



Πλατφόρμα ανάλυσης και κατηγοριοποίησης συμπεριφοράς κακόβουλου λογισμικού με τη χρήση μηχανικής μάθησης

Κυριάκος Στεφανίδης, Βασίλης Πίκουλης

Ερευνητής Β', Συνεργαζόμενος Ερευνητής

Ινστιτούτο Βιομηχανικών Συστημάτων



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο
Περιφερειακής Ανάπτυξης



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΘΡΩΤΙΚΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΑΝΕΚ

ΕΠΑΝΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



Εισαγωγή

Η απειλή των κυβερνοεπιθέσεων και του κακόβουλου λογισμικού

- Ως το 2023, περί τα **5.2 τρις δολάρια**¹ περιουσιακών στοιχείων θα βρίσκονται υπό απειλή
- **28%** του συνόλου των κυβερνοεπιθέσεων αφορά τη χρήση κακόβουλου λογισμικού

Η ανίχνευση κακόβουλου λογισμικού παραμένει ανοιχτό και δύσκολο πρόβλημα

- Απειλή που συνεχώς εξελίσσεται
- Η έλευση της Βαθιάς Μηχανικής Μάθησης έφερε πληθώρα νέων τεχνικών
- Έλλειψη πρότυπων συνόλων εκπαίδευσης και ελέγχου των μεθόδων

¹Kelly Bissel, et. al., *Ninth Annual Cost of Cybercrime Study*. The Cost of Cybercrime, Ponemon Institute LLC, Accenture plc, 2019

Αποτελέσματα Επιγραμματικά

Δυο συστήματα ανίχνευσης κακόβουλου λογισμικού δημιουργήθηκαν στο πλαίσιο του έργου

- Συστήματα που βασίζονται στη **στατική** ανάλυση του λογισμικού
- Το πρώτο σύστημα χρησιμοποιεί το σύνολο χαρακτηριστικών EMBER και **random forests**
- Το δεύτερο βασίζεται στη χρήση **graph kernels** και Support Vector Machines

Τα συστήματα ενσωματώθηκαν στην πλατφόρμα ανάλυσης κακόβουλου λογισμικού Sisyfos

- Υποστηρίζεται χειροκίνητη και αυτόματη ανάλυση όπως και μαζική ανάλυση αρχείων
 - Μέσω web interface
 - Μέσω REST API
- Συμπεριλαμβάνει διάφορα ενσωματωμένα modules στατικής και δυναμικής ανάλυσης

Προσπάθεια διασύνδεσης της πλατφόρμας με την πλατφόρμα κυβερνοασφάλειας αυτόνομων οχημάτων του ευρωπαϊκού έργου nioVe



Ανίχνευση κακόβουλου λογισμικού με χρήση χαρακτηριστικών του EMBER και random forests

Το σύνολο δεδομένων EMBER

- **600.000** δείγματα για εκπαίδευση, **200.000** για επαλήθευση/έλεγχο
- Δείγματα από καλόβουλο & κακόβουλο λογισμικό
- **2351** χαρακτηριστικά για κάθε δείγμα (strings, κεφαλίδα, εντροπία, κ.α.)
- Εργαλείο ανοικτού κώδικα για την εξαγωγή των χαρακτηριστικών από νέα δεδομένα

Ταξινόμηση με χρήση random forests

- 1.000 δυαδικά δέντρα αποφάσεων
- 48 χαρακτηριστικά ανά δέντρο
- Η απόφαση λαμβάνεται από την πλειοψηφία των επιμέρους ταξινομήσεων

Υλοποίηση σε Python

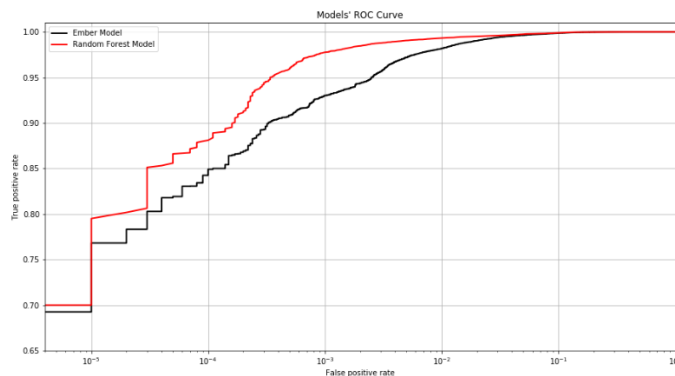
- Χρήση των βιβλιοθηκών scikit-learn και numpy

Ανίχνευση κακόβουλου λογισμικού με χρήση χαρακτηριστικών του EMBER και random forests

Ακρίβεια μοντέλου: **99.2%**

Βελτιώνει το μοντέλο
αναφοράς του EMBER

Μεγαλύτερη πιθανότητα
ανίχνευσης για το ίδιο ποσοστό
εσφαλμένου συναγερμού



Πιθανότητα εσφαλμένου συναγερμού	Πιθανότητα ορθής ανίχνευσης	
	EMBER	Random Forests
1%	98.5 %	99.0 %
0.1 %	96.4 %	98.8 %

Ανίχνευση κακόβουλου λογισμικού με χρήση χαρακτηριστικών του EMBER και random forests

Τα σύνολα εκπαίδευσης και ελέγχου του EMBER:

- ✓ Έχουν προέλθει από την ίδια διαδικασία συλλογής και από τον ίδιο οργανισμό
- ✓ Συλλέχθηκαν με απόσταση μόλις δύο μηνών μεταξύ τους

Έλεγχος απόδοσης σε **νέο σετ** δεδομένων

- ✓ **89.000** κακόβουλα εκτελέσιμα αρχεία από το αποθετήριο VirusShare
- ✓ Δεδομένα που έχουν συλλεχθεί με διαφορετικό τρόπο χρόνο από το EMBER
- ✓ Από το κάθε δείγμα εξάγεται το ίδιο σετ των 2351 χαρακτηριστικών που χρησιμοποιήθηκαν για την εκπαίδευση

Συγκριτικά αποτελέσματα:

Δεδομένα ελέγχου	Μοντέλο ανίχνευσης	
	EMBER	Random Forests
EMBER	98.9 %	99.0 %
VirusShare	84.2 %	87.7 %



Ανίχνευση κακόβουλου λογισμικού με χρήση χαρακτηριστικών του EMBER και random forests

Μελέτη ευαισθησίας ως προς τα χρησιμοποιούμενα χαρακτηριστικά:

- ✓ Χρήση **μικρού** υποσυνόλου **σημαντικών** χαρακτηριστικών
- ✓ Εξαγωγή σημαντικότερων χαρακτηριστικών με βάση το **κέρδος πληροφορίας**

Σημαντικότερα χαρακτηριστικά

- ✓ Εικονικό μέγεθος τμημάτων στην μνήμη
- ✓ Εισαγόμενες & εξαγόμενες συναρτήσεις
- ✓ Εντροπία τμημάτων

Αποτελέσματα μοντέλου με χρήση των **10 σημαντικότερων** χαρακτηριστικών:

Αριθμός χαρακτηριστικών	Ακρίβεια	Χρόνος εκπαίδευσης (λεπτά)
2351	99.2 %	2195
10	96.1 %	23

Ανίχνευση κακόβουλου λογισμικού με χρήση χαρακτηριστικών του EMBER και random forests

Επίδραση του μεγέθους του συνόλου εκπαίδευσης:

- Αναμενόμενα μη ικανοποιητική απόδοση για πολύ μικρά μεγέθη συνόλων (≤ 1000)
- Απώλεια $\leq 1\%$ της απόδοσης σε μεσαίου μεγέθους σύνολα (≈ 50.000),
- Η αύξηση στην απόδοση γίνεται ολοένα και «ακριβότερη» για ≥ 100.000

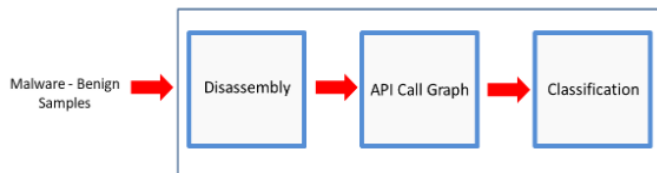
Πλήθος δειγμάτων εκπαίδευσης	Ακρίβεια	Χρόνος εκπαίδευσης (λεπτά)
1.000	92.6 %	0.2
5.000	97.0 %	2.1
10.000	97.6 %	8.8
30.000	98.2 %	21.6
100.000	98.6 %	132
600.000	99.2 %	2195

Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Το σύστημα συνδυάζει τη στατική ανάλυση με τη μοντελοποίηση γράφων
Ταξινόμηση με χρήση Support Vector Machines

Βασικά βήματα αλγορίθμου:

1. Αποσυναρμολόγηση (**disassembly**) του δείγματος
2. Γράφος Ελέγχου Ροής → Γράφος Κλήσεων API → *Αφηρημένος Γράφος Κλήσεων*
3. Χρήση **πυρήνα** βασισμένου στα random walks για συγκρίσεις μεταξύ γράφων.
4. Ταξινόμηση με χρήση γραμμικού **SVM**.



Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Σύνολα δεδομένων:

- ✓ 997 δείγματα **κακόβουλων** εκτελέσιμων από τα VirusShare, VirusTotal
- ✓ 557 **καλόβουλα** εκτελέσιμα από έμπιστες πηγές (Windows, Git, Cygwin, κ.α.)

Η πλατφόρμα *Ghidra* της NSA

- ✓ Εργαλείο ανοικτού κώδικα για την ανάλυση λογισμικού (*disassembly*)
- ✓ Εύρεση δομικών μπλοκ κώδικα, και των κλήσεων API που αυτά πραγματοποιούν

Αφηρημένος Γράφος Κλήσεων Συστήματος

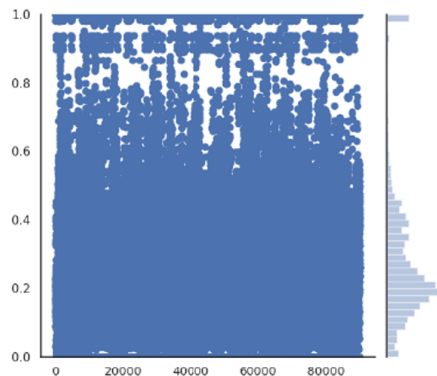
1. Γράφος Ελέγχου Ροής (διασύνδεση μεταξύ μπλοκ κώδικα)
2. Γράφος Κλήσεων API (αντικατάσταση κόμβων/μπλοκ με κλήσεις API)
3. Αφηρημένος Γράφος (συγχώνευση κόμβων, εξάλειψη σειράς εκτέλεσης)

Random Walk Graph Kernel

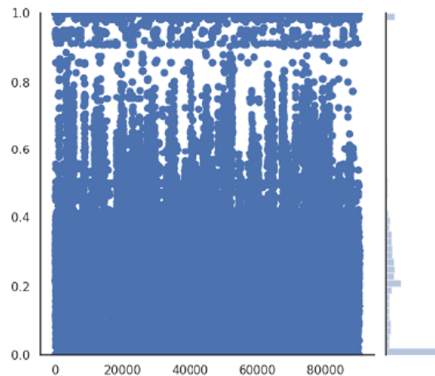
- ✓ Εύρεση «εσωτερικού γινομένου» μεταξύ γράφων (ποσοτικοποίηση **ομοιότητας** γράφων)

Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

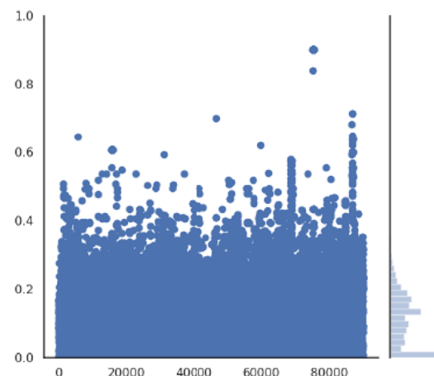
Τιμές πυρήνα (ομοιότητας) για ζεύγη δειγμάτων του συνόλου εκπαίδευσης



καλόβουλο/καλόβουλο



κακόβουλο/κακόβουλο



καλόβουλο/κακόβουλο

Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Εκπαίδευση SVM

- ✓ Χωρίζουμε το διαθέσιμο σύνολο σε δείγματα εκπαίδευσης/δείγματα ελέγχου
- ✓ Μέσω πειραματισμού καθορίστηκε ως βέλτιστη η αναλογία 90% - 10%
- ✓ 100 διαφορετικά ζεύγη συνόλων σύνολα με τυχαία επιλογή

Μετρικές

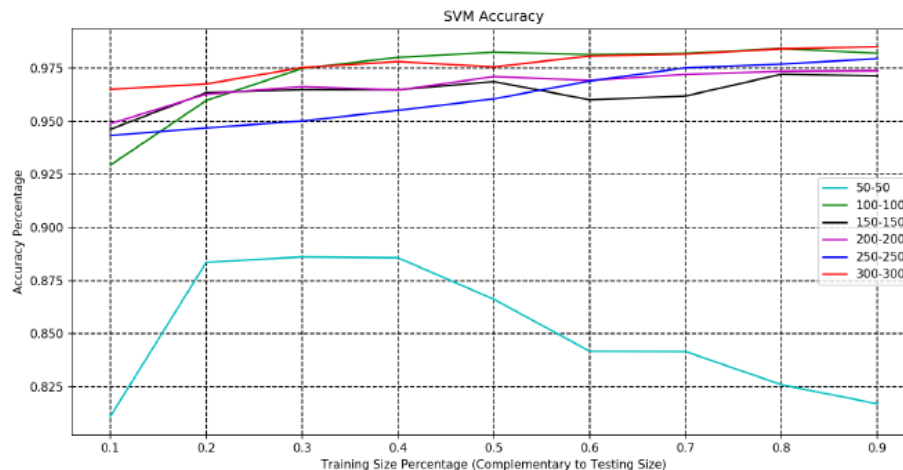
- ✓ Ακρίβεια (ποσοστό σωστών προβλέψεων)
- ✓ ROC AUC (εμβαδό κάτω από την καμπύλη ROC)
- ✓ Precision (ποσοστό σωστών ανιχνεύσεων)
- ✓ Recall (ποσοστό κακόβολου λογισμικού που ανιχνεύθηκε)

Αποτελέσματα ταξινόμησης

- ✓ Όλες οι χρησιμοποιούμενες μετρικές οδηγούν σε επιδόσεις άνω του **98%**,
- ✓ Πολύ ικανοποιητική απόδοση δεδομένου του σχετικά **μικρού συνόλου** εκπαίδευσης
- ✓ Καταδεικνύει την **αποτελεσματικότητα** των τεχνικών που χρησιμοποιήθηκαν

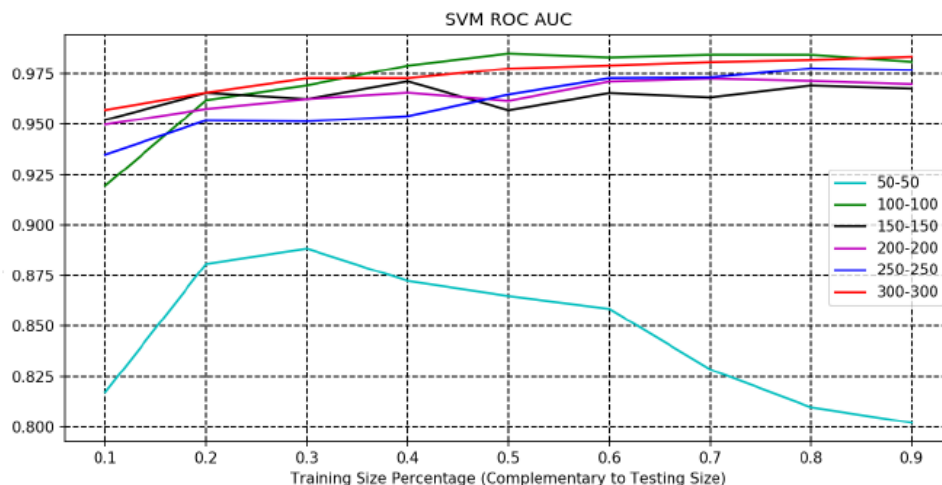
Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Ακρίβεια μοντέλου για διάφορα μεγέθη και αναλογίες συνόλων εκπαίδευσης



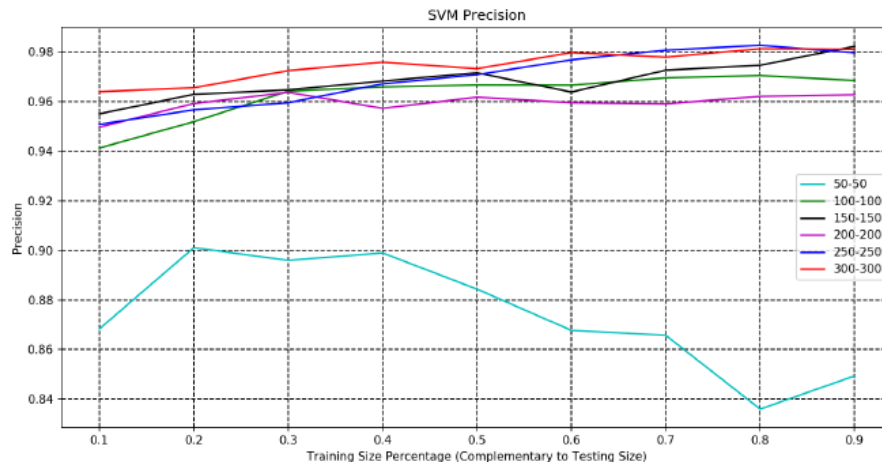
Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Μετρήσεις **ROC - AUC** για διάφορα μεγέθη και αναλογίες συνόλων εκπαίδευσης



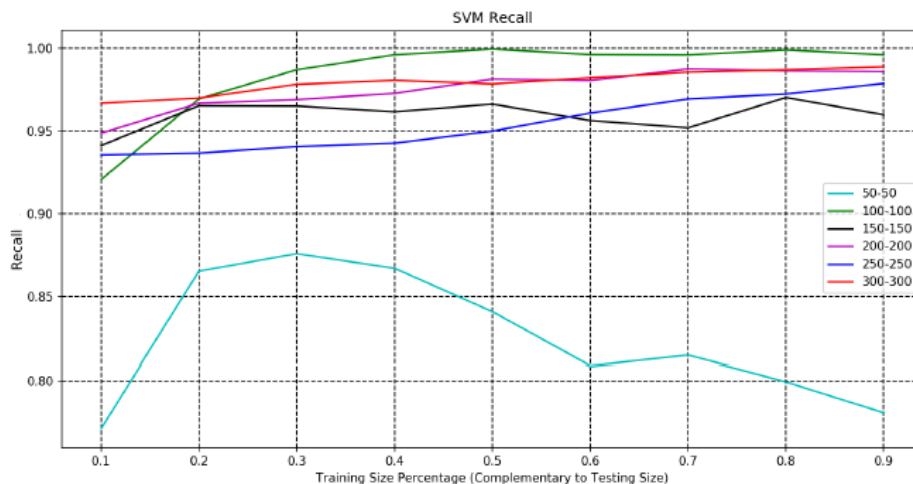
Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Μετρήσεις του **precision** για διάφορα μεγέθη και αναλογίες συνόλων εκπαίδευσης



Ανίχνευση κακόβουλου λογισμικού με βάση τον Γράφο Κλήσεων API

Μετρήσεις του **recall** για διάφορα μεγέθη και αναλογίες συνόλων εκπαίδευσης



Ολοκλήρωση με την πλατφόρμα sisyfos

Παρέχει ένα ολοκληρωμένο
περιβάλλον ανάλυσης
κακόβουλου λογισμικού

✓ Βασισμένο στο cuckoo sandbox

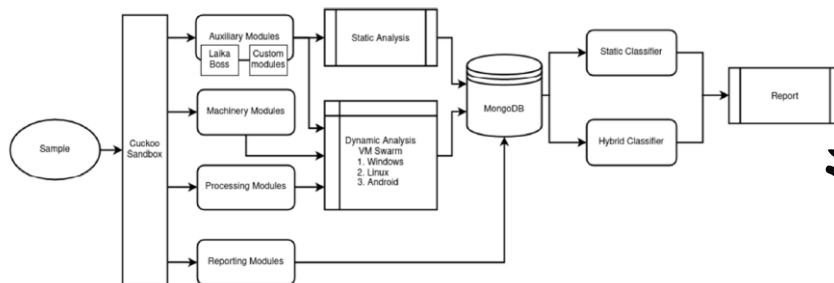
Τρία βασικά υποσυστήματα

✓ Orchestrator

✓ Στατική ανάλυση

✓ Δυναμική ανάλυση

✓ Ταξινόμηση



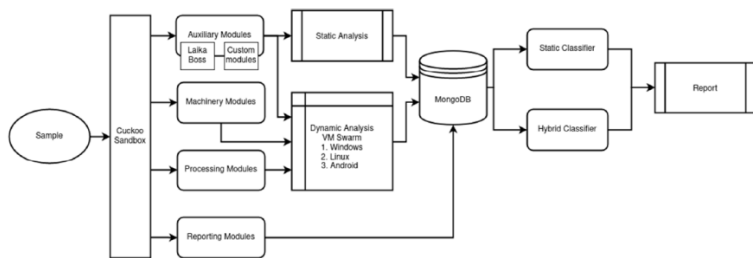
Orchestrator

Python Scripts για την μαζική φόρτωση
και ανάλυση δειγμάτων

sample -> cuckoo and modules ->
database -> classifier

Web interface μέσω του cuckoo sandbox

Web service για την μαζική
μεταφόρτωση



cuckoo Dashboard Recent Pending Search [Submit] [Import]

Summary

File pscp.exe.metadata [Download] [Resubmit sample]

Summary	Size	Type	MD5	SHA1	SHA256	SHA512	CRC32	codecap	Yara
	144.0B	ASCII text	9920c516416b94176433f4b826984	162854c3e08f1eb152b24c37f6b9a33942e0c	6b55b88395481a44278710902764b78a98f6c5085a07312d84e8d6c1e811	997039f9		None matched	

Score

This file shows numerous signs of malicious behavior.
The score of this file is 4.6 out of 10.

Feedback
Exporting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	June 15, 2021, 2:44 a.m.	June 15, 2021, 2:47 a.m.	165 seconds	none	Show Analyzer Log Show Cuckoo Log

Signatures

- Queries for the computername (5 events)
- Checks if process is being debugged by a debugger (2 events)
- Tries to locate where the browsers are installed (1 event)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- Checks whether any human activity is being performed by constantly checking whether the foreground window changed
- Queries the disk size which could be used to detect virtual machine with small fixed size or dynamic allocation (5 events)
- Creates a shortcut to an executable file (22 events)

Στατική Ανάλυση

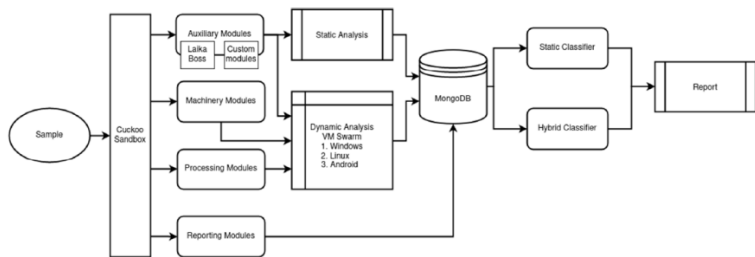
Εύκολη εξαγωγή χαρακτηριστικών

Βασικά εργαλεία στατικής ανάλυσης (cuckoo)

- ✓ file metadata
- ✓ resources
- ✓ basic binary info
- ✓ printable strings
- ✓ Virus scanning services

Άλλα εργαλεία

- ✓ entropy measurement
- ✓ Ember feature extraction
- ✓ Binary disassembly (υπο ολοκλήρωση)
- ✓ Laika Boss
- object unpacking and scanning



cuckoo Dashboard Recent Pending Search Submit Import

Static Analysis

Static Analysis Strings Antivirus IRMA LAIKABOSS EMBER

PE Compile Time: 2013-03-03 11:39:46
PE Imphash: c139b07474203469853c4622877273

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00001000	0x00002fb2	0x00003000	6.32908619141
.rdata	0x00004000	0x00000892	0x00000a00	4.0882763689
.data	0x00005000	0x00000564	0x00000600	3.33395714059
.rsrc	0x00006000	0x0001af4d	0x0001b000	7.99614041423
.reloc	0x00021000	0x000002c2	0x00000400	2.70439774212

Resources

Name	Offset	Size	Language	Sub-language	File type
RT_RCDATA	0x00020c30	0x00000319	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_RCDATA	0x00020c30	0x00000319	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_RCDATA	0x00020c30	0x00000319	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_RCDATA	0x00020c30	0x00000319	LANG_ENGLISH	SUBLANG_ENGLISH_US	data

Imports

Library KERNEL32.dll:

- 0x004000 LocalAlloc
- 0x004004 LocalFree
- 0x004008 RtlDnsName
- 0x00400c LoadLibraryA
- 0x004010 GetModuleHandleA
- 0x004014 CloseHandle
- 0x004018 ReadFile
- 0x00401c GetFileSize

Library ntdll.dll:

- 0x004078 _seprintf
- 0x00407c _vsnprintf
- 0x004080 memset
- 0x004084 UnTerminateProcess
- 0x004088 sprintf
- 0x00408c RtlCompareMemory
- 0x004090 RtlProtectVirtualMemory
- 0x004094 RtlProtectVirtualMemory

Library RPCRT4.dll:

- 0x004064 GuidToStringA
- 0x004068 RpcStringFreeA

Library SHELL32.dll:

- 0x004070 ShellExecuteA

Δυναμική Ανάλυση

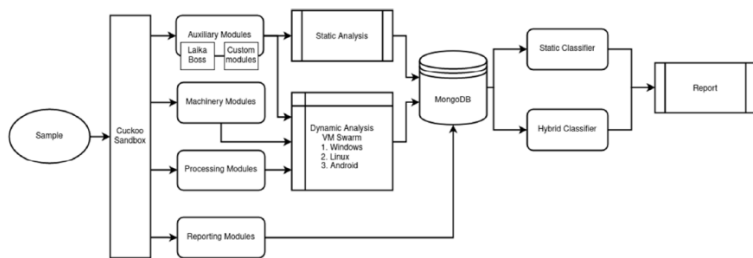
Sandboxes (windows VMs)

Cuckoo/VirtualBox για την διαχείριση των VMs

- ✓ 6~50 παράλληλα VMs δυνατότητα
- ✓ VMCloak για απόκρυψη του sandbox
- Εγκατάσταση κοινών εφαρμογών

Χαρακτηριστικά

- ✓ file system
- ✓ registry
- ✓ network
- ✓ dynamic signatures
 - unpacking
 - code injection in child processes



cuckoo Dashboard Recent Pending Search Submit Import

Behavioral Analysis

Search

Process tree

- cmd.exe (PID: 2816)
 - rundll32.exe (PID: 2948)
 - AcroRd32.exe (PID: 1948)
 - Adobe_Updater.exe (PID: 192)
 - explorer.exe (PID: 988)
 - Process contents

AcroRd32.exe
PID: 1948
Parent PID: 2948

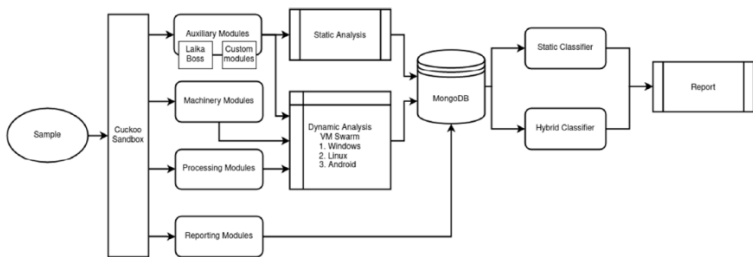
default registry file network process services synchronisation explore office pdf

Time & API	Arguments	Status	Return	Repeated
RegOpenKeyExW June 15, 2021, 3:45 a.m.	regkey: Software\Adobe\Acrobat Reader\9.0\ORO base_handle: 0x80000002 key_handle: 0x00000000 options: 0 access: 0x02000000 regkey: HKEY_LOCAL_MACHINE\Software\Adobe\Acrobat Reader\9.0\ORO		2	0
RegOpenKeyExW June 15, 2021, 3:45 a.m.	regkey: SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters base_handle: 0x80000002 key_handle: 0x00000004 options: 0 access: 0x02000000 regkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters	1	0	0

Ταξινόμηση

Τρείς ταξινομητές

- Ενσωματωμένος ταξινομητής του cuckoo (hybrid)
- random forests (static)
- API call graph (static)



The screenshot displays the Cuckoo Sandbox web interface. At the top, there's a navigation bar with 'Dashboard', 'Recent', 'Pending', and 'Search' options. Below this, the 'Signatures' section lists various detection rules with their event counts and expandable details. The 'Screenshots' section shows a grid of 12 thumbnail images of a Windows desktop environment. At the bottom, a table provides details for a specific analysis.

Name	Response	Post-Analysis Lookup	IP Address	Status	Action
time.windows.com			8.8.8.8	Active	Moloch
www.msfnrcsi.com			194.177.211.137		

[illegible]



Ευχαριστούμε