Hakka`s Ephemeral Hacker Life ~Reasons for Defeat~

初華の儚いハッカーライフ

～敗北の理由（わけ）～

Story

悪の集団がブラックハッカーを雇い、サイバー攻撃により大金を
稼ぐことが日常だったトキオシティ。
最近では、世のセキュリティ対策が強化され上手くいかなくなっていた。
サイバー攻撃を成功させるために、トキオシティの中で最も勢力が大きい
悪の集団は天才少女ハッカーと呼ばれる「火都初華」をヘッドハンティングする。
天才と呼ばれるハッカーは、このトキオシティのセキュリティ対策を
すり抜けることができるのか……。

登場人物

『安全ファースト株式会社』
セキュリティエバンジェリスト
愛想（あいそ） 零二（れいじ）

天才少女ハッカー
火都（ひいと） 初華（はっか）

悪の集団


トキオシティ
109
セキュリティNo.1
Security City
NO ! HACKER
我々の集団は、初華(はっか)をチームに加えることで更に強くなるな
ん、聞いてるのか初華？
う、うん…
さぁ、我々のアジトについたぞ
ココ？
ギィ…
ギロリ
そうだ今日から初華のアジトにもなる


全員集まってるか？
今日は紹介したい
メンバーがいるんで
聞いてくれ
う、うう……
今日から我々の
チームを
指揮してくれる
天才少女ハッカー
として裏で有名な
火都初華(ひいとはっか)だ
PON!
みんな、名前は
聞いたことがあるん
じゃないか？
さぁ、初華
みんなに挨拶
でもしてくれ
う、うん……
今日から
チームを
指揮する
火都初華
だって……
ざわ・・・・
その姿は初めて見るが
こんな幼かったのか……
火都初華(ひいとはっか)
です
初華、早速だがチームの
メンバーにいろいろと
教えてくれないか？
う、うん
あなた達は
トキオシティで最近強化された
セキュリティ対策を
すり抜けられないって聞いてる
わたしがあなた達に
新しい攻撃手法を
教えてあげる


そうなんだよな、最近セキュリティ対策が強化されてきてな…
どうやったら攻撃を成功させられるんだ初華？
う、うん…
まずは攻撃サイトに誘導するためにリンクをクリックさせないとね
ペラ
ペラ
ペラ
最近はメールのリンクは怪しいってみんな思ってるからSNSを使うことにするわ
メールでリンクを送ると解析されちゃうし
これなら解析されないしみんな危険だって思わないから
!?
な、なるほど…
俺はまだこのチームに入ったばかりで全くわからなかったぞ
?
でもリンクがクリックされた後はそれがURLフィルタリングで検知されないようにしないといけないんじゃ？
不明なWebサイトをブロックしている企業も多いだろ？


それは大丈夫
こんなときのために
何ヶ月も運用している
動画サイトがあるわ
もちろん、普通に動画しか
置いてないから、
どんなURLフィルタリングでも
動画サイトと分類されるはず
攻撃のときだけ
攻撃コードを置いて
後で直ぐに削除すれば
いいってこと

さすが！
用意周到じゃん
さすが！

そ、そうだ…
CAPTCHA(キャプチャ)も入れておこうかな
CAPTCHA(キャプチャ)？


うん
CAPTCHA(キャプチャ)は
知ってるでしょ？
Webサイトにログインするときに
横断歩道や信号機の画像を
選択させるあれよ
これなら、攻撃コードが
セキュリティツールに
解析されないし
アクセスしてくる人を
安心させられるの
横断歩道
すべてのタイルを選択してください。
確認

後はどうやって
ファイルをパソコンまで
届けるかだよな…

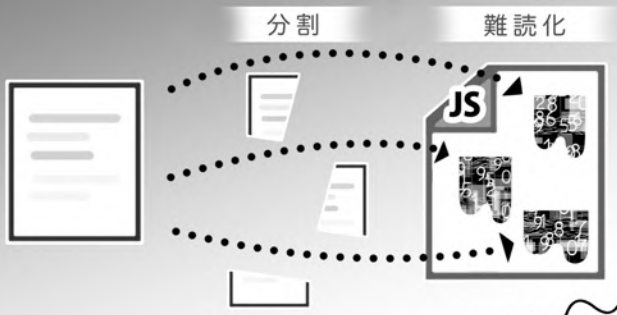
企業のネットワークには
不審なファイルを解析して
ブロックするための

アンチウイルスや
サンドボックスといったのが
いっぱい入っているからな

うん
それも簡単

ネットワークにファイルを
流さなければいいんだから

ファイルを複数のデータに分けて
JavaScriptで書いておけばOK



JavaScriptを読み込んだ
ブラウザが勝手に組み立てて
パソコンにダウンロードしてくれる

流れるのはファイルじゃないから
解析すらされないってこと

JavaScriptとデータも難読化しておけば、
Webページのソースコードを解析することもできないわ

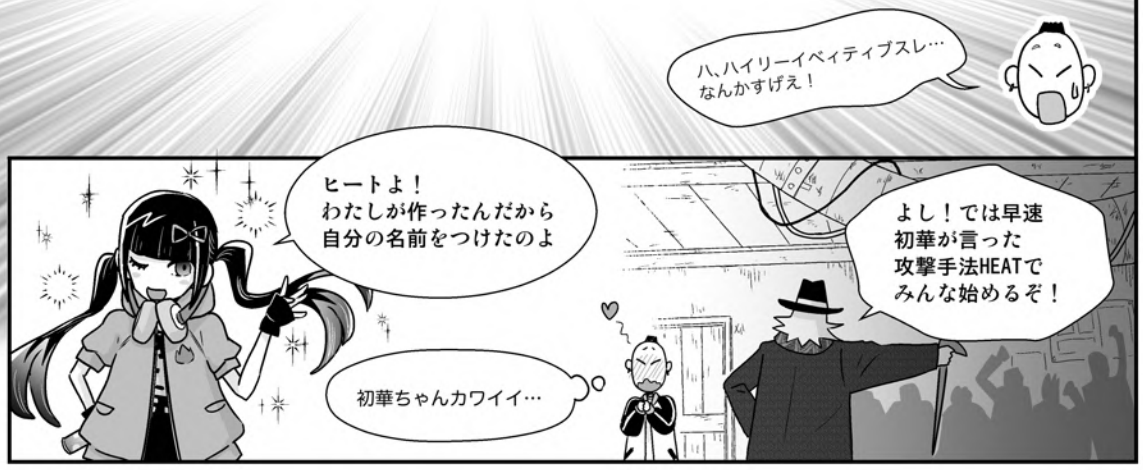
うん
これで、完璧

おおお！

わたしが開発したこれらの攻撃手法は
HEATっていうの

Highly Evasive Adaptive Threats

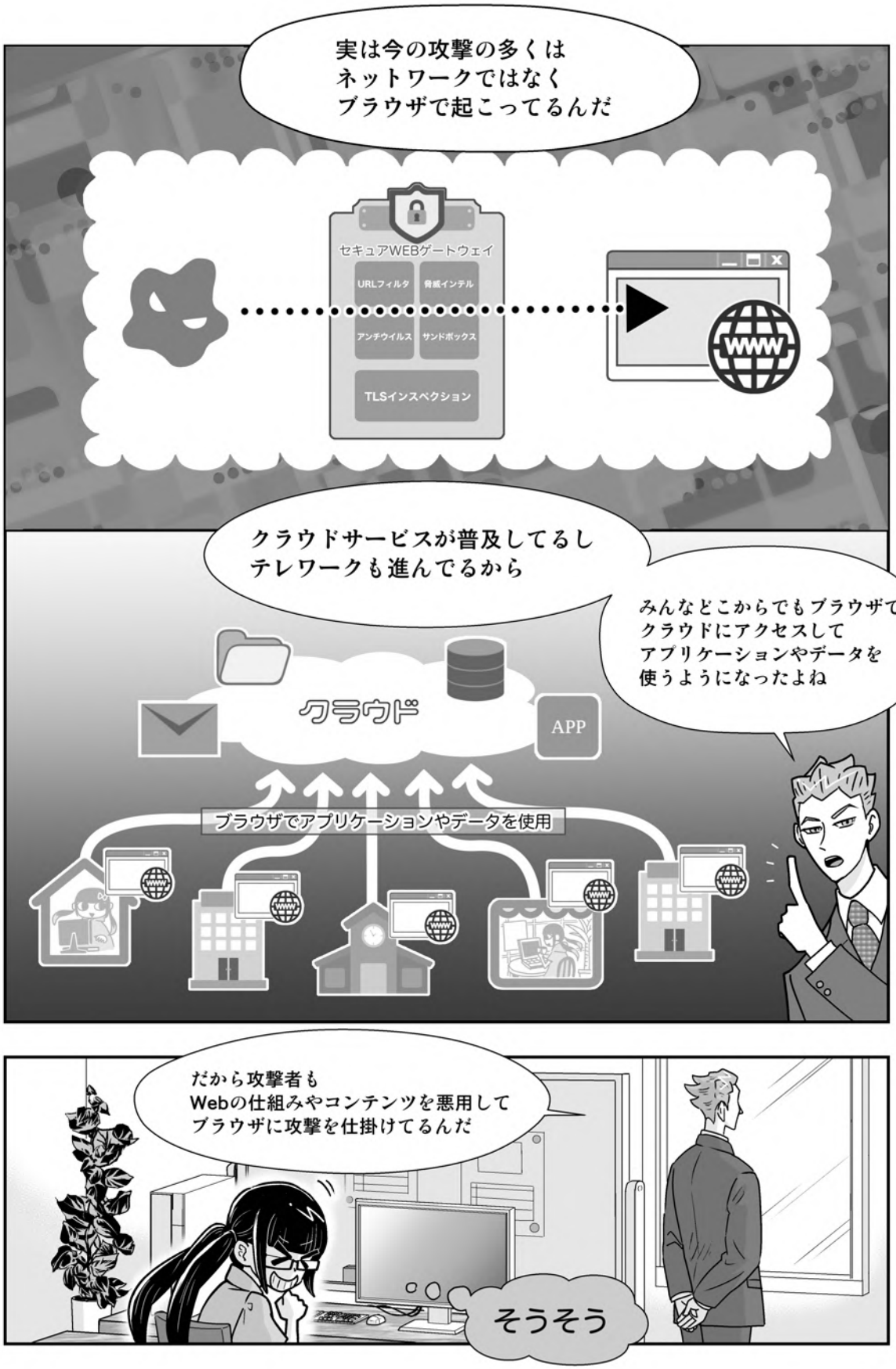
–高度に、回避的で、適応型の脅威–




成功率上がっているけど
この企業だけ失敗が続いているみたいで…
え!!
み、みせて！
え!?
ホント……
これは原因を解明しないといけないよね……
新しいセキュリティ対策だとしたら他の企業が取り入れる前にすり抜けられるようにしなきゃ
わ、わたし…この企業に潜入して原因を突き止めてくる
おいおい、そんな危険なコトして大丈夫なのか？
だ、大丈夫！
すぐ原因を解明して戻ってくる！
初華ちゃんステキ……


安全ファースト株式会社
攻撃が失敗した企業のセキュリティ担当部署に社員として潜入できたわ


さて、初華さん
新しくウチに
入社してくれた
わけだけど
今の
セキュリティ対策の
多くがネットワークで
行われてるのは
知ってるよね
愛想 零二（あいそ れいじ）
セキュリティ担当部署
エバンジェリスト
は、はい
ファイアウォール、IPS、
URLフィルタリング、
アンチウイルス、
サンドボックス……
まあ色々
あるけど
これらのセキュリティ対策が
どうやって攻撃をブロック
してるかというと
ネットワークに流れる
データを解析してるわけ
そ、それって
どういうこと
なんですか？
例えば、トラフィックから
ファイルを取り出して
シグネチャと
照らし合わせたり
仮想マシンで
動かしたりして
それが良いか悪いかを
判断してる
でも、ファイルを
取り出せなかったら
解析できないし
取り出せても
良いか悪いかの
判断を間違えることが
あるしで
OK
NG
結局攻撃がすり抜けて
被害になってるのが
現状…
そうよ、これこそ
わたしたちの
攻撃じゃん
これは最近のニュースを
見てもわかるでしょ
あんなに有名な企業も
サイバー攻撃によって
ランサムウェアの被害に遭ってる
A社もB社もC社も
わたしたちが攻撃
したやつじゃん


実は今の攻撃の多くは
ネットワークではなく
ブラウザで起こってるんだ
セキュアWEBゲートウェイ
URLフィルタ
脅威インテル
アンチウイルス
サンドボックス
TLSインスペクション
WWW
クラウドサービスが普及してるし
テレワークも進んでるから
みんなどこからでもブラウザで
クラウドにアクセスして
アプリケーションやデータを
使うようになったよね
クラウド
APP
ブラウザでアプリケーションやデータを使用
だから攻撃者も
Webの仕組みやコンテンツを悪用して
ブラウザに攻撃を仕掛けてるんだ
そうそう

そこで攻撃を
ネットワーク
ではなく
ブラウザで
見るようにして

良いか悪いかの
判断も止めることで
すり抜けをなくす
ことができるんだ

え？ブラウザで見る
ってどういうこと
なんですか？

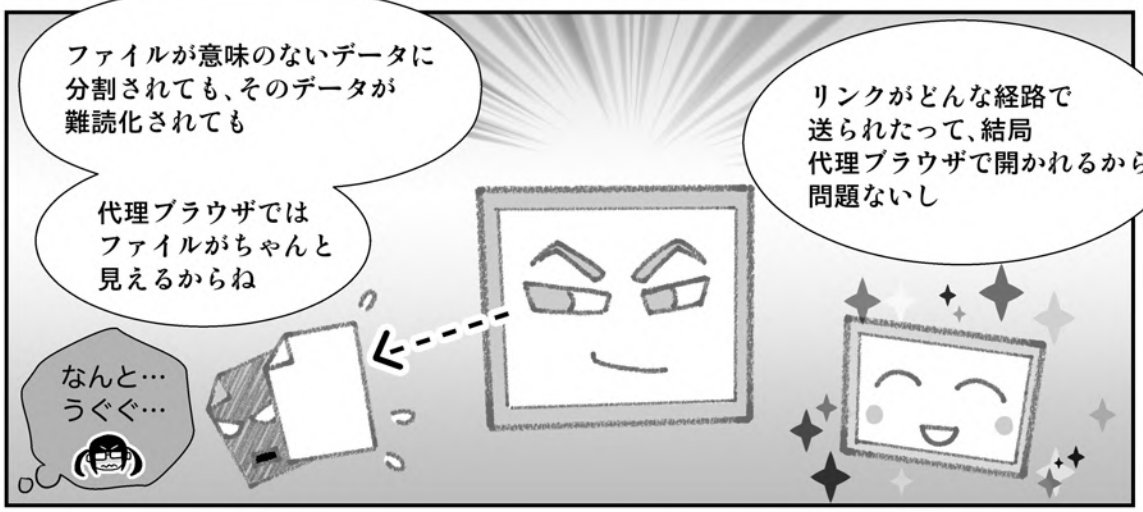
具体的に説明すると…
パソコンとインターネットの間に
代理ブラウザを用意して

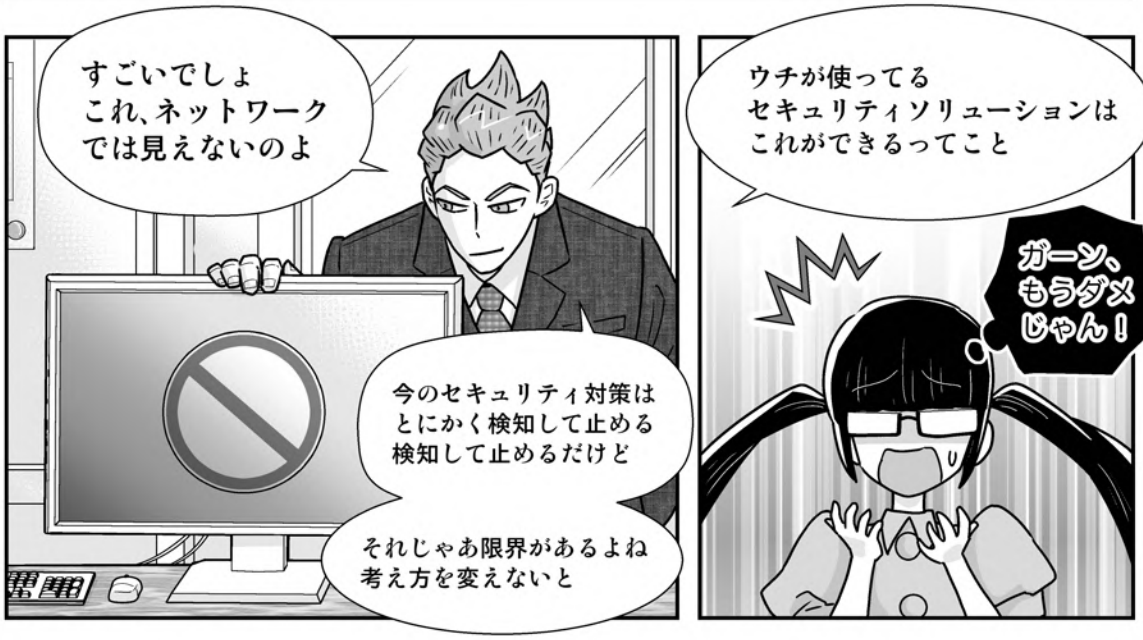
そこで全ての
コンテンツを
実行した後

**安全なものだけを
パソコンのブラウザに
届けるということ**

良いか悪いかに
関係なくね


こうすれば標的のブラウザで
起こるであろう全てを
代理ブラウザで把握できるし
標的のブラウザには
安全なものしか届かないから
SECURITY
よ、よく喋るわね
この人……
ランサムウェアにも
感染することはない
ということになる


ファイルが意味のないデータに
分割されても、そのデータが
難読化されても
代理ブラウザでは
ファイルがちゃんと
見えるからね
なんと…
うぐぐ…
リンクがどんな経路で
送られたって、結局
代理ブラウザで開かれるから
問題ないし


すごいでしょ
これ、ネットワーク
では見えないのよ
今のセキュリティ対策は
とにかく検知して止める
検知して止めるだけど
それじゃあ限界があるよね
考え方を変えないと
ウチが使ってる
セキュリティソリューションは
これができるってこと
ガーン、
もうダメ
じゃん！


ちなみに、ウチで使ってるのは
Menlo Security の
アイソレーション！
MENLO
SECURITY


わかったかな？
天才少女ハッカー
「火都初華」さん？
しかも潜入した
こともバレてた……


初華は、まだ
戻らないのか？
初華ちゃん
早く帰ってきて〜！
最近どこの企業でも
攻撃がたて続けに
失敗してるぞ！

MENLO SECURITY

メンロ・セキュリティ・ジャパン株式会社

〒100-0004 東京都千代田区大手町1-6-1 大手町ビル4階 FINOLAB
www.menlosecurity.jp

お問い合わせ