



インシデントレスポンスに求められる 脅威のモニタリングと標的型攻撃の可視化の必要性

アーバーネットワークス株式会社
シニアシステムズエンジニア
藤原 哲士

目次

1. アーバーネットワークスの紹介
2. サイバー攻撃の増加と標的型攻撃の特徴・対策
3. インシデントレスポンスに求められるもの
4. 「事象分析」へのアプローチ
- Arbor Spectrumを用いたオペレーションイメージ

1. アーバーネットワークスの紹介



3

アーバーネットワークスとは

本社所在地：米国マサチューセッツ州バーリントン

- 主要海外拠点：ロンドン、シンガポール、東京

沿革

- 2000年 米国マサチューセッツ州バーリントンで設立
- 2005年1月 1st ワールドワイド・インフラストラクチャ・セキュリティ レポート発表
- 2013年9月 Packetloopを買収

事業内容

- キャリア・ネットワーク、データセンター、エンタープライズ向け、ネットワーク・セキュリティ/マネージメント・ソリューションの提供

主な製品 / ソリューション

- Arbor SP/TMS (サービス・プロバイダ向けDDoS対策ソリューション)
- Arbor APS (Availability Protection System: エンタープライズ向けDDoS対策ソリューション)
- Arbor Spectrum (エンタープライズ向け内部脅威検知、セキュリティインシデント分析ソリューション)
- Arbor Cloud (クラウド型DDoS対策ソリューション)

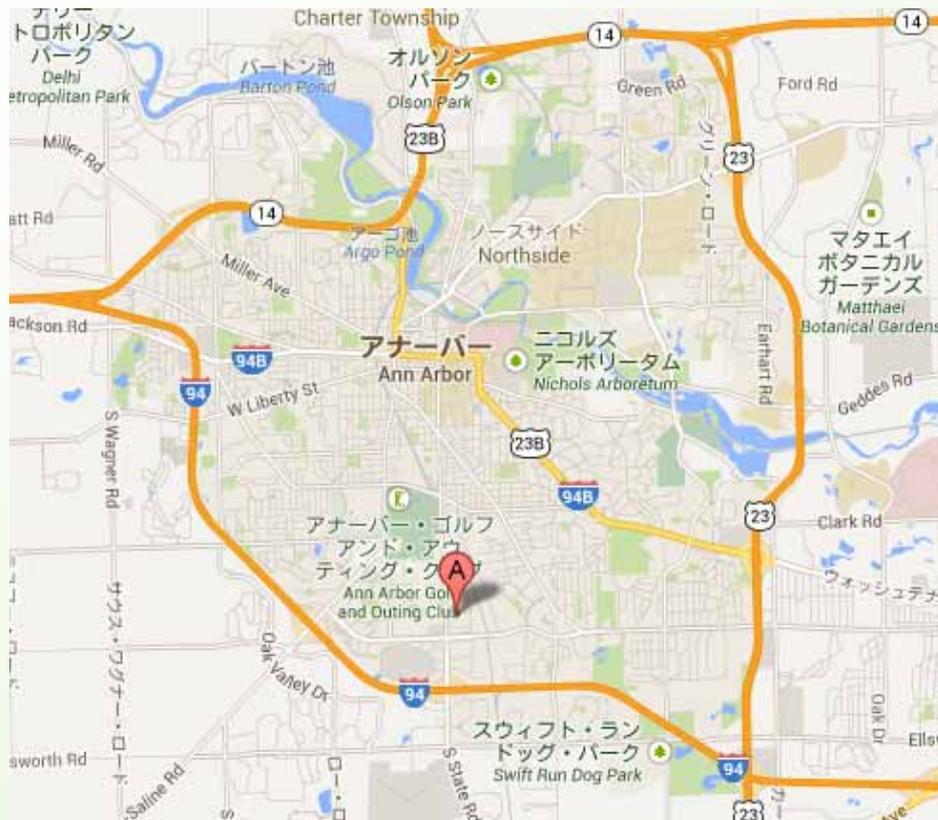


4

アーバーネットワークスとは



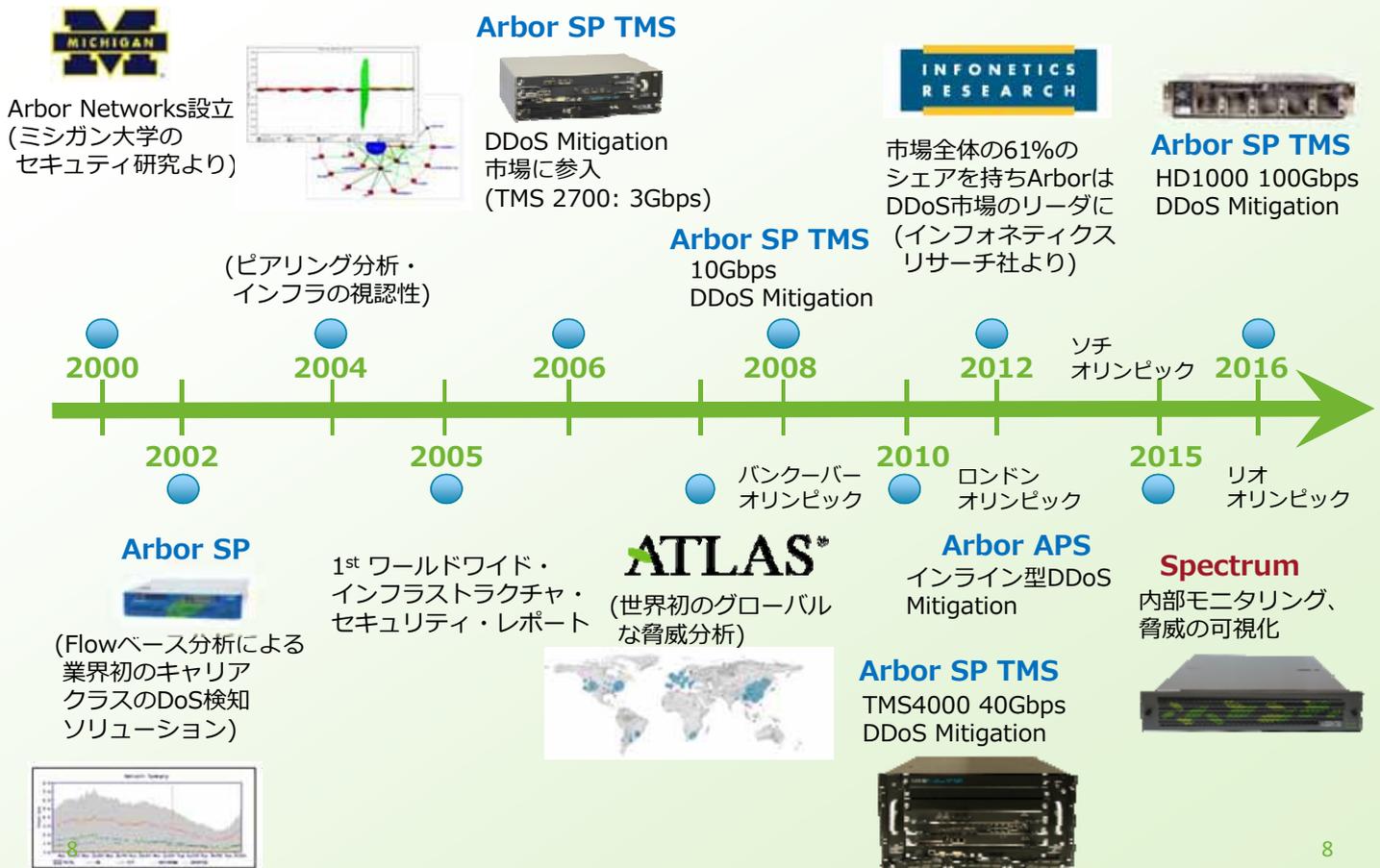
アーバーネットワークスとは



アーバーネットワークスとは

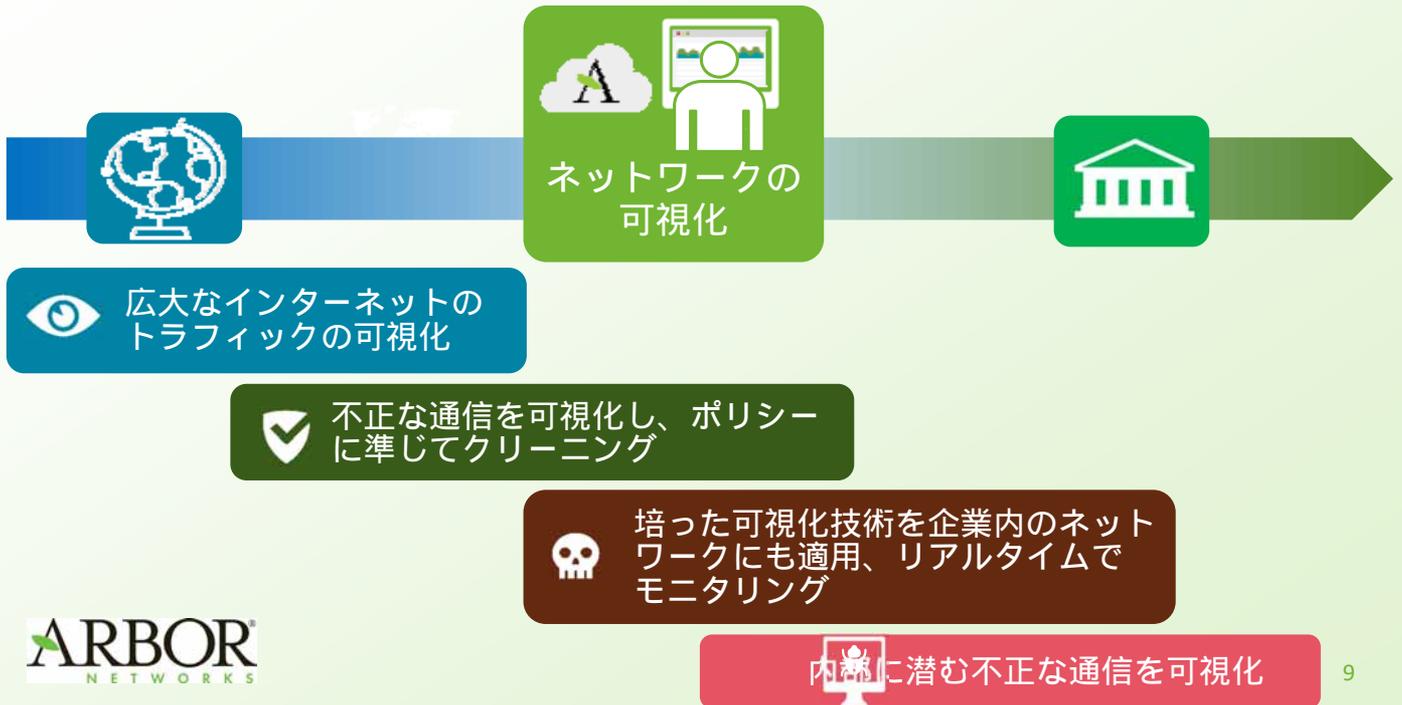


アーバーネットワークス 17年間の軌跡



アーバーネットワークスのビジョン

何が起きているのかを可視化をすることが、脅威への適切な対応を可能にする



世界最大級のネットワーク監視システム

90% Tier1サービスプロバイダの90%がARBORのお客様



107

ARBORの製品は107ヶ国に展開



40%のインターネット・トラフィックをATLASで監視

40% by 139 ISPs

さらに下記のデータソースを保有

- IPv4 2.63億 (総数約43億)
- Dark IPv4 176万
- ASN 44,570

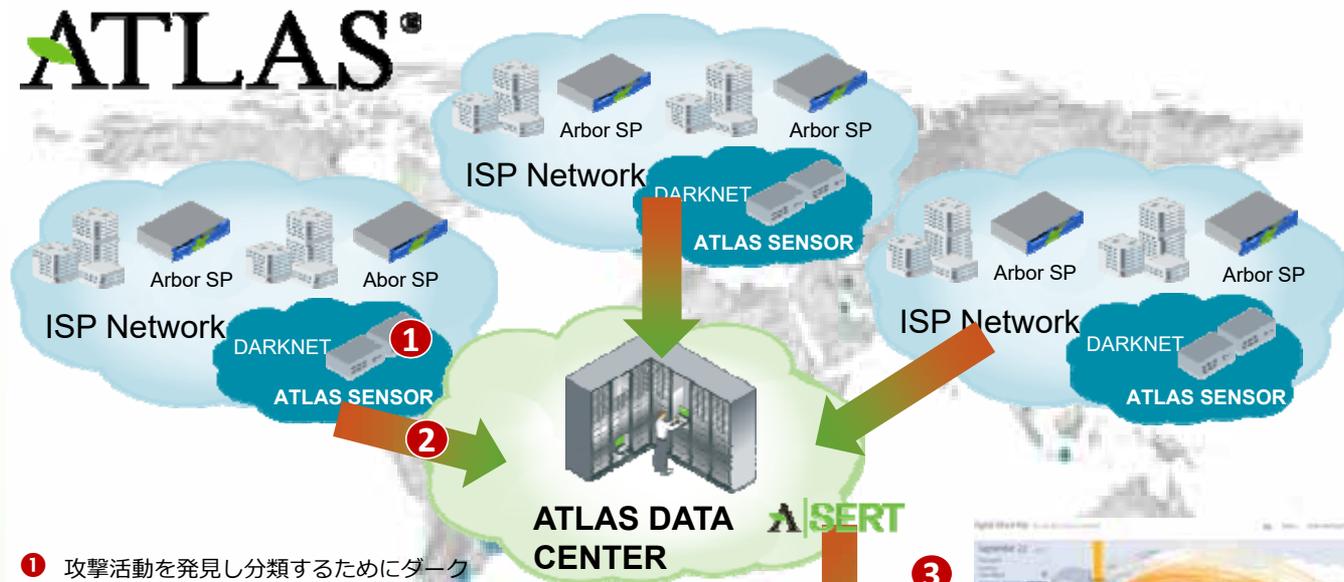


ARBORの市場ポジションはキャリア・エンタープライズ・モバイルのDDoS市場において61%のシェア [Infonetics Research Dec 2011]



ARBORは革新的なセキュリティとネットワーク可視化技術を17年間に渡り提供

ATLAS[®]



- ① 攻撃活動を発見し分類するためにダークネット空間でATLAS SENSORが展開される。
- ② ARBORのArbor SP、サードパーティおよび脆弱性のデータと組み合わせてATLAS DATA CENTERに送信される。
- ③ 研究チーム(ASERT)は、そのデータを結合し分析した結果をポータル・サイトに公開する。
 - ・過去24時間の攻撃種類トップ
 - ・過去24時間の攻撃における送信元など



140 Tbps

ピーク時最大140Tbpsのインターネット・トラフィックをATLASで収集

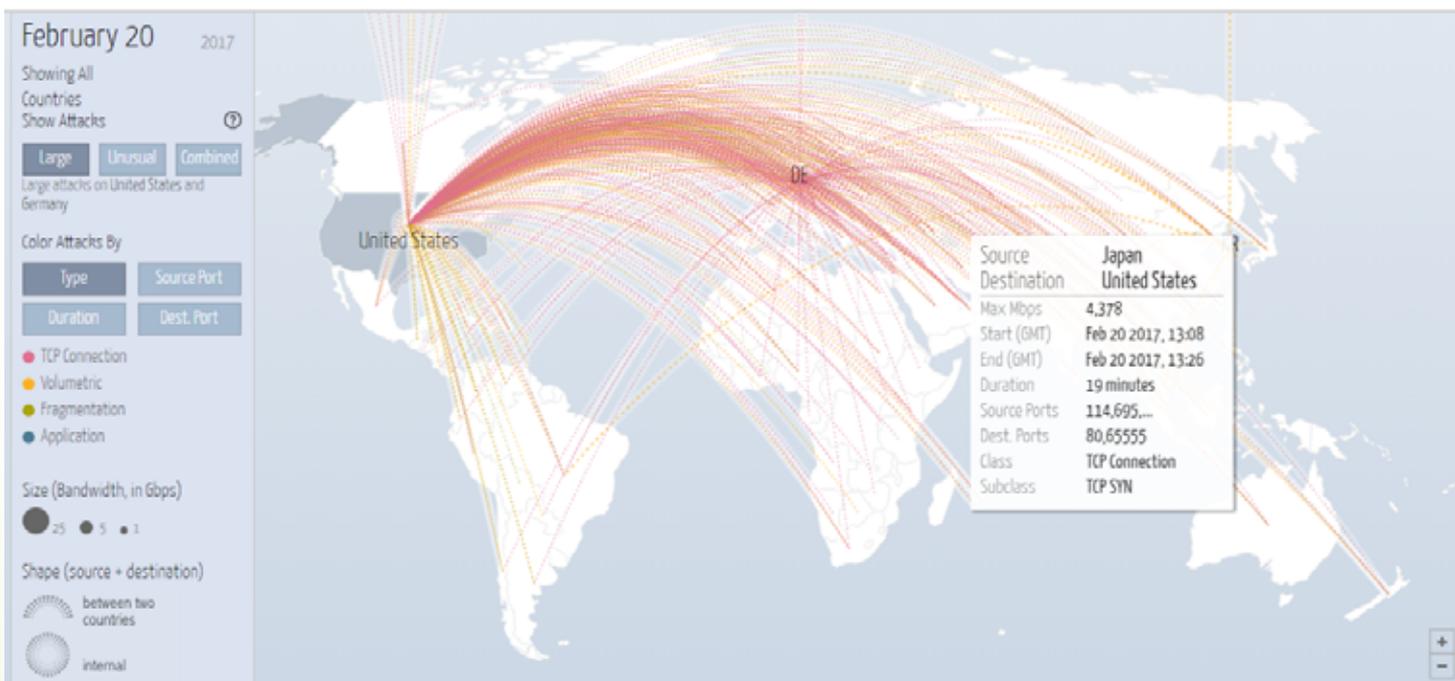
<http://digitalattackmap.com/>

Digital Attack Map

<http://www.digitalattackmap.com/>

Digital Attack Map Top daily DDoS attacks worldwide

Map · Gallery · Understanding DDoS · FAQ · About · [Social Media Icons]



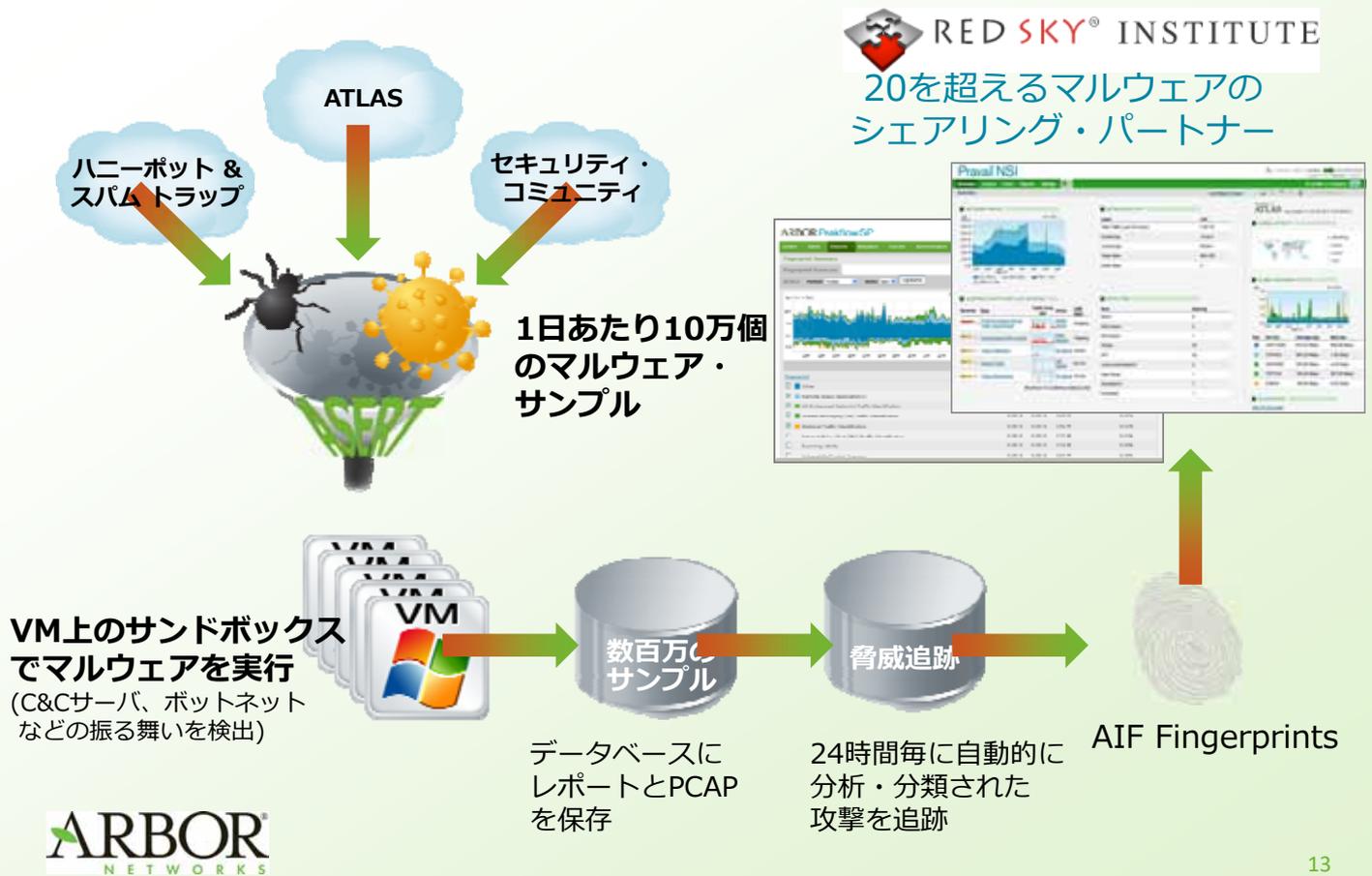
Powered by Google Ideas. DDoS data ©2013, Arbor Networks, Inc.



Privacy & Terms



ASERT (Advanced Threat にフォーカスした解析チーム)



13

2. サイバー攻撃の増加と 標的型攻撃の特徴・対策

増加するサイバー攻撃

サイバー攻撃相談件数

2020年
東京オリンピック



IPA J-CRAT相談件数よりグラフ化



リオオリンピックに関連するDDoS攻撃



2015 | 2016



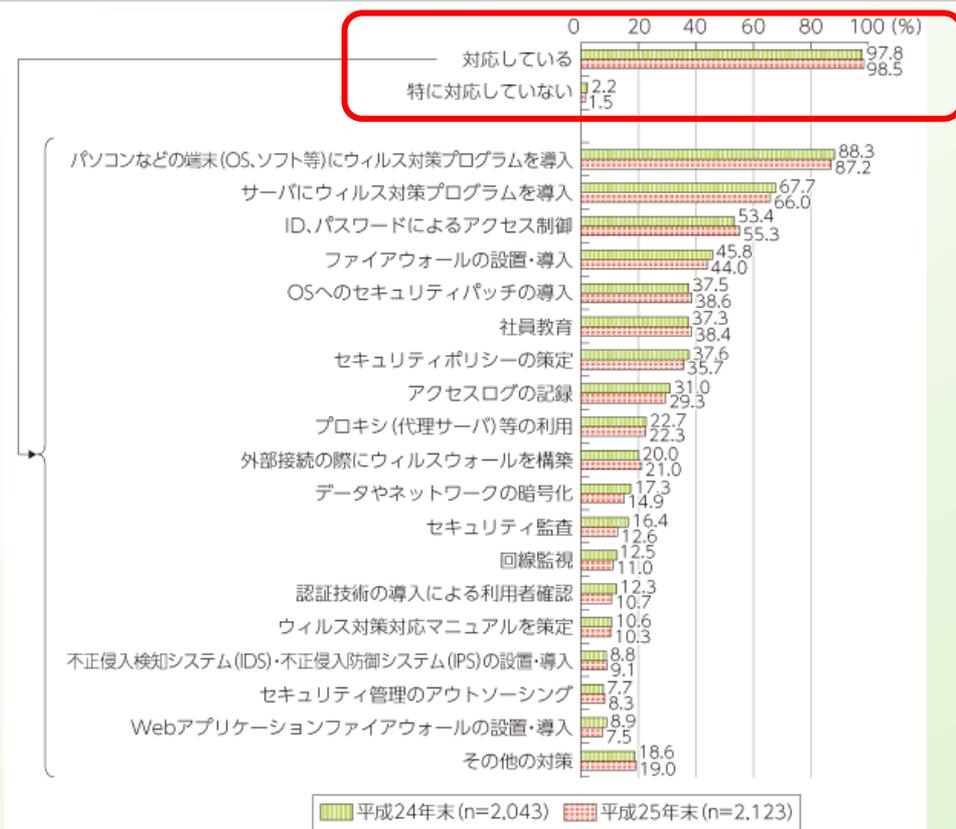
IoT ボットネットによる最初のDDoS攻撃活動

イベント期間中



アーバーネットワークスATLASよりデータ収集

企業のセキュリティ対策の実施状況



総務省H26年度情報通信白書

<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/image/n5303080.png>

サイバー攻撃への対策（例は一部）



入口対策

- FW
- IPS/IDS
- Sandbox



内部対策

- 認証サーバ
- Anti Virus
- ネットワーク機器



出口対策

- URLフィルタリング
- NG-FW
- Proxy Server



ログ監視、分析

- SIEM、アクセスログ分析ツール



デジタル・フォレンジック

- コンピュータフォレンジック、ネットワークフォレンジック



拡大する被害

2016/6/14	⑨その他のサービス業	旅行業	グループ企業への標的型攻撃により、顧客の個人情報が社外に漏えい
-----------	------------	-----	---------------------------------

当該企業は2016年6月14日、不正アクセスによる個人情報流出の可能性について報道発表を行った。3月15日に同社のインターネット販売を受け持つ子会社の従業員が標的型攻撃電子メールを開封したことにより、子会社の端末がマルウェアに感染した。マルウェア感染後、社内で不審な通信が観測されているほか、社内サーバ内に攻撃者が作成したとみられるCSV形式のファイルが作成され、その後削除された形跡が発見されており、セキュリティ会社を交えた検討の結果、個人情報漏えいの可能性があるとの判断に至っている。漏えいした個人情報は自社分が678万名、このほかに提携先企業が扱う個人情報34万件以上ある。個人情報の内容には、氏名・性別・生年月日・電子メールアドレス・住所・郵便番号・パスポート番号・パスポート取得日が含まれている。情報漏えいの可能性に関する公表が遅れた理由として、対象者の特定が不十分な	国内	34万件
---	----	------

※IPA サイバーセキュリティ経営ガイドライン解説書 被害事例より抜粋



標的型攻撃の特徴

数字で見る標的型攻撃



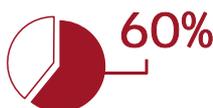
2016年の標的型攻撃は平均7個以上のツールを用い、クリティカルな脆弱性を突いていました。



44%の標的型攻撃は直接的にはマルウェアを含んでいませんでした。



2015-2016年にかけて、25%の標的型攻撃はDDoSと同時に行われました。

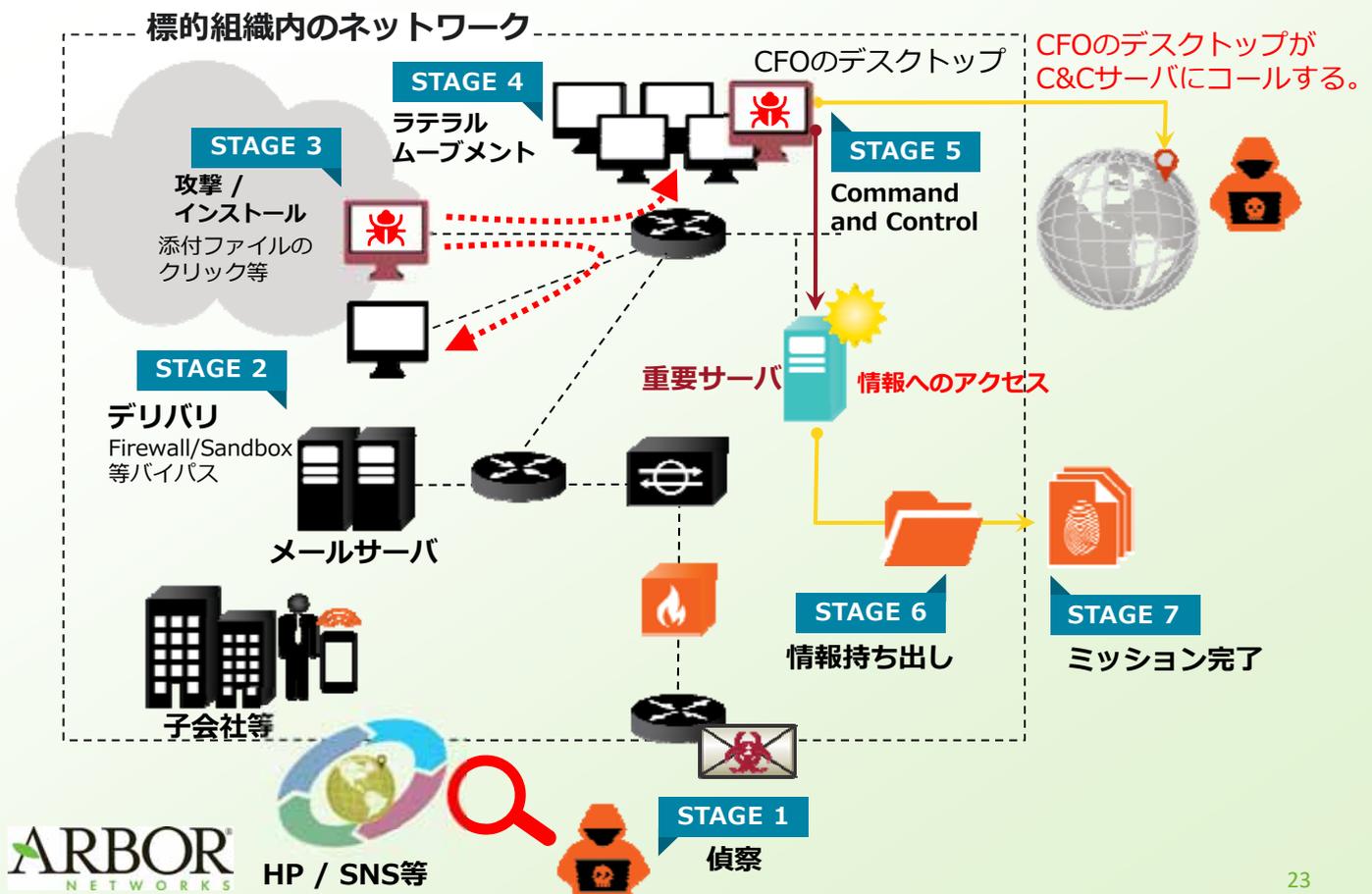


60%の企業はクリティカルなセキュリティインシデントを調査するために、3日間以上要しています。



マルウェアの平均的な潜伏期間は140日を超えています。

標的型攻撃キャンペーン一例



標的型攻撃への考えの変化



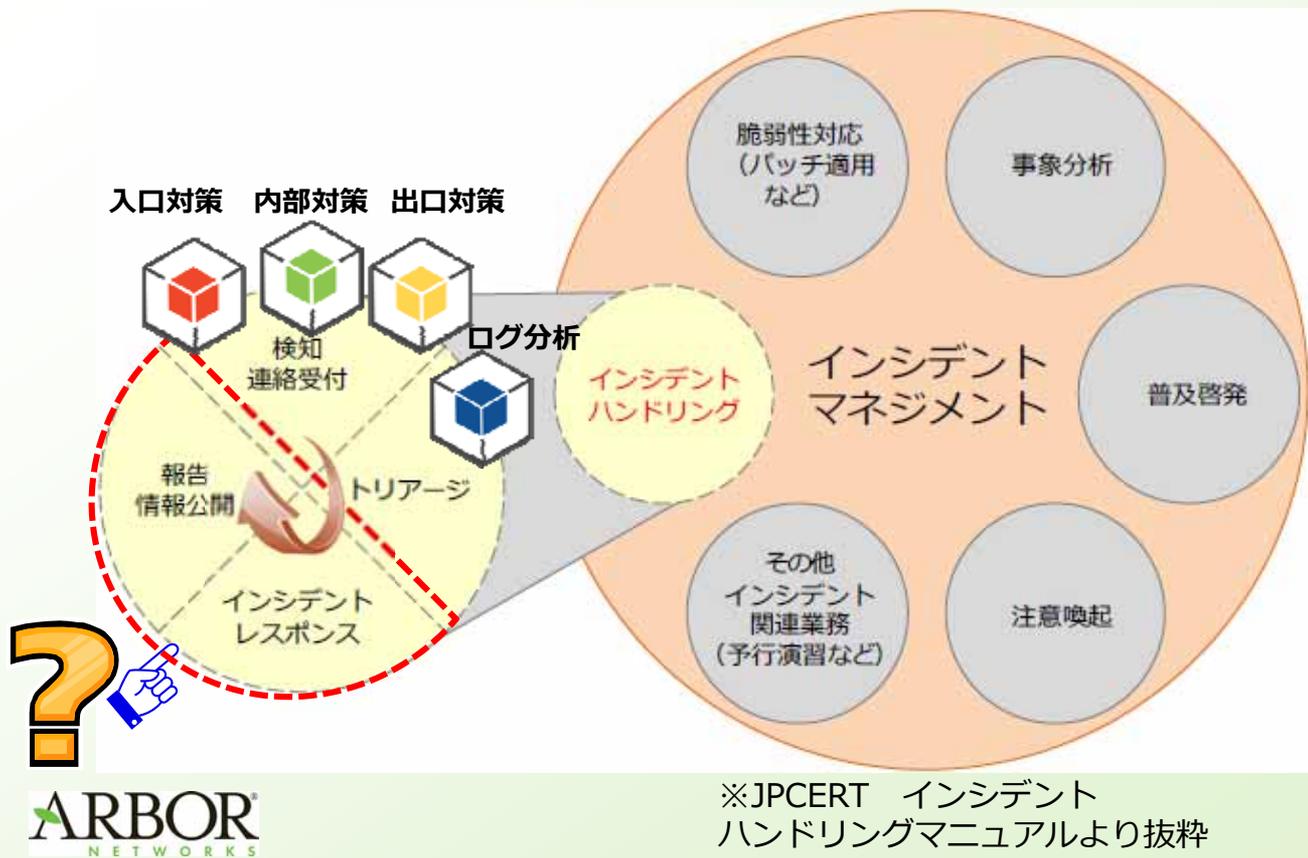
攻撃者は執拗な攻撃の中で、たった一度の成功で100%の目的を達成することができる。



企業は常に勝ち続けなければならないが、入口対策で100%検知、防御することは不可能。

侵入・感染は止められないが、被害を最小限に食い止めよう！

脅威（インシデント）に対するプロセス



25

3. インシデントレスポンスに求められるもの

インシデントレスポンスとは

■ デジタル・フォレンジック研究会

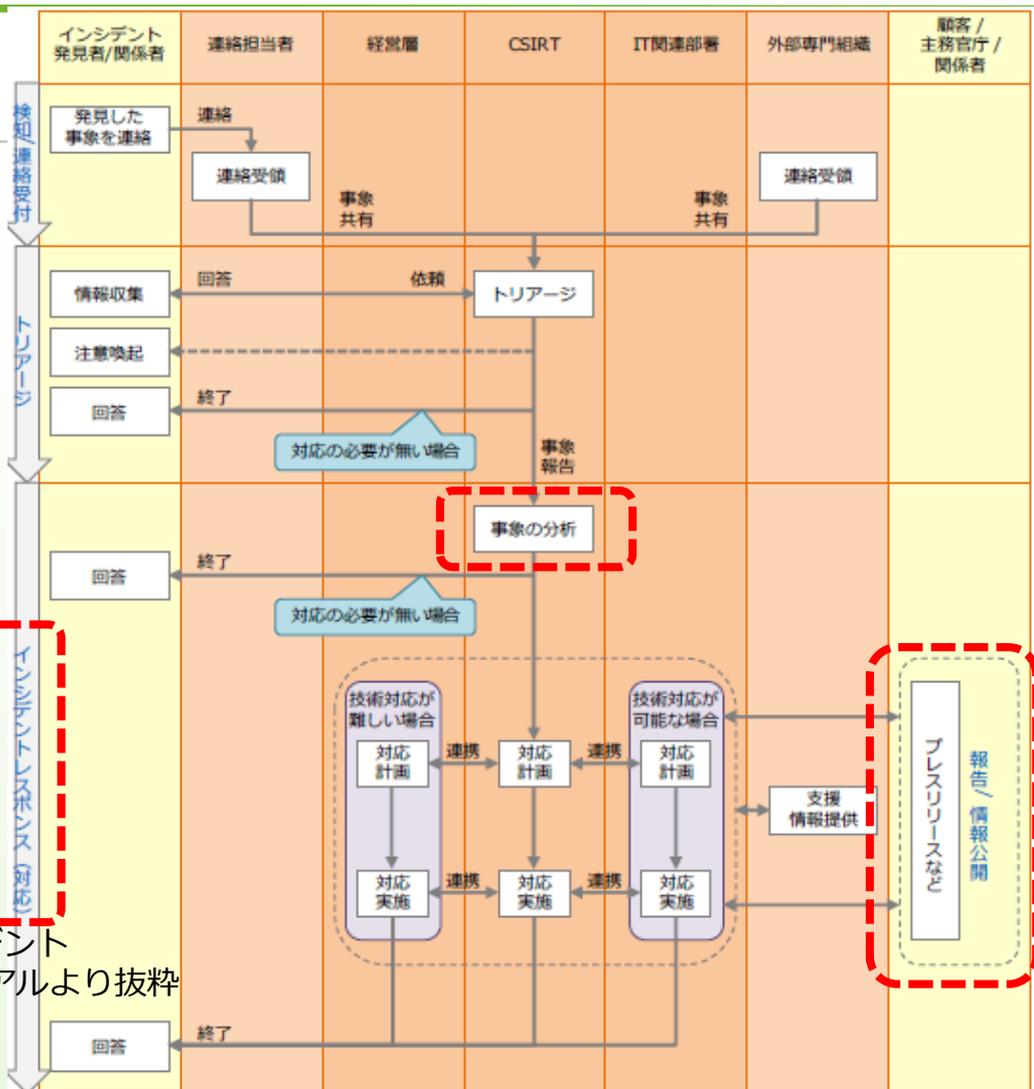
コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等

■ JPCERT

インシデントが発生した後の被害を最小限にするための「事後」対応を、インシデント対応(レスポンス)



<https://digitalforensic.jp/home/what-df/>
<https://www.jpcert.or.jp/ir/#response>



※JPCERT インシデント
 ハンドリングマニュアルより抜粋





※JPCERT インシデント
ハンドリングマニュアルより抜粋


もし、、、

適切なインシデントレスポンスが
なされない場合には、、、



という結果になることもあります。

鍵となる「事象の分析」



インシデントレスポンスの初動対応

 **事象の分析**



鍵となる「事象の分析」



事象の分析



具体的な手順や使用するべきツール、予め準備するリソース等が定義されているものではありません。



行うべき指針は、NISTより勧告されています。



33

鍵となる「事象の分析」

NIST（米国標準技術研究所）「コンピュータインシデント対応ガイド」（日本語訳：IPA/NRI secure）によると、

インシデント対応チームは、各事件の分析と検証を行うために素早く作業し、各ステップを文書化する。事件が起きたとチームが確信した場合には、チームは迅速に初動分析を行い、影響のあるネットワーク、システム、アプリケーションなどの事件の範囲、事件の犯人や原因、どうやって事件が起きたか(どのツールや攻撃方法が使用されたか、どの脆弱性が悪用されたか)を特定する。初動分析を通じて、事件の封じ込めや、事件の影響のより詳しい分析など、以降の行動に優先度を付けるのに十分な情報を得ることができる。

と記載されています。



34

「事象の分析」のポイント



各ステップを記録、可視化



素早く影響範囲を特定



事象の根本原因の特定



例えば、、、

ある端末がマルウェアに感染していた！



- 外部から操作された形跡は？
- 影響範囲（他への感染等）は？
- 外部への情報流出の疑いは？
- 関連事象は？ その時刻は？
- 疑いの通信のデータはあるか？



例えば、、、

URLフィルタリングシステムにおいて、ある端末がフィッシングサイトへアクセスした事を検知！



- 他に該当URLにアクセスした端末は？
- アクセスした端末の通信状況は？
- その後の端末の挙動は？



例えば、、、

データ漏えいを社外から指摘された！



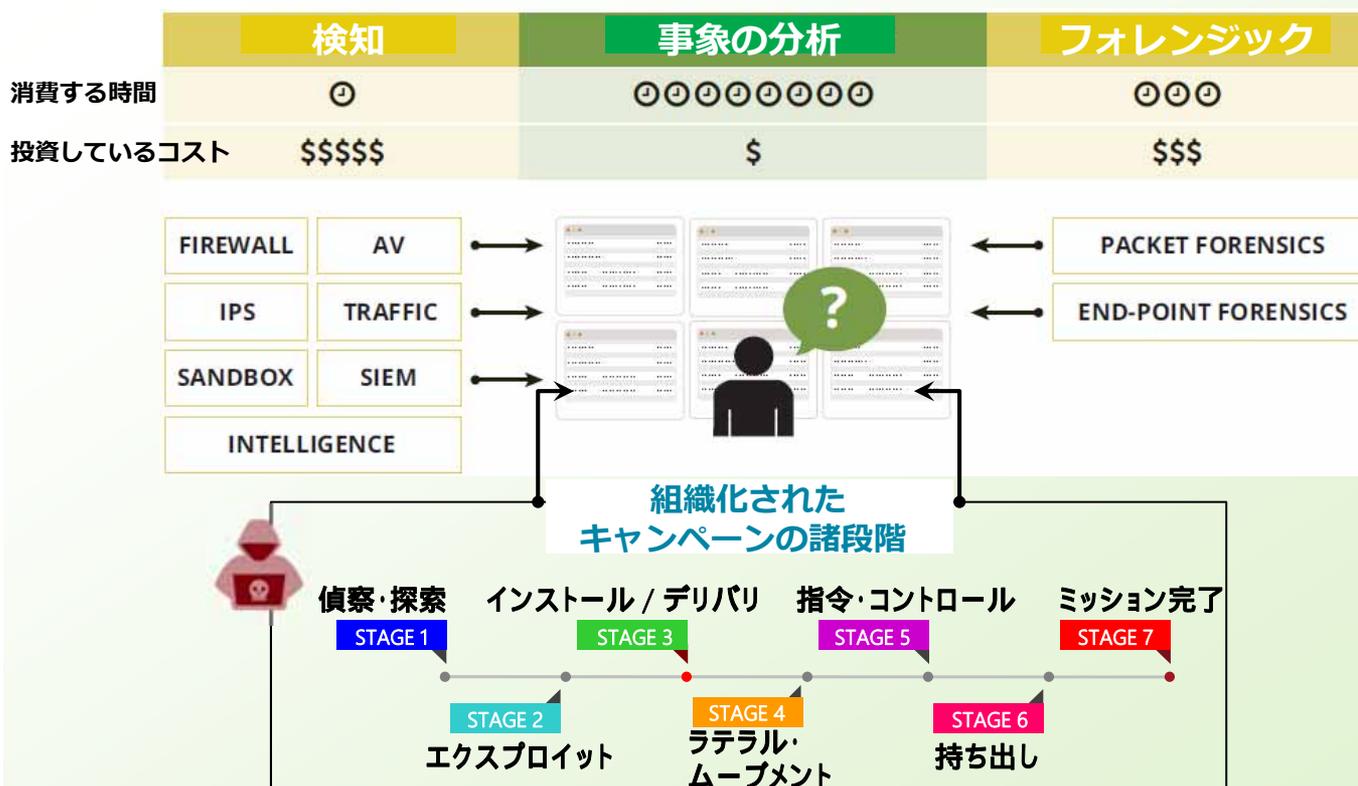
- 社内の機密情報サーバからデータを多くダウンロードした端末は？
- アクセスした端末の時間も確認したい



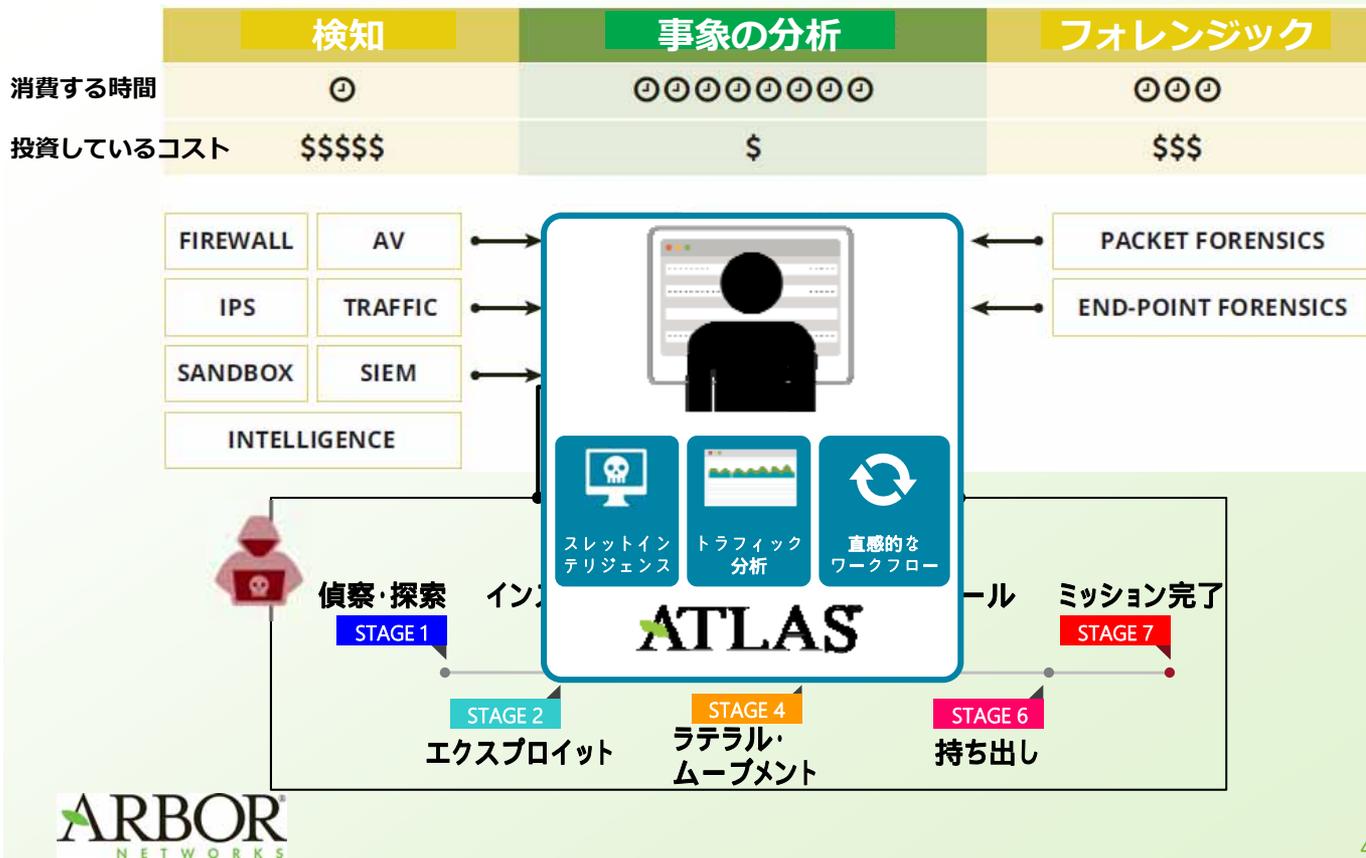
4. 「事象分析」へのアプローチ



従来の手法とインシデントレスポンスのギャップ



事象分析へのアプローチ



アーバーネットワークスのアプローチ



各ステップを記録、可視化



セキュリティフォレンジック



素早く影響範囲を特定



内部ネットワークのモニタリング



事象の根本原因の特定



能動的探索、脅威のハンティング

セキュリティフォレンジック

内部ネットワークのモニタリング

能動的探索、脅威のハンティング

インシデントレスポンスの強化
with Arbor Spectrum



43

他のアプローチ

■ SIEM

サードパーティのログを集約、異常分析や相関分析を実行。あらかじめ定義されたテンプレートや、カスタマイズしたルールによってアラートを生成。

→脅威検知をより高度にするアプローチ。

■ デジタル・フォレンジック

ファイルのハッシュ、イメージや操作ログの保存、またネットワークトラフィックの全てを保存して証拠として利活用。

→インシデントに対する証拠提示。

Arbor Spectrumとは異なる手法



44

Arbor Spectrumを用いた オペレーションイメージ

注意点

次項より紹介している製品画面キャプチャに表示されているIPアドレス、ホスト名等はあくまでも例（細工したデータ）です。それらが実際に不審なものであるという意味はございません。

アーバーネットワークスのアプローチ



各ステップを記録、可視化



セキュリティフォレンジック



素早く影響範囲を特定



内部ネットワークのモニタリング



事象の根本原因の特定



能動的探索、脅威のハンティング



47

Arbor Spectrum “セキュリティフォレンジック”

【ケース1】

SpectrumにてPoisonIvyを検知。時系列とパケット内容を確認して分析チームにエスカレーションを行いたい。

Arbor Spectrum Indicators Hunting Host Discovery Connections Investigations Help Settings Settings

Indicators Summary View [Grid] [List] Date Range 2017-03-04 10:56 → 2017-03-05 10:56

Activity [By Policy] [By Client] 48

1 unique profiles identified Sort: Newest

PoisonIvy [High] [ATLAS] - Malware - 1 Client 4 Mar 2017 10:47:12

ATLAS Indicators [clear selection] Groups Sort: newest

PoisonIvy

Overview

PoisonIvy is a backdoor agent program that grants the attacker access to the infected PC to access files, take screenshots, modify settings, and download other programs. The malware may be delivered via Trojan horse downloads. The attacker has a Windows GUI control panel, while the infected PC has no outward signs of compromise. The infected PC contacts the attacker's server for commands using an encrypted channel. The malware is capable of accessing and downloading arbitrary files on the PC, altering the computer's configuration and processes, capturing screenshots or audio, logging keystrokes, and capturing traffic as well. A plugin architecture is being developed to support third-party additions.

Find ATLAS

Category: Malware

Severity: High

Confidence: High

References: ARB-2013-0013

Indicators Sort: newest

Client	Server
192.168.12.143:42748	129.174.188.35:50000

4 Mar 2017 10:47:12



48

Arbor Spectrum “セキュリティフォレンジック”

The screenshot shows the Arbor Spectrum interface. At the top, there are tabs for Summary, Sources, Destinations, Indicators/Services, and Analysis. Below these is a table with columns for Time, Source, Indicator, and Destination. A specific indicator, 'PoisonIvy - 129.174.188.35', is highlighted. A red arrow points from a yellow callout box to this indicator. Below the table, there is a section for 'Indicator information' showing the indicator's name, severity, and confidence. A red arrow points from another yellow callout box to a list of communication events for this indicator, which are shown in a table with columns for time, source, destination, and protocol.

トップ画面等から、ある脅威（例では PoisonIvy）をクリックすることで、本脅威に関する情報を集約。

脅威に関する通信状況を時系列（ステップ毎に）に可視化。



Arbor Spectrum “セキュリティフォレンジック”

The screenshot shows the 'Indicator Information' section for 'PoisonIvy - 129.174.188.35'. A red arrow points from a yellow callout box to a specific communication event in a list. The event is expanded to show detailed information, including general information, Ethernet II details, Internet Protocol Version 4 details, and Transmission Control Protocol details. A red arrow points from the yellow callout box to the 'Transmission Control Protocol' section.

各通信はドリルダウンすることでヘッダ情報まで瞬時に確認可能。

Arbor Spectrum “セキュリティフォレンジック”

Indicator information

PoisonIvy - 129.174.188.35
ATLAS — Malware

Severity: High
Confidence: High

6:47:08 AM 192.168.20.143 → TCP → 129.174.188.35
6:47:08 AM 129.174.188.35 → TCP → 192.168.20.143
6:47:08 AM 192.168.20.143 → TCP → 129.174.188.35
6:47:08 AM 129.174.188.35 → TCP → 192.168.20.143
6:47:08 AM 192.168.20.143 → TCP → 129.174.188.35
6:47:08 AM 129.174.188.35 → TCP → 192.168.20.143

14881780360...pcap

148817803626 (92.168.20.143-129.174.188.35-40149-3009) (1).pcap [Wireshark 1.12.6 (v1.12.6-0-g0e3f0d from master-1.12)]

Wireshark等で瞬時にペイロードまで含めた詳細が確認可能。

検知した脅威はraw dataを保持。pcap形式でダウンロード可能でありフォレンジックとしての利用が可能。

クリックしてダウンロード。

極短時間で、脅威の検知からネットワークフォレンジック情報にリーチ。

51

アーバーネットワークスのアプローチ



各ステップを記録、可視化



セキュリティフォレンジック



素早く影響範囲を特定



内部ネットワークのモニタリング



事象の根本原因の特定



能動的探索、脅威のハンティング

52

Arbor Spectrum “内部ネットワークモニタリング”

【ケース2】

Spectrum、または他の監視装置において、ある端末のPortScanを検知。その端末の不審な挙動を追う為に、通信量含めて確認したい。



Arbor Spectrum “内部ネットワークモニタリング”

Arbor Spectrum

Indicators Hunting Host Dossier Connections Investigations Help Settings Satoshi

Hunting 4,339 indicators by 17 sources or Covering 1 day at a 1 hour resolution with a total

探索活動であるPort Scanでフィルタ。

SIG Port Scans X Clear Severity: High Med Low Save Searches (0)

Source	IP Address	Port	DST	Indicator	Reference
<input type="checkbox"/>	27.0.1.214	293			
<input type="checkbox"/>	204.39.94.20	293			
<input type="checkbox"/>	198.108.24.38	293			
<input type="checkbox"/>	198.108.80.7	292			
<input type="checkbox"/>	123.125.115.102	291			
<input type="checkbox"/>	198.111.237.7	288			
<input type="checkbox"/>	100.1.1.82	4.3k			
<input type="checkbox"/>	192.168.20.50	1			
<input type="checkbox"/>	192.168.20.78	1			

Port Scanの組み合わせがリストアップ。宛先を192.168.20.78でフィルタ。

送信元は192.168.20.50で内部端末と判明。内部ネットワークでの探索活動の疑い有り。

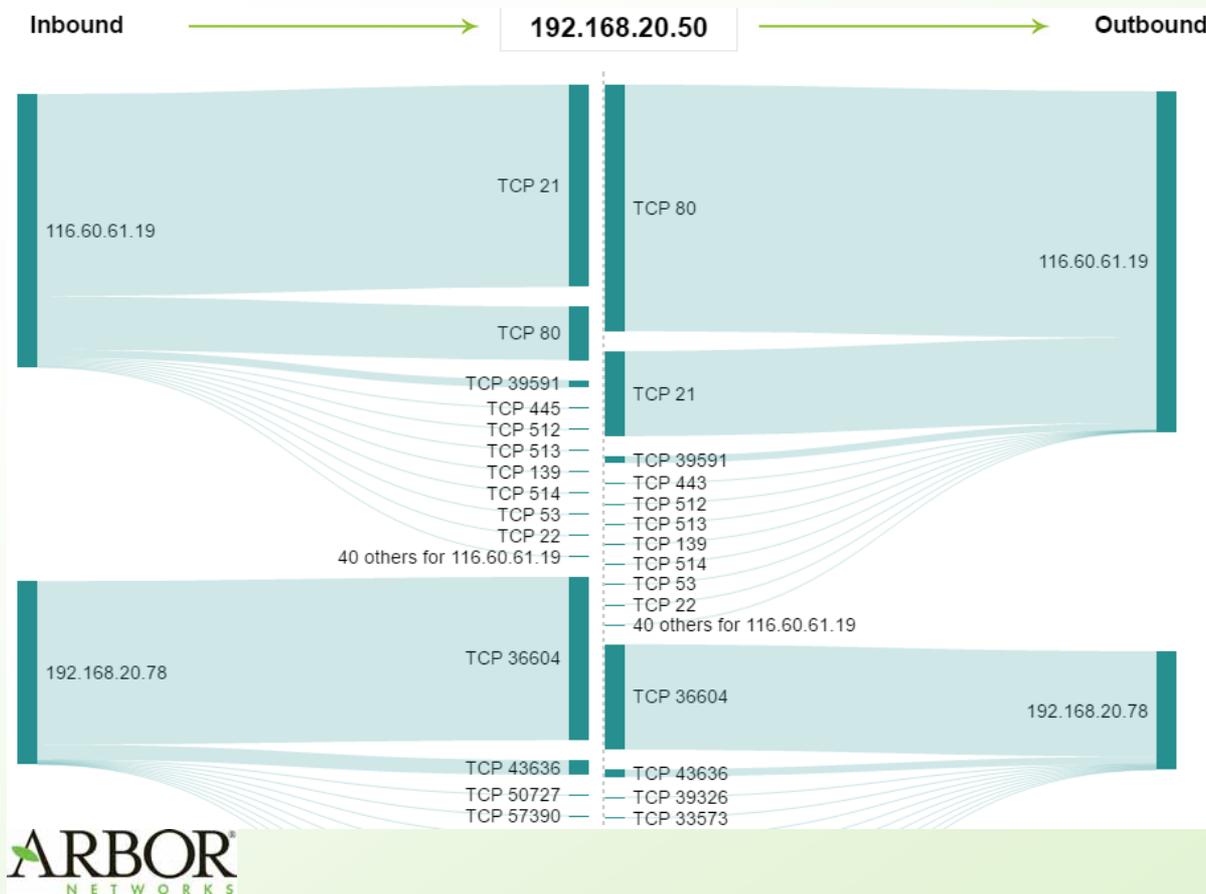
DST_ADDR 192.168.20.78 X SIG Port Scans X Clear Severity: High Med Low

Source	IP Address	Destination	IP Address	Indicator	Port	DST
<input type="checkbox"/>	192.168.20.50	<input checked="" type="checkbox"/>	192.168.20.78	<input checked="" type="checkbox"/> Port Scans	1	<input type="checkbox"/> Other

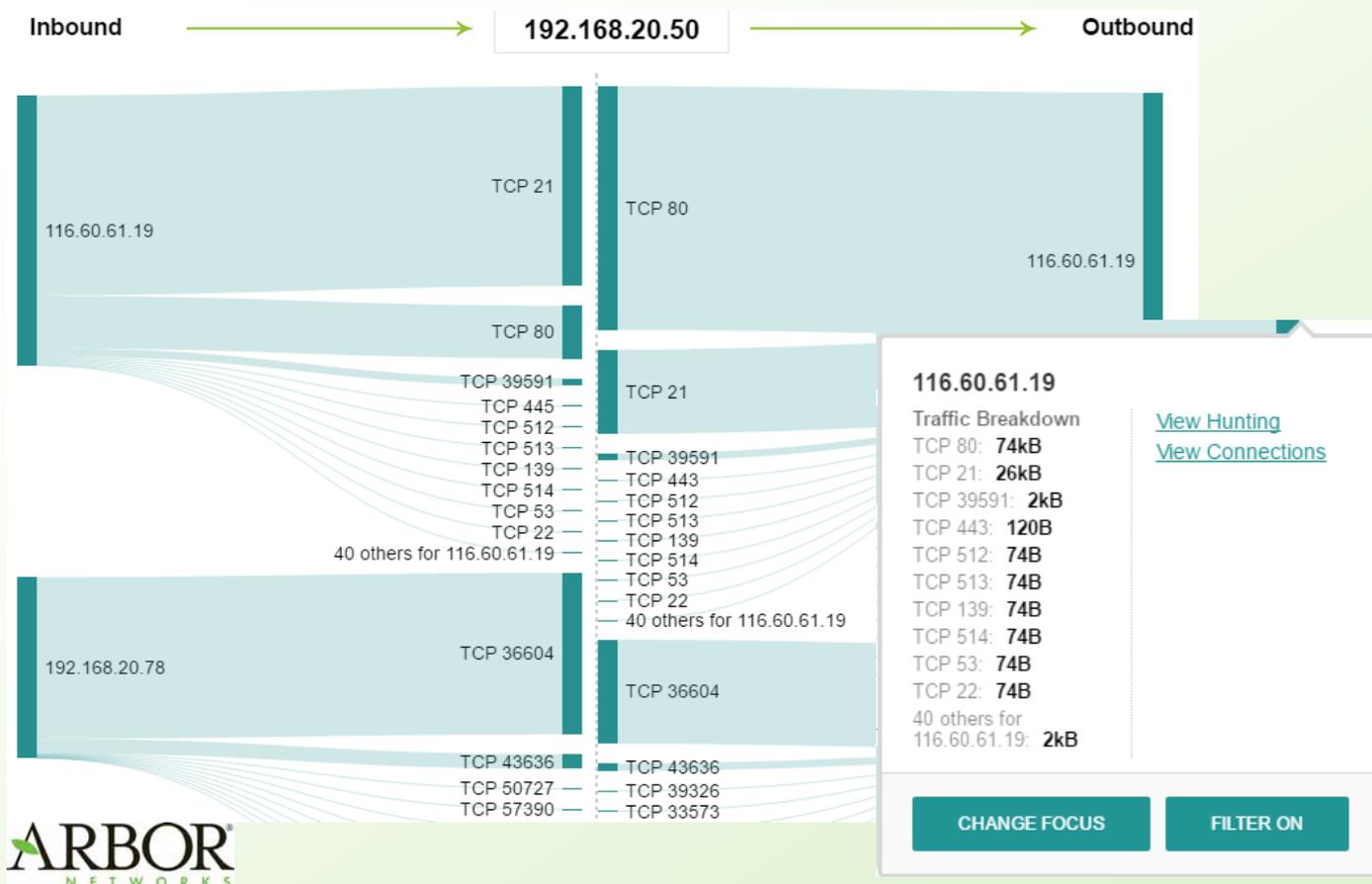
ARBOR NETWORKS

54

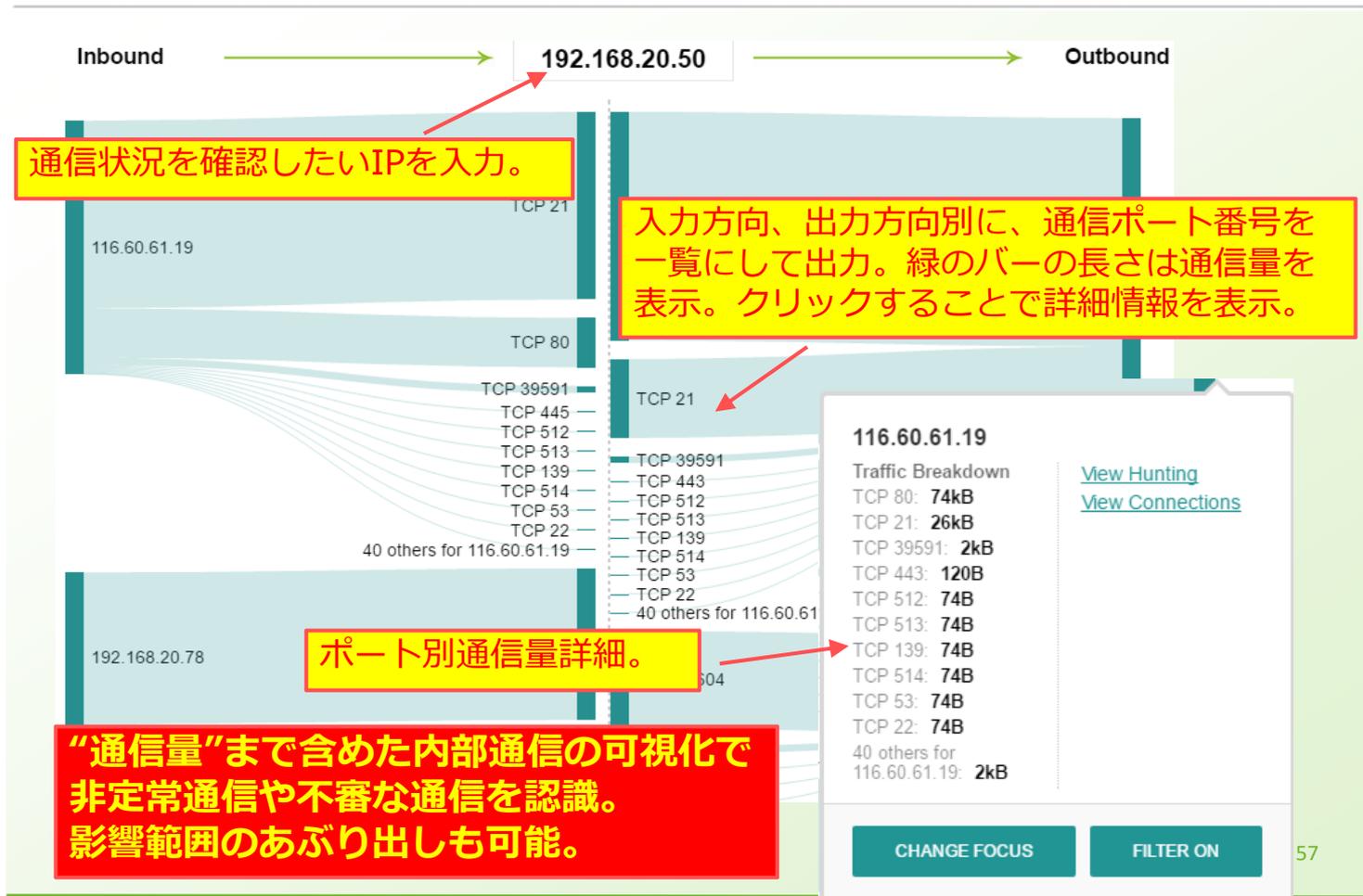
Arbor Spectrum “内部ネットワークモニタリング”



Arbor Spectrum “内部ネットワークモニタリング”



Arbor Spectrum “内部ネットワークモニタリング”



アーバーネットワークスのアプローチ



各ステップを記録、可視化



セキュリティフォレンジック



素早く影響範囲を特定



内部ネットワークのモニタリング



事象の根本原因の特定



能動的探索、脅威のハンティング

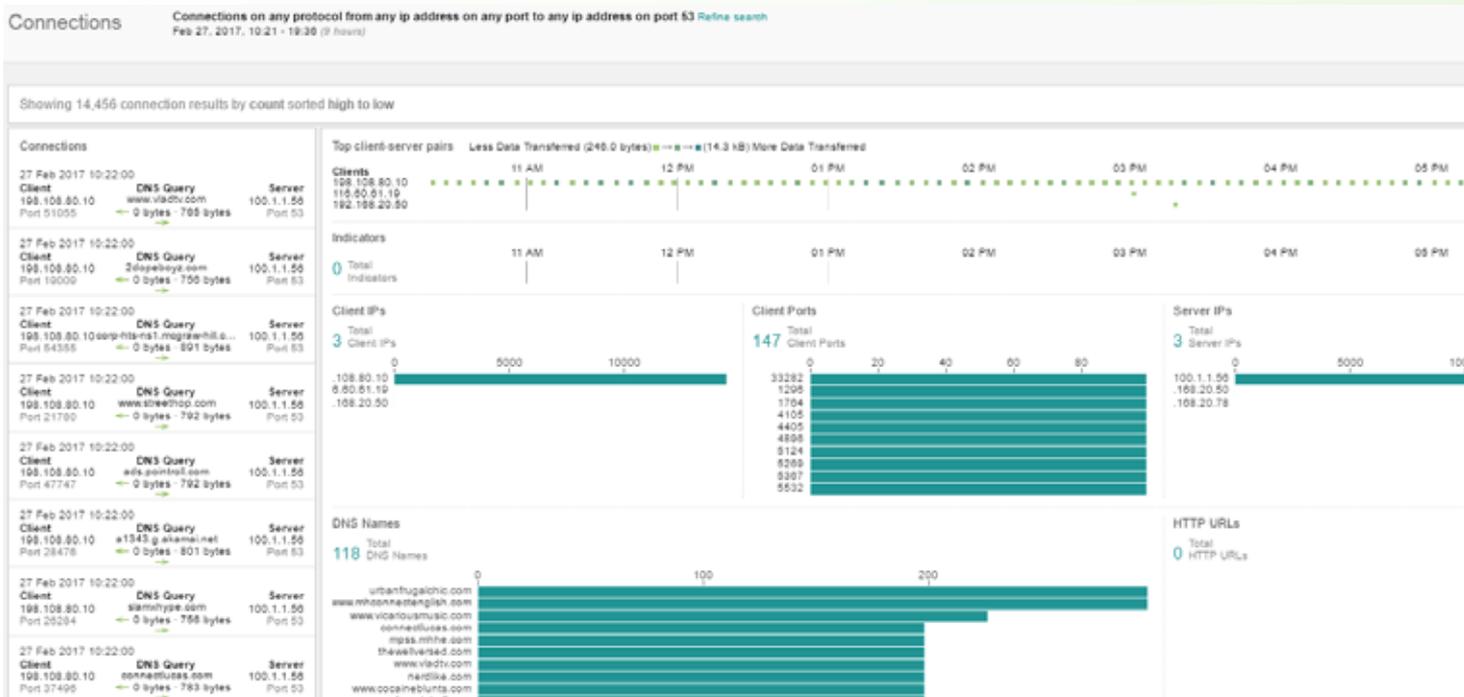
Arbor Spectrum “能動的探索、ハンティング”

【ケース3】
DNSサーバ、もしくはSIEMにてDNSサーバへの
qpsの上昇を検知。要因を調査したい。



Arbor Spectrum “能動的探索、ハンティング”

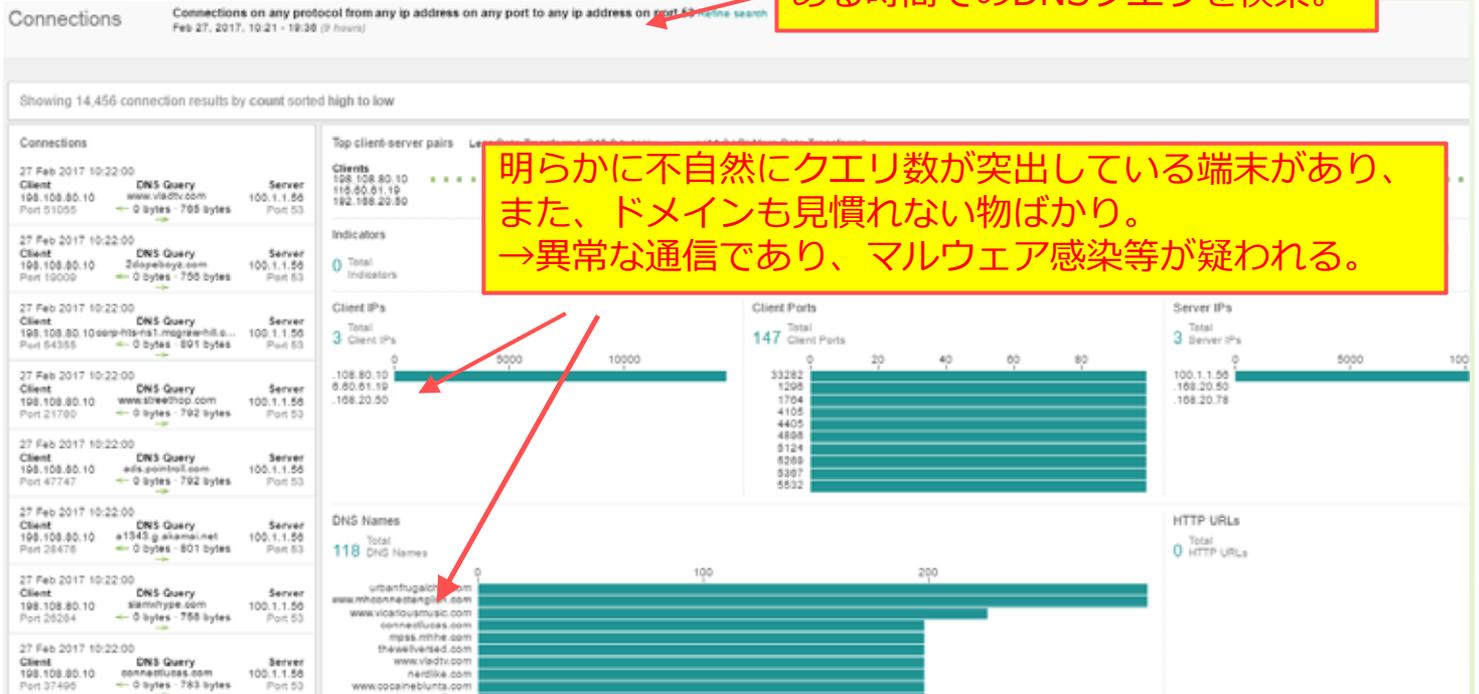
DNSのクエリから不審な端末をハンティング。



Arbor Spectrum “能動的探索、ハンティング”

DNSのクエリから不審な端末をハンティング。

ある時間でのDNSクエリを検索。



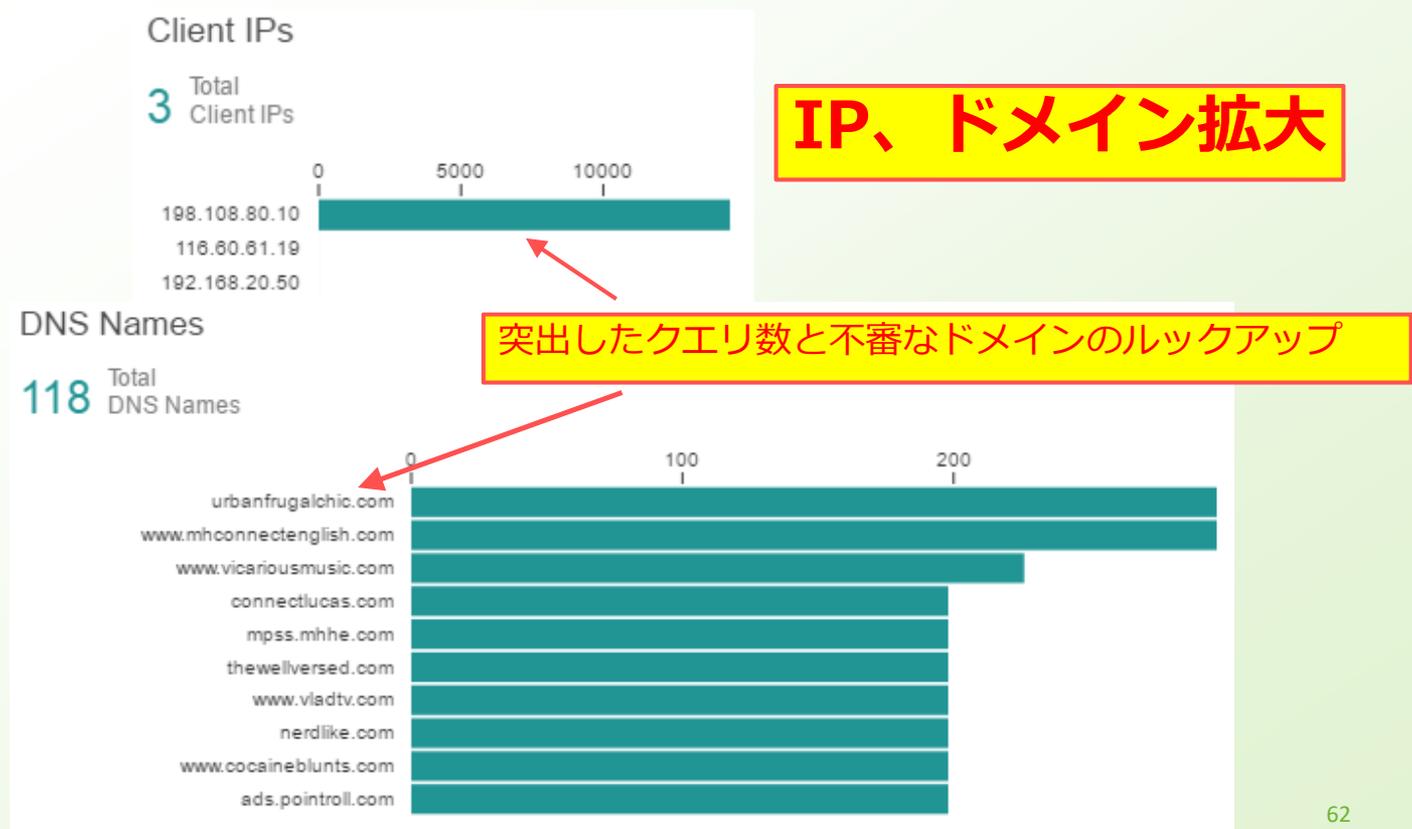
明らかに不自然にクエリ数が突出している端末があり、また、ドメインも見慣れない物ばかり。
→異常な通信であり、マルウェア感染等が疑われる。



Arbor Spectrum “能動的探索、ハンティング”

DNSのクエリから不審な端末をハンティング。

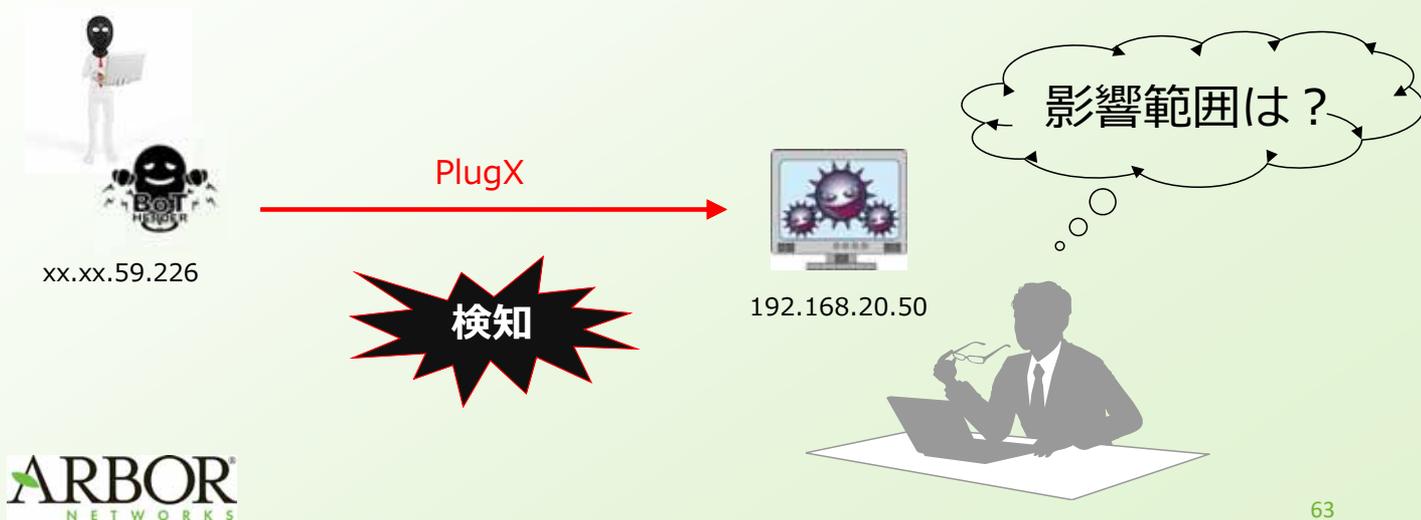
IP、ドメイン拡大



Arbor Spectrum “能動的探索、ハンティング”

【ケース4】

SpectrumでPlugXを検知。該当端末の感染だけなのかどうか、影響範囲を速やかに調査したい。



Arbor Spectrum “能動的探索、ハンティング”

PlugXの検知から脅威活動の探索と全容の把握。

Activity

6 unique policies violated

DarkComet

Zeus

PoisonIvy

PlugX

Citadel

XtremeRAT

ATLAS Indicators

PlugX

Overview

PlugX is a Remote Access Tool (RAT) that has been used in APT campaigns since at least 2008. It is often spread as an email phishing attacks. PlugX allows a remote user to connect to the infected machine in order to gather information, log keystrokes, take screenshots, and more.

Feed: ATLAS

Categories: Campaigns And Targeted Attacks

Severity: High

Confidence: Low

References: ARB-2014-0184

Indicators

Client

192.168.20.50:51168

192.168.19.50:51168

Server

Other Actions

View Hunting

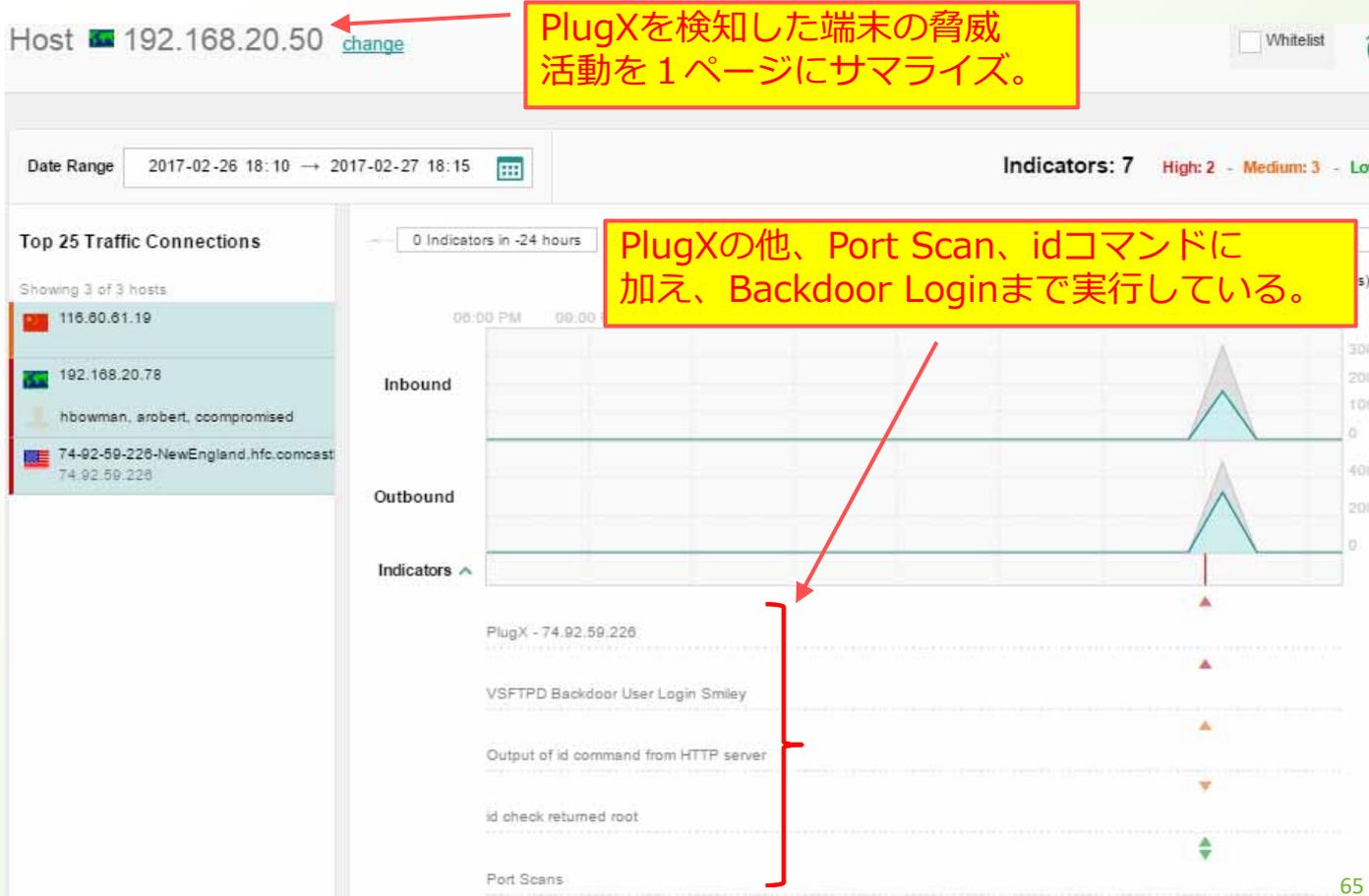
View Host Dossier for Client

View Host Dossier for Server

View Connections

PlugXを検知。被疑クライアントに対して調査を開始。

Arbor Spectrum “能動的探索、ハンティング”



PlugXを検知した端末の脅威活動を1ページにサマライズ。

PlugXの他、Port Scan、idコマンドに加え、Backdoor Loginまで実行している。

Arbor Spectrum “能動的探索、ハンティング”

27 Feb 2017 15:00:00 - 27 Feb 2017 16:00:00

ET EXPLOIT VSFTPD Backdoor User Login Smiley

Indicator traffic

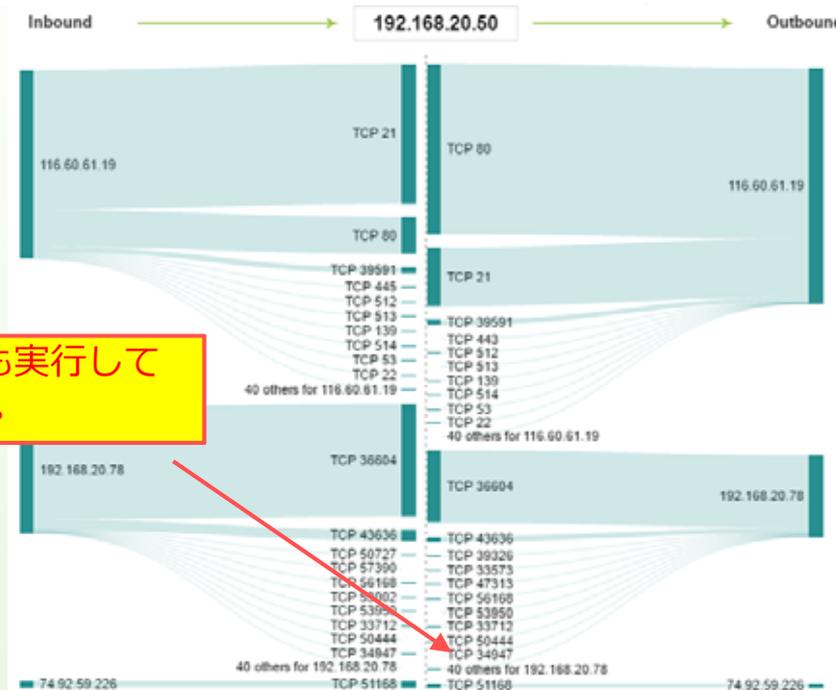
Severity: High

Events: 1

Top Destination host: 192.168.20.78

[Similar Indicators](#)

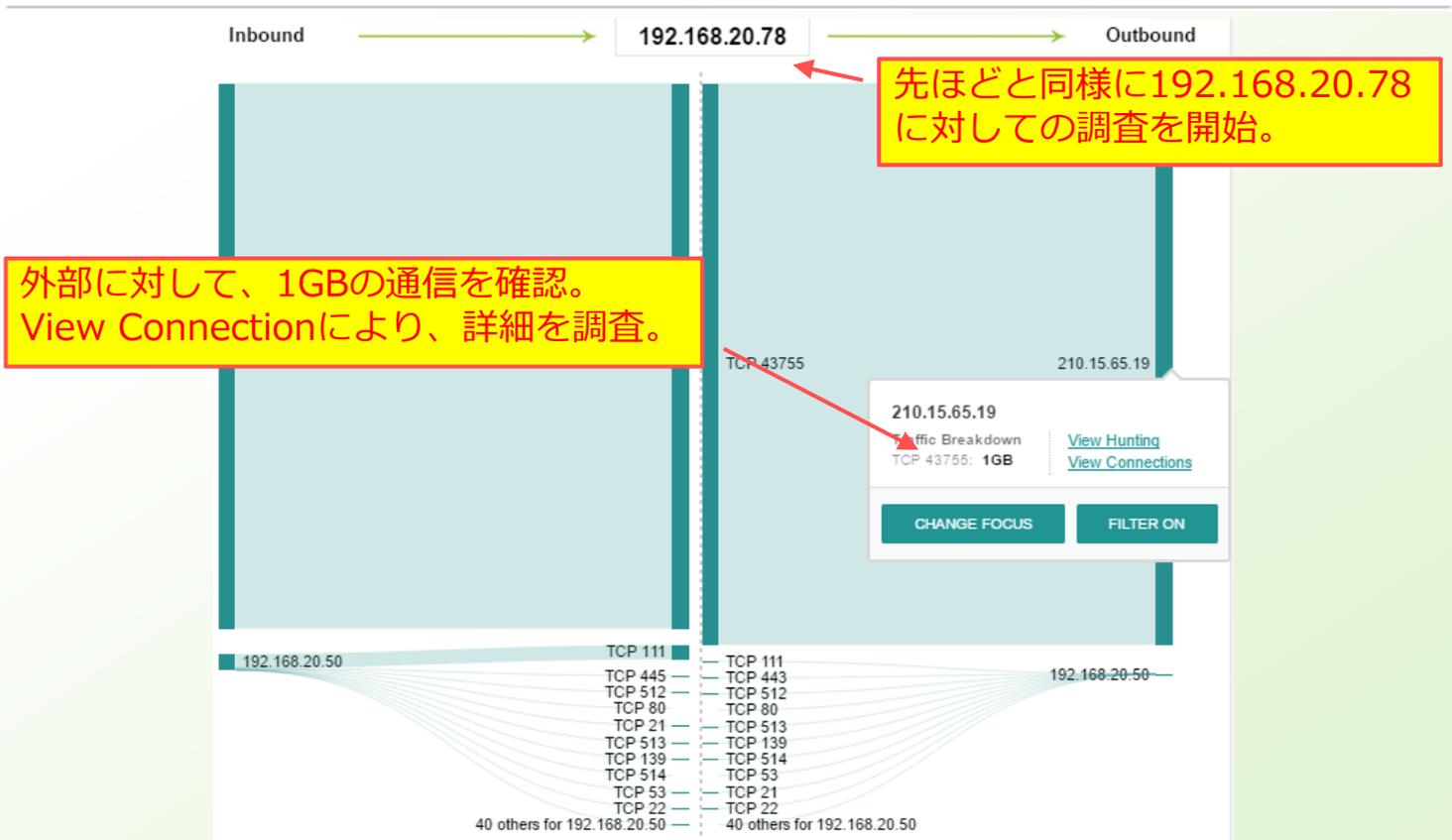
内部の192.168.20.78に対して不正なログインを実行。



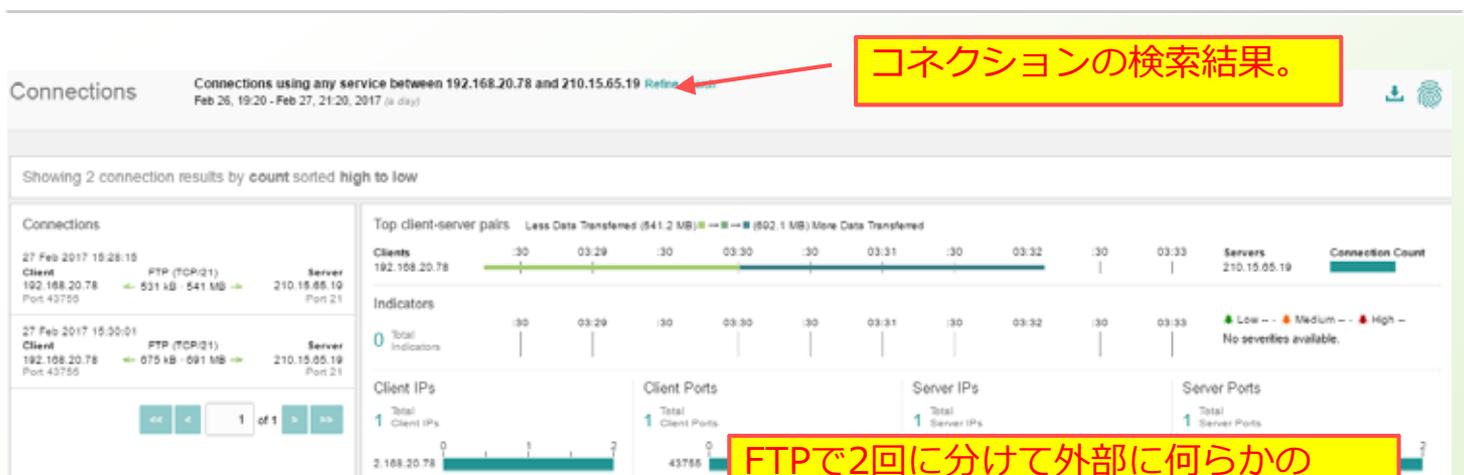
実際にPort Scanも実行していることがわかる。



Arbor Spectrum “能動的探索、ハンティング”



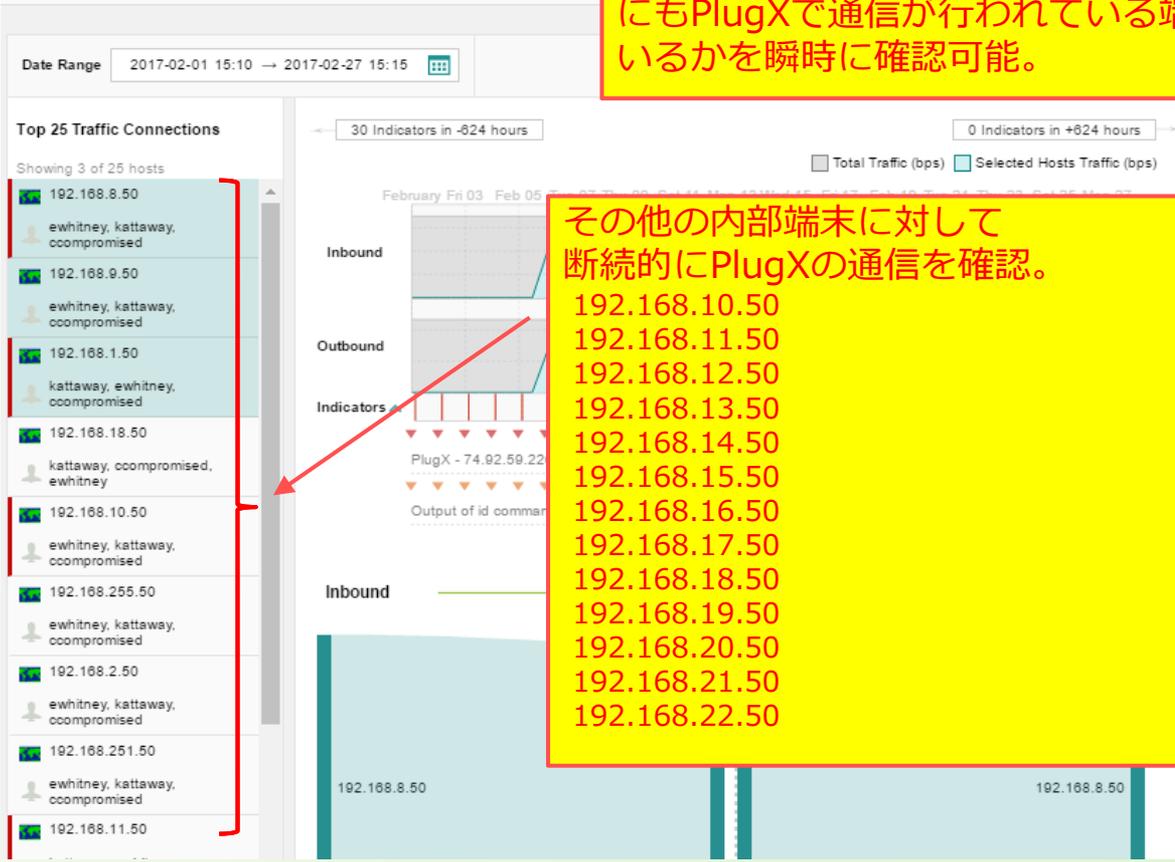
Arbor Spectrum “能動的探索、ハンティング”



Arbor Spectrum “能動的探索、ハンティング”

Host 74.92.59.226 [change](#)
74-92-59-226-NewEngland.hfc.comcastb...

サーバ側観点で調査することで、その他にもPlugXで通信が行われている端末がいるかを瞬時に確認可能。



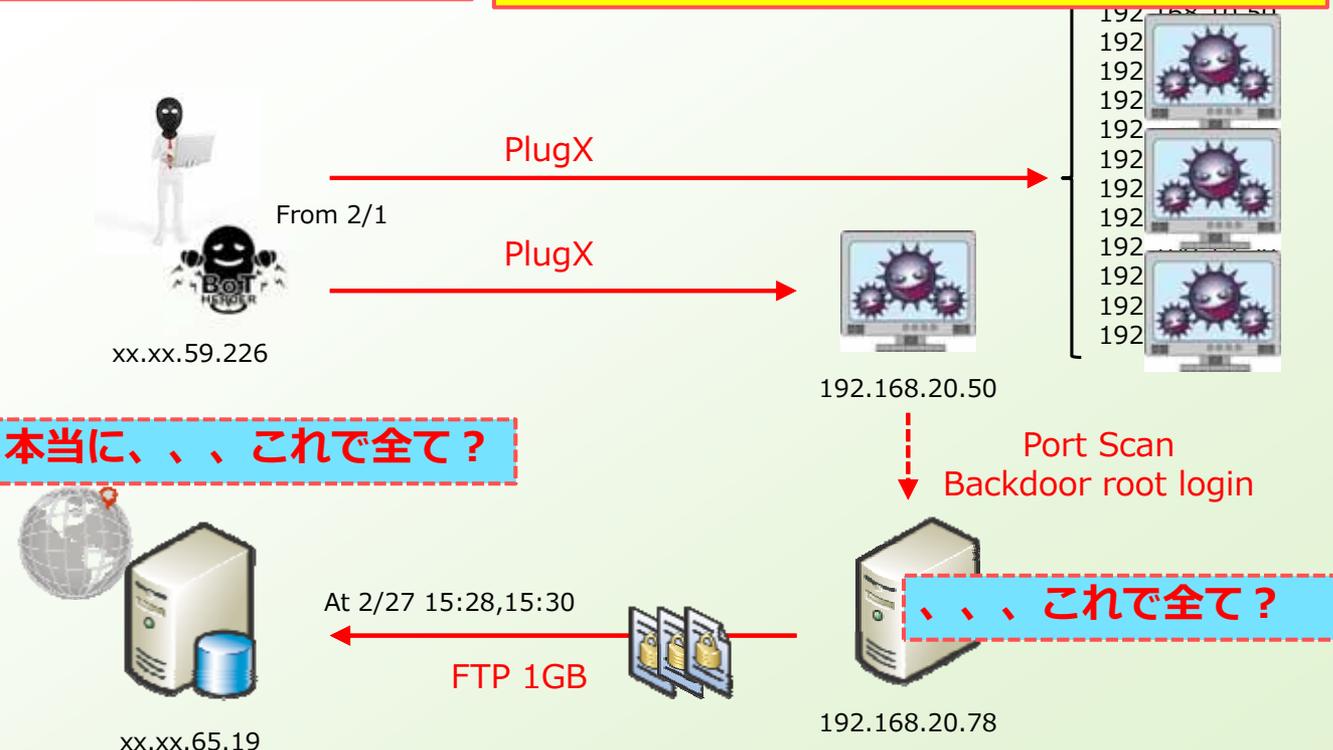
その他の内部端末に対して断続的にPlugXの通信を確認。

192.168.10.50
192.168.11.50
192.168.12.50
192.168.13.50
192.168.14.50
192.168.15.50
192.168.16.50
192.168.17.50
192.168.18.50
192.168.19.50
192.168.20.50
192.168.21.50
192.168.22.50

Arbor Spectrum “能動的探索、ハンティング”

これが全体像！

攻撃キャンペーンの全容



求められるスピーディなインシデントレスポンス

適切なモニタリングと脅威の可視化

攻撃の全体像の正しい把握

漏えいした情報と感染原因の特定

関係各所への確実、かつ迅速な報告

まとめ

アーバーネットワークスのアプローチは、**ネットワークモニタリング観点からのインシデントレスポンスの改善**です。色々なトリガーから脅威活動の迅速な可視化を実現します。可視化をすることで、より重点的に深堀すべき調査内容をあぶりだしていくことができます。

今あるセキュリティ資産をより有効に活用するためにも、現在のインシデントレスポンス能力を見直してることが重要と考えます。

ご静聴ありがとうございました。

お問い合わせは
sfujiwara@arbor.net
japanall@arbor.net
までお願いします。