



SIN CLASIFICAR



Informe Código Dañino CCN-CERT ID-03/16

“Trojan:Win32/ponmocup”

Febrero de 2016

SIN CLASIFICAR

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT	5
2. RESUMEN EJECUTIVO	6
3. CARACTERÍSTICAS	7
4. PROCEDIMIENTO DE INFECCIÓN.....	10
4.1 Vectores de infección	10
4.2 Interacciones con el sistema afectado.....	11
4.2.1 Interacciones con un sistema Virtualizado / <i>Sandbox</i>	11
4.2.2 Interacciones con un sistema real.....	12
5. PERSISTENCIA EN EL SISTEMA	16
5.1 PERSISTENCIA EN SISTEMAS VIRTUALIZADOS / SANDBOX	16
5.2 PERSISTENCIA EN SISTEMAS REALES	17
6. CONEXIONES DE RED	18
6.1 Conexiones establecidas contra el C&C	18
6.2 Conexiones establecidas en un sistema virtual / <i>sandbox</i>	20
6.3 Información del atacante	21
6.3.1 IMAGEHUT4.CN	21
6.3.1.1 DIRECCIÓN IP	21
6.3.1.2 GEOLOCALIZACIÓN	23
6.3.1.3 WHOIS 23	
6.3.2 MONTYINC.NET.....	24
6.3.2.1 DIRECCIÓN IP	24
6.3.2.2 GEOLOCALIZACIÓN	25
6.3.2.1 WHOIS.....	25
7. DETECCIÓN	26
7.1 UTILIDAD DEL SISTEMA	26
7.2 MANDIANT.....	26
8. DESINFECCIÓN.....	27
8.1 Manual.....	27
8.2 Automática	29
9. ALGORITMOS	30
10.ARCHIVOS DE CONFIGURACION.....	35

10.1	Archivo de configuración "dll"	35
10.2	Archivo de Dominios "dll"	37
11.	REFERENCIAS	37
12.	ANEXOS	38
	ANEXO I – REGLAS DE DETECCIÓN	38
	REGLA SNORT	38
	REGLA YARA.....	38
	IOC.....	39

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis de una variante del código dañino "Ponmocup".

La principal característica de "Ponmocup" es la capacidad que tiene para comprometer y controlar equipos, de forma que pasen a ser nuevos nodos de una red *botnet*.

Para realizar parte de sus acciones iniciales (ej. instalación) y operar correctamente "Ponmocup" requerirá de un servidor *on-line* que actúe como mando y control (C&C). Si éste es el caso, "Ponmocup" se comunicará periódicamente con él, enviando y recibiendo información de forma cifrada. Los algoritmos utilizados en este caso son algoritmos propios.

Otra característica interesante es la capacidad que posee este código dañino para detectar "cómo" y "dónde" está siendo ejecutado. Por ejemplo, en equipos virtualizados o máquinas de análisis puede cambiar su comportamiento y actuar como un simple *dropper*, descargando y ejecutando otros códigos dañinos.

"Ponmocup" utiliza diversas técnicas para garantizar con éxito su persistencia en los sistemas ya comprometidos. Dichas técnicas se expondrán más adelante.

La *botnet* de "Ponmocup" está considerada como una de las mayores descubiertas hasta el momento. [\[1\]](#)

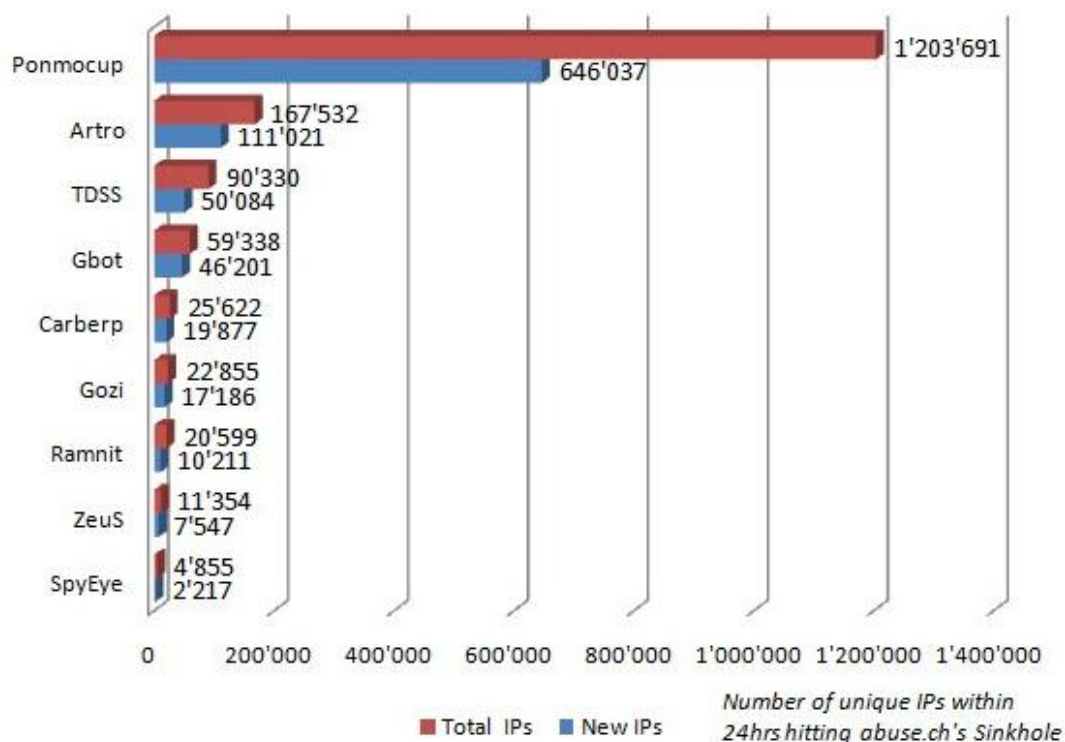


Ilustración 1. Tamaño de la "botnet" del código dañino "ponmocup"

Según VirusTotal, 38 de 57 motores antivirus detectan el código analizado como dañino, suponiendo un riesgo medio/bajo si se dispone de alguna solución antivirus.

3. CARACTERÍSTICAS

A continuación se muestran algunas propiedades estáticas del fichero analizado.

La firma del código dañino es la siguiente:

MD5	8e105ca9ef1571eec69a181efc32138a
SHA1	197e12789d4cfd7234ef7d6754db7d3855cd52ee

```
viper ponmocup > pe sections
[*] PE Sections:
-----+-----+-----+-----+-----+
| Name      | RVA      | VirtualSize | RawDataSize | Entropy    |
|-----+-----+-----+-----+-----+
| .text     | 0x1000   | 0x5c68      | 24576       | 6.62103337583 |
| .rdata    | 0x7000   | 0x155c      | 8192        | 3.74482248869 |
| .data     | 0x9000   | 0xb2838     | 368640      | 5.94978462577 |
| .rsrc     | 0xbc000  | 0x400       | 4096        | 1.12267656169 |
|-----+-----+-----+-----+-----+

viper ponmocup > pe compiletime
[*] Compile Time: 2009-07-09 13:10:23

viper ponmocup > pe imports
[*] DLL: KERNEL32.dll
- 0x407048: ExpandEnvironmentStringsW
- 0x40704c: lstrlenA
- 0x407050: lstrlenW
- 0x407054: MultiByteToWideChar
- 0x407058: GetVersionExA
- 0x40705c: LoadLibraryA
- 0x407060: GetWindowsDirectoryA
- 0x407064: GetProcAddress
- 0x407068: WideCharToMultiByte
- 0x40706c: GetFileAttributesA
- 0x407070: GetFileAttributesW
- 0x407074: GetWindowsDirectoryW
- 0x407078: LockResource
- 0x40707c: LoadResource
- 0x407080: FindResourceExW
- 0x407084: GetSystemDefaultLangID
- 0x407088: GlobalAlloc
- 0x40708c: GlobalFree
- 0x407090: IsBadWritePtr
- 0x407094: GetSystemDirectoryW
- 0x407098: GetSystemDirectoryA
- 0x40709c: lstrcpynW
- 0x4070a0: ExpandEnvironmentStringsA
- 0x4070a4: CreateDirectoryW
- 0x4070a8: CreateDirectoryA
- 0x4070ac: GetCommandLineA
- 0x4070b0: EnumResourceNamesW
- 0x4070b4: VirtualProtect
- 0x4070b8: FreeLibrary
- 0x4070bc: RtlUnwind
```

```

- 0x4070e0: GetStdHandle
- 0x4070e4: GetModuleFileNameA
- 0x4070e8: UnhandledExceptionFilter
- 0x4070ec: FreeEnvironmentStringsA
- 0x4070f0: GetEnvironmentStrings
- 0x4070f4: FreeEnvironmentStringsW
- 0x4070f8: GetLastError
- 0x4070fc: GetEnvironmentStringsW
- 0x407100: SetHandleCount
- 0x407104: GetFileType
- 0x407108: HeapDestroy
- 0x40710c: HeapCreate
- 0x407110: VirtualFree
- 0x407114: HeapFree
- 0x407118: GetACP
- 0x40711c: GetOEMCP
- 0x407120: GetCPInfo
- 0x407124: HeapAlloc
- 0x407128: VirtualAlloc
- 0x40712c: HeapReAlloc
- 0x407130: HeapSize
- 0x407134: QueryPerformanceCounter
- 0x407138: GetTickCount
- 0x40713c: GetCurrentThreadId
- 0x407140: GetCurrentProcessId
- 0x407144: GetSystemTimeAsFileTime
- 0x407148: LCMAPStringA
- 0x40714c: LCMAPStringW
- 0x407150: GetStringTypeA
- 0x407154: GetStringTypeW
- 0x407158: GetLocaleInfoA
- 0x40715c: GetSystemInfo
[*] DLL: ADVAPI32.dll
- 0x407000: RegQueryValueExW
- 0x407004: RegCloseKey
- 0x407008: RegQueryValueExA
- 0x40700c: RegOpenKeyA
- 0x407010: RegCreateKeyExA
- 0x407014: RegSetValueExW
- 0x407018: RegSetValueExA
- 0x40701c: FreeSid
- 0x407020: SetFileSecurityW
- 0x407024: SetSecurityDescriptorDacl
- 0x407028: InitializeSecurityDescriptor
- 0x40702c: GetAce
- 0x407030: AddAccessAllowedAce
- 0x407034: InitializeAcl
- 0x407038: GetLengthSid
- 0x40703c: LookupAccountSidW
- 0x407040: AllocateAndInitializeSid
    viper ponmocup > pe peid
[*] PEiD Signatures:
- Microsoft Visual C++ v7.1 EXE
- Microsoft Visual C++ v7.0
    viper ponmocup >

```

Ilustración 2. Detalles del código dañino

El compilador detectado en este caso ha sido: Microsoft Visual C + v7-10.

La mayor parte del código de la muestra se encuentra cifrado de cara a evadir las detecciones de los antivirus.

El algoritmo de cifrado utilizado es propio, lo cual es un indicio de que este tipo de código dañino es generado masivamente y alterado en cada compilación para generar nuevas muestras.

```
.data:00461F6C 40 00 ; SEH scope table for function 401618
.data:00461F78 ; int dword_461F78[]
.data:00461F78 FF FF 00 00 dword_461F78 dd 0FFFFh ; DATA XREF: sub_4026F8↑r
.data:00461F78 ; sub_4026F8+1E↑o
.data:00461F78 ; sub_4026F8:loc_402730↑r
.data:00461F78 ; sub_4026F8+4A↑w
.data:00461F78 ; descifraCodigo_461F7C+66↑w
.data:00461F7C ; -----
.data:00461F7C ; int loc_461F7C[]
.data:00461F7C loc_461F7C: ; DATA XREF: descifraCodigo_461F7C+34↑r
.data:00461F7C 48 ; -----
.data:00461F7C dec eax
.data:00461F7D 8F ; -----
.data:00461F7D db 8Fh ; 8
.data:00461F7E ; -----
.data:00461F7E BB 54 5F 3E 4F mov ebx, 4F3E5F54h
.data:00461F83 4E dec esi
.data:00461F84 29 C7 sub edi, eax
.data:00461F86 08 CF or bh, cl
.data:00461F88 5C pop esp
.data:00461F89 05 E7 21 65 DB add eax, 00B6521E7h
.data:00461F89 ; -----
.data:00461F8E C1 ; -----
.data:00461F8E db 0C1h ; -
.data:00461F8F ; -----
.data:00461F8F loc_461F8F: ; CODE XREF: .data:0046200E↑p
.data:00461F8F B9 07 9F 9A 7E mov ecx, 7E9A9F07h
.data:00461F94 3F aas
.data:00461F95 0B 24 F6 or esp, [esi+esi*8]
.data:00461F98 45 inc ebp
.data:00461F99 C8 BB D0 2B enter 0FFFFD0BBh, 2Bh
.data:00461F9D FC cld
.data:00461F9E 58 pop eax
.data:00461F9F 38 23 cmp [ebx], ah ; CODE XREF: .data:00461FB1↑j
.data:00461FA1 7D 87 jge short loc_461F2A
.data:00461FA3 89 9C C7 E9 A2+ mov [edi+eax*8-46A35D17h], ebx
.data:00461FAA 10 4A 24 adc [edx+24h], cl
.data:00461FAB 85 mnscd
```

Ilustración 3. Detalles del código dañino

Además, para evadir el análisis por sistemas automatizados, utiliza diversas técnicas de detección de máquinas virtuales:

Comprobación de espacio libre que devuelve la llamada a "GetDiskFreeSpaceEx".

```

002C9698 loc_2C9698:                                ; CODE XREF: DetectaSandBoxesVMWARE+121Tj
002C9698                                ; DetectaSandBoxesVMWARE+12F1j
002C9698      push    104h                                ; uSize
002C96A0      lea     edx, [ebp+DirectoryName]
002C96A6      push    edx                                ; lpBuffer
002C96A7      call    ds:GetSystemDirectoryA
002C96AD      mov     [ebp+var_249], 0
002C96B4      lea     eax, [ebp+TotalNumberOfFreeBytes]
002C96B8      push    eax                                ; lpTotalNumberOfFreeBytes
002C96BB      lea     ecx, [ebp+TotalNumberOfBytes]
002C96C1      push    ecx                                ; lpTotalNumberOfBytes
002C96C2      push    esi                                ; lpFreeBytesAvailableToCaller
002C96C3      lea     edx, [ebp+DirectoryName]
002C96C9      push    edx                                ; lpDirectoryName
002C96CA      call    ds:GetDiskFreeSpaceExA
002C96D0      test    eax, eax
002C96D2      jnz     short loc_2C96EC
002C96D4      mov     dword ptr [ebp+TotalNumberOfBytes], esi
002C96D8      mov     dword ptr [ebp+TotalNumberOfBytes+4], esi
002C96E0      mov     dword ptr [ebp+TotalNumberOfFreeBytes], esi
002C96E6      mov     dword ptr [ebp+TotalNumberOfFreeBytes+4], esi
002C96EC      loc_2C96EC:                                ; CODE XREF: DetectaSandBoxesVMWARE+172Tj
002C96EC      cmp     dword ptr [ebp+TotalNumberOfBytes+4], esi
002C96F2      jnz     short loc_2C96FE
002C96F4      or      [ebp+var_254], 40000000h

```

Ilustración 4. Detección VM (GetDiskFreeSpaceEx)

Op-code especial para VirtualPC.

```

002C9B80 FinVMWARECHECK_CHECKVIRTUALPC:          ; CODE XREF: DetectaSandBoxesVMWARE+561Tj
002C9B80      mov     [ebp+ms_exc.registration.TryLevel], 2
002C9B87      xor     ebx, ebx
002C9B89      xor     eax, eax
002C9B8B      inc     eax
002C9B8C      upcext  7, 0Bh
002C9B90      mov     [ebp+var_314], ebx
-----

```

Ilustración 5. Detección VM (Virtual PC)

Localización de librerías de depuración cargadas en el proceso.

```

002C9E3E      mov     byte ptr [esi+ebx], 2Eh
002C9E42      inc     esi
002C9E43      mov     [ebp+var_250], esi
002C9E49      mov     [ebp+ms_exc.registration.TryLevel], 6
002C9E50      call    BuscaDebugDlls ; intenta detectar distintas dll de log/depurado:
002C9E50                                ; pstorec,dbghep,SbieDll,dir_log,api_watch
002C9E55      mov     edi, eax

```

Ilustración 6. Detección VM (Búsqueda de DLL)

4. PROCEDIMIENTO DE INFECCIÓN

4.1 Vectores de infección

Se ha podido constatar que para distribuir "Ponmocup" no se hace uso de ningún tipo de vulnerabilidad como vector de infección, sino que se distribuye principalmente haciendo uso de técnicas de ingeniería social. Se engaña al usuario para que descargue y ejecute el archivo que contiene el código dañado.

En la documentación consultada, las URLs analizadas que utiliza como vector de infección tienen comprometido el archivo ".htaccess".

Dicho archivo contiene una redirección que es la que se encarga de hacer llegar al usuario el archivo infectado. [\[2\]](#)

4.2 Interacciones con el sistema afectado

Una vez iniciado el código dañino se encargará de descifrar su propio código y ejecutarlo desde memoria.

```

.text:00401683 C7 05 20 23 46+      mov     dword_462320, 87D75850h
.text:0040168D 8D 4D 80      lea     ecx, [ebp+var_80]
.text:00401690 51          push    ecx
.text:00401691 E8 26 13 00 00      call    descifraCodigo_461F7C
.text:00401696 83 C4 04      add     esp, 4
.text:00401699 68 24 23 46 00      push    offset f101dProtect ; lpf101dProtect
.text:0040169E 6A 40          push    40h ; f1NewProtect
.text:004016A0 8B 15 4C 20 46+      mov     edx, dword ptr loc_46204C
.text:004016A6 A1 50 20 46 00      mov     eax, lpAddress
.text:004016AB 2B D0          sub     edx, eax
.text:004016AD 52          push    edx ; dwSize
.text:004016AE 50          push    eax ; lpAddress
.text:004016AF FF 15 B4 70 40+      call    ds:VirtualProtect
.text:004016B5 68 00 02 00 00      push    200h
.text:004016BA 8B 45 10          mov     eax, [ebp+arg_8]
.text:004016BD 50          push    eax
.text:004016BE 8D 4D 80      lea     ecx, [ebp+var_80]
.text:004016C1 51          push    ecx
.text:004016C2 E8 3D 17 00 00      call    ExtraeYEjecutaExeEnMemoria
.text:004016C7 8D 55 80      lea     edx, [ebp+var_80]

```

Ilustración 7. Código de la función de descifrado

Tras hacer esto, se inicia el proceso de detección de máquinas virtuales y SandBox, mediante las técnicas descritas en el apartado de características.

4.2.1 Interacciones con un sistema Virtualizado / Sandbox

Cuando el código dañino detecta que está siendo ejecutado dentro de un entorno virtualizado, o que está siendo depurado, realiza las siguientes acciones:

- Extrae en `%APPDATA%` un archivo ejecutable y escoge para él un nombre aleatorio seleccionado de uno de los archivos contenidos en la carpeta `%WINDIR%\system32` al que añade al final una serie de caracteres aleatorios. Durante el análisis realizado el archivo se ha denominado "WMnetMgrd.exe", suma de "WMnetMg.dll" más los caracteres aleatorios "rd". También ha modificado su extensión de ".dll" a ".exe" (en la [sección 9](#) se puede ver el pseudo-código del algoritmo usado).

La firma para el archivo extraído durante el análisis ha sido:

MD5	b382562d633a466f4e0bf0b42233ec17
SHA1	01a1244f1df87d87b1d37f195de61c8d8e90af6a

Se debe tener en cuenta que el archivo ".exe" creado es único en cada sistema infectado ya que se añaden unos bytes al final del propio archivo cada vez que es generado.

- Una vez creado el nuevo archivo ".exe", lo ejecuta usando la llamada a la API "CreateProcessA"

- c) Este nuevo proceso modifica el fichero *hosts*, añadiendo la redirección a localhost (127.0.0.1) de los siguientes dominios para impedir la navegación hacia los mismos:
- thepiratebay.org
 - www.thepiratebay.org
 - mininova.org
 - www.mininova.org
 - forum.mininova.org
 - blog.mininova.org
 - suprbay.org
 - www.suprbay.org
- d) Finalmente, el “.exe” ejecutado realiza una petición GET utilizando el protocolo HTTP a la dirección `http://imagehut4.cn/update/utu.dat`, con el objetivo de descargarse un nuevo fichero ejecutable ofuscado y ejecutarlo en el sistema comprometido. Durante el análisis realizado, se ha verificado que esta dirección URL no se encuentra disponible.

4.2.2 Interacciones con un sistema real

En el caso de que “Ponmocup” no detecte la presencia de *Sandboxes* o máquinas virtuales, procede de la siguiente manera:

- a) Extrae una librería en `%APPDATA%` y le asigna un nombre aleatorio utilizando el mismo algoritmo explicado en la [sección 4.2.1 a\)](#), con la única diferencia de que la extensión generada es “.dll”.

```

?CDE14 50                                push    eax                                ; Size
?CDE15 8B 8D B8 E6 FF FF                mov     ecx, [ebp+Str]                    ; bytes del archivo a escribir
?CDE1B 51                                push    ecx                                ; Str
?CDE1C 8D 95 B8 F9 FF FF                lea     edx, [ebp+var_648]                ; Nombre aleatorio extraido de system32:
?CDE1C                                ; 'flTMCH.exe',0
?CDE1C                                ; 'cs-G2N.exe',0
?CDE1C                                ; 'sbeioq.dll',0
?CDE1C                                ; 'KBDUGHRV',0
?CDE1C                                ;
?CDE1C                                ; Estos nombres son los que ha escogido en diferentes ejec
?CDE22 8D 8D BC FA FF FF                lea     ecx, [ebp+var_544]                ; Buffer destino
?CDE28 E8 E3 A2 FF FF                call    GuardaArchivoRutaAleatoria        ; El resultado dela ruta seleccionada esta en [ebp+var_544]
?CDE28                                ; 'C:\Users\Administrador\AppData\Roaming\KBDUGHRV.dll',0
?CDE2D 89 85 F0 E6 FF FF                mov     [ebp+bMutextDetectado], eax
?CDE33 B8 D8 15 32 00                mov     eax, offset bufferTelemetria     ; "E3&r2=1&n=15003&n=1&v=1db10106&v6=1&a="...
?CDE38 8D 48 01                lea     ecx, [eax+1]
?CDE3B EB 03                jmp     short loc_2CDE40
?CDE3B                                ; -----
?CDE3D 8D 49 00                db      8Dh, 49h, 0
?CDE3D                                ; -----
?CDE40                                ;
?CDE40                                ;
?CDE40                                ; loc_2CDE40:
?CDE40                                ; CODE XREF: WinMain(x,x,x,x,x)+A8Bfj
?CDE40                                ; WinMain(x,x,x,x,x)+A954j
?CDE40 8A 10                mov     dl, [eax]

```

Ilustración 8. Extracción librería del “bot”

La firma para el archivo generado es:

MD5	072a950be8dbdcff917b2d1f5f5b288
SHA1	ea621f06b689e20a7273601b0a3e7643f868ae56

b) A continuación crea varios valores en el registro de Windows:

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\2 o HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\2	Este valor se utiliza para almacenar los dominios usados por la "dll". El contenido se encuentra cifrado usando una rutina propia de HASH .
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\4 o HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\4	Este valor se utiliza para almacenar la configuración usada por la "dll". El contenido se encuentra cifrado usando una rutina propia de HASH .
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5 o HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5	Este valor se utiliza para almacenar la ruta y nombre de la "dll". El contenido se encuentra cifrado usando una rutina propia de HASH .
HKCU\SYSTEM\CurrentControlSet\1 o HKLM\SYSTEM\CurrentControlSet\1	CRC del nombre y ruta de la "dll".
HKCU\SYSTEM\CurrentControlSet\3 o HKLM\SYSTEM\CurrentControlSet\3	CRC de los dominios.
HKCU\SYSTEM\CurrentControlSet\4 o HKLM\SYSTEM\CurrentControlSet\4	CRC de la configuración.
HKCU\SYSTEM\CurrentControlSet\{numero} o HKLM\SYSTEM\CurrentControlSet\{numero}	Indicadores de distintos pasos realizados durante la instalación
HKCU\Software\<Nombre aleatorio>\<valor aleatorio> o HKLM\Software\<Nombre aleatorio>\<valor aleatorio>	Valor binario que será leído y cargado por la "dll".

En las siguientes ilustraciones se pueden ver las claves de registro creadas:

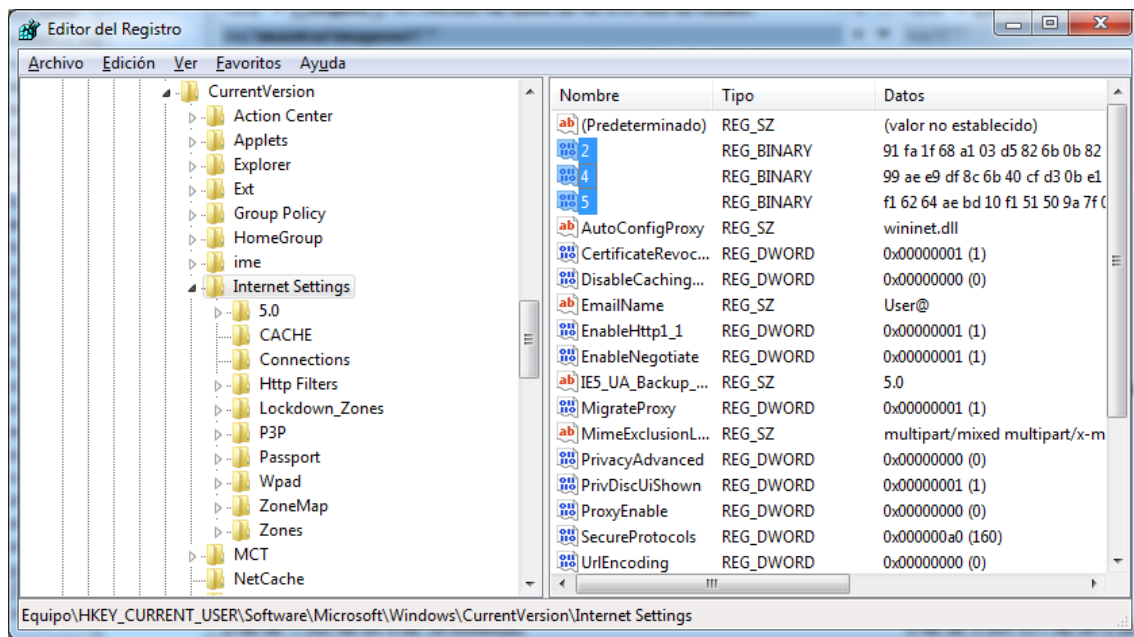


Ilustración 9. Claves de registro creadas en "Internet Settings"

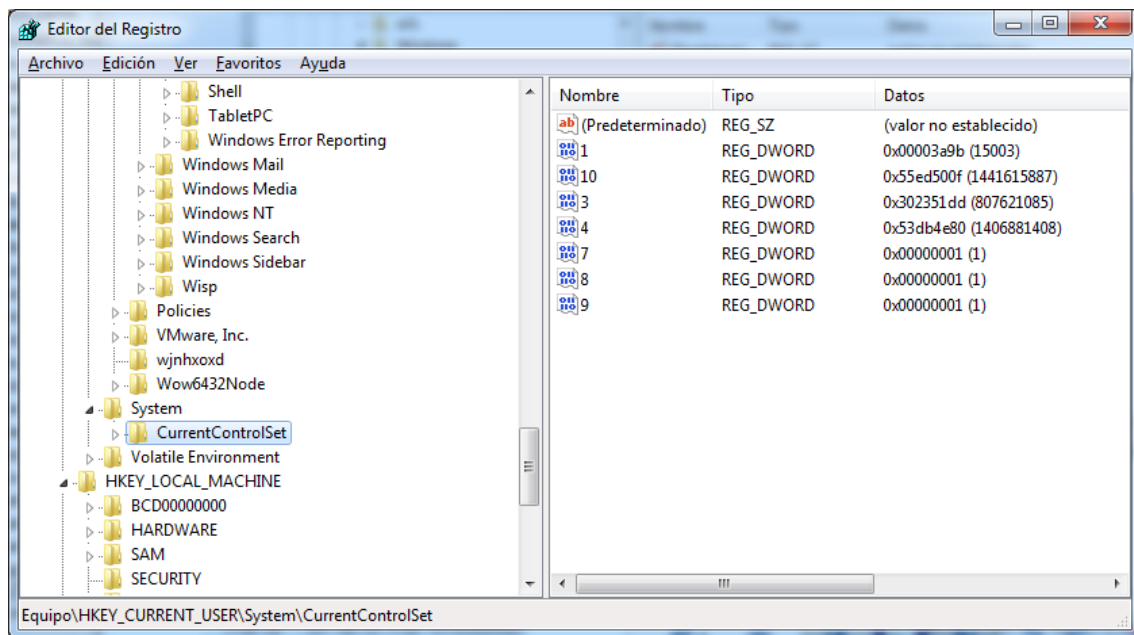


Ilustración 10. Claves de registro creadas en "CurrentControlSet"

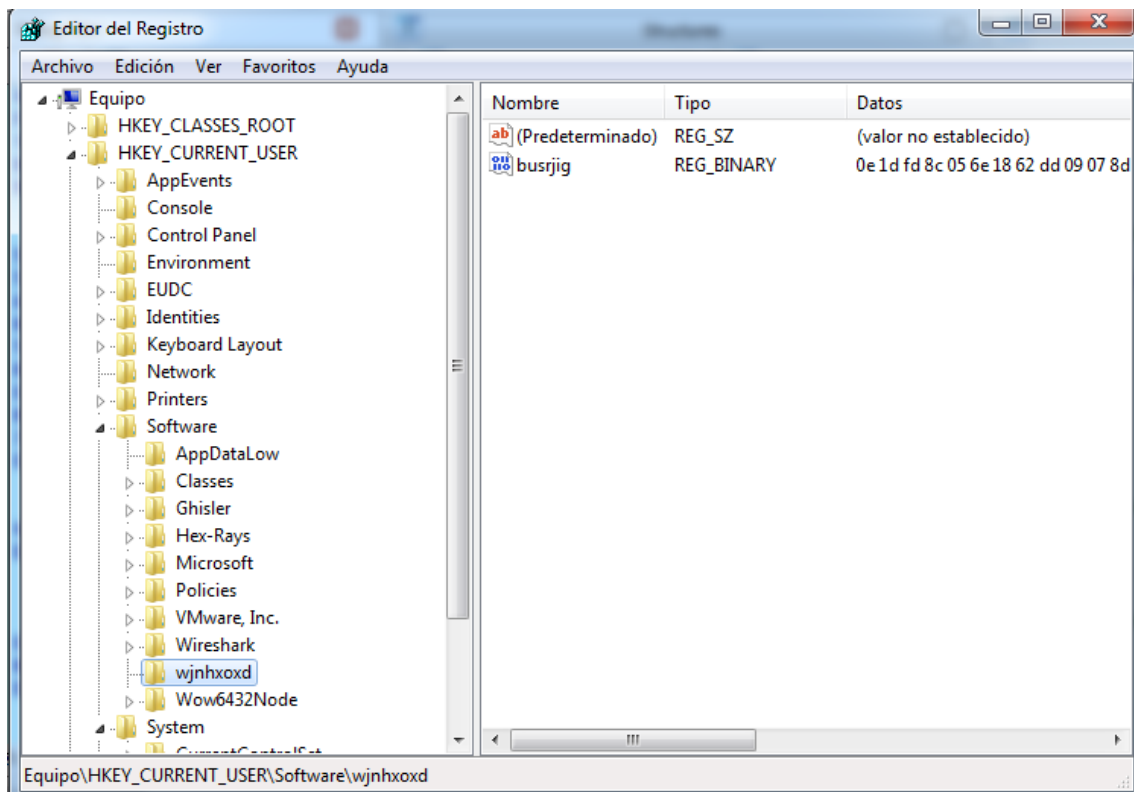


Ilustración 11. Claves de registro aleatoria creada en "Software\wijnhoxd"

En la siguiente ilustración se puede ver el [contenido](#) de la clave "2" antes de ser cifrada e introducida en el registro:

```

CE000C E8 4F D1 FF FF      call     CreateCave_1e6_1.currencontrolset_extrae_cadena_texto_grande ; "1100", "12", "900", 0Ah
CE000C                                     ; "1100", "13", "172000", 0Ah
CE000C                                     ; "1100", "14", "30", 0Ah
CE000C                                     ; "1100", "15", "10", 0Ah
CE000C                                     ; "1500", "10", "12", 0Ah
CE000C                                     ; "1500", "100", "1", 0Ah
CE000C                                     ; "1500", "101", "xklmcomp.com|globalnetscan.com",
CE000C                                     ; "1500", "102", "/feed.php?s=", 0Ah
CE000C                                     ; "1500", "103", "ying.*|ivvbox.*|atdmt.*|img.y
CE000C                                     ; scorecardresearch.com|google-analytics.com|66.
CE000C                                     ; googlehosted.com|gmodules.com|g-mail.com|gma
CE000C                                     ; gmodule.com|googlecode.com|googleearth.com|g
CE000C                                     ; googlenail.com|googletalk.com|googleuserconte
CE000C                                     ; mupads.*|gstatic.*|abmr.*|alexametrics.com"
CE000C                                     ; "1500", "104", "/search\x5C?*q=*|google.*|q=|/sea
CE000C                                     ; q=|/search\x5C?*q=*|bing.*|q=|/search\x5C?*q=*|w
CE000C                                     ; q=|/aol/search\x5C?*q=*|search.aol.com|q=|/searc
CE000C                                     ; search.icq.com|q=|/url\x5C?*q=*|google.*|q=|/url
CE000C                                     ; q=|/yhs/search\x5C?*q=*|search.yahoo.*|q=|/r
CE000C                                     ; ector/sredir\x5C?*query=*|sea
CE0111 89 85 30 E6 FF FF      mov     [ebp+var_19D0], eax
CE0117 B8 D8 15 32 00      mov     eax, offset bufferTelemetry ; "&3&r2=1&n=15003&n=1&v=1db10106&v6=1&a="...
```

Ilustración 12. Cadena de texto con parte de la configuración del "bot"

Una vez generadas las claves de registro, se crea una tarea programada con el objetivo de ejecutar la "dll" en el próximo inicio del sistema.

Para realizar esta acción se genera un archivo con nombre aleatorio en la carpeta del sistema: "%WINDIR%\system32\task". A este archivo se le asigna la extensión ".job", que es usada por el programador de tareas de Windows.

- c) A continuación, la "dll" es ejecutada usando la utilidad del sistema "rundll32.exe" pasándole como parámetro la ruta de esta "dll". Esta ejecución se realiza mediante la API "CreateProcessA".

- d) Se establece la clave de registro encargada de iniciar la "dll" en cada inicio del sistema. [3]
- e) Se desactiva la funcionalidad de "Recuperar Sistema". [4]
- f) Se genera y ejecuta un archivo ".bat" en la ruta "%TEMP%" con el nombre "~uninst" seguido de un valor numérico (en el análisis realizado se generó el archivo con nombre "~uninst7804.bat").

Este archivo ".bat" es ejecutado mediante la llamada a la API "CreateProcessA" y su objetivo es eliminar los archivos utilizados durante el proceso de instalación de "Ponmocup".
- g) Finalmente envía la información recopilada durante el proceso de instalación de "Ponmocup" al servidor C&C. La información que envía son marcas de tiempo entre cada paso realizado durante la instalación, además de los cambios que ha realizado en el sistema (claves de registro creadas, "dll" creada, CRC de los archivos creados, etc.).

Todo este proceso tiene como objetivo extraer una "dll" que ha de realizar tareas determinadas. Por ejemplo, descargar nuevos módulos desde direcciones URL específicas y hacerlos residentes en memoria.

Como se puede apreciar, durante el proceso de instalación se han creado numerosas claves de registro. Estas claves son usadas por la "dll" para obtener la configuración necesaria que indicará cómo actuar y desde dónde realizar las descargas de nuevos ficheros mencionadas anteriormente.

Estas claves de registro contienen datos cifrados de la ruta y nombre de la "dll" usada, [dominios](#), [datos de configuración](#) e incluso información binaria que la "dll" ejecutará en memoria.

5. PERSISTENCIA EN EL SISTEMA

Para garantizar su persistencia "Ponmocup" tiene dos métodos distintos de actuación, en función de si ha detectado que está ejecutando dentro de un entorno Virtualizado/Sandbox, o en una máquina real.

5.1 PERSISTENCIA EN SISTEMAS VIRTUALIZADOS / SANDBOX

Cuando "Ponmocup" ha detectado una máquina virtual / Sandbox:

- a) Selecciona de manera aleatoria el nombre de algún fichero existente en `%WINDIR%\system32` y aplica el mismo algoritmo explicado en la [sección 4.2.1 a\)](#).
- b) Genera un "exe" con ese nombre en `%APPDATA%`
- c) Añade un valor con la ruta del fichero creado en la clave de registro de autorun `"[HKLM | HKCU]\software\microsoft\windows\currentversion\run"`

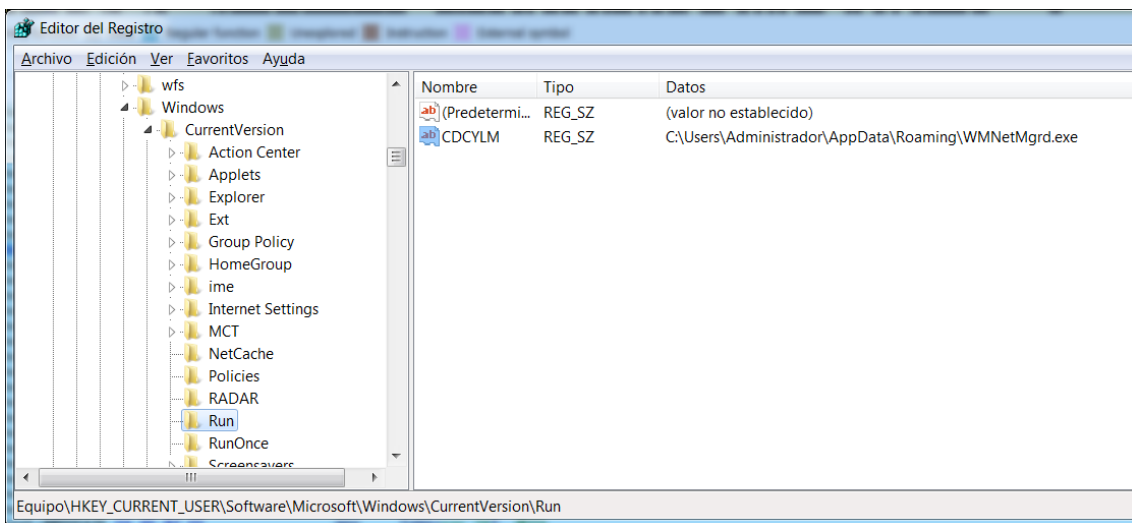


Ilustración 13. Claves de registro creadas para la persistencia en VM / Sandbox

5.2 PERSISTENCIA EN SISTEMAS REALES

Cuando "Ponmocup" no ha detectado ninguna máquina virtual o *Sandbox*:

- Selecciona de manera aleatoria el nombre de algún fichero existente en `%WINDIR%\system32` y aplica el mismo algoritmo explicado en la [sección 4.2.1 a\)](#).
- Genera una librería "dll" con el nombre seleccionado en `%APPDATA%`
- Crea una tarea programada para ejecutar mediante `rundll32` la función principal de la "dll". Esta tarea se ejecutará en el próximo inicio del sistema.

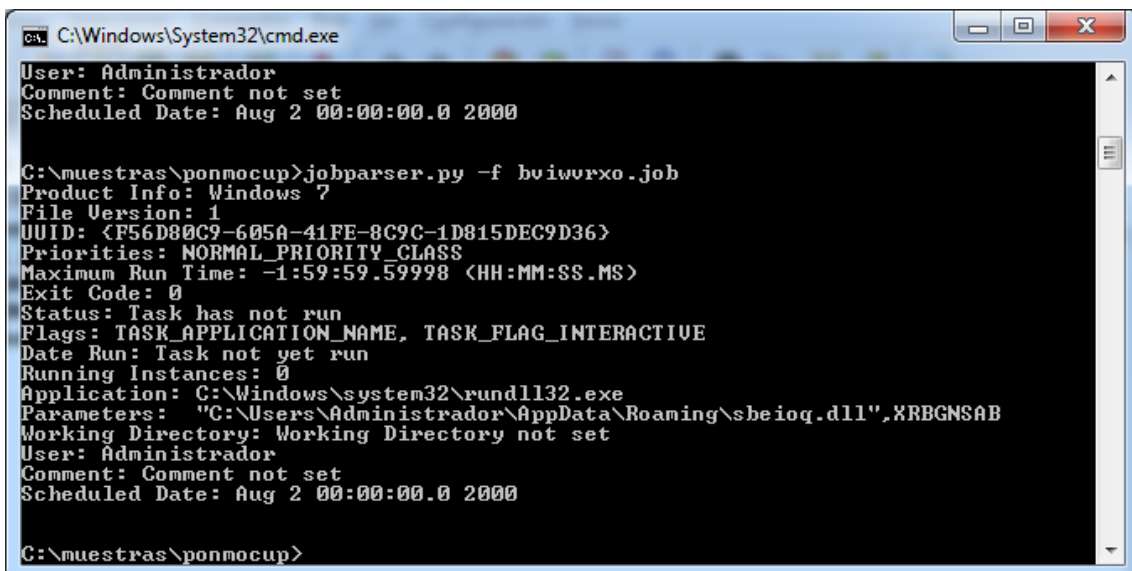


Ilustración 14. Tarea programada

- Añade un valor aleatorio en la clave de registro de "Autorun": `[HKLM | HKCU]\software\microsoft\windows\currentversion\run`, con el

comando "rundll32.exe" para asegurarse la ejecución en cada inicio del sistema. En la siguiente ilustración se puede ver un ejemplo de la clave de registro creada:

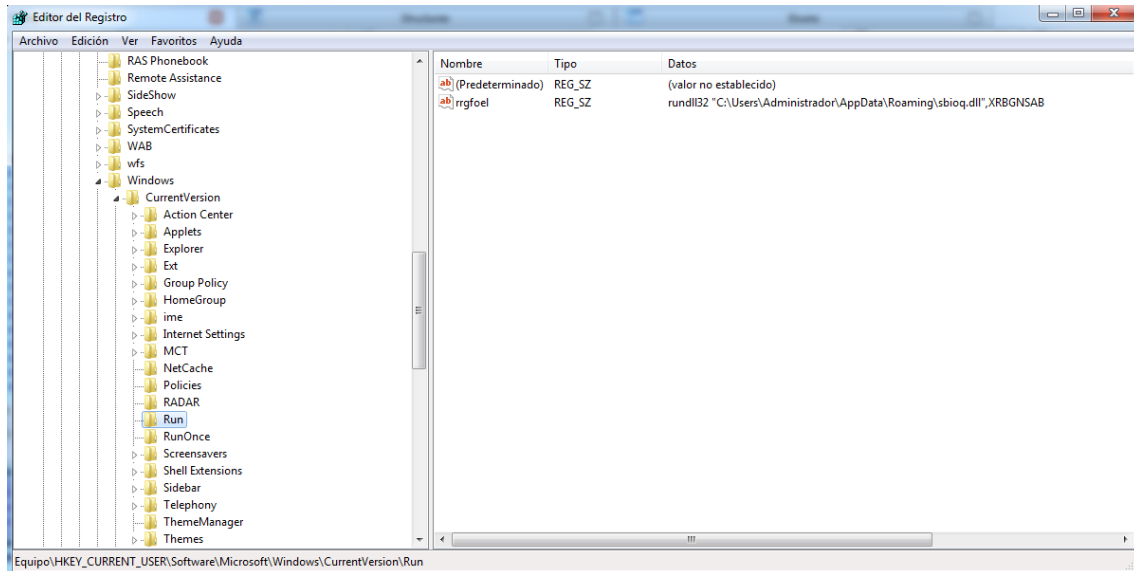


Ilustración 15. Claves de registro creadas para la persistencia en máquina real

Y finalmente, desactiva la recuperación del sistema para así dificultar las tareas de desinfección, para ello hará uso de la función no documentada "DisableSR" de la librería "srclient.DLL" de Microsoft:

```

35D97 8B 54 35 A4      mov     [ebp+esi+ProcName], dl
35D9B 40              inc     eax
35D9C 89 45 90      mov     [ebp+var_70], eax
35D9F EB CF      jmp     short loc_2C5D70      ; decodifica:
                                ; 'DisableSR',0
35DA1              ; -----
35DA1              loc_2C5DA1:                  ; CODE XREF: DisableSystemRecovery+1481j
35DA1 0F B7 C0      movzx   eax, ax
35DA4 C6 44 05 A4 00  mov     [ebp+eax+ProcName], 0
35DA9 8D 40 A4      lea     ecx, [ebp+ProcName]      ; 'DisableSR',0
35DAC 51          push    ecx                    ; lpProcName
35DAD 8B 55 98      mov     edx, [ebp+hLibModule]    ; srclient.dll
35DB0 52          push    edx                    ; hModule
35DB1 FF D3      call    ebx ; GetProcAddress
35DB3 89 45 84      mov     [ebp+var_7C], eax
35DB6 85 FF      test    edi, edi
35DB8 0F 84 84 00 00 00  jz      loc_2C5E42
35DBE 6A 00      push    0
35DC0 FF D7      call    edi
35DC2 89 45 80      mov     [ebp+var_80], eax

```

Ilustración 16. Desactivación de "SystemRecovery"

6. CONEXIONES DE RED

Como se ha comentado, "Ponmocup" altera su comportamiento en función del tipo de sistema en el que se encuentre. Algo común es que siempre contactará con su C&C para informarle del tipo de instalación que ha realizado.

6.1 Conexiones establecidas contra el C&C

Todas las comunicaciones realizadas contra el C&C utilizan el siguiente User-Agent:



Ilustración 17. Uso del User-Agent durante la conexión con el C&C

La comunicación es establecida mediante el protocolo HTTP haciendo uso de las APIS de Windows:

"InternetOpenA"
"InternetOpenUrlA"
"InternetReadFile"
"InternetCloseHandle"

El dominio al que conecta es "montyinc.net". Esta dirección se encuentra establecida de forma estática dentro del binario de "Ponmocup".

La conexión es configurada para realizar dos reintentos. Los tiempos de espera son establecidos en 15 minutos para la recepción, y 30 segundos para la conexión y envío. En la siguiente imagen se puede observar cómo son configurados estos parámetros:

```

002C1127      push     4                ; dwBufferLength
002C1129      lea      eax, [ebp+Buffer] ; 30000 ms = 30 segundos
002C112C      push     eax                ; lpBuffer
002C112D      push     2                ; dwOption = INTERNET_OPTION_CONNECT_TIMEOUT
002C112F      push     esi                ; hInternet
002C1130      mov     edi, ds:InternetSetOptionA
002C1136      call    edi ; InternetSetOptionA
002C1138      mov     [ebp+Buffer], ebx ; 30000 ms = 30 segundos
002C113B      push     4                ; dwBufferLength
002C113D      lea      ecx, [ebp+Buffer]
002C1140      push     ecx                ; lpBuffer
002C1141      push     5                ; dwOption = INTERNET_OPTION_CONTROL_SEND_TIMEOUT
002C1143      push     esi                ; hInternet
002C1144      call    edi ; InternetSetOptionA
002C1146      mov     [ebp+Buffer], 900000 ; 900000 ms = 15 minutos
002C114D      push     4                ; dwBufferLength
002C114F      lea      edx, [ebp+Buffer]
002C1152      push     edx                ; lpBuffer
002C1153      push     6                ; dwOption = INTERNET_OPTION_CONTROL_RECEIVE_TIMEOUT
002C1155      push     esi                ; hInternet
002C1156      call    edi ; InternetSetOptionA
002C1158      mov     [ebp+var_20], 2 ; 2 reintentos
002C115F      push     4                ; dwBufferLength
002C1161      lea      eax, [ebp+var_20]
002C1164      push     eax                ; lpBuffer
002C1165      push     3                ; dwOption = INTERNET_OPTION_CONNECT_RETRIES
002C1167      push     esi                ; hInternet
002C1168      call    edi ; InternetSetOptionA

```

Ilustración 18. Configuración de tiempos de espera para el C&C

El envío de datos hacia el C&C se realiza mediante peticiones GET.

A continuación se muestran un ejemplo de los datos enviados al C&C tras realizar la instalación del código dañino

```

html/license_DB32C92504C636C070A0E9089CD55FF91CCEA4B8B02986222EFC240400
56312F2'824A007F3FDD65B64D42BC18E893955BA01B14ED148B23551E508C931B4CE0A
19

```

Los datos son enviados de forma cifrada sobre protocolo HTTP y contienen una telemetría completa de todo el proceso de instalación en el sistema así como datos recopilados sobre el propio sistema afectado.

6.2 Conexiones establecidas en un sistema virtual / sandbox

Si se ha detectado que se está ejecutando bajo una máquina virtual o *sandbox*, además de enviar información al C&C, se realiza el intento de descarga de un nuevo binario. A continuación se muestra la información de estas conexiones.

El *User-Agent* utilizado para realizar la descarga del nuevo binario es:

User-Agent
Mozilla/4.0 (compatible; MSIE 7.0 ; Windows NT 5.2; SV1)

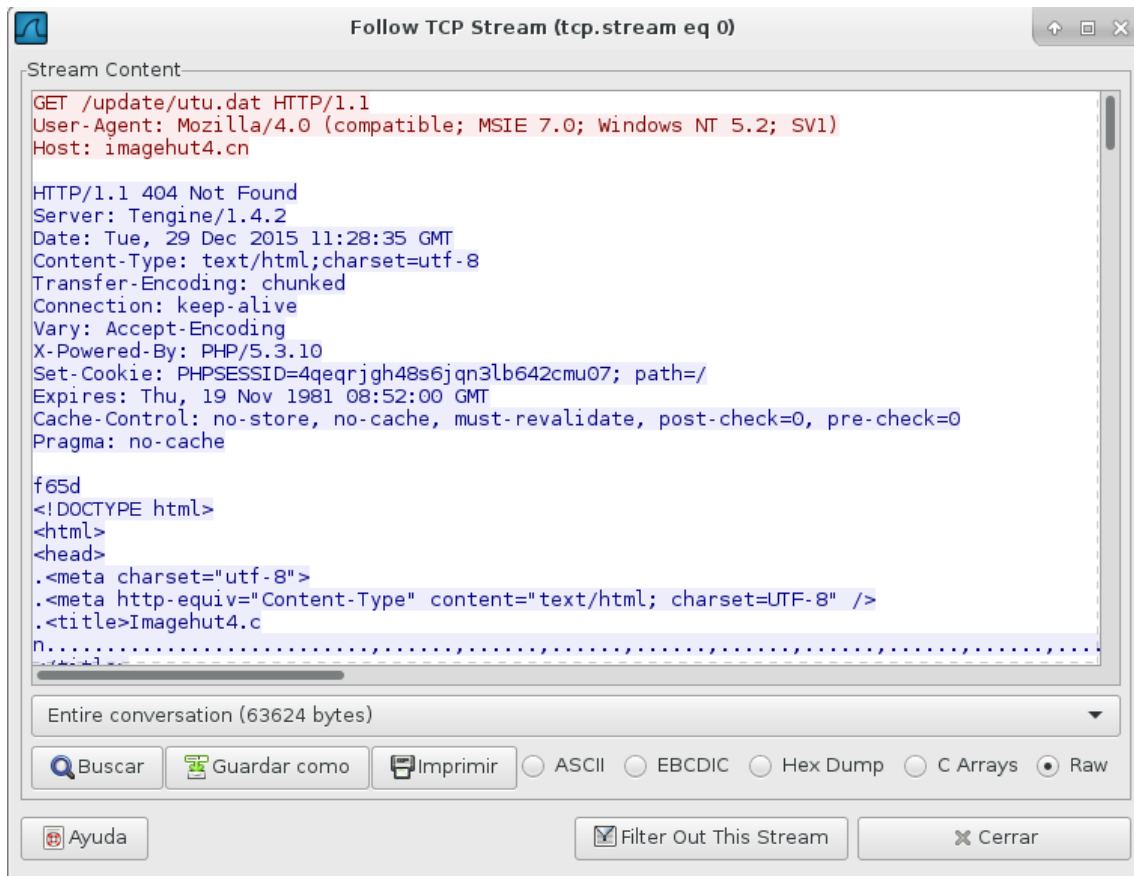


Ilustración 19. Uso del User-Agent durante la conexión de descarga

La comunicación es establecida mediante el protocolo HTTP haciendo uso de las APIS de Windows:

"InternetOpenA"
"InternetOpenUrlA"
"InternetReadFile"
"InternetCloseHandle"

La dirección *host* hacia la que conecta es "imagehut4.cn". Esta dirección se encuentra establecida de forma estática dentro del binario que actúa como *dropper*.

En el momento del análisis el archivo "utu.dat" no estaba disponible en el servidor.

6.3 Información del atacante

6.3.1 IMAGEHUT4.CN

6.3.1.1 DIRECCIÓN IP

Según la información facilitada por Robtex.com, el dominio "imagehut4.cn" se corresponde con la dirección 123.254.111.190

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
imagehut4.cn	A		imagehut4.cn	65.19.157.235		65.19.128.0/18 Hurricane Electric HURRICANE-4	AS6939 HURRICANE Hurricane Electric	Fremont, United States
				123.254.111.190	hkhdc.laws.ms	123.254.104.0/21 123.254.111.0/24 Proxy-registered route object CLOUDIE-HK Unit 1604, Perfect Industrial Building 31st Tai Yau Street, San Po Kong Kowloon NA	AS133731 RAINBOW-2 Rainbow Network Limited	Hong Kong
	NS (missing in zone)			ns1.dnbiz.com	205.164.14.67	205.164.0.0/18 55 S. Market St. NET-205-164-14-64	AS18779 ENERGY- GROUP, NETWORKS Energy Group Netwo	San Jose, United States
				ns2.dnbiz.com	205.164.14.79			
	MX		mail.skrimple.com	23.23.149.79	ec2-23-23-149-79.compute-1.amazonaws.com	23.22.0.0/15 Amazon EC2 IAD prefix AMAZON- EC2-USEAST-10	AS14618 Amazon- AES-IAD Amazon- AES-IAD	Ashburn, United States
				23.23.152.148	ec2-23-23-152-148.compute-1.amazonaws.com	54.224.0.0/15 Amazon EC2 IAD prefix AMAZON-2011L		
				54.225.102.91	ec2-54-225-102-91.compute-1.amazonaws.com	54.242.0.0/15 Amazon EC2 IAD prefix AMAZON-ZIAD1		
				54.243.145.112	ec2-54-243-145-112.compute-1.amazonaws.com	184.72.128.0/17 Amazon IAD prefix AMAZON-EC2-7		
				54.243.155.13	ec2-54-243-155-13.compute-1.amazonaws.com			
				184.72.252.56	ec2-184-72-252-56.compute-1.amazonaws.com			

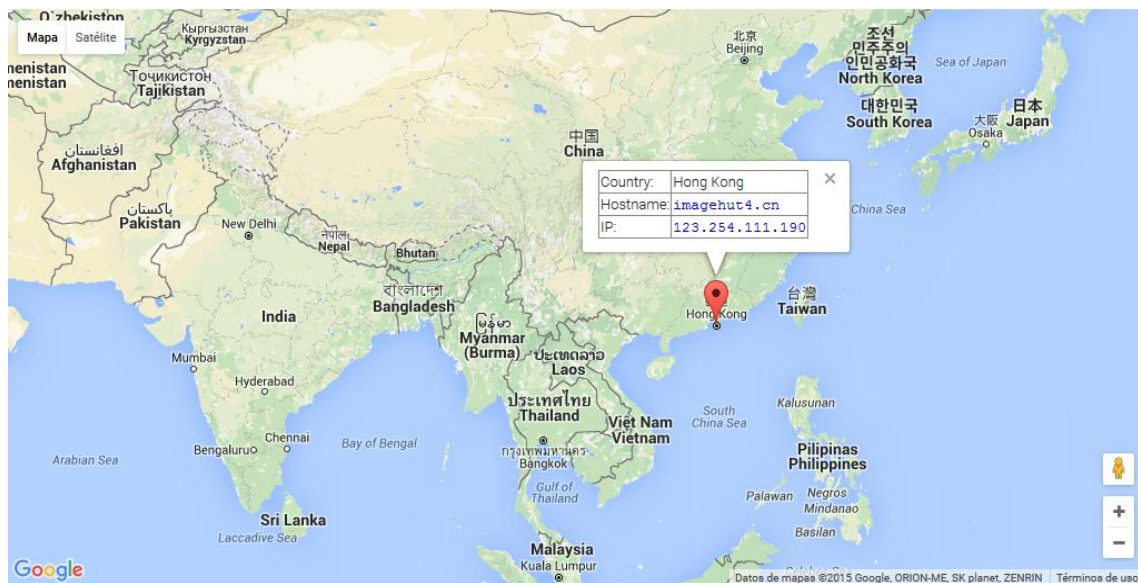
Existen otros dominios que poseen la misma dirección IP, son los siguientes:

xn--fiqs8s44ps61b.biz	abranet.cn	acadesine.cn
aikutu.cn	aimengmeng.cn	akalmas.cn
alicpc.cn	anyea.cn	appebb.cn
aprilmay.cn	bagudi.cn	baihuakai.cn
bbail.cn	belfirst.cn	bianmitong.cn
c-memo.cn	cargym.cn	catupiry.cn
cop-1.cn	corigin.cn	dahuya.cn
dehoplast.cn	delitebaskets.cn	dfate.cn
dl-5.cn	dqbj.cn	dristone.cn
evaye.cn	fheyes.cn	filmco.cn
frumenty.cn	goldroland.cn	golss.cn
gotoco.cn	grandcoupe.cn	greest.cn
hadaka.cn	handifoam.cn	hiflon.cn
honeypad.cn	horrax.cn	jgnt.cn
jinshadao.cn	jiujiemei.cn	jiulongfang.cn
jiyuntong.cn	jj-max.cn	jkrup.cn
joinshow.cn	joyyen.cn	jsaeg.cn
jukeyun.cn	julot.cn	kaiseki.cn
kkmiss.cn	laosxg.cn	lasuit.cn
leanel.cn	legrass.cn	lichangan.cn
lillet.cn	linyiq.cn	lishengyu.cn
lizhifang.cn	lobbied.cn	loginous.cn
lotvis.cn	luminize.cn	manqia.cn
mgi.cn	mingshitong.cn	miramer.cn
natureclean.cn	ndione.cn	neighs.cn
njsinaite.cn	nnt520.cn	nuevopak.cn
nystay.cn	paroven.cn	phlatlight.cn
piela.cn	poligo.cn	polismart.cn
portress.cn	primerip.cn	promil.cn
qiyanshan.cn	raydel.cn	rialtos.cn
royalmelody.cn	runcolour.cn	sanlusy.cn
sengsuo.cn	squired.cn	stormseal.cn
suciy.cn	sukuo.cn	supalock.cn
trampolins.cn	trepan.cn	uidp.cn
vialox.cn	xingfuy.cn	xingguanglu.cn

zhfrd.cn	15345.com	1daili.com
266303.com	520chanel.com	795788.com
838982.com	aifalv.com	alyj.com
bendijing.com	bengao.com	bffw.com
cnlook.com	dadianwan.com	dajinchuan.com
fenkeng.com	guizhongmiyou.com	haorao.com
huboshi.com	maoshang.com	mubiao.com
nuankou.com	ouyeda.com	qianbilipin.com
qmtxtv.com	shuoniu.com	xinlonghui.com
yingjianta.com	od.my	aguang.net
shipi.net	townsendspres.net	zaoying.net
*.aiat6.cn	www.bizhixiu.cn	222ccc.com.cn
annuan.com.cn	ceel.com.cn	hong-qiao.com.cn
nikesport.com.cn	omiz.com.cn	qx8.com.cn
www.cqxy.cn	*.syjl.cn	www.airtelghana.com
www.chinahuaxia.com	mail.gddasheng.com	www.ningdai.com
*.taihushi.com	*.pkj.net	221.65.76.118.adsl-pool.sx.cn
174.214.204.221.adsl-pool.sx.cn	56.228.134.61.adsl-pool.sx.cn	

6.3.1.2 GEOLOCALIZACIÓN

En el momento del análisis, la dirección IP 123.254.111.190 se encuentra ubicada en Hong Kong como se muestra en la siguiente imagen:



6.3.1.3 WHOIS

A continuación se muestra información extendida whois facilitada por el sitio web "whois.net":

Domain Name: imagehut4.cn
 ROID: 20130729s10001s64898887-cn
 Domain Status: ok
 Registrant ID: whois_private
 Registrant: WHOIS PRIVACY PROTECTION SERVICE
 Registrant Contact Email: whois.private.service@gmail.com
 Sponsoring Registrar: Dnbiz Limited
 Name Server: ns1.dnbiz.com

Name Server: ns2.dnbiz.com
 Registration Time: 2013-07-29 10:32:08
 Expiration Time: 2016-07-29 10:32:08
 DNSSEC: unsigned

6.3.2 MONTYINC.NET

6.3.2.1 DIRECCIÓN IP

Según la información facilitada por Robtex.com, el dominio "montyinc.net" se corresponde con la dirección IP 173.230.158.166

Base	Record Preference	Name	IP Number	Reverse	Routes	AS	Location
montyinc.net	A	montyinc.net	173.230.158.166	li200-166.members.linode.com	173.230.144.0/20 LINODE-US	AS6939 HURRICANE Hurricane Electric	Absecon, United States
	NS	x.h.03.net.baskingshark.ns1					
		x.h.03.net.baskingshark.ns2					
	NS (only in SOA)	ns1.baskingshark.net	178.79.157.231	ns1.baskingshark.net	178.79.128.0/18 Linode-2 LINODE-UK Linode, LLC	AS15830 TELECITY-LON TELECITYGROUP INTERNATIONAL	United Kingdom

Ilustración 20. Registros encontrados del Dominio "montyinc.net"

Existen otros dominios que poseen la misma dirección IP, son los siguientes:

extraperlo.biz	iesnaretrack.biz	pheer.biz
thejacksonfive.biz	upagent99.biz	b0tx.com
beistellened.com	beslime.com	besprutaness.com
bigfootkillme.com	brzuchy.com	gabcircle.com
installstorm.com	lbdmcmfuinc.com	microsoftgroups.com
obamawebcam.com	oryxyioosnrmfvvq.com	qaoxnspmwxwemhu.com
rhopaloceros.com	smotri123.com	thesexydude.com
usashopsoftusa.com	win32updater.com	yougotissuez.com
binaryfeed.in	niceshot.in	povertyba.in
sexme.in	aburame.info	kwqoutmkxpjvupsm.info
pse1jo2po3.info	shume.info	xinapxe.info
gusanodeseda.mobi	clan-uchiha.net	defintelsucks.net
dxupusopmqpofs.net	gusanodeseda.net	guys4us.net
montyinc.net	q8still.net	sexytechnology.net
thefuelworkz.net	victoryltd.net	alumnigroup.org
saudi-cool.org	http-harddrive.us	hostmaster.thejacksonfive.biz
*.b0tx.com	hostmaster.b0tx.com	mail.b0tx.com
x2.b0tx.com	x3.b0tx.com	*.bigfootkillme.com
www.bigfootkillme.com	www.brzuchy.com	www.fget-career.com
*.installstorm.com	config.installstorm.com	down.installstorm.com
ku.installstorm.com	ku1.installstorm.com	ns1.microsoftgroups.com
ns2.microsoftgroups.com	www.microsoftgroups.com	www.qaoxnspmwxwemhu.com
*.smotri123.com	hostmaster.smotri123.com	new.smotri123.com
*.thesexydude.com	hostmaster.thesexydude.com	mail.thesexydude.com
*.usashopsoftusa.com	www.usashopsoftusa.com	windowsmedia.net.in
*.niceshot.in	mail.niceshot.in	nice.niceshot.in
*.povertyba.in	www.povertyba.in	www.sexme.in
www.kwqoutmkxpjvupsm.info	*.pse1jo2po3.info	webmail.shume.info
*.defintelsucks.net	www.defintelsucks.net	*.guys4us.net
nali.guys4us.net	www.guys4us.net	*.oqdbvkrfvgvrqk.net
*.q8still.net	parta.q8still.net	*.thefuelworkz.net
four.thefuelworkz.net	*.alumnigroup.org	loot.alumnigroup.org
*.saudi-cool.org	sam3.saudi-cool.org	ns2.http-harddrive.us
li200-166.members.linode.com		

6.3.2.2 GEOLOCALIZACIÓN

En el momento del análisis, la dirección IP 173.230.158.166 se encuentra ubicada en Estados Unidos, como se muestra en la siguiente imagen:

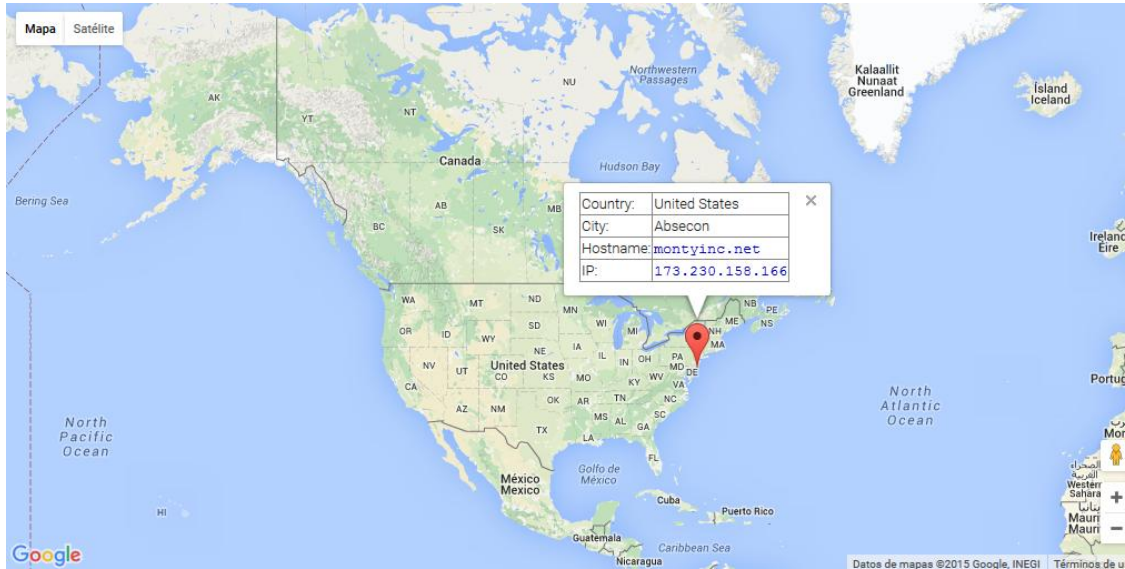


Ilustración 21. Geolocalización del Dominio "montyinc.net"

IP Information Results for 173.230.158.166						
Country	Country Code	Region	City	Latitude	Longitude	ISP
us	us	nj	absecon	39.420090	-74.499840	hurricane electric i...
United States	US	New Jersey	Absecon	39.489899	-74.477303	Linode
United States	US	California	Fremont	37.548271	-121.988571	Linode

Ilustración 22. Información de la dirección IP "173.230.158.166"

6.3.2.1 WHOIS

A continuación se muestra información extendida whois facilitada por el sitio web "whois.net":

```

Domain Name: MONTYINC.NET
Registrar: BIGROCK SOLUTIONS LIMITED
Sponsoring Registrar IANA ID: 1495
Whois Server: Whois.bigrock.com
Referral URL: http://www.bigrock.com
Name Server: NS1.SINKHOLE.CH
Name Server: NS2.SINKHOLE.CH
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Updated Date: 30-nov-2015
Creation Date: 07-apr-2011
Expiration Date: 07-apr-2016

```

>>> Last update of whois database: Tue, 29 Dec 2015 09:52:39 GMT <<<

7. DETECCIÓN

Para detectar si un equipo se encuentra o ha estado infectado para cualquiera de sus usuarios se empleará la herramienta del sistema "regedit.exe" (editor del registro), o bien se ejecutará alguna de las herramientas de Mandiant como el "Mandiant IOC Finder" o el colector generado por RedLine@ con los indicadores de compromiso generados para su detección.

Se recomienda iniciar sesión con un usuario que posea derechos administrativos en el sistema para realizar las siguientes comprobaciones.

7.1 UTILIDAD DEL SISTEMA

Se ejecutará la utilidad "regedit.exe" (inicio > ejecutar > regedit) y se localizará la existencia de las siguientes entradas en el registro, tanto en HKEY_LOCAL_MACHINE como en HKEY_CURRENT_USER

```
"Software\Microsoft\Windows\CurrentVersion\Internet Settings"
```

```
"System\CurrentControlSet"
```

Después, se comprobará si estas entradas contienen valores con nombres comprendidos entre el 1 y el 10, como en las ilustraciones 8 y 9 de este documento.

Si se encuentra alguna de esas entradas de registro, significa que el equipo se encuentra infectado.

7.2 MANDIANT

Se ha generado un nuevo archivo indicador de compromiso. El nombre del indicador generado es "**Ponmocup - CCN-CERT**" con GUID "a209da74-723c-46af-ad88-abfd39be1f67".

Se utilizará el indicador con alguna de las herramientas de las que dispone Mandiant como "Mandiant_ioc_finder" o para la confección de un recolector de evidencias mediante "Mandiant RedLine".

Se recomienda consultar la guía de seguridad CCN-STIC-423 Indicadores de Compromiso (IOC), donde se recoge qué es un indicador de compromiso, cómo crearlo y cómo identificar equipos comprometidos.

Name: Ponmocup	T..	R..
Author: CCN-CERT		
GUID: a209da74-723c-46af-ad88-abfd39be1f67		
Created: 2015-12-09 16:15:36Z		
Modified: 2015-12-14 11:34:38Z		

Description:

IOCs para detectar:

- Dropper MD5
- Registry keys
- Snort

Add: AND OR Item ▾

- OR
 - Registry Key Path contains HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\8
- OR
 - Registry Key Path contains HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\9
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\1
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\2
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\3
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\4
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\5
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\6
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\7
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\8
- OR
 - Registry Key Path contains HKLM\System\CurrentControlSet\9
- OR
 - Snort Rule, double click to view or edit
- OR
 - Snort Rule, double click to view or edit

Ilustración 23. Indicadores de compromiso IOCs

8. DESINFECCIÓN

8.1 Manual

A continuación se detallan los pasos necesarios para llevar a cabo una desinfección manual de "Ponmocup" en el equipo:

En primer lugar, se ejecutará la utilidad "regedit.exe" (inicio > ejecutar > regedit) para localizar las siguientes entradas en el registro, tanto en HKEY_LOCAL_MACHINE como en HKEY_CURRENT_USER:

```
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\1"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\2"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\3"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\4"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\5"
```

"Software\Microsoft\Windows\CurrentVersion\Internet Settings\6"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\7"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\8"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\9"
"Software\Microsoft\Windows\CurrentVersion\Internet Settings\10"
"System\CurrentControlSet\1"
"System\CurrentControlSet\2"
"System\CurrentControlSet\3"
"System\CurrentControlSet\4"
"System\CurrentControlSet\5"
"System\CurrentControlSet\6"
"System\CurrentControlSet\7"
"System\CurrentControlSet\8"
"System\CurrentControlSet\9"
"System\CurrentControlSet\10"

Una vez eliminadas dichas claves se procederá a buscar la siguiente entrada en el registro, igual que en el caso anterior, tanto en HKEY_LOCAL_MACHINE como HKEY_CURRENT_USER:

"Software\Microsoft\Windows\CurrentVersion\Run\"

En esta entrada se deberá de localizar un nombre generado aleatoriamente que contendrá como valor, o bien un nombre de archivo con extensión ".exe", o bien "rundll32.exe" seguido de un nombre de librería con extensión ".dll".

En el caso estudiado en este informe, se han generado las siguientes claves:

Clave generada para el archivo ".exe"

"HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CDCYLM"

Con el valor:

"%APPDATA%\VMNetMgrd.exe"

Clave generada para el archivo ".dll"

"HKCU\Software\Microsoft\Windows\CurrentVersion\Run\RRGFOL"

Con el valor:

Rundll32 "%APPDATA%\sbioq.dll",XRBGNSAB

Una vez localizados nombre y ruta se procede a eliminar el archivo y la clave de registro.

En la siguiente imagen se puede ver la clave mencionada para el archivo ".exe".

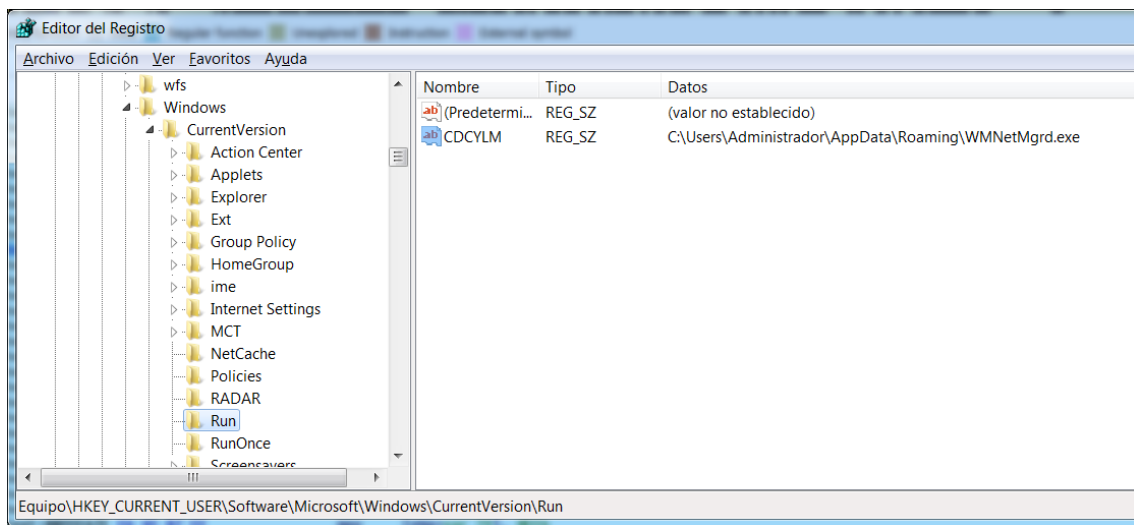


Ilustración 24. Claves de registro creadas para la persistencia

Por último se localizará la clave "HKLM\Software\<nombre aleatorio>\<valor aleatorio>" o "HKCU\Software\<nombre aleatorio>\<valor aleatorio>" y se eliminará.

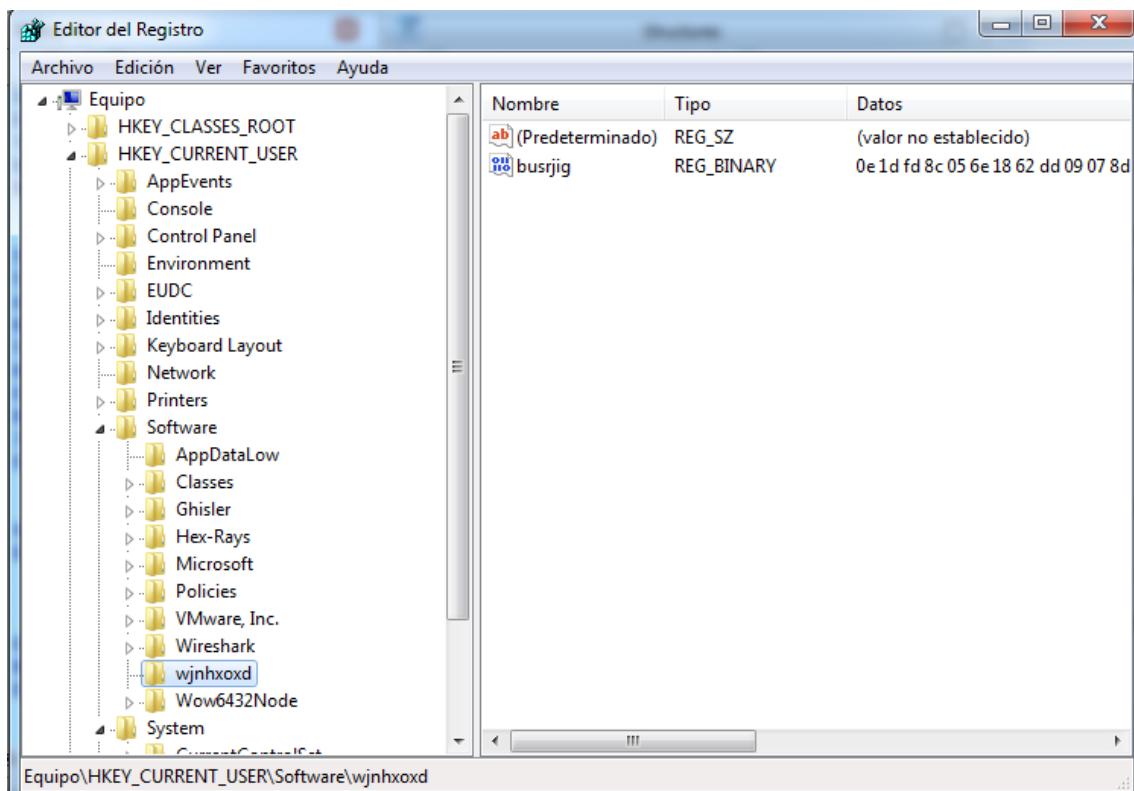


Ilustración 25. Clave de registro creada con valores aleatorios

8.2 Automática

Se aconseja instalar un software antivirus en todos aquellos equipos en los que se haya detectado algún indicador de compromiso o encontrado algún archivo o clave

de registro indicados, y realizar un análisis completo del sistema para desinfectarlo completamente.

NOTA: estas recomendaciones son aplicables también a dispositivos removibles.

9. ALGORITMOS

A continuación se muestra el pseudo-código de varios algoritmos usados por el instalador y la "dll" de "ponmocup"

```
int __fastcall decodeString1(int a1, int a2, int a3, int a4, signed int a5)
{
    int v5; // ebx@1
    int i; // esi@1
    int v7; // edx@3
    int v9; // [sp+14h] [bp-24h]@1
    int v10; // [sp+18h] [bp-20h]@1

    v10 = a1;
    v5 = a2 + *(_BYTE *)a4 % (a3 - a2 + 1);
    v9 = *(_BYTE *)a4 + 1 % 3;
    for ( i = 0; i < v5; ++i )
    {
        v7 = *(_BYTE *)((i + 2) % a5 + a4) % 26 + 65;
        if ( v9 == 1 || v9 == 2 && i )
            LOBYTE(v7) = (unsigned __int16)(*(_BYTE *)((i + 2) % a5 + a4) % 26) + 97;
        a1 = v10;
        *(_BYTE *)(i + v10) = v7;
    }
    *(_BYTE *)(v5 + a1) = 0;
    return a1;
}

void __fastcall generaHASH(int datos, signed int lenDatos, int buf_destino, int lenDestino, int nIteraciones)
{
    signed int contadorBucleTabla; // edi@1
    signed int i; // eax@3
    unsigned __int8 tmpIDX; // cl@6
    signed int TotalVueltasBucle; // eax@7
    char *v9; // esi@10
    char v10; // bl@10
    char *v11; // eax@10
    unsigned __int8 v12; // dl@11
    int j; // esi@11
    unsigned __int8 v14; // al@13
    char *v15; // eax@13
    char v16; // ST19_1@13
    char *v17; // ecx@13
    int buf_datos; // [sp+Ch] [bp-12Ch]@1
    signed int size_buf_datos1; // [sp+10h] [bp-128h]@1
    char contadorTabla; // [sp+1Bh] [bp-11Dh]@6
    unsigned __int8 contadorTablaa; // [sp+1Bh] [bp-11Dh]@11
```

```

char tabla[256]; // [sp+1Ch] [bp-11Ch]@5
void *v23; // [sp+11Ch] [bp-1Ch]@1
CPPEH_RECORD ms_exc; // [sp+120h] [bp-18h]@1

v23 = (void *)cookieDword;
size_buf_datos1 = lenDatos;
buf_datos = datos;
contadorBucleTabla = 0;
ms_exc.registration.TryLevel = 0;
if ( buf_destino && lenDestino )
{
    for ( i = 0; i < 256; ++i )
        tabla[i] = i;
    tmpIDX = 0;
    contadorTabla = 0;
    while ( 1 )
    {
        TotalVueltasBucle = lenDatos;
        if ( lenDatos <= 256 )
            TotalVueltasBucle = 256;
        if ( contadorBucleTabla >= TotalVueltasBucle )
            break;
        v9 = &tabla[(unsigned __int8)++contadorTabla];
        v10 = *v9;
        tmpIDX += *v9 + *(_BYTE *) (contadorBucleTabla % size_buf_datos1 + buf_datos);
        v11 = &tabla[tmpIDX];
        *v9 = *v11;
        *v11 = v10;
        ++contadorBucleTabla;
        lenDatos = size_buf_datos1;
    }
    v12 = 0;
    contadorTablaa = 0;
    for ( j = -nIteraciones; j < lenDestino; *(_BYTE *) (j + buf_destino) ^= &tabla[(unsigned __int8)(v16 + *v15)] )
    {
        v14 = contadorTablaa + 1;
        contadorTablaa = v14;
        v15 = &tabla[v14];
        v12 += *v15;
        v16 = *v15;
        v17 = &tabla[v12];
        *v15 = *v17;
        *v17 = v16;
        j += j < 0 ? 1 : 0;
    }
}
ms_exc.registration.TryLevel = -1;
cookie(v23);
}
void __thiscall GeneraStringAleatoria(void *this, int a2)
{
    unsigned __int64 datos; // [sp+Ch] [bp-68h]@1

```

```

void *v3; // [sp+14h] [bp-60h]@1
_BYTE buf_destino[64]; // [sp+18h] [bp-5Ch]@1
__int16 v5; // [sp+55h] [bp-1Fh]@1
char v6; // [sp+57h] [bp-1Dh]@1
void *v7; // [sp+58h] [bp-1Ch]@1
CPPEH_RECORD ms_exc; // [sp+5Ch] [bp-18h]@1

v7 = (void *)cookieDword;
v3 = this;
ms_exc.registration.TryLevel = 0;
buf_destino[0] = 0;
memset(&buf_destino[1], 0, 0x3Cu);
v5 = 0;
v6 = 0;
datos = __rdtsc();
generaHASH((int)&datos, 8, (int)buf_destino, 64, 4096);
decodeString1(a2, buf_destino, 64);
ms_exc.registration.TryLevel = -1;
cookie(v7);
}
char * __thiscall ObtenNombreArchivoRandomSystem32(char *this)
{
    char *v1; // edi@1
    char v2; // al@2
    int v3; // ebp@3
    unsigned int v4; // ebx@3
    unsigned int v5; // edi@4
    HANDLE v6; // esi@4
    char *v7; // eax@5
    signed int v8; // kr00_4@7
    time_t v9; // esi@16
    unsigned int v10; // esi@16
    char *result; // eax@18
    char *v12; // edi@19
    signed int v13; // [sp+10h] [bp-250h]@3
    char *v14; // [sp+14h] [bp-24Ch]@1
    char v15; // [sp+18h] [bp-248h]@4
    char v16; // [sp+44h] [bp-21Ch]@5
    char v17; // [sp+157h] [bp-109h]@1
    CHAR Buffer; // [sp+158h] [bp-108h]@1
    int v19; // [sp+25Ch] [bp-4h]@1

    v19 = cookieDword;
    v14 = this;
    GetSystemDirectoryA(&Buffer, 0x104u);
    v1 = &v17;
    do
        v2 = (v1++)[1];
    while ( v2 );
    *(_DWORD *)v1 = 707668572;
    v3 = 0;
    v1[4] = 0;
    v4 = 0;

```

```

v13 = 1;
while ( 1 )
{
    v5 = 0;
    v6 = FindFirstFileA(&Buffer, (LPWIN32_FIND_DATA)&v15);
    if ( v6 != (HANDLE)-1 )
        break;
LABEL_14:
    if ( v13 == 1 )
    {
        if ( v5 < 0xA )
            goto LABEL_18;
        v9 = time(0);
        v10 = -1160008259 * (GetTickCount() + v9);
        v3 = v10 % v5;
        v4 = (v10 >> 10) % 0x24;
    }
    if ( (unsigned int)++v13 > 2 )
    {
        LABEL_18:
            GeneraStringAleatoria(v14, 8);
            return v14;
        }
    }
    while ( 1 )
    {
        v7 = strchr(&v16, '.');
        if ( v7 )
            *v7 = 0;
        v8 = strlen(&v16);
        if ( v8 < 4 || v8 >= 10 )
            goto LABEL_12;
        if ( v13 == 2 && v5 == v3 )
            break;
        ++v5;
    LABEL_12:
        if ( !FindNextFileA(v6, (LPWIN32_FIND_DATA)&v15) )
        {
            FindClose(v6);
            goto LABEL_14;
        }
    }
    v12 = strcpy(v14, &v16);
    if ( v4 >= 0xA )
    {
        v12[v8] = v4 + (v12[v8 - 1] > 90 ? 97 : 65) - 10;
        v12[v8 + 1] = 0;
        result = v12;
    }
    else
    {
        v12[v8] = v4 + 48;
        v12[v8 + 1] = 0;
    }
}

```

```

    result = v12;
}
return result;
}
unsigned int __fastcall checksum(_BYTE *a1, int a2)
{
    unsigned int v2; // eax@1
    _BYTE *v3; // esi@1
    int v4; // edi@2
    unsigned int v5; // edx@3
    char v6; // cl@3
    unsigned int v7; // eax@3
    unsigned int v8; // eax@3
    unsigned int v9; // eax@3
    unsigned int v10; // eax@3
    unsigned int v11; // eax@3
    unsigned int v12; // eax@3
    unsigned int v13; // eax@3

    v2 = -1;
    v3 = a1;
    if ( a2 )
    {
        v4 = a2;
        do
        {
            v5 = *v3;
            v6 = (v2 ^ *v3++) & 1;
            v7 = (v6 != 0 ? 0xEDB88320 : 0) ^ (v2 >> 1);
            v5 >>= 1;
            v8 = (((unsigned __int8)v7 ^ (unsigned __int8)v5) & 1) != 0 ? 0xEDB88320 : 0 ^ (v7 >> 1);
            v5 >>= 1;
            v9 = (((unsigned __int8)v8 ^ (unsigned __int8)v5) & 1) != 0 ? 0xEDB88320 : 0 ^ (v8 >> 1);
            v5 >>= 1;
            v10 = (((unsigned __int8)v9 ^ (unsigned __int8)v5) & 1) != 0 ? 0xEDB88320 : 0 ^ (v9 >> 1);
            v5 >>= 1;
            v11 = (((unsigned __int8)v10 ^ (unsigned __int8)v5) & 1) != 0 ? 0xEDB88320 : 0 ^ (v10 >> 1);
            v5 >>= 1;
            v12 = (((unsigned __int8)v11 ^ (unsigned __int8)v5) & 1) != 0 ? 0xEDB88320 : 0 ^ (v11 >> 1);
            v5 >>= 1;
            v13 = (((unsigned __int8)v12 ^ (unsigned __int8)v5) & 1) != 0 ? 0xEDB88320 : 0 ^ (v12 >> 1);
            v2 = (((unsigned __int8)v13 ^ (unsigned __int8)(v5 >> 1)) & 1) != 0 ? 0xEDB88320 : 0 ^ (v13 >> 1);
            --v4;
        }
        while ( v4 );
    }
    return ~v2;
}

```

10. ARCHIVOS DE CONFIGURACION

10.1 Archivo de configuración "dll"

```
"1100","10","1200"
"1100","11","300"
"1100","12","900"
"1100","13","172800"
"1100","14","30"
"1100","15","10"
"1500","10","12"
"1500","100","1"
"1500","101","xklmcomp.com|globalnetscan.com"
"1500","102","/feed.php?%s"
"1500","103","*yimg.*|*ivwbox.*|*atdmt.*|*img.youtube.*|*adbureau.net|*scorecardresearch.co
m|*google-analytics.com|66.232.11?.*|66.232.12?.*|*googlehosted.com|*gmodules.com|*g-
mail.com|*gmail.com|*gmodule.com|*googlecode.com|*googleearth.com|*googleemail.com|*goo
glemail.com|*googletalk.com|*googleusercontent.com|*googlevideos.com|*mupads.*|*gstatic.*|*
abmr.*|*alexametrics.com"
"1500","104","/search\x5C?*q=*|google.*|q=|/search\x5C?*q=*|www.google.*|q=|/search[\x5C?;]
*p=*|*search.yahoo.*|p=|/web\x5C?*q=*|*ask.com|q=|/search\x5C?*q=*|bing.*|q=|/search\x5C
?*q=*|www.bing.*|q=|/aol/search\x5C?*q=*|search.aol.com|q=|/search/results.php\x5C?*q=*|se
arch.icq.com|q=|/url\x5C?*q=*|google.*|q=|/url\x5C?*q=*|www.google.*|q=|/yhs/search[\x5C?;]
*q=*|*search.yahoo.*|q=|/redirector/sredir\x5C?*query=*|*search.aol.com|query=|/aol/search\x5
C?*query=*|*search.aol.com|query=|/\x5C?ver*q=*|*search.toolbars.alexa.com|q="
"1500","105","*google.*|/search\x5C?*q=*|*google.*|q=|*google.*|url\x5C?*q=*|*google.*|q=|*g
oogle.*|acl\x5C?*q=*|*google.*|q=|*search.yahoo.*|search[\x5C?;]*p=*|*yahoo.*|p=|*ask.com/
web\x5C?*q=*|*ask.com|q=|*bing.*|search\x5C?*q=*|*bing.*|q=|*search.aol.com/aol/search\x5C
?*q=*|*aol.com|q=|*search.icq.com/search/results.php\x5C?*q=*|*icq.com|q=|*search.icq.com/
search/results.php\x5C?*q=*|*aol.com|q=|*search.yahoo.*|yhs/search[\x5C?;]*q=*|*yahoo.*|q=
|*search.aol.com/aol/search\x5C?*query=*|*search.aol.com|query=|*search.toolbars.alexa.com/\x
5C?ver*q=*|*search.toolbars.alexa.com|q="
"1500","106","image/*|/*script*|text/css"
"1500","107","1"
"1500","108","www.google.com"
"1500","109","/intl/en/options/"
"1500","110","%s&%pin1%&%uid%&%pin2%&v=%pgn_ver%"
"1500","111","2"
"1500","112","4"
"1500","113","ask.com|bing|facebook|gmail|google|hotmail|msn|myspace|twitter|yahoo|youtub
e|craigslist|aol.com|ebay|wikipedia"
"1500","114","novotelcor.net|intuitionsearch.net"
"1500","115","/%s"
"1500","116","1"
"1500","117","1"
"1500","118","http://msdn.microsoft.com/en-us/aa570318.aspx"
"1500","119","604800"
"1500","120","2"
"1500","121","http://www.google.com/|http://www.ask.com/"
"1500","122","600"
"1500","123","*google.*|/s\x5C?*|*|204 No Content"
"1500","124","0"
"1500","125","http://www.alextraffic.com/in.cgi?12"
```

```
"1500","126","*/link.php?id=*/xxx\x5C?p=*/a2/out.cgi*/abrindo.php*/at/out.cgi*/at
3/out.cgi*/atx/out.cgi*/cgi-bin/g\x5C?*/cgi-bin/lpt/o\x5C?*/cgi-bin/o.cgi*/cgi-
bin/out.cgi?url=*/cgi-
bin/tm3/*}/cj_out.php*/cju/out.php*/ct/cx.php*/delivery/ck.php\x5C?*/ecj/out.cgi*/e
pt/out.php*/fcj/out.php*/ftt/o.php*/gal.cgi\x5C?*/gal.php\x5C?*/go.php*Id=*/lpt/lpt
out.cgi*/lpt/lptouth.cgi*/newcj/out.fcgi*/newcj/out.php*/o.php*Id=*/out.php*Id=*/o
ut.php*u=*/out.php?url=*/out.php*urls=*/outss.php*/r/out.php*/rb4/cout.cgi*/sc/o
ut.php*/scj/out.cgi*/sloth_out.php*/sr/out.php*/st/st.php*/streamrotator/out.php*/
sun/c.cgi*/tbase.php\x5C?*/tgp/o.php*/thumb.php*/tp/out.php*/trade.php*Id=*/tt-
out.php*/vanilla/process.php*/Id=*/go.php*/Id=*/o.php*/Id=*/out.php*/Id=*/trade.php*/
cgi-
bin/ucj/c.cgi*/chokertraffic.com/resell/*go.trafficshop.com/*id=*/link.php*/trafficholder.c
om/in/in.php*/tsprotraffic.com/in/*u=*/out.php*/url=*/cgi-
bin/out.cgi*/url=*/out.php*/urls=*/out.php*"
"1500","127","900"
"1500","200","0"
"1500","201",""
"1500","202",""
"1500","300","3600"
"1500","301",""
"1500","302","/cgi-bin/rokfeller2.cgi?n="
"1500","303","/cgi-bin/rokfeller3.cgi?v=%stat_ver%"
"1500","400","0"
"1500","401",""
"1500","402",""
"1500","403","0"
"1500","404",""
"1500","405",""
"1500","406",""
"1500","101000","1"
"1500","101001","xklmcomp.com|globalnetscan.com"
"1500","102000","1"
"1500","102001","/feed.php?%s"
"1500","110000","1"
"1500","110001","%s&%pin1%&%uid%&%pin2%&v=%pgn_ver%"
"1500","114000","1"
"1500","114001","novotelcor.net|intuitionsearch.net"
"1500","115000","1"
"1500","115001","/%s"
"1500","128000","1"
"1500","128001","100"
"1501","10","<default>"
"2000","10","3"
"2000","11",""
"2000","12","/cgi-bin/rokfeller3.cgi?v=%stat_ver%"
"2000","100","http://www.chokertraffic.org/tds/main|http://www.trafficholder.org/vtds/main|http://www.brokertraffic.net/in/main|http://www.alextraffic.com/out/main"
"2000","101","http://sttraffic.com/"
"2000","102","*.flw|*.fla|*.pdf|*.jar|*.war|*.swf|*.exe"
"2000","103","4tube.com|bigtube.com|deviantclip.com|drtuber.com|empflix.com|foxytube.com|h
ardsextube.com|heavy.com|keezmovies.com|livejasmin.com|mofosex.com|moviegator.com|pornh
ost.com|pornhub.com|pornotube.com|pornoxo.com|porntelecast.com|porntown.com|redtube.co
m|shufuni.com|slutload.com|tnaflx.com|tube8.com|xhamster.com|xvideos.com|youhot.com|youj
```

```
izz.com|youporn.com|yporn.com"  
"2000","104","86400"  
"2000","105","1"  
"2000","106","300"  
"2000","107","40"  
"2000","108","20"  
"2000","109","0"  
"2000","110","30"  
"2000","111","180"  
"2000","112","2"  
"2000","113","2"  
"2000","114","0"  
"2000","115","5"  
"2000","116","10"  
"2000","117","3"  
"2000","118","0"  
"2000","119","3"  
"2000","120","0"  
"2000","121","explorer.exe"  
"2000","122","12"
```

10.2 Archivo de Dominios "dll"

```
abccornet.com,avengoinc.com,gtoolbar.net
```

11. REFERENCIAS

[1] How Big is Big? Some Botnet Statics - Abuse.ch

<https://www.abuse.ch/?p=3294>

[2] Ponmocup, lots changed, but not all - c-apt-ure.blogspot.com.es

<http://c-apt-ure.blogspot.com.es/2012/03/ponmocup-lots-changed-but-not-all.html>

12. ANEXOS

ANEXO I – REGLAS DE DETECCIÓN

REGLA SNORT

```

alert udp any any -> any 53 (content:"montyinc|03|net"; msg:"Trojan Ponmocup
Domain Request detected");

alert tcp any any -> any 80 (content:"GET";content:"/html/license_";content:"
Mozilla/5.0 |28|Windows|3B| U|3B| MSIE 8.0|3B| Windows NT 6.0|3B| en-US|29|";
msg:"Ponmocup GET detected.");

alert udp any any -> any 53 (content:" imagehut4|02|cn"; msg:"Trojan Ponmocup
Downloader Domain Request detected");

```

REGLA YARA

```

import "pe"
rule Trj_Ponmocup {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Ponmocup Installer"

    strings:
        $mz = { 4d 5a }
        $pac = { 48 8f bb 54 5f 3e 4f 4e }
        $unp = { 8b b8 7c 1f 46 00 33 c8 }

    condition:
        ($mz at 0) and ($pac at 0x61f7c) and ($unp at 0x29f0)
}

rule Trj_Ponmocup_Downloader {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Ponmocup Downloader"

    strings:
        $mz = { 4d 5a }
        $vb5 = "VB5" fullword ascii
        $tpb = "www.thepiratebay.org" fullword wide
        $ua = "Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.2;
sv1)" fullword wide

    condition:
        ($mz at 0) and ($vb5) and ($tpb) and ($ua)
}

```

```
rule Trj_Ponmocup_dll {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Ponmocup Bot DLL"

    strings:
        $mz = { 4d 5a }
        $pck = { 00 81 23 00 33 3E 00 00 3B F4 56 00 00 00 7D 00 }
        $upk = { 68 F4 14 00 10 A1 6C C0 02 10 FF D0 59 59 E9 7A }

    condition:
        ($mz at 0) and ($pck at 0x8a50) and ($upk at 0x61f)
}
```

IOC

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="a209da74-723c-46af-ad88-
abfd39be1f67" last-modified="2015-12-14T13:21:32"
xmlns="http://schemas.mandiant.com/2010/ioc">
    <short_description>Ponmocup</short_description>
    <description>IOCs para detectar:
    -Dropper
    -Registry keys
    -Network Traffic
    - Dropper
    - MD5
    - Registry keys
    - Snort </description>
    <authored_by>CCN-CERT</authored_by>
    <authored_date>2015-12-09T16:15:36</authored_date>
    <links />
    <definition>
        <Indicator operator="OR" id="bc1ebe24-d0c9-4a76-afa0-f8159d7c2b25">
            <IndicatorItem id="cac6c86b-278e-4f53-bc47-341743418ef9"
condition="is">
                <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
                <Content type="md5">8e105ca9ef1571eec69a181efc32138a</Content>
            </IndicatorItem>
            <Indicator operator="OR" id="c2183c21-e78b-450c-85e6-6924a677caca">
                <IndicatorItem id="ac5e1f3c-d152-4520-8adc-e6cd560eb540"
condition="contains">
                    <Context document="RegistryItem" search="RegistryItem/KeyPath">
```

```

type="mir" />
    <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\1</Content>
    </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="b8e31ed9-9735-43c0-916f-75446b207523">
    <IndicatorItem          id="bf79aca4-28d9-48ef-8d35-6c8b1f2a0ba7"
condition="contains">
        <Context    document="RegistryItem"    search="RegistryItem/KeyPath"
type="mir" />
        <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\2</Content>
        </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="c5dce7ec-d448-4a3b-ad9e-0fd072dac9fb">
        <IndicatorItem          id="0b68bc0b-f11d-4561-aeb2-2dd21b84c1d8"
condition="contains">
        <Context    document="RegistryItem"    search="RegistryItem/KeyPath"
type="mir" />
        <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\3</Content>
        </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="4c80149c-560a-40a0-8ba0-1b08bceafd83">
        <IndicatorItem          id="e2966808-3ad5-4290-bae8-00267ca968f2"
condition="contains">
        <Context    document="RegistryItem"    search="RegistryItem/KeyPath"
type="mir" />
        <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\4</Content>
        </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="343fe92a-a631-4f3e-a5ef-73de7fcac3a0">
        <IndicatorItem          id="278b2e49-bd9d-4c34-9750-b0571502c25b"
condition="contains">
        <Context    document="RegistryItem"    search="RegistryItem/KeyPath"
type="mir" />
        <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\5</Content>
        </IndicatorItem>
    </Indicator>

```

```

<Indicator operator="OR" id="bd30e400-333c-4391-8995-19b59a13f4b6">
  <IndicatorItem
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\6</Content>
  </IndicatorItem>
</Indicator>
  <Indicator operator="OR" id="9a98e112-4efa-4399-b7cd-a5fff433dcca">
    <IndicatorItem
condition="contains">
      <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
      <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\7</Content>
    </IndicatorItem>
  </Indicator>
  <Indicator operator="OR" id="a1a29caf-f500-4ee8-8820-50749ace3726">
    <IndicatorItem
condition="contains">
      <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
      <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\8</Content>
    </IndicatorItem>
  </Indicator>
  <Indicator operator="OR" id="d6d06aaf-a070-4436-a727-728844d2d55d">
    <IndicatorItem
condition="contains">
      <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
      <Content
type="string">HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\9</Content>
    </IndicatorItem>
  </Indicator>
  <Indicator operator="OR" id="b90546fb-fff1-4582-b919-ec87216c6a6b">
    <IndicatorItem
condition="contains">
      <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
      <Content type="string">HKCU\System\CurrentControlSet\1</Content>

```

```

</IndicatorItem>
</Indicator>
<Indicator operator="OR" id="07fd9b52-b80c-4525-abd9-82a70cdd0e96">
  <IndicatorItem id="3bc75e5a-b4a0-4f68-89e6-49b218c57b6e"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKCU\System\CurrentControlSet\2</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="5c4456a8-3355-458c-9721-f9ac69bb40ca">
  <IndicatorItem id="14d31b59-30b1-4ca8-8300-048cfd618093"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKCU\System\CurrentControlSet\3</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="2912a55d-4671-4a94-8720-5d43b2df3720">
  <IndicatorItem id="bd2e9430-79ca-4b01-b6c2-20df4533aa35"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKCU\System\CurrentControlSet\4</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="a7b484f4-cf7a-421e-9182-d48ca493e058">
  <IndicatorItem id="09802d27-360a-44b6-996a-4e44a13516ea"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKCU\System\CurrentControlSet\5</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="8b8a0853-6a40-477b-9298-a0af7cb63d4b">
  <IndicatorItem id="51f092c5-fbca-4c4d-ae3-949539031cb0"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKCU\System\CurrentControlSet\6</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="29800f4d-fa93-4681-aae8-36d6b219f045">
  <IndicatorItem id="8d2bba2d-9b1d-40d1-bfd8-f916282da730"

```

```

condition="contains">
  <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
  <Content type="string">HKCU\System\CurrentControlSet\7</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="19af0d97-4ab9-4737-ac28-8da0d1698f2f">
  <IndicatorItem id="0a9ad3c8-c472-45d1-91ca-79bb2604c12b"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKCU\System\CurrentControlSet\8</Content>
    </IndicatorItem>
  </Indicator>
  <Indicator operator="OR" id="12ddd90f-bc2b-438c-82eb-6f1f00964e50">
    <IndicatorItem id="011f9f16-9ba4-42e5-b348-a2b69269c91a"
condition="contains">
      <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
      <Content type="string">HKCU\System\CurrentControlSet\9</Content>
      </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="3f3200bd-e00b-4161-a663-7b18aa4a3d7d">
      <IndicatorItem id="107893d1-e2fb-40ac-80d4-6492f6e67662"
condition="contains">
        <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
        <Content
type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\1</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="0455227b-6867-4b9c-bd6e-af21bdad2450">
        <IndicatorItem id="d1d75f6b-b519-479e-a229-f4cc51b0a47e"
condition="contains">
          <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
          <Content
type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\2</Content>
          </IndicatorItem>
        </Indicator>
        <Indicator operator="OR" id="43ee8661-71c2-436c-b887-82cc9f12d55f">
          <IndicatorItem id="73bcc92b-24c8-417a-87c9-90189436f1bd"
condition="contains">

```

```

type="mir" />
  <Context document="RegistryItem" search="RegistryItem/KeyPath"
  type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
  Settings\3</Content>
    </IndicatorItem>
  </Indicator>
  <Indicator operator="OR" id="97bda1e9-a4e5-470f-b5d8-992a0929ec5e">
    <IndicatorItem id="8317fd34-74f9-4560-9954-57a78548f6b4"
    condition="contains">
      <Context document="RegistryItem" search="RegistryItem/KeyPath"
      type="mir" />
        <Content
        type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
        Settings\4</Content>
          </IndicatorItem>
        </Indicator>
        <Indicator operator="OR" id="4262b84b-288b-4973-94ac-bf8bcf134adf">
          <IndicatorItem id="89c99189-741e-415f-8b79-5287dc5928ba"
          condition="contains">
            <Context document="RegistryItem" search="RegistryItem/KeyPath"
            type="mir" />
              <Content
              type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
              Settings\5</Content>
                </IndicatorItem>
              </Indicator>
              <Indicator operator="OR" id="b30bf410-8a35-4b95-a309-59483431f868">
                <IndicatorItem id="e9dbccf8-20f7-4372-8b07-d49c8477389b"
                condition="contains">
                  <Context document="RegistryItem" search="RegistryItem/KeyPath"
                  type="mir" />
                    <Content
                    type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
                    Settings\6</Content>
                      </IndicatorItem>
                    </Indicator>
                    <Indicator operator="OR" id="4e1f7266-3aa6-41d1-8cff-a86eba6d847c">
                      <IndicatorItem id="14637258-02e1-4c22-a4ce-7f0ac4bc7c58"
                      condition="contains">
                        <Context document="RegistryItem" search="RegistryItem/KeyPath"
                        type="mir" />
                          <Content
                          type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
                          Settings\7</Content>
                            </IndicatorItem>
                          </Indicator>

```

```

<Indicator operator="OR" id="05f73715-2909-4584-8313-bc77f3c4c073">
  <IndicatorItem
    condition="contains"
    id="c94ff5ef-3271-4a9c-bc64-e4ae0f864aff"
    type="mir" />
    <Context document="RegistryItem" search="RegistryItem/KeyPath" />
    <Content
      type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
      Settings\8</Content>
    </IndicatorItem>
  </Indicator>
  <Indicator operator="OR" id="f6369a6e-c465-4a1c-9b3a-dad08c43dd46">
    <IndicatorItem
      condition="contains"
      id="b1aec9a5-f627-4ca9-9482-91a728132772"
      type="mir" />
      <Context document="RegistryItem" search="RegistryItem/KeyPath" />
      <Content
        type="string">HKLM\Software\Microsoft\Windows\CurrentVersion\Internet
        Settings\9</Content>
      </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="2538830d-5221-4d17-a6e3-351f71c8b823">
      <IndicatorItem
        condition="contains"
        id="a9d41017-353e-4301-8581-1af534b7f339"
        type="mir" />
        <Context document="RegistryItem" search="RegistryItem/KeyPath" />
        <Content type="string">HKLM\System\CurrentControlSet\1</Content>
      </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="adfad41a-5310-4b12-af49-6b8e4dfb4bd8">
      <IndicatorItem
        condition="contains"
        id="7b1442e6-45fa-4b79-917d-f66622df5385"
        type="mir" />
        <Context document="RegistryItem" search="RegistryItem/KeyPath" />
        <Content type="string">HKLM\System\CurrentControlSet\2</Content>
      </IndicatorItem>
    </Indicator>
    <Indicator operator="OR" id="856f6df3-2b1a-46b2-b7e6-ed3bf101a9ae">
      <IndicatorItem
        condition="contains"
        id="1209ba7b-ff4e-45cd-8d5e-2db91288b8a0"
        type="mir" />
        <Context document="RegistryItem" search="RegistryItem/KeyPath" />
        <Content type="string">HKLM\System\CurrentControlSet\3</Content>
      </IndicatorItem>
    </Indicator>
  </Indicator operator="OR" id="f449f045-78ef-429b-89b7-b16f761cf4ff">

```

```

<IndicatorItem id="c26f67bd-233d-4f57-99ba-66079cf4be77"
condition="contains">
  <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
  <Content type="string">HKLM\System\CurrentControlSet\4</Content>
</IndicatorItem>
</Indicator>
<Indicator operator="OR" id="4353cb74-c2a7-48e8-b4ff-9a2a6c55086e">
  <IndicatorItem id="1bd0ed48-0ae9-4f00-87cb-b951e15fac03"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKLM\System\CurrentControlSet\5</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="1774e577-3d30-4773-ac2d-e1d84a34fa07">
  <IndicatorItem id="c45cd815-0bb6-4ff1-987c-370ceb08200f"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKLM\System\CurrentControlSet\6</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="05a123ca-76fe-435a-a2e9-ce885786fb54">
  <IndicatorItem id="5e6b66c4-376d-4591-af9b-240d8056c4d1"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKLM\System\CurrentControlSet\7</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="b1f367bd-4984-4a27-bbad-f66f47687543">
  <IndicatorItem id="9284c2e1-add8-4f20-86e5-09ef26215b67"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />
    <Content type="string">HKLM\System\CurrentControlSet\8</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="8318e310-5fc5-45f3-bf96-09f7e47e19ee">
  <IndicatorItem id="2a05a564-20c9-40b0-ba10-934867fdc31c"
condition="contains">
    <Context document="RegistryItem" search="RegistryItem/KeyPath"
type="mir" />

```

```

    <Content type="string">HKLM\System\CurrentControlSet\9</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="5677a87a-5de9-4071-b690-889588b86df4">
  <IndicatorItem          id="bc3784bb-1ee4-4a1e-9d7d-67c7e8330617"
condition="contains">
    <Context document="Snort" search="Snort/Snort" type="mir" />
    <Content type="string">alert udp any any -&gt; any 53
(content:"montyinc|03|net"; msg:"Trojan Ponmocup Domain Request detected";
sid:1000002; )
  </Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="578c0239-a08c-4b23-b2ba-841031685513">
  <IndicatorItem          id="3067df7c-dbb3-49e2-aaa8-035fb6079afc"
condition="contains">
    <Context document="Snort" search="Snort/Snort" type="mir" />
    <Content type="string">alert tcp any any -&gt; any 80
(content:"GET";content:"/html/license_";content:"Mozilla/5.0 |28|windows|3B|
U|3B| MSIE 8.0|3B| windows NT 6.0|3B| en-US|29|"; msg:"Ponmocup GET
detected."; sid:1000004; )</Content>
  </IndicatorItem>
</Indicator>
</Indicator>
</definition>
</ioc>

```