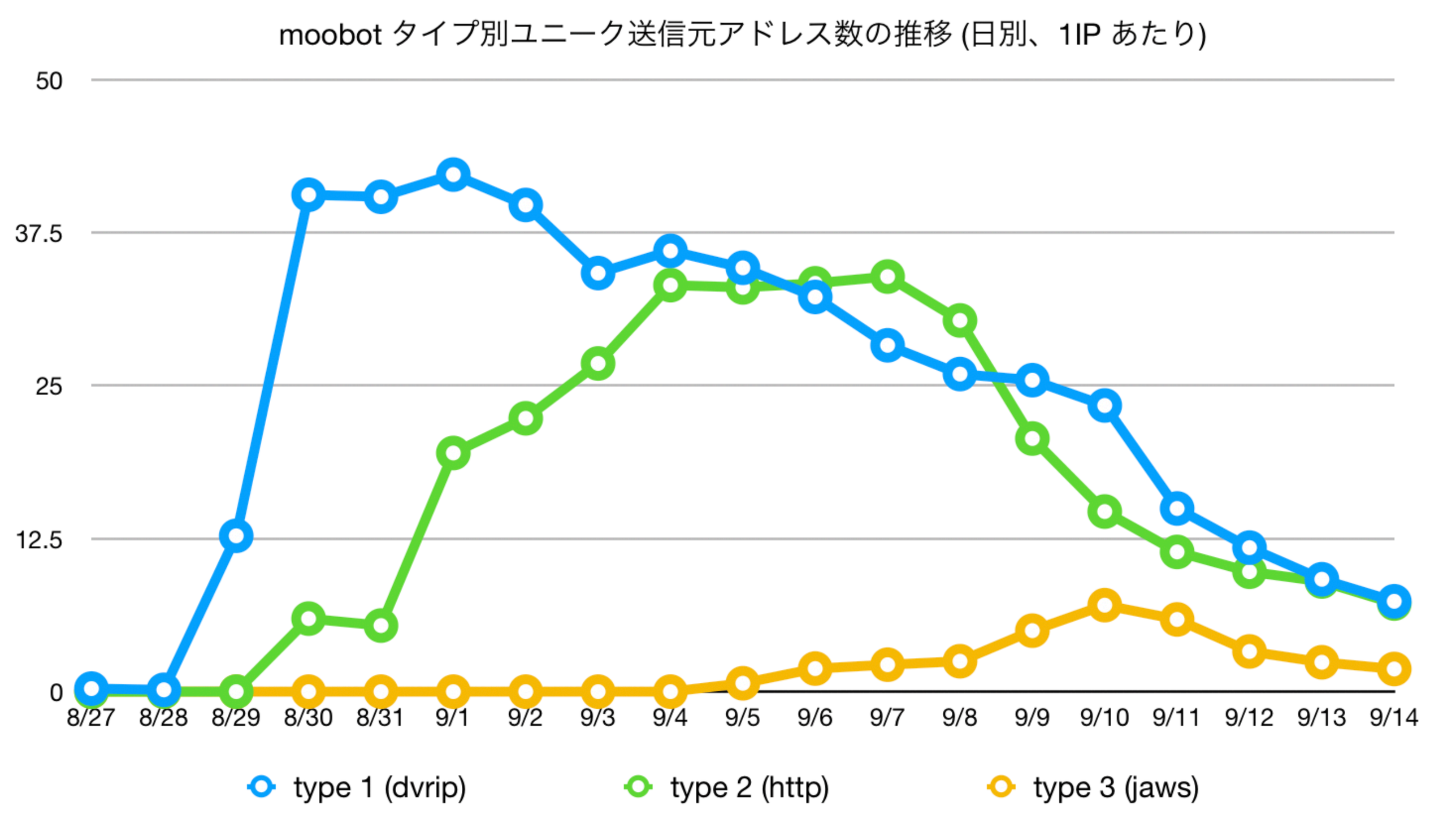
■ DDoS 攻撃の概要

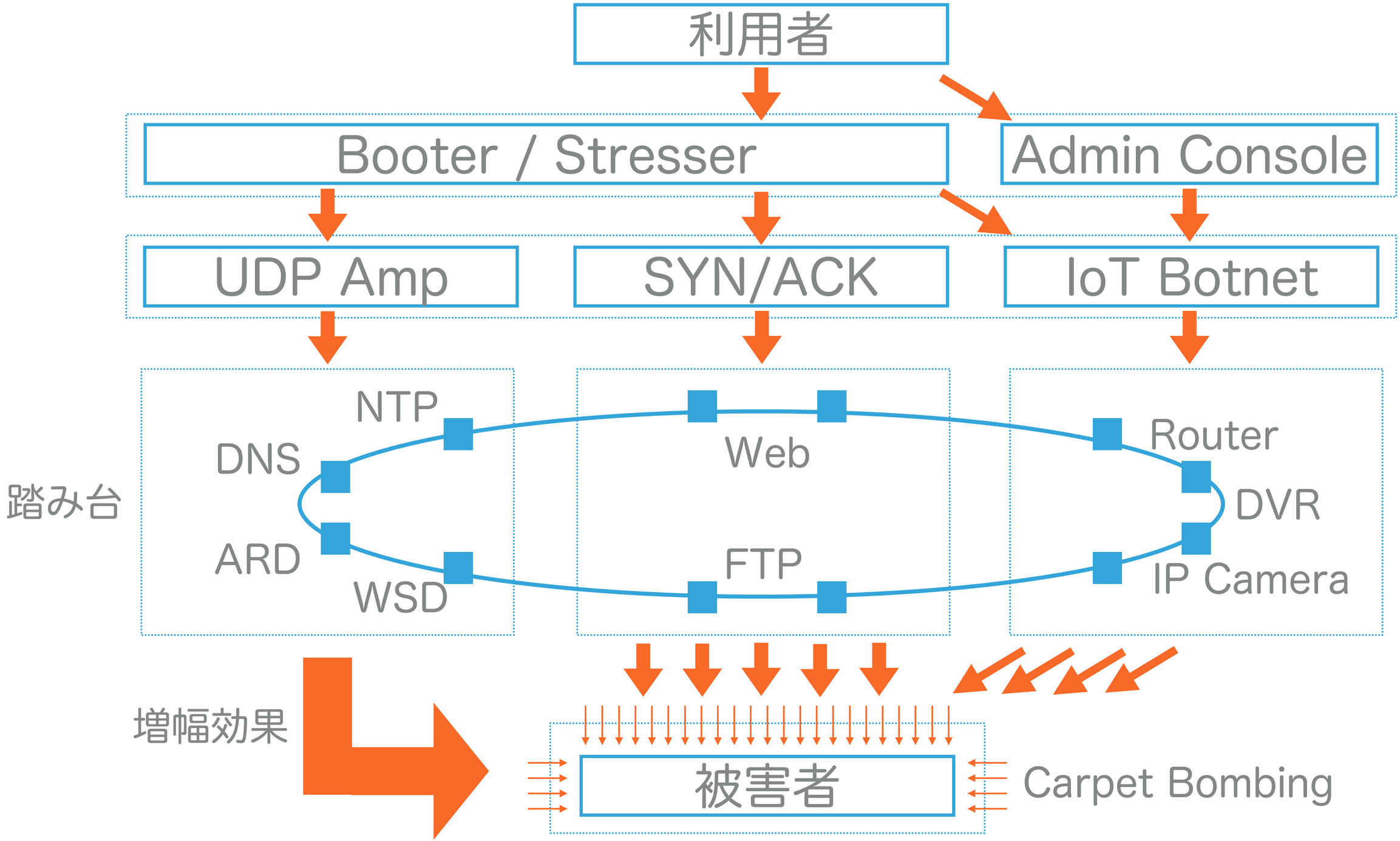
一連の攻撃は日本時間の 9/7 2:40 頃から始まり、最初に被害を受けたのは Wikipedia でした[1]。その後、攻撃対象は Twitch から Blizzard へと変わりました。

- Malicious attack on Wikipedia—What we know, and what we're doing – Wikimedia Foundation
- Recent DDoS Attacks Impacting Game Service - Community / General Discussion - World of Warcraft Forums

各サイトへの攻撃発生時刻はおよそ以下のとおりです。Twitch と Blizzard に対しては 2日間にわたり断続的に攻撃が発生しています。IIJ では該当時間帯のボットネットの活動を監視しており、時刻とアドレスのデータは C2 サーバからの攻撃指令の内容に基づいています。

https://sect.iij.ad.jp/d/2019/09/175257.html


moobot タイプ別ユニーク送信元アドレス数の推移 (日別、1IP あたり)
50
37.5
25
12.5
0
8/27
8/28
8/29
8/30
8/31
9/1
9/2
9/3
9/4
9/5
9/6
9/7
9/8
9/9
9/10
9/11
9/12
9/13
9/14
type 1 (dvrip)
type 2 (http)
type 3 (jaws)


利用者
Booter / Stresser
Admin Console
UDP Amp
SYN/ACK
IoT Botnet
踏み台
NTP
DNS
ARD
WSD
Web
FTP
Router
DVR
IP Camera
増幅効果
被害者
Carpet Bombing

標的型攻撃 + ランサムウェア

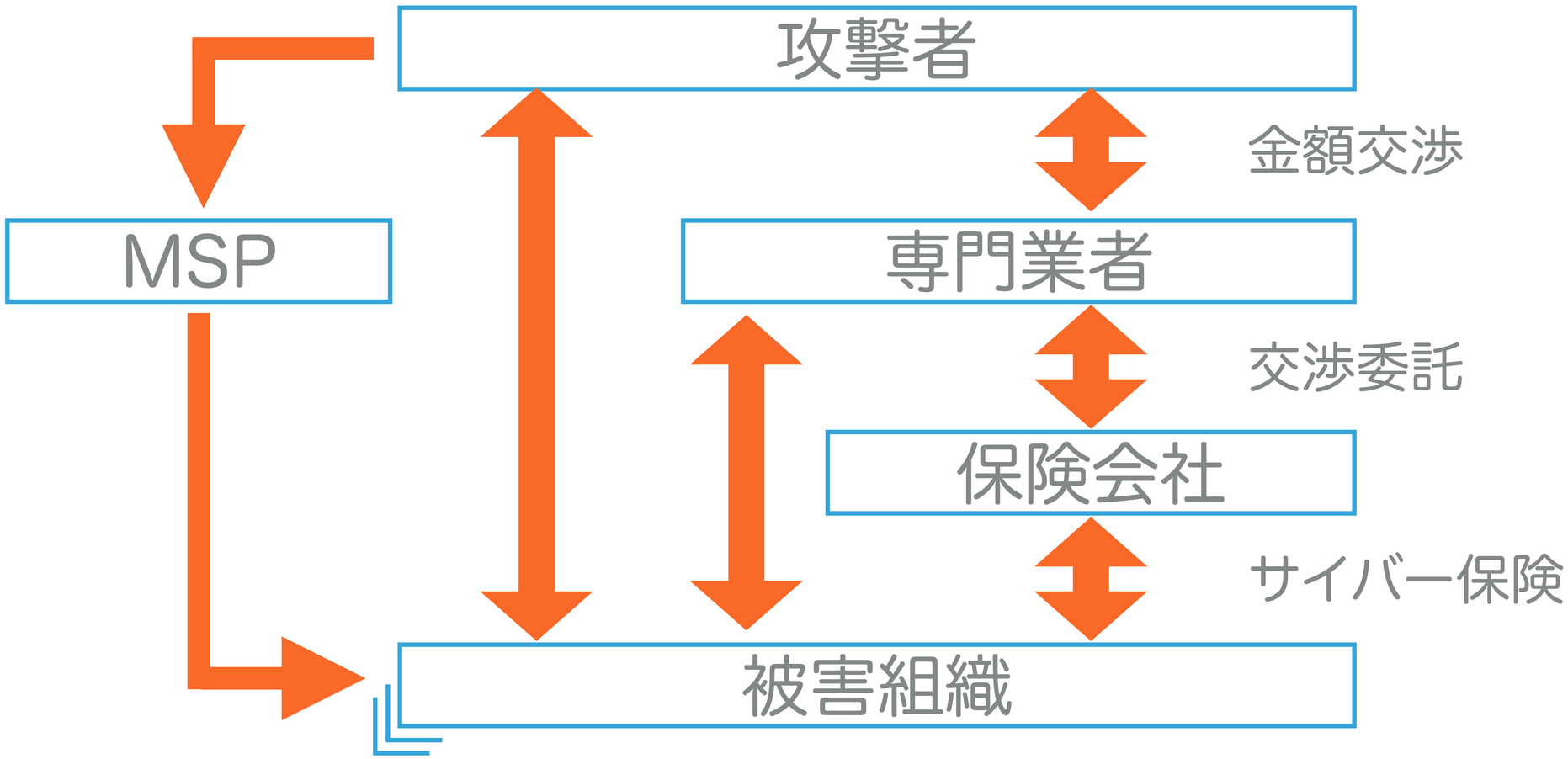
- 侵入からマルウェア感染に至る攻撃手法は標的型攻撃に近い
  → 組織内での横展開の活動もあり
- 長期間に渡る潜伏、調査活動
  → 攻撃に慣れてくると短くなる傾向
- 最後にランサムウェアに一斉に感染させる
- 特定の業種、組織が狙われるケースが多い (病院、地方自治体など)

標的型ランサムウェア

“Opportunistic” Ransomware		“Targeted” Ransomware
不特定多数の個人	攻撃対象	特定企業、業種の組織
スパムメール ドライブバイダウンロード	初期感染	スピアフィッシング RDP による侵入
なし (あるいは自動)	感染拡大	手動による横展開 (潜伏調査期間あり)
低額 (端末単位)	身代金	高額 (組織単位、交渉の余地あり)
Locky, Cerber など	例	Ryuk, Dharma など

時期	被害組織	ランサムウェア	身代金支払い	攻撃の特徴
2017年 6月	NAYANA	Erebus	あり	韓国のホスティングプロバイダー NAYANA で 6/10 に 153台の Linux サーバが Erebus ランサムウェアに感染。3,400〜5,000 の Web サイトに影響。2重のバックアップも含めてすべてのデータが暗号化されており、復旧が困難に。攻撃者は当初 1台あたり 10 BTCを要求。4日間にわたる交渉の結果、トータル 397.6 BTC (13億ウォン相当) で決着。
2018年 1月	Hancock Health	SamSam	あり	RDP から侵入し、バックアップデータを先に破壊。攻撃者は 4 BTC ($55K 相当) を要求。 1/11 感染、1/13 身代金支払い、1/14 復旧
2018年 3月	アトランタ市	SamSam	なし	攻撃者は 6 BTC ($51K 相当) を要求。市は緊急対応として $2.6M 相当のサービスを調達。 (復旧のために $17M 相当の支出が必要との試算)
2019年 3月	ジョージア州 ジャクソン郡	Ryuk	あり	攻撃者と交渉の末、$400K 相当の身代金を支払い。侵入経路は不明だが、攻撃者はシステム内に数週間潜伏していた可能性がある。
2019年 3月	Norsk Hydro	LockerGoga	なし	攻撃者は Active Directory を利用した可能性がある。多数の IT システムが影響を受け停止し、プラント操業は手動操作に切り替えて継続。復旧まで約 3ヶ月、約50〜55億円相当の被害金額を想定。
2019年 5月	ボルチモア市	RobbinHood	なし	攻撃者は 13 BTC ($76K 相当) を要求。復旧に1ヶ月以上。$18M 相当の被害金額を想定。
2019年 5月	フロリダ州 リビエラビーチ	Ryuk	あり	攻撃者は 65 BTC ($600K 相当) を要求。復旧のため、合計 400台の PCを $941K で購入。
2019年 6月	フロリダ州 レイクシティ	Ryuk	あり	攻撃者は 86 BTC を要求、交渉の結果 42 BTC ($460K 相当) を支払い。サイバー保険が適用された。
2019年 8月	テキサス州 22の地域	REvil	なし	攻撃者はトータル $2.5M を要求。MSP (TSM Consulting) 経由で感染した (ConnectWise Control が利用された)。

特異なビジネス構造



対策の考え方

- 侵入経路はメールと RDP が大半を占める
  → マルウェアやフィッシング対策など、基本をしっかりやる
- バックアップ
- 事業継続の観点を忘れずに

(参考情報)

2018年観測レポート振り返り – wizSafe Security Signal -安心・安全への道標- IIJ https://wizsafe.iij.ad.jp/2019/03/601/
Return to Normalcy: False Flags and the Decline of International Hacktivism https://www.recordedfuture.com/international-hacktivism-analysis/
DDoS-as-a-Service: Investigating Booter Websites — University of Twente Research Information https://research.utwente.nl/en/publications/ddos-as-a-service-investigating-booter-websites
NETSCOUT Threat Intelligence Report | NETSCOUT https://www.netscout.com/blog/asert/netscout-threat-intelligence-report
UDP-Based Amplification Attacks | CISA https://www.us-cert.gov/ncas/alerts/TA14-017A
A Call to ARMS: Apple Remote Management Service UDP Reflection/Amplification DDoS Attacks | NETSCOUT https://www.netscout.com/blog/asert/call-arms-apple-remote-management-service-udp
New DDoS Attack-Vector via WS-Discovery/SOAPoverUDP, Port 3702 https://zero.bs/new-ddos-attack-vector-via-ws-discoverysoapoverudp-port-3702.html
Anatomy of a SYN-ACK attack - Akamai Security Intelligence and Threat Research Blog https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html
Root cause analysis and incident report on the August DDoS attack https://www.prnewswire.com/news-releases/root-cause-analysis-and-incident-report-on-the-august-ddos-attack-300905405.html
The Botnet Cluster on the 185.244.25.0/24 https://blog.netlab.360.com/the-botnet-cluster-on-185-244-25-0-24-en/

2019 年ランサムウェア最新動向 | トレンドマイクロ https://resources.trendmicro.com/jp-docdownload-form-m129-web-2019-ransomware.html
Early Findings: Review of State and Local Government Ransomware Attacks https://www.recordedfuture.com/state-local-government-ransomware-attacks/
Research Report Examines Ransomware Negotiations and Response https://go.flashpoint-intel.com/forrester/forrester-guide-to-paying-ransomware
Targeted Ransomware: Proliferating Menace Threatens Organizations | Symantec Blogs https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat
Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread
The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks — ProPublica https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks