The Glocalization of Chinese Underground Market

Anna C. , Jack L.

Speakers

- Anna CHUNG
  - iSight Partners Cyber Threat Researcher
- Jack LIN
  - Some CERT Researcher

Glocalization of Underground Economy

丹堤咖啡會員個資傳被駭　千筆資料遭登國外網站

Hannah Wang

2015年 05月 29日 00:22

社會中心／台北報導

國內知名的丹堤咖啡（Dante Coff
出個資遭駭客入侵，千萬筆的客戶
洩，被刊登在俄羅斯網站上，而且
外洩19天，但丹堤咖啡對此完全不
情，目前丹堤咖啡已緊急通知該網
人移除相關資訊，並向台北市刑警

新聞

丹堤咖啡遭駭，5000筆會員個資外洩

有民眾發現國外論壇網站張貼疑似丹堤咖啡五千筆會員資料，包括姓名、性別、聯絡電話及住址，丹堤已緊急聯絡該論壇刪除資料，同時加強清查補強內部系統安全。

文/ 蘇文彬 | 2015-05-29 發表

按讚加入iThome粉絲團

What is “Glocalization”?

- A combination of the words "globalization" and "localization" used to describe a product or service that is developed and distributed globally, but is also fashioned to accommodate the user or consumer in a local market.

Agenda

- Major changes since 2011
- Who is the target
- How do cyber crime actors make money out of your data
- Chinese underground characters
- Current situation on the Chinese underground market
- TTPs of how Chinese actors targeting JP online bank users
- Conclusion and prediction
- Q & A

Timeline

- 2011 : Cyber crime advertisement everywhere!!
- 2012 : Major strike down by Chinese law enforcement
- 2013 : All cyber crime discussion and ads switch to IM (QQ)
- 2014 : New monetization service introduced to China

  US- Green Dot

  Japan & S Korea – Online game credits monetization

  French – DDoS stressers
- 2015 : Aggressive cyber crime activity targeting Japan

What are hackers interested in?

- Payment information ⟶ Online Shopping Sites
- Online banking credentials ⟶ Banks
- Personal Identifiable Information ⟶ (HR company, Telecom companies)
- Email login credentials or any account include a password and your email information ⟶ (pretty much everywhere…)

How do cyber crime actors make money

- Payment information
  - Making purchase online and resell the products.
  - Making payment on behalf of local consumers

- Online banking credentials (Banks)
  - Transfer money to multiple money mule accounts

- Personal Identifiable Information
  - Send out spamming email and messages, to lure actor contact the fraudsters

- Email login credentials (pretty much everywhere…)
  - Identify password reused accounts from other websites
  - Login email accounts to look for sensitive information

Chinese Underground Characters

- Average price is lower than other regions
- A large number of cyber crime actors involved
- Each actor covers/specialized a very small part of cyber crime activities
- Mostly target on individual victims, not enterprise.
- Communication highly rely on instant messaging (QQ)
- Most underground deals go through Alipay (Only small proportion accept Bitcoin or WMZ)
- Financial profit is the highest priority, very few actors care about the reputation

Current Status of CN Underground

	US	UK&AU	Eastern Europe & Russian Forums	Japan	S. Korea	Other SE Asian Countries
Login credentials	√	√		√	√	√
debit and credit card information	√	√	√	√	√	√
Green Dot prepaid card/ accounts	√					
eBay accounts	√	√		√		
PayPal accounts and credits	√	√				
Facebook accounts	√					
Money mule services	√			√	√	
Payment services	√			√	√	
POS services	√					
Online Bank source code				√		
Online game accounts				√	√	
Bank accounts for rent				√		
Phishing sites				√		
Malware obfuscation				√	√	

日本を踏み台に米韓へサイバー攻撃する中国犯罪グループ　押収「代理サーバー」から“仰天犯罪情報”

産経新聞 5月21日（木）20時38分

警視庁などが東京都豊島区の業者から昨年押収した中国向け「プロキシ（代理）サーバー」から、個人情報やハッキングツールが大量に見つかっている。サーバーは中国にいる犯行グループがサイバー犯罪に悪用しているとみられ、代理サーバーが「犯罪インフラ」となっていたことが改めて浮き彫りとなった。捜査幹部によると「これでも解析が終わったのはごく一部」。警視庁がサーバーの解析を急ぎ、全容解明を進める。

関係先を捜索し、押収した大量のパソコンをトラックに積む捜査員。「プロキシサーバー」がサイバー犯罪に悪用されている

■中国の接続は各国が制限

代理サーバーは利用者と接続先を中継するサーバーで、本来、企業によるネット接続の一元管理や接続速度を速くする目的で設けられる。またサーバーを中継すると、接続先に残るＩＰアドレス（ネット上の住所）が代理サーバーのものに置き換わるため、匿名性が高くなるという特徴もある。

中国など特定の国からの接続は犯罪目的が多く、多くの国の金融機関などが接続を制限する傾向にある。こうしたことから中国の犯罪グループは代理サーバーを利用してＩＰアドレスを日本のものに置き換え、さまざまなサイトに接続して犯行を繰り返していたとみられている。

警視庁などは昨年１１月、豊島区の代理サーバー業者「ＳＵＮテクノ」の関係先などを家宅捜索し、不正入手したパスワードでネットに接続したとして、これまでに同社社長や従業員の中国人ら男８人を、不正アクセス禁止法違反容疑などで逮捕した。

■パスワードの使い回し狙う

家宅捜索で押収した中継サーバーは、いまも警視庁が解析を進めている。約半年たった４月には一定の内容がわかり、同庁が公表した。

サーバーの中から見つかったのは、アカウント乗っ取りのためのハッキングツール▽インターネットバンキングの不正送金に使うフィッシングサイトの画面▽約５０６万人分のＩＤやパスワードなど、さまざまな犯罪ツールだ。

特に目を引くのが、パスワードの使い回しに目を付けてプログラミングされたハッキングツールで、何らかの理由で流出したＩＤとパスワードを読み込ませると、そのＩＤとパスで別のサイトにもログインできるか自動的に調べる仕組みを持っている。防衛策として、誤ったＩＤやパスワードを連続して入れると、不正と認識して遮断するサイトもあるが、今回確認されたツールは数秒単位でＩＰアドレスを変える機能を持っており、連続接続が可能となっている。

利用者が複数のサイトでパスワードを使い回していればログインでき、アカウントの乗っ取りができてしまう。犯罪者にログインされれば、預金を別口座に送金されたり、勝手に買い物をされたりする可能性がある。

ツールは代理サーバー内で、約５０６万人分の日本、米国、韓国、台湾の個人情報と一緒に保存されていた。ツールを通した流出データのうち５万９千人分が、ネット通販大手「楽天」や「アマゾンジャパン」、無料通信アプリ「ＬＩＮＥ（ライン）」のサイトでログインに成功していた。

http://www.sankei.com/premium/news/150520/prm1505200006-n1.html

關鍵詞

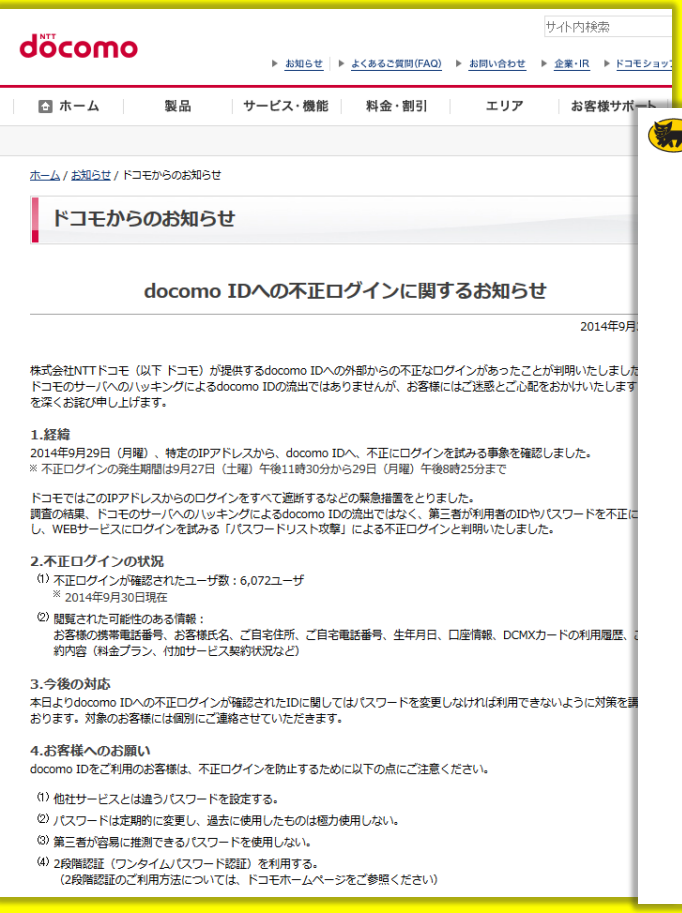
「犯罪インフラ」

パスワードの使い回し

中国犯罪グループ

代理サーバー

フィッシングサイト



docomo

サイト内検索

お知らせ | よくあるご質問(FAQ) | お問い合わせ | 企業・IR | ドコモショップ

ホーム | 製品 | サービス・機能 | 料金・割引 | エリア | お客様サポート

ホーム / お知らせ / ドコモからのお知らせ

ドコモからのお知らせ

docomo IDへの不正ログインに関するお知らせ

2014年9月

株式会社NTTドコモ（以下 ドコモ）が提供するdocomo IDへの外部からの不正なログインがあったことが判明いたしました。
ドコモのサーバへのハッキングによるdocomo IDの流出ではありませんが、お客様にはご迷惑とご心配をおかけいたします
を深くお詫び申し上げます。

1.経緯

2014年9月29日（月曜）、特定のIPアドレスから、docomo IDへ、不正にログインを試みる事象を確認しました。
※ 不正ログインの発生期間は9月27日（土曜）午後11時30分から29日（月曜）午後8時25分まで

ドコモではこのIPアドレスからのログインをすべて遮断するなどの緊急措置をとりました。
調査の結果、ドコモのサーバへのハッキングによるdocomo IDの流出ではなく、第三者が利用者のIDやパスワードを不正に
し、WEBサービスにログインを試みる「パスワードリスト攻撃」による不正ログインと判明いたしました。

2.不正ログインの状況

(1) 不正ログインが確認されたユーザ数：6,072ユーザ
※ 2014年9月30日現在

(2) 閲覧された可能性のある情報：
お客様の携帯電話番号、お客様氏名、ご自宅住所、ご自宅電話番号、生年月日、口座情報、DCMXカードの利用履歴、ご
約内容（料金プラン、付加サービス契約状況など）

3.今後の対応

本日よりdocomo IDへの不正ログインが確認されたIDに関してはパスワードを変更しなければ利用できないように対策を講
おります。対象のお客様には個別にご連絡させていただきます。

4.お客様へのお願い

docomo IDをご利用のお客様は、不正ログインを防止するために以下の点にご注意ください。

(1) 他社サービスとは違うパスワードを設定する。
(2) パスワードは定期的に変更し、過去に使用したものは極力使用しない。
(3) 第三者が容易に推測できるパスワードを使用しない。
(4) 2段階認証（ワンタイムパスワード認証）を利用する。
（2段階認証のご利用方法については、ドコモホームページをご参照ください）

NEWS RELEASE

ヤマトホールディング
ヤマト運輸株式

平成26年9月

クロネコメンバーズWebサービスへの不正ログインに関するお知らせ

このたび、ヤマトホールディングス傘下のヤマト運輸株式会社（本社：東京都中央区・代表取締役社長 山内 雅喜）が提供するクロネコメンバーズ（主に個人の方を対象とした会員制サービス）のWebサービスにおきまして、外部から不正ログインがあり、一部のお客様の個人情報が閲覧された可能性があることが判明しました。クロネコメンバーズのお客様をはじめとする皆様にはご迷惑とご心配をお掛けいたしましたことを心よりお詫び申し上げます。

1．経緯

平成26年9月25日（木）、特定のIPアドレスからの不正なログインを確認し、緊急の措置として、該当のIPアドレスからのログインを遮断するなどの対策を講じました。調査の結果、不正なログインに使用されたID・パスワードは弊社で使用されていないものが多数含まれており、他社サービスのID・パスワードを使用した「パスワードリスト攻撃※」による不正ログインと判明しました。

※「パスワードリスト攻撃」・・・ 他社サービスから流出した可能性のあるIDとパスワードを利用して、Webサービスにログインを試みる手法です。

2．不正ログインの状況

（1）不正ログイン件数：10,589件（不正ログイン試行件数は約19万件）※9/26 17:00現在
（2）閲覧された可能性のある項目：
クロネコID、メールアドレス、利用の端末種別（パソコンまたは携帯・スマートフォン）、氏名、氏名ふりがな、電話番号、性別、郵便番号、住所
※ クロネコメンバーズ会員のうち、メールアドレスを登録していないお客様は、今回の事象による被害の可能性はございません。

3．弊社の対応策

個人情報を不正に閲覧された可能性のあるクロネコIDは、パスワードを変更しなければ使用できないように対策を講じております。対象のお客様へは、弊社より個別にご案内いたします。

4．お客様へのお願い

お客様には不正ログイン防止の観点から、定期的なパスワードの変更をお願いいたします。なお、パスワードを設定する際は以下の点にご注意ください。
（1）他のサービスでご利用になっているパスワードを使用しない。
（2）定期的にパスワードを変更し、過去に使用したものは極力使用しない。
（3）第三者が容易に推測できるパスワードを使用しない。

SAGAWA TRANSPORT COMMUNICATION

お知らせ

WEBトータルサポート（旧Webサービス）会員情報への不正ログインに関するお知らせ

2014.09.29

このたび弊社が提供するWEBトータルサポート（旧Webサービス）にご登録いただいているお客さまの会員情報に、外部から不正ログインがあり、一部のお客さまの個人情報が閲覧された可能性があることが判明しました。皆さまにはご迷惑とご心配をお掛けいたしましたことを心よりお詫び申し上げます。

1.経緯

弊社では不正アクセスへの監視を定期的に実施しております。その結果、9月28日（日）に「WEBトータルサポート（旧Webサービス）」システムにおいてサーバ高負荷状態が発生したことを確認いたしました。緊急でアクセス解析を行ったところ、特定のIPアドレスからの不正なログインがあり、緊急の措置として、該当のIPアドレスからのログインを遮断するなどの対策を講じました。調査の結果、不正なログインに使用されたID・パスワードは弊社で使用されていないものが多数含まれており、他社サービスのID・パスワードを使用した「パスワードリスト攻撃」による不正ログインと推測されます。

2.不正ログインの状況

1. 不正ログイン件数：34,161件（個人会員：33,501件、法人会員：660件）
2. 閲覧された可能性のある項目
WEB会員ID、メールアドレス、氏名、氏名カナ、郵便番号、住所、電話番号、性別

3.弊社の対応

個人情報を不正に閲覧された可能性のあるWEB会員IDは、パスワードを変更しなければ使用できないように対策を講じております。なお、対象のお客さまへは弊社より個別にご案内いたします。

4.お客さまへのお願い

お客さまには不正ログイン防止の観点から、定期的なパスワードの変更をお願いいたします。なお、パスワードを設定する際には以下の点にご注意ください。

http://itpro.nikkeibp.co.jp/atcl/column/14/346926/100700073/?SS=imgview&FD=-41675079

企業名(サービス名)	漏洩の原因*1	対外公表日	漏洩、もしくは漏洩の可能性のあるデータ件数
NTTドコモ(「My docomo」など)	リスト型攻撃	9月30日	6072件
佐川急便(「Webサービス」)	リスト型攻撃	9月29日	3万4161件
ヤマト運輸(「クロネコメンバーズWebサービス」)	リスト型攻撃	9月26日	1万589件
日本航空	標的型攻撃	9月24日	最大約75万件
東日本旅客鉄道(「My JR-EAST」)	リスト型攻撃	9月12日	約2万1000件
米グーグル(「Gmail」)	リスト型攻撃	9月10日(米国時間)	約500万件
NTTコミュニケーションズ、NTTレゾナント(「gooポイント」など)	リスト型攻撃	7月30日	1265件
NTTコミュニケーションズ(「思い出あんしん保管」)	脆弱性を突いた侵入	7月23日	378件
NTTドコモ(「法人モバイル管理サービス」)	内部犯行	9月9日	1053件
東日本旅客鉄道(「Suicaポイントクラブ」)	リスト型攻撃	8月18日	756件
ベネッセホールディングス	内部犯行	7月9日	3504万件
サイバーエージェント	リスト型攻撃	6月23日	3万8280件
はてな	リスト型攻撃	6月20日	2398件
ミクシィ	リスト型攻撃	6月17日	約26万件
ドワンゴ	リスト型攻撃	6月13日	約29万5000件
LINE	リスト型攻撃	6月12日	303件
パナソニック(「CLUB Panasonic」)	リスト型攻撃	4月23日	7万8361件
全日本空輸(「ANAマイレージクラブ」)	総当たり攻撃	3月10日	9件
ミクシィ	リスト型攻撃	2月28日	1万6972件
ソフトバンクモバイル(「My SoftBank」)	リスト型攻撃	2月28日	344件
横浜銀行	内部犯行	2月5日	キャッシュカード口座80件、クレジットカード口座52件
日本航空(JALマイレージバンク)	総当たり攻撃	2月3日	43件
ストリーム(「ECカレント」など)	脆弱性を突いた侵入	1月30日	最大9万4359件
スタイライフ	リスト型攻撃	1月21日	最大2万4158件

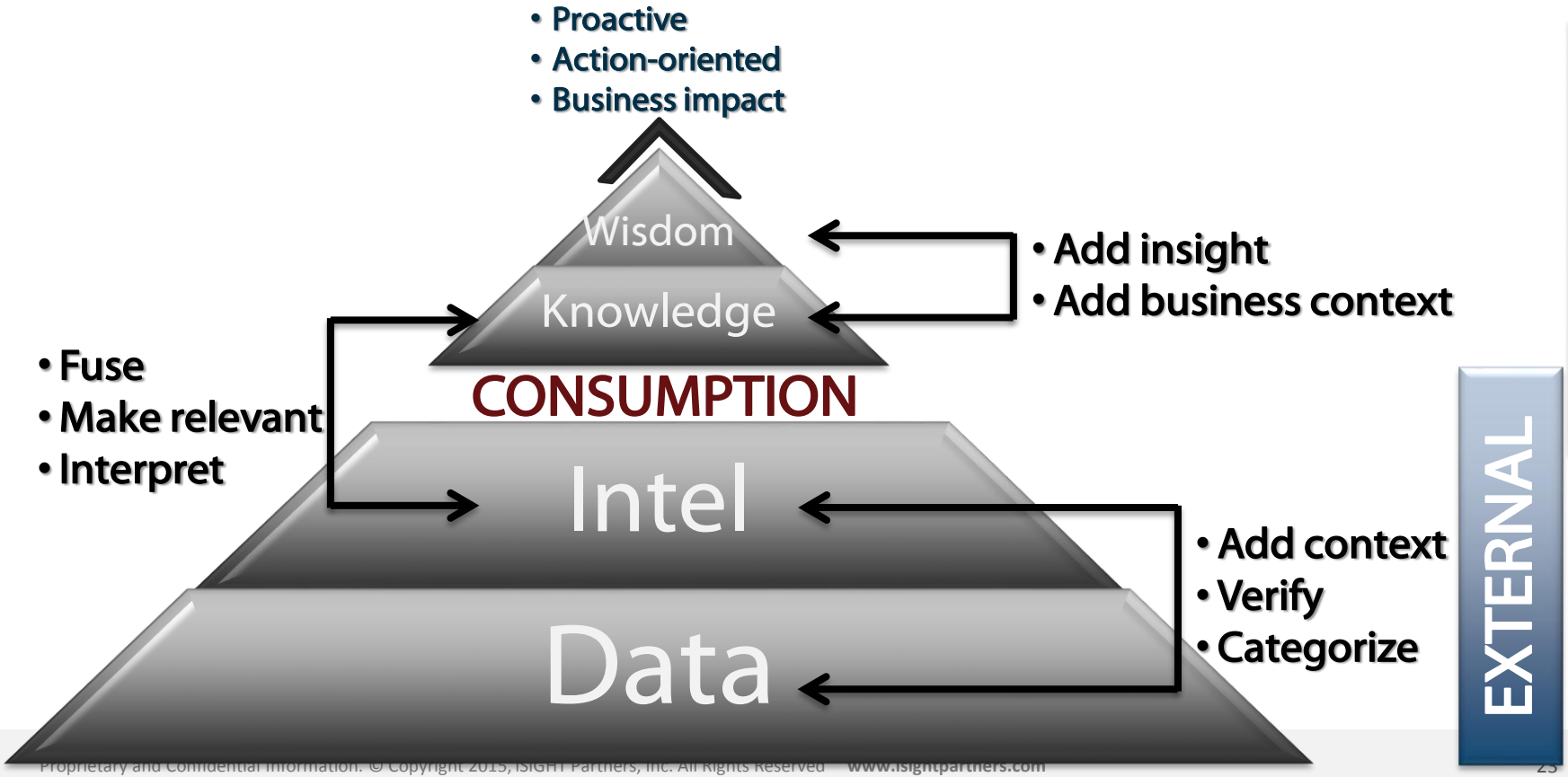
*1 一部本誌推定　出所:「ITpro」の記事を基に作成

http://itpro.nikkeibp.co.jp/atcl/column/14/346926/100700073/?SS=imgview&FD=1379216241&ST=security

Conclusion and Prediction

- Activities against Japan and S. Korea is more aggressive than other countries, and it will continuously grow.
- Due to the language barrier and information access, the money laundering approaches is approximately two years behind Eastern Europe.
- More activities will target neighbor countries such as Singapore, Malaysia, Philippine, and Myanmar.
- More actors might physically move to these neighbor countries for its rich target, fast internet, and loose law enforcement.

Threat Intelligence Pyramid



Q & A

THANK YOU!!!

