進化を続ける攻撃手法に対するF5のソリューションと適用例

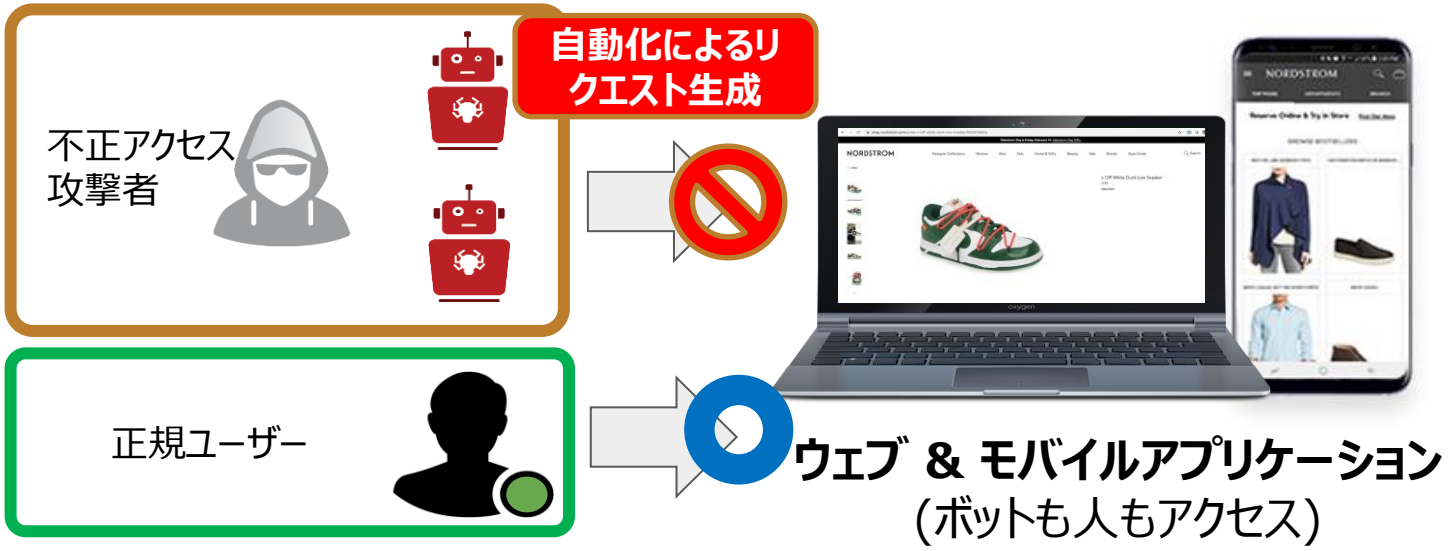
アジェンダ

- 進化したツールやサービスの悪用
- 巧妙化した人による不正アクセス
- 求められる対策/ソリューション
- F5ソリューションご紹介

進化したツールやサービスの悪用

人がアクセスしたように見せかけて自動化による大量のリクエストを送信

- **効率化のため攻撃者はリクエストを自動化するための仕組みを構築**してターゲットに侵入、情報を取得、不正行為を実行します。
- サービス/サイトはオープンにする必要があり(不特定がアクセスされる)、**自動化されたアクセスだけをフィルタする仕組みが必要**。



ポイント: 自動化されて生成されたリクエストは検知してアクセスさせないことが重要

自動化による大量のリクエストかどうか完全には判別できなくなってきている

- 最近の傾向

  - ✓ 既存の対策ソリューション(WAFなど)で検知されないように**”人”がアクセスしているように見せかけるようにリクエストを生成**してきています。

  - ✓ ”人”がアクセスしているように見せかけるリクエストをツールを使って**比較的簡単に自動で多くのリクエストを生成できる**ようになってきています。

自動化されたリクエストの生成を支援するツール

- UIにより自動化リクエストを生成するためのツール
  - ✓ Sentry MBA
- Free Proxy/Open Proxy
- CAPTCHA Solvers
  - ✓ 2CAPTCHA
- ヘッドレスブラウザ (ヘッドレスでJavaScriptの実行)
  - ✓ Phantomjs / triflejs
- Scriptable Consumer Browsers (UIテストツール)
  - ✓ Selenium
- フィンガープリントの偽造
  - ✓ Fraudfox
- ブラウザ操作の自動化ツール
  - ✓ browser automation studio

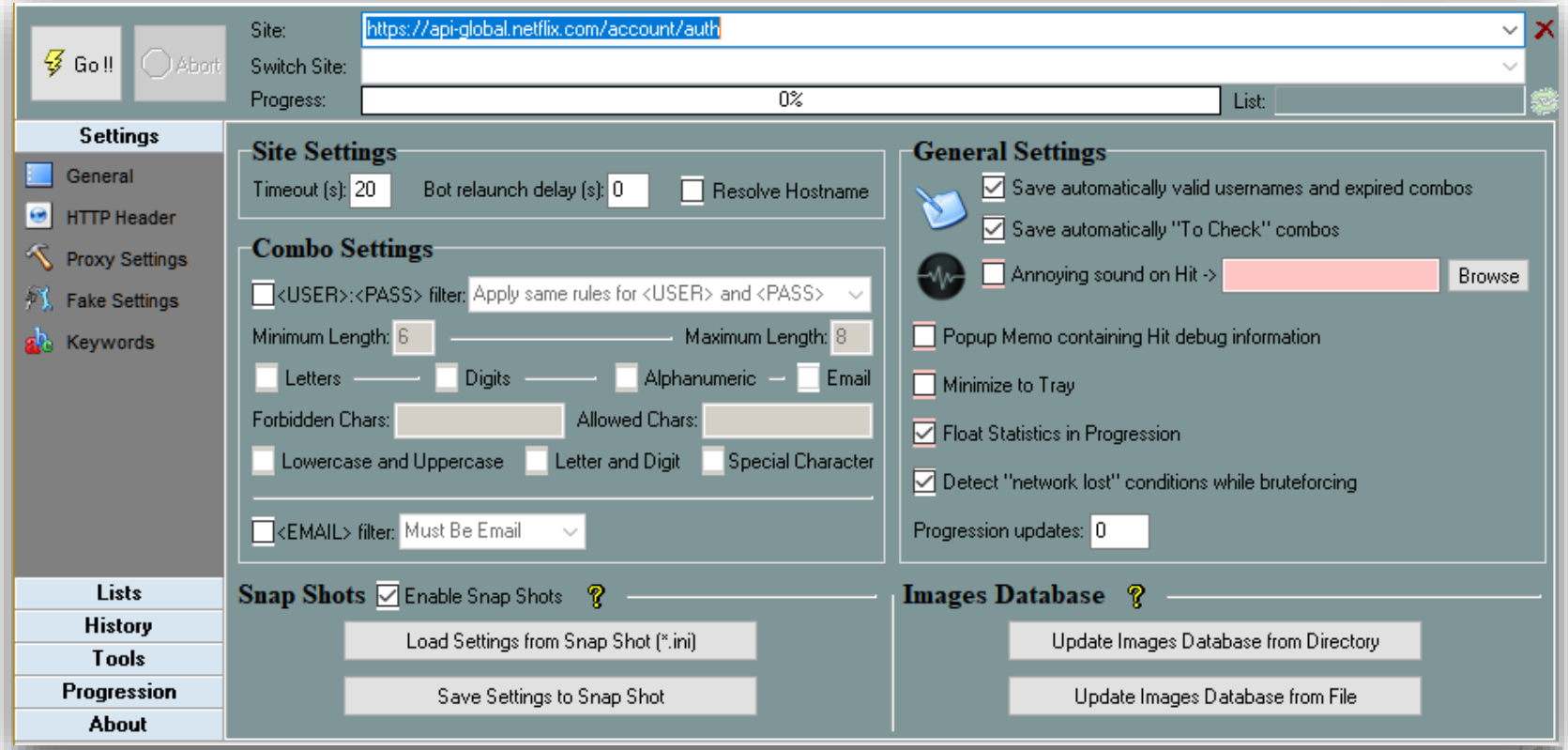
自動化されたリクエストの生成を支援するツール

UIにより自動化リクエストを生成するためのツール: Sentry MBA

自動化されたリクエストの生成を支援するツール

UIにより自動化リクエストを生成するためのツール: Sentry MBA

- IDパスワードリスト型攻撃を簡単に行うためのUIツール



自動化されたリクエストの生成を支援するツール

UIにより自動化リクエストを生成するためのツール: Sentry MBA

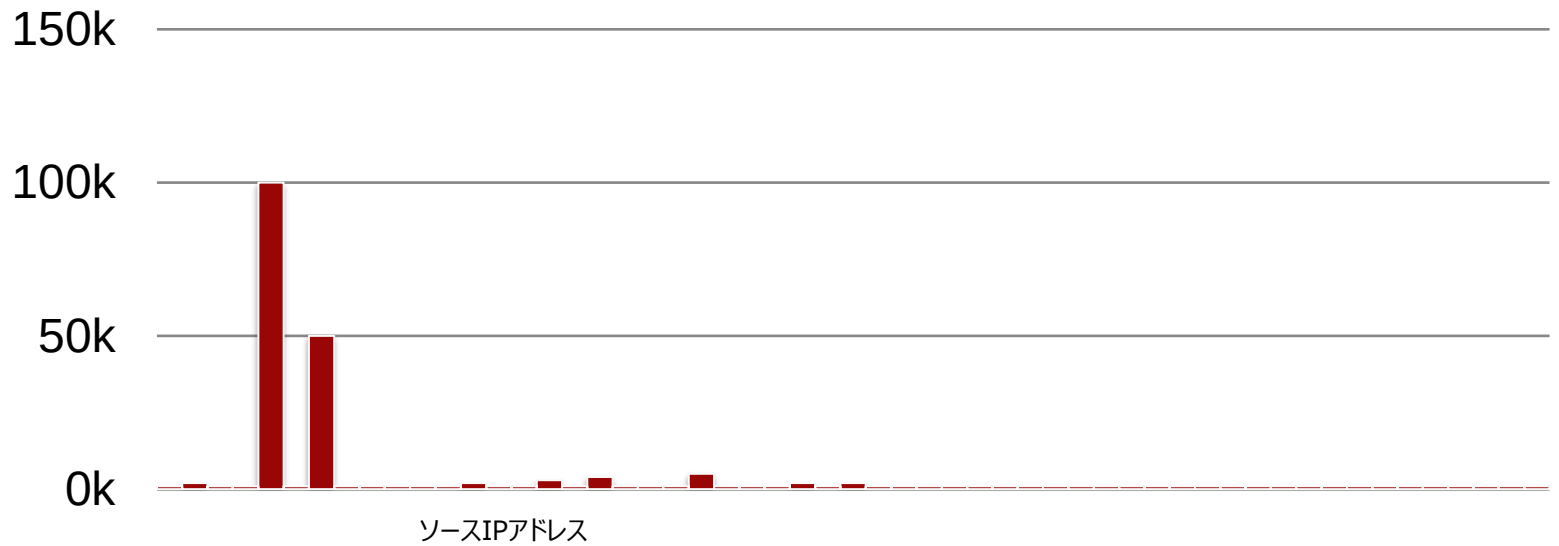
- Sentry MBAの設定基本動作
  - ✓ Config設定 > ターゲットの指定
  - ✓ ID/Passwordリストの指定
  - ✓ 実行 > IDとパスワードが有効なものが返される

自動化されたリクエストの生成を支援するツール

UIにより自動化リクエストを生成するためのツール

UIにより自動化リクエストを生成するツールへの対抗策: IP Rate Limit

- 特定のIPアドレスから指定時間内で指定した回数のリクエストが送信された場合はブロックする。

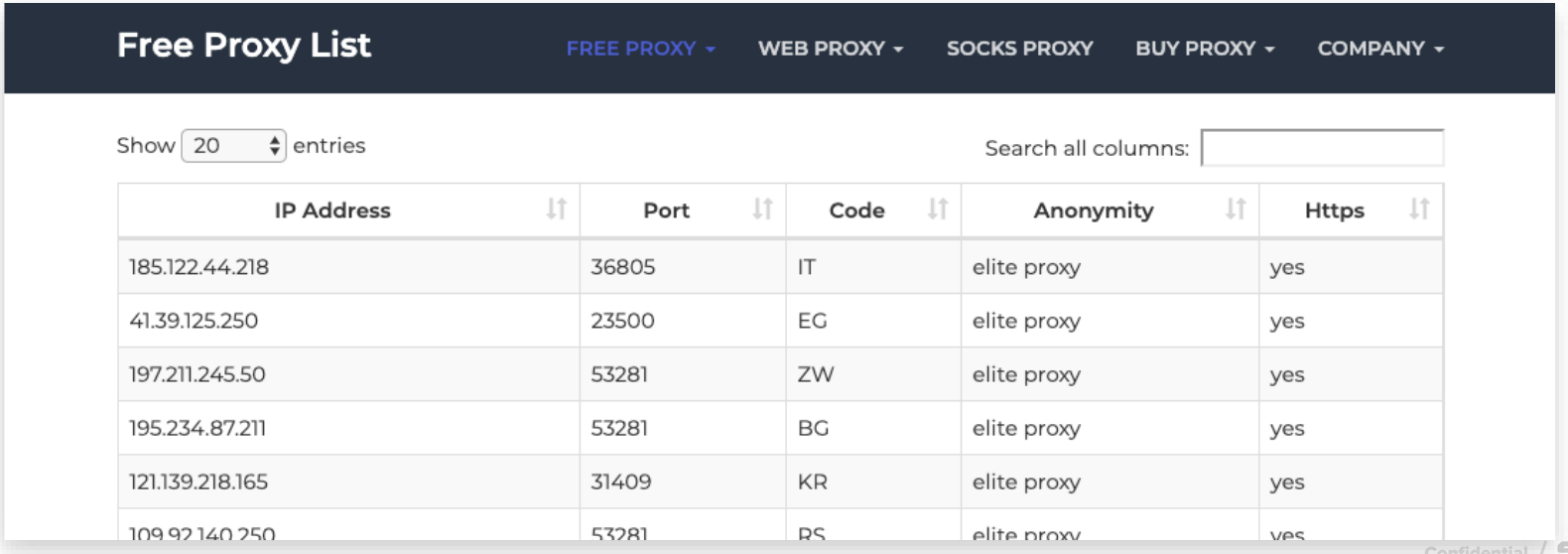


自動化されたリクエストの生成を支援するツール

Open Proxy/Free proxy

自動化されたリクエストの生成を支援するツール
Open Proxy/Free proxy

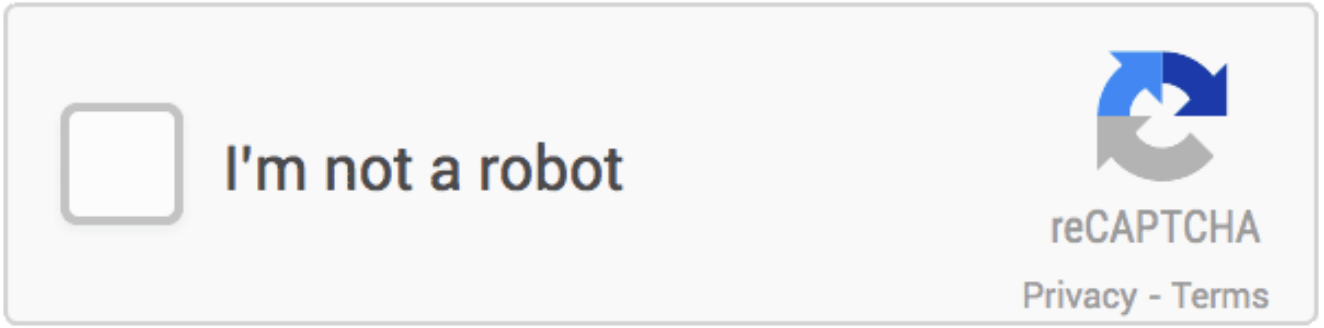
- リクエスト送信元を隠匿するためにフリーで利用できるプロキシが多く公開されており、簡単に利用できるようになっています。
- リクエストを自動送信する場合にはこれらのProxyをローテーションさせて利用することで同一IPからリクエストを送信させないようにします。
- プロキシリストの更新頻度が頻繁で1日でProxyの60%程度は新しく追加されたものであるケースも。防御する側で毎日、ブラックリストに追加していくのは困難。



自動化されたリクエストの生成を支援するツール

Open Proxy/Free proxy

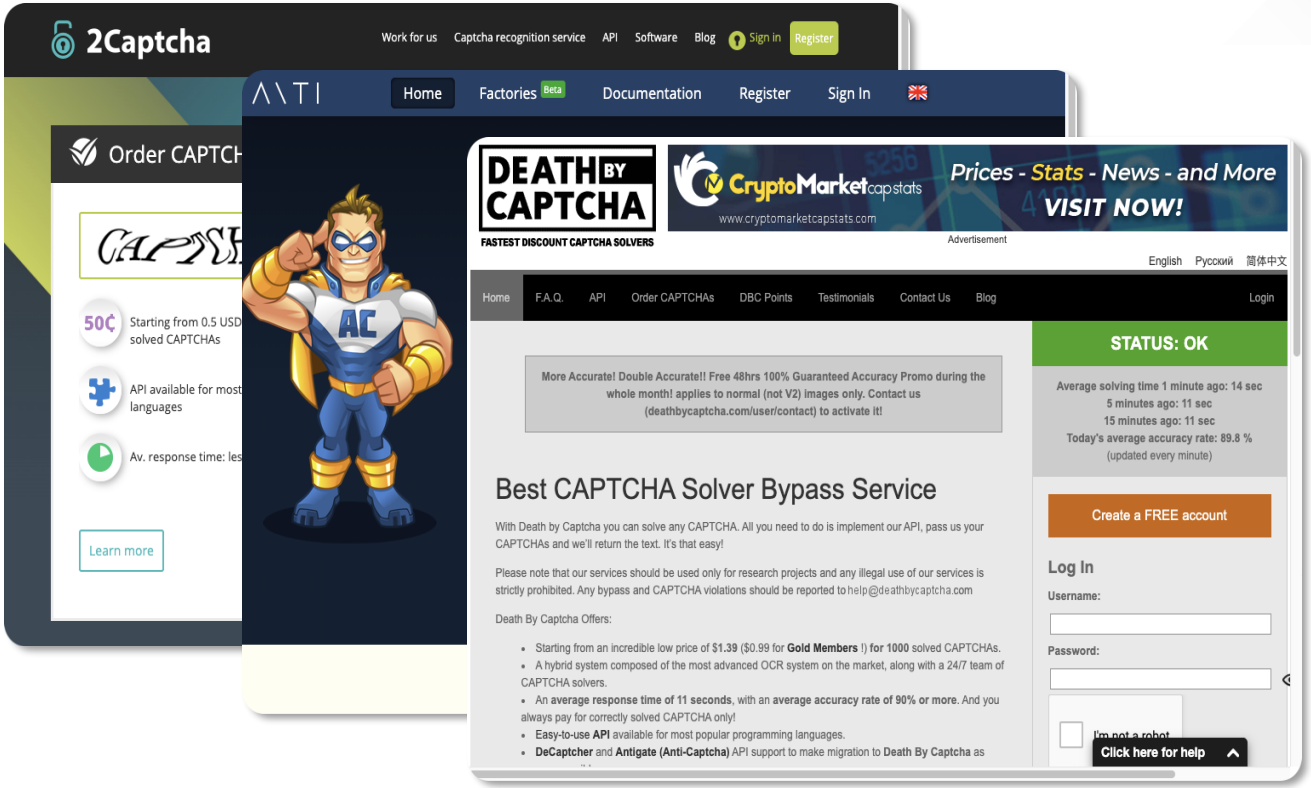
Open Proxy/Free proxyへの対抗策: CAPTCHA



自動化されたリクエストの生成を支援するツール
CAPTCHA Solvers

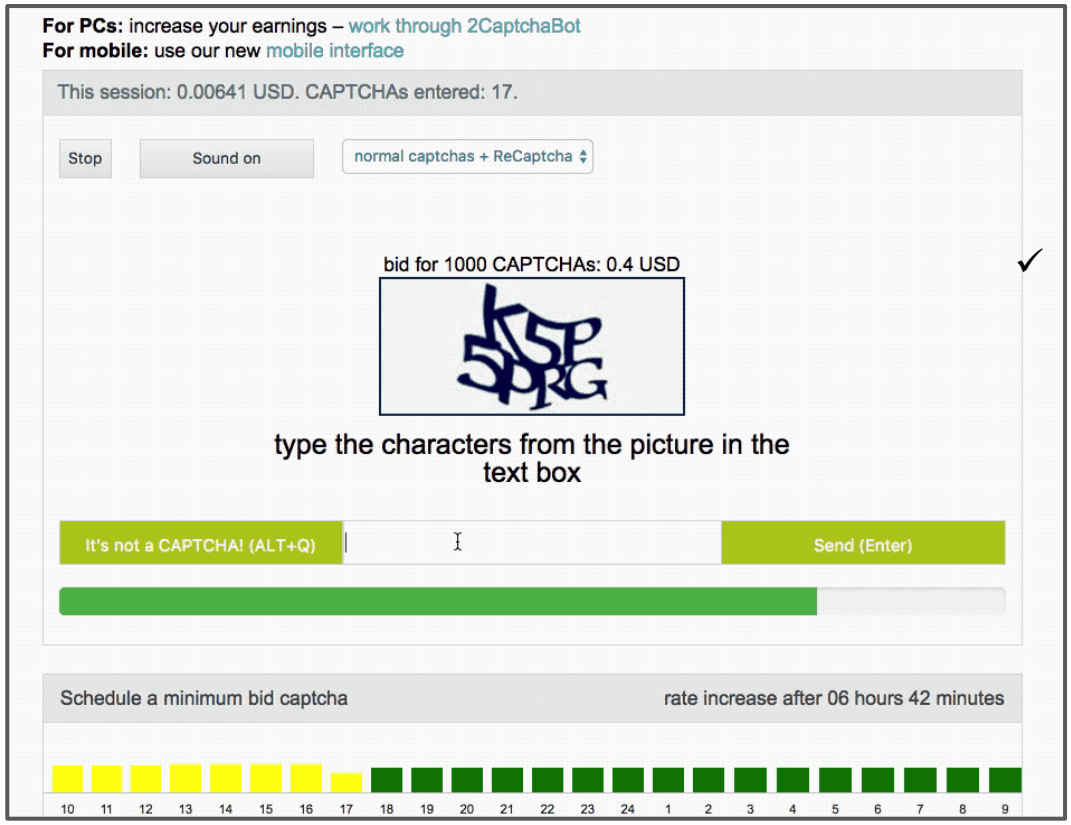
自動化されたリクエストの生成を支援するツール
CAPTCHA Solvers

- CAPTCHAの処理を有償で代行で実行してくれるサービス



自動化されたリクエストの生成を支援するツール
CAPTCHA Solvers: 2CAPTCHA

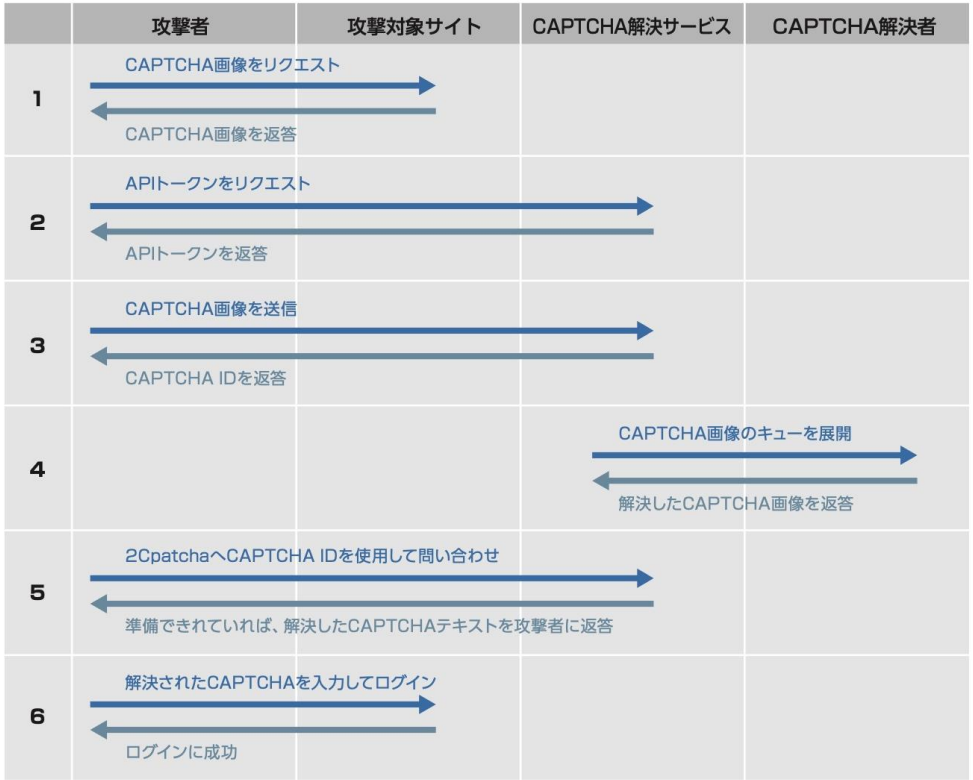
- “人”がCAPTCHAの処理を行う。
- アルバイト感覚でキャプチャの回答をすると金銭の支払いが得られます。



✓ 実際に”人”が処理をしている画面例

自動化されたリクエストの生成を支援するツール
CAPTCHA Solvers: 2CAPTCHA

- 実際の通信フロー



マクニカネットワークス株式会社 様　作成 「悪性Botによる脅威」から抜粋

自動化されたリクエストの生成を支援するツール
CAPTCHA Solvers

CAPTCHA Solversへの対抗策：JavaScriptを多用したWebアプリケーション

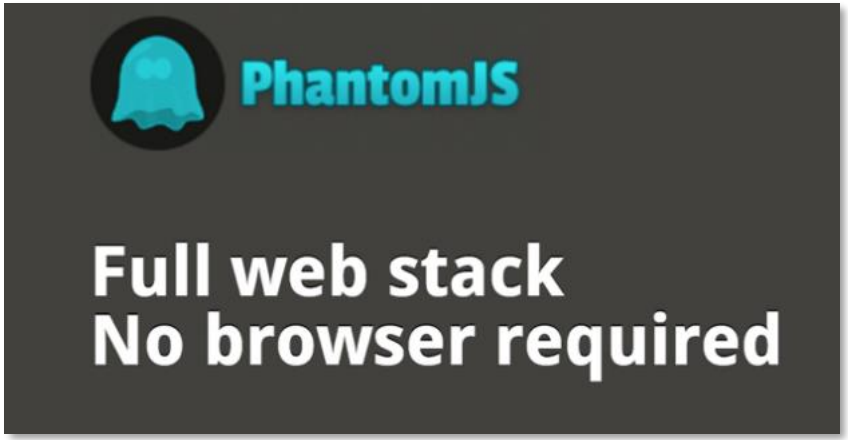
- プログラムから実行される自動化されたリクエストがJavaScriptの実行処理をできないことに注目して対策を実施する。

自動化されたリクエストの生成を支援するツール

ヘッドレスブラウザ(ヘッドレスでJavaScriptの実行): Phantomjs / triflejs

自動化されたリクエストの生成を支援するツール
ヘッドレスブラウザ (ヘッドレスでJavaScriptの実行): Phantomjs / triflejs

- ヘッドレスブラウザとはBrowserのUIを利用せずに動作できるブラウザのこと。つまりコマンドラインやスクリプトを使ってブラウザの動作を定義・実行できるブラウザ。
- JavaScriptも実行可能。Webスクレイピング目的で利用されるケースが多い



自動化されたリクエストの生成を支援するツール

ヘッドレスブラウザ (ヘッドレスでJavaScriptの実行): Phantomjs / triflejs

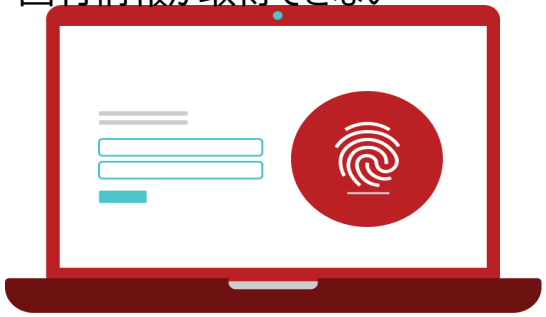
Scriptable WebViewへの対抗策: HTTPリクエストヘッダーの違いの検知やフィンガープリントの利用

ヘッダーの順が違う

```
GET / HTTP/1.1
Host: localhost:1337
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ru;q=0.6
```

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US,*
Host: localhost:1337
```

ヘッドレスブラウザではデバイス/ブラウザ固有情報が取得できない



Cookies
Timezone of browser and IP
Operating system detection
Useragent information
Operating system, browser languages
Screen size of device, browser, windows
Installed fonts
Installed plugins
Battery level
GPU information
Cursor, scrolling behavior
And more...

自動化されたリクエストの生成を支援するツール

Scriptable Consumer Browsers（UIテストツール): Selenium

自動化されたリクエストの生成を支援するツール
Scriptable Consumer Browsers （UIテストツール): Selenium

- UIテストツールとして有名で実際のブラウザ実行環境を再現できるツール

自動化されたリクエストの生成を支援するツール
Scriptable Consumer Browsers （UIテストツール）

UIテストツールへの対抗策: デジタルフィンガープリント/ブラウザフィンガープリント

- デジタルフィンガープリント/ブラウザフィンガープリント(ブラウザのタイムゾーン、言語、プラグイン、OS種別など)を利用してデバイスを識別し不正アクセスで利用されてるデバイスを認識する。
- デバイスを識別することでデバイス単位で不正アクセスをモニタ・検知する。

ブラウザフィンガープリント/デジタルフィンガープリントで取得される一般的な情報例

Cookies
Timezone of browser and IP
Operating system detection
Useragent information
Operating system, browser languages
Screen size of device, browser, windows
Installed fonts
Installed plugins
Battery level
GPU information
Cursor, scrolling behavior
And more...

同一デバイスであれば不変

不正アクセス元のデバイス特定

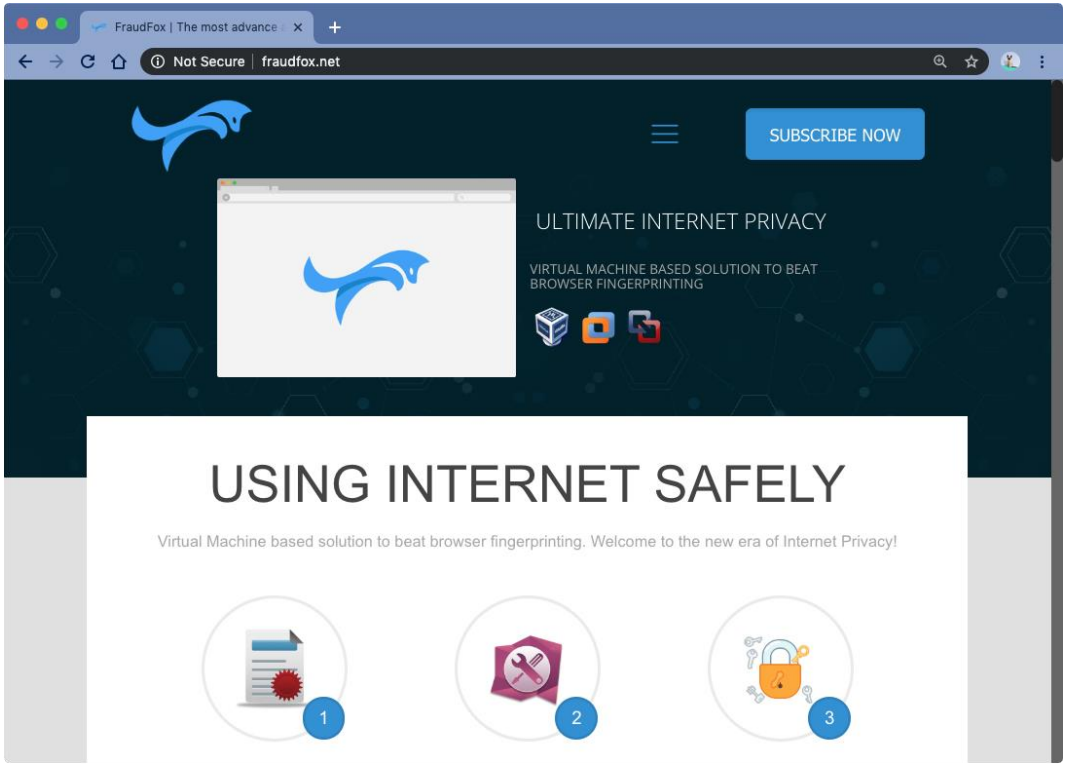
ブラウザフィンガープリントはリスクベース認証や効果的な広告表示のために広く利用されています。

自動化されたリクエストの生成を支援するツール

フィンガープリントの偽造: Fraudfox

自動化されたリクエストの生成を支援するツール
フィンガープリントの偽造: Fraudfox

- デジタルフィンガープリント/デジタルフィンガープリントをラインダムに生成してリクエストで利用できるツールでデバイスを隠匿化できる。



自動化されたリクエストの生成を支援するツール
フィンガープリントの偽造

ブラウザフィンガープリント偽造への対抗：ブラウザ上の操作を監視する

- ブラウザ上での操作を監視すると明らかに”人”が操作したものではないことがわかる。

✓ 明らかに早いキーボードキーストロークなど”人”が操作したものではないことがわかる

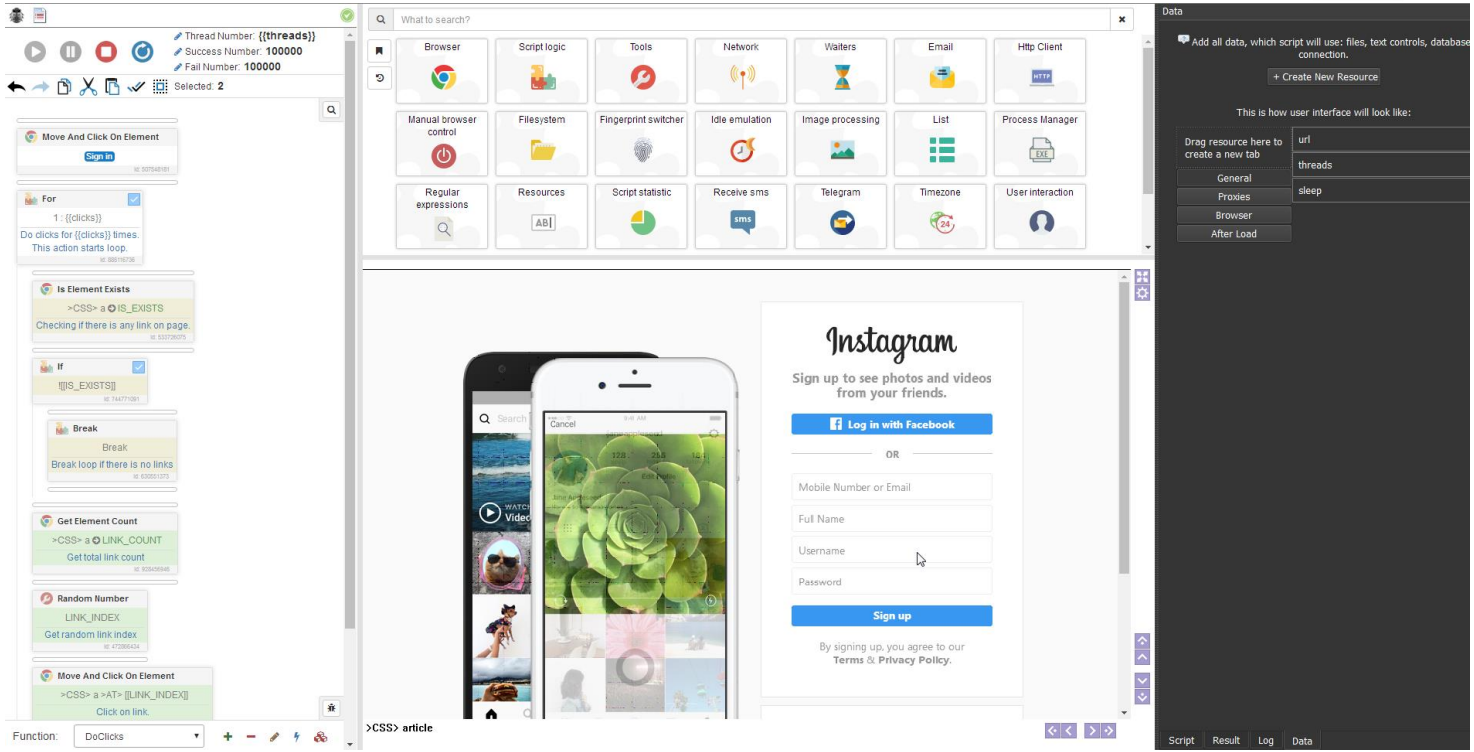
自動化されたリクエストの生成を支援するツール

ブラウザ操作の自動化ツール: browser automation studio

自動化されたリクエストの生成を支援するツール

ブラウザ操作の自動化ツール: browser automation studio

- ブラウザ上での実際の動作を定義して実行できるツール
- マウスやキーボードの動きも定義して実行できる。



自動化されたリクエストの生成を支援するツール
ブラウザ操作の自動化ツール: browser automation studio

- マウスの動きが若干、直線的、キーボードのキーストロークも一定間隔ではあるが、不正アクセスにためには十分(防御側を騙せるレベル)

Browser Automation Studioを利用した実際の動作例

自動化されたリクエストの生成を支援するツール
今後の方向性

自動化されたリクエストの生成を支援するツール
今後の方向性

- ツールが洗練されていく
  - ✓ 今後の方向性としてはアプリケーションや対策ソシューションから検知されないように**まるで”人”がアクセスしているかのようにリクエストを生成できるようにツールなどが洗練されていく**と思われます(人がアクセスしているように見せかけるアクセス手法、攻撃手法を“イミテーションアタック”と呼んでいます)。

- 既存ソリューションでは自動化されたリクエストの検知がますます困難に
  - ✓ WAFなどに代表されるような**企業の管理者がルールセットを記述するような対策方法では限界がある。**常に専門エンンジをキープしてトレーニングしていくにはコストがかかってしまいます。

巧妙化した人による不正アクセス

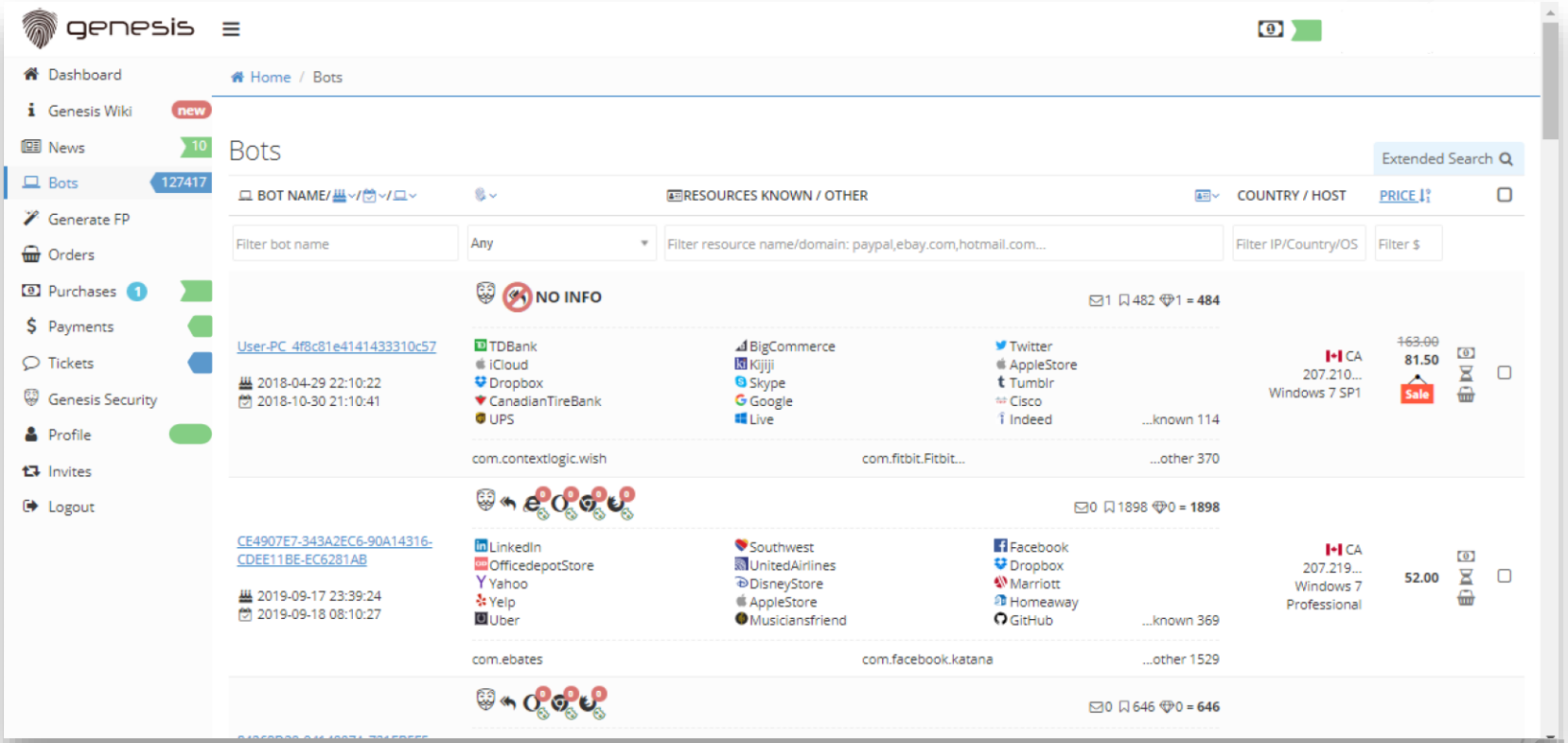
ユーザアクセス環境を盗んでアクセス元デバイスになりすます

Genesis: アカウント/環境スクレイピング

ユーザアクセス環境を盗んでアクセス元デバイスになりすます

Genesis: アカウント/環境スクレイピング

- 不正なマルウェアより盗まれたアイデンティティ情報(ID/パスワードやセッションCookieなど)やブラウザのデジタルフィンガープリント/フィンガープリントを販売しているサイト

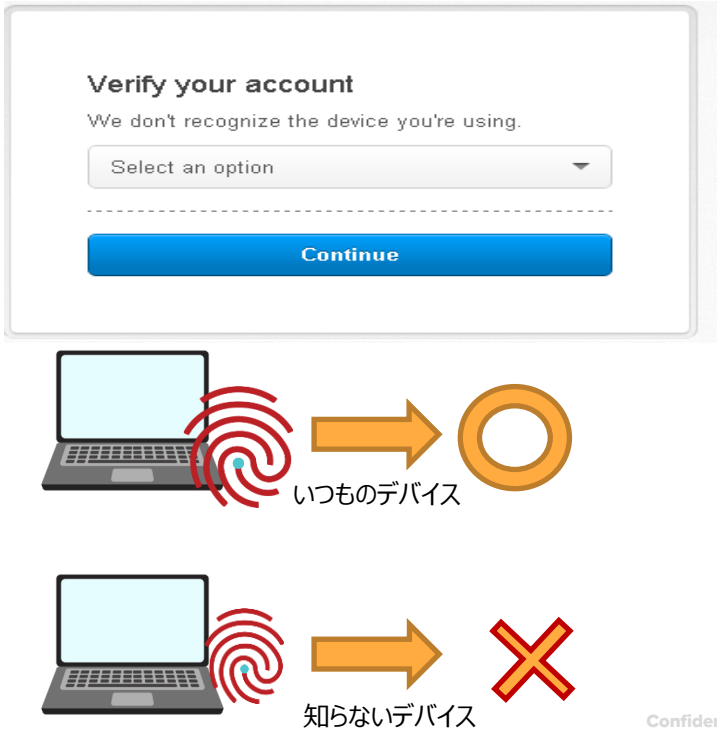


ユーザアクセス環境を盗んでアクセス元デバイスになりすます
Genesis: アカウント/環境スクレイピング

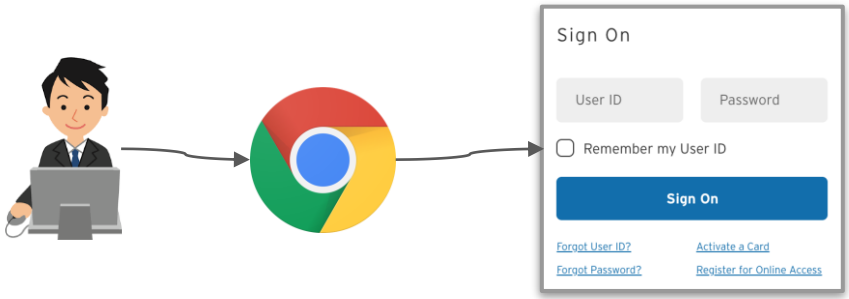
- ユーザが利用しているブラウザから得られる情報(デジタルフィンガープリント/ブラウザフィンガープリント)を元にデバイスの識別を行い、いつも利用しているデバイスかどうかを確認するサイトが多い。
- 環境情報(フィンガープリント)も盗まれてしまうと被害者のデバイス/環境になりすましが可能となってしまう。

デジタルフィンガープリント/ブラウザフィンガープリント

Cookies
Timezone of browser and IP
Operating system detection
Useragent information
Operating system, browser languages
Screen size of device, browser, windows
Installed fonts
Installed plugins
Battery level
GPU information
Cursor, scrolling behavior
And more...



ユーザアクセス環境を盗んでアクセス元デバイスになりすます
Genesis: アカウント/環境スクレイピング



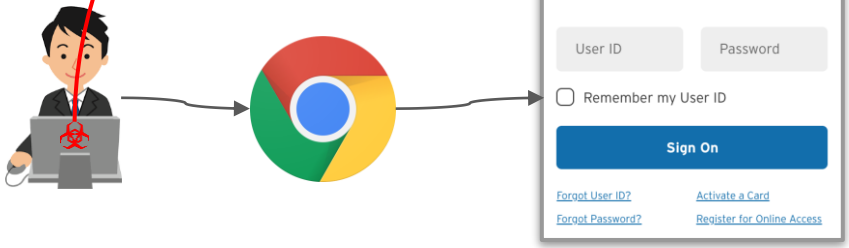
ユーザがいつも利用しているサイトにログイン

ユーザアクセス環境を盗んでアクセス元デバイスになりすます
Genesis: アカウント/環境スクレイピング

マルウェアがサイトのログインID
やパスワード、ブラウザフィンガー
プリント情報収集して送信

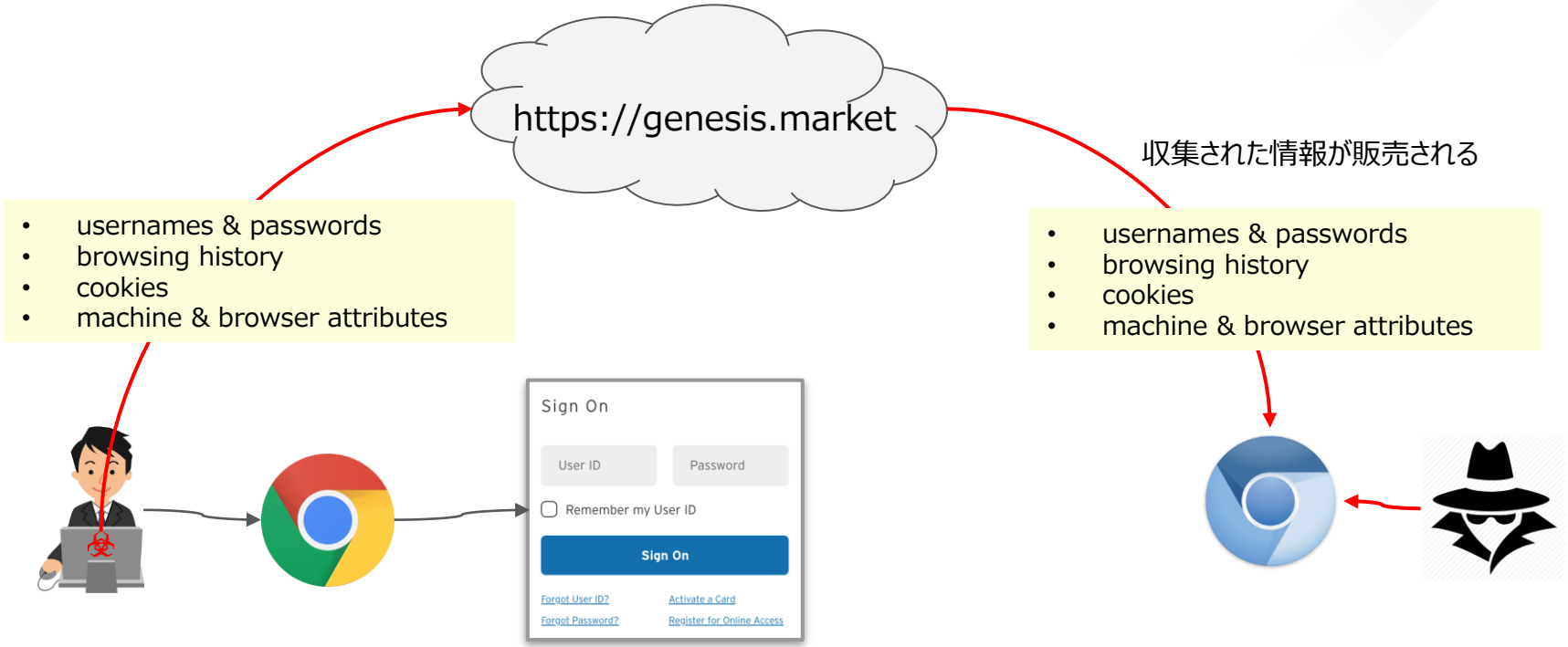
https://genesis.market

- usernames & passwords
- browsing history
- cookies
- machine & browser attributes



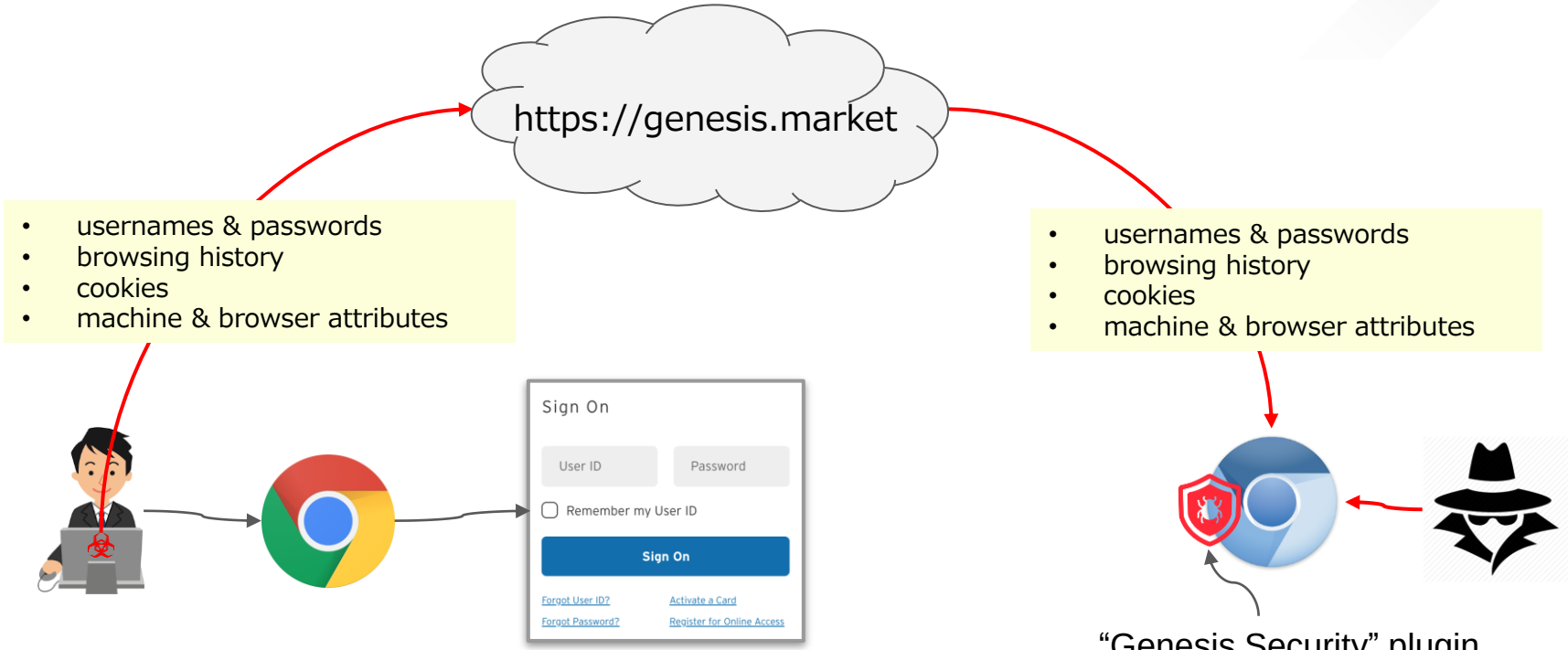
ユーザアクセス環境を盗んでアクセス元デバイスになりすます

Genesis: アカウント/環境スクレイピング



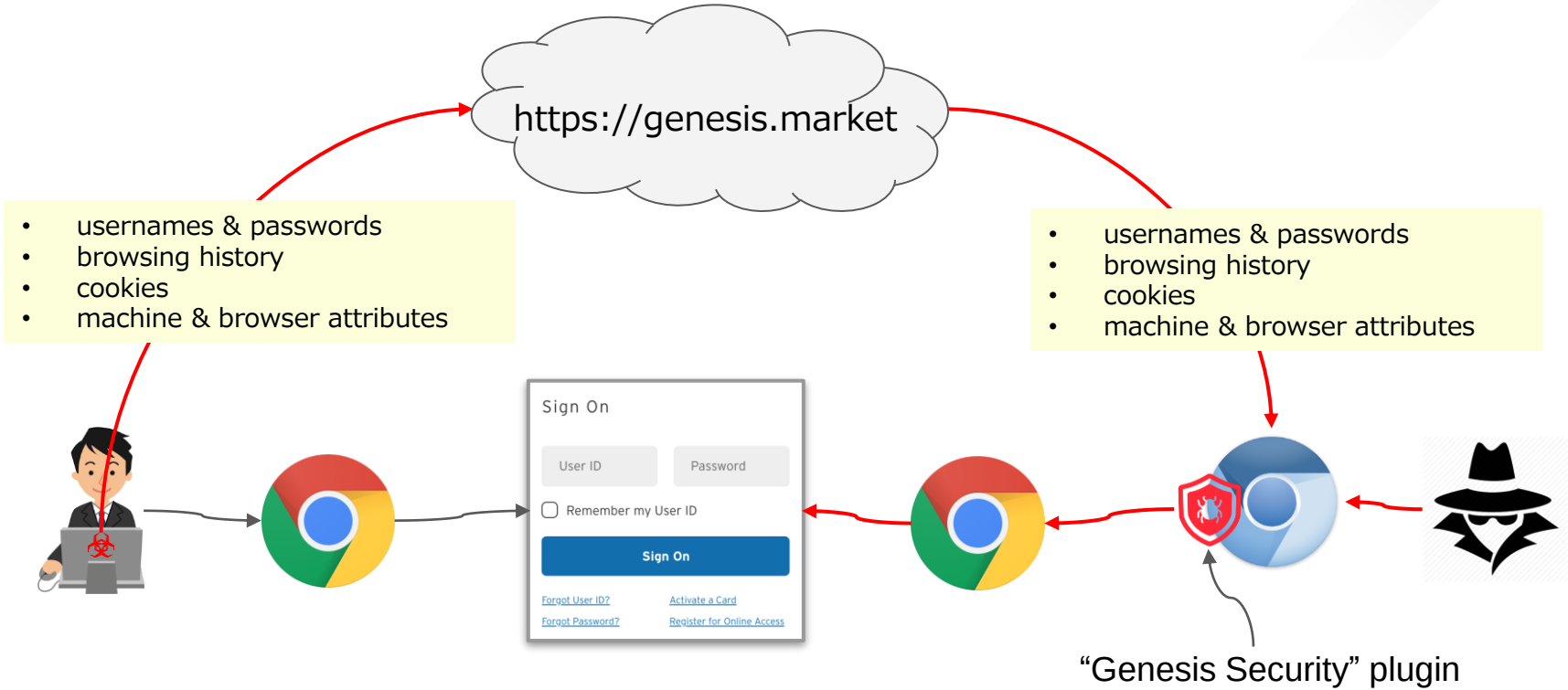
ユーザアクセス環境を盗んでアクセス元デバイスになりすます

Genesis: アカウント/環境スクレイピング



ユーザアクセス環境を盗んでアクセス元デバイスになりすます

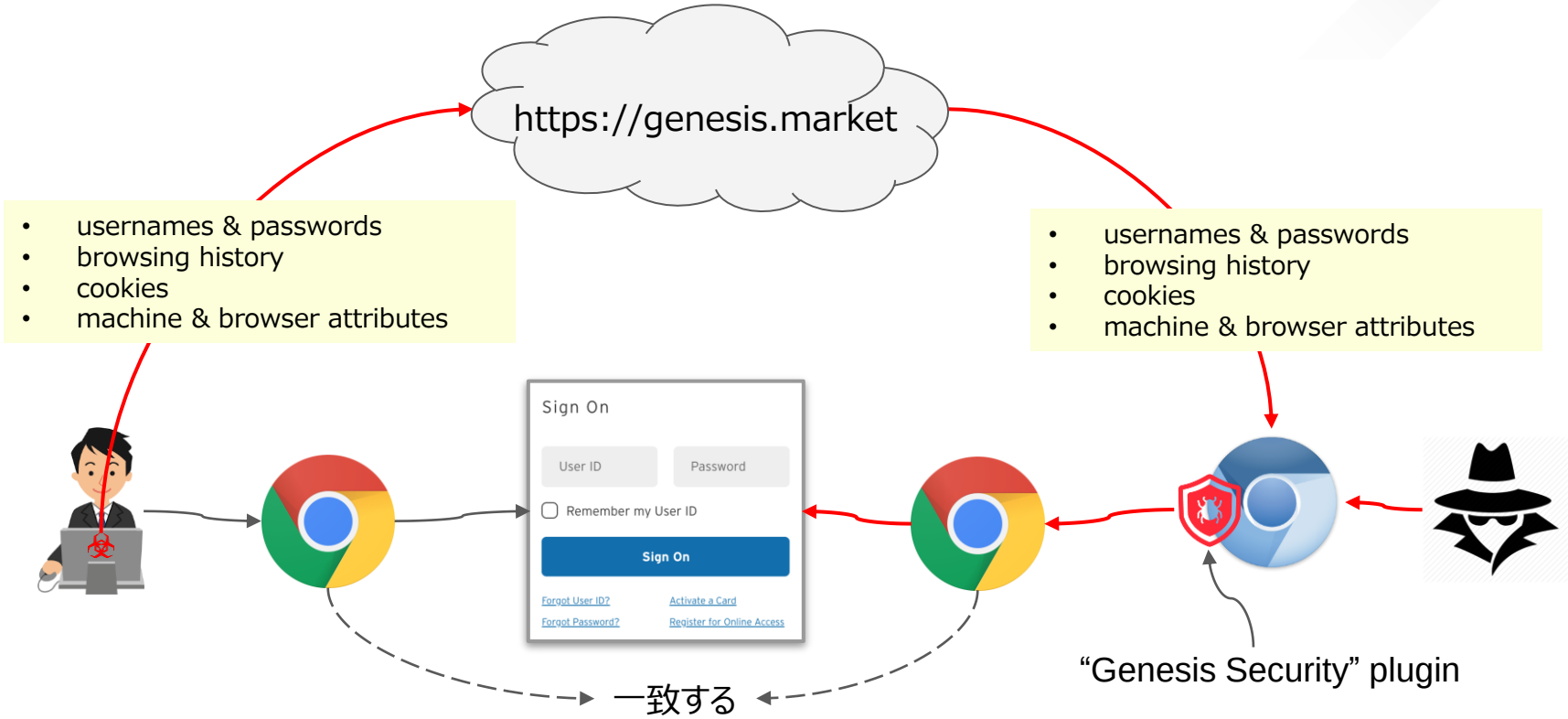
Genesis: アカウント/環境スクレイピング



Genesisプラグイン経由でアクセスすると情報を盗まれたユーザのデジタル・ブラウザフィンガープリント情報をエミュレートして接続する

ユーザアクセス環境を盗んでアクセス元デバイスになりすます

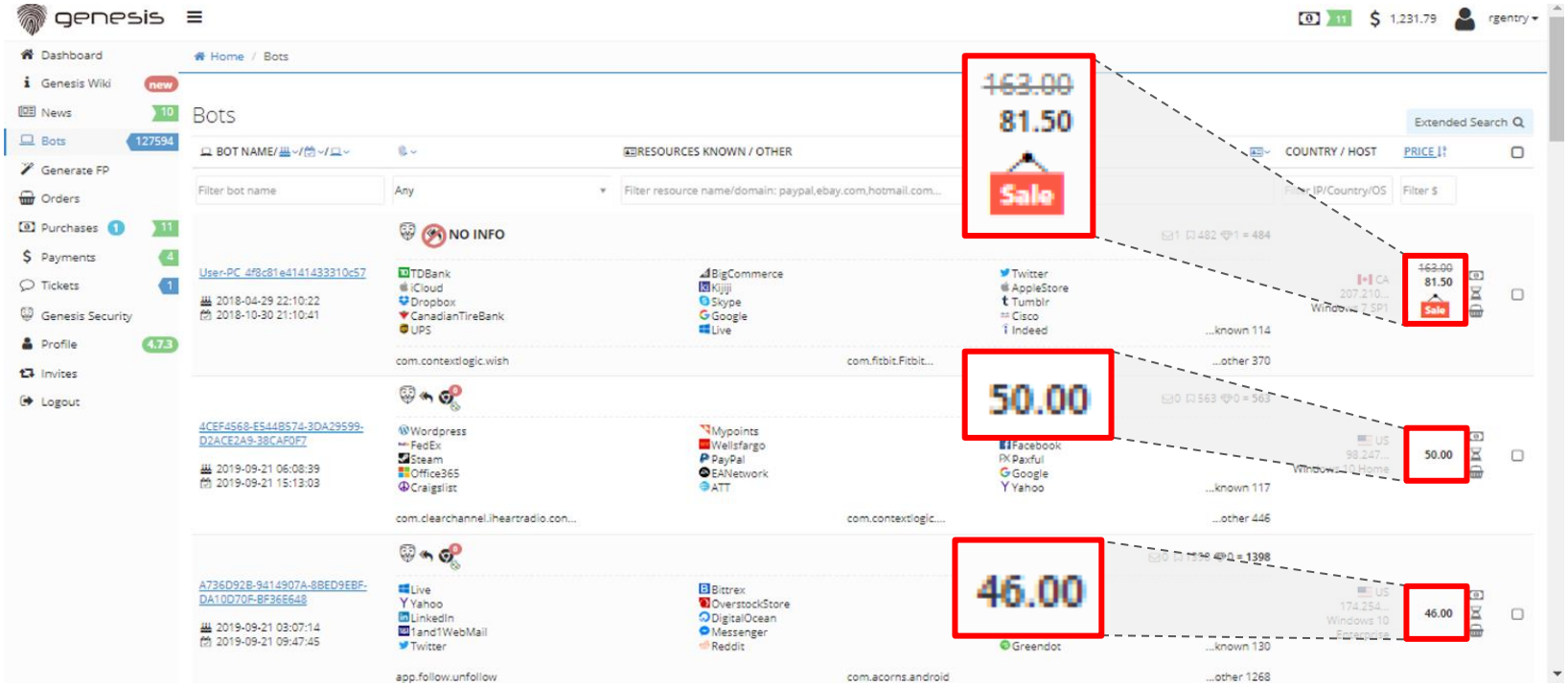
Genesis: アカウント/環境スクレイピング



ユーザアクセス環境を盗んでアクセス元デバイスになりすます

Genesis: アカウント/環境スクレイピング

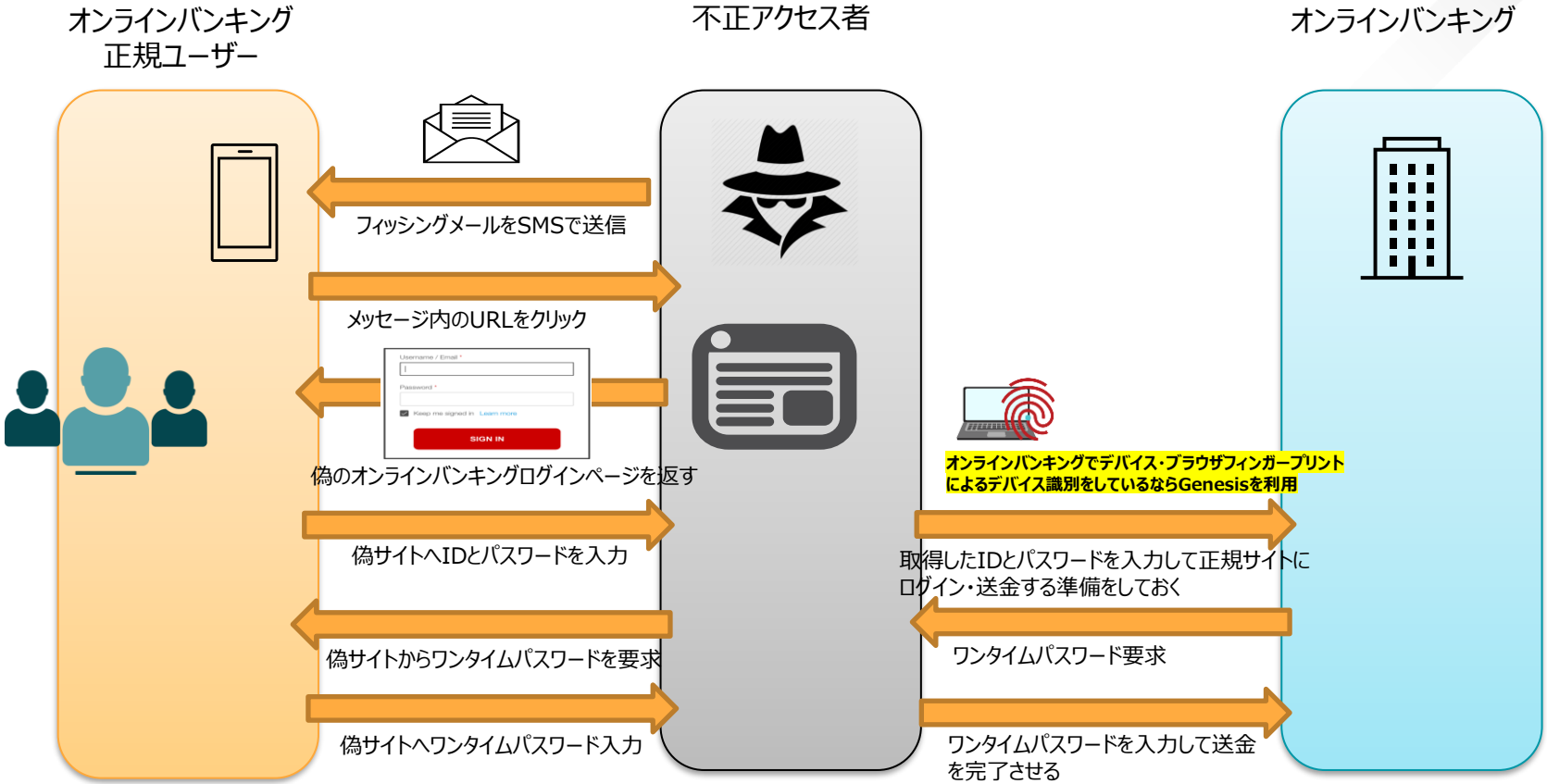
- デジタルフィンガープリント/ブラウザフィンガープリントの購入には費用がかかるが、精度の高い情報であるため
  マニュアルによる(“人”)による不正アクセスで悪用される可能性が高い。



2 要素認証を突破する不正アクセス

巧妙化した人による不正アクセス

スミッシング(SMS+フッシング)を利用したワンタイムパスワードの不正取得例



巧妙化した人による不正アクセス

まとめ

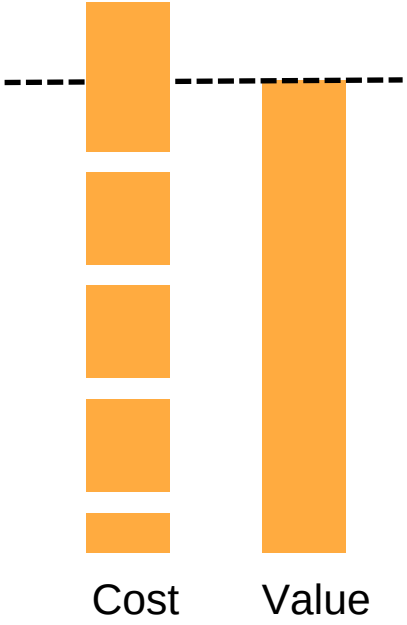
- 特定のユーザを狙った“人”による不正アクセスが今後増加すると思われます。
- 多要素認証/多段階認証を利用すれば人によるオンライン詐欺行為は防止できるか？
  - ✓ 多要素認証/多段階認証は有効ではあるが、バイパスされる可能性があり完全ではない。
  - ✓ ECサイトなどITスキルも違っている多くのユーザーに利用してもらうためにはユーザー操作性を高める必要があり単純に多要素認証/多段階認証をサイトの多くで導入するということでは解決しないケースも。

求められる対策/ソリューション

不正アクセスも経済合理性で行われる

- 不正アクセスにかかるコスト(対策を突破する金銭/労力)よりも得られる価値が高ければ不正アクセス者は手を変えて不正アクセスを試みようとします。
- 逆にコストよりも得られる価値が低くなってしまえば不正アクセス者はコスト的に損になるため不正アクセスを行いません。
- 不正アクセスにかかるコストはツールの進化により下がってきています。

不正アクセスを行う価値あり



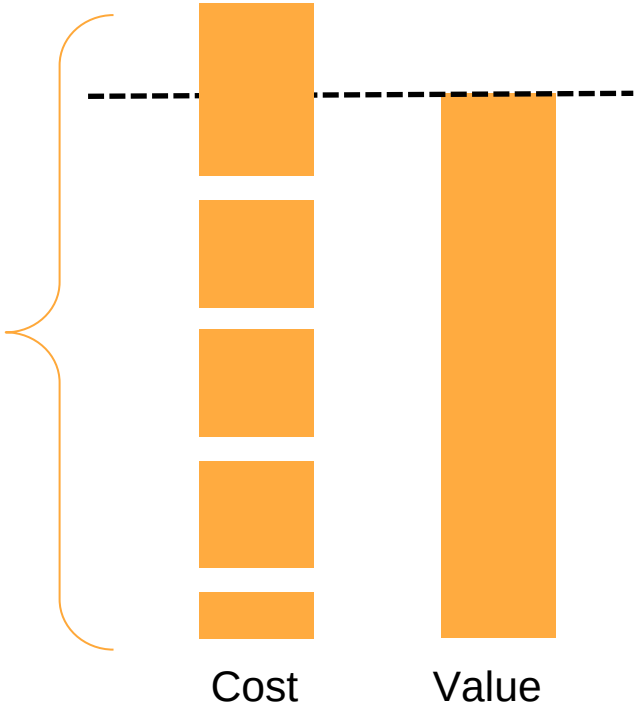
不正アクセスを行う価値がない

※不正アクセスのスキルを示すための場合は別

不正アクセスも経済合理性で行われる

不正アクセス者が不正アクセスを成功させるためのコスト、労力を大幅にあげるようにする。日々対策をアップデートする。

- 不正アクセスを諦めてもらう
- 別のサイトに行ってもらう



不正アクセスを止めさせるために、いかにそのサイトへの不正アクセスが高コストになることを不正アクセス者に示す

高いハードルを作ってしまえば良いのか？
ユーザ操作性は損なってはいけない

- 複雑な操作を必要とする対策や複雑な認証操作を導入すると、ITリテラシーも異なるユーザがアクセスする場合、そもそもアプリケーション(サービス)を利用してもらえないことになってしまうため注意が必要。

- ユーザ操作性は損なわずに対策を行っていくことが重要です。

不正アクセスのハードルが低いところを探して狙ってきます

- 同じアプリケーション(サービス)でも対策が不十分なところを狙って不正アクセスが行われます。同一レベルので不正アクセス対策が必要です。

- 例) オンラインバンキングへのログインは2要素認証が必要であるが、オンライン振替処理の登録は2要素認証が必要ではない。

求められる対策/ソリューション

現状

- 自動化されたものか人がアクセスしたものか判別がしづらい状況に
- ルールベースの設定による対策では巧妙化した不正アクセスに対抗できない
- 特定のユーザをターゲットとした不正アクセスの増加

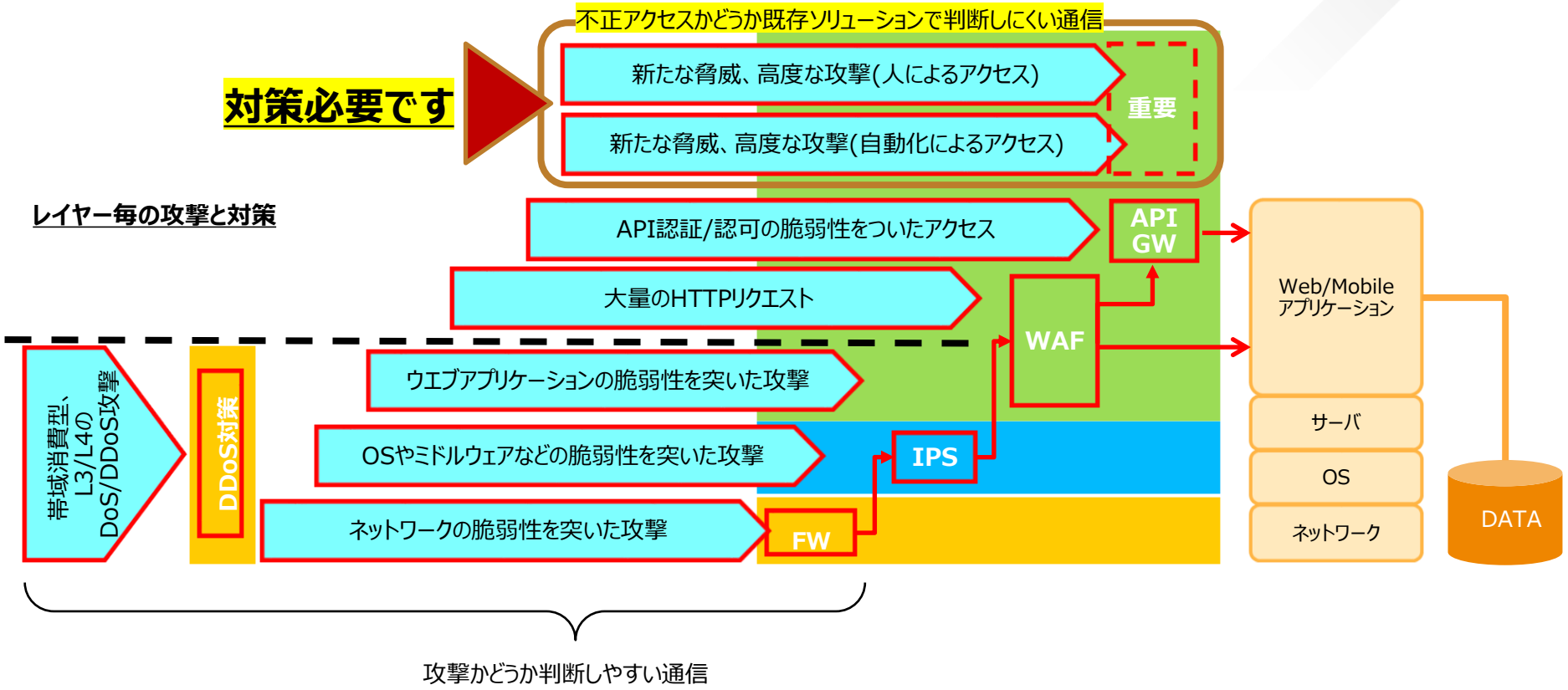
- 問題なくとも常に監視
  - ✓ ツールやアッタク手法は日々、進化しており問題ないと考えていても常に監視していく必要があります。

- 専門家に任せた方が良い
  - ✓ 人がアクセスしたものか判別が難しいため判定には高度なスキルが必要、対策も日々アップデートしていく必要がある。不正なアクセスの検知・対策には専門スキル、ノウハウをもつ対策ベンダーを利用して不正アクセスのコストが高くなることを攻撃者にわかってもらう。

- アプリケーション内のユーザジャーニーの認証を検討する
  - ✓ 人によるオンライン詐欺行為はユーザ認証強化だけではブロックできないため認証をパスした後のトランザクション全体(アプリケーション上でのユーザージャーニー=利用フロー)の認証(問題ないユーザーのアプリのフロー？ or 不正アクセス者のアプリのフロー？)を実施すべき。

攻撃者の侵入するためのコストと得られる価値(金銭)/対策のためのコスト/ユーザ操作性は損なわない　のバランスを対策検討時に考慮

求められる対策/ソリューション



F5ソリューションご紹介

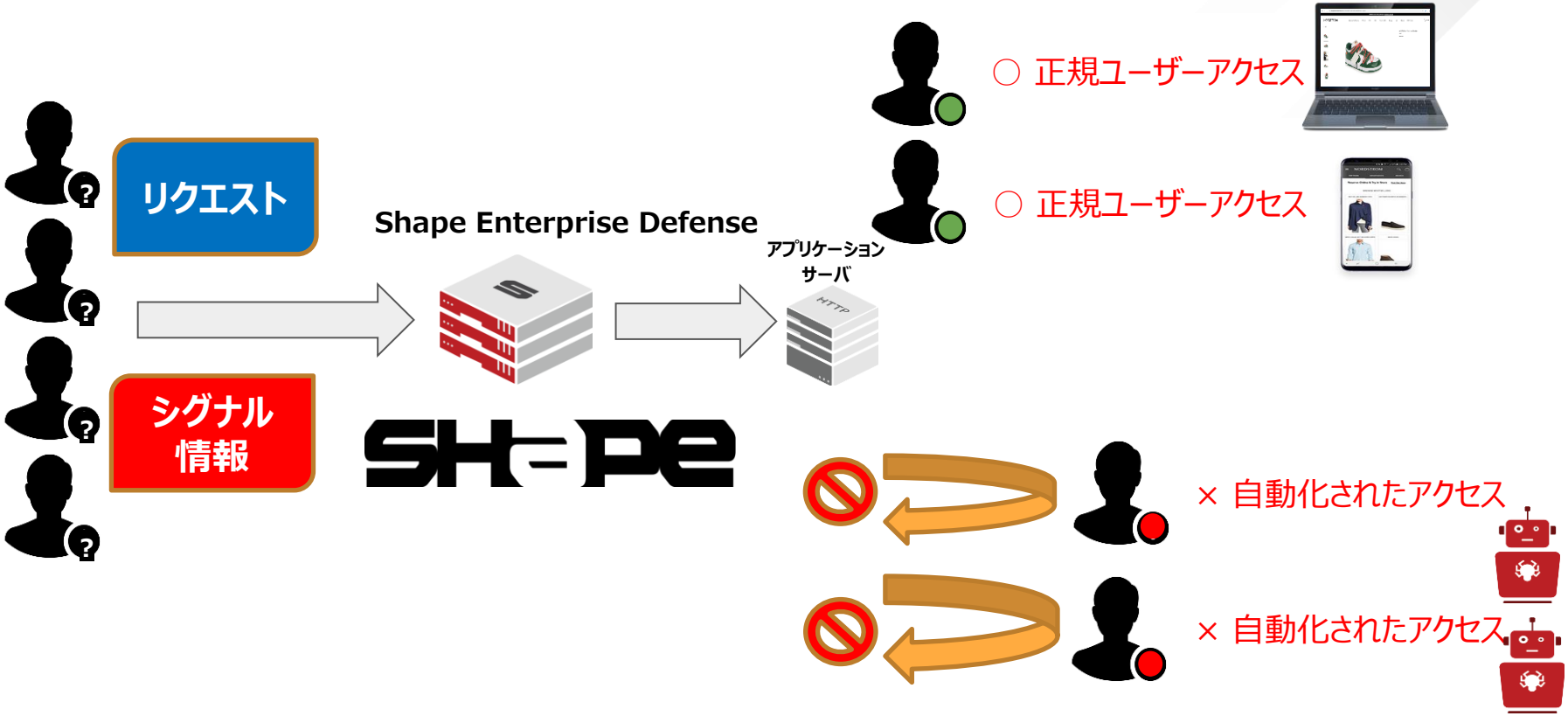
Shape Security ソリューション一覧

- **Shape Enterprise Defense**
- **Shape AI Fraud Engine**
- **Shape Device ID**
- **Shape Client Side Defense**
- **Shape Recognize**

Shape Enterprise Defense

Shape Enterprise Defense

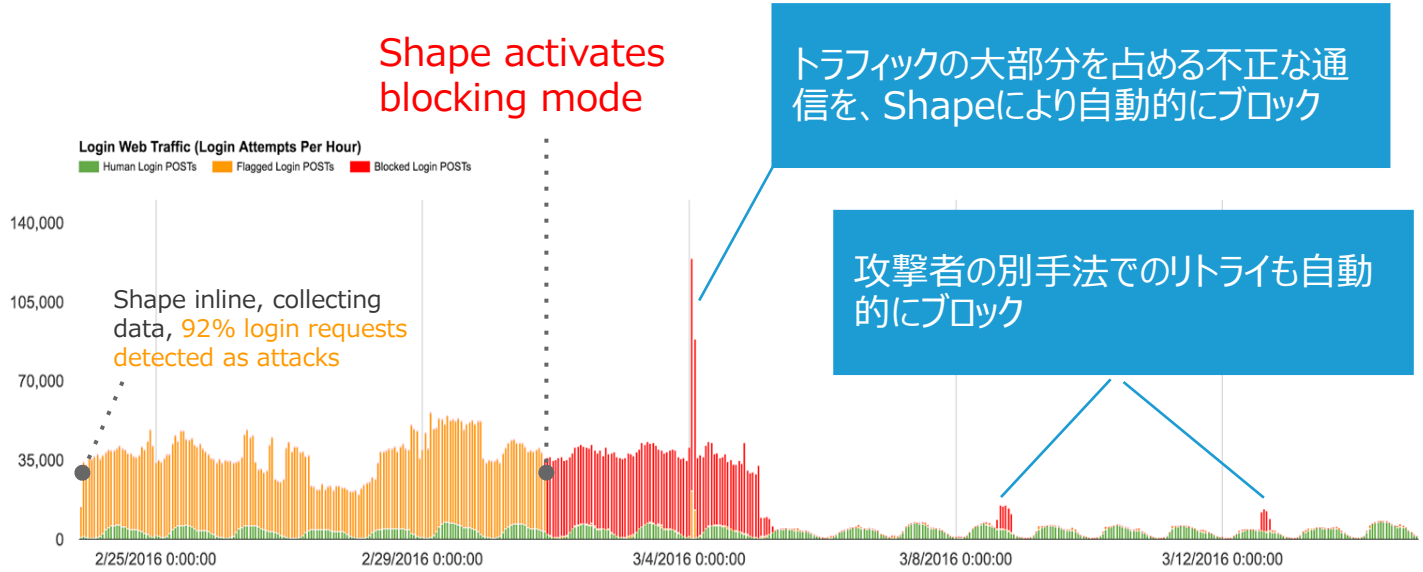
シグナル情報を利用して人によるアクセスか自動化されたアクセスかを明らかにする



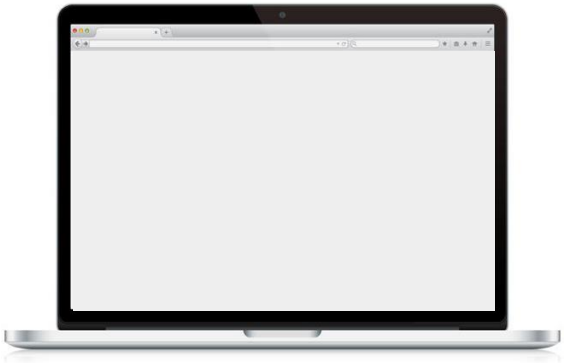
Shape Enterprise Defense

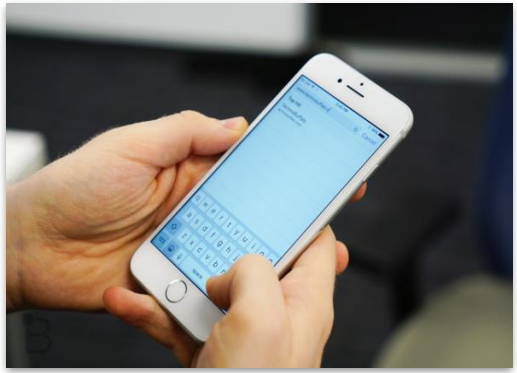
Web/Mobileアプリケーションへの自動化されたアクセスを検知するソリューション

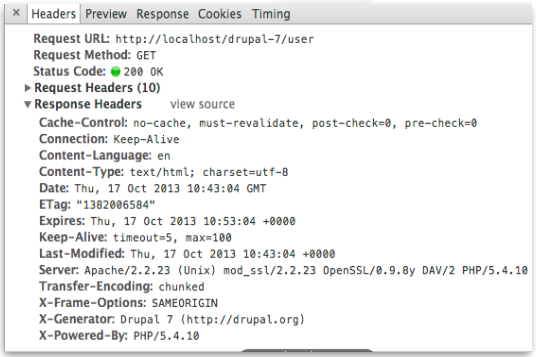
- リクエストから得られるシグナル情報をもとにリクエストが自動化されて生成されたものかを判断
- 保護処理として、ブロッキング、リダイレクト等をリアルタイムの実施



Shape Enterprise Defense
シグナル情報







環境情報 (Environment)

誰が？

振る舞い検知 (Behavior)

どのように？

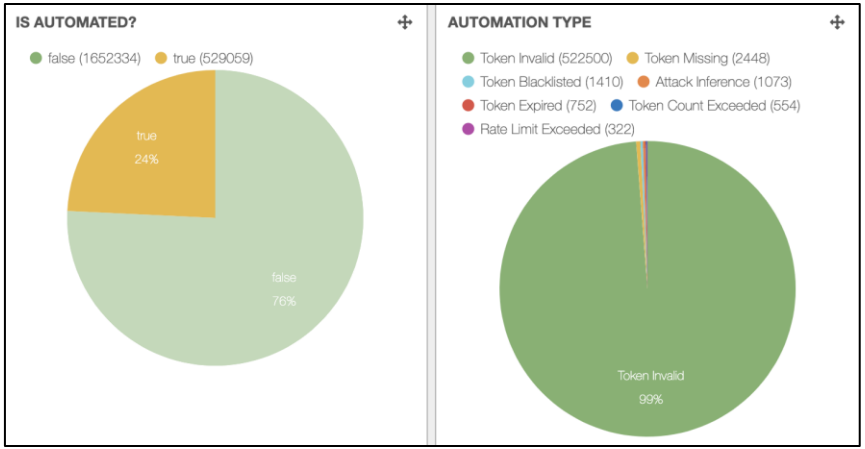
ネットワーク情報 (Network)

どこから？

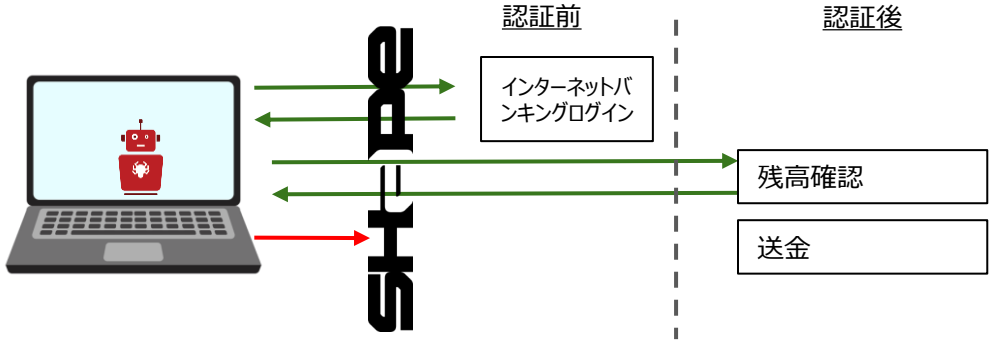
Shape Enterprise DefenseのJava Scriptを利用してクライアントから収集

Shape Enterprise Defense
分析と判断: リクエストは自動化されたアクセスなのか？

環境情報 ＋ 振る舞い ＋ ネットワーク ＝ 自動化 Yes/No



Shapeはそれぞれのトランザクションをチェック



例)

- マルウェアに感染していないユーザからのアクセス => 許可
- マルウェアに感染している場合、マルウェアがセッションハイジャックして不正な送金 => リクエストを拒否

Shape Enterprise Defense
他社と比較した優位性

1 フルマネージドサービス
24x365 SOC

設定変更や新たな脅威への対応は全てサービス側で実施。お客様側でルール調整などの設定変更を行なっていただく必要はありません。

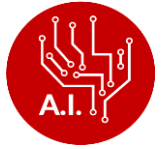
2 多要素シグナルの収集力

クライアント環境 (OS,Browser等)
キー、マウス操作
ネットワーク情報 などの多様なシグナル**をモバイル/PCの双方で取得**

3 JavaScriptの技術力

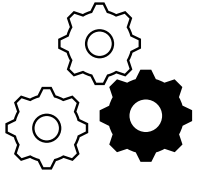
お客様独自のJavaScriptコードを動的生成
バイトコード化し、高度な難読化を実現

4 独自AIによる高い検知率



グローバル規模で収集したデータ分析
既知の攻撃への対応
ゼロデイ攻撃への対応

5 アドオン機能の充実



Device ID, Invisible MFA,
SAFE(マニュアル不正アクセス検知)、
Client-Side Defenseなど既存機能
をエンハンスするアドオン機能が充実

6 ”人”によるオンライン詐欺行為の検知

アドオン機能のShape AI Fraud Engine(SAFE)を利用することで”人”によるオンライン詐欺行為の検知が可能

7 デプロイメントオプションが豊富

プロキシコンポーネントのオンプレミス/クラウド選択可に加えて既存環境との複数の連携オプションを提供します。