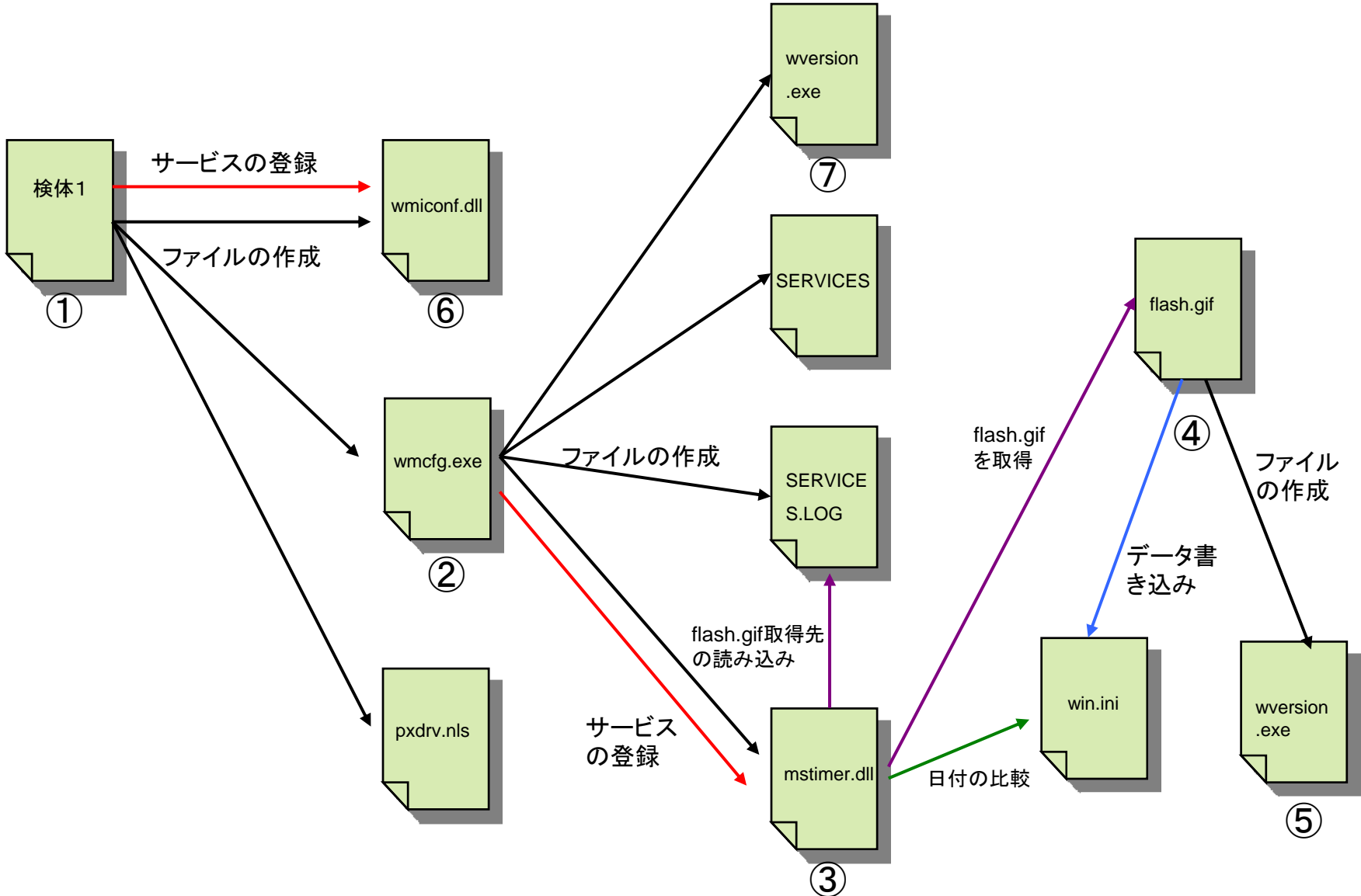
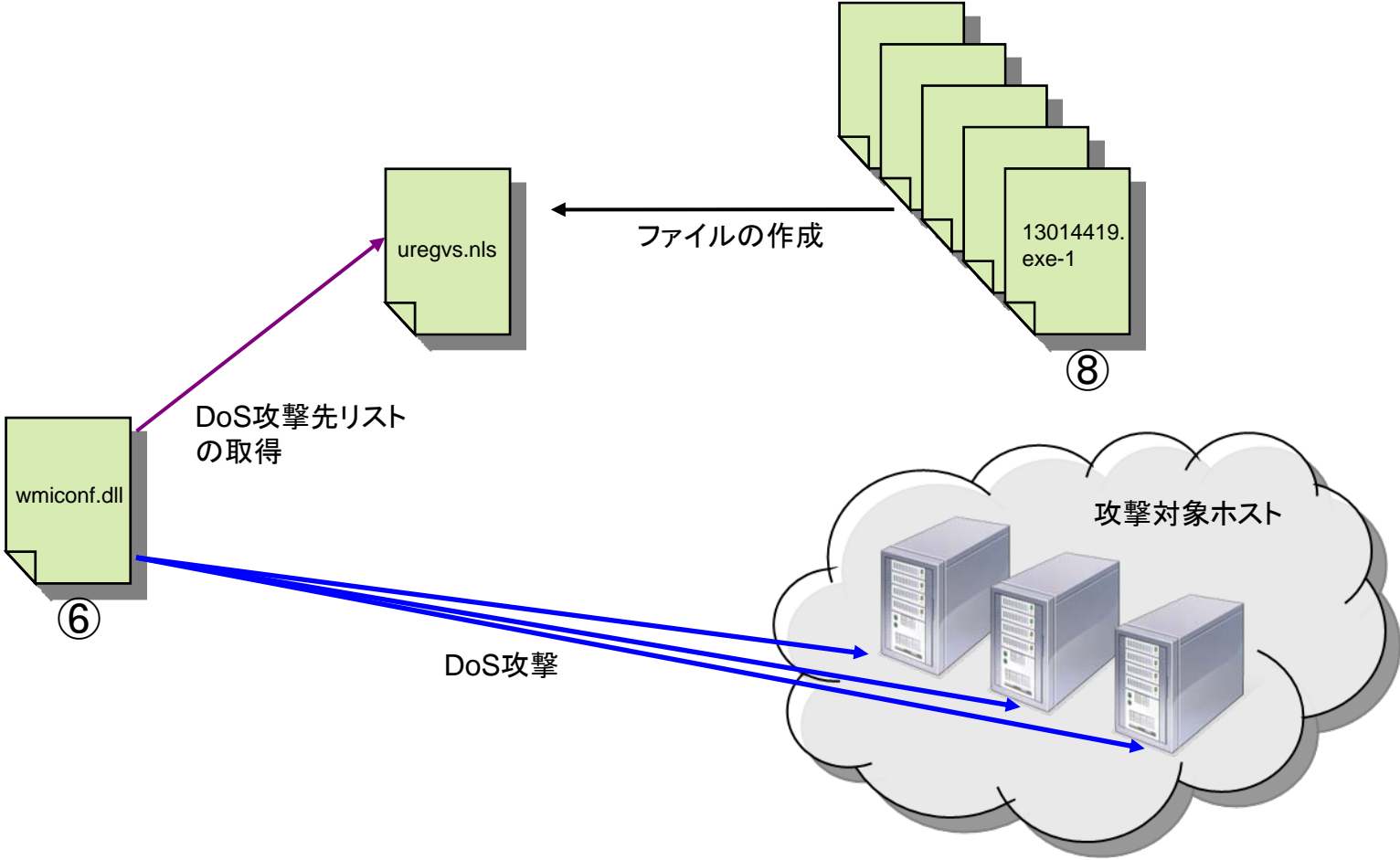


Mydoom(亜種)動作概要



①～⑦をクリックすると詳細報告書を閲覧することができます。

DoS攻撃概要



⑥、⑧をクリックすると詳細報告書を閲覧することができます。

1 対象ファイル

ファイル名：検体1（トレンドマイクロ受領ファイル）

ファイルサイズ：374,651 バイト

ハッシュ値（MD5）：0F394734C65D44915060B3690B1A972D

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

(1) ファイルの作成

C:\Windows\System32\

へ

wmcfg.exe

wmiconf.dll

pxdrv.nls

を作成する。

(2) サービスの登録

HKLM\SYSTEM\CurrentControlSet\Services\WmiConfig\ServiceDll

へ

wmiconf.dll

等を登録することで、wmiconf.dll をサービスとして起動させる。

(3) 外部へのアクセス

213.33.116.41(TCP 53)

216.199.83.203(TCP 80)

213.23.243.210(TCP443)

へ接続し、ランダムなデータを送信する。

1 対象ファイル

ファイル名 : **wmcfg.exe** (検体 1 が作成するファイル)

ファイルサイズ : 88,064 バイト

ハッシュ値 (MD5) : 1CBA81FEA0F34511C026E77CFA1F0EF6

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

(1) **wmcfg.exe** の動作

C:\Windows\System32\

へ

mstimer.dll

wversion.exe

を作成し、

C:\Windows\System32\config\

へ

SERVICES

SERVICES.LOG

を作成する。

SERVICES、**SERVICES.LOG** のデータは同一であった。

(2) サービスの登録

HKLM\SYSTEM\CurrentControlSet\Services\mstimer\ServiceDll

へ

mstimer.dll

を登録することで、**mstimer.dll** をサービスとして起動させる。

(3) 自分自身の削除

バッチファイルを作成し、自分自身の削除を行う。

1 対象ファイル

ファイル名：mstimer.dll (wmcfg.exe が作成するファイル)

ファイルサイズ：45,056 バイト

ハッシュ値 (MD5)：93322E3614BABD2F36131D604FB42905

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

(1) Win.ini の確認

C:\Windows\win.ini

のデータを読み取り、セクション名に

MSSOFT

がある場合、キー名

LastName

の値を取得し、PC の日時情報を基にした値と比較する。比較した値がキー名より大きければ、wversion.exe を実行する。

(2) flash.gif のダウンロード

wmcfg.exe が作成する

C:\Windows\System32\config\SERVICES.LOG

から、flash.gif のダウンロード先のリストを読み込み、リスト内のホストの 80 番ポートに接続し、flash.gif のダウンロードを行う。リストは暗号化された状態で保存されている。

リストは以下のとおりである。

h t t p : // 2 0 0 . 6 . 2 1 8 . 1 9 4 / flash . gif

h t t p : // 2 0 1 . 1 1 6 . 5 8 . 1 3 1 / x a m p p / i m g / flash . gif

h t t p : // 2 0 2 . 1 4 . 7 0 . 1 1 6 / flash . gif

h t t p : // 7 5 . 1 5 1 . 3 2 . 1 8 2 / flash . gif

h t t p : // 1 2 2 . 1 5 5 . 5 . 1 9 6 / s h o p / i m a g e s / flash . gif

h t t p : // n e w r o z f m . c o m / i m g / g l a p h / flash . gif

h t t p : // 9 2 . 6 3 . 2 . 1 1 8 / flash . gif

h t t p : // 1 6 3 . 1 9 . 2 0 9 . 2 2 / flash . gif

(3) メール送信

HKCU\Software\Microsoft\WAB\WAB4\Wab File Name

から、WAB ファイルの保存場所を取得し、WAB ファイル内のメールアドレスに対して、メールを送信する。

送信されたメールは図1であった。



図1 送信メール

1 対象ファイル

ファイル名 : flash.gif

ファイルサイズ : 41,168 バイト

ハッシュ値 (MD5) : 233214D0B3E04Df6282F1056EB31C5CE

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

対象ファイルの先頭は JPG となっているが、209 バイト目 (0xD0) に PE ヘッダ (MZ) が確認された。(図 1)

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00000000	4A	50	47	00	00	00	00	00	34	00	00	00	01	00	00	00	JPG.....4.....
00000010	0C	00	00	00	28	00	00	00	58	E7	04	21	F8	F2	D1	B0(...X...!・ム-
00000020	9E	96	00	2C	BC	E3	C3	F0	9D	3B	E3	A5	D7	20	DF	9D	;.s)や&の墓d..す
00000030	A8	3B	19	73	29	AC	70	26	B9	EE	7A	64	9A	1C	82	B7
00000040	01	00	00	00	80	00	00	00	80	00	00	00	60	00	00	00	V.葫Y>ニS・I;ヒツア.
00000050	56	2E	E4	D7	59	3E	C6	53	F6	5E	B4	3B	CB	AF	A7	7F	.テウ・.ブルK..栄
00000060	FE	C3	B3	DD	EF	40	FF	C9	87	6A	4B	9C	07	C2	9E	C4	Iad凰假V5..KけA
00000070	AC	BD	86	D1	33	77	37	E7	65	9A	EA	3C	E8	B7	BE	F5	Ut鴉~M・r.t・.
00000080	A2	B4	AE	64	99	80	96	99	56	35	08	0A	4B	B7	65	41Rar!...又尽..
00000090	04	EC	85	DB	C8	70	AC	8B	50	52	2C	AC	78	43	3B	81
000000A0	C8	55	BE	AC	9E	F6	7E	4D	EB	9E	72	FE	74	85	49	9D
000000B0	14	00	00	00	52	61	72	21	1A	07	00	CF	90	73	00	00
000000C0	0D	00	00	00	00	00	00	00	02	00	00	00	00	A0	00	00
000000D0	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....
000000E0	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	ク.....@.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00
00000110	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..コ..エ.^!ク.L^!Th
00000120	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000130	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000140	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$......
00000150	69	8A	E3	B6	2D	EB	8D	E5	2D	EB	8D	E5	2D	EB	8D	E5	

図 1 対象ファイルのバイナリデータ

先頭 208 バイトを削除し、拡張子を exe に変更し実行した。

(1) ファイルの作成

C:¥Windows¥System32¥

へ

wversion.exe

を作成する。

(2) Win.ini への書き込み

C:¥Windows¥Win.ini

へ

[MSSOFT]

LastName=40004

FirstName=3

Location=Y

を書き込む。

(3) 自分自身の削除

バッチファイルを作成し、自分自身の削除を行う。

4 その他

作成される wversion.exe は、wmcfg.exe が作成する wversion.exe とはファイルサイズが異なる。

1 対象ファイル

ファイル名 : wversion.exe (flahs.gif が作成するファイル)

ファイルサイズ : 36,864 バイト

ハッシュ値 (MD5) : F5C6B935E47B6A8DA4C5337F8DC84F76

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

(1) ファイルの圧縮

対象ファイルを実行すると、doc、xls 等の拡張子のファイルをパスワード付き ZIP で圧縮し、圧縮したファイルの拡張子を gz とする。圧縮前のファイルは削除される。パスワードはランダムな文字列となっている。

(2) MBR の上書き

対象ファイルを実行すると、ディスクの先頭から 1 M バイトを特定データで上書きする。そのため、次回起動時に OS が起動できなくなる。(図 1)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4D	65	6D	6F	72	79	7D	6F	66	7D	74	68	65	7D	49	6F	Memory of the In
00000010	64	65	70	65	6E	64	65	6E	63	65	20	44	61	79	00	00	dependence Day
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000070	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
00000080	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
00000090	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
000000A0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
000000B0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
000000C0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
000000D0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
000000E0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
000000F0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
00000100	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
00000110	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
00000120	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU
00000130	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUUUU

図 1 上書き後のデータ

1 対象ファイル

ファイル名：wmiconf.dll（検体1が作成するファイル）

ファイルサイズ：バイト

ハッシュ値（MD5）：50C97BF514643D9E60980985DB0908CA

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

(1) 攻撃先リストの取得

C:\Windows\System32\uregvs.nls

から攻撃対象ホスト、攻撃開始日時、攻撃終了日時等の情報を入手する。

uregvs.nls は、13014419.exe-1、13014421.exe-1、13014423.exe-1、13014424.exe-1、13014425.exe-1が作成するファイルであり、攻撃対象ホスト等の情報はそれぞれ異なる。(⑧参照)

(2) 対象ホストへの攻撃

uregvs.nls の情報から、感染 PC の日時が攻撃時間の範囲であれば、対象のホストに攻撃を行う。

現在確認できている攻撃は、

- HTTP GET Request Flood
- UDP Flood
- Ping Flood

である。

(3) Windows ファイアウォールの無効

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\

Parameters\FirewallPolicy\StandardProfile

を変更することで、Windows ファイアウォールを無効にする。

1 対象ファイル

ファイル名 : wversion.exe (wmcfg.exe が作成するファイル)

ファイルサイズ : 32,768 バイト

ハッシュ値 (MD5) : 04A3552A78ED2F8DC8DC9A77EE9EB281

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

(1) サービスの停止

mstimer.dll を実行しているサービス「mstimer」を停止させる。

(2) ファイルの削除

C:\Windows\system32\mstimer.dll

C:\Windows\system32\config\SERVICES

C:\Windows\system32\config\SERVICES.LOG

を削除し、バッチファイルを作成し自分自身の削除を行う。

1 対象ファイル

- (1) ファイル名 : 13014419.exe-1
ファイルサイズ : 24,576 バイト
ハッシュ値 (MD5) : 6350758B62484765239057218BD81D9E
- (2) ファイル名 : 13014421.exe-1
ファイルサイズ : 32,768 バイト
ハッシュ値 (MD5) : 6E5B00560A3C5BB92DFACb3766D6D7BC
- (3) ファイル名 : 13014423.exe-1
ファイルサイズ : 24,576 バイト
ハッシュ値 (MD5) : 9B08939834B2FE265EBAEDCCEBD3D470
- (4) ファイル名 : 13014424.exe-1
ファイルサイズ : 33,841 バイト
ハッシュ値 (MD5) : BCB69C1BAB27F53A0223E255D9B60D87
- (5) ファイル名 : 13014425.exe-1
ファイルサイズ : 32,768 バイト
ハッシュ値 (MD5) : E199D5C70745C363B734F499A3E065A9

2 検証環境

Windows XP SP3

Windows Server 2003

3 動作概要

- (1) ファイルの作成

C:\Windows\system32\

へ

uregvs.nls

を作成する。

作成されたファイルは、対象ファイルによって異なるデータであった。

バイナリエディタで作成されたファイルを開くと、www.whitehouse.gov、www.faa.gov といった文字列が確認された。

- (2) 自分自身の削除

バッチファイルを作成し、自分自身の削除を行う。