

Persistenza

Il Malware ottiene la persistenza andando a modificare il registro di windows:

```
0402872 push offset SubKey ; "Software\Microsoft\Windows\CurrentVersion\Run"
```

In esso sono contenuti tutti i programmi così detti di “avvio”, cioè quei programmi che vengono eseguiti all'avvio di windows.

Possiamo analizzare in che modo viene compiuta la modifica:

1. Viene aperta la chiave da modificare con RegOpenKey, questa chiamata è preceduta dai parametri che vengono caricati sullo stack dalla funzione assembly “push”

```
push 2          ; samDesired
push eax        ; ulOptions
push offset SubKey ; "Software\Microsoft"
push HKEY_LOCAL_MACHINE ; hKey
call esi ; RegOpenKeyExW
```

2. In seguito vengono passati la key aperta e lpValueName come parametri della funzione RegSetValueExW, essa accetta come parametri un valore da settare e la chiave già aperta

```
04028A8 push ecx      ; lpValueName
04028A9 push edx      ; hKey
04028AA call ds:RegSetValueExW
```

Analisi funzioni web

Come possiamo semplicemente notare dai commenti di assembly, il client utilizzato è windows explorer versione 8.0

```
push 1          ; dwAccessType
push offset szAgent ; "Internet Explorer 8.0"
call ds:InternetOpenA
```

Con esso il malware tenta di connettersi all'url “http://www.malware12com”

```
offset szUrl    ; "http://www.malware12COM
esi           ; hInternet
edi ; InternetOpenUrlA
```

Utilizzando la funzione “InternetOpenUrlA”

Bonus 1

LEA: è il comando “load effective address”, è utilizzato per rendere più semplice la gestione degli array in memoria e dei pointer per renderlo più simile a linguaggi di più alto livello come C

Bonus 2

I file sono log di catture di wireshark, procedo con l'analisi del primo:

Primo Log

192.168.0.136	192.168.0.32	DNS	74 Standard query 0xd5cc A www.google.com
192.168.0.136	192.168.0.32	DNS	76 Standard query 0x0c0a A wpad.localdomain
192.168.0.136	192.168.0.32	DNS	79 Standard query 0xa25f A accounts.google.com
192.168.0.136	192.168.0.32	DNS	75 Standard query 0x47e6 A www.gstatic.com
192.168.0.136	192.168.0.32	DNS	89 Standard query 0xff74b A clientservices.googleapis.com
192.168.0.32	192.168.0.136	DNS	90 Standard query response 0xd5cc A www.google.com A 172.217.21.68
192.168.0.32	192.168.0.136	DNS	95 Standard query response 0xa25f A accounts.google.com A 216.58.205.77
192.168.0.136	172.217.21.68	GQUIC	1392 Client Hello, PKN: 1, CID: 1396259301962547755
192.168.0.136	192.168.0.32	DNS	75 Standard query 0x47e6 A www.gstatic.com
192.168.0.32	192.168.0.136	DNS	91 Standard query response 0x47e6 A www.gstatic.com A 216.58.208.163
192.168.0.32	192.168.0.136	DNS	105 Standard query response 0xff74b A clientservices.googleapis.com A 216.58.205.67
192.168.0.136	216.58.205.77	GQUIC	1392 Client Hello, PKN: 1, CID: 17089400091932018403

Inizia con una serie di query dns per richiedere gli ip di quei domini

In uno dei pacchetti possiamo vedere l'user agent che viene utilizzato:

```
-org:ser vice:dia  
l:1 USE R-AGENT:  
Google Chrome/8  
0.0.3987 .149 Win  
dows ..
```

La maggior parte dei pacchetti viaggia sulla 443, quindi la comunicazione è crittata

Poi vediamo questo

GQUIC	816 Payload (Encrypted), PKN: 82, CID: 139625930191
DNS	74 Standard query 0x2b99 A protonmail.com
GQUIC	63 Payload (Encrypted), PKN: 158
DNS	101 Payload (Encrypted), PKN: 159
TCP	874 443 → 52208 [PSH, ACK] Seq=1121 Ack=59810 Win=64240 Len=0
TCP	54 52208 → 443 [ACK] Seq=1121 Ack=59810 Win=64240 Len=0
DNS	82 Standard query 0xd965 A zulxgskcmll.localdomain
DNS	83 Standard query 0x9910 A arbemiumbjil.localdomain
DNS	87 Standard query 0x5975 A dobipdlkeblatpi.localdomain
TCP	1394 443 → 52208 [PSH, ACK] Seq=59810 Ack=1121 Win=64240 Len=1340 [T]
TCP	1394 443 → 52208 [PSH, ACK] Seq=61150 Ack=1121 Win=64240 Len=1340 [T]
TCP	54 52208 → 443 [ACK] Seq=1121 Ack=59810 Win=64240 Len=0

Oltre alle query DNS, che ci fanno risalire ai siti visitati, l'unica cosa che possiamo fare in questa cattura è filtrare le richieste e selezionare quelle con protocollo HTTP

Destination	Protocol	Length	Info
213.171.164.42	HTTP	491	GET / HTTP/1.1
192.168.0.136	HTTP	412	HTTP/1.1 301 Moved Permanently (text/html)
213.171.164.42	HTTP	503	GET / HTTP/1.1
192.168.0.136	HTTP	64	HTTP/1.1 200 OK (text/html)
213.171.164.42	HTTP	647	GET /favicon.ico HTTP/1.1
192.168.0.136	HTTP	1439	HTTP/1.1 200 OK (image/x-icon)
104.83.75.240	HTTP	415	GET /cookie_solution/iubenda_cs.js HTTP/1.1
192.168.0.136	HTTP	720	HTTP/1.1 200 OK (application/javascript)
104.83.75.240	HTTP	453	GET /cookie_solution/iubenda_cs/core-cd40c5caf396e9e6430490ac6bae6c41.js HTTP/1.1
192.168.0.136	HTTP	1236	HTTP/1.1 200 OK (application/javascript)
104.83.75.240	HTTP	420	GET /cookie-solution/confs/js/879340.js HTTP/1.1
192.168.0.136	HTTP	760	HTTP/1.1 200 OK (application/javascript)
104.83.75.240	HTTP	421	GET /cookie_solution/jquery-1.7.2.min.js HTTP/1.1
192.168.0.136	HTTP	815	HTTP/1.1 200 OK (application/javascript)
104.83.75.240	HTTP	634	GET /cookie_solution/iframe_bridge.html?origin=http%3A%2F%2Fcerca.italianweb.net%2F&method=
192.168.0.136	HTTP	278	HTTP/1.1 200 OK (text/html)
178.62.192.243	HTTP	550	OPTIONS /write?db=hits1 HTTP/1.1
192.168.0.136	HTTP	445	HTTP/1.1 204 No Content
178.62.192.243	HTTP	604	POST /write?db=hits1 HTTP/1.1 (application/x-www-form-urlencoded)
192.168.0.136	HTTP	675	HTTP/1.1 204 No Content

s), 1236 bytes captured (9888 bits) on interface \Device\NPF_{FED1266A-2} 0000 00 0c 29 70 59 59 00 50 56 f4 27 ec 08 00 45

Qui possiamo vedere in chiaro tutti i dati che sono stati scambiati, compresi i file javascript, e i parametri passati dalle richieste:

```

[TRESPONSE IN Frame: 3300]
File Data: 32 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "hits,cp" = "879340,pv_nocs=1 value=1"
    Key: hits,cp
    Value: 879340,pv_nocs=1 value=1

```

Secondo log

Destination	Protocol	Length	Info
192.168.0.136	TCP	60	443 → 52062 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.0.136	TCP	60	443 → 52061 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.1.121	TCP	66	[TCP Port numbers reused] 52062 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.1.189	TCP	66	52064 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
192.168.0.32	DNS	76	Standard query 0x3d6e A wpad.localdomain
192.168.1.121	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 52062 → 443 [SYN] Seq=0 Win=64240 Len=0
192.168.0.32	DNS	79	Standard query 0x543e A accounts.google.com
239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
192.168.0.32	DNS	74	Standard query 0xb77 A www.google.com
192.168.0.32	DNS	76	Standard query 0x3d6e A wpad.localdomain
192.168.0.136	DNS	90	Standard query response 0xb77 A www.google.com A 172.217.21.68
192.168.0.136	DNS	95	Standard query response 0x543e A accounts.google.com A 216.58.205.77
172.217.21.68	HTTP	1200	GET / HTTP/1.1

Anche qui possiamo vedere i siti cercati, a giudicare da quello che si vede si pu ipotizzare che si effettui un login con l'account google

192.168.0.136	TCP	1134	443 → 52080 [PSH, ACK] Seq=10291 Ack=1110 Win=64240 Len=0
31.13.86.4	TCP	54	52088 → 443 [ACK] Seq=1115 Ack=17391 Win=64240 Len=0
192.168.0.32	DNS	72	Standard query 0x6117 A facebook.com
192.168.0.136	TCP	1394	443 → 52088 [PSH, ACK] Seq=17391 Ack=1115 Win=64240 Len=0
192.168.0.136	TCP	1514	443 → 52088 [ACK] Seq=18731 Ack=1115 Win=64240 Len=1460

Qui vediamo che viene fatta una query dns per facebook.com

TLSv1.3	1514 Application Data
TLSv1.3	1369 Application Data
TCP	54 52088 → 443 [ACK] Seq=1633 Ack=69333 Win=64240 Len=0
DNS	88 Standard query response 0x6117 A facebook.com A 31.13.86.36
TLSv1.3	208 Application Data
TCP	60 443 → 52081 [ACK] Seq=38995 Ack=1267 Win=64240 Len=0
TLSv1.3	89 Application Data
TLSv1.3	158 Application Data
TLSv1.3	148 Application Data
TCP	60 443 → 52080 [ACK] Seq=82256 Ack=4417 Win=64240 Len=1220 [TCP segment of a retransmission]

Qui la risposta del server DNS

1274	443 → 52086 [PSH, ACK] Seq=783476 Ack=4417 Win=64240 Len=1220 [TCP segment of a retransmission]
54	52086 → 443 [ACK] Seq=4417 Ack=783476 Win=64240 Len=0
103	Standard query response 0xd631 A safebrowsing.googleapis.com A 172.217.16.138
1394	Application Data
54	52086 → 443 [ACK] Seq=4417 Ack=784816 Win=62900 Len=0

Chiamate a api di google

DNS	75 Standard query 0x78ce A mail.google.com
DNS	80 Standard query 0xe0bf A fonts.googleapis.com
DNS	73 Standard query 0x56fc A www.gmail.com
GQUIC	347 Payload (Encrypted), PKN: 138, CID: 172467417871241
GQUIC	63 Payload (Encrypted), PKN: 236

Poi gmail.com

192.168.1.189	TCP	66 [TCP Retransmission] [TCP Port number]
23.111.157.86	UDP	66 15644 → 4000 Len=24
192.168.0.136	UDP	62 4000 → 15644 Len=20
192.168.1.189	TCP	66 [TCP Retransmission] [TCP Port number]
192.168.1.189	TCP	66 [TCP Retransmission] [TCP Port number]

Qui vediamo delle comunicazioni con protocollo UDP

QQ91c	70 Payload (Encrypted), PKT: 44, CID: 10040001007202003000
DNS	88 Standard query response 0x91cf A www.alice.it A 217.169.121.227
TCP	66 52097 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
TCP	66 52098 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
TCP	60 80 → 52097 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
TCP	54 52097 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
HTTP	495 GET / HTTP/1.1
TCP	60 80 → 52097 [ACK] Seq=1 Ack=442 Win=64240 Len=0
TCP	60 80 → 52098 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
TCP	54 52098 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
HTTP	586 HTTP/1.1 301 Moved Permanently (text/html)
DNS	80 Standard query 0x47e5 A www.telecomitalia.it
TCP	54 52097 → 80 [ACK] Seq=442 Ack=533 Win=63708 Len=0
DNS	80 Standard query 0x47e5 A www.telecomitalia.it
DNS	96 Standard query response 0x47e5 A www.telecomitalia.it A 156.54.82.96
TCP	66 52099 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Qui vediamo ricerche a alice.it e telecomitalia, esse sono HTTP quindi tutte in chiaro

....
DNS	70 Standard query 0x2e2b A www.tim.it
TCP	54 52099 → 80 [ACK] Seq=456 Ack=516 Win=63725 Len=0
DNS	100 Standard query response 0x2e2b A www.tim.it CNAME tim.it A 156.54.69.9
TCP	66 52100 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

E per ultimo a tim.it