平成 30 年 5 月 1 日

国立大学法人名古屋大学共同研究

「日商エレクトロニクス社取扱いセキュリティ機器の有用性、及び効果的利用法に関する共同研究」　報告書

（監修）
国立大学法人名古屋大学
情報基盤ネットワーク研究部門・准教授
嶋田 創

（作成）
日商エレクトロニクス株式会社
セキュリティ本部　セキュリティプロダクト部
市川隆一

目次

1 研究概要

日商エレクトロニクス株式会社（以下、「日商エレクトロニクス」と言います）取扱いのセキュリティ機器の有用性、及び効果的利用法に関する共同研究を実施した。

本件研究で使用する日商エレクトロニクス取扱いセキュリティ機器は Vectra Networks 社製品である。

2 序論

2.1 研究背景

サイバー攻撃が巧妙化する中で、境界防御では防げずに内部感染を許してしまった脅威への対策が急がれている。企業などの組織に対するサイバー攻撃のうち最も甚大な被害をもたらす標的型攻撃では、数か月にも渡る内部潜伏期間を通じて内部に浸潤して機密情報を奪う事例が多数報告されており、通常、「C&C 通信基盤構築」、「偵察」、「活動範囲の拡大」、「実行（データの持ち出し等）」のキルチェーンに沿って攻撃が進行する。標的型攻撃においては、攻撃者は境界防御を突破するためにマルウェア作成キットなどでカスタム版マルウェアを作成し、マルウェア作成時点での境界防御のシグネチャに反応しないことを確認して送り込むため、そのマルウェアはシグネチャによる判定が困難なものとなる。そのため、シグネチャではなく振る舞い検知が有効な手段と言われている。

本研究で使用する装置は、偵察と活動範囲の拡大を行う潜伏フェーズにおける振る舞い検知を目的とした装置であり、他の侵入フェーズ（境界防御）や事故後の調査フェーズ向けの装置を含めて、複数の装置から構成される防御ソリューションにおいて、それらを効率よく連携して運用するための仕組みと発生したインシデントに対応できる人材育成が大きな課題となっている。

また、従来では外部サイトへの DDoS 攻撃の端末や外部に対する攻撃の踏み台が主な用途であったボットネットも、最近では仮想通貨のマイニングのために資源を窃取したりダークネットへの中継サーバ構築に利用されるなど、新手の利用が登場してきている。本研究で対象とする振る舞い検知では、このようなボットネットの振る舞いも検知対象としている。

2.2 研究目的

日商エレクトロニクス取扱い機器（Vectra Networks 社製品）の効果検証、及び、実運用に振る舞い検知の挙動の研究、また、それに基づく侵入検知システム全般の効果的な利用方法を開発する。

2.3 研究内容

ハニーポットおよび実組織内ネットワーク環境を模したマルウェア検体実行環境を利用し、近年の高度且つ巧妙化するマルウェア動作を分析・学習、その特徴や攻撃者のプロファイルを深く理解し、それに基づく効果的な検知方法、防御方法を調査（仮説立案）する。また、今後登場する可能性の高い攻撃を予測し、その攻撃に対する効果的対処法、及び、日商エレクトロニクス取扱機器の効果的利用方法を開発する。

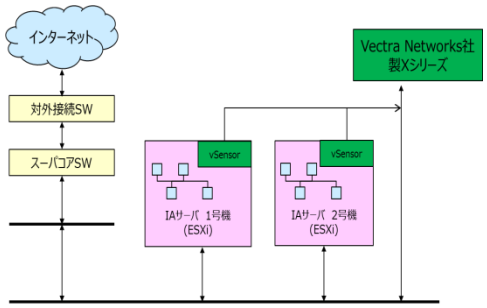
3 実施方法および機材

3.1 実施方法

3.1.1 概要

名古屋大学内に仮想マシン(以下、VM)ホスト用 IA サーバを 2 台設置し、各 IA サーバに仮想マシンハイパーバイザとして VMware ESXi(以下、ESXi)を搭載する。各 ESXi の中に仮想マシンを作成し、ハニーポット群を構成する。ハニーポット群は 10 台の Windows7 クライアントと 4 台の Windows Server からなる実組織環境を模したグループと、複数のオープンソースのハニーポットソフトウェアを利用してインターネット側からの攻撃の呼び込みに注力するグループの 2 群からなる。前者の実組織環境を模したグループは、Windows Server が外部へのポート公開を伴うハニーポットであるとともに、Windows7 クライアント上でマルウェアを動作させてその挙動を観測する、マルウェア観察環境を兼ねる物となっている。いずれのハニーポット群に対しても、ネットワークの上流に設置したファイアウォールにてアクセス制御を行い、ハニーポット群から外部への通信の試みを最小化し、万が一の事故時の対策を実施している。ハニーポット内のネットワークトラフィックは本研究の機材である Vectra Networks 社製仮想センサ（vSensor）がキャプチャし、分析に必要なメタデータを生成する。生成したメタデータは同社製の分析装置（X シリーズ）に送られ、ハニーポット内のマルウェアやその他の悪意のあるもと考えられる疑わしい振る舞いを分析・可視化する。これにより、実際のマルウェアによる攻撃、および、その他の悪意のあるアクセスの特徴が、どのような形で可視化した情報となるか観察し、機材の運用や効果的な利用方法を開発する。以下、ハニーポットの構成の概要を図 3.1.1 に示す。

図 3.1.1 ハニーポット構成概要



VM ホストである 2 台の IA サーバ上の ESXi 内に各々Vectra Networks 社製の仮想センサ（vSensor）を配置し、ハニーポットの通信をキャプチャする。vSensor が生成したメタデータを同社製 X シリーズに送り、攻撃を分析・可視化する。（「3.2 機材」参照）

3.1.2 ハニーポット群構成

ハニーポット群を構成する機器、ソフトウェア、および、そのバージョンは以下の通りである。

VM ホスト用 IA サーバ： ヒューレット・パッカード・エンタープライズ社製 ProLiant DL360 x 2 台

ハイパーバイザ： VMware ESXi 6.5.0 x 2 台

仮想マシン： 表 3.1 に示す通り、ESXi 内に仮想マシンを作成し、ゲスト OS として、クライアント用 OS として Windows7、サーバ用 OS として Windows Server 2012、Linux(Ubuntu)をインストールし、表 3.1 に記すホスト名と用途のもとに運用した。

表 3.1a ESXi 1 号機

各仮想マシンが利用する共通リソース：G/W:133.xx.xx.126, DNS: 133.x.x.2, 133.x.x.4

NTP:133.x.x.9

OS	仮想マシン名	ホスト名	用途
Win2012	AD_Srv-113	AD_Srv-113	ハニーポット用 Active Directory サーバ， FTP/FILE サーバ
Win2012	win2012_114	sv2	ハニーポット用サーバ
Win2012	win7_105	sv1	ハニーポット用サーバ
Windows7	win7_115	Rdp	ハニーポット用 PC RDP サービス ON
Windows7	win7_116	cl1	ハニーポット用 PC
Windows7	win7_117	cl2	ハニーポット用 PC
Windows7	win7_118	cl3	ハニーポット用 PC
Windows7	win7_119	cl4	ハニーポット用 PC
Windows7	win7_120	cl5	ハニーポット用 PC
Windows7	win7_121	cl6	ハニーポット用 PC
Windows7	win7_122	cl7	ハニーポット用 PC
Windows7	win7_122	cl8	ハニーポット用 PC
Win2012	win2012_master	sv1	ハニーポット用サーバ
Windows7	win7_master	N/A	ハニーポット用 PC のテンプレート

表 3.1b ESXi 2 号機

各仮想マシンが利用する共通リソース：G/W:133.xx.xx.126， DNS: 133.x.x.2, 133.x.x.4

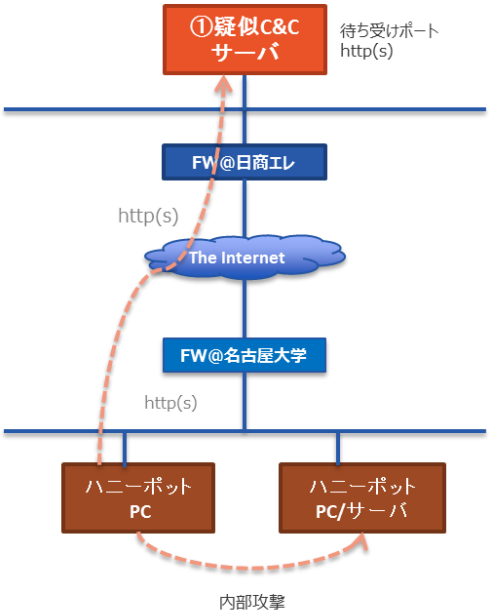
NTP:133.x.x.9

OS	仮想マシン名	ホスト名	用途
Ubuntu Linux (64)	T-Pot	thirstybibliography	オープンソース利用ハニーポット用サーバ
Ubuntu Linux (64)	Cowrie	host	オープンソース利用ハニーポット用サーバ
Ubuntu Linux (64)	dionaea	host	オープンソース利用ハニーポット用サーバ
Ubuntu Linux (64)	Glastopf	host	オープンソース利用ハニーポット用サーバ
Ubuntu Linux (64)	Suricata	suricata-virtual-machine	オープンソース利用ハニーポット用サーバ

3.1.3 疑似標的型攻撃環境

本研究チームが事前に挙動を完全に把握できている擬似標的型攻撃を観測させるため、ハニーポットに対して本研究チーム自らが疑似攻撃を行う環境を用意した。 図 3.1.3 に示す通り、インターネットを介した外部に疑似 C&C サーバを構築し、ハニーポット内のホストと HTTP (80/TCP)および HTTPS（443/TCP）で通信可能な環境を用意し、HTTP(S)を利用した指令とデータ窃取を模した通信を可能とした。

図 3.1.3 疑似攻撃環境



日商エレクトロニクス内に疑似C&CサーバとしてLinux(CentOS 6.4)を設置した。擬似C&Cサーバは124.xx.xx.118というIPアドレスを与えられ、クライアントからのHTTP(S)によるコネクトバックを待ち受けるために　Apacheが動作している。ハニーポット内からC&CサーバへPOSTメソッドを利用してデータを窃取する疑似攻撃を行うため、ApacheはPOSTを許可する設定としてある。

疑似C&Cサーバはインターネットに晒されるため、ファイアウォールを設置し、ハニーポット内のソースIPアドレス以外のパケットを拒否する設定としてある。

3.2 機材（Vectra Networks 社製品）

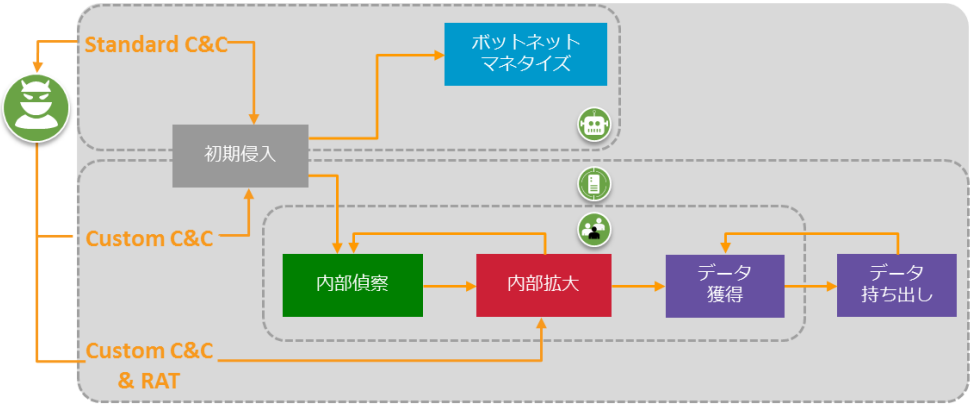
3.2.1 機材概要

Vectra Networks 社製 X・S シリーズ装置（以下、監視装置と言います）は、内部ネットワークのトラフィックをパッシブにキャプチャし、標的型攻撃の侵入フェーズ後の攻撃を可視化する装置である。監視装置はブレイン（X シリーズ）と呼ばれるトラフィック収集兼分析する装置と、トラフィックを収集し、分析に必要なメタデータを生成するセンサ（S シリーズ）と呼ばれる装置から構成される。

一般的な標的型攻撃においては、内部に侵入したマルウェアはまず C&C サーバと通信を行う基盤を構築し、その後、キルチェーンに沿って内部感染拡大のための攻撃を進行させ、最終的に重要なデータを窃取する。標的型攻撃のキルチェーンはロッキードマーティン社が最初に提唱したと言われているが、その後各セキュリティベンダーから様々な派生版キルチェーンが発表されており、Vectra Networks 社は図 3. 2「Vectra Networks 社の想定する標的型攻撃キルチェーン」を提唱している。Vectra Networks 社の想定する標的型攻撃キルチェーンでは、初期侵入後の挙動が、主にマネタイズを行うボットネットの構築と、データ窃取を目的とした従来型の標的型攻撃の 2 種類に分かれる点が特徴となる。このマネタイズでは、近年価値の上昇が著しい仮想通貨のマイニングがよく利用されている。標的型攻撃は C&C サーバと通信を繰り返しながら「内部偵察」、「内部拡大」、「データ獲得」と攻撃が進行し、最終的に、アクセス元制限などで守られているサーバ上のデータ(多くは機密データ)が持ち出される。（機密データの窃取）

図 3.2 Vectra Networks 社の想定する標的型攻撃キルチェーン

（出典：Vectra Networks, Inc.提供「Automated Threat Management in Real Time」）



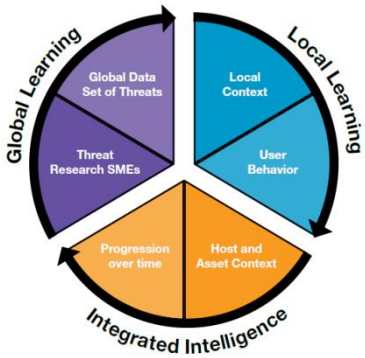
Vectra Networks 社製監視装置(以下、監視装置)はパッシブにキャプチャしたトラフィックを装置に内蔵されたＡＩにより分析し、キルチェーンの攻撃を可視化するアプライアンスシステムである。

3.2.2 機材（監視装置）の AI モデル

監視装置は以下の AI を採用している。

・Global Learning：教師付学習（例：ランダムフォレスト）
・Local Leaning：教師なし学習（例：k 平均法）
・Integrated Intelligence：相関分析／スコアリング（例：Bayesian network）

図 3.2 監視装置の AI モデル
（出典：Vectra Networks, Inc.提供「The data science behind Cognito AI threat detection models」）



Global Learning は Vectra Networks 社のラボ内で、研究者がトレーニング用データを監視装置に与えて検知力（未知の入力に対する「見分ける」能力）を向上させている。例えば、検知アルゴリズムの１つである「Suspicious HTTP」は、HTTP Header や User Agent の異常からマルウェアの疑いのある HTTP 通信を特定するものであるが、Global Learning によって作成されている。

Local Leaning は個々の監視装置が取得したネットワークトラフィックから通常状態のネットワークトラフィックの特徴を学習し、ベースラインを作成する。そのうえで、ベースラインから逸脱した通信を異常な振る舞いとして検知する。例えば、検知アルゴリズムの「Kerberos Client Activity」はホストの Kerberos 認証を学習し、ベースラインを作成する。そのうえで、通常とは異なる認証リクエストを発行した場合、異常とみなして検知するものであるが、この検知アルゴリズムは Local Leaning を構成する要素の１つとして採用されている。

Integrated Intelligence は検知した異常な振る舞いを相関分析し、スコアリング（Threat Score と Certainty Score）による脅威の優先度付けを行う。特に、標的型攻撃では多種多様な攻撃手段を用いてデータの窃取という最終目標の達成を目指すため、検知された異常な振る舞いの同士の相関をもとに、「ある標的型攻撃がどこまで進行しているか」「その進行している標的型攻撃の中で最もデータ窃取などの最終目標に近づいている異常な振る舞いはどれか」という脅威の優先度付けが重要となる。Bayesian network は因果関係の記述に優れたモデルの１つであり、他の相関分析モデルなどと併用して Integrated Intelligence を構成する。

3.3 研究方法

監視装置の活用方法を研究するためには、監視対象となるホストにマルウェアが感染し、キルチェーンに沿った攻撃が進行し、その振る舞いを監視装置が検知する必要がある。
監視対象ホスト（ハニーポット）上で攻撃が感染・進行するために、以下の３通りの方法を試み、監視装置が検知した攻撃の内容からマルウェアの特徴を捉えて、効果的な活用方法を研究・開発した。

- 攻撃の呼び込み：　ハニーポット内に攻撃を呼び込む（攻撃されるのを待つ）
- 検体の実行：　ハニーポット内で、事前にダウンロードしたマルウェア検体を手動で実行する
- 疑似攻撃：　ハニーポットに対して、研究者が自ら疑似攻撃を行う

3.3.1 攻撃・監視期間

「攻撃の呼び込み」、「検体の実行」、「疑似攻撃」は以下の日時に行いました。

- 攻撃の呼び込み：　2017 年 11 月 22 日開始（待機開始）
- 検体の実行　2017 年 10 月 6 日から（表 4.1.1「マルウェア検体の実行」を参照）
- 疑似攻撃：　2018 年 1 月 23 日から適宜疑似攻撃を実行
  （疑似攻撃を実行した同日に監視装置が検知しているため、検知日時を参照）

4 結果

4.1 可視化結果

4.1.1 実際の攻撃による可視化

4.1.1.1 攻撃の呼び込み

監視装置で特に検知される攻撃を呼び込むことはできなかった。ただし本研究環境を利用して名古屋大学側が実施した IDS の自動チューニングの研究において、ESXi 2 号機（「表 3.1b ESXi 2 号機」参照）のハニーポット群をオープンソースの IDS Surikata で監視したところ 162 個にシグネチャが反応するという結果を得ている Surikata ではシグネチャに反応があったのに対して監視装置において反応が無かった理由は、監視装置はマルウェアが侵入した後の振る舞いを分析・検知することに注力していることから、安全性を重視したハニーポットために、マルウェアがハニーポットに侵入したとしても動作までには至らず、侵入後のキルチェーン（侵入後の偵察、内部拡大等の振る舞い）へと進行しなかったものと考えられる。これは、不必要に多数のアラートを出してネットワーク管理者を疲弊させるよりは、散発的な個々の攻撃に対しては高い脅威度を示さずにおいた方が良いという考え方に沿う。もし、監視対象ネットワークにおいて細かな攻撃に対しての検知の必要性もある場合は、シグネチャ型 IDS を補完に用いる運用とする方法が考えられる。

なお、名古屋大学側で実施した IDS の自動チューニング研究については、低トラフィック量のハニーポットに対して多数のシグネチャを設定したチューニング情報収集用 IDS を設置し、得られたシグネチャ反応をもとに、高トラフィック量への耐性を必要とする実運用 IDS に設定するシグネチャを厳選するというも

のとなっている。以下のチューニング情報収集期間とチューニング結果検証期間における評価において、設定するシグネチャ数を 174 個へ絞った場合においても、デフォルトシグネチャから見逃し率を 34 ポイント改善するという成果を得た。

- チューニング情報収集期間（2017 年 12 月 23 日から 3 日間）
- チューニング結果検証期間（2017 年 12 月 27 日から 3 日間）
- シグネチャ：チューニング情報収集用 IDS に設定したシグネチャ：68,675 個
- Snort VRT Rules と Emerging Threat Rules

（出典：名古屋大学工学部電気電子情報工学科　大橋 宗治氏、名古屋大学情報戦略　長谷川皓一氏、名古屋大学情報基盤センター山口由紀子氏、嶋田創氏著　「ハニーポットへの攻撃に対する IDS 検知反応を利用したシグネチャの自動チューニング」 情報処理学会第 80 回全国大会予稿集 493-494 ページ 2018 年 3 月刊行）

4.1.1.2 検体の実行

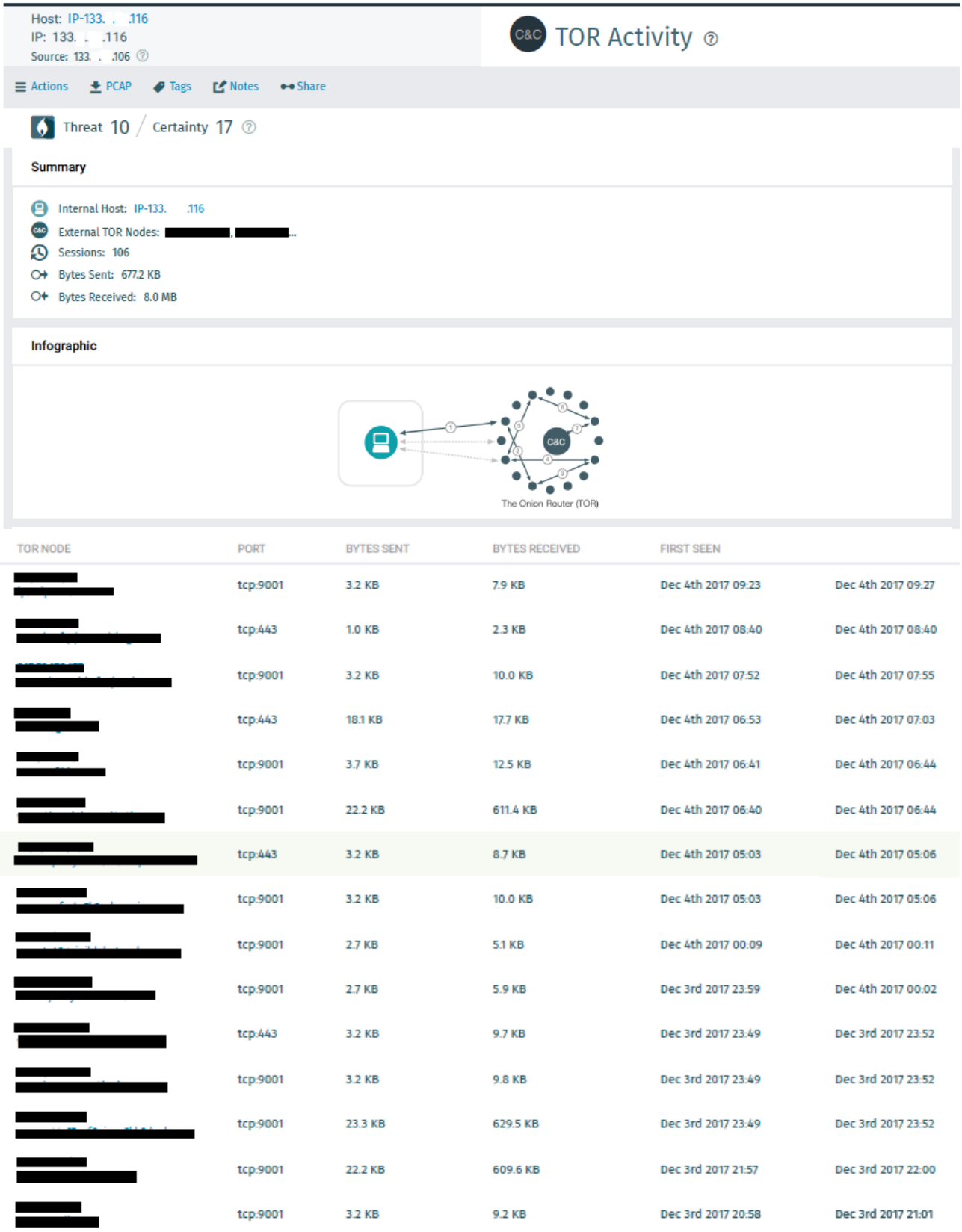
インターネット上の実マルウェア検体提供サービスから入手したマルウェアを ESXi 1 号機（「表 3.1b ESXi 1 号機」参照）のハニーポット群を構成する Windows7 クライアント上で手動実行し、1 週間程度の期間､監視装置において挙動を観測した｡表4.1.1(マルウェア検体の実行)に2017/11/8と2017/11/28の試行のまとめを記す。なお、各試行の前に、各 Windows7 クライアントはマルウェア感染の無いクリーンな VM に戻してある。

表 4.1.1 マルウェア検体の実行(11/8 および 11/28 の試行)

ファイル名	名称（symantec）	試行回数	実行ホスト	実行日時	挙動
hoge.exe	Backdoor.Trojan	1	cl1	2017/10/6 11:00	反応なし
vfd.exe	Backdoor.Trojan	1	cl1	2017/11/8 15:23	反応なし
uyitfu65uy	Ransom.Locky.B	1	cl2	2017/11/8 15:30	反応なし
ress.exe	Trojan.Nancrat	1	cl3	2017/11/8 15:32	xx.xx.xx.xxに10005で通信
sydney2.exe	Trojan.Gen	1	cl4	2017/11/8 15:47	疑わしいプロセスが起動
adeleke.exe	W32.Golroted	1	cl5	2017/11/8 15:41	反応なし
mnbv374	Infostealer.Lokibot	1	cl7	2017/11/8 15:51	反応なし
sxss.exe	Trojan.Gen.8!cloud	1	cl1	2017/11/28 14:30	反応なし、プログラム常駐
1100.exe	Trojan.Bebloh	1	cl2	2017/11/28 14:35	9001ポートに通信痕跡あり
file1.exe	Trojan.FakeAV	1	cl4	2017/11/28 14:40	反応なし
1201310150317521926.exe	Trojan.Gen.2	1	cl5	2017/11/28 14:43	反応なし
1201310141836074477.exe	Infostealer.Jackpos	1	cl7	2017/11/28 14:48	xx.xx.xx.xxと通信
JHgd476	Trojan.Horse	1	cl8	2017/11/28 15:05	反応なし

監視装置は cl1 において TOR（The Onion Router）の通信を検知した。図 4.1.1 に監視装置のウェブインタフェース上での検知結果の提示の様子を記す。TOR 通信の検知および脅威度と同時に、TOR の入り口ノードの IP アドレス、TOR とのセッション数、TOR との送受信バイト数、観測された通信の時系列が提示されている。それほど高くない脅威度が提示されているが、現時点での送受信バイト数が少ないため、脅威度を低目に提示し、他により脅威度の高い案件の優先処理を妨げないようにしていると推測する。cl1 以外のホストについては特に検知は無かった）

図 4.1.1 TOR Activity 検知(監視装置のウェブインタフェースより)



TOR NODE	PORT	BYTES SENT	BYTES RECEIVED	FIRST SEEN	
[redacted]	tcp:9001	3.2 KB	7.9 KB	Dec 4th 2017 09:23	Dec 4th 2017 09:27
[redacted]	tcp:443	1.0 KB	2.3 KB	Dec 4th 2017 08:40	Dec 4th 2017 08:40
[redacted]	tcp:9001	3.2 KB	10.0 KB	Dec 4th 2017 07:52	Dec 4th 2017 07:55
[redacted]	tcp:443	18.1 KB	17.7 KB	Dec 4th 2017 06:53	Dec 4th 2017 07:03
[redacted]	tcp:9001	3.7 KB	12.5 KB	Dec 4th 2017 06:41	Dec 4th 2017 06:44
[redacted]	tcp:9001	22.2 KB	611.4 KB	Dec 4th 2017 06:40	Dec 4th 2017 06:44
[redacted]	tcp:443	3.2 KB	8.7 KB	Dec 4th 2017 05:03	Dec 4th 2017 05:06
[redacted]	tcp:9001	3.2 KB	10.0 KB	Dec 4th 2017 05:03	Dec 4th 2017 05:06
[redacted]	tcp:9001	2.7 KB	5.1 KB	Dec 4th 2017 00:09	Dec 4th 2017 00:11
[redacted]	tcp:9001	2.7 KB	5.9 KB	Dec 3rd 2017 23:59	Dec 4th 2017 00:02
[redacted]	tcp:443	3.2 KB	9.7 KB	Dec 3rd 2017 23:49	Dec 3rd 2017 23:52
[redacted]	tcp:9001	3.2 KB	9.8 KB	Dec 3rd 2017 23:49	Dec 3rd 2017 23:52
[redacted]	tcp:9001	23.3 KB	629.5 KB	Dec 3rd 2017 23:49	Dec 3rd 2017 23:52
[redacted]	tcp:9001	22.2 KB	609.6 KB	Dec 3rd 2017 21:57	Dec 3rd 2017 22:00
[redacted]	tcp:9001	3.2 KB	9.2 KB	Dec 3rd 2017 20:58	Dec 3rd 2017 21:01

TOR 通信は、図 4.1.1 を含めて 2017 年 11 月 28 日、29 日、30 日、12 月 1 日、3 日、4 日、2018 年 1 月 8 日、9 日、10 日、11 日、12 日、13 日、14 日、15 日に検知している。(その後は観察していない)

4.1.1.3 疑似攻撃

表 4.1.1.3 「疑似攻撃」記載の攻撃を行ったところ、いくつかの擬似攻撃において監視装置が検知した。個々の擬似攻撃は、標的型攻撃のキルチェーンの各段階における典型的な攻撃を模倣しており、侵入したマルウェアが内部ネットワークをスキャン（偵察：Reconnaissance）し、サーバ（AD, FTP, ファイル共有等）を探す段階、および、見つかったサーバのアカウントを窃取（内部拡大：Lateral Movement）し、盗み出したアカウントを用いて、データを外部サーバへ持ち出す段階の攻撃を模倣している。

3.1.3 節に記したように、擬似 C&C サーバはインターネットを介した外部に設置してあり、構築に利用したソフトウェアは以下の通りである。

- 外部サーバ：
  - 仮想化基盤: VMware vSphere 5.5.0
  - OS: CentOS release 6.4　64bit 版
  - Web サーバ: Apache 2.2.15
  - WebDAV システム: BitKinex 3.2.3

表 4.1.1.3 疑似攻撃

模倣している攻撃	疑似攻撃手順（手動操作）	監視装置による検知	
		有無	検知内容
侵入したマルウェアが内部ネットワークを偵察する	nmap を使用して、ポートスキャンを実行する ターゲット：133.xx.xx.67 TCP ポート：21-25, 42, 53, 80, 110-113, 135-143, 199, 256, etc.	有	PortScan を検知 可視化情報： ターゲットアドレス、スキャン回数、成功・失敗回数
攻撃システム（ルートキットのようなもの）をダウンロードする	cURL を使用して疑似 C&C サーバ内にあらかじめ用意しておいたファイルを手動でダウンロードする # curl -k http(s)://（疑似 C&C サーバ上のファイルパス）	無	N/A
ポートスキャン後、侵入を受けて C&C サーバへ定期通信を開始 ⇒監視装置のキャンペーン機能に反応するかを検証する	cURL を使用して疑似 C&C サーバから疑似コマンドファイルをダウンロードさせるスクリプトを用意し、1 分おき、5 分おき、10 分おきの 3 パターンで 10 回以上を自動実行 # curl -k http(s)://(疑似 C&C サーバのグローバル IP)/(疑似コマンドファイルのパス、ファイル）/ >> NUL	無	N/A
FTP/FILE にブルートフォース攻撃し、ログイン ID を盗む	ブルートフォース攻撃システムを使用して、AD_Srv-113（FTP)サーバに対してログイン攻撃を行う ・user 名とパスワードの組みあわせでは 7000 組以上 ・約 7000 組の中に正解のログインパスワードが 1 組含まれている（1 組正解が含まれている） ・攻撃は 10 回行う ファイルサーバへは手動で数十回ログイン攻撃を行う（数十回に 1 度成功するように操作）	無	N/A
盗んだ FILE サーバのログイン ID/パスワードを用いてファイルを持ち出し	net use コマンドで対象ホストの共有フォルダにドライブマッピングし、データをコピーする # net use T: ¥¥(AD サーバの IP アドレス)¥neshare /user:victim01 (パスワードを入力） # copy コマンドでローカルディスクにコピーする WebDAV システムを使用して上記操作でコピーしたファイルを	有	Data Smuggler と Smash And Grab を検知 Data Smuggler: 内部ホストからデータを受けとり、受け取り後直ぐに外部ホストへ持ち出す振る舞い Smash And Grab:大きなサイズのデータが一度に持ち出された振る舞い

	疑似 C&C へ送る		

- WebDAV システム
  - 表 4.1.1.3 疑似攻撃の最終行で行っている外部ホストへのデータの持ち出しは、WebDAV システムを用いて手動で行った。（図 4.1.1.3　WebDAV システム「WebDAV システム」を参照）

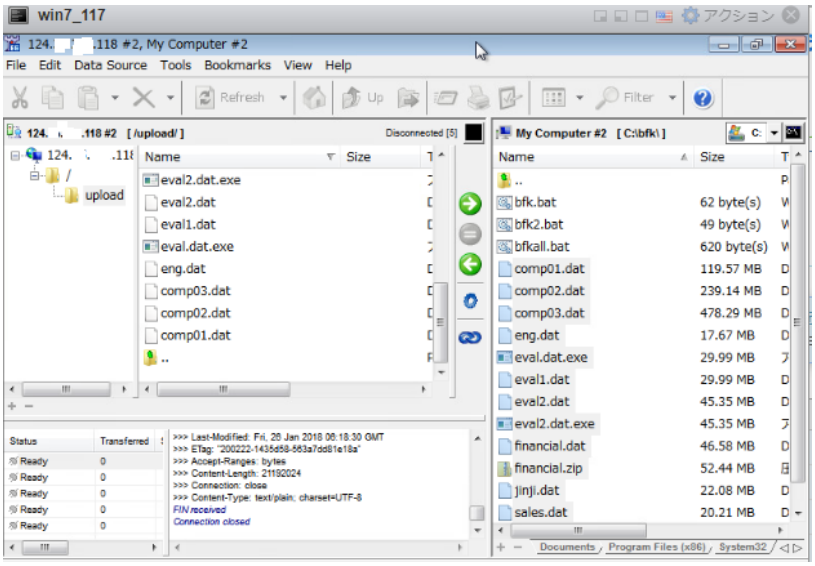


図 4.1.1.3　WebDAV システム

疑似攻撃用の WebDAV システムとして、本研究では BitKinex 3.2.3 を使用した。

事前に疑似外部サーバにインストールした Apache に WebDAV システムからアクセス許可設定（POST の許可）し、アップロード用のディレクトリ（/upload）を作成しておく。

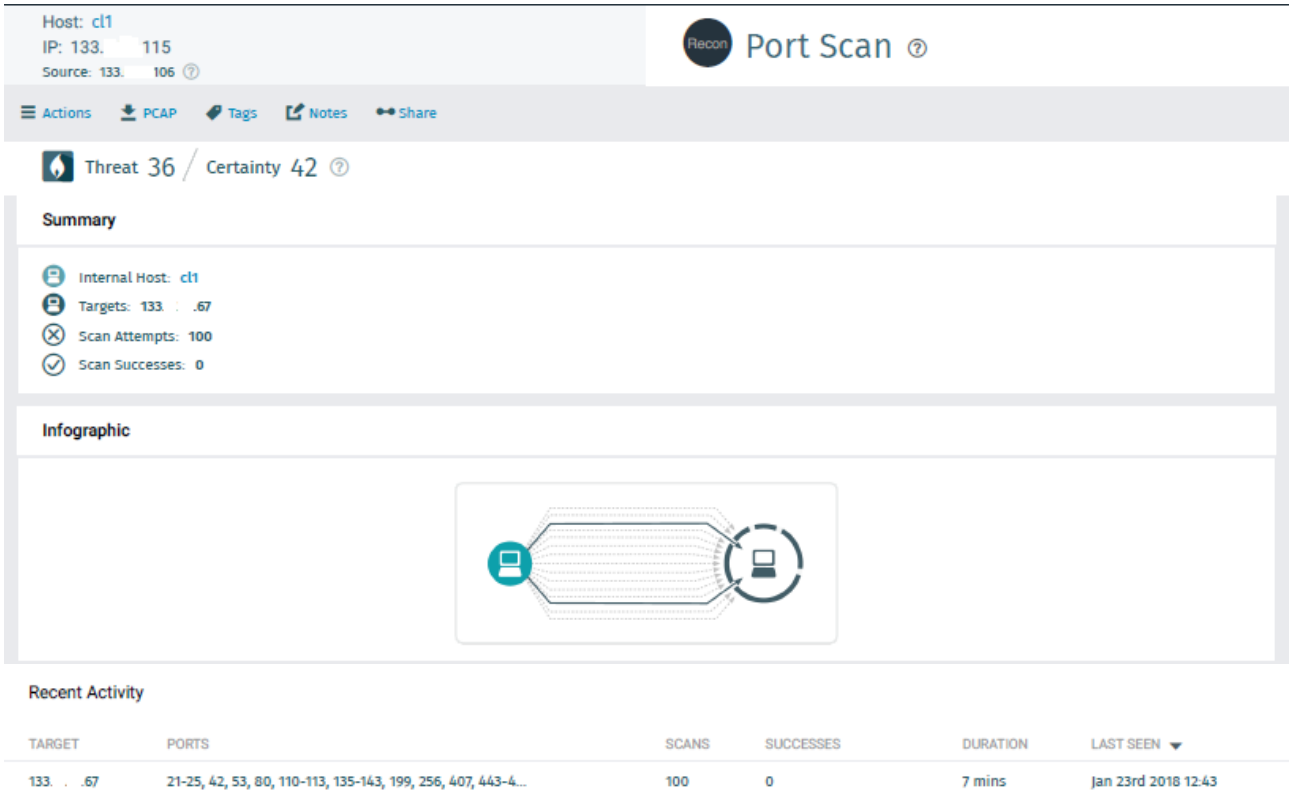
窃取した情報の送出の擬似攻撃においては、ハニーポット内の PC 上に WebDAV システムをインストールし、マウスによる操作（ドラッグ＆ドロップ）によりファイルを外部に持ち出す。

疑似攻撃により検知した各振る舞い（PortScan, Data Smugger, Smash And Grab）について説明する。

- PortScan 検知

図 4.1.1.3a （PortScan 検知）に監視装置のウェブインタフェース上での検知結果の提示の様子を記す。PortScan 元、PortScan 先、PortScan 回数、PortScan 成功数(応答のあった回数)、最近のスキャン活動の詳細が提示されている。ハニーポット内 PC（cl1: 133.xx.xx.116）が 133.xx.xx.67 に対して PortScan していることが検知されている。この振る舞いはマルウェアが内部ホストの中に攻撃対象を偵察する行為の 1 つである。今回の疑似攻撃では、FTP サーバ（21/TCP）や SMB プロトコルに寄るファイル共有（445/TCP）のサービスを提供しているホストを探している（スキャン）振る舞いを検知している。

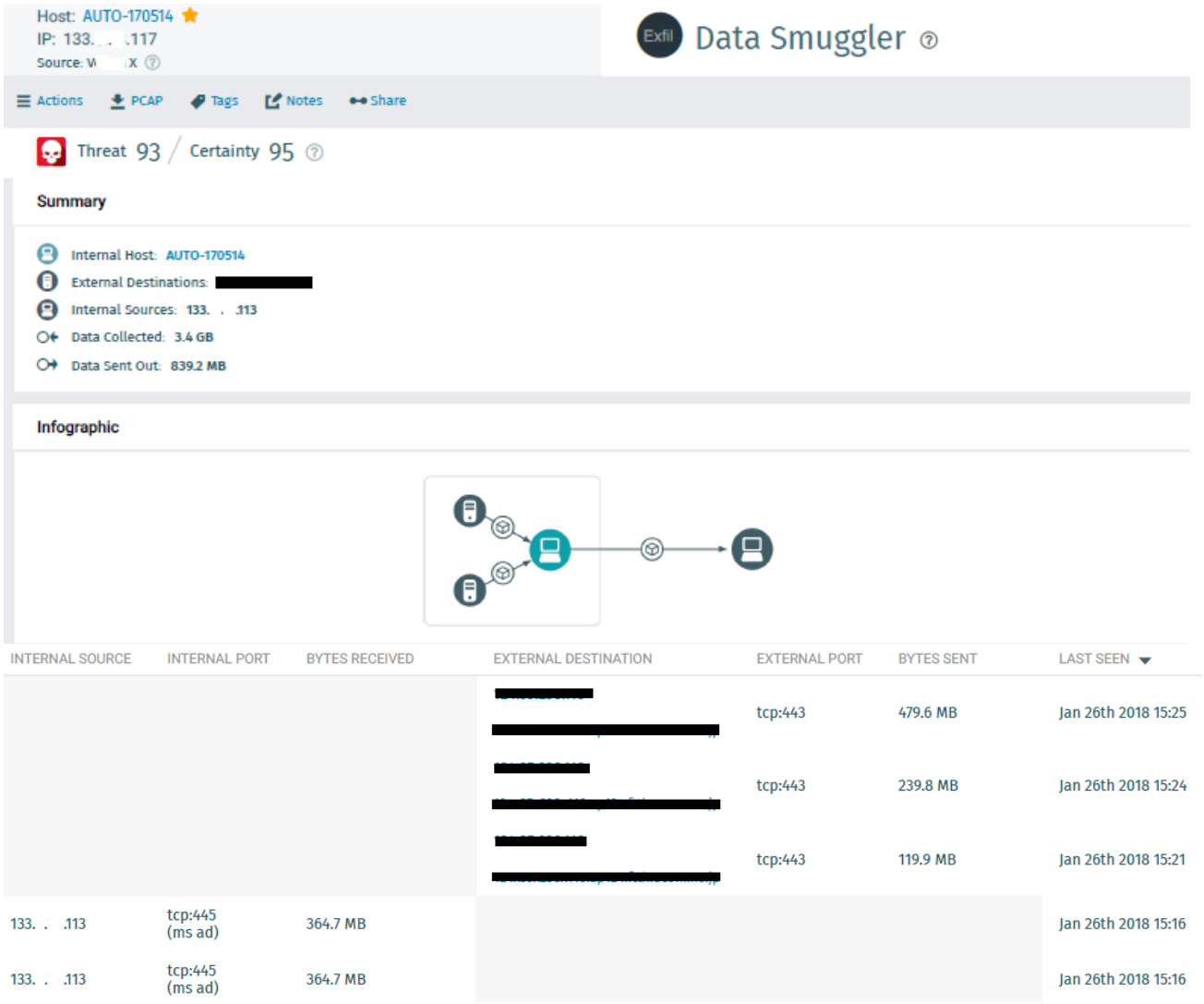
図 4.1.1.3a PortScan 検知(監視装置画面のウェブインタフェースより)



- Data Smuggler 検知

図 4.1.1.3b （Data Smuggler 検知）に監視装置のウェブインタフェース上での検知結果の提示の様子を記す。データ収集を行っている内部ホスト、内部の収集先ホスト、外部送出先ホスト、内部の収集先からの収集量、外部送出先への送出量が提示されている。提示された情報より、マルウェアに疑似感染したホスト（cl2: 133.xx.xx.117）がファイル共有サーバ（133.xx.xx.113）からデータを取り出し、引き続いて外部ホスト（134.xx.xx.118）に取り出したファイルを持ち出している振る舞いを検知している様子が見て取れる。この振る舞いは当該ホストが外部へデータを持ち出す際の中継サーバとなっていることを示しており、標的型攻撃のキルチェーンの最終段階にあたるため、高い脅威度数を与え、ネットワーク管理者に優先的に対応するよう促している。

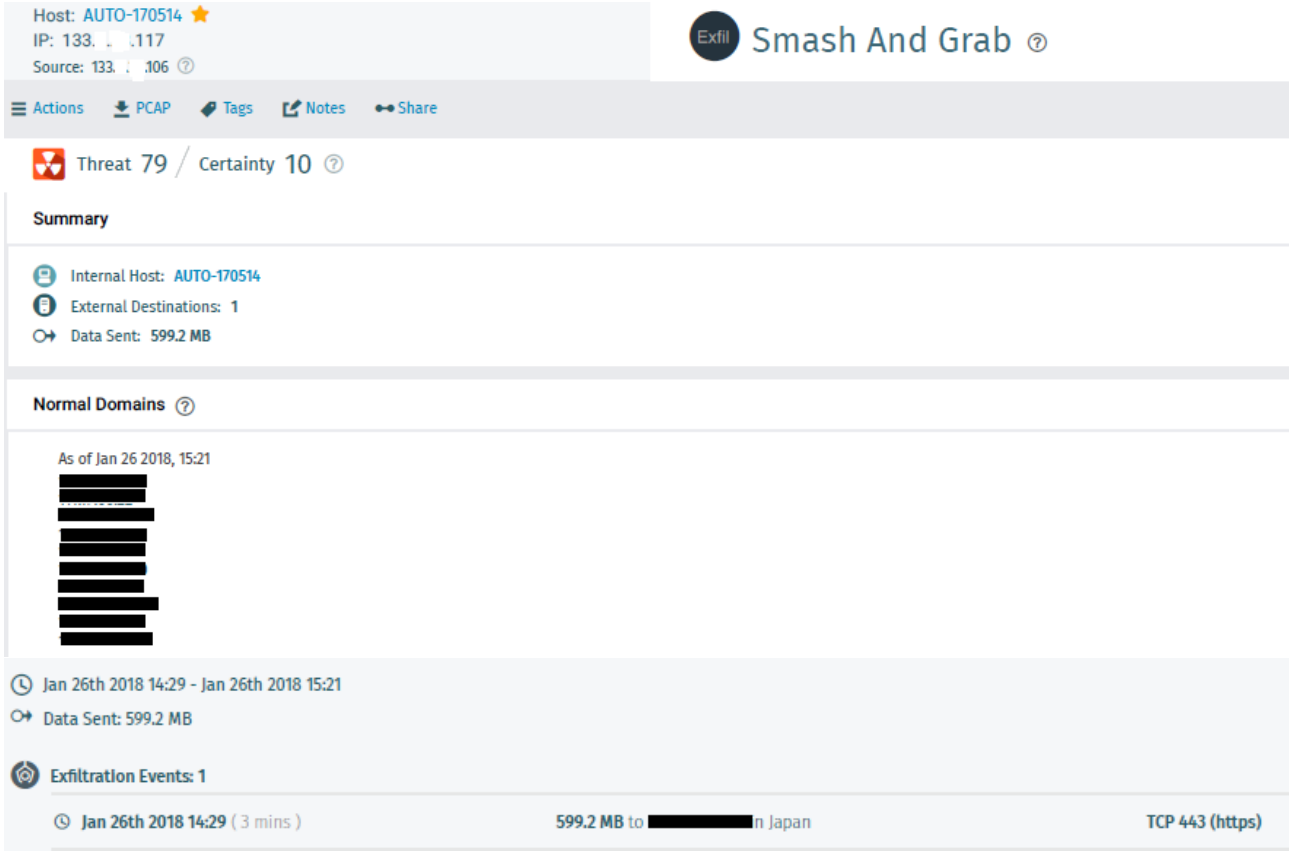
図 4.1.1.3 b Data Smuggler 検知(監視装置のウェブインタフェースより)



- Smash And Grab 検知

図 4.1.1.3c （Smash And Grab 検知）に監視装置のウェブインタフェース上での検知結果の提示の様子を記す。データ収集を行っている内部ホスト、外部送出先ホスト、外部送出先への送出量が提示されている。提示された情報より、マルウェア感染を模した挙動をするホスト（cl2: 133.x.x.117）が外部ホスト（134.x.x.118）に大きなサイズのデータを持ち出している振る舞いを検知している様子が見て取れる。Data Smuggler との違いは内部の収集先を中継しないことであり、大きなサイズのファイルを短時間に持ち出す場合に多くみられる振る舞いである。本擬似攻撃実験のように、Data Smuggler と Smash And Grab の両方の検知反応が出る事例も多い。

図 4.1.1.3 c Smash And Grab 検知(監視装置のウェブインタフェースより)



5 考察

5.1 検知結果について

- C&C の振る舞い

「4.1.1.2 検体の実行」の結果から、内部侵入したマルウェアの中には C&C サーバとの通信に TOR を利用するものがあると考えられる。HTTP(S)トンネル等の他の C&C 振る舞いは検知されておらず、マルウェア侵入後の初期段階の C&C 通信に TOR が使われていると考える。TOR やダーク Web を利用した C&C 通信が使われるとシグネチャによる防御は困難なものになるため、内部ホストと外部ホストとの異常な振る舞いを機械学習により検知・可視化する方法は有効である。

「4.1.1.3 疑似攻撃」の結果から、内部ホストと内部ホストの通信と、内部ホストと外部ホストの両方を合わせて監視することで、Data Smuggler のように中継サーバを介したデータの持ち出しの可視化が可能になる。

標的型攻撃の場合、攻撃者にとって価値のあるデータを見つけるまでの間に、偵察や内部拡大の指示・結果応答等の C&C が繰り返されると考えられるため、繰り返される C&C を相関分析することで Data Smuggler のようなデータ窃取に至る前に早期発見・対策できると推断する。近年の C&C は検知を逃れるために通信頻度の低減や HTTPS の利用など、一般通信から C&C をあぶり出すことが難しくなって来ている。長期的な観測をもとに相関分析が可能な本監視装置は、標的型攻撃対策として優れていると考えられる。

- Data Smuggler の振る舞い

「4.1.1.3 疑似攻撃」の結果から、別の内部ホストからデータを取り出し、そのデータの一部を外部ホストへ持ち出す振る舞いを検知している。これは、標的型攻撃で用いられる多種のマルウェアのうち、中継サーバの役割を担うマルウェアの振る舞いであるが、今回は疑似攻撃として手動で同じ振る舞いを行った場合も検知している。このことはマルウェアだけでなく、内部犯行を検知できる可能性を示唆している。一方内部犯行を検知できるということは、False-Positive として業務上許可された振る舞いを検知する可能性も含んでいる（例：業務ルールに沿って他ホストからログを収集して、外部分析サーバに送信した等）。したがって、マルウェアや内部犯行をシグネチャによる白黒判定ではなく、振る舞いによるグレーゾーンの可視化で行う場合は後述（5.1.1「False-Positive について」）する False-Positive に留意する必要がある。

またマルウェアの検知なのか、内部犯行（業務上妥当なものを含む）なのかを判定する方法のひとつに、C&C の検知有無を調べることが有効と考えられる。もし、C&C も検知されている場合はマルウェアの可能性が大きく、検知されていない場合は内部犯行の可能性が大きいと考えられる。

- Port Scan / Smash And Grab の振る舞い

「Data Smuggler」 同様に、手動操作（疑似攻撃）により検知している。Port Scan は内部ネットワークの中で、TCP/UDP ポートサービスが提供されているホストを探す振る舞い（偵察）であり、Smash And Grab は大きなサイズのデータを外部ホストに持ち出している振る舞いを検知している。いずれの場合も「Data Smuggler」同様に False-Positive に留意する必要がある。

5.1.1 False-Positive について

内部ネットワークに侵入した標的型攻撃用マルウェアはシグネチャによる防御を主とする境界防御を突破してきたものであり、シグネチャによる白黒判定の検知は有効でないと考えられる。振る舞いによる判定はグレーゾーンを可視化できるが、明確な白黒判定ではないため False-Positive を軽減する仕組みが必要不可欠なものになる。なお、ここで言う False-Positive は、誤検知と過検知やノイズを明確に分けて捉えるべきである。例えばデータが持ち出されていないのに、持ち出したと検知した場合は誤検知、持ち出されてはいるが業務上妥当な振る舞い（許可された持ち出し）の場合は過検知、業務上の妥当性はなく、故意または過失によるものはノイズと定義し、運用を考察する。

False-Positive をここでは以下の 3 つに分類・定義する。

- 誤検知
  当該振る舞いが行われていないのに、行ったとして判別されたもの
  原因と対策：監視装置の検知アルゴリズムのチューニングやバグ等を改修する
- 過検知
  当該振る舞いが業務上妥当なものや、C&C 通信相手／データ持ち出し先等と検知された外部ホストは、実際には関連企業・団体等、業務上問題がない通信相手であった場合等
  原因と対策：当該振る舞いや通信相手をホワイトリスト化
- ノイズ：
  過失等による業務上妥当性の無い操作、退職者 PC／撤退システム等が残っている等
  原因と対策：内部ネットワークに負荷をかけており、また実際に標的型マルウェアに攻撃された場合に、発見の邪魔（木を隠すには森の中状態）になるため、クリーンナップすべきもの

誤検知については検知システムベンダー（本研究においては Vectra Networks 社）へ依頼または共同開発することになるが、過検知とノイズについては「運用」でカバーすることができる。

5.2 運用システムの開発について

効果的且つ効率的な運用を開発するために、装置の能力の他、運用の仕組みと運用する人を考慮する必要がある。装置の能力としては、「検知力の向上」が最も重要であるが、前述の過検知／ノイズの判別のための他システムとの連携やインシデント対応のために関連組織とのコラボレーションの仕組み、そして運用・設計する人材の育成を考慮しなければならない。

- 検知力の向上
  - 検知能力の向上による検知感度の向上と誤検知の軽減
- 運用の向上
  - システム連携とコラボレーションの仕組み
- 人材育成
  - 仕組み自体の設計、ノウハウの共有と蓄積等

5.2.1 検知力の向上

検知力の向上のためには、検知感度／精度を上げることと、検知する適応範囲を拡大するという 2 つが必要と考える。検知感度／精度を上げるためには新手のサイバー攻撃を予測し、検知アルゴリズムを強化することである。適応範囲を広げるためには、例えば IoT や ICS(Industrial Control System)で使用されているプロトコルに対応していくことが必要である。IoT はプロトコルの標準化が進む中、業界標準となるプロトコルを見極めていく必要があり、ICS については分野（例えば、電力、化学プラント等）ごとに独自プロトコルが存在するため、対応していくための絞り込みと独自のプロトコルを実装している各分野のベンダとの共同開発が必要になる。

5.2.2 運用の向上

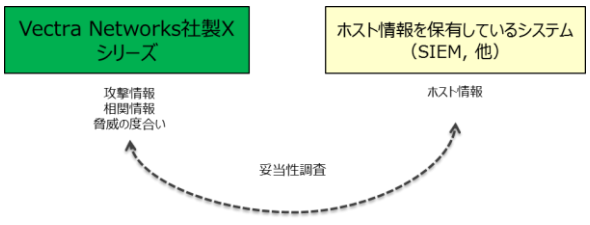
可視化したマルウェアの情報には False-Positive(誤検知、過検知、ノイズ)が含まれており、これを判定するためには検知した振る舞いが業務上妥当なものか否かを調査する必要がある。妥当性が確認できない場合には、インシデントとして影響範囲や優先度を把握・共有した上で関係部署と連携して対応することになる（コラボレーション）。

したがって監視システム（または監視システムと他システムが連携したシステム）は以下の情報を提供する必要がある。

- False-Positive 判定のために業務上妥当なものであるかを確認できる情報
  - 攻撃情報：ホスト名、IP アドレス、攻撃情報（タイプ、キルチェーン、タイムスタンプ、データ量、外部サーバアドレス）、他
  - ホスト情報：当該ホストの OS、使用ソフトウェア、所有者情報、他
- 重要度合いを計数化して、優先度付けできる情報
  - 脅威の度合い： スコア、グラフ、他
  - 相関情報：他に検知されているものとの相関、外部脅威情報の共有、他

監視装置は上記のホスト情報を除いたもの（攻撃情報、脅威の度合い、相関情報）が提供されているので、ホスト情報を SIEM(Security Information and Event Management)等のホスト情報を保有しているシステムと連携することでカバーできると考える。システム連携の手段として、監視装置もサポートしている syslog や REST API（システムの双方向コミュニケーションのために GET メソッドだけでなく、 POST も実装されることが重要）、そして最近登場し始めたオーケストレーションツールの利用が有力と考える。また関連組織とのコラボレーションに必要な脅威情報の共有の手段として STIX(Structured Threat Information Expression)は有力な 1 つの候補と考える。

図 5.2.2 妥当性調査のための連携システム



5.2.3 人材育成

攻撃の可視化（脅威検知、攻撃の特徴、俯瞰的可視化等）を行うためには膨大なデータソース（ログ、トラフィック等）を分析する必要があり、人が行うことはもはや困難である。AI（機械学習で得られた知識

からマルウェアの特徴や状況を推論）が担っていくことが望ましいと考える。人は攻撃の可視化は行わず、AI から得られた可視化情報を活用して素早く対応することと、ネットワークの利便性を損なうことなく防御の仕組みを設計することに注力すべきである。したがって、インシデント情報を基に迅速に対応できる人材と、コラボレーションの仕組み作りや人材育成自体の仕組みを設計できる人を育成することが重要である。その第一歩として、攻撃可視化の分野には積極的に AI を導入すべきと考える。

6 結論

6.1 まとめ

標的型攻撃は高度な技術を利用し巧妙化が進んでいると同時に、目的(データ窃取など)を達成するために手段をかえつつしつこく攻撃を続けて来る傾向が、引き続き観測されている。そのため、従来型のシグネチャベースの境界防御だけでは不十分であり、境界防御を突破して内部ネットワークに侵入したマルウェアが潜伏しつつ攻撃を進行させる段階において早期発見・対応する仕組みがますます重要となっている。

境界部よりも通信量の多い内部ネットワークにおいて脅威を検知・可視化するためには、膨大なデータソース（ログやトラフィック）を収集・分析する必要があり、機械学習と可視化するための推論を備えたＡＩの活用が必要不可欠である。可視化したマルウェアを False-Positive であるか否か判別するためには、検知した振る舞いが業務上妥当なものであるか否かを調査・確認する必要があり、妥当でない場合はマルウェアの情報を他部署と共有し、インシデントとして対応しなければならない。そのための社内外組織とのコラボレーションや業務情報を照合するためのシステム連携が重要な鍵となる。システムとの連携やコラボレーションに必要な情報共有の手段として REST API と STIX などが有力候補と考える。

攻撃の可視化を AI に任せ、システム連携とコラボレーションによる効果的な運用が進むと、人は「インシデント発生時の迅速な意思決定と行動」と「安心・安全、且つ利便性のあるネットワークを維持しつつ、効果的な防御の仕組み作り」に注力することができる。そのような人材を今後育成していく必要がある。

本研究では運用の具体的な開発にまでは至っていないが、開発へ向けての方向性を提示できたと考える。本研究で使用した監視装置（Vectra Networks 社製品）は AI を活用した内部ネットワークのスコアリングによる優先度付けや俯瞰的可視化、更に、他システムとの連携に必要な REST API や外部脅威情報を共有するための STIX のインポート／エクスポートを提供しており、過検知／ノイズ調査やインシデント対応のコラボレーションの仕組みを具体的に設計することが可能と推断する。今後は他システムとの具体的な連携設計やコラボレーションのガイドライン策定へと繋げていきたいと思う。

7 参考文献

参考文献：

「ハニーポットへの攻撃に対する NIDS 検知反応を利用したシグネチャの自動チューニング」（情報処理学会第 80 回全国大会）
　名古屋大学工学部電気電子情報工学科　大橋 宗治氏、名古屋大学情報戦略　長谷川皓一氏、名古屋大学情報基盤センター山口由紀子氏、嶋田創氏
「人工知能は人間を超えるか　ディープラーニングの先にあるもの」（東京大学准教授　松尾豊氏著、株式会社 KADOKAWA）
Wikipedia（キーワード：「キルチェーン」）
「Understanding.ai」、「The data science behind Cognito AI threat detection models」Vectra Networks, Inc.

登録商標：

以上