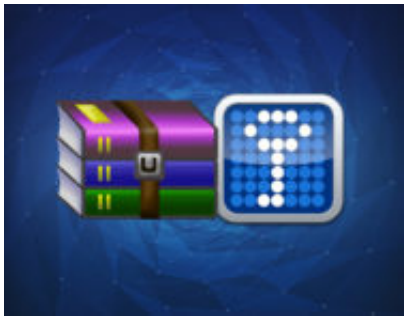
StrongPity, un Advanced Persistent Threat macchiato di sangue

Date : 22 novembre 2017



Estate 2016 un APT si diffonde in Italia! Chi si cela dietro l’APT StrongPity?

Nell'estate del 2016 un’APT chiamato StrongPity si è diffuso in Italia, in Belgio e in Turchia attraverso un attacco di watering hole infettando software legittimi. Di solito gli Advacend Persistent Thread utilizzano la tecnica dello spear-phishing per attaccare l’obiettivo prestabilito, in questo caso gli autori di StrongPity, hanno sfruttato un attacco di watering hole andando ad “avvelenare” i siti dei distributori di WinRAR Italia e Belgio e, in Turchia, due portali di distribuzione software.

In Italia era stato compromesso il sito del distributore di *WinRAR* dal 24 maggio al 1 giugno 2016, dove veniva scaricata una versione di *WinRAR* "alterata" che conteneva all'interno il malware StrongPity. In Belgio, il sito del distributore di *WinRAR.BE* era stato compromesso re-indirizzando il download al sito "**ralrab.com**" da dove si scaricavano versioni infette con StrongPity. In Turchia, invece, era stato utilizzato come veicolo di infezione/diffusione il software *TrueCrypt*.

Ringraziamo per la collaborazione il distributore italiano di WinRAR, che ci ha messo a disposizione le 3 versioni "alterate" da StrongPity: WRar531it, WinRAR-x64-531it, WRar393it. Per la nostra analisi abbiamo preso in esame il file WRar531it.exe (dimensione: 2843648 byte - MD5: 71BFE79ADBD00F6D0E928437198AFBCD).

Prima di eseguire il file infetto WRar531it.exe con StrongPity, analizziamo le risorse contenute all'interno del dropper.

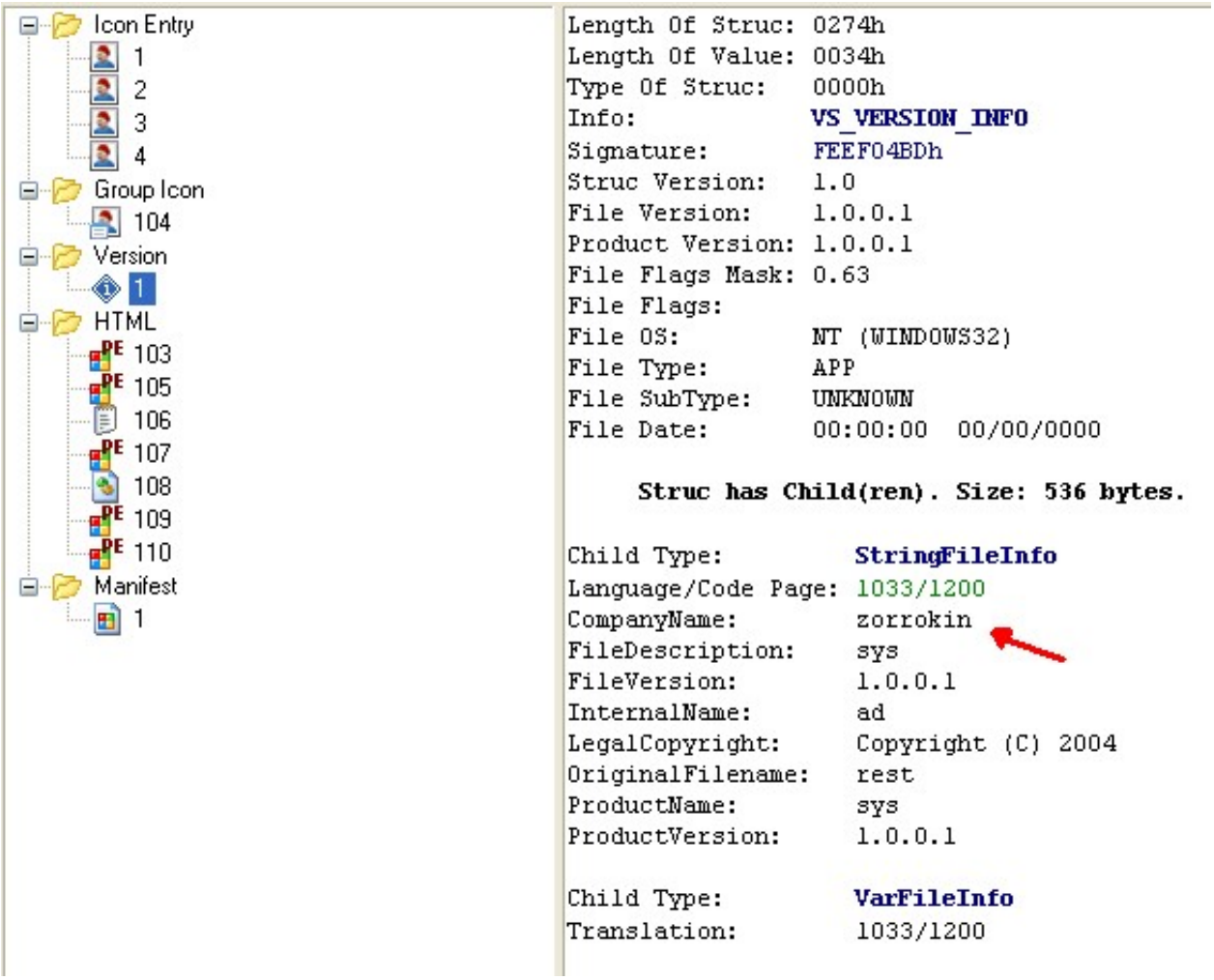


Fig. 1 Le risorse del file WRar531it.exe infettato con StrongPity

Nella versione analizzata il campo società "CompanyName" è contrassegnato con la parola: “**zorrokin”**, come possiamo vedere in figura 1.
Questa parola "zorrokin" la troveremo in ogni file di WinRAR infettato da **StrongPity.**
"Zorrokin" è una parola turca che significa Zorro.

All'interno delle risorse del file, troviamo una cartella denominata HTML che contiene 7 risorse enumerate nel seguente ordine: 103, 105, 106, 107, 108, 109, 110 (fig. 1). In ogni risorsa troviamo un file. Nella risorsa 103 troviamo il setup originale di WinRAR, nella 105 la libreria wrlck.dll, nella 107 la libreria prst.dll, nella 109 il modulo nvvscv.exe, nella 110 il modulo wndplyr.exe, tutte queste risorse contengono file eseguibili. Invece la 106 e la 108 contengono rispettivamente file di dati wrlck.cab e prst.cab.

I moduli di StrongPity sono contenuti nelle risorse: 105, 106, 107, 108, 109 e 110.

In figura2 possiamo vedere lo schema di impacchettamento del file WRar531it.exe da parte degli autori di StrongPity.

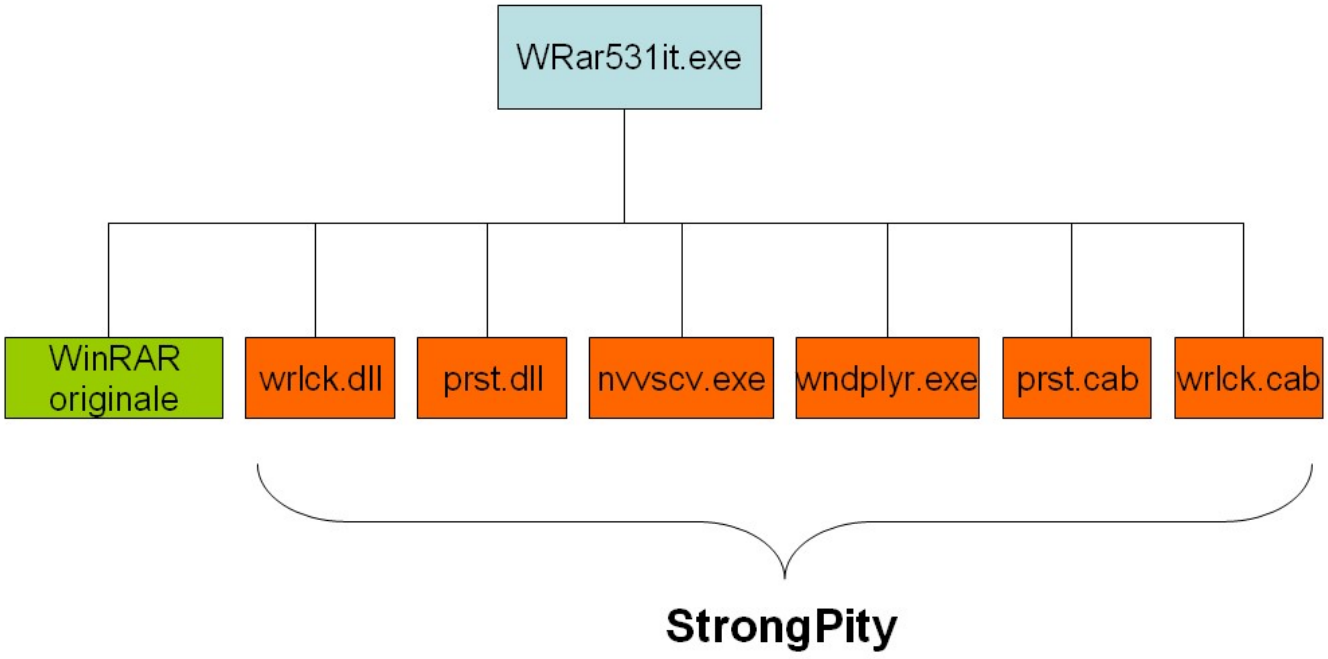


Fig. 2: Impacchettamento di StrongPity

Quando la vittima esegue il file infetto WRar531it.exe, vengono estratti all'interno della cartella *%temp%* dell'utente i seguenti file:

- %userprofile%\AppData\Local\temp\procexp.exe
- %userprofile%\AppData\Local\temp\sega\nvvscv.exe
- %userprofile%\AppData\Local\temp\sega\prst.cab
- %userprofile%\AppData\Local\temp\sega\Prst.dll
- %userprofile%\AppData\Local\temp\sega\wndplyr.exe
- %userprofile%\AppData\Local\temp\sega\wrlck.cab
- %userprofile%\AppData\Local\temp\sega\wrlck.dll

Il file ***procexp.exe*** contiene la versione originale di ***WinRAR***, invece gli altri file estratti sono i moduli di StrongPity. A questo punto vengono eseguiti il file procexp.exe per l'installazione di WinRAR e il file **nvvscv.exe** di StrongPity.

E' interessante notare che la cartella denominata "sega" creata da StrongPity fa riferimento alla società giapponese di videogiochi Sega Corporation. In altre varianti di StrongPity, ad esempio quella contenuta in TrueCrypt, la cartella creata in %temp% era denominata "eagames", facendo così riferimento ad un'altra società di videogiochi l'*Electronic Arts Games*.

StrongPity modifica il file di registro in modo da eseguire il modulo nvvscv.exe ad ogni avvio:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[Nvdia] = %userprofile%\AppData\Local\temp\sega\nvvscv.exe

Questo modulo è responsabile del caricamento delle librerie dll:

- *dll* (keylogger)
- *dll* (modulo di comunicazione con i server di Comando & Controllo)

Sia Prst.dll sia wrlck.dll esportano un'unica funzione denominata: *start_thread*.

Il modulo nvvscv.exe crea 2 thread, a cui vengono passati come parametro il nome della libreria da caricare (*Prst.dll* e *wrlck.dll*) , dopo vengono chiamate le rispettive funzioni esportate: *start_thread*.

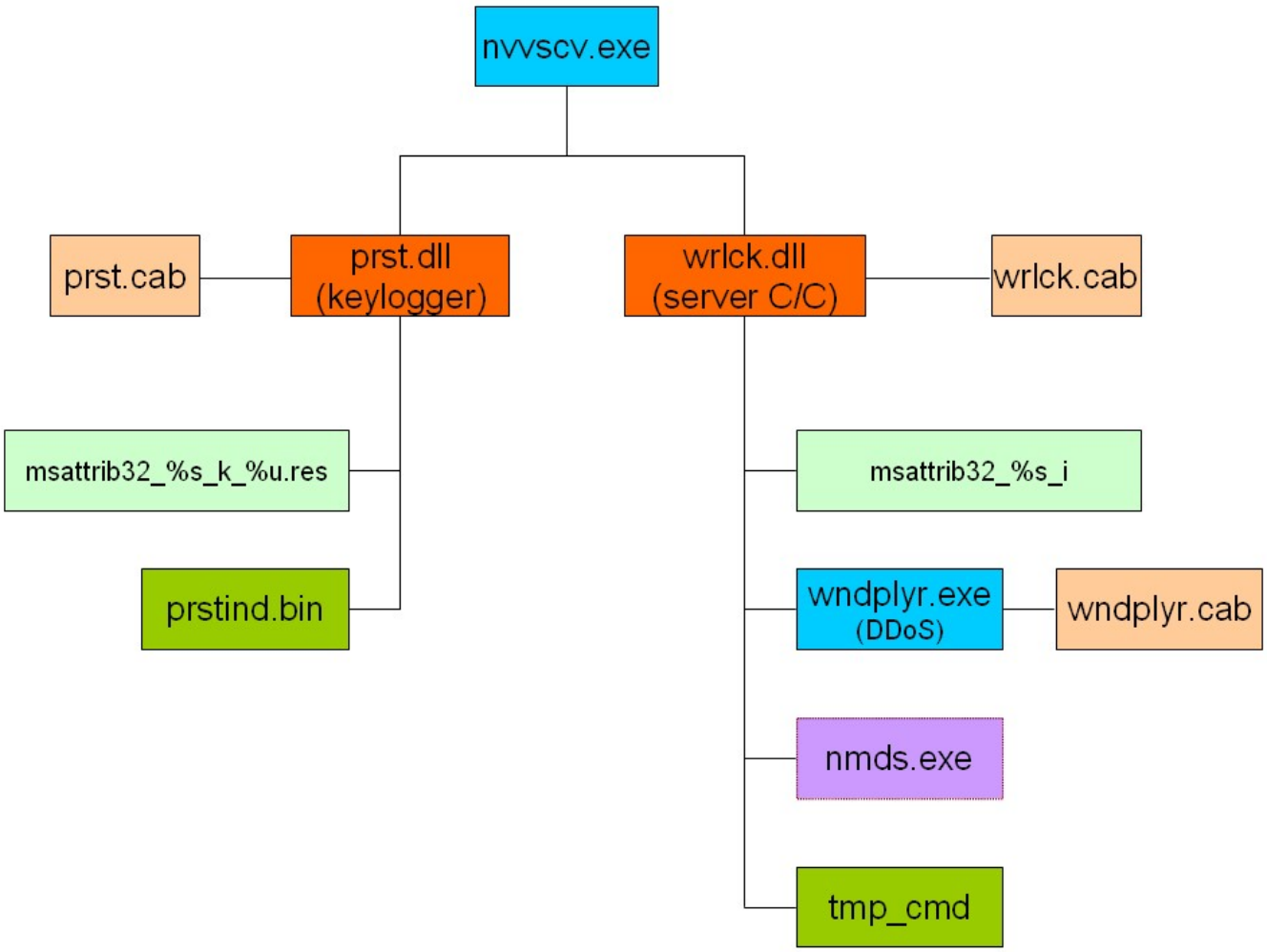


Fig. 3 Schema dei moduli di StrongPity con i rispettivi file dati

Modulo keylogger: prst.dll

Il modulo “*prst.dll”* di StrongPity è quello che funge da keylogger. La funzione *start_thread* all'inizio legge il file di configurazione "*prst.cab*", il cui contenuto è cifrato, come si può vedere in figura 4:

```
00000000  77 72 73 73 7E 2C 63 7F 63 0D 0A 60 6F 6A 63 7D   wrss~,c.c..`ojc}
00000010  6F 6A 6A 67 2C 63 7F 63 0D 0A 70 6F 68 74 65 77   ojjg,c.c..pohtew
00000020  2C 63 7F 63 0D 0A 77 72 73 73 7E 2C 63 7F 63 0D   ,c.c..wrss~,c.c.
00000030  0A 60 6F 6A 63 7D 6F 6A 6A 67 2C 63 7F 63 0D 0A   .`ojc}ojjg,c.c..
00000040  70 6F 68 74 65 77 2C 63 7F 63 0D 0A 77 72 73 73   pohtew,c.c..wrss
00000050  7E 2C 63 7F 63 0D 0A 60 6F 6A 63 7D 6F 6A 6A 67   ~,c.c..`ojc}ojjg
00000060  2C 63 7F 63 0D 0A 70 6F 68 74 65 77 2C 63 7F 63   ,c.c..pohtew,c.c
00000070  0D 0A 0A 20                                       ...
```

Fig. 4 File di configurazione prst.cab

In figura 5 possiamo vedere l'algoritmo di cifratura utilizzato da StrongPity, dove per ogni byte vengono eseguite operazioni di shift e xor.

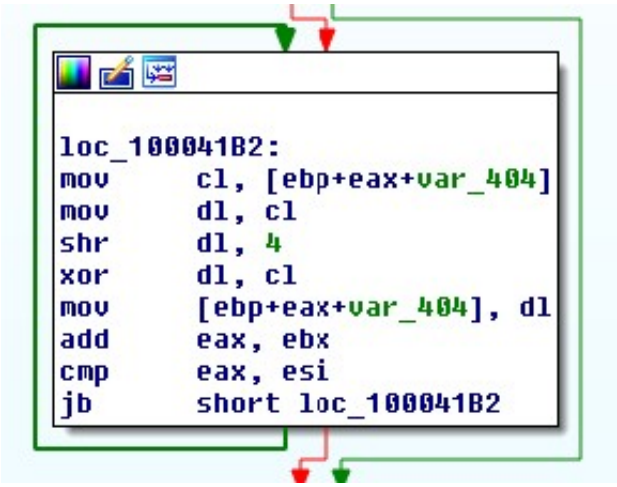


Fig. 5 Algoritmo di cifratura di StrongPity

Dopo aver decifrato il file di configurazione "*prst.cab*", si ottiene la seguente lista di programmi:

- exe (client SSH e Telnet)
- exe (programma di FTP)
- exe (programma di FTP)
- exe (crea sessioni di desktop remoto)
- exe (remote connections manager: RDP, VNC, ICA, etc.)

Di seguito viene letto il file "*prstind.bin*" che, se non dovesse essere già presente, viene creato e inizializzato con il valore 0 (DWORD 64 bit), altrimenti in caso contrario viene letto il valore numerico presente nel file stesso. Il file “*prstind.bin*" è utilizzato solamente a memorizzare un

contatore. Il keylogger crea un timer che, ogni 180 secondi, incrementa il contatore memorizzato nel "*prstind.bin*".

Per implementare le funzioni di keylogger, il modulo "*prst.dll*" si aggancia a tutti i tasti (minuscoli e maiuscoli) con la funzione RegistryHotKey. Quando viene premuto un tasto, il keylogger lo intercetta, determina il processo di appartenenza e il titolo della "finestra" in cui è stato premuto il tasto. Se il processo appartiene a uno dei programmi della lista contenuta in "*prst.cab*", allora il keylogger memorizza il nome del processo, il titolo della finestra e i tasti premuti nel file "*msattrib32_%s_k_%u.res*", dove:

- %s è la stringa che contiene il numero di serie del volume del disco C:
- %u è un numero (0, 1, 2, etc.) del contatore memorizzato nel file *bin*

esempio: msattrib32_2564879395_k_0.res

Come possiamo vedere dalla lista dei programmi contenuti in "*prst.cab*", a StrongPity interessa intercettare le credenziali di accesso di FTP, SSH, telnet, RDP, etc. In questo modo StrongPity potrà accedere indisturbato, avendo rubato le credenziali di accesso, via ftp, telnet, desktop remoto alle macchine server e client della vittima, con la possibilità di rubare ogni documento in essa contenuto.

Modulo di gestione c&c*: wrlck.dll*

Il modulo "*wrlck.dll*" di StrongPity è responsabile della gestione del sistema di comando & controllo. All'inizio viene letto il file di configurazione "*wrlck.cab*", il cui contenuto è cifrato, come si può vedere in figura 6:

```
00000000  6E 73 73 77 74 39 2D 2D 6B 7E 75 67 77 77 6F 62   nsswt9--k~ugwwob
00000010  2C 65 69 6B 2D 60 6A 67 77 77 7E 2D 64 72 73 73   ,eik-`jgww~-drss
00000020  63 75 60 6A 7E 74 2C 77 6E 77 0A 6E 73 73 77 74   cu`j~t,wnw.nsswt
00000030  39 2D 2D 6B 7E 75 67 77 77 6F 62 2C 65 69 6B 2D   9--k~ugwwob,eik-
00000040  60 6A 67 77 77 7E 2D 73 72 75 73 6A 63 74 2C 77   `jgww~-srusjct,w
00000050  6E 77 0A 6E 73 73 77 74 39 2D 2D 77 6F 68 6D 73   nw.nsswt9--wohms
00000060  72 75 73 6A 63 2C 6B 63 2D 60 6A 67 77 77 7E 2D   rusjc,kc-`jgww~-
00000070  64 72 73 73 63 75 60 6A 7E 74 2C 77 6E 77 0A 6E   drsscu`j~t,wnw.n
00000080  73 73 77 74 39 2D 2D 77 6F 68 6D 73 72 75 73 6A   sswt9--wohmsrusj
00000090  63 2C 6B 63 2D 60 6A 67 77 77 7E 2D 73 72 75 73   c,kc-`jgww~-srus
000000A0  6A 63 74 2C 77 6E 77 0A 70 68 6F 73 0A 31 33 0A   jct,wnw.phos.13.
000000B0  31 33 0D 0A                                       13..
```

Fig. 6 File di configurazione wrlck.dll

Dopo aver decifrato il file di configurazione, si ottengono i seguenti siti:

https://myrappid.com/flappy/butterflys.php	Primo server di C&C
https://myrappid.com/flappy/turtles.php	
https://pinkturtle.me/flappy/butterflys.php	Secondo server di C&C

https://pinkturtle.me/flappy/turtles.php

Alla fine del file di configurazione "*wrlck.cab*" vi troviamo un codice: "wnit". Analizzando altri file di configurazione di Strongpity, presi dalle versioni alterate di WinRAR Italia, Belgio e dal software TrueCrypt, il codice indicato dovrebbe rappresentare l'ID della campagna:

Software	**Codice**	**Campagna**
WinRAR Italia	wnit	Italia
WinRAR Belgio	winrarbe	Belgio
TrueCrypt	szlk02	Turchia

StrongPity in base alla versione del sistema operativo, determina se la macchina infettata è un client oppure un server. A questo punto inizia ad enumerare il contenuto delle seguenti cartelle:

- C:\Program Files
- C:\Program Files (x86)

per individuare le sottocartelle presenti (non ricorsivo). I nomi delle sottocartelle di "C:\Program Files" e di "C:\Program Files (x86)" saranno salvate nel file "*msattrib32_%s_*i" in forma cifrata, dove %s rappresenta un codice che ne identifica la campagna e il numero di serie del volume del disco.

Il thread principale di StrongPity in modo ciclico si collega al server di comando e controllo. Come abbiamo visto StrongPity utilizza 2 server di comando e controllo, il primo *myrappid.com* è quello principale, nel caso non riesca a collegarsi prova con *pinkturtle.me*.

La prima richiesta che fa è tipo post alla pagina *https://myrappid.com/flappy/turtles.php*, con la seguente richiesta: name=

esempio: name=wnit_2564879395

La risposta del server viene memorizzata nel file *tmp_cmd*, il quale è un file strutturato per ricevere nuovi moduli e configurazioni di StrongPity. Se il file che deve ricevere si chiama *wndplyr.cab* allora vengono eseguiti i moduli *wndplyr.exe* e *nmds.exe*, in caso contrario verrà eseguito solamente il modulo *nmds.exe*.

All'interno della cartella "sega" non abbiamo trovato il file *nmds.exe* che, probabilmente, viene creato in particolari circostanze che non siamo riusciti a riprodurre, poiché i domini di C&C di StrongPity erano offline.

Invece la pagina https://myrappid.com/flappy/butterflys.php è utilizzata da StrongPity per inviare le informazioni relative al computer della vittima e le credenziali di accesso carpite dal modulo di keylogger.

Se StrongPity non riesce a collegarsi al server *myrappid.com* allora verrà contattato il server di riserva *pinkturtle.me*.

Interessante notare che i domini *myrappid.com* e *pinkturtle.me* sono stati registrati rispettivamente il 19 e il 21 gennaio 2016 e sono appoggiati nello stesso server con indirizzo ip 109.236.92.237. Sempre in questo server troviamo un altro dominio *mytoshba.com* anch'esso registrato il 19 gennaio 2016. Invece il dominio "fake" *ralrab.com* (ip 139.59.15.88), che era stato utilizzato per l'attacco di watering hole di WinRar Belgio, era stato registrato il 27 ottobre 2015, molto tempo prima di sferrare l'attacco al distributore di WinRar in Belgio.

Modulo DDoS: wndplyr.exe

Il modulo di StrongPity *wndplyr.exe* è progettato per eseguire attacchi DDoS verso un obiettivo prestabilito. Questo modulo viene eseguito dalla libreria *wrlck.dll* quando riceve il comando dal server di C&C di creare il file *wndplyr.cab*, che contiene le informazioni del sito da attaccare.

Il file *wndplyr.cab* è cifrato ed è strutturato in questo modo:

A questo punto esegue un attacco DDoS cercando di connettersi all'infinito alla pagina del sito indicato nel file di configurazione.

Il 25 maggio 2016 alle ore 18:41 (ora italiana) il modulo di StrongPity *wndplyr.exe* lanciava un attacco DDoS (del tipo HTTP flood) verso il sito dell'ordine degli avvocati curdi della città di **Diyarbakir**: *diyarbakirbarosu.org.tr,* come possiamo vedere dal file *wndplyr.cab* decifrato (figura 7).

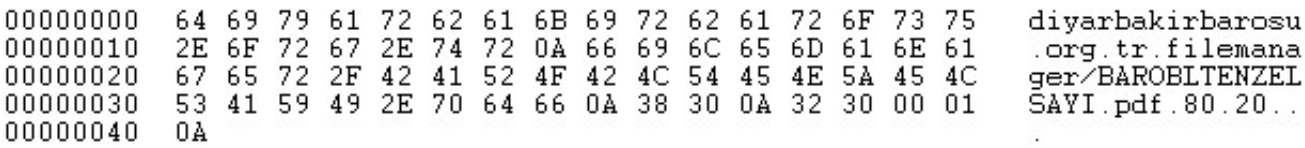


Fig. 7 File di configurazione wndplyr.cab decifrato

Il file di configurazione conteneva le seguenti informazioni:

- Dominio da attaccare: diyarbakirbarosu.org.tr
- Pagina: filemanager/BAROBLTENZELSAYI.pdf
- Protocollo: 80

Il 25 maggio 2016 StrongPity ha eseguito un attacco DDoS di tipo HTTP flood contro: http://diyarbakirbarosu.org.tr/filemanager/BAROBLTENZELSAYI.pdf

Il nome del file "*BAROBLTENZELSAYI.pdf*" dovrebbe significare in turco "*BARO BÜLTEN ÖZEL SAYI*" che in pratica tradotto in italiano altro non è che "AVVOCATI NEWSLETTER EDIZIONE SPECIALE". Non siamo a conoscenza del contenuto di tale documento, provando ad accedervi si ottiene l'errore 403 di accesso negato alla pagina. Cercando con Google il termine "BAROBLTENZELSAYI.pdf" oppure "BAROBLTENZELSAYI" non si ottengono risultati,

molto probabilmente il documento non è stato indicizzato, ma gli autori di StrongPity erano a conoscenza dell'esistenza di tale documento.

A che pro StrongPity cerca di sabotare il sito dell'ordine degli avvocati di Diyarbakir? Per rispondere a questa domanda probabilmente è necessario capire che cosa è la "*Diyarbakir Bar Association*" e chi era l'avvocato curdo **Tahir Elçi** attivista dei diritti umani (figura 8).

La “Diyarbakir Bar Association” (*diyarbakirbarosu.org.tr*) è un’organizzazione che lavora per i diritti umani e lo stato di diritto in Turchia. L'ex presidente dell'associazione Diyarbakir Bar, l'avvocato curdo Tahir Elçi, veniva assassinato il 28 novembre 2015 nel distretto di Diyarbakir in uno scontro a fuoco, mentre stava tenendo un incontro pubblico presso il minareto a quattro colonne vicino alla moschea di "Sheikh Matar".

Fig. 8 L’avvocato Tahir Elçi presidente dell’ordine degli avvocati della città di Diyarbakir

L'avvocato curdo *Tahir Elçi* era stato arrestato il 20 ottobre 2015 con l’accusa di aver fatto propaganda per il partito PKK in un programma TV della CNN turca, dove considerava il PKK un'organizzazione non terroristica, per poi venir rilasciato sotto cauzione alcuni giorni dopo e infine assassinato il 28 novembre 2015.

Inoltre in base alle nostre analisi, il 1° settembre 2016 alle ore 15:05 (ora italiana) il modulo di StrongPity *wndplyr.exe* eseguiva un attacco DDoS (del tipo HTTP flood) verso l'indirizzo IP *95.85.30.15* accedendo alla pagina "*xsyndll*". Non siamo a conoscenza del motivo dell’attacco verso quell’indirizzo IP geolocalizzato ad Amsterdam, il quale sembrerebbe ospitare un server “Nixideon.TK” relativo ad un videogioco chiamato “Nixideon Revolution” sviluppato in Turchia, ma è anche utilizzato come proxy attraverso la porta 5555. Questo tipo di attacco rimane avvolto in un alone di mistero, a partire dalla pagina attaccata “xsindll”, la quale coincide proprio con il modulo denominato “xsyn.dll” di StrongPity, che troviamo nella versione alterata di TrueCrypt distribuita in Turchia. Nella versione di TrueCrypt distribuita in Turchia, oltre a contenere l’APT StrongPity, il dropper era stato infettato con un altro APT chiamato “Truvasys”, le cui prime versioni risalgono all’autunno del 2015.

Conclusioni

StrongPity è un malware di spionaggio in grado di carpire informazioni riservate, come credenziali di accesso a server o computer client, attraverso programmi di ftp (filezilla, winscp), client SSH (putty), desktop remoto (mstsc, mRemoteNG) e di eseguire attacchi mirati DDoS. StrongPity si è diffuso maggiormente in Italia, Belgio e Turchia. Dalla nostra analisi si deduce che gli autori del progetto StrongPity potrebbero essere turchi, molto probabilmente vicini al regime attualmente al governo. StrongPity fa parte di un progetto APT iniziato nel 2015 o precedentemente con il malware TruvaSys. A partire da novembre 2016 si è aggiunto un nuovo APT classificato sotto il nome di NEODYMIUM, il quale utilizza una componente backdoor sviluppata dalla nota società tedesca FinFisher GmbH, che potrebbe essere un evoluzione di StrongPity o una nuova fase di questo APT “made” in Turchia.

A cura di: **Gianfranco Tonello**