Avaddon ランサムウェアの解析

解析レポート

2020

安全なネット活用のための

セキュリティ情報

はじめに

マルウェアなどのインターネット上の脅威は日々高度化・巧妙化が進み、法人、個人を問わず金銭的被害や機密情報の漏えいなどリスクも増大しています。このような状況においては、被害に遭わないために最新動向を知り、適切なセキュリティ対策を実施することが重要です。

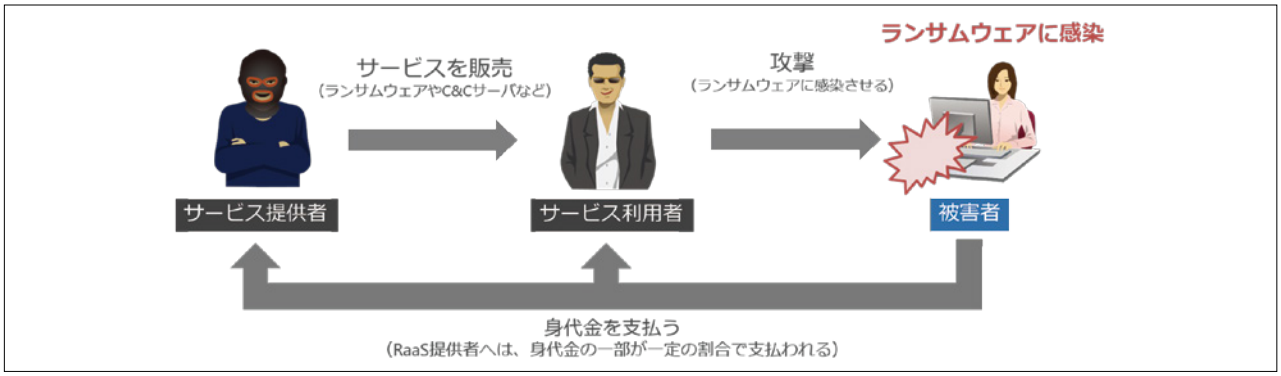
サイバーセキュリティに関する研究を担うサイバーセキュリティラボを中核に、最新の脅威やマルウェアの動向の情報収集および分析を実施し、セキュリティ対策に必要な情報をレポートとして発行しています。

「Avaddon（アヴァドン）」は2020年に確認されたRaaS型のランサムウェアです。
本レポートでは、Avaddonの日本国内に向けた攻撃事例や、Avaddonの各バージョンにおける内部構造の変化を紹介します。

contents

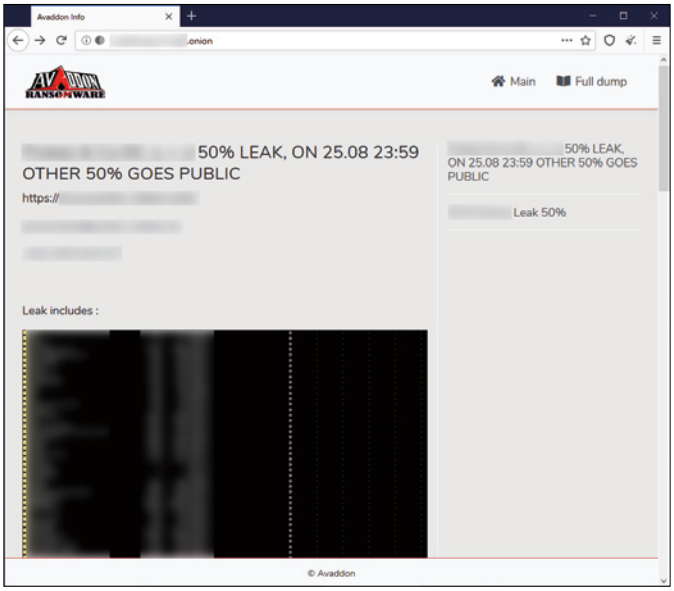
1. Avaddonランサムウェアの概要

AvaddonはRaaS（Ransomware as a Service）として提供されているランサムウェアです。2020年6月上旬にAvaddonのサービス提供者はロシア語のフォーラム上で「Avaddonアフィリエイトプログラム」と題してサービスを開始しました。Avaddonランサムウェアを使った攻撃は数多くのバリエーションが確認されており、複数の攻撃者がサービスを利用していると考えられます。



RaaS（Ransomware as a service）のイメージ

また、8月にはAvaddonのサービス提供者は窃取した機密情報を公開するためのWebサイトを立ち上げています。これは二重の脅迫（double extortion）と呼ばれる手法で、被害者からさらなる金銭を要求するためにMazeやNemty等多くのランサムウェアのオペレーターが採用しています。現時点ではAvaddonランサムウェア自体にファイル等を抽出する機能が確認されていないことから、他のツールを使用して情報を窃取していると考えられます。
9月1日時点で、3つの組織が脅迫の対象となっています。

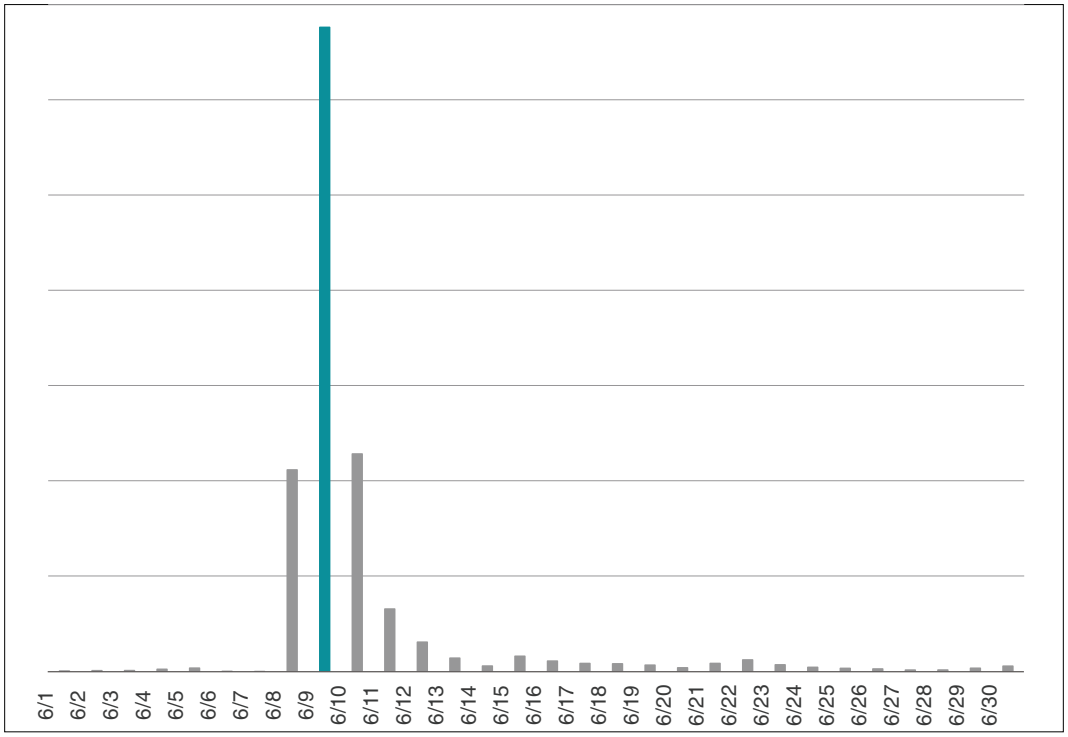


Avaddonの情報公開脅迫Webサイト

2. Avaddonランサムウェアの感染経路

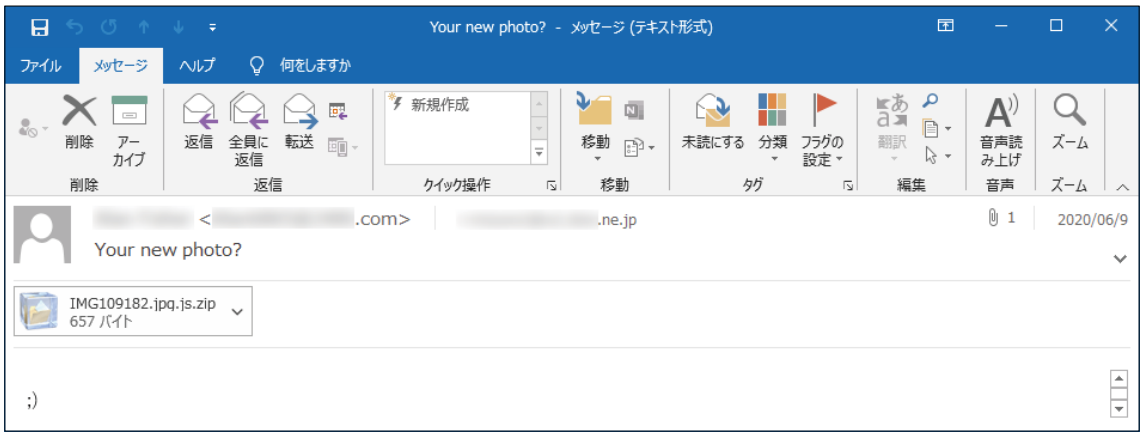
Avaddonランサムウェアの感染経路は複数確認されています。RIGエクスプロイトキットを悪用したDrive-By Download攻撃や、Excelマクロを添付したメールによる攻撃等が確認されていますが、本稿ではとりわけ多く拡散されたPhorpiexボットネットを使用した攻撃について分析します。

Phorpiexは2019年の初め頃に登場したボットネットです。過去にはGandCrabランサムウェアの配信にも使われています。
2020年6月5日頃、Phorpiexボットネットを使用したAvaddonランサムウェアの拡散は始まりました。6月9日には日本のメールアドレス宛にメールが多数送信されました。
このメールはESET製品でJS/Danger.ScriptAttachmentとして検出されています。



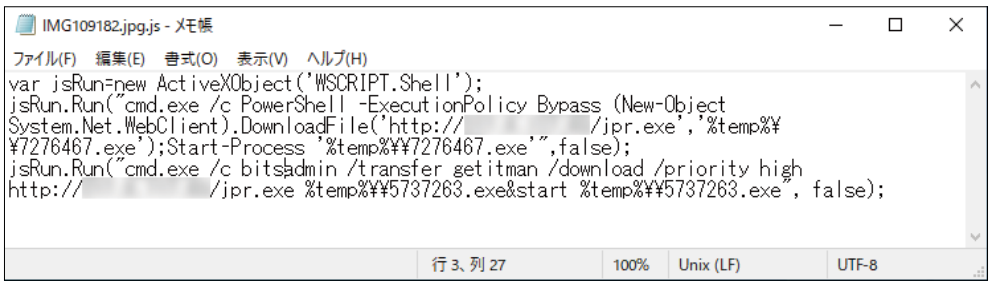
JS/Danger.ScriptAttachmentの日別検出数の推移（2020年・日本国内）

日本のメールアドレス宛に送られたメールは「You look good here」等の件名で、本文には顔文字が書かれています。



JPドメインのメールアドレス宛のメール

添付ファイルのファイル名は「IMG{数字6桁}.jpg.js.zip」や「Photo_{数字6桁}_jpg.js.zip」の形式で、中には画像ファイルに偽装したJavaScriptダウンローダーが含まれています。

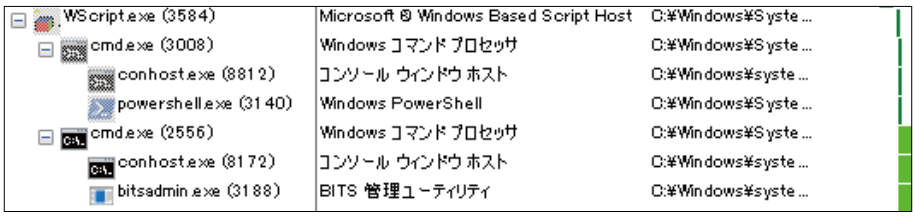


JavaScript形式のダウンローダー

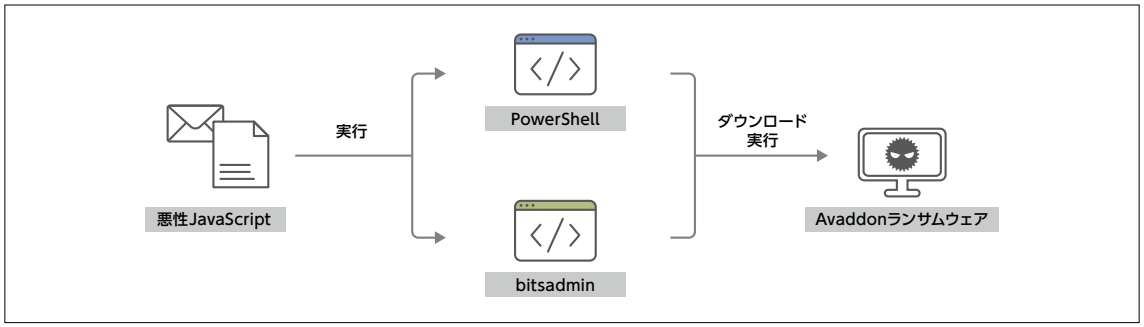
7月7日頃からは難読化され大量のダミーコードが挿入されたJavaScriptダウンローダーが確認されています。

JavaScript形式のダウンローダー(難読化されたバージョン)

これらのJavaScriptはPowerShellとbitsadminをそれぞれ実行してAvaddonランサムウェアのダウンロードおよび実行を試みます。bitsadminはWindowsに標準でインストールされているコマンドラインツールで、インターネット上にあるファイルのダウンロードが可能です。
マルウェアがPowerShellを悪用することは一般によく知られており、PowerShellの通信をブロックする製品・運用も多いことから、別の手法を併用していると考えられます。



JavaScript形式ダウンローダーのプロセスツリー



Avaddonランサムウェアのダウンロードの流れ

3. Avaddonランサムウェアの解析

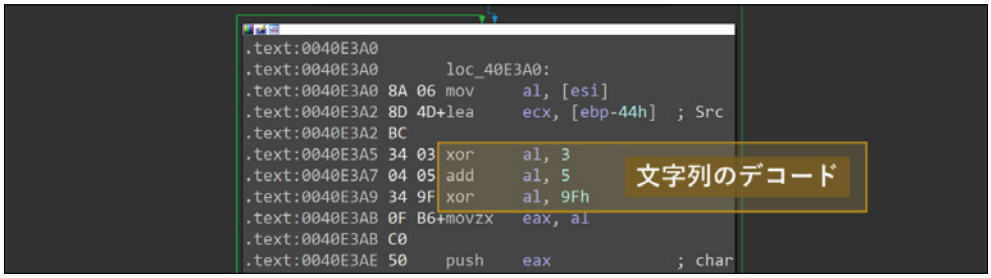
PhorpiexボットネットでAvaddonランサムウェア本体を詳しく解析します。

Avaddonはいくつかの文字列を暗号化してプログラム内部に保持しており、その暗号化(復号)方法は複数のバリエーションが確認されています。本稿では、その暗号化方式ごとにバージョン番号を独自に採番しています。以降、注釈がない限り全バージョン共通の特徴・挙動です。

バージョン	観測日	主な変更点	文字列のデコード計算式
1	2020/6/5		sub 2 xor 43h
2	2020/6/21	• デバッグ検知機構の変更 • 取得する端末情報の変更	sub 4 xor 92h
3	2020/7/7	• ロケールIDチェックの変更 • 暗号化ファイルの拡張子の変更 • ランサムノートの変更	xor 3 add 5 xor 9Fh

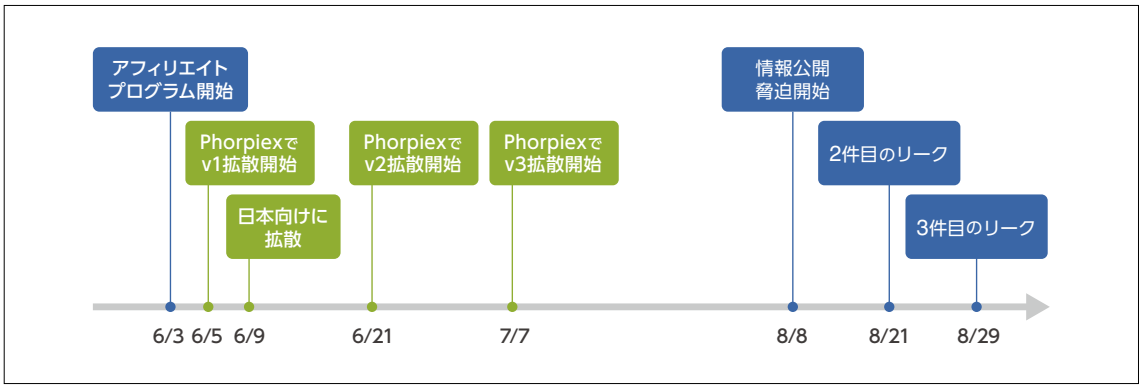
Avaddonバージョンの推移

暗号化されている文字列は、変更するレジストリの値や実行するコマンドなどです。アンチウイルスプログラムによる検出や解析者による解析を防ぐため、暗号化されていると考えられます。リストに含まれる文字列はバージョンにより差異があります。



文字列をデコードするコードの一部

復号した文字列(色付きは差分)



Avaddonに関連するイベントのタイムライン

Avaddonランサムウェアはファイルを暗号化するだけではなく、様々な機能を持っています。以下、順番に紹介します。

- 環境検知
- 自身のコピーとスケジュール作成
- UACの無効化とバイパス
- プロセスとサービスの終了
- ファイル復元の防止
- ファイルの暗号化
- ランサムノートの作成

■ 環境検知

Avaddonには実行されたOSの言語環境をチェックする機能が備わっており、以下の環境では暗号化せずにプロセスが終了します。言語のリストにはロシアおよびウクライナで使用される言語が含まれており、アフィリエイトプログラムがロシア語のフォーラムで展開されていることと関連性があります。
バージョン3ではウクライナ語の代わりにチェロキー語（アメリカ合衆国の一部で使用される言語）がロケールIDのリストに含まれていますが、これにはアンチウイルス製品のシグネチャによる検出を回避する狙いがあると考えられます。

ロケールID
- 0x419: ロシア語
- 0x422: ウクライナ語 ※バージョン1および2
- 0x45C: チェロキー語 ※バージョン3

キーボードレイアウト
- 0x419: ロシア語
- 0x485: サハ語（主にロシアで使用される言語）
- 0x444: タタール語（主にロシアで使用される言語）
- 0x422: ウクライナ語

```
v11 = GetUserDefaultLCID();
v12 = v11 != 0x419 && v11 != 0x422;
v13 = v10 && v12;
v14 = (unsigned __int16)GetKeyboardLayout(0);
if ( v14 != 0x419 && v14 != 0x485 && v14 != 0x444 && v14 != 0x422 && v13 )
```

言語環境をチェックするコード(バージョン1および2)

```
v2 = GetUserDefaultLCID();
v3 = v2 == 0x419 || v2 == 0x45C;   バージョン3で変更
v4 = (unsigned __int16)GetKeyboardLayout(0);
if ( v4 == 0x419 || v4 == 0x485 || v4 == 0x444 || v4 == 0x422 )
  result = 1;
```

言語環境をチェックするコード(バージョン3)

また、IsDebuggerPresent関数を使いデバッガーで実行されているかどうかを検知します。
次に、GetThreadContext関数でハードウェアブレークポイントが使用されているかどうかを確認します。
バージョン2以降ではCheckRemoteDebuggerPresent関数も使われています。

```
if ( !IsDebuggerPresent() )
{
  memset(&Context.Dr0, 0, DEBUG_DATA_KdPrintCircularBufferPtrAddr);
  Context.ContextFlags = CONTEXT_DEBUG_REGISTERS;
  v8 = GetCurrentThread();
  if ( !GetThreadContext(v8, &Context) || !Context.Dr0 && !Context.Dr1 && !Context.Dr2 && !Context.Dr3 )
  {
```

デバッガーを検知するコード(バージョン1)

```
if ( !IsDebuggerPresent() )
{
  pbDebuggerPresent = 1;
  v0 = GetCurrentProcess();
  if ( CheckRemoteDebuggerPresent(v0, &pbDebuggerPresent) )   バージョン2で追加
  {
    if ( !pbDebuggerPresent && !IsDebuggerPresent() )
    {
      memset_(&Context.Dr0, 0, DEBUG_DATA_KdPrintCircularBufferPtrAddr);
      Context.ContextFlags = CONTEXT_DEBUG_REGISTERS;
      v1 = GetCurrentThread();
      if ( !GetThreadContext(v1, &Context) || !Context.Dr0 && !Context.Dr1 && !Context.Dr2 && !Context.Dr3 )
        result = 0;
```

デバッガーを検知するコード(バージョン2および3)

■ 自身のコピーとスケジュール作成

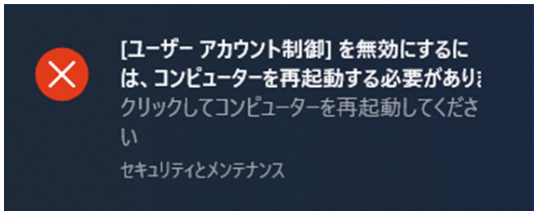
実行ファイル自身を%APPDATA%\Microsoft\Windowsフォルダーにコピーし、自動的に実行されるようにタスクスケジューラに登録します。既に暗号化を行っている場合は繰り返し暗号化を行うことはありません。

タスクスケジューラに登録されたタスク

■ UACの無効化とバイパス

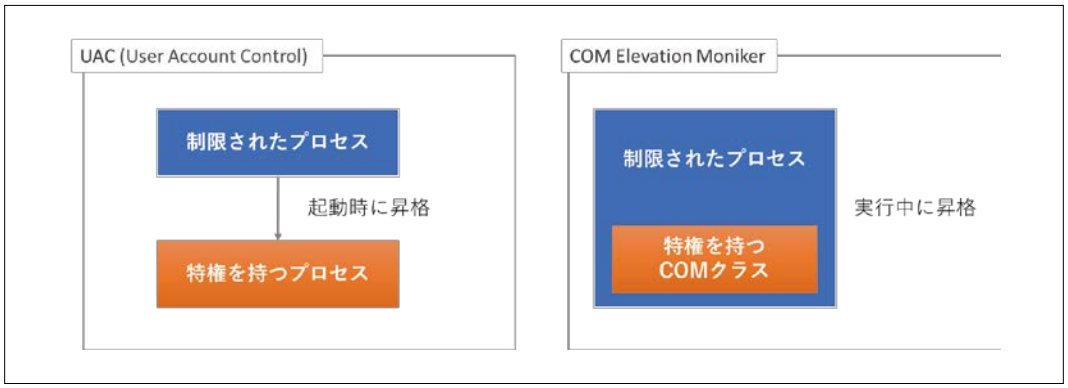
ユーザーアカウント制御(UAC)を無効にするため、以下のレジストリ値を0に設定します。設定が変更されると再起動を促す通知が表示され、再起動後に設定が有効になります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
```



再起動を促す通知

管理者権限で実行されなかった場合はCOM Elevation Moniker[1]と呼ばれる手法を悪用して、UACをバイパスして管理者権限によるコード実行を試みます。UACの無効化がプロセス全体の権限を昇格させるのに対して、COM Elevation Monikerは制限されたプロセスの中でCOMクラスの権限を昇格させます。これにより、(いくつか制限はあるものの)特権を必要とする機能の実行が可能になります。



UACとCOM Elevation Monikerのイメージ

```
while ( CoGetObject(pszName, &pBindOptions, &iid, &ppv) )
  ;                                    // pszName = Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
result = ppv;
```

COM Elevation Monikerで権限を昇格するコード

1 The COM Elevation Moniker | Microsoft

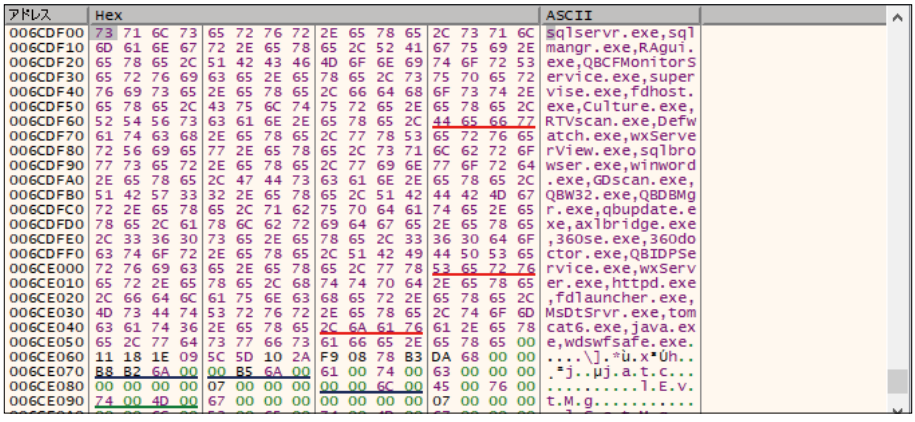
https://docs.microsoft.com/en-us/windows/win32/com/the-com-elevation-moniker

■ プロセスとサービスの終了

以下のプロセスが実行されていた場合、終了させます。

文書作成プログラムやアンチウイルスプログラム、データベース関連のプログラム等がリストに含まれています。これらのプロセスに開かれている作業中のファイルを暗号化するための機能と考えられます。

```
sqlservr.exe
sqlmangr.exe
RAgui.exe
QBCFMonitorService.exe
supervise.exe
fdhost.exe
Culture.exe
RTVscan.exe
Defwatch.exe
wxServerView.exe
sqlbrowser.exe
winword.exe
GDscan.exe
QBW32.exe
QBDBMgr.exe
qbupdate.exe
axlbridge.exe
360se.exe
360doctor.exe
QBIDPService.exe
wxServer.exe
httpd.exe
fdlauncher.exe
MsDtSrvr.exe
tomcat6.exe
java.exe
wdswfsafe.exe
```

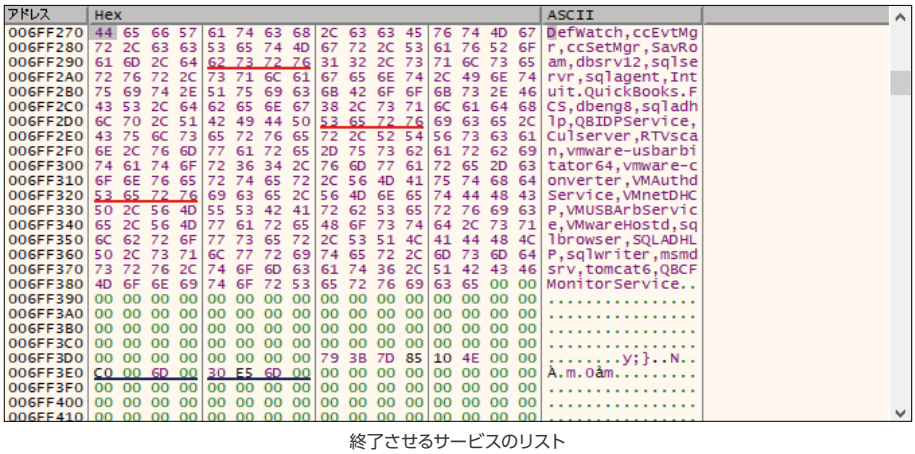


アドレス	Hex	ASCII
006CDF00	73 71 6C 73 65 72 76 72 2E 65 78 65 2C 73 71 6C	sqlservr.exe,sql
006CDF10	6D 61 6E 67 72 2E 65 78 65 2C 52 41 67 75 69 2E	mangr.exe,RAgui.
006CDF20	65 78 65 2C 51 42 43 46 4D 6F 6E 69 74 6F 72 53	exe,QBCFMonitorS
006CDF30	65 72 76 69 63 65 2E 65 78 65 2C 73 75 70 65 72	ervice.exe,super
006CDF40	76 69 73 65 2E 65 78 65 2C 66 64 68 6F 73 74 2E	vise.exe,fdhost.
006CDF50	65 78 65 2C 43 75 6C 74 75 72 65 2E 65 78 65 2C	exe,Culture.exe,
006CDF60	52 54 56 73 63 61 6E 2E 65 78 65 2C 44 65 66 77	RTVscan.exe,Defw
006CDF70	61 74 63 68 2E 65 78 65 2C 77 78 53 65 72 76 65	atch.exe,wxServe
006CDF80	72 56 69 65 77 2E 65 78 65 2C 73 71 6C 62 72 6F	rView.exe,sqlbro
006CDF90	77 73 65 72 2E 65 78 65 2C 77 69 6E 77 6F 72 64	wser.exe,winword
006CDFA0	2E 65 78 65 2C 47 44 73 63 61 6E 2E 65 78 65 2C	.exe,GDscan.exe,
006CDFB0	51 42 57 33 32 2E 65 78 65 2C 51 42 44 42 4D 67	QBW32.exe,QBDBMg
006CDFC0	72 2E 65 78 65 2C 71 62 75 70 64 61 74 65 2E 65	r.exe,qbupdate.e
006CDFD0	78 65 2C 61 78 6C 62 72 69 64 67 65 2E 65 78 65	xe,axlbridge.exe
006CDFE0	2C 33 36 30 73 65 2E 65 78 65 2C 33 36 30 64 6F	,360se.exe,360do
006CDFF0	63 74 6F 72 2E 65 78 65 2C 51 42 49 44 50 53 65	ctor.exe,QBIDPSe
006CE000	72 76 69 63 65 2E 65 78 65 2C 77 78 53 65 72 76	rvice.exe,wxServ
006CE010	65 72 2E 65 78 65 2C 68 74 74 70 64 2E 65 78 65	er.exe,httpd.exe
006CE020	2C 66 64 6C 61 75 6E 63 68 65 72 2E 65 78 65 2C	,fdlauncher.exe,
006CE030	4D 73 44 74 53 72 76 72 2E 65 78 65 2C 74 6F 6D	MsDtSrvr.exe,tom
006CE040	63 61 74 36 2E 65 78 65 2C 6A 61 76 61 2E 65 78	cat6.exe,java.ex
006CE050	65 2C 77 64 73 77 66 73 61 66 65 2E 65 78 65 00	e,wdswfsafe.exe.
006CE060	11 18 1E 09 5C 5D 10 2A F9 08 78 B3 DA 68 00 00	....\].*ù.x³Úh..
006CE070	B8 B2 6A 00 00 B5 6A 00 61 00 74 00 63 00 00 00	¸²j..µj.a.t.c...
006CE080	00 00 00 00 07 00 00 00 00 00 6C 00 45 00 76 00	..........l.E.v.
006CE090	74 00 4D 00 67 00 00 00 00 00 00 00 07 00 00 00	t.M.g...........

終了させるプロセスのリスト

以下のサービスを終了させます。
リストにはデータベース関連のサービスが多く含まれており、データベースファイルが重要なターゲットであることが伺えます。

DefWatch
ccEvtMgr
ccSetMgr
SavRoam
dbsrv12
sqlservr
sqlagent
Intuit.QuickBooks.FCS
dbeng8
sqladhlp
QBIDPService
Culserver
RTVscan
vmware-usbarbitator64
vmware-converter
VMAuthdService
VMnetDHCP
VMUSBArbService
VMwareHostd
sqlbrowser
SQLADULP
sqlwriter
msmdsrv
tomcat6
QBCFMonitorService



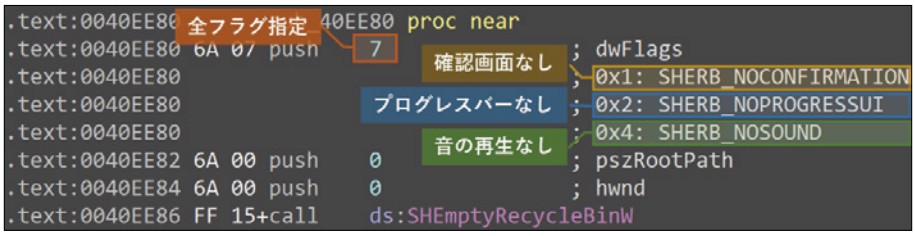
終了させるサービスのリスト

■ ファイル復元の防止

シャドウコピーからのファイル復旧や自動修復を防ぐため、以下のコマンドを実行します。

```
wmic.exe SHADOWCOPY /nointeractive
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
vssadmin.exe Delete Shadows /All /Quiet
```

また、SHEmptyRecycleBin関数でゴミ箱を空にします。



ゴミ箱を空にするコード

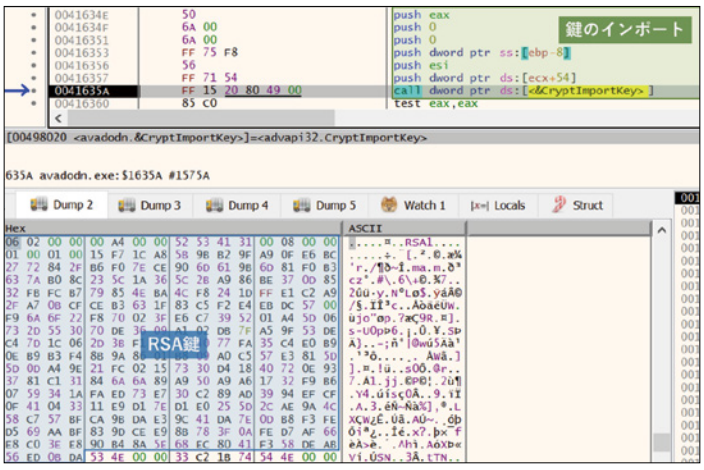
■ ファイルの暗号化

GetLogicalDrives関数で現在のコンピューターの論理ドライブの情報をすべて取得し、WNetGetConnection関数でネットワークドライブのUNCパスを取得します。

また、NetShareEnum関数を使ってSMB共有フォルダーのパスを列挙します。

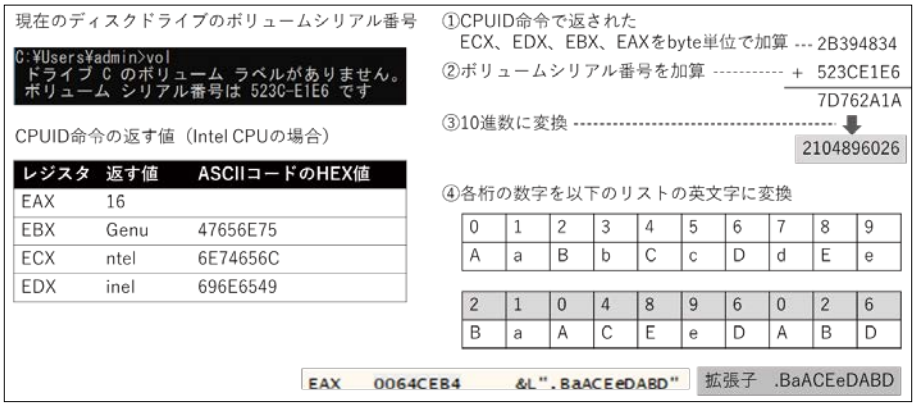
取得・列挙したフォルダーのファイルをCryptEncrypt関数でAES暗号化します。

ファイルの暗号化に使用したAES鍵はRSA公開鍵で暗号化されます。



RSA鍵と鍵のインポート処理

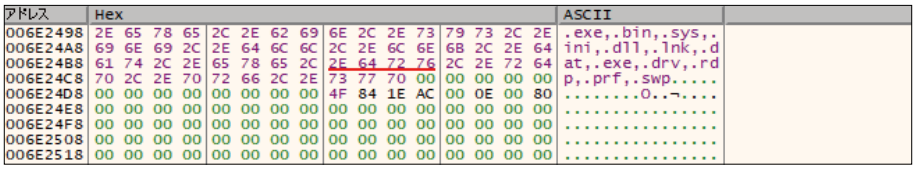
暗号化されたファイルには拡張子.avdnが付与されます。(バージョン1および2)
バージョン3では、Avaddonが実行されているディスクドライブのボリュームシリアル番号とCPUの種類に依存する9～10文字の英文字の拡張子が付与されます。



暗号化されたファイルに付与される拡張子の生成(バージョン3)

以下の拡張子のファイルは暗号化の対象から除外されます。

```
.exe .bin .sys .ini .dll .lnk .dat .exe .drv .rdp .prf .swp
```



除外する拡張子のリスト

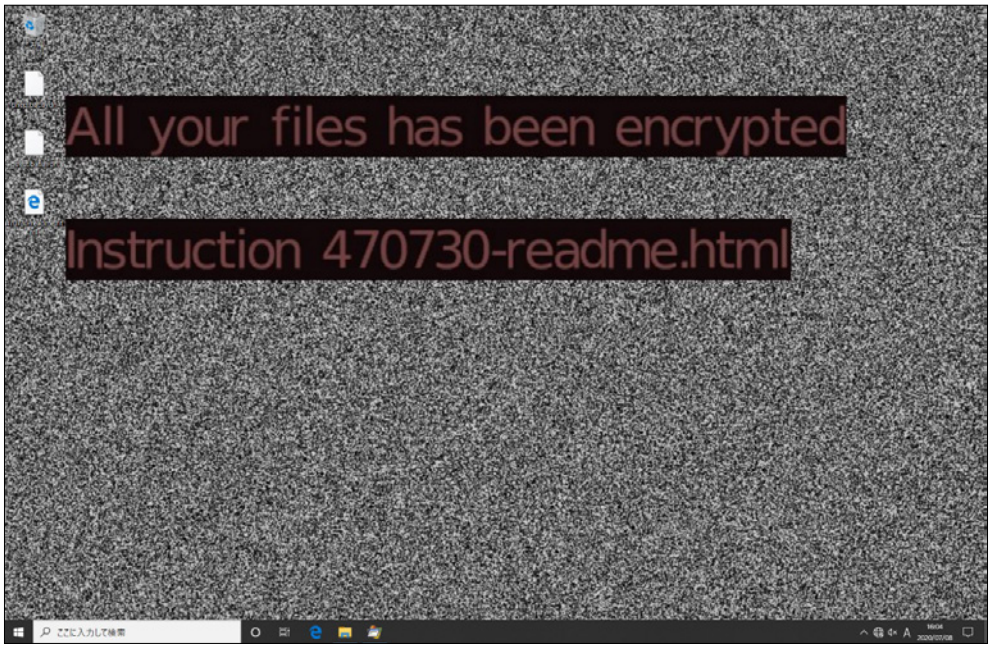
以下のフォルダー内のファイルは暗号化の対象から除外されます。

```
%SYSTEMDRIVE%
%PROGRAMFILES(x86)%
%USERPROFILE%
ProgramData
Program Files
%ALLUSERSPROFILE%
AppData
%PUBLIC%
Tor Browser
MSOCache（バージョン3のみ）
```

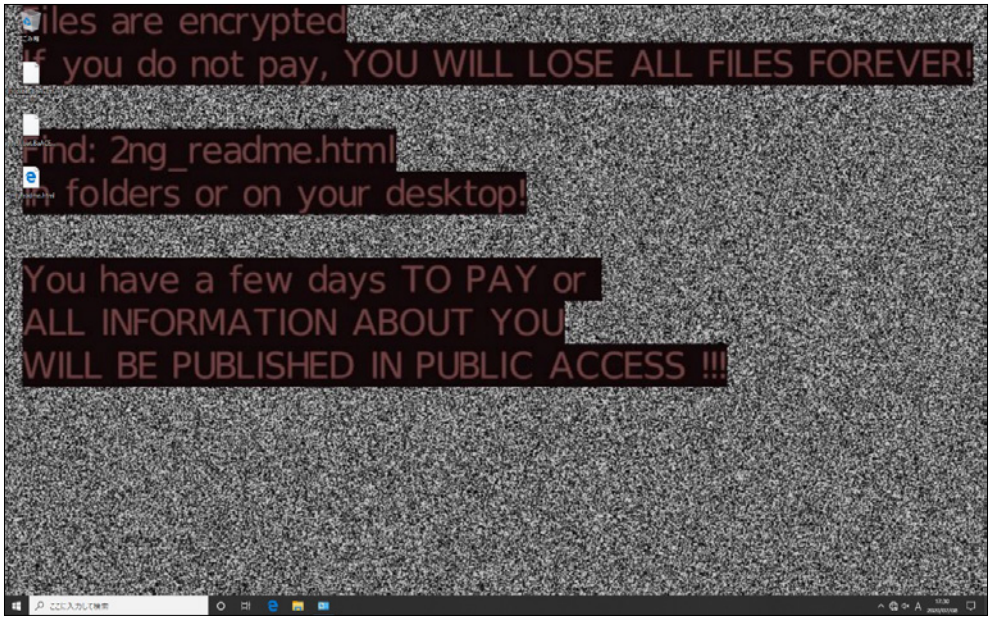
ただし、以下のフォルダーのファイルは暗号化されます。

```
\Program Files\Microsoft\Exchange Server
\Program Files (x86)\Microsoft\Exchange Server
\Program Files\Microsoft SQL Server
\Program Files (x86)\Microsoft SQL Server
```

暗号化後、デスクトップの壁紙が変更されます。
バージョン3以降では、支払いに応じない場合はデータを公開するという旨の脅迫文が追加されています。

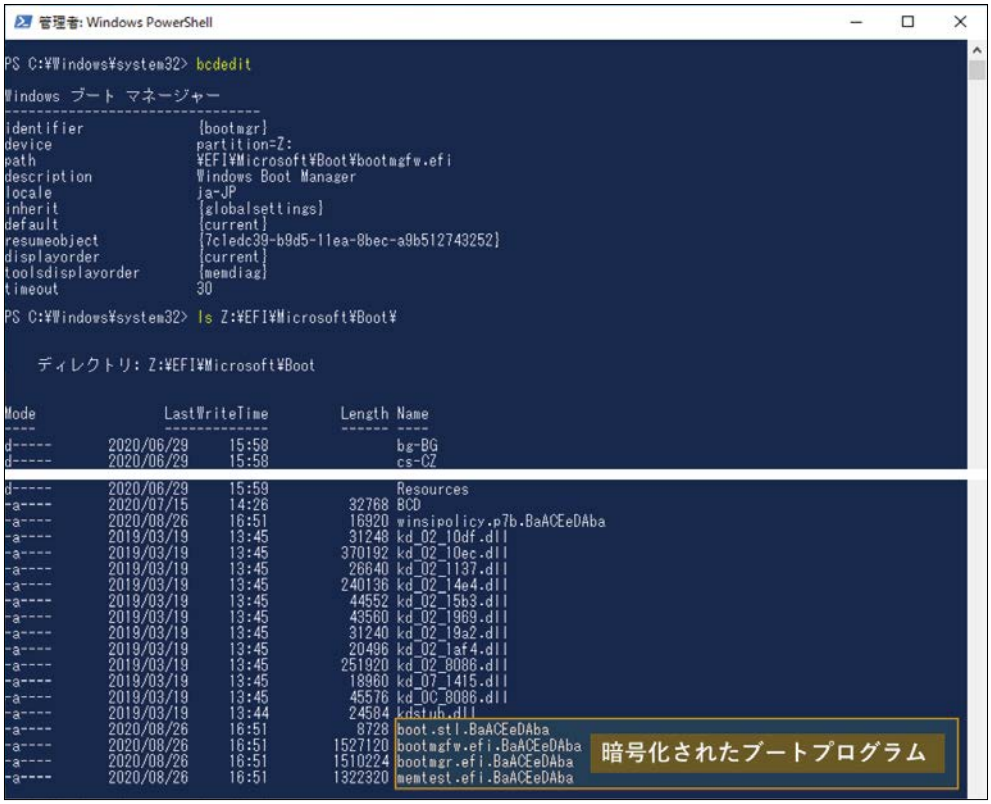


感染後のデスクトップ(バージョン1および2)



感染後のデスクトップ(バージョン3)

なお、AvaddonがVMware上で実行されている場合、AvaddonはWindows ブート マネージャーにドライブレターを割り当てた後にブートプログラムを暗号化します。そのため、一度再起動を行うとWindowsが起動しなくなります。



暗号化されたWindows ブート マネージャー

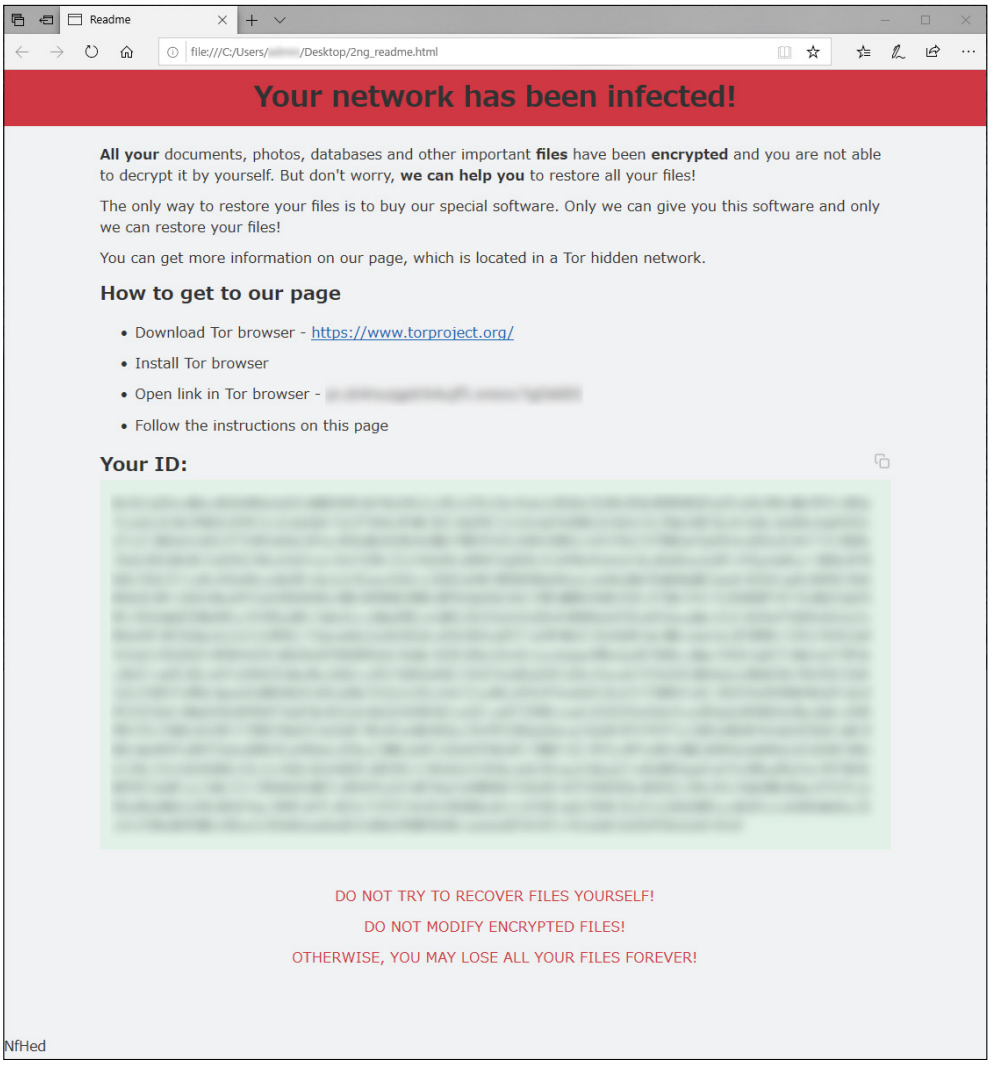
```
Attempting to start up from:
 → Windows Boot Manager... No Media.
 → EFI VMware Virtual SCSI Hard Drive (0.0)... No compatible bootloader found.
 → EFI Floppy... No Media.
 → EFI VMware Virtual SATA CDROM Drive (1.0)... No Media.
 → EFI Network... unsuccessful.
 → EFI Internal Shell (Unsupported option)... unsuccessful.
 → EFI Network...
```

Windowsの起動に失敗する様子

■ ランサムノートの作成

HTML形式のランサムノート(身代金要求文書)を各フォルダーに作成します。

ランサムノートには身代金の支払い方法や”Your ID”の文字列が記載されています。



ランサムノート（身代金要求文書）

“Your ID”には、暗号化された以下の情報が含まれています。攻撃者が感染PCの状態を知るため、これらの情報を収集していると考えられます。収集する情報はAvaddonのバージョンによって差異があります。

“Your ID”に含まれる情報	バージョン1	バージョン2	バージョン3
グローバルIDアドレス	○	○	○
ファイルの暗号化に使用したAES鍵	○	○	○
各ディスクドライブの情報 • ドライブレター • 容量［GB］（小数点未満切り捨て） • ローカルかネットワークかのフラグ		○	○
OSの言語		○	○
コンピューター名		○	○
暗号化したファイルに付与された拡張子			○

各バージョンの”Your ID”に含まれる情報

```
0081550E 39 45 31 38 43 32 32 42 45 44 41 45 33 39 30 37 9E18C22BEDAE3907
0081551E 45 45 46 46 38 36 32 36 31 37 31 41 36 35 37 41 EEFF8626171A657A
0081552E 42 30 44 44 44 38 41 22 2C 22 68 64 64 22 3A 20 B0DDD8A","hdd":
0081553E 5B 7B 22 6E 61 6D 65 22 3A 22 43 22 2C 22 73 69 [{"name":"C","si
0081554E 7A 65 22 3A 35 39 2C 22 74 79 70 65 22 3A 22 6C ze":59,"type":"l
0081555E 6F 63 61 6C 22 7D 2C 7B 22 6E 61 6D 65 22 3A 22 ocal"},{"name":"
0081556E 44 22 2C 22 73 69 7A 65 22 3A 30 2C 22 74 79 70 D","size":0,"typ
0081557E 65 22 3A 22 6C 6F 63 61 6C 22 7D 5D 2C 22 6C 61 e":"local"}],"la
0081558E 6E 67 22 3A 22 4A 61 70 61 6E 65 73 65 22 2C 22 ng":"Japanese","
0081559E 6E 61 6D 65 22 3A 22 44 45 53 4B 54 4F 50 2D 46 name":"DESKTOP-F
```

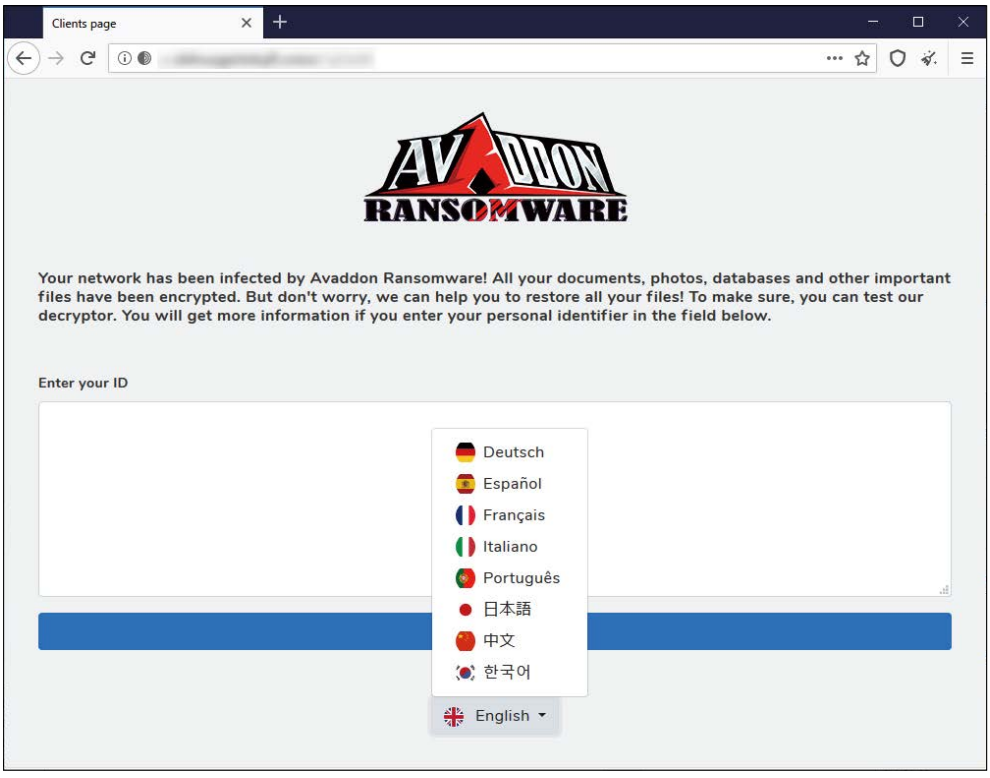
“Your ID”に含まれる情報の一部(バージョン3)

感染PCのグローバルIPアドレスはapi.myip.comに対してHTTPリクエストを送信することで取得します。myip.comは攻撃者が用意したWebサイトではなく、一般的に利用されているWebサイトです。

api.myip.comのレスポンスデータの例

4. 身代金の支払いWebサイト

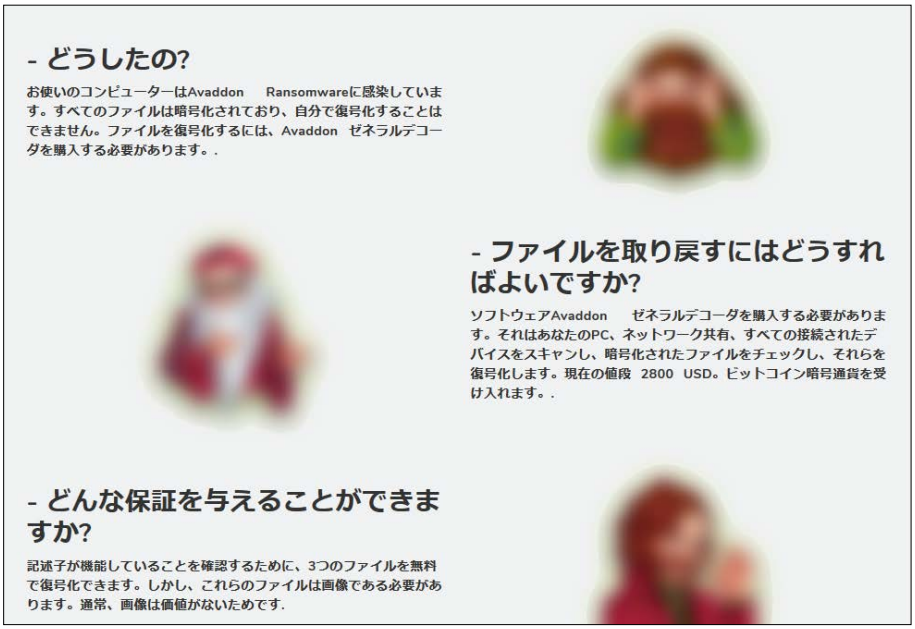
身代金の支払いWebサイトはonionドメイン上に用意されており、日本語のほか8つの言語に対応しています。ランサムノートに記載された”Your ID”を入力することで、次の画面に進みます。



身代金支払いWebサイトのスタートページ

次のページでは、身代金の金額、送付先のビットコインアドレス、身代金の支払い期限等の情報が表示されます。このページにアクセスした時点で、支払い期限のカウントが開始されます。身代金の金額や支払い期限はいくつかのパターンを確認しており、Avaddonインフラの利用者（攻撃者）が設定可能であると考えられます。
FAQページやデコーダのテスト用ページ、チャットによるサポートなども用意されています。

身代金支払いWebサイトのメインページ



身代金支払いWebサイトのFAQページ

身代金支払いWebサイトのデコーダテストページ

5. まとめ

AvaddonはRaaSで提供される高機能なランサムウェアです。頻繁にバージョンアップを重ねており、今後さらに機能が増えることも考えられます。
また、Avaddonの運営者は8月には情報公開脅迫を始めています。脅迫の対象は今後も増え続けることが予想されます。
ランサムウェアへの感染や機密情報の窃取を防ぐために、以下のセキュリティ対策を推奨します。

■ ランサムウェアへの感染やツールによる情報窃取を防ぐための対策

- オペレーティングシステムやソフトウェアに常に最新の更新プログラムを適用する
- エンドポイントのアンチウイルス製品を導入し、最新の状態に保つ
- Officeのマクロ実行設定が無効になっていることを確認する
- スクリプトファイル（JavaScript、VBScript等）を開く規定のアプリケーションをテキストエディタ等に変更する（スクリプトファイルを実行させないようにする）
- ファイアウォールの設定を見直す

■ ランサムウェアに感染した場合に被害を最小限に抑えるための対策

- 定期的にバックアップを取得し、バックアップはネットワークのセグメントを分けておく
- ファイルサーバーのアクセス権設定やファイル共有の設定を確認する
- 管理共有を無効にする
- ファイアウォールの設定を見直す

6. IoCs（侵入の痕跡情報）

ダウンローダー（JavaScript）

平文	a481d2b64c546f68d55e1fd23e57ada80b6b4e2c3dd7b0466380dba465f3d318
難読化	6389e3c49b6f4009ca0f1631436d481065a3b3cfab7a15a073edbb61dd971c73

Avaddon（実行形式ファイル）

v1	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
v2	fa4626e2c5984d7868a685c5102530bd8260d0b31ef06d2ce2da7636da48d2d6
v3	7b4a13c022f0948f0a7ace0c2ea8b85af4f596338af14c3a1be2e63f55cbb335

強くて軽い。
妥協なきセキュリティ。

ESET®

ENJOY SAFER TECHNOLOGY™

Canon キヤノンマーケティングジャパン株式会社

〒108-8011 東京都港区港南2-16-6 CANON S TOWER TEL. 03-6701-3452

MWJY2010CMJ_PDF