PIPELINE
ACTIONABLE CYBER THREAT DATA

DNS監視技術によりネットワークのパフォーマンスを劇的に改善させた某ISPの導入事例

" お客様のデータを最大限に引き出し、
「重大な意思決定」時に
よりよい成果を生み出し続けるサポートをいたします。 "

会社概要

PIPELINE Security はインフラ、 Eメール、クラウド、ウェブ・アプリケーションへ革新的なデータインテリジェンスソリューションを提供している日本のプロバイダーです。これまで日本、アジア、中東の最大手通信会社、MSP,CSP, ISP様よりご導入いただいております。

社名	**PIPELINE株式会社**
オフィス	東京、シンガポール、ダッカ
HP	http://www.pipelinesecurity.net
設立年	2015年1月22日
資本金	1,000万円
従業員	21人
事業内容	Spamhaus, SURBL, Scamadvisor データ管理者（アジア・中東・アフリカ） IOC・脅威データプロバイダー クラウド・アプリログの管理と分析 モニタリング、オプティマイゼーション データ・インテリジェンス・サービス・プロバイダー AI、ディープラーニング、機械学習

製品・ソリューション：幅広い産業に導入

製品			ソリューション		サービス	
Fense	Threat IDR	DatalaiQ	脅威情報	Vision	アナリティクス インテリジェンス	SecOps

企業　ISP MSP TEL　製造　大学　医療　金融

セキュリティ２０２１：トータルソリューションをご提供

区分	商品名	商品特徴
製品	Fense	• Endpoint Security • プライバシー、監視、保護
	DatalaiQ	• 効果的なログの集中管理 • セキュリティ・アナリティクスとインテリジェンス
ソリューション	脅威情報	• セキュリティ・データ・フィード
	Vision	• データフィードの管理ソリューション
サービス	アナリティクス インテリジェンス	• ログによる検知・応答サービス • AI、ディープラーニング、機械学習
	SecOps	• DevSecOps & SecOps Service

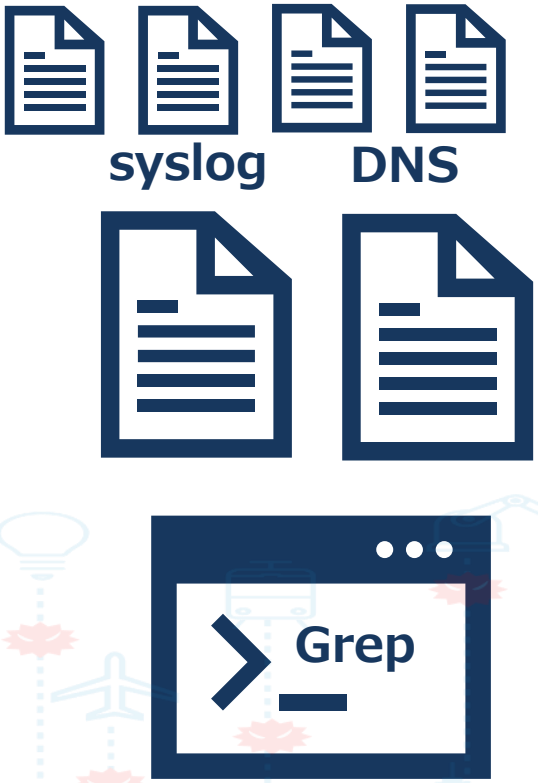
お客様について

企業、住宅、公共施設向けに、無線や光ファイバによる接続サービスを提供する大手ISP。また、インターネットサービスに加えて、CDN、VPS、コロケーションなどで構成されるデータセンターを運営し、インターネットエクスチェンジに直接接続しています。

お客様の課題について

- お客様のユーザーは一般家庭と企業の両方のユーザーが混在
- マルウェアのダウンロードやアクセスに気づかず、**ボットネット**となって不要なトラフィックを送信してしまうユーザー（**DNS Amp**）
- 詐欺的なサイトにアクセスして、**データ情報が漏洩**するユーザー
- メールスパム、クリプトジャッキング、または攻撃によりパブリックIPがブロックされ、**レピュテーションやサービスに支障**

既存のアプローチ



- grep、syslog、linuxの伝統的なツールを使った調査
- 不要なトラフィックを効果的に監視するために、ユーザーのルーターをモニター
- 異常なトラフィックを検知するために、被害者の送信元アドレスのリストを作成するスクリプトを設計
- 公共のインターネットサービスでは、特定の受信および送信トラフィックにアクセス提供

既存のアプローチ

既存のアプローチが効果的であると思われる一方で、問題が大きくなっていることは明らかでした。

1. ファイアウォールのルールが**特定のルーター**を持つユーザー様にしか実装できてない。
2. 感染したユーザーやメンテナンス時に導入するルールを**手動で設定**している。
3. ユーザーからの報告、フィードバック、コールセンターが**マルウェア**の唯一の検出手段である。
4. **DDoSやその他の悪意**のあるトラフィックを生み出す感染したユーザーが全体的のネットワークを通過している。

新たなソリューションの必要条件

1.ユーザーのプライベートデータやトラフィック必要としまない

2. ユーザーに最小限のリソースで集中的なモニタリング・保護

3. DNSデータをゾーンに分割すること

4. ブロックとバイパスは、特定のドメインとサブドメインに対して選択できること

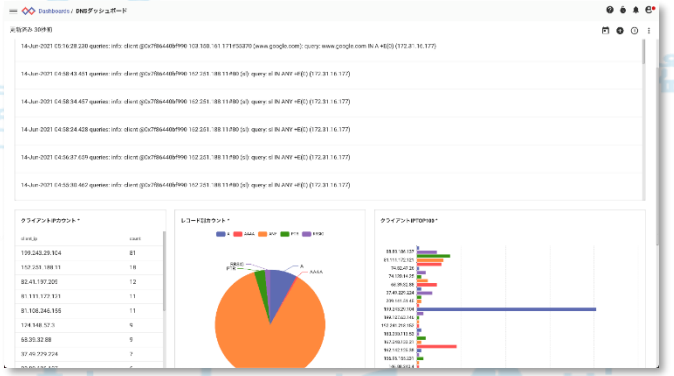
弊社が提供したソリューション

1. 不要なオーバーブロッキングを防ぐための
   データクリーニングサービスを提供

2. カスタムRPZデータフィード管理ポータルを実装

3. DNSデータ分析ダッシュボードを構築して、
   脅威のハンティングと異常検出を支援

4. 興味深いデータのソースを追加して、
   さらなる相関関係と分析を可能にする。



DNSクエリによるデータ流出の検出

不審なクエリの大量発生

DGAドメインのようにランダムな文字で表示される

特定のドメインに対して変なサブドメインクエリが生成される。

MTyUE20352x325kdafj…. これ何？

Name	A
MTkyLjE2OC4xMzEuMToxMzk9TklM.10086hyl.com.	
MTkyLjE2OC4xMzEuMToxMzU9TklM.10086hyl.com.	
MTkyLjE2OC4xMzEuMTo0NDU9TklM.10086hyl.com.	
MTkyLjE2OC4zLjE6MTM5PU5JTA.10086hyl.com.	
MTkyLjE2OC4zLjE6MTM1PU5JTA.10086hyl.com.	
MTkyLjE2OC4zLjE6NDQ1PU5JTA.10086hyl.com.	
MTAuMTAuMTAuMTA6MjI9TklM.10086hyl.com.	
MTAuMTAuMTAuMToyMj1TU0gtMi4wLU9wZW5TU0hfNy42cDEgVWJ1bnR1LTQNCg.10086hyl.com.	
MTAuMTAuMTAuMjM6MTM5PU5JTA.10086hyl.com.	
MTAuMTAuMTAuMjM6MTM1PU5JTA.10086hyl.com.	
MTAuMTAuMTAuMjMvMjQ.2596996162.net.10086hyl.com.	
MTkyLjE2OC4zLjEvMjQ.2596996162.net.10086hyl.com.	
10086hyl.com.	

（サンプル）

DNSクエリによるデータ流出の検出

特定のドメインに対して変なサブドメインクエリが生成される。

サブドメインのクエリはbase64でエンコードされていました。
感染したノードのスキャン結果がクエリによって流出していた

Decode: Base64
10.10.10.1:22=SSH-2.0 Ubuntu

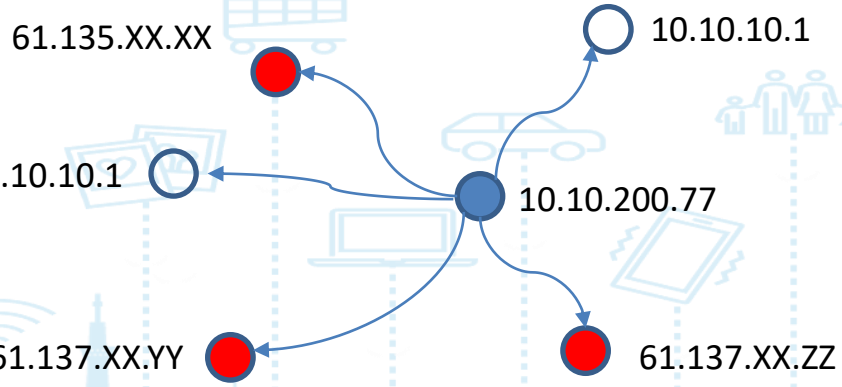
sub	decode
MTkyLjE2OC4xMzEuMToxMzk9TklM	192.168.131.1:139=NIL
MTkyLjE2OC4xMzEuMToxMzU9TklM	192.168.131.1:135=NIL
MTkyLjE2OC4xMzEuMTo0NDU9TklM	192.168.131.1:445=NIL
MTkyLjE2OC4zLjE6MTM5PU5JTA	192.168.3.1:139=NI
MTkyLjE2OC4zLjE6MTM1PU5JTA	192.168.3.1:135=NI
MTkyLjE2OC4zLjE6NDQ1PU5JTA	192.168.3.1:445=NI
MTAuMTAuMTAuMTA6MjI9TklM	10.10.10.10:22=NIL
MTAuMTAuMTAuMToyMj1TU0gtMi4wLU9wZW5TU0hfNy42cDEgVWJ1bnR1LTQNCg	10.10.10.1:22=SSH-2.0-OpenSSH_7.6p
MTAuMTAuMTAuMjM6MTM5PU5JTA	10.10.10.23:139=NI
MTAuMTAuMTAuMjM6MTM1PU5JTA	10.10.10.23:135=NI
MTAuMTAuMTAuMjMvMjQ	10.10.10.23/
MTkyLjE2OC4zLjEvMjQ	192.168.3.1/
10086hyl	◆M<◆⊙◆
MTAuMTAuMTAuMjM6NDQ1PU5JTA	10.10.10.23:445=NI

（サンプル）

スレットハンティングwith DNSが可能になった

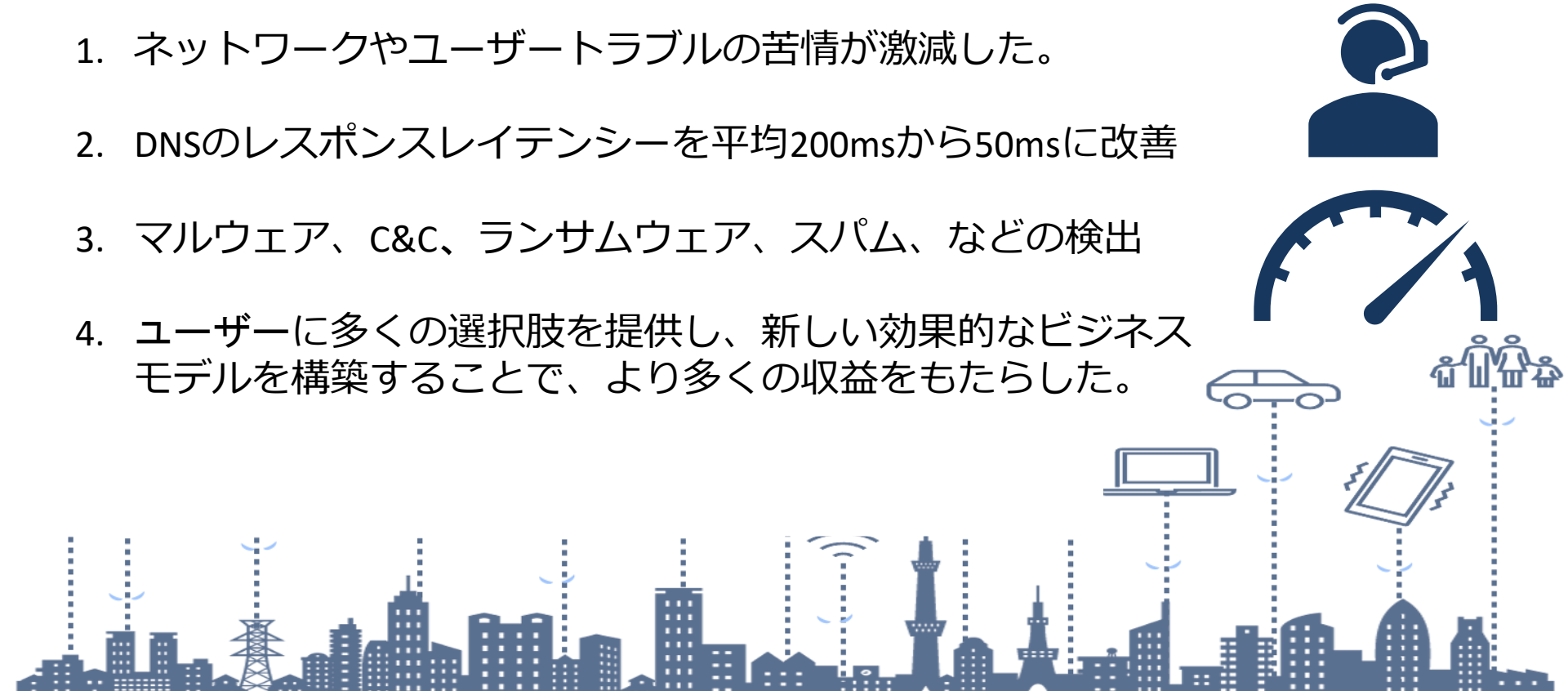
タイムスタンプ	ドメイン	Aレコード	カテゴリー	ローカル	リモート
Mar 18th, 2021 @ 02:22:51.970	c2domains1.com		attackpage	10.10.10.1:53	10.10.200.77:46478
Mar 18th, 2021 @ 02:23:11.662	c2domains2.com	61.135.XX.XX	attackpage	10.10.10.1:53	10.10.200.77:41839
Mar 18th, 2021 @ 02:24:13.662	c2domains3.com		attackpage	10.10.10.1:53	10.10.200.77:34266

1. DomainとIPを特定する
2. タイムスタンプの前後に他の通信
3. Netflow, Bro ,sflowなどの相関関係



皆様にとってどれくらいの価値がありますか？

1. ネットワークやユーザートラブルの苦情が激減した。
2. DNSのレスポンスレイテンシーを平均200msから50msに改善
3. マルウェア、C&C、ランサムウェア、スパム、などの検出
4. ユーザーに多くの選択肢を提供し、新しい効果的なビジネスモデルを構築することで、より多くの収益をもたらした。



独自のDNSインテリジェンスを構築する方法を知りたいですか？

SCAN ME

Thank you DNS Summer Days 2021!

www.pipelinesecurity.net

お問い合わせ

シンプルでインテリジェントな集中データ・ログ管理構築をサポート

パイプライン
PIPELINE

お客様のデータを活用して、より良い意思決定を行います。