## Analisi malware

La funzione DLLMain si trova all'indirizzo 1000D02E

```
:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
:1000D02E _DllMain@12     proc near               ; CODE XREF: DllEntryPoint+4B↓p
:1000D02E                                         ; DATA XREF: sub_100110FF+2D↓o
:1000D02E
:1000D02E hinstDLL        = dword ptr  4
:1000D02E fdwReason       = dword ptr  8
:1000D02E lpvReserved     = dword ptr  0Ch
```

Indirizzo della funzione "gethostbyname"

| | | | |
|---|---|---|---|
| 100163C8 | 11 | inet_addr | WS2_32 |
| 100163CC | 52 | gethostbyname | WS2_32 |
| 100163D0 | 12 | inet_ntoa | WS2_32 |

Queste sono le variabili locali, che hanno l'offset negativo

```
.text:10001656 var_675          = byte ptr -675h
.text:10001656 var_674          = dword ptr -674h
.text:10001656 hModule          = dword ptr -670h
.text:10001656 timeout          = timeval ptr -66Ch
.text:10001656 name             = sockaddr ptr -664h
.text:10001656 var_654          = word ptr -654h
.text:10001656 in               = in_addr ptr -650h
.text:10001656 Parameter        = byte ptr -644h
.text:10001656 CommandLine      = byte ptr -63Fh
.text:10001656 Data             = byte ptr -638h
.text:10001656 var_544          = dword ptr -544h
.text:10001656 var_50C          = dword ptr -50Ch
.text:10001656 var_500          = dword ptr -500h
.text:10001656 var_4FC          = dword ptr -4FCh
.text:10001656 readfds          = fd_set ptr -4BCh
.text:10001656 phkResult        = HKEY__ ptr -3B8h
.text:10001656 var_3B0          = dword ptr -3B0h
.text:10001656 var_1A4          = dword ptr -1A4h
.text:10001656 var_194          = dword ptr -194h
.text:10001656 WSAData          = WSAData ptr -190h
```

Il parametro invece è questo con offset positivo

```
.text:10001656 arg_0            = dword ptr  4
```

E' una backdoor

```
74 ; char aBackdoorServer[]
74 aBackdoorServer db 0Dh,0Ah               ; DATA XREF: sub_100042DB+B5↑o
74                 db 0Dh,0Ah
74                 db '**********************************',0Dh,0Ah
74                 db '[BackDoor Server Update Setup]',0Dh,0Ah
74                 db '**********************************',0Dh,0Ah
74                 db 0Dh,0Ah,0
DB                 align 4
```

Riesce a rilevare se si trova su una VM, e si elimina da sola

```
t_bat[]
b '.\vmselfdel.bat',0
e[]
```

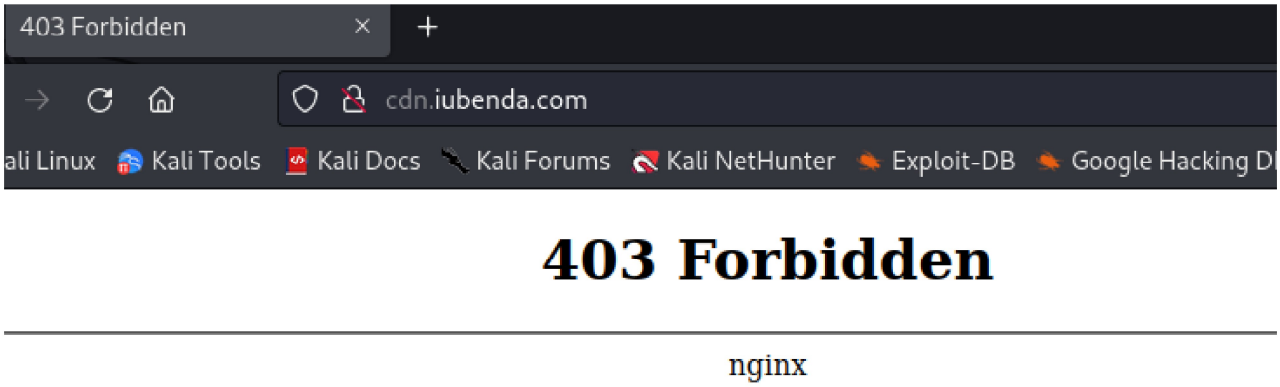
```
    align 4
sterDDDDDD[]
DDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
                        ; DATA XREF: sub_1000FF58+145↑o
    db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
    db 0Dh,0Ah
    db 'Machine UpTime  [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
    db 'ds]',0Dh,0Ah
    db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
    db 'nds]',0Dh,0Ah
    db 0Dh,0Ah
    db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
    db 0Dh,0Ah,0
0095C5C[]
:                       ; DATA XREF: sub_1000FF58+4B↑o
                        ; sub_1000FF58+2F1↑o
```

Fa anche la simpatica

Comunque in generale ottiene persistenza e si lancia con svchost

## Bonus

Analisi cattura n2




Che sia un sito aziendale che ha controlli su ip permessi e non?

```
└─$ whois 104.83.75.240
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#

# start

NetRange:       104.64.0.0 - 104.127.255.255
CIDR:           104.64.0.0/10
NetName:        AKAMAI
NetHandle:      NET-104-64-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Akamai Technologies, Inc. (AKAMAI)
RegDate:        2014-04-22
Updated:        2014-04-22
Ref:            https://rdap.arin.net/registry/ip/104.64.0.0


OrgName:        Akamai Technologies, Inc.
OrgId:          AKAMAI
Address:        145 Broadway
City:           Cambridge
```

Analisi cattura n5

```
192.168.0.136   51.138.12.221   TCP      66 52094 → 46551 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
51.138.12.221   192.168.0.136   TCP      60 46551 → 52094 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.0.136   51.138.12.221   TCP      54 52094 → 46551 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.0.136   51.138.12.221   TLSv1.2  73 Ignored Unknown Record
51.138.12.221   192.168.0.136   TCP      60 46551 → 52094 [ACK] Seq=1 Ack=20 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2  73 Ignored Unknown Record
192.168.0.136   51.138.12.221   TCP      54 52094 → 46551 [ACK] Seq=20 Ack=20 Win=64221 Len=0
```

Con questo ip avvengono grossi scambi di informazione

```
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=1 Ack=48 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2   73 Ignored Unknown Record
192.168.0.136   51.138.12.221   TLSv1.2  232 Client Hello
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=20 Ack=226 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2 1180 Server Hello, Certificate, Server Key Exchange, Server Hello Done
192.168.0.136   51.138.12.221   TLSv1.2  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messa
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=1146 Ack=319 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2  105 Change Cipher Spec, Encrypted Handshake Message
192.168.0.136   51.138.12.221   TLSv1.2  140 Application Data
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=1197 Ack=405 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2  244 Application Data
192.168.0.136   51.138.12.221   TLSv1.2  624 Application Data
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=1387 Ack=975 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2  142 Application Data
192.168.0.136   51.138.12.221   TLSv1.2  201 Application Data
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=1475 Ack=1122 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2   87 Application Data
192.168.0.136   51.138.12.221   TLSv1.2  545 Application Data
51.138.12.221   192.168.0.136   TCP       60 46551 → 52096 [ACK] Seq=1508 Ack=1613 Win=64240 Len=0
51.138.12.221   192.168.0.136   TLSv1.2  209 Application Data
```

Però sembra essere qualcosa di microsoft

```
└─$ whois 51.138.12.221
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '51.136.0.0 - 51.138.255.255'

% Abuse contact for '51.136.0.0 - 51.138.255.255' is 'abuse@microsoft.com'

inetnum:        51.136.0.0 - 51.138.255.255
org:            ORG-MA42-RIPE
netname:        MICROSOFT
descr:          Microsoft Limited UK
country:        GB
admin-c:        DH5439-RIPE
tech-c:         MRPA3-RIPE
status:         LEGACY
mnt-by:         RIPE-NCC-LEGACY-MNT
mnt-by:         MICROSOFT-MAINT
created:        2015-05-21T17:18:28Z
last-modified:  2016-07-25T09:38:58Z
source:         RIPE
```