簡単お手軽異常検知

JANOG41ミーティング発表資料

2017年1月26日

シスコシステムズ合同会社
石川 章史

自己紹介

- 石川 章史(いしかわ あきふみ)
- シスコ12年目(弊社でこの勤続年数はベテランと言われる)で，セキュリティ製品の設計やセキュリティのコンサル業務を経て，現在はSOCで働いております。
- ちなみに「シスコさんのSOCって北米にしかないんでしょう？」と尋ねられることがありますが，アメリカ，ポーランドそして日本にもSOCはあります。
- ルーティングは RIPv2 VLSMぐらいまでの知識で止まってますので，ルーティングのことは聞かないでください。

目的など

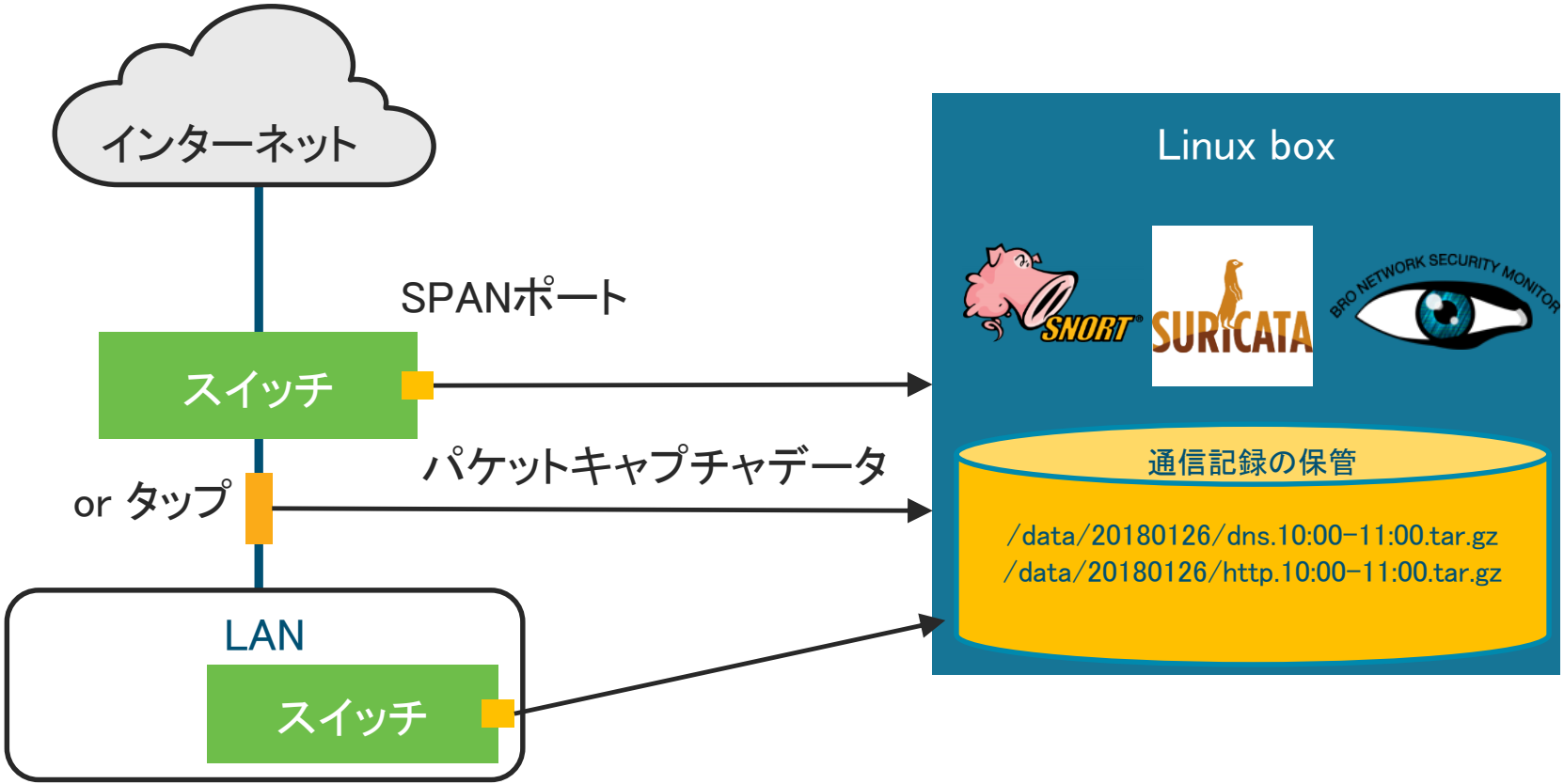
- ネットワークやホストの振る舞いにおいて，何かインシデントの予兆となるようないつもと異なるイベントを見つけたい
- バッファオーバフロー攻撃など，いわゆる攻撃の検知とは異なり，ベンダの準備する IDS/IPSのルールは普段と異なるイベントの検知には向かない
- AlertやSyslogはあくまで機器が反応した結果の出力であり，これらの機器が反応しなければ何もわからない
- 正当な通信を含めた通信記録には何かヒントがあるはず。とりあえず通信を記録して，ちょっといつもと違うルールは後で考えることに

IDS/IPS/NMSツール

- 通信を記録するために使用できる代表的なツール
  - Suricata
    - https://suricata-ids.org
  - Bro
    - https://www.bro.org
  - Snort
    - https://www.snort.org

(*) インストールや設定方法は上記サイトをご参照ください

システム構成


インターネット
SPANポート
スイッチ
パケットキャプチャデータ
or タップ
LAN
スイッチ
Linux box
SNORT
SURICATA
BRO NETWORK SECURITY MONITOR
通信記録の保管
/data/20180126/dns.10:00-11:00.tar.gz
/data/20180126/http.10:00-11:00.tar.gz

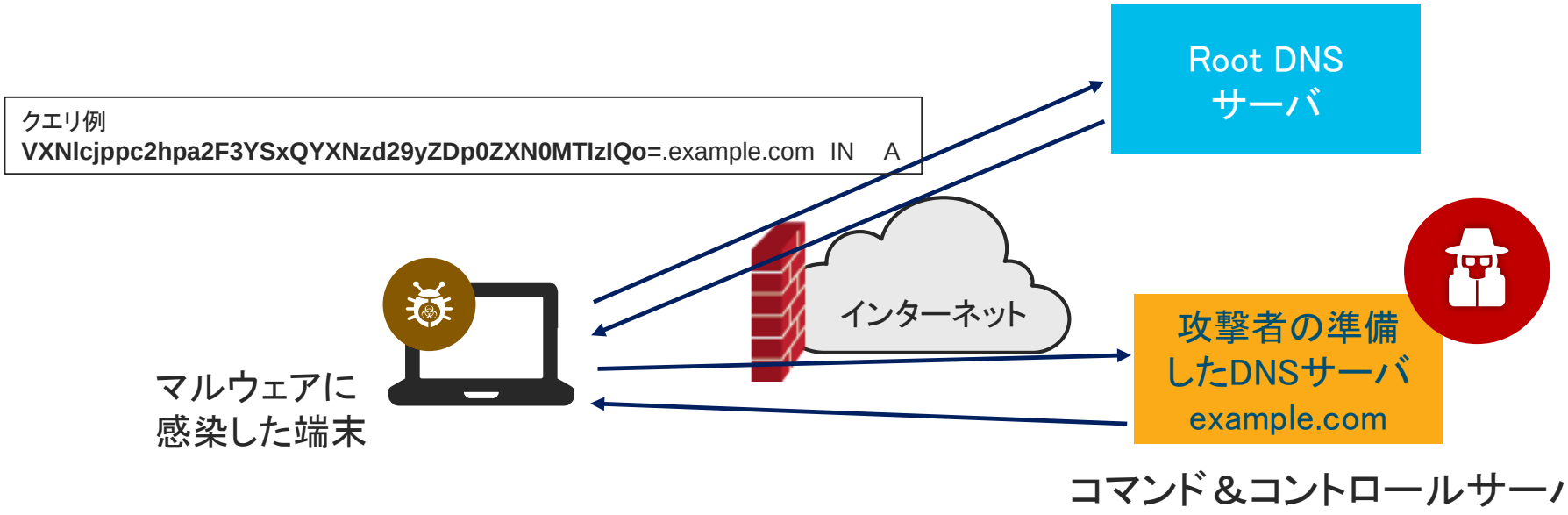
通信記録の保管

- スイッチのSPANポートやタップ機器などから取得したパケットキャプチャデータを Linux BOXに入力し，Snort/Suricata/Broなどのツールですべて（機器がとりこぼさない限り）記録
- 紹介したツールはパケットキャプチャデータをテキストへ変換して保存可
- プロトコル別に 1時間毎に保存
  - /data/20180126/dns.10:00-11:00.tar.gz
  - /data/20180126/http.10:00-11:00.tar.gz
- 例. DNSクエリ＆レスポンス

生成時間	Source IP	Port	Destination IP	Port	Protocol	Transaction ID	Query	RR	Response
1516801833	198.51.100.1	33835	203.0.113.110	53	udp	31579	www.example.com	A	192.0.2.10

異常な通信の例: DNSトンネリング

- 攻撃者は予めドメイン(example.com)を取得し，DNSクエリが自身の準備したNSサーバに到達するようにする。



DNSトンネリングパケットの例

- ホスト名に情報を埋め込み，何らかのエンコーディングをして外に送信
- コマンド＆コントロールサーバとの通信に使用され，時には情報漏えいなども
- 例 BASE64によるエンコード

VXNlcjppc2hpa2F3YSxQYXNzd29yZDp0ZXN0MTIzIQo=.example.com

  - ホスト名部分をデコードすると　User:ishikawa,Password:test!

簡単お手軽検知ルール

- シンプルに 30文字の以上のホストをひっかける
  - # zcat /data/20180126/dns.10:00-11:00.tar.gz | cut -f9 | egrep '.{30,}'

- もちろんDNSトンネリングが検知ができますが，誤検知も発生するためホワイトリストが必要。最近のホスト名は長い....

誤検知。そしてホワイトリスト行き

(1) 動的 IP系
hostXXXXXXX-static.YYYYYYYY.retail.telecomitalia.it

(2) クラウド系
ioc-testX-apilb-XXsXXXXXX-YYYYYYYY.us-east-X.elb.amazonaws.com

(3) 灯台下暗し系
1-a0acab665808f62a584426b26abf6a.rf-adfe2ko9.senderbase.org

一定期間の運用後，誤検知は減りテスト用のDNSトンネリングパケットは検知できた

その他のルール：資産管理システムに基づく未知のサーバ検知ルール

- 例. HTTP Proxy通信
  - 通信記録

生成時間	Source IP	Port	Destination IP	Port	Type
1516801833	198.51.100.1	33835	203.0.113.1	8080	Tunnel:HTTP

  - 既存サーバを資産管理システムから抽出
    - Proxyサーバ1: 203.0.113.1
    - Proxyサーバ2: 203.0.113.2
    - Proxyサーバ3: 203.0.113.3
  - 未知のIPアドレスが Proxyとして動作した場合にひっかける
    - # zcat /data/20180126/tunnel.10:00-11:00.tar.gz. | cut -f5 | grep -vw “203.0.113.1” | grep -vw “203.0.113.2” | grep -vw “203.0.113.3”

Proxyに限らずあらゆるサーバの検知が可能

まとめ

- 環境に応じたホワイトリストが作成できれば非常に高精度なルールになる
- 最終防衛ラインのようなものかもしれない。このようなシンプルなルールが何らかのインシデントを検知した時は既に重大インシデントが発生しているかもしれない
- 高度化する攻撃を検知するためには何重にも検知ルールの網をかけるべき。そういった観点では有効だと考える
- grep, cutそして awkは最強!
- ホスト名は短くしてください....
- 近い将来AIが誤検知無しで見つけてくれるはずなので将来的にはそれに期待
- 副次的な効果として，通信履歴の取得はマルウェア感染端末の過去の通信先のチェックなど有効利用可

ご清聴ありがとうございました。


CISCO