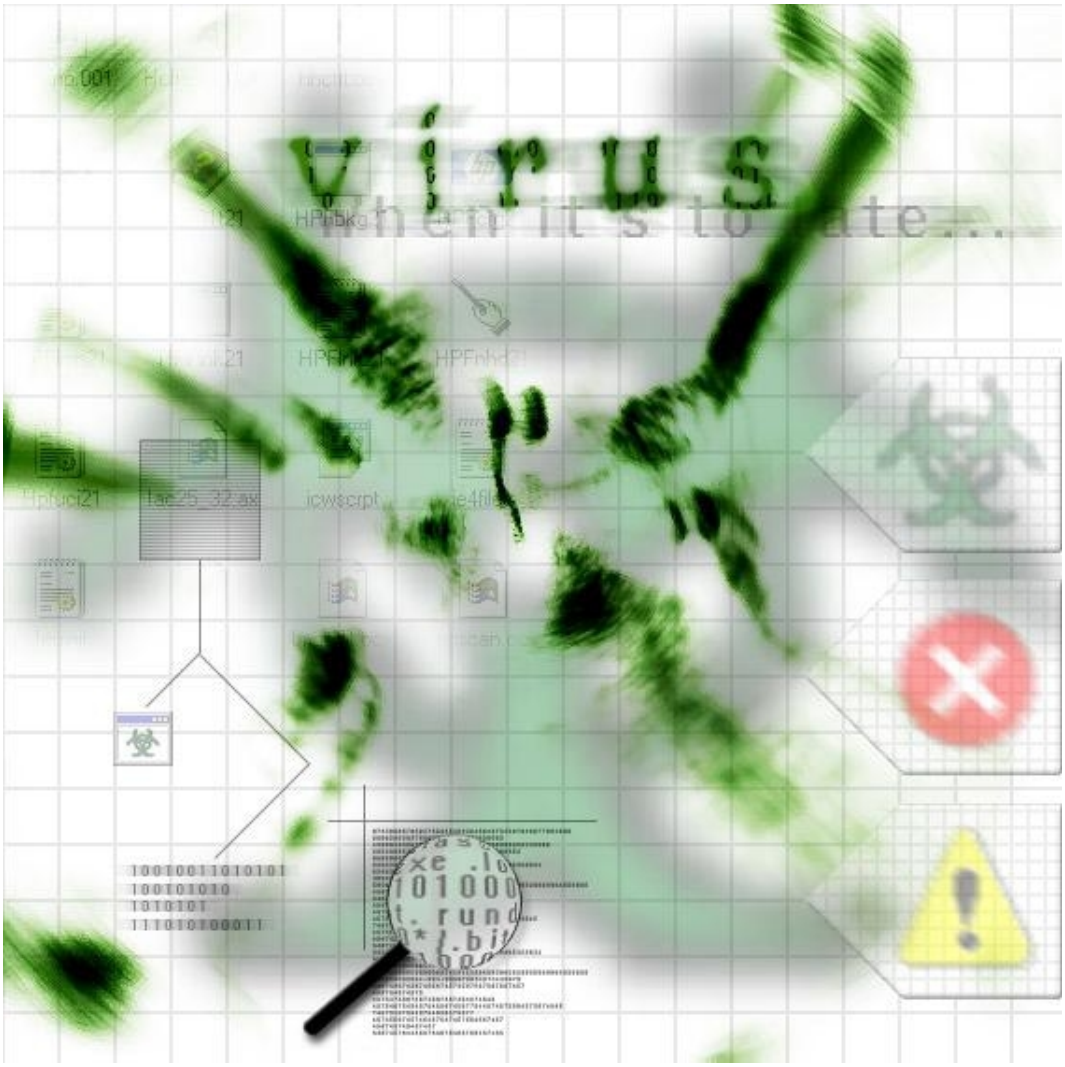
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



Βασικά στοιχεία ιομορφικού λογισμικού

Μανώλης Βασιλομανωλάκης

email: icsd03006 at icsd.aegean.gr

Τι είναι ένας ιός;

Θέλοντας να δώσουμε έναν γενικό ορισμό για το τι είναι ένας ιός, θα λέγαμε πως είναι ένα είδος προγράμματος (κώδικας) που είναι ικανό να δημιουργεί αντίγραφα του εαυτού του (πιθανώς τροποποιημένα) και εισάγεται σκοπίμως σε κάποιο πρόγραμμα ηλεκτρονικού υπολογιστή ή σε κάποιο σύστημα.

Είναι σημαντικό να αναφέρουμε ότι **κάθε** ιός έχει μία ταυτότητα/υπογραφή (signature) η οποία δεν είναι τίποτα άλλο από μία σειρά (string) από bytes.

Ιστορική αναδρομή – οι πρώτοι ιοί

Υπάρχουν πολλές και διαφορετικές απόψεις για το πότε ακριβώς δημιουργήθηκε καθώς και για το ποιος ήταν ο πρώτος **ιός**. Είναι ωστόσο γνωστό ότι οι *Univac 1108* και *IBM 360/370* είχαν δεχθεί ιούς (συγκεκριμένα τους "*Pervading Animal*" και "*Christmas tree*") οπότε μπορούμε να πούμε σχεδόν σίγουρα πως ο πρώτος ιός δημιουργήθηκε κάπου στις αρχές του 1970 (παρόλο που ο όρος «ιός» ήρθε πολύ αργότερα –πιθανόν το 1983 από τον *Fred Cohen* (*University of Southern California*)-).

Την περίοδο εκείνη (τέλη του 1960 με αρχές του 1970) έκαναν περιοδικά την εμφάνισή τους διάφορα προγράμματα –με την ονομασία the Rabbit-, τα οποία κλωνοποιούσαν τον εαυτό τους, και καταλάμβαναν πόρους του συστήματος μειώνοντας κατά συνέπεια την παραγωγικότητα του. Αυτά πιθανότατα δεν αντιγράφονταν από σύστημα σε σύστημα και ήταν αυστηρά τοπικά φαινόμενα (λάθη ή φάρσες από τους προγραμματιστές συστημάτων που συντηρούσαν αυτούς τους υπολογιστές). Το πρώτο περιστατικό που θα μπορούσε να ονομαστεί «επιδημία ενός ιού υπολογιστών» συνέβη στον Univac 1108 και ήταν ο "*Pervading Animal*" ο οποίος συγχωνευόταν στο τέλος εκτελέσιμων αρχείων.

Το πρώτο πρόγραμμα καταπολέμησης ιών (**anti-virus**) ήρθε στις αρχές της δεκαετίας του ’70 όταν μετά την εμφάνιση του ιού Creeper (τα συστήματα στα οποία είχε εισχωρήσει τύπωναν το μήνυμα: 'I'M THE CREEPER : CATCH ME IF YOU CAN.') στο Arpanet (στρατιωτικό δίκτυο των ΗΠΑ από το οποίο ήρθε στη συνέχεια το internet) δημιουργήθηκε ο Reaper ο οποίος ήταν ουσιαστικά ένας νέος ιός ο οποίος διαδιδόταν μέσα από το δίκτυο και όταν έβρισκε κάποιον υπολογιστή μολυσμένο από τον Creeper έσβηνε τον ιό.

Το 1981 κάνει την εμφάνισή του ο elk-cloner (δημιουργήθηκε από έναν 15 άχρονο μαθητή) ο οποίος δρούσε στους Apple II υπολογιστές, ενώ ο πρώτος ιός για IBM-PC ήρθε το 1986, ο λεγόμενος Brain virus που προκάλεσε πανδημία. Ο τελευταίος που σύμφωνα με τους δημιουργούς του (δύο αδέλφια από το Πακιστάν) είχε σαν σκοπό την μέτρηση της «πειρατείας» στην χώρα τους, όμως εξαπλώθηκε στιγμιαία σε ολόκληρο τον κόσμο, ήταν και ο πρώτος που είχε stealth ικανότητες.

Κατηγορίες ιών

Σε γενικές γραμμές υπάρχουν ποικίλοι τρόποι για να κατηγοριοποιήσει κανείς τους ιούς. Ενδεικτικά βλέπουμε μερικές κατηγορίες ιών παρακάτω:

- Boot sector infectors
- Macro Viruses
- Polymorphic Viruses
- Air-born Viruses
- Script Viruses
- Program Viruses

Γενικές τεχνικές απόκρυψης

- **Stealth**
  Κάποιοι ιοί προσπαθούν να "ξεγελάσουν" τα αντι-ιικά προγράμματα με το να παρεμποδίζουν τα αιτήματα τους στο λειτουργικό σύστημα.

- **Polymorphism**
  Οι ιοί μπορούν για να αποφύγουν την ανίχνευσή τους να είναι πολυμορφικοί (το πώς ακριβώς γίνεται αυτό θα αναλυθεί παρακάτω)

- **Metamorphic**
  Για να αποφύγουν την ανίχνευση με τη χρήση της προσομοίωσης (Generic Decryptor) χρησιμοποιούν μεταμορφικές μηχανές (metamorphic engines) για να αλλάξουν τελείως τον κώδικά τους (οι ιοί αυτοί είναι εξαιρετικά μεγάλοι πχ ο Simile που έχει 14000 γραμμές κώδικα assembly).

Οι κατηγορίες ιών που θα δούμε αναλυτικά παρακάτω είναι: boot sector, polymorphic, και macro.

1. Boot Sector ιοί

Γενικά χαρακτηριστικά

Οι **boot sector** ιοί μπορούν να μολύνουν ή να αντικαθιστούν με τον δικό τους κώδικα, τόσο το DOS boot sector όσο και το Master Boot Record (MBR). Το MBR είναι ένα μικρό πρόγραμμα που τρέχει κάθε φορά που ανοίγει ο υπολογιστής, το οποίο έχει στον έλεγχό του το boot sequence και καθορίζει από ποιο partition θα κάνει εκκίνηση (boot) ο υπολογιστής. Γενικά το MBR βρίσκεται στο πρώτο τομέα (sector) του σκληρού δίσκου.

Γίνεται εύκολα αντιληπτό ότι από τη στιγμή που το MBR εκτελείται κάθε φορά που ανοίγει ο υπολογιστής, η μόλυνσή του από έναν ιό είναι άκρως επικίνδυνη. Από τη στιγμή που θα μολυνθεί ο κώδικας εκκίνησης του δίσκου, ο ιός θα φορτώνεται **στη μνήμη** σε **κάθε** άνοιγμα του υπολογιστή. Από τη μνήμη ο boot sector ιός μπορεί να μολύνει κάθε δίσκο (local ή removable) που διαβάζεται από το σύστημα.

Οι ιοί αυτοί μπορούν να προκαλέσουν μία ποικιλία προβλημάτων ανάκτησης δεδομένων ή και στοιχείων εκκίνησης. Σε κάποιες περιπτώσεις μάλιστα είναι δυνατόν να προκληθεί απώλεια δεδομένων – και μάλιστα από ολόκληρα κομμάτια του δίσκου. Επίσης πολύ συχνά ο υπολογιστής γίνεται ξαφνικά ασταθής, αποτυγχάνει να ξεκινήσει, ή δεν μπορεί να εντοπίσει τον σκληρό δίσκο. Σε τέτοιες περιπτώσεις μηνύματα λάθους όπως: “invalid system disk” είναι συχνό φαινόμενο.

Η μετάδοση αυτών του ιομορφικού λογισμικού γίνεται συνήθως (ή καλυτέρα γινόταν -αφού στο παρελθόν πολλά floppy disks χρησιμοποιούνταν ως bootable disks) από μολυσμένα floppy disks. Σήμερα η μετάδοσή τους γίνεται κατά βάση μέσω δικτύων (και του Διαδικτύου φυσικά) από downloads αρχείων ή και από μολυσμένα emails. Στις περισσότερες των περιπτώσεων όλοι οι δίσκοι (με ενεργοποιημένη την εγγραφή στη μνήμη) σε έναν μολυσμένο υπολογιστή θα “κωλύσουν” τον ιό.

Μερικοί γνωστοί/συνήθεις boot sector ιοί είναι:

- Brain
- Monkey
- NYB (γνωστός και ως B1)
- Stoned
- Form
- Michelangelo

Και πολλοί άλλοι.

Τρόποι αντιμετώπισης – αντίμετρα

Ένα μεγάλο πρόβλημα με τους ιούς αυτούς είναι η απομάκρυνσή τους, και αυτό γιατί συχνά είναι δύσκολο για ένα antivirus πρόγραμμα να καθαρίσει το MBR την ώρα που εκτελείται το λειτουργικό σύστημα.

Γενικά η πρόληψη είναι θέμα επαγρύπνησης και αποφυγής επαφής με άγνωστους δίσκους. Πέρα από τα γενικά αντίμετρα που θα αναλυθούν στη συνέχεια υπάρχουν κάποιοι τρόποι για να μειώσουμε την πιθανότητα μόλυνσης από έναν boot sector ιό. Καταρχάς είναι δυνατόν να γίνουν κάποιες ρυθμίσεις στο CMOS (**c**omplementary **m**etal **o**xide **s**emiconductor) ώστε να μην είναι δυνατή η εγγραφή στον boot τομέα του σκληρού δίσκου. Αυτό αν και

μπορεί να βοηθήσει κάπως, είναι πιθανόν να δημιουργήσει προβλήματα (πχ όταν θελήσουμε να ξανα εγκαταστήσουμε το λειτουργικό μας σύστημα). Ακόμη είναι καλό οι διάφοροι removable δίσκοι που χρησιμοποιούμε να είναι κλειδωμένοι (write protected) και να τους χρησιμοποιούμε μόνο σε υπολογιστές που έχουμε βεβαιωθεί ότι είναι ασφαλείς.

Παραδείγματα boot sector ιών

Ο ιός monkey

Ο ιός monkey είναι ένας boot sector ιός που προσβάλλει το Master Boot Record (MBR) του σκληρού δίσκου (αλλά και το boot sector των δισκετών), εμφανίστηκε το 1991 στο Edmonton του Καναδά, και γρήγορα διαδόθηκε στις ΗΠΑ, στην Αυστραλία και την Μεγάλη Βρετανία. Ο monkey είναι εκτός των άλλων **stealth** ιός -από τη στιγμή που καταφέρει να εξαπλωθεί στη μνήμη δεν μπορεί να εντοπιστεί στον σκληρό δίσκο ή σε κάποια δισκέτα. Η απομάκρυνσή του παρακωλύεται περαιτέρω από το γεγονός ότι δεν υπάρχει πρόσβαση στον σκληρό δίσκο αν προσπαθήσουμε να επανεκινήσουμε το σύστημα χρησιμοποιώντας κάποια δισκέτα εκκίνησης αφού λαμβάνουμε μηνύματα του τύπου: “Invalid drive specification”. Ο τρόπος **διάδοσης** του είναι να προσπαθήσουμε να κάνουμε boot το σύστημα με μία δισκέτα που είναι μολυσμένη. Σε αυτή τη περίπτωση αυτό που θα συμβεί είναι ότι θα προσπαθήσει το σύστημα να ξεκινήσει, διαβάζοντας την δισκέτα (για να δει εάν είναι boot δισκέτα) και θα τυπώσει το κλασικό μήνυμα: “Non-system disk or disk error”. Από τη στιγμή αυτή ο ιός έχει εισβάλει στον υπολογιστή – πρώτα στο MBR και έπειτα στη μνήμη. Αυτό που συμβαίνει (σαν σύμπτωμα) σε ένα σύστημα που έχει μολυνθεί από τον ιό πρακτικά είναι ότι όλο το σύστημα και η διαθέσιμη μνήμη μειώνεται κατά 1,024 bytes. Η εκκαθάριση τελικά του ιού μπορεί να γίνει είτε με την χρήση κάποιου αντι-ιικού προγράμματος (αναγκαστικά μέσω κάποιας δισκέτας εκκίνησης) είτε με τη χρήση εργαλείων FDISK (όπως πχ το Norton Disk Doctor) που μπορούν να ξαναφτιάξουν (να κάνουν “rebuild”) το Master Boot Sector. Επίσης είναι δυνατόν να επαναφέρουμε τις αρχικές ρυθμίσεις του πρωτότυπου Master Boot Record και του partition table εάν έχει γίνει backup πριν την μόλυνση.

Ο ιός NYB [ή B1]

Ο ιός NYB (New York boot) είναι ένας τυπικός Boot Sector (εμφανίστηκε κάπου στα τέλη του 1994), ο οποίος μολύνει όπως και ο monkey μόνο αν προσπαθήσουμε να κάνουμε εκκίνηση ενός συστήματος με μία μολυσμένη δισκέτα. Εκείνη τη στιγμή ο ιός περνάει στο Main Boot Record και στη συνέχεια “κατοικεί” στην high dos μνήμη σε κάθε επανεκκίνηση του υπολογιστή. Ο NYB είναι και αυτός ένας stealth ιός οπότε οι διάφορες αλλαγές στο MBR δεν είναι ορατές. Κάθε φορά που έχουμε πρόσβαση στη δισκέτα υπάρχει 1/512 πιθανότητα να ενεργοποιηθεί ο ιός. Τότε υπάρχει η περίπτωση να καταστραφεί η κεφαλή της δισκέτας (και επομένως και η ίδια η

δισκέτα). Τέλος ενδιαφέρον έχει ότι από τους περισσότερους μελετητές των ιών “ξέφυγε”, ένας άλλος τρόπος ενεργοποίησης του. Έτσι το σύστημα μπορεί συντριβή εάν επιχειρηθεί εγγραφή όταν το ρολόι του υπολογιστή έχει όλα τα πεδία μηδέν (όταν δηλαδή είναι μεσάνυχτα).

2. Πολυμορφικοί (Polymorphic) ιοί

Γενικά χαρακτηριστικά

Πολυμορφικός ιός είναι αυτός που παράγει μία μεγάλη ποικιλία από διαφορετικά αντίγραφα του εαυτού του (τα οποία είναι λειτουργικά). Η

Αυτή η στρατηγική υποθέτει ότι το αντι-ιικό πρόγραμμα δεν θα μπορέσει να εντοπίσει όλα τα διαφορετικά στιγμιότυπα του ιού. Ένας τρόπος για την αποφυγή ανίχνευσης είναι η κρυπτογράφηση του εαυτού τους (self-encryption) με ένα μεταβλητό κλειδί. Κάποιοι πιο εξελιγμένοι πολυμορφικοί ιοί (πχ V2p6) ωστόσο αλλάζουν τις ακολουθίες οδηγιών μέσα στις μεταβλητές τους με το να παραβάλουν τις οδηγίες κρυπτογράφησης με “θορυβώδη” (noise) οδηγίες, με το να εναλλάσσουν αμοιβαία ανεξάρτητες οδηγίες, ή ακόμα και με τη χρησιμοποίηση ποικίλων συχνοτήτων οδηγιών με πανομοιότυπα net effects. Μία από τις πιο εξελιγμένες μορφές πολυμορφισμού που χρησιμοποιείται είναι η Dark Angel's Multiple Encryptor (DAME), που εμφανίζεται με μία μορφή object module (άλλες γεννήτριες πολυμορφικότητας είναι οι: MTE, TPE, NED κα). Με τη βοήθειά της, οποιοσδήποτε ιός μπορεί να γίνει πολυμορφικός με το να προσθέσει συγκεκριμένες κλήσεις στον assembly κώδικά του και συνδέοντας τον με την DAME και γεννήτριες τυχαίων αριθμών.

Η εμφάνιση των πολυμορφικών ιών μετέτρεψε την επιστήμη της ανίχνευσης των ιών σε ένα εξαιρετικά **δύσκολο** και **ακριβό** εγχείρημα. Αυτό δεν σημαίνει απαραίτητα ότι οι πολυμορφικοί ιοί είναι οι πιο καταστροφικοί (υπάρχουν απλοί ιοί που μπορούν να σβήσουν όλα τα δεδομένα από τον σκληρό δίσκο (format) ή να δημιουργήσουν μεγάλα προβλήματα στο BIOS). Το μεγάλο πλεονέκτημά τους είναι η δυσκολία εντοπισμού τους. Η απλή πρόσθεση όλο και περισσότερων συμβολοσειρών (strings) αναζήτησης σε απλούς ανιχνευτές είναι προφανές ότι δεν μπορεί πάντα να επιλύσει επαρκώς το πρόβλημα, αφού πλέον είναι δυνατόν να μην υπάρχει ένα συγκεκριμένο string από bytes που να ταυτοποιεί τον ιό.

Μερικοί πολυμορφικοί ιοί είναι:

- Chameleon (από τους πρώτους πολυμορφικούς)
- Bootache
- CivilWar
- Uruguay
- MVF

- Moctezuma
- PcFly

Και διάφοροι άλλοι.

Ας δούμε τον κώδικα ενός “απλού” ιού που κάνει reset έναν ελεγκτή και στην συνέχεια reboot το σύστημα:

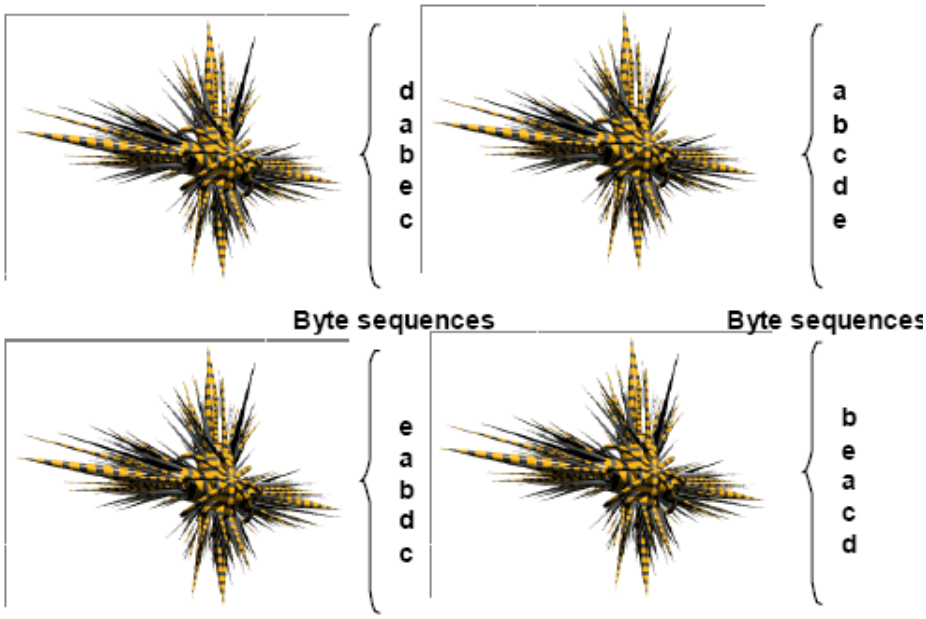
```
00001                                              # reboot.s
00002
00003
00004
00005 0000           8816       0080                    mov 0x80,dl
00006 0004           8826       000D                    mov 0x0d,ah
00007 0008           CD                      13         int 0x13
00008 000A           CD                      19         int 0x19
00009                                                   end
```

Ο ιός αυτός θα έχει ταυτότητα: 88 16 00 80 88 26 00 0d cd 13 cd 19 που είναι 12 bytes. Τώρα προσθέτοντας μερικές εντολές (nop, jump κα) που στην πραγματικότητα δεν κάνουν τίποτα ο κώδικας παίρνει την μορφή:

```
00001                                              # reboot.s
00002
00003
00004
00005 0000           EB           10                    jmp L1
00006 0002           90                                 nop
00007 0003           8826       000D            L2:     mov 0x0d,ah
00008 0007           EB           0F                    jmp L3
00009 0009           90                           L4:     nop
00010 000A           90                                 nop
00011 000B           CD                      13         int 0x13
00012 000D           90                                 nop
00013 000E           90                                 nop
00014 000F           90                                 nop
00015 0010           CD                      19         int 0x19
00016                       00000012>            L1:
00017 0012           8816       0080                    mov 0x80,dl
00018 0016           EB           EB                    jmp L2
00019 0018           88FF                         L3:     mov bh,bh
00020 001A           EB           ED                    jmp L4
00021                                                   end
```

Τώρα αν και ο ιός έχει την ίδια λειτουργία η υπογραφή του έχει γίνει πλέον τελείως διαφορετική: eb 10 90 88 26 00 0d eb 0f 90 90 cd 13 90 90 90 cd 19 88 16 00 80 88 ff eb ed. Βλέπουμε λοιπόν πόσο εύκολο είναι να δημιουργήσουμε πολλές διαφορετικές υπογραφές, δημιουργώντας έτσι έναν απλό πολυμορφικό ιό.

Παρακάτω βλέπουμε πως θα μπορούσαμε να απεικονίσουμε έναν πολυμορφικό ιό που μεταλλάσσεται



Τρόποι αντιμετώπισης – αντίμετρα

Οι τρόποι που χρησιμοποιούνται από τα διάφορα αντι-ιικά προγράμματα για την ανίχνευση πολυμορφικών ιών ποικίλουν. Οι συνηθέστεροι είναι :

- Scan Strings
- Variable Scan Strings
- Cryptanalysis
- Generic Decryptor
- Heuristic analysis

Το απλό **Scan String** (αναζήτηση συμβολοσειράς) είναι η ανίχνευση για συγκεκριμένες ακολουθίες από bytes.

Πχ.

το scan string που είναι της μορφής: aa ?? bb ?? cc
μπορεί να εντοπίσει ιούς μόνο της μορφής: aa xx bb xx cc

Το **Variable Scan String** (μεταβλητή αναζήτηση συμβολοσειράς) είναι μία βελτίωση του παραπάνω που λειτουργεί με δυναμικό τρόπο.

Πχ. το scan string που είναι της μορφής: aa * bb * cc

Μπορεί να εντοπίζει ιούς των μορφών: aa xx xx bb xx xx xx xx cc
ή
aa bb xx xx xx cc
κτλ.

Η κρυπτανάλυση (**Cryptanalysis**) λειτουργεί με το να εντοπίζει ένα μέρος από το σώμα του ιού, να εκτελεί μία βασική κρυπτανάλυση πάνω σε αυτό και τελικά εάν είναι επιτυχής να τον εντοπίζει.

Το **Generic Decryptor** (Γενικός Αποκρυπτογράφος) λειτουργεί με το να προσομοιώνει οδηγίες σε έναν πολυμορφικό αποκρυπτογράφο με σκοπό να αναγκάσει τον ιό να αποκρυπτογραφηθεί μόνος του και στην συνέχεια τον εντοπίζει με μία απλή αναζήτηση συμβολοσειράς.

Η **Heuristic analysis** –ευριστική ανάλυση- (από τα πιο δυνατά όπλα των αντι-ιικών προγραμμάτων) αναζητούν αντιφατικότητες μεταξύ του κώδικα που αναλύεται και του κώδικα που πρέπει να έχει κανονικά ένα πρόγραμμα.

Παραδείγματα πολυμορφικών ιών

Ο MVF ιός

Ο MVF (ή και Arkanoid) είναι ένας πολυμορφικός ιός που εμφανίστηκε το 1992 στη Ρωσία, και έχει σαν στόχο τα .COM αρχεία (συμπεριλαμβανομένου του COMMAND.COM). Από τη στιγμή που ένα μολυσμένο πρόγραμμα εκτελεστεί ο MVF εγκαθίσταται στην μνήμη ως TSR (**t**erminate and **s**tay **r**esident). Από τη στιγμή που βρίσκεται ο ιός στη μνήμη θα μολύνει κάθε .COM πρόγραμμα που εκτελείται. Προγράμματα μολυσμένα με τον ιό θα έχουν μία αύξηση μεγέθους της τάξης των 1,898 με 1,909 bytes με τον MVF να βρίσκεται στο τέλος του αρχείου. Αξιοσημείωτο είναι ότι μέσα στον κώδικα του ιού βρίσκεται κρυπτογραφημένο το παρακάτω κείμενο (το οποίο δεν εμφανίζεται στα μολυσμένα αρχεία):

"????????COM"
"THE MVF-FILEVIRUS"
"Programmed 1991 by the MVF"
"MAD Virus Factory"
"No.0001"
".COM"*

Στα συστήματα στα οποία έχει εισχωρήσει ο MVF είναι πιθανόν να παρατηρούνται καθυστερήσεις στην εκτέλεση .COM αρχείων (αυτό συμβαίνει πολύ συχνά όταν έχει μολυνθεί το COMMAND.COM).

3. Οι Macro ιοί

Γενικά χαρακτηριστικά

Γενικά, οι **μακρο εντολές** μπορούν να χρησιμοποιηθούν σε προγράμματα όπως το Word και το Excel, για να αυτοματοποιήσουν σύνθετους ή επαναλαμβανόμενους στόχους. Μόλις γραφτούν, ορίζεται σε αυτές ένας συνδυασμός πλήκτρων, ή κάποιο κουμπί από μία εργαλειοθήκη που θα ενεργοποιεί την μακρο εντολή.

Οι μακρο εντολές αποθηκεύονται σαν μία σειρά οδηγιών σε μία γλώσσα όπως η visual basic. Από τη στιγμή που καταγραφεί μια μακρο εντολή ο χρήστης μπορεί να την επεξεργαστεί ή ακόμα και να προσθέσει πιο περίπλοκες εντολές που δεν είναι κανονικά εγγράψιμες. Αυτό δίνει στον έμπειρο χρήστη τη δυνατότητα όχι μόνο να αυτοματοποιήσει λειτουργίες μέσα στο πρόγραμμα αλλά και να εκτελεί βασικές εντολές του συστήματος όπως διαγραφή, μετονομασία, ή αλλαγή των ιδιοτήτων αρχείων.

Ένας **μακρο ιός** χρησιμοποιεί την δύναμη και την λειτουργικότητα των μακροεντολών για να δημιουργήσει αντίγραφα του εαυτού του και για να διαδοθεί. Όταν ένας χρήστης λαμβάνει και ανοίγει ένα αρχείο που περιέχει έναν μακροϊό, αυτός (ο ιός) είτε θα εκτελεστεί αυτόματα είτε από τον συνδυασμό κάποιων πλήκτρων, την εκτέλεση κάποιας εντολής από το menu επιλογών, το πάτημα κάποιου κουμπιού μιας εργαλειοθήκης κα. Στη συνέχεια ο ιός θα αντιγραφτεί στο σύστημα (ο τρόπος μπορεί να ποικίλει ανάλογα με τις λεπτομέρειες του ιού). Ο macro ιός θα είναι παρών πλέον στα αρχεία που ανοίγει ο χρήστης και μπορεί να μεταδοθεί με πολλούς διαφορετικούς τρόπους. Μερικά πολύ επικίνδυνα πράγματα που μπορεί να κάνει ένας τέτοιος ιός είναι να διαγράψει/τροποποιήσει τα περιεχόμενα ενός κειμένου, να αλλάξει τις ρυθμίσεις του Word, να τοποθετήσει κωδικό πρόσβασης, να αντιγράψει έναν DOS ιό στο σύστημα ή και να παρεμβάλει επιβλαβής γραμμές κώδικα στα αρχεία config.sys και autoexec.bat.

Θεωρητικά ένας μακρο ιός μπορεί να γραφτεί για οποιοδήποτε πρόγραμμα που αποθηκεύει μακρο εντολές σε μορφή που μπορεί να ανοιχτεί και να επεξεργαστεί χρησιμοποιώντας μία γλώσσα όπως Word Basic και Visual Basic. Στην πράξη ωστόσο οι περισσότεροι που έχουν βρεθεί αφορούν κυρίως το Word και το Excel.

Μία άλλη ενδιαφέρουσα ιδιότητα των μακροϊών είναι ότι μπορούν ενδεχομένως να διαδίδονται σε διαφορετικές πλατφόρμες, όπως από Mac σε PC κα. Οι macro ιοί υφίστανται και μεταδίδονται μέσα στο περιβάλλον κάθε εφαρμογής το οποίο για τις μακρο εντολές είναι κοινό στις διαφορετικές πλατφόρμες. Οι διάφοροι ιοί που προσπαθούν να προκαλέσουν ζημιά σε ένα μέρος του συστήματος του χρήστη έξω από το word δεν θα είναι σε θέση να κάνουν το ίδιο πράγμα σε μία διαφορετική πλατφόρμα (Πχ. ένας μακρο ιός που προσπαθεί να επεξεργαστεί το αρχείο config.sys του χρήστη σε ένα pc

θα δυσκολευτεί να κάνει το ίδιο πράγμα σε έναν Mac, ο οποίος δεν έχει κανένα αρχείο Config.sys.). Συνοψίζοντας δηλαδή ένας μακρο ιός που διαδίδεται και μπορεί να προκαλεί βλάβες σε ένα σύστημα, μπορεί να διαδίδεται σε κάποιο άλλο, αλλά να μην προκαλεί κάποια βλάβη. Υπάρχει η δυνατότητα βέβαια ένας macro ιός να βρίσκει/εντοπίζει σε ποιο σύστημα τρέχει (αν είναι pc,mac ή κάτι άλλο) και να αλλάζει την συμπεριφορά του ανάλογα, όμως κάτι τέτοιο δεν είναι σύνηθες.

Μερικοί μακρο ιοί είναι:

- Concept (από τους πρώτους που εμφανίστηκαν -1995
- Melissa
- DMV
- Nuclear
- NiceDay
- Groov

Τρόποι αντιμετώπισης – αντίμετρα

Όταν τον Αύγουστο του 1995 έκανε την εμφάνιση του ο πρώτος μακρο ιός -στην πραγματικότητα δεν ήταν ο πρώτος, αφού κάποιες αντι-ιικές εταιρίες είχαν πειραματικά δημιουργήσει ιούς που μεταδίδονταν από ένα κείμενο στο άλλο, ωστόσο σχεδόν κανείς δεν ενδιαφέρθηκε για αυτό το μάλλον αποτυχημένο πείραμα- η αντι-ιική κοινότητα βρέθηκε απροετοίμαστη. Αξιοσημείωτο μάλιστα είναι ότι αν παρατηρούσε κανείς την τότε βιβλιογραφία σε σχέση με τους ιούς θα έβλεπε ότι στην ερώτηση, *αν μπορεί ένα κείμενο να περιέχει κάποιον ιό,* η απάντηση ήταν απλή: ΟΧΙ. Έτσι η πρώτη βιαστική αντιμετώπιση της επιδημίας μακρο ιών που προέκυψε ήταν η δημιουργία άλλων ιών που μεταδίδονταν από κείμενο σε κείμενο και έσβηναν τις κακόβουλες μακρο εντολές. Οι τρόποι για την ανίχνευση των μακρο ιών πλέον ποικίλουν. Ένας πολύ απλός είναι με την ανίχνευση του ονόματος του ιού. Επίσης επειδή ένα μεγάλο μέρος των νέων ιών που κυκλοφορούν είναι ουσιαστικά “αλλαγμένες” εκδόσεις παλιών, είναι δυνατόν να γίνεται η ανίχνευση με βάση το βασικό σώμα ενός ιού. Τέλος χρησιμοποιείται και η ευριστική ανάλυση που είδαμε παραπάνω.

Παραδείγματα μακρο ιών

Ο ιός Concept

Ο ιός concept εμφανίστηκε για πρώτη φορά το 1995 και είχε σαν στόχους το Microsoft word (windows) 6.x και 7.x, το word for macintosh 6.x καθώς και τα ίδια τα λειτουργικά συστήματα windows 95 και windows nt. Ο ιός εκτελείται κάθε φορά που ανοίγει ένα μολυσμένο έγγραφο και προσπαθεί να μολύνει το NORMAL.DOT. Αν εντοπίσει κάποια από τις μακρο εντολές “payload” ή “filesaveas” υποθέτει ότι ο ιός υπάρχει ήδη οπότε σταματάει την λειτουργία

του. Αν όμως δεν βρει τις παραπάνω εντολές τότε αρχίζει να γράφει τις κακόβουλες εντολές και εμφανίζει ένα μικρό μήνυμα στην οθόνη:

Το μήνυμα αυτό εμφανίζεται μόνο κατά την αρχική μόλυνση του NORMAL.DOT. Από τη στιγμή αυτή ο ιός περνάει σε κάθε κείμενο που δημιουργήθηκε με την “Save As” εντολή. Ο concept αποτελείται από τις ακόλουθες μακρο εντολές:

AAAZAO
AAAZFS
AutoOpen
FileSaveAs
PayLoad

Να παρατηρήσουμε εδώ ότι η AutoOpen και η FileSaveAs είναι ονόματα που υπάρχουν και υπό φυσιολογικές συνθήκες στο word. Το PayLoad που βλέπουμε παραπάνω περιέχει το εξής κείμενο:

```
Sub MAIN
        REM That's enough to prove my point
End Sub
```

Το οποίο δεν εκτελείται ποτέ.

Ο ιός Melissa

Ο ιός Melissa έκανε την εμφάνισή του την Παρασκευή 26 Μαρτίου 1999 και μπόρεσε να διαδοθεί σε ολόκληρο τον κόσμο μέσα σε μερικές ώρες –κάτι που δεν είχε ξανασυμβεί μέχρι τότε. Εξαπλώθηκε με το να στέλνει αυτόματα σε email τον εαυτό του από τον ένα χρήστη στον άλλο. Όταν ο ιός ενεργοποιηθεί τροποποιεί τα έγγραφα του χρήστη παρεμβάλλοντας κάποια σχόλια από μία γνωστή τηλεοπτική σειρά (“The Simpsons”). Ανησυχητικό είναι το γεγονός ότι μπορεί να στείλει και εμπιστευτικές πληροφορίες ενός χρήστη σε έναν άλλο. Ο ιός “χτύπησε” μεγάλους οργανισμούς όπως η Microsoft και η Intel – η Microsoft μάλιστα αναγκάστηκε να κλείσει τελείως το σύστημα ηλεκτρονικού ταχυδρομείου της για να σταματήσει την περεταίρω εξάπλωση του ιού.

Ο Melissa αρχικά μεταδόθηκε σε φόρουμ συζητήσεων (alt.sex). Ο ιός εστάλη στους χρήστες με το όνομα LIST.DOC που περιείχε κωδικούς πρόσβασης από ιστοσελίδες που είχαν χαρακτηριστεί X-rated (σεξουαλικού περιεχομένου). Όταν κάποιος άνοιγε το αρχείο, ο μακρο ιός εκτελείτο και έστελνε το LIST.DOC με email σε 50 άτομα από το address book του χρήστη.

Το email είχε την μορφή:

From: (name of infected user)
Subject: Important Message From (name of infected user)
To: (50 names from alias list)

Here is that document you asked for ... don't show anyone else ;-)
(Attachment: LIST.DOC)

Ο Melissa ενεργοποιείται αν εκτελεστεί τα λεπτά από το ρολόι του συστήματος συμπίπτουν με την ημερομηνία (πχ 18:27 στις 27 κάποιου μήνα).Σε αυτή τη περίπτωση ο ιός παρέμβαλλε στα κείμενα του μολυσμένου υπολογιστή το παρακάτω κείμενο:

"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here". This text, as well as the alias name of the author of the virus, "Kwyjibo", are all references to the popular cartoon TV series called "The Simpsons".

Γενικά αντίμετρα

Υπάρχουν μερικοί τρόποι για να μειώσουμε την πιθανότητα να “κολλήσει” το σύστημά μας έναν ιό και να αυξήσουμε το ενδεχόμενο να καθαρίσει “σωστά” εάν προσβληθεί.

- Εγκατάσταση ενός καλού **αντι-ιικού προγράμματος**, τακτική ενημέρωσή του και ένας τουλάχιστον έλεγχος του συστήματος κάθε εβδομάδα

Εδώ πρέπει να σημειωθεί ότι ένα πρόγραμμα που είναι δημοφιλές **δεν** είναι και απαραίτητα καλό –υπάρχουν άλλοι παράγοντες όπως πόσο συχνά ενημερώνεται για νέους ιούς, εάν χρησιμοποιεί όλες τις σύγχρονες μεθόδους ανίχνευσης ιών κα.

- Δημιουργία **backup** αρχείων

Πολύ σημαντικό αφού μας εγγυάται την ασφάλεια των δεδομένων μας και για άλλα –εκτός των ιών- ενδεχόμενα (πρόβλημα με τον σκληρό δίσκο κτλ)

- Χρήση κάποιου **Firewall**

- **Ενημέρωση** των χρηστών ενός συστήματος για τον κίνδυνο των ιών και το πώς μπορούν να προφυλαχθούν

- Χρήση πιο **ασφαλών λειτουργικών συστημάτων**

Είναι **γεγονός** ότι οι περισσότεροι δημιουργοί ιών στοχεύουν κατά του λογισμικού της Microsoft. Στατιστικά το 2001 υπήρχαν περίπου **60,000 windows** ιοί, περίπου 5 για εμπορικές Unix εκδόσεις, και γύρω στους **40** για **Linux**.

References

1. Wikipedia
http://en.wikipedia.org

2. Indiana University – Information Knowledge Base
http://kb.iu.edu

3. Mark Ludwig: The giant black book of computer viruses

4. Webopedia
http://www.webopedia.com

5. McAfee: Virus Information Library
http://vil.nai.com

6. F-Secure: Security Information Center
http://www.f-secure.com

7. Jess Silverman: Understanding Polymorphic Viruses
http://www.commercialventvac.com/~jeffs

7. Rogue Warrior: Guide to improving Polymorphic Engines

8. Scott Grannerman, Security Focus: Linux vs Windows Viruses

9. Dr Nic Peeling and Dr Julian Satchell: Analysis of the Impact of open Source Software