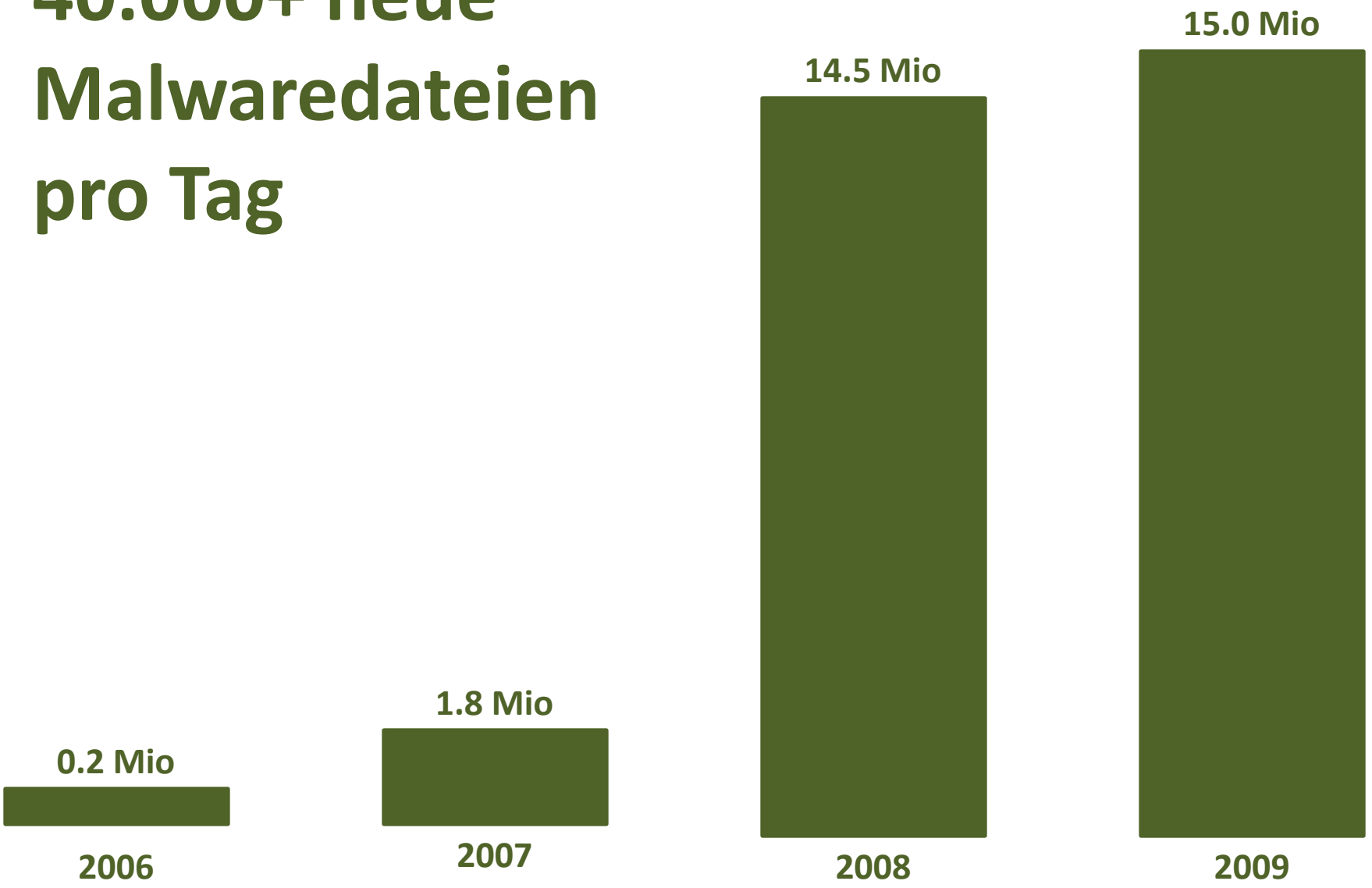
Moderne Malwareklassifikation

Sebastian Porst, zynamics GmbH

sebastian.porst@zynamics.com

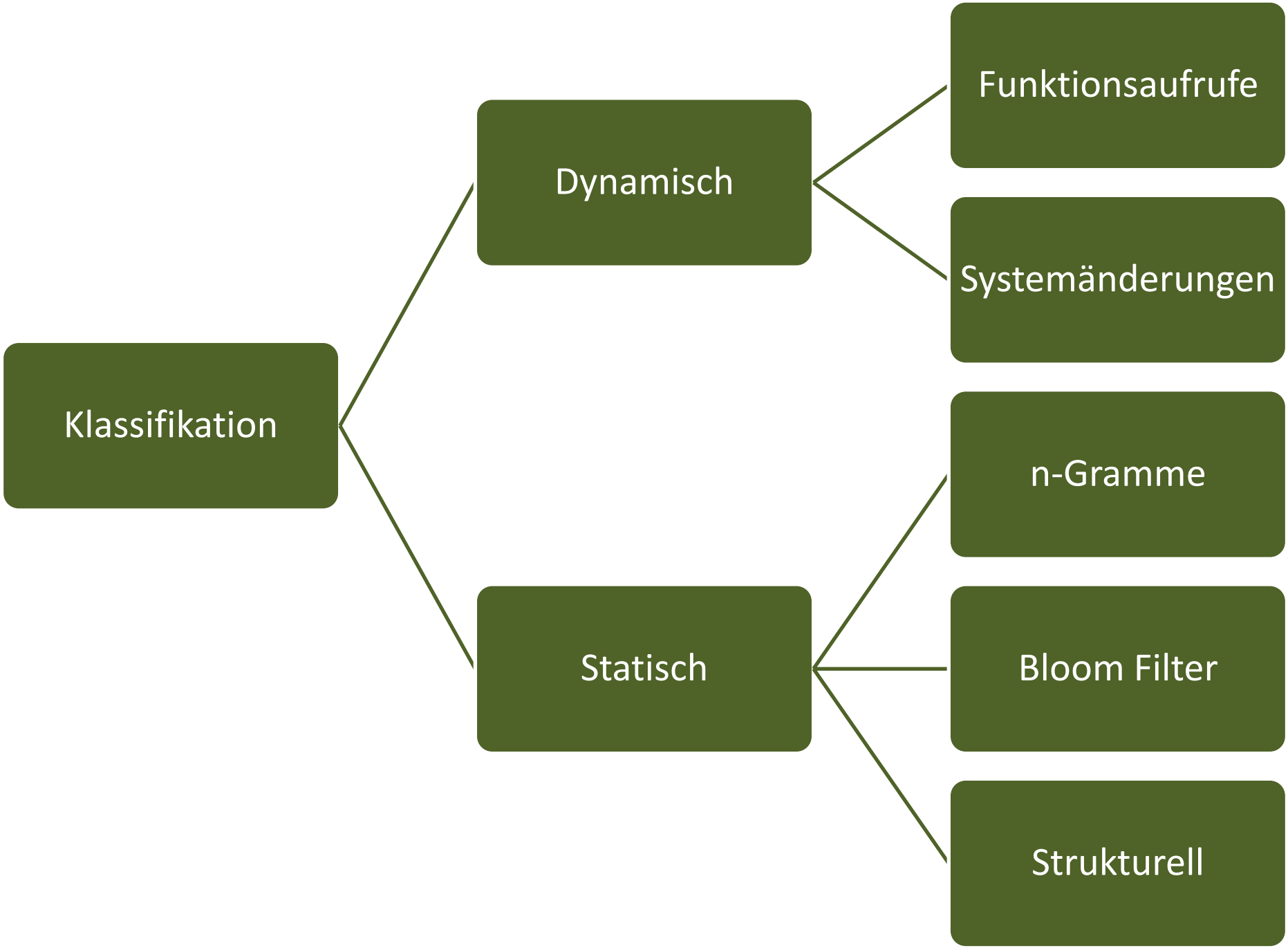
40.000+ neue Malwaredateien pro Tag



Quelle: Kaspersky Security Bulletin 2009. Malware Evolution 2009

Was tun?

- Erkennung
- Analyse
- Klassifikation


Klassifikation
Dynamisch
Statisch
Funktionsaufrufe
Systemänderungen
n-Gramme
Bloom Filter
Strukturell

Dynamisch

Programmverhalten wird berücksichtigt

Statisch

Programmstruktur wird berücksichtigt

Dynamisch

Funktionsaufrufe

Dynamisch

Funktionsaufrufe

Funktionsaufrufe protokollieren

=

ReadFile

Process32First

lstrcpy

...

Dynamisch

Funktionsaufrufe

Mit bekannter Malware vergleichen

=

Sequenzen von Funktionsaufrufen

Bibliothek aufbauen

Editierdistanz

Dynamisch

Funktionsaufrufe

Vorteile

Einfach zu realisieren

Überwachung erfolgt prozessübergreifend

Nachteile

Programme müssen ausgeführt werden

Anfällig für Täuschungsversuche

Dynamisch

Systemänderungen

Dynamisch

Systemänderungen

Veränderungen protokollieren

=

Datei C:\windows\foo.exe wurde geschrieben

Server an Port 80 angemeldet

Lädt Datei von IRC Server runter

...

Dynamisch

Systemänderungen

Mit bekannter Malware vergleichen

=

Sequenzen von Systemänderungen

Bibliothek aufbauen

Editierdistanz

Dynamisch

Systemänderungen

Vorteile

Einfach zu realisieren

Überwachung erfolgt prozessübergreifend

Weniger anfällig für Täuschungsversuche

Nachteile

Programme müssen ausgeführt werden

Statisch

n-Gramme

Statisch

n-Gramme

n-Gramme berechnen

=

Programm disassemblieren

Befehle erkennen

Mnmemonic-Sequenzen zählen

Statisch

n-Gramme

Mit bekannter Malware vergleichen

=

n-Gramme berechnen

Bibliothek aufbauen

Cosinus

Statisch

n-Gramme

Vorteile

Einfach und schnell

Berücksichtigt gesamte Datei

Robust gegenüber Codebewegungen

Nachteile

In der Praxis nur für kleine n möglich

Anfällig gegenüber Compileränderungen

Kann sehr leicht getäuscht werden

Statisch

Bloom Filter

Statisch

Bloom Filter

Bloom Filter berechnen

=

Datei disassemblieren

Basic Blocks erkennen

Basic Blocks hashen

Hashwerte in Vektor speichern

Statisch

Bloom Filter

Mit bekannter Malware vergleichen

=

Bloom Filter berechnen

Bibliothek aufbauen

Vektorvergleich

Statisch

Bloom Filter

Vorteile

Skaliert wunderbar

Nachteile

Entwicklung der Hashfunktion sehr schwierig

Hashfunktion ist anfällig für kleine Änderungen

Statisch

Strukturell

Statisch

Strukturell

Flussgraphen berechnen

=

Datei disassemblieren

Funktionen erkennen

Flussgraph erstellen

Graphstruktur hashen

Statisch

Strukturell

Mit bekannter Malware vergleichen

=

Flussgraphen berechnen

Bibliothek aufbauen

Hashvergleich

Statisch

Strukturell

Vorteile

Berücksichtigt das komplette Programm

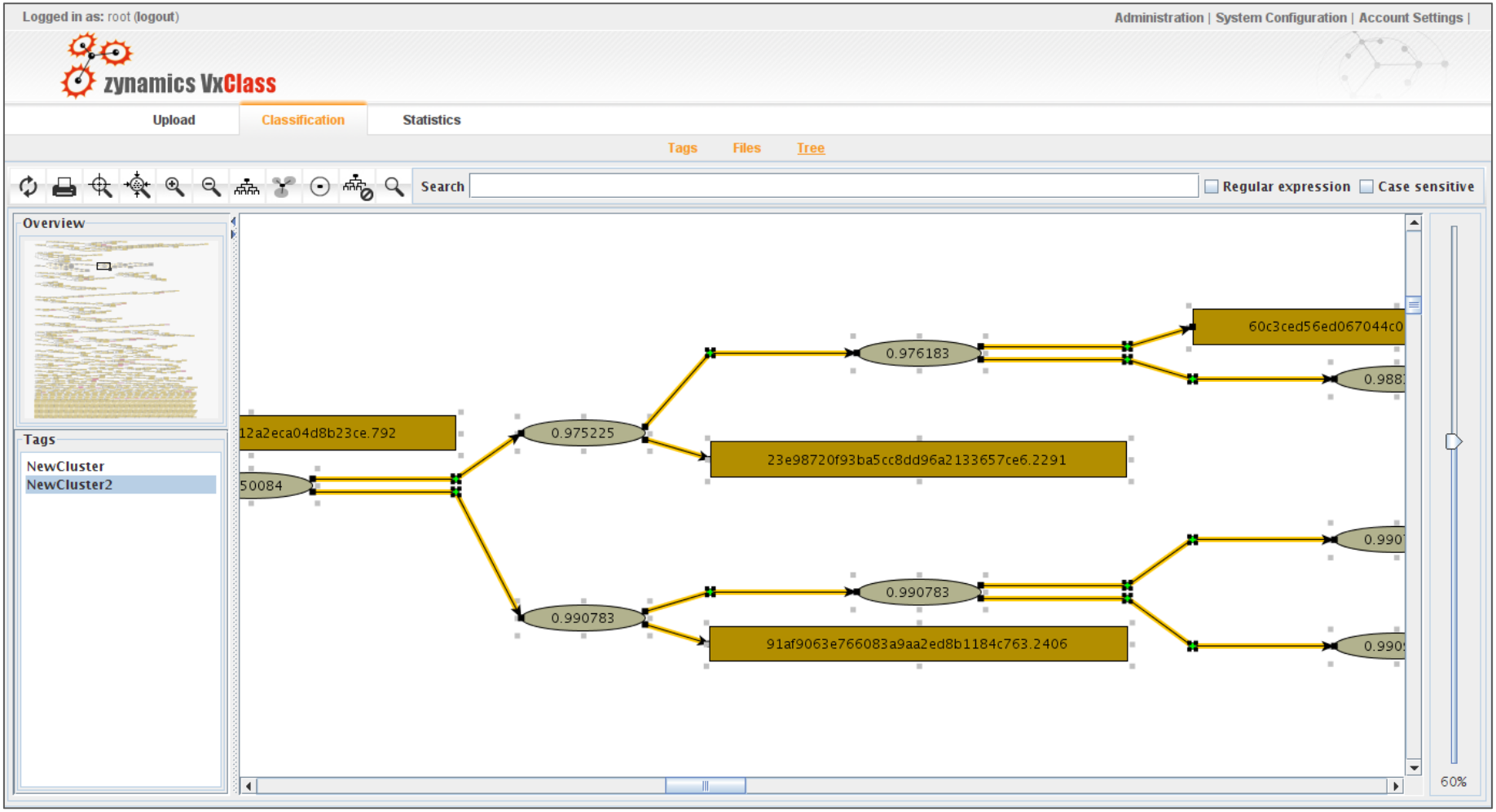
Robust gegenüber Änderungen

Nachteile

Vollständiges Disassembly wird benötigt

Zu langsam für Endnutzergeräte

Resultate


Logged in as: root (logout)
Administration | System Configuration | Account Settings |
zynamics VxClass
Upload
Classification
Statistics
Tags
Files
Tree
Search
Regular expression
Case sensitive
Overview
Tags
NewCluster
NewCluster2
12a2eca04d8b23ce.792
50084
0.975225
0.976183
0.990783
0.990783
60c3ced56ed067044c0
23e98720f93ba5cc8dd96a2133657ce6.2291
91af9063e766083a9aa2ed8b1184c763.2406
60%

Weitere Ideen

- Kombinationen
- Andere Methoden
- Signaturgeneration
- Angriffe korrelieren