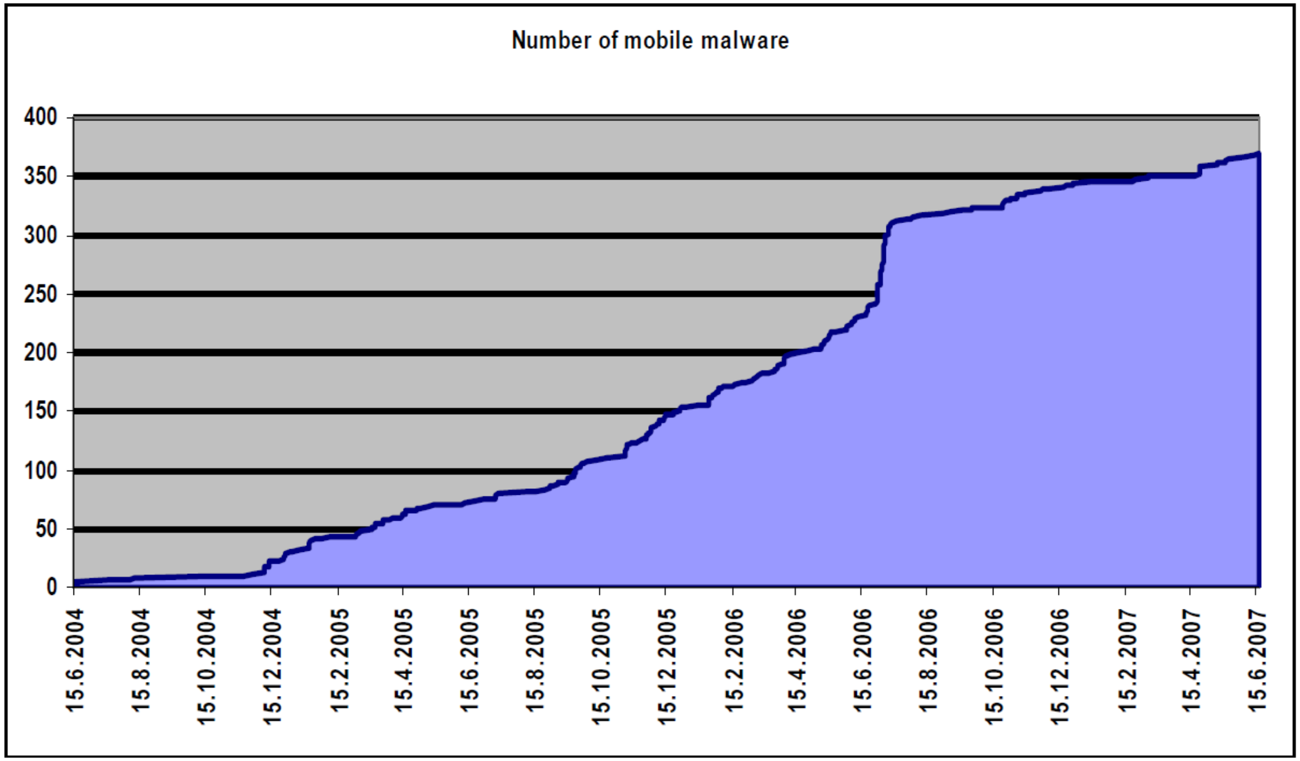
AUTOMATED MOBILE MALWARE CLASSIFICATION

zynamics GmbH

Status Quo: Mobile Malware

- The deluge of mobile malware that was predicted has not happened yet

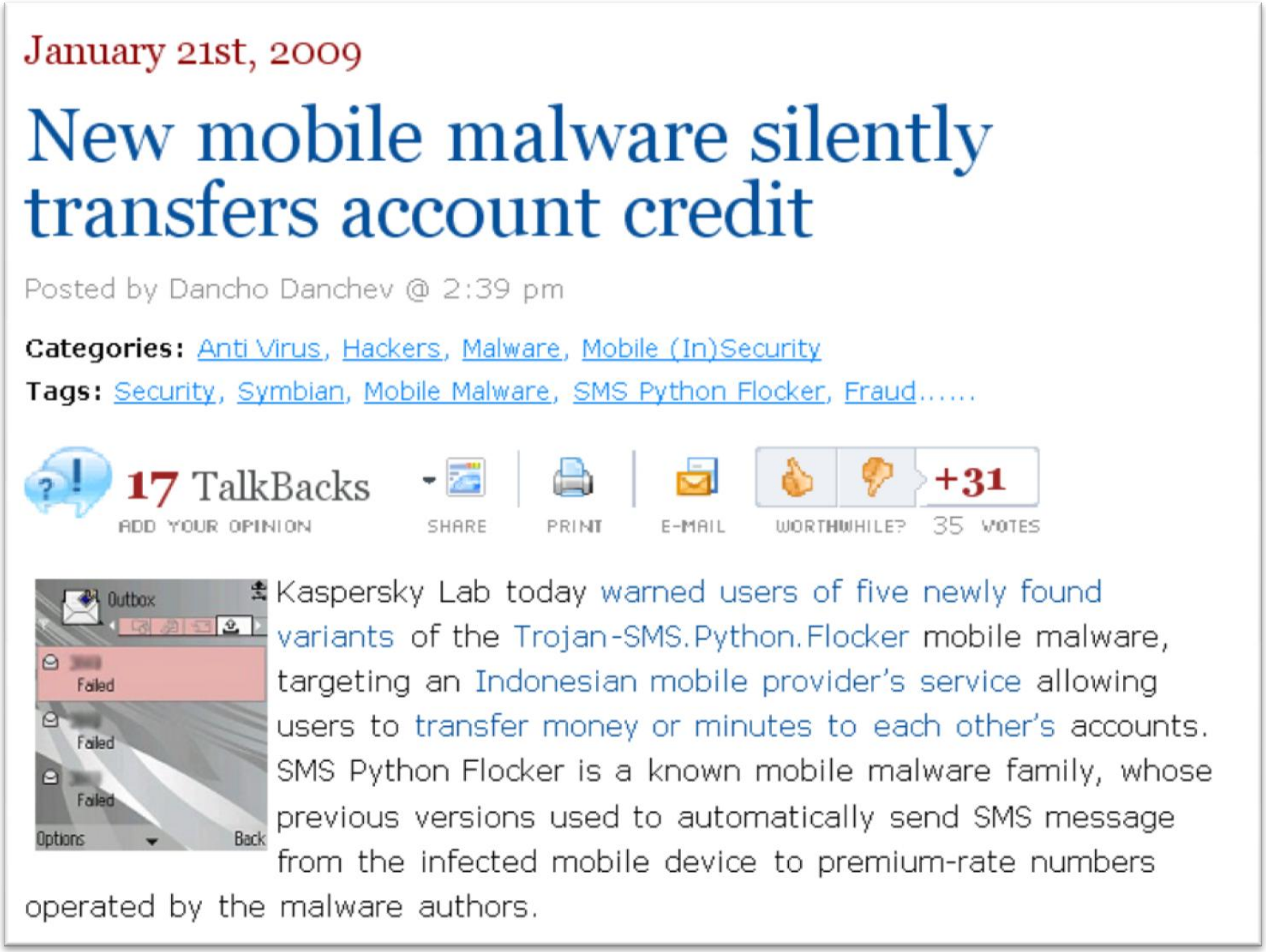


Data source: F-Secure

Status Quo: Mobile Malware

- This does not mean that mobile malware is not a threat
- More money moving through GSM means more incentive to build malware
- Result: There WERE and WILL be outbreaks

News Item



January 21st, 2009

New mobile malware silently transfers account credit

Posted by Dancho Danchev @ 2:39 pm

Categories: Anti Virus, Hackers, Malware, Mobile (In)Security

Tags: Security, Symbian, Mobile Malware, SMS Python Flocker, Fraud……

Kaspersky Lab today warned users of five newly found variants of the Trojan-SMS.Python.Flocker mobile malware, targeting an Indonesian mobile provider's service allowing users to transfer money or minutes to each other's accounts. SMS Python Flocker is a known mobile malware family, whose previous versions used to automatically send SMS message from the infected mobile device to premium-rate numbers operated by the malware authors.

Problem: Variants

- A lot of filtering can be done using MD5
  - But: Fraudsters learned to obfuscate
- Variants are easy to create
- In the Windows world:
  - 20k MD5-different variants of the same malware **each month**

Problem: Variants

- Ways to determine whether a file is a variant of a known malware are needed. Preferrably:
  - Fast
  - Cheap
  - Reliable
  - Easily adapted to future threats

Current approach

- Analysis is
  - Not done at all
  - Done manually by a security expert
  - Done in some ad-hoc automated fashion

Problem: Variants

- Manual approaches do not satisfy our requirements:

Fast:	No
Cheap:	No
Reliable:	Depends on the guy
Easily adaptable	Depends on the guy

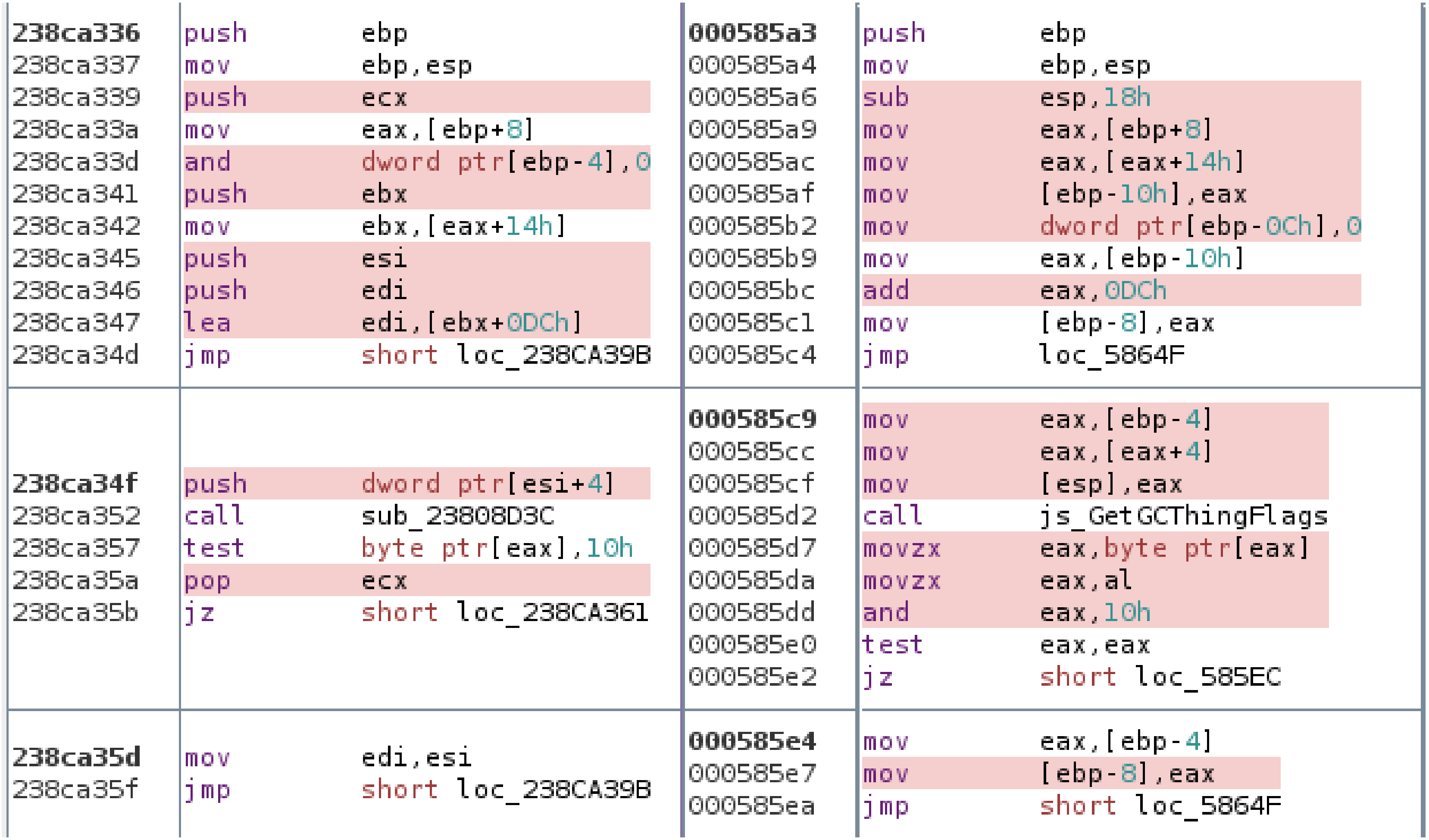
Program Comparison

- How would we check if a file is a variant ?
- Program comparison tools are needed
- Surprise: We have built some
  - In use in the ITSec and AV world since 2004
  - „Best Paper“ at SSTIC 2005
  - Germany‘s biggest privately funded research prize 2006
    - We beat Siemens and T-Systems

Program Comparison

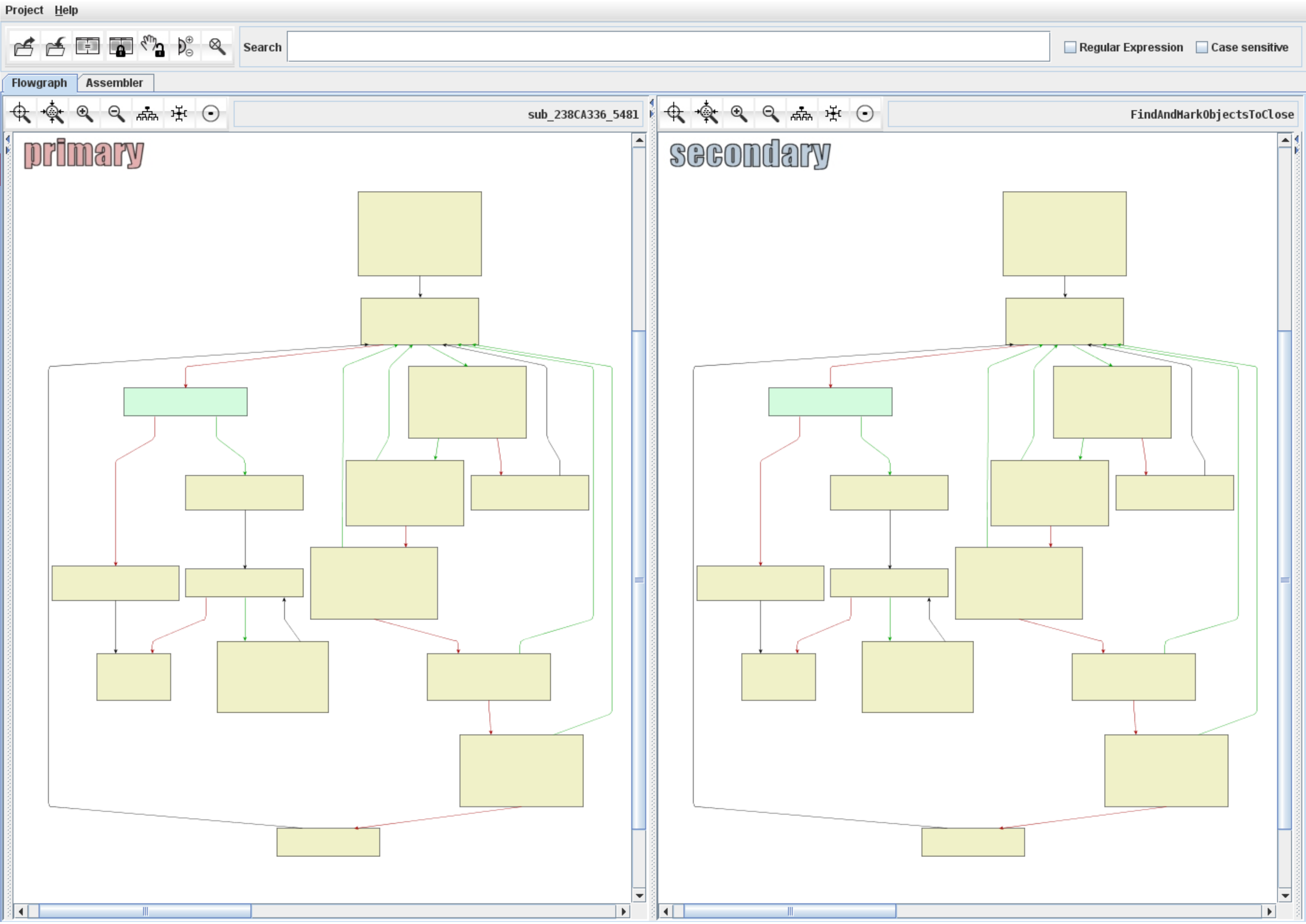
- Core principle: Comparison is structural
- Instructions may change a lot, the program structure only slightly
- Graphs are generated from the programs
- Comparison happens on these graphs

Status Quo: The Windows World



```
238ca336  push   ebp
238ca337  mov    ebp,esp
238ca339  push   ecx
238ca33a  mov    eax,[ebp+8]
238ca33d  and    dword ptr[ebp-4],0
238ca341  push   ebx
238ca342  mov    ebx,[eax+14h]
238ca345  push   esi
238ca346  push   edi
238ca347  lea    edi,[ebx+0DCh]
238ca34d  jmp    short loc_238CA39B

238ca34f  push   dword ptr[esi+4]
238ca352  call   sub_23808D3C
238ca357  test   byte ptr[eax],10h
238ca35a  pop    ecx
238ca35b  jz     short loc_238CA361

238ca35d  mov    edi,esi
238ca35f  jmp    short loc_238CA39B
```

```
000585a3  push   ebp
000585a4  mov    ebp,esp
000585a6  sub    esp,18h
000585a9  mov    eax,[ebp+8]
000585ac  mov    eax,[eax+14h]
000585af  mov    [ebp-10h],eax
000585b2  mov    dword ptr[ebp-0Ch],0
000585b9  mov    eax,[ebp-10h]
000585bc  add    eax,0DCh
000585c1  mov    [ebp-8],eax
000585c4  jmp    loc_5864F

000585c9  mov    eax,[ebp-4]
000585cc  mov    eax,[eax+4]
000585cf  mov    [esp],eax
000585d2  call   js_GetGCThingFlags
000585d7  movzx  eax,byte ptr[eax]
000585da  movzx  eax,al
000585dd  and    eax,10h
000585e0  test   eax,eax
000585e2  jz     short loc_585EC

000585e4  mov    eax,[ebp-4]
000585e7  mov    [ebp-8],eax
000585ea  jmp    short loc_5864F
```



□ Regular Expression □ Case sensitive

sub_238CA336_5481

FindAndMarkObjectsToClose

Program Comparison

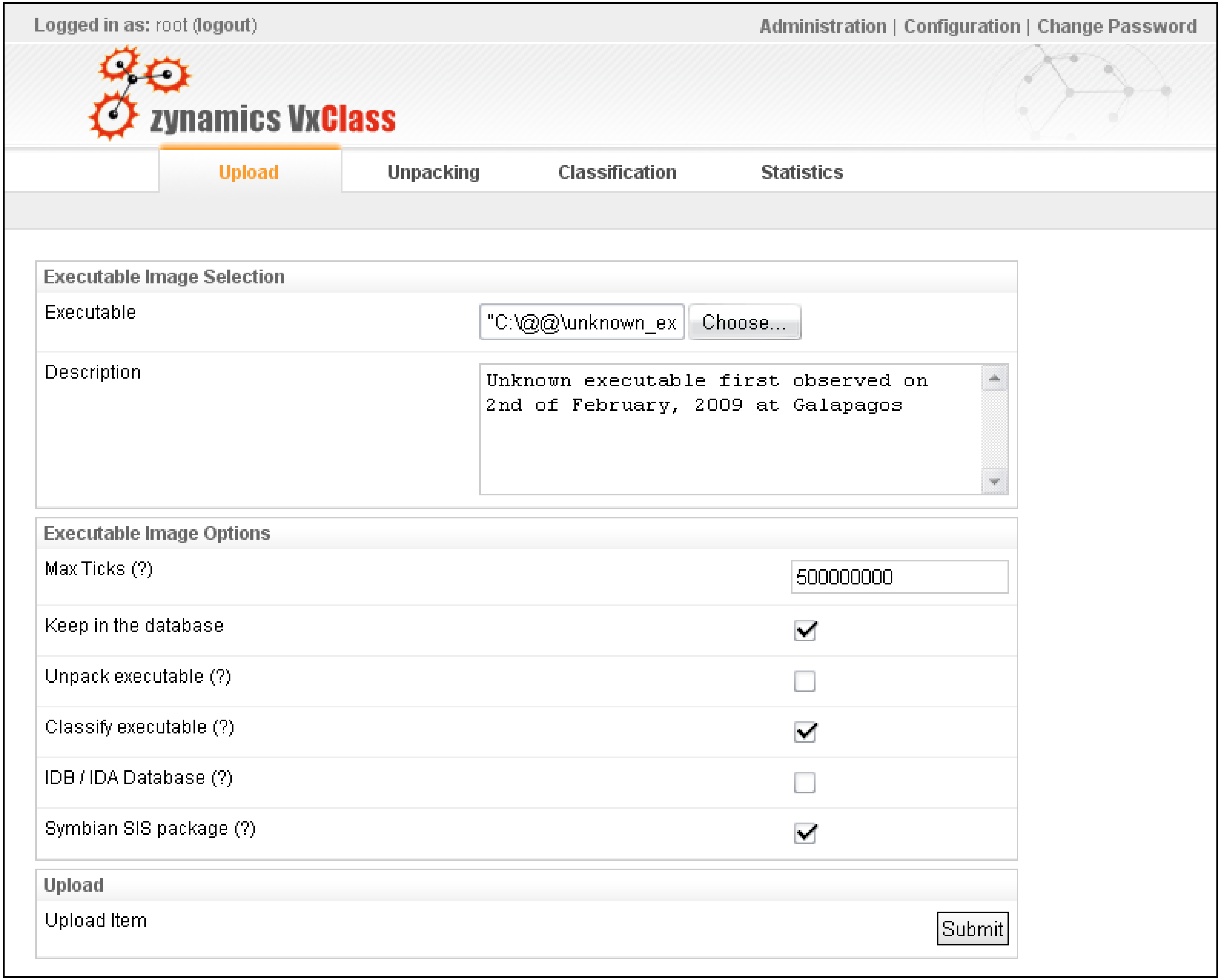
- Our comparison is strong because ...
  - The entire program is taken into consideration
  - Recompiling does not fool us
  - Stable parts are identified
  - Large changes do not matter much

VxClass for Mobile Malware

- VxClass compares executables
- A library of known malware is kept
- New executables can be checked if they are similar to existing malware
- Easy to use, Reliable, Cheap

Case Study

- Unknown executable is received
- MD5 does not match anything
- Is it a variant of an existing piece of malware ?



Logged in as: root (logout)
Administration | Configuration | Change Password
zynamics VxClass
Upload
Unpacking
Classification
Statistics

Executable Image Selection

Executable "C:\@@\unknown_ex Choose...

Description

Unknown executable first observed on 2nd of February, 2009 at Galapagos

Executable Image Options

Max Ticks (?) 500000000

Keep in the database ☑

Unpack executable (?) □

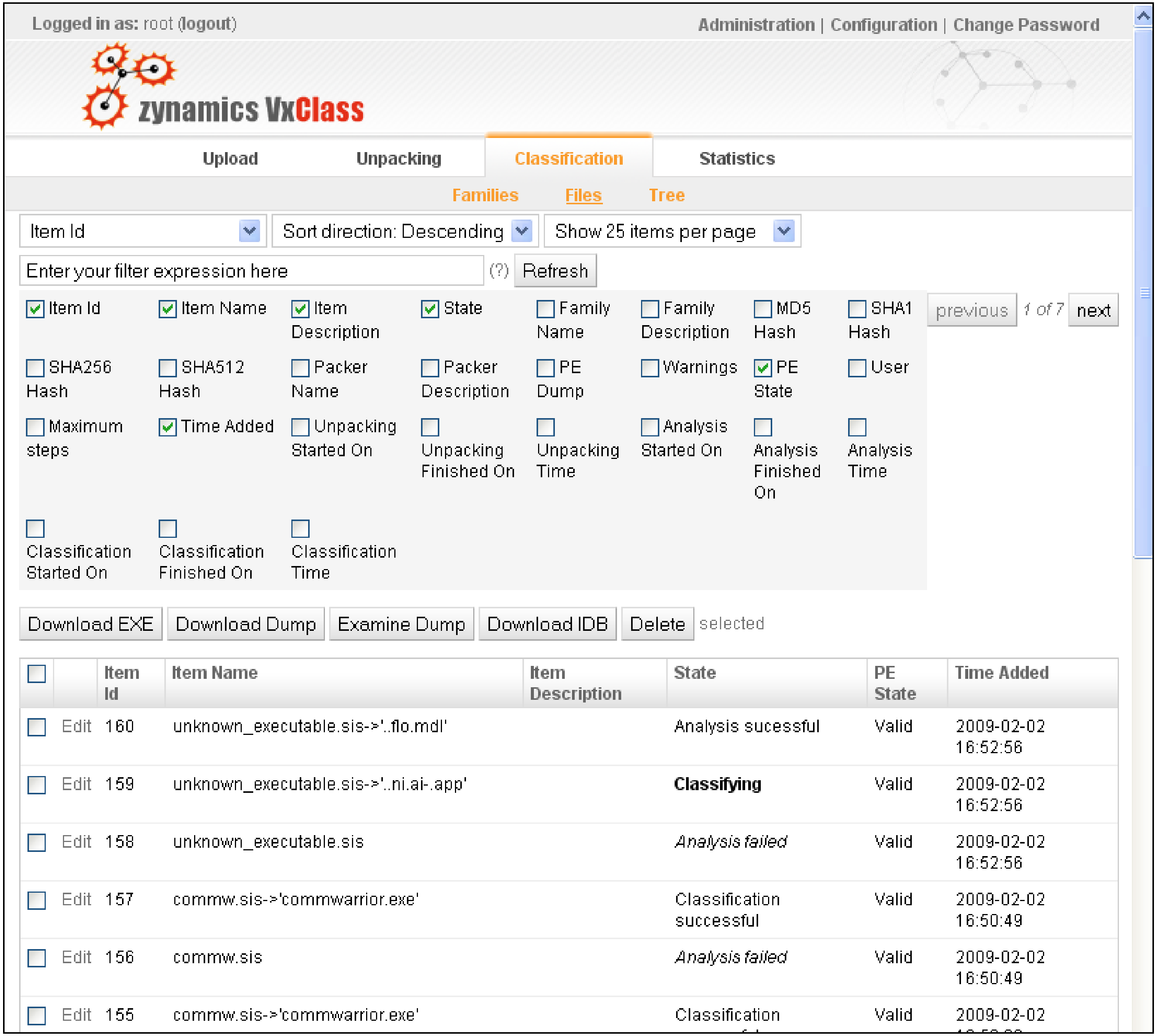
Classify executable (?) ☑

IDB / IDA Database (?) □

Symbian SIS package (?) ☑

Upload

Upload Item Submit



Item Id ▾ | Sort direction: Descending ▾ | Show 25 items per page ▾

Enter your filter expression here (?)

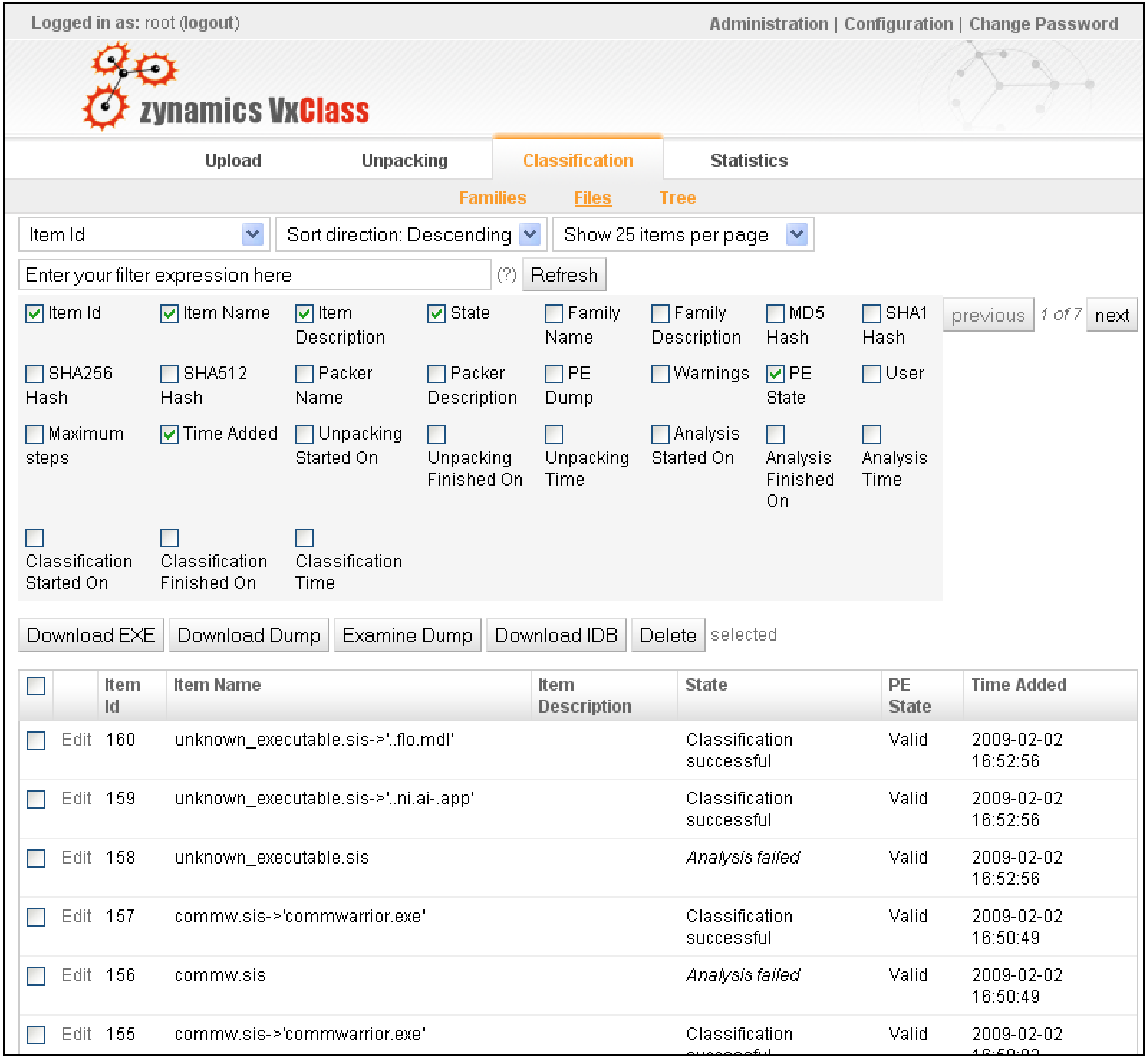
☑ Item Id ☑ Item Name ☑ Item Description ☑ State □ Family Name □ Family Description □ MD5 Hash □ SHA1 Hash

□ SHA256 Hash □ SHA512 Hash □ Packer Name □ Packer Description □ PE Dump □ Warnings ☑ PE State □ User

□ Maximum steps ☑ Time Added □ Unpacking Started On □ Unpacking Finished On □ Unpacking Time □ Analysis Started On □ Analysis Finished On □ Analysis Time

□ Classification Started On □ Classification Finished On □ Classification Time

□		Item Id	Item Name	Item Description	State	PE State	Time Added
□	Edit	160	unknown_executable.sis->'..flo.mdl'		Analysis sucessful	Valid	2009-02-02 16:52:56
□	Edit	159	unknown_executable.sis->'..ni.ai-.app'		**Classifying**	Valid	2009-02-02 16:52:56
□	Edit	158	unknown_executable.sis		*Analysis failed*	Valid	2009-02-02 16:52:56
□	Edit	157	commw.sis->'commwarrior.exe'		Classification successful	Valid	2009-02-02 16:50:49
□	Edit	156	commw.sis		*Analysis failed*	Valid	2009-02-02 16:50:49
□	Edit	155	commw.sis->'commwarrior.exe'		Classification	Valid	2009-02-02



Item Id | Sort direction: Descending | Show 25 items per page

Enter your filter expression here (?)

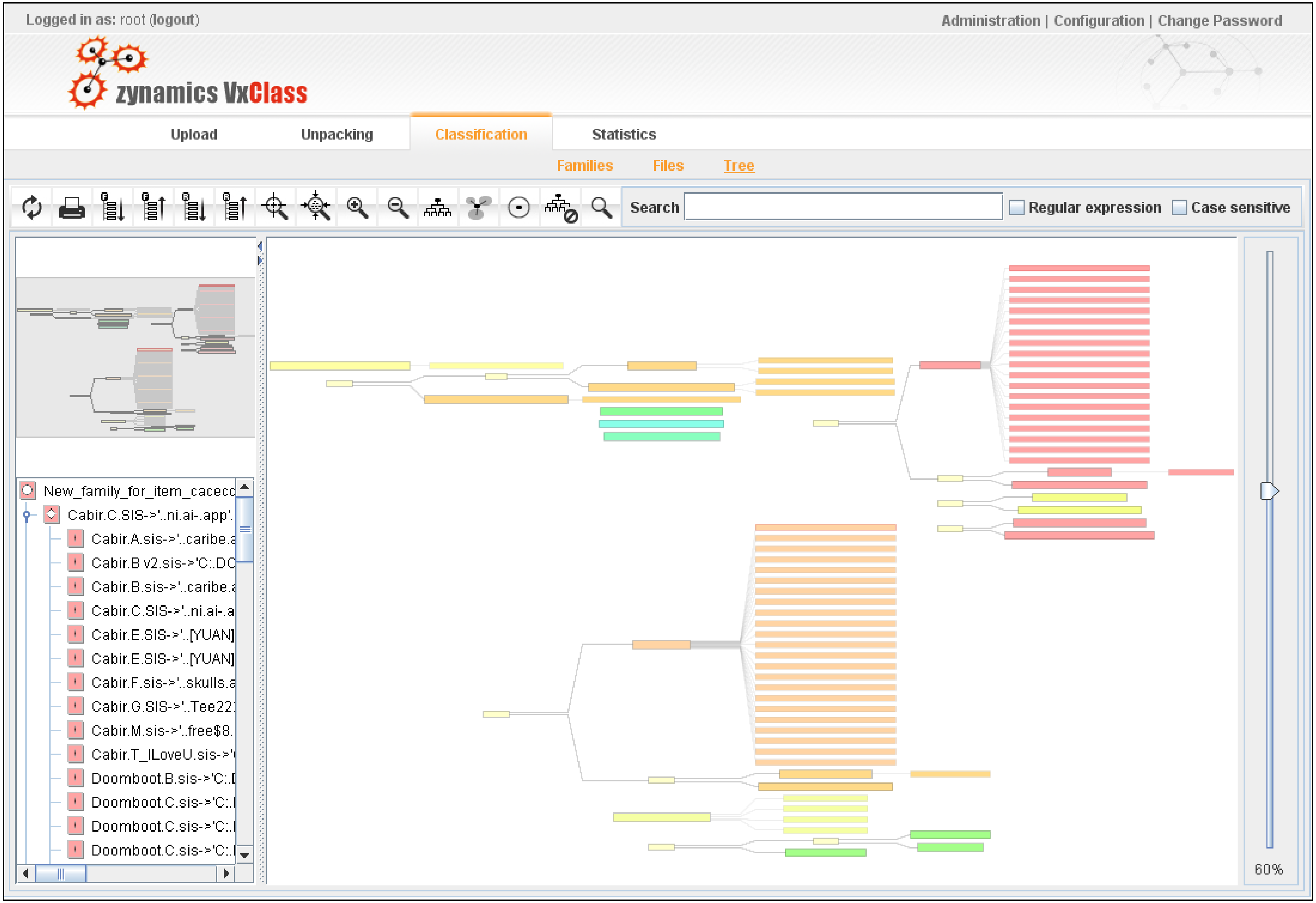
☑ Item Id ☑ Item Name ☑ Item Description ☑ State ☐ Family Name ☐ Family Description ☐ MD5 Hash ☐ SHA1 Hash

☐ SHA256 Hash ☐ SHA512 Hash ☐ Packer Name ☐ Packer Description ☐ PE Dump ☐ Warnings ☑ PE State ☐ User

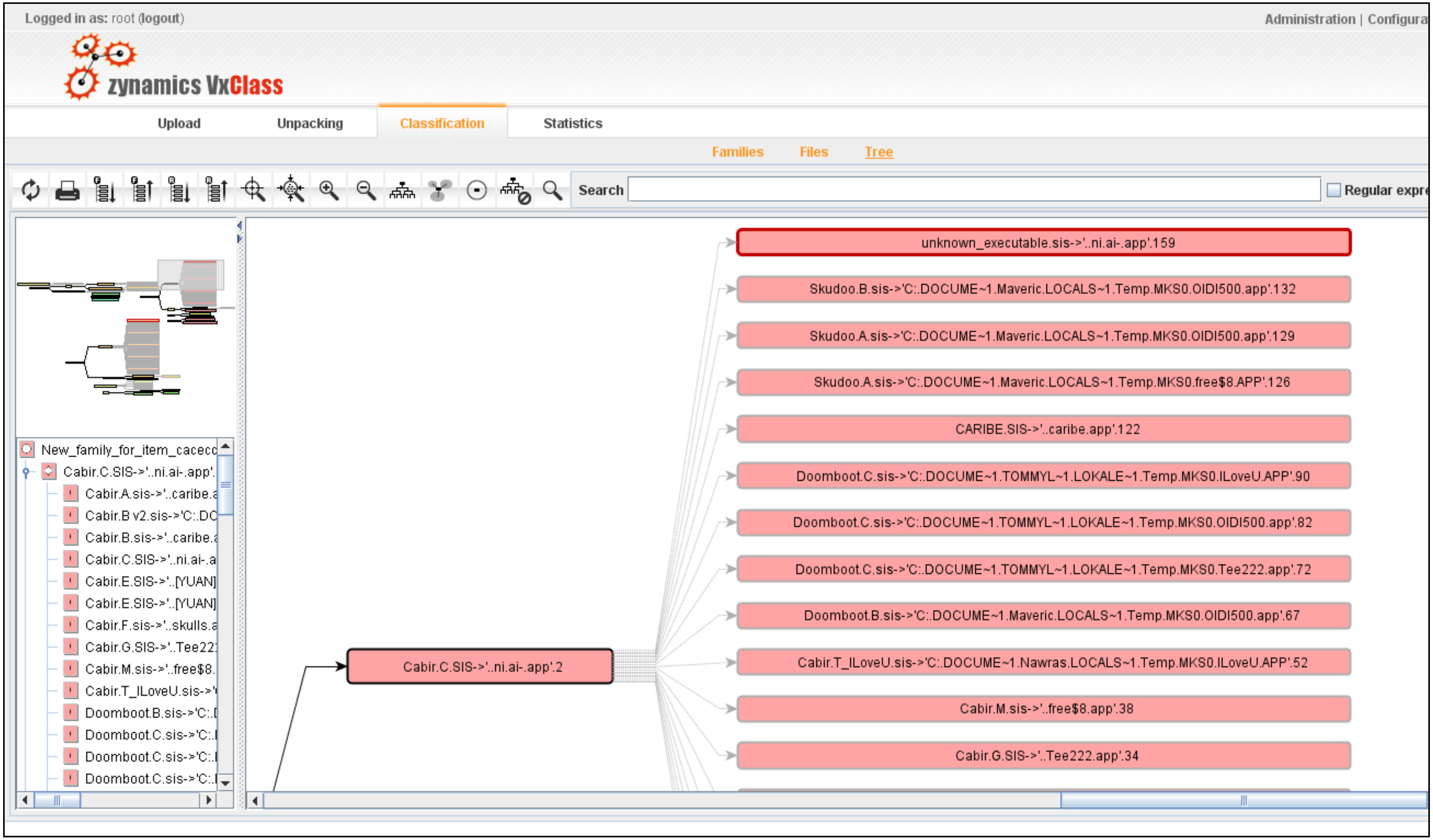
☐ Maximum steps ☑ Time Added ☐ Unpacking Started On ☐ Unpacking Finished On ☐ Unpacking Time ☐ Analysis Started On ☐ Analysis Finished On ☐ Analysis Time

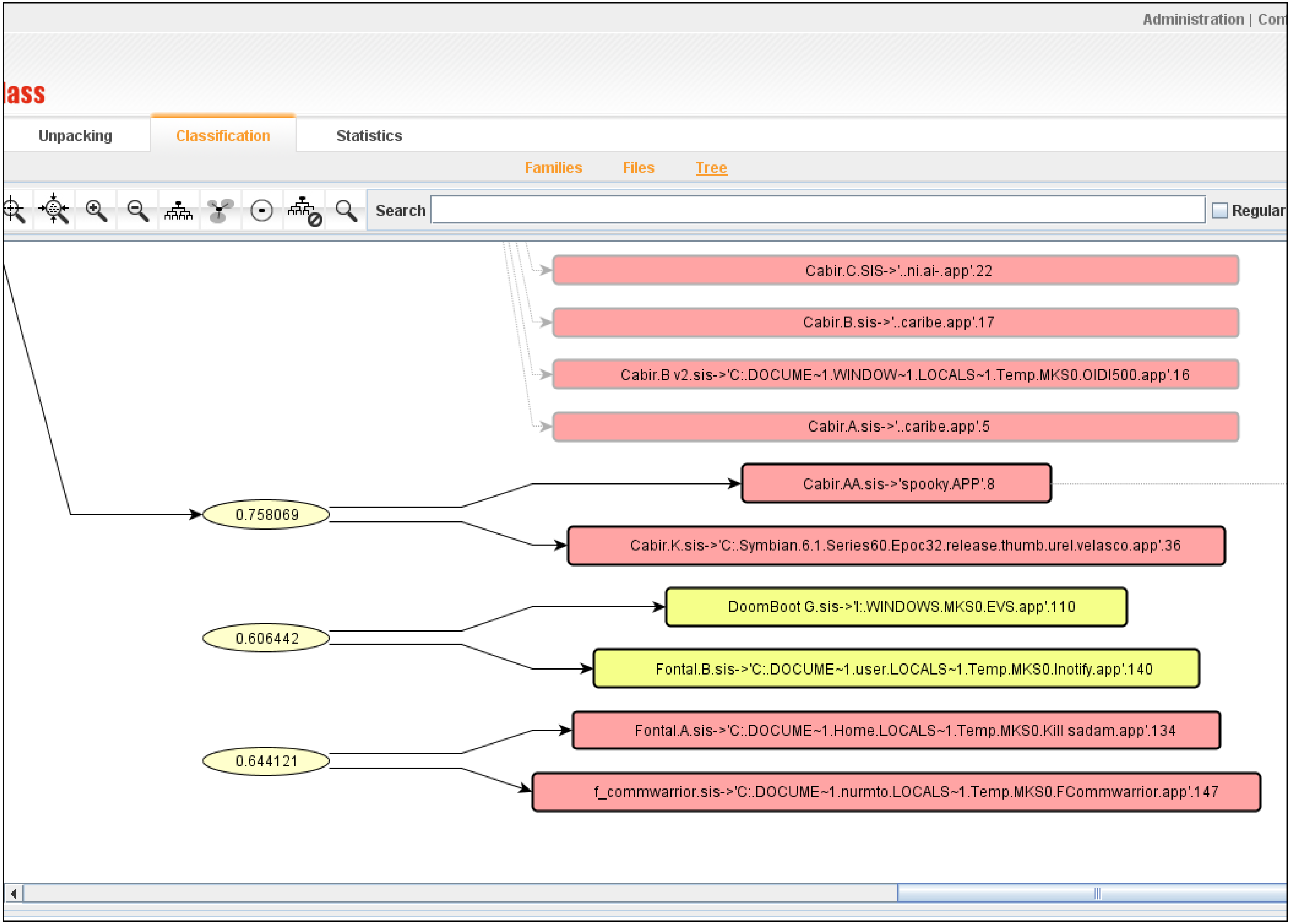
☐ Classification Started On ☐ Classification Finished On ☐ Classification Time

☐		Item Id	Item Name	Item Description	State	PE State	Time Added
☐	Edit	160	unknown_executable.sis->'..flo.mdl'		Classification successful	Valid	2009-02-02 16:52:56
☐	Edit	159	unknown_executable.sis->'..ni.ai-.app'		Classification successful	Valid	2009-02-02 16:52:56
☐	Edit	158	unknown_executable.sis		*Analysis failed*	Valid	2009-02-02 16:52:56
☐	Edit	157	commw.sis->'commwarrior.exe'		Classification successful	Valid	2009-02-02 16:50:49
☐	Edit	156	commw.sis		*Analysis failed*	Valid	2009-02-02 16:50:49
☐	Edit	155	commw.sis->'commwarrior.exe'		Classification	Valid	2009-02-02



New_family_for_item_cacecc
Cabir.C.SIS->'..ni.ai-.app'.
Cabir.A.sis->'..caribe.a
Cabir.B v2.sis->'C:.DC
Cabir.B.sis->'..caribe.a
Cabir.C.SIS->'..ni.ai-.a
Cabir.E.SIS->'..[YUAN]
Cabir.E.SIS->'..[YUAN]
Cabir.F.sis->'..skulls.a
Cabir.G.SIS->'..Tee22
Cabir.M.sis->'..free$8.
Cabir.T_ILoveU.sis->'
Doomboot.B.sis->'C:.[
Doomboot.C.sis->'C:.[
Doomboot.C.sis->'C:.[
Doomboot.C.sis->'C:.[


Logged in as: root (logout)
Administration | Configura
zynamics VxClass
Upload
Unpacking
Classification
Statistics
Families
Files
Tree
Search
Regular expre
New_family_for_item_cacecc
Cabir.C.SIS->'..ni.ai-.app'.
Cabir.A.sis->'..caribe.a
Cabir.B v2.sis->'C:.DC
Cabir.B.sis->'..caribe.a
Cabir.C.SIS->'..ni.ai-.a
Cabir.E.SIS->'..[YUAN]
Cabir.E.SIS->'..[YUAN]
Cabir.F.sis->'..skulls.a
Cabir.G.SIS->'..Tee22
Cabir.M.sis->'..free$8.
Cabir.T_ILoveU.sis->'
Doomboot.B.sis->'C:.I
Doomboot.C.sis->'C:.I
Doomboot.C.sis->'C:.I
Doomboot.C.sis->'C:.I
unknown_executable.sis->'..ni.ai-.app'.159
Skudoo.B.sis->'C:.DOCUME~1.Maveric.LOCALS~1.Temp.MKS0.OIDI500.app'.132
Skudoo.A.sis->'C:.DOCUME~1.Maveric.LOCALS~1.Temp.MKS0.OIDI500.app'.129
Skudoo.A.sis->'C:.DOCUME~1.Maveric.LOCALS~1.Temp.MKS0.free$8.APP'.126
CARIBE.SIS->'..caribe.app'.122
Doomboot.C.sis->'C:.DOCUME~1.TOMMYL~1.LOKALE~1.Temp.MKS0.ILoveU.APP'.90
Doomboot.C.sis->'C:.DOCUME~1.TOMMYL~1.LOKALE~1.Temp.MKS0.OIDI500.app'.82
Doomboot.C.sis->'C:.DOCUME~1.TOMMYL~1.LOKALE~1.Temp.MKS0.Tee222.app'.72
Doomboot.B.sis->'C:.DOCUME~1.Maveric.LOCALS~1.Temp.MKS0.OIDI500.app'.67
Cabir.C.SIS->'..ni.ai-.app'.2
Cabir.T_ILoveU.sis->'C:.DOCUME~1.Nawras.LOCALS~1.Temp.MKS0.ILoveU.APP'.52
Cabir.M.sis->'..free$8.app'.38
Cabir.G.SIS->'..Tee222.app'.34


Administration | Con
lass
Unpacking
Classification
Statistics
Families
Files
Tree
Search
□ Regular
Cabir.C.SIS->'..ni.ai-.app'.22
Cabir.B.sis->'..caribe.app'.17
Cabir.B v2.sis->'C:.DOCUME~1.WINDOW~1.LOCALS~1.Temp.MKS0.OIDI500.app'.16
Cabir.A.sis->'..caribe.app'.5
Cabir.AA.sis->'spooky.APP'.8
0.758069
Cabir.K.sis->'C:.Symbian.6.1.Series60.Epoc32.release.thumb.urel.velasco.app'.36
DoomBoot G.sis->'I:.WINDOWS.MKS0.EVS.app'.110
0.606442
Fontal.B.sis->'C:.DOCUME~1.user.LOCALS~1.Temp.MKS0.Inotify.app'.140
Fontal.A.sis->'C:.DOCUME~1.Home.LOCALS~1.Temp.MKS0.Kill sadam.app'.134
0.644121
f_commwarrior.sis->'C:.DOCUME~1.nurmto.LOCALS~1.Temp.MKS0.FCommwarrior.app'.147

Multi-User capability

- Web-based
- Log in via username/password or SSL certificates
- Automation: Interaction via XMLRPC

Multi-User capability

- Different users can upload samples
- Three levels of permissions:
  - Public: All users can download the sample
  - Protected: All users can see, but not download the sample
  - Private: No other users can see the sample

Business Case

Basic scenario:

- Recognize new malware variants
- Limit risk of outbreak
- Low-cost
- Fast response time

Business Case

Advanced scenario (with shared samples):

- Neighborhood watch
  - Who else has seen this before ?
  - Where ?
  - When ?
  - Who should I talk to ?
- Improve communication

Pricing

Telco-Style: Base Fee + Volume

- Basic:
  - 200 € / month
  - 50 € per uploaded executable
- Medium:
  - 500 € / month
  - 10 uploads included, 30 € each afterwards
- Flat rate:
  - 999 € / month
  - No volume fee*

Pricing

- Only available to GSMA members
- The basic and medium packages may be shared between business entities

Pricing

This includes

- Providing the server / service
- Backups
- Email support

Roadmap

We will watch and adapt to new threats

- Windows Mobile Executables
- Of current relevance: .pyc
- Widgets
- iPhone executables
- Android

Summary

- We provide strong methods that identify malware variants
- Cheap, Fast, Accurate
- Any questions ?

Contact us !

info@zynamics.com