Ομάδα Εργασίας IA4

Προπαρασκευαστικές δράσεις για την δημιουργία Ελληνικού Κέντρου Επείγουσας Αντιμετώπισης Ψηφιακών Απειλών (GR-CERT)

Στέφανος Γκρίτζαλης
Διομήδης Σπινέλης
Πέτρος Μπέλσης
Βασίλης Βλάχος

Ατζέντα

- Η ομάδα IA4
- Σύγχρονες Απειλές
- Διεθνής Εμπειρία
- Ελληνική Εμπειρία
- GR-CERT
- Οδικός Χάρτης

Η ομάδα εργασίας IA4

Συντονιστές

Στέφανος Γκρίτζαλης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

Διομήδης Σπινέλης

Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Οικονομικό Πανεπιστήμιο Αθηνών

Rapporteurs

Πέτρος Μπέλσης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

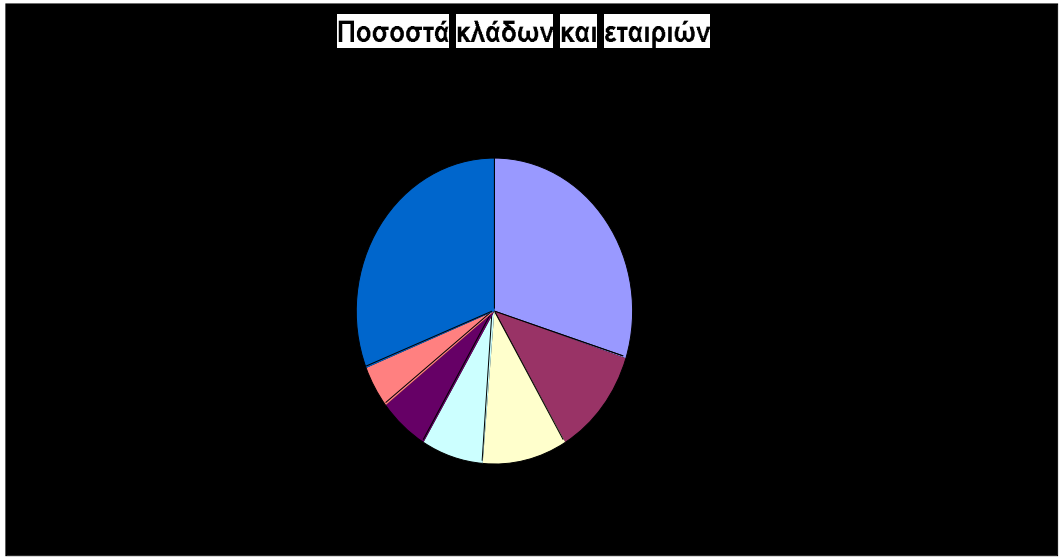
Βασίλης Βλάχος – Ιωάννα Ματζουράτου

Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας

Οικονομικό Πανεπιστήμιο Αθηνών

Η ομάδα IA4

Στατιστικά στοιχεία



Κλάδοι και εταιρίες	Ποσοστό
Πανεπιστημιακός χώρος	30%
Εταιρίες τηλεπικοινωνιών	11.50%
Τραπεζικός κλάδος	10%
Εταιρίες Πληροφορικής	7%
Κυβερνητικοί Οργανισμοί	6%
Νομικός τομέας	4.50%
Άλλες εταιρίες και ιδρύματα	31%

Σύγχρονες Απειλές

- Κακόβουλο Λογισμικό
  - Ιοί, Worms, Δούρειοι Ίπποι κλπ
- Απάτες
  - Νιγηριανή απάτη ή 4-1-9
- Κλοπή Ταυτότητας
- Κυβερνοεκβιασμοί
- Κυβερνοτρομοκρατία
- Κυβερνοπόλεμος

Σύγχρονες Απειλές

Κυβερνοπόλεμος

Κυβερνοτρομοκρατία

Κυβερνοαπάτες

Κρίσιμες υποδομές κοινής ωφέλειας
Οικονομικά ιδρύματα
Μ.Μ.Ε
Τηλεπικοινωνίες
Κυβερνητικά – στρατιωτικά συστήματα

Εκβιασμοί
Βιομηχανική κατασκοπία
Προσωπικά δεδομένα
Spam
Οικονομικές απάτες

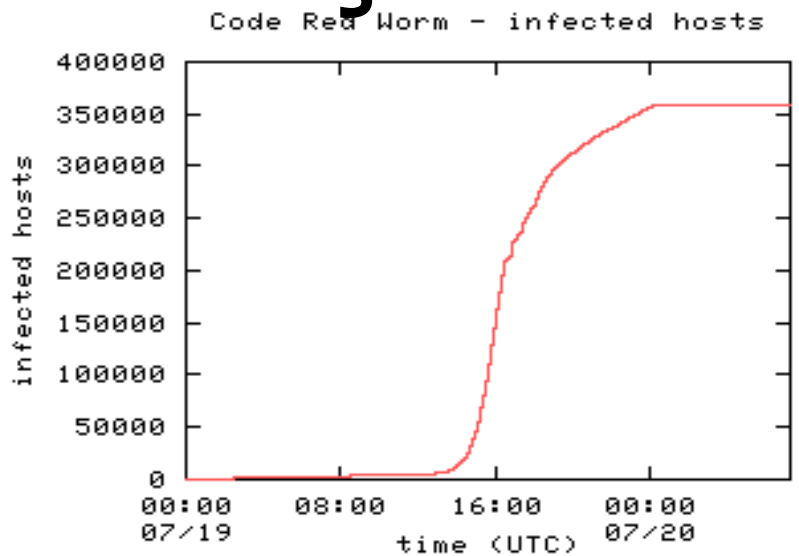
Σύγχρονες Απειλές

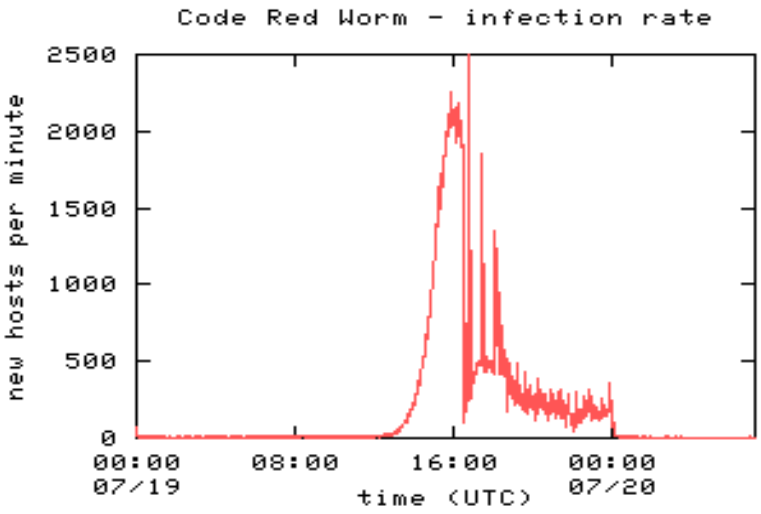
Code Red v1

- Λόγω προβλήματος στην γεννήτρια ψευδοτυχαίων αριθμών εξαπλώθηκε περιορισμένα

Code Red v2

- Προσέβαλε **359.000** συστήματα σε **14** ώρες
- Μέγιστος ρυθμός επιτυχούς προσβολής στόχων **2000** συστήματα ανά ’
- Ρυθμός ανίχνευσης νέων στόχων από κάποιο προσβεβλημένο σύστημα είναι **11** ανιχνεύσεις ανά ”
- Μη καταστροφικό φορτίο
- Εξαπέλυσε **DDOS** επίθεση κατά του δικτυακού τόπου του Λευκού Οίκου
- Ο μολυσμένος πληθυσμός διπλασιάζεται κάθε **37’**

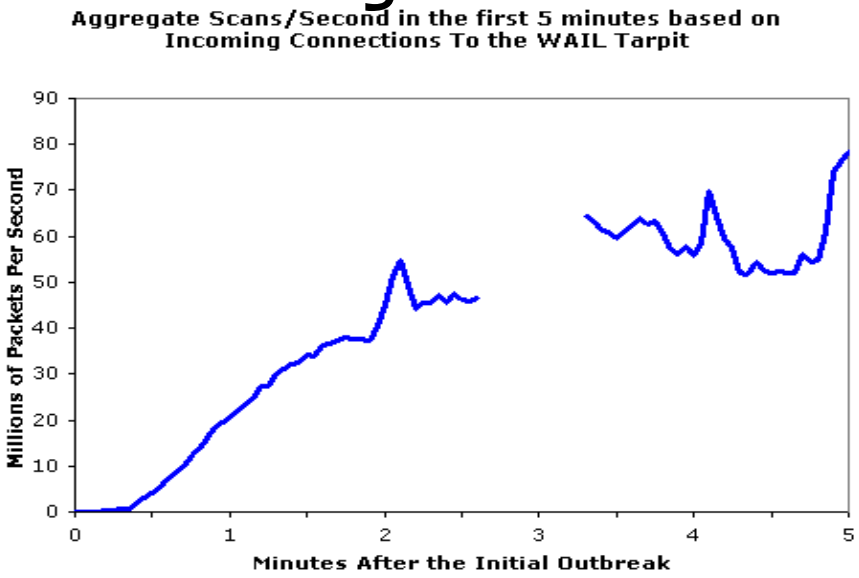


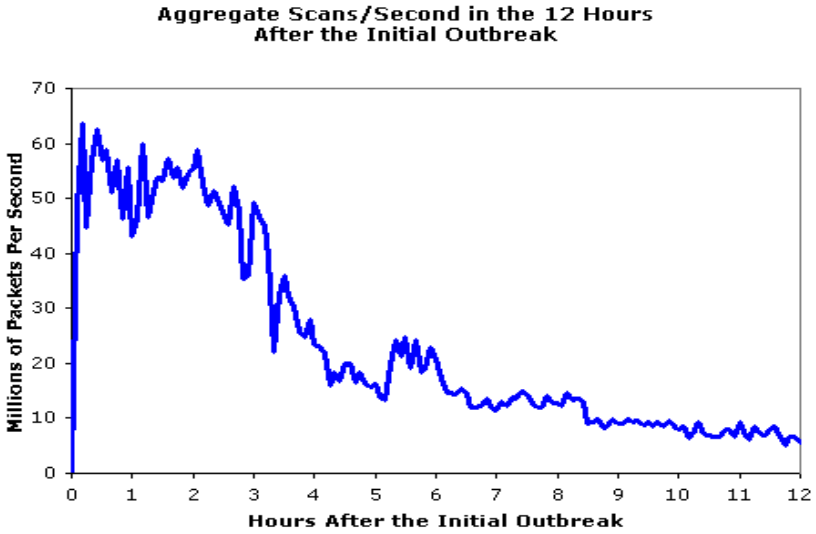


Σύγχρονες Απειλές

Saphire/Slammer

- Τα περισσότερα ευπαθή συστήματα (90%) μολύνθηκαν τα πρώτα 10′ από την εμφάνιση του δικτυακού σκουληκιού
- Ο μολυσμένος πληθυσμός διπλασιάζεται κάθε 8.5″
- Μέγιστος ρυθμός ανιχνεύσεων 55.000.000 ανά ″ και 4000 ανά ″ ανά δικτυακού σκουληκιού
- Τουλάχιστον 75.000 συστήματα μολύνθηκαν ακυρώνοντας πτήσεις, διακόπτοντας την λειτουργία ATM και τμημάτων του Internet. Δεν μετέφερε καταστροφικό φορτίο

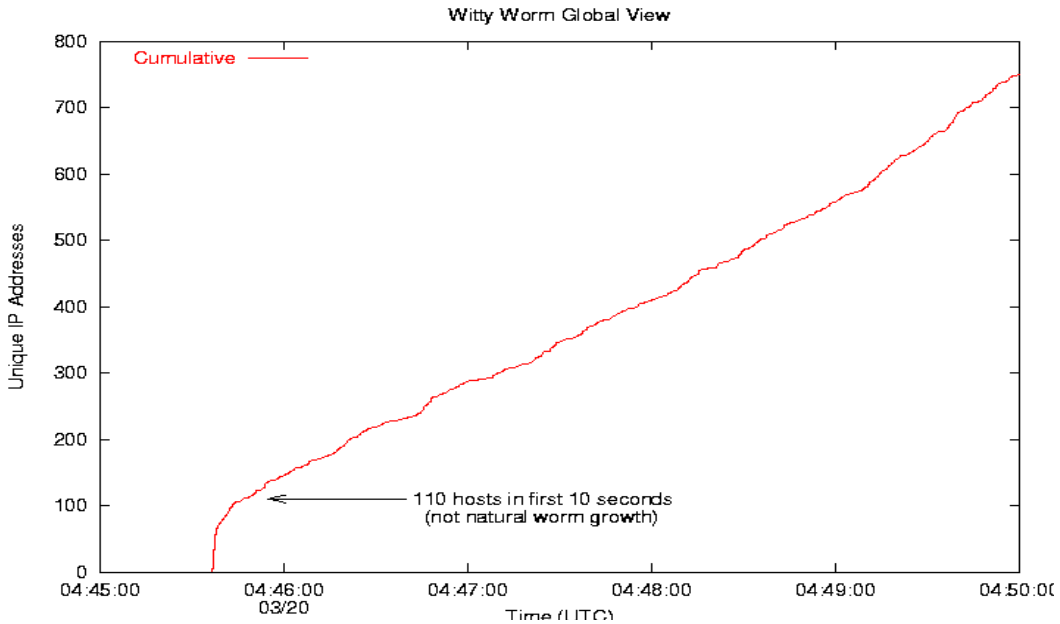


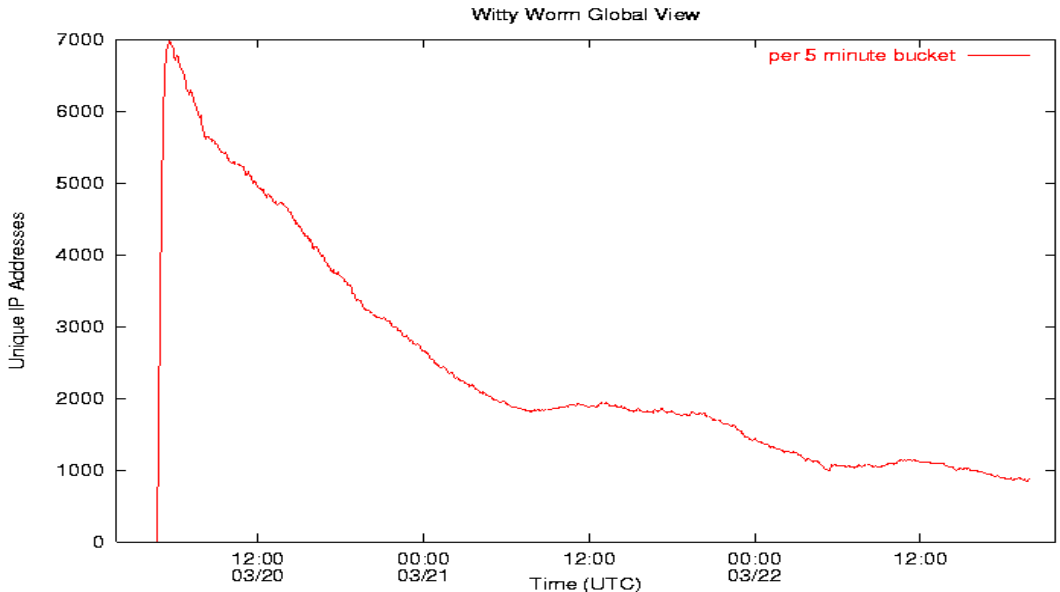


Σύγχρονες Απειλές

Witty (19/03/04)

- Φέρει καταστροφικό φορτίο
- 1 μέρα μετά την ανακοίνωση της αδυναμίας ασφαλείας
- Στόχευε σε επαρκώς προστατευμένα συστήματα
- Ξεκίνησε με οργανωμένο τρόπο χρησιμοποιώντας κάποια λίστα στόχων (110-160)
- Το σύνολο του ευάλωτου πληθυσμού(12000 PCs) μολύνθηκε σε 45’





Σύγχρονες Απειλές

Nimda (18/09/01)

- Προσβάλει εξυπηρετητές δικτύου (**web servers**)
- Εξαπλώνεται μέσω ηλεκτρονικού ταχυδρομείου
- Χρησιμοποιεί κοινόχρηστα δίκτυα (**network shares**)
- Τοποθετεί κακόβουλο κώδικα στις σελίδες των εξυπηρετητών που έχει προσβάλλει
- Χρησιμοποιεί κερκόπορτες άλλων εφαρμογών (**Code Red**)

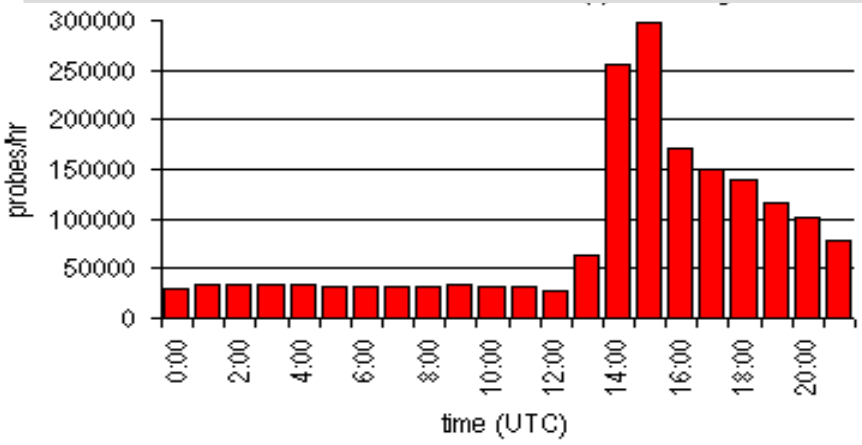
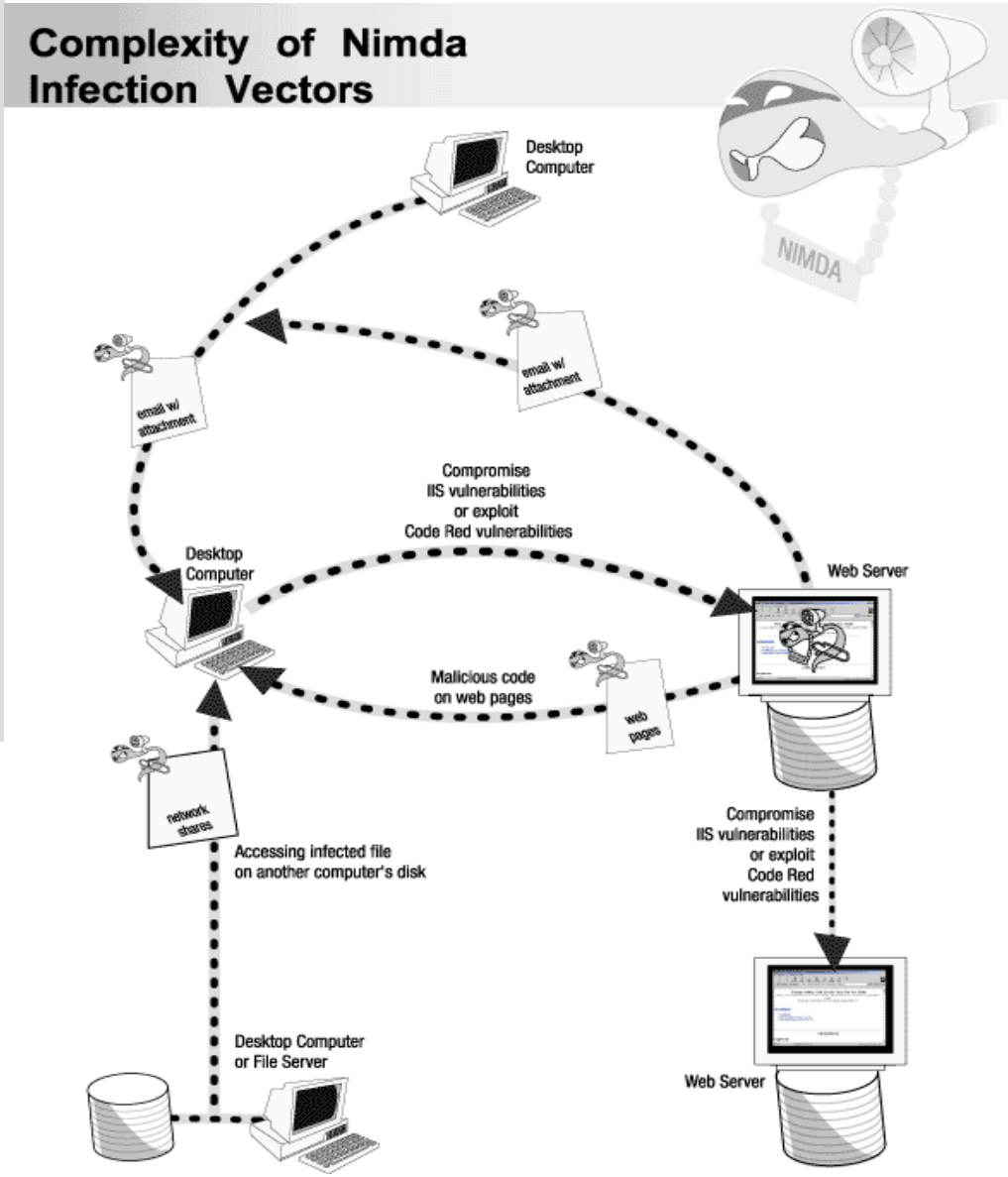


Figure 3: Port 80 probes / hr for September 18th. Time in UTC.



Σύγχρονες Απειλές

Λάθρα σκουλήκια

Επιφέρουν ελάχιστο επιπλέον φόρτο στο Internet και ανιχνεύονται εξαιρετικά δύσκολα

Ιδανικά για εφαρμογές διαμοιρασμού αρχείων σε περιβάλλον ομότιμων δικτύων

Gnuman και άλλα 25 σκουλήκια για ομότιμα δίκτυα

Σύγχρονες Απειλές

Warhol Worms

Στο μέλλον ο καθένας θα είναι διάσημος για *15'*

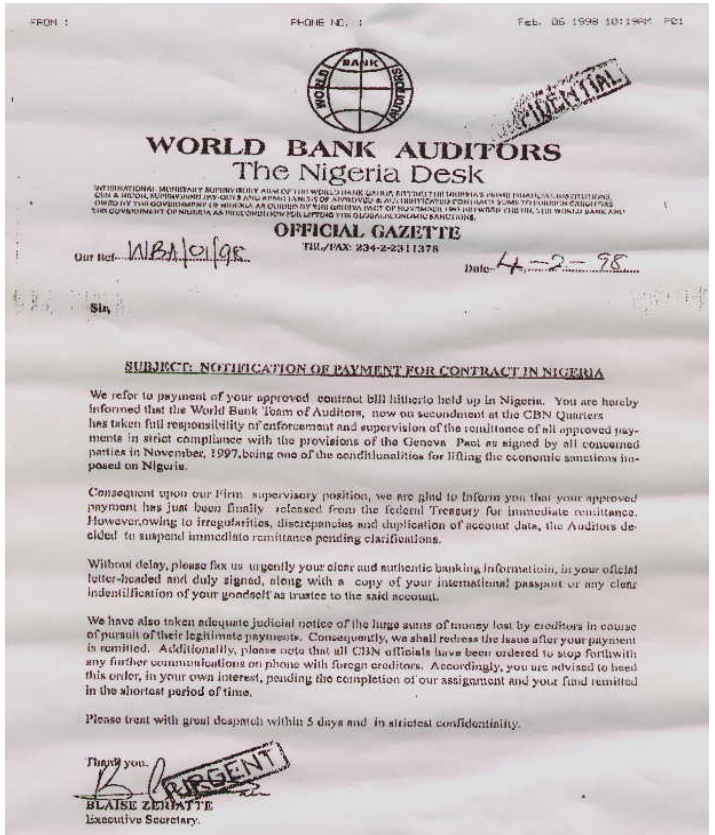
Andy Warhol, 1979

Flash Worms: Ένα σκουλήκι τύπου Flash θα μπορούσε να μολύνει όλους τους ευπαθείς εξυπηρετητές του διαδυκτίου σε λιγότερο από 1'

Σύγχρονες Απειλές

Νιγηριανή απάτη (ή 4-1-9)

- Κυρίως από εγκληματικές ομάδες στην Αφρική
- Συμμετοχή κρατικών αξιωματούχων
- Απαγωγές – Απειλές



WORLD BANK AUDITORS
The Nigeria Desk
OFFICIAL GAZETTE
TEL./FAX: 234-2-2311378

Our Ref. WBA/01/98 Date 4-2-98

Sir,

SUBJECT: NOTIFICATION OF PAYMENT FOR CONTRACT IN NIGERIA

We refer to payment of your approved contract bill hitherto held up in Nigeria. You are hereby informed that the World Bank Team of Auditors, now on secondment at the CBN Quarters has taken full responsibility of enforcement and supervision of the remittance of all approved payments in strict compliance with the provisions of the Geneva Pact as signed by all concerned parties in November, 1997, being one of the conditionalities for lifting the economic sanctions imposed on Nigeria.

Consequent upon our Firm supervisory position, we are glad to inform you that your approved payment has just been finally released from the federal Treasury for immediate remittance. However, owing to irregularities, discrepancies and duplication of account data, the Auditors decided to suspend immediate remittance pending clarifications.

Without delay, please fax us urgently your clear and authentic banking information, in your official letter-headed and duly signed, along with a copy of your international passport or any clear indentification of your goodself as trustee to the said account.

We have also taken adequate judicial notice of the huge sums of money lost by creditors in course of pursuit of their legitimate payments. Consequently, we shall redress the issue after your payment is remitted. Additionally, please note that all CBN officials have been ordered to stop forthwith any further communications on phone with foreign creditors. Accordingly, you are advised to heed this order, in your own interest, pending the completion of our assignment and your fund remitted in the shortest period of time.

Please treat with great despatch within 5 days and in strictest confidentiality.

Thank you.

BLAISE ZERATTE
Executive Secretary.

CONFIDENTIAL

URGENT

Σύγχρονες Απειλές

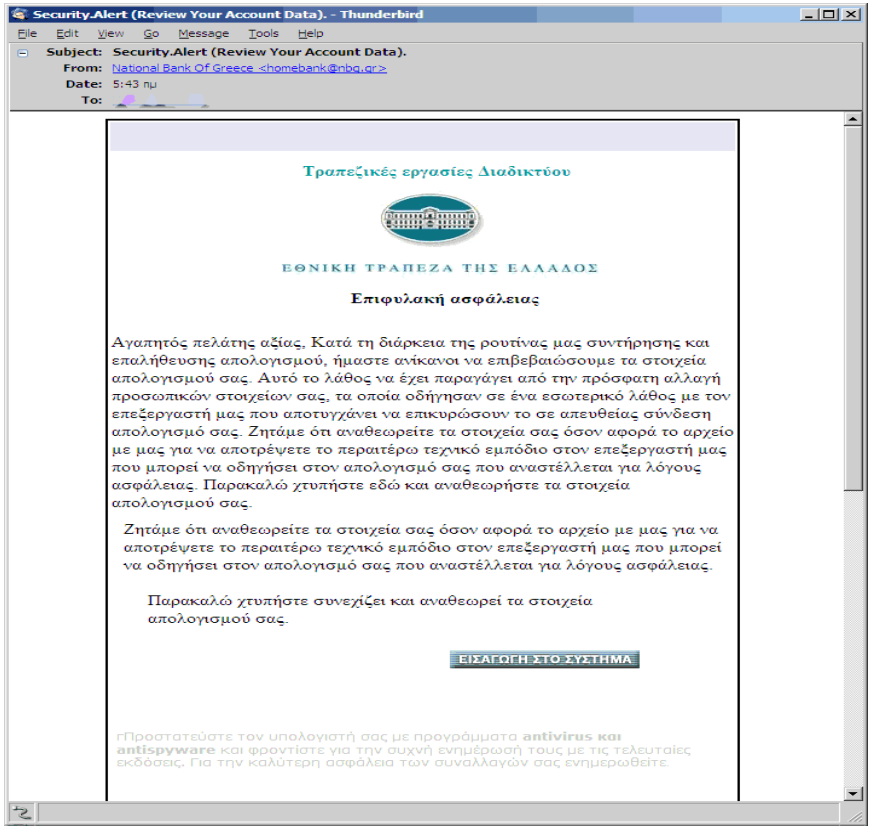
- Χρηματιστηριακές απάτες (Pump and Dump)

- Εμπορικές απάτες

Σύγχρονες Απειλές

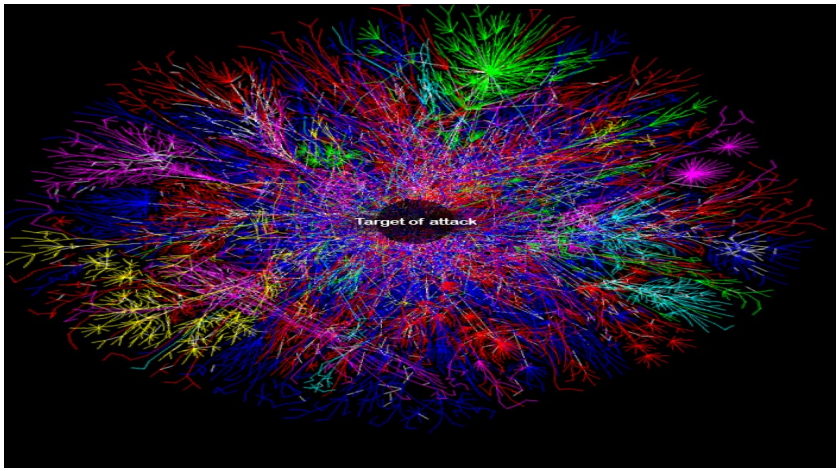
Phishing

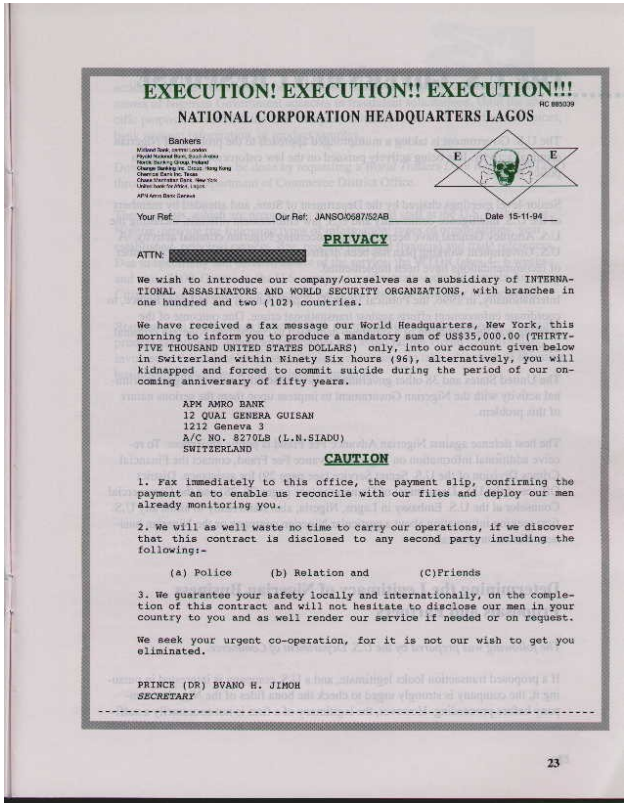
- Ελλάδα (κυριώς τράπεζες)
- Εξωτερικό (δημοπρασίες, τράπεζες, ηλεκτρονικές πληρωμές)



Σύγχρονες Απειλές

Φυσικές Απειλές και Κυβερνοεκβιασμοί(DDoS)





EXECUTION! EXECUTION!! EXECUTION!!!

NATIONAL CORPORATION HEADQUARTERS LAGOS

Bankers

Your Ref:_____ Our Ref: JANSO/0687/52AB_____ Date 15-11-94___

PRIVACY

ATTN: [redacted]

We wish to introduce our company/ourselves as a subsidiary of INTERNATIONAL ASSASINATORS AND WORLD SECURITY ORGANIZATIONS, with branches in one hundred and two (102) countries.

We have received a fax message our World Headquarters, New York, this morning to inform you to produce a mandatory sum of US$35,000.00 (THIRTY-FIVE THOUSAND UNITED STATES DOLLARS) only, into our account given below in Switzerland within Ninety Six hours (96), alternatively, you will kidnapped and forced to commit suicide during the period of our oncoming anniversary of fifty years.

APM AMRO BANK
12 QUAI GENERA GUISAN
1212 Geneva 3
A/C NO. 8270LB (L.N.SIADU)
SWITZERLAND

CAUTION

1. Fax immediately to this office, the payment slip, confirming the payment an to enable us reconcile with our files and deploy our men already monitoring you.

2. We will as well waste no time to carry our operations, if we discover that this contract is disclosed to any second party including the following:-

(a) Police (b) Relation and (C)Friends

3. We guarantee your safety locally and internationally, on the completion of this contract and will not hesitate to disclose our men in your country to you and as well render our service if needed or on request.

We seek your urgent co-operation, for it is not our wish to get you eliminated.

PRINCE (DR) BVANO H. JIMOH
SECRETARY

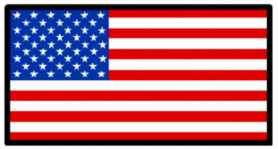
23

Διεθνής Εμπειρία

Morris Worm (1988)

- Προσέβαλλε 6.000 υπολογιστές (10% ARPANET)
- Σημαντικές δυσκολίες αντιμετώπισης του
- Οδήγησε στη δημιουργία του πρώτου CERT

Διεθνής Εμπειρία

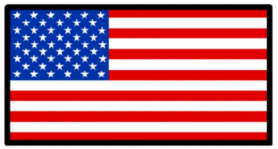


Carnegie Mellon University - CERT/CC

- Υπεύθυνο για τον συντονισμό των ειδικών κατά τη διάρκεια επειγόντων περιστατικών ασφάλειας (DARPA)
- US – CERT (09/ 2003) Department of Homeland Security-Cert/CC
- Υδρυτικό μέλος του FIRST (Forum of Incident Response and Security Teams)
- Συμβουλεύει κυβερνητικούς ηγέτες, επιτροπές του Κογκρέσου και άλλους φορείς (National Threat Assessment Center, National Security Council, Homeland Security Council, Office of Management and Budget / General Services Administration Electronic Government Initiatives κ.α)

CarnegieMellon Software Engineering Institute CERT®Coordination Center

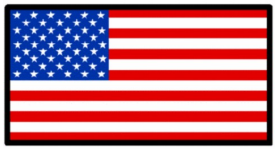
Διεθνής Εμπειρία



Αποστολή του CERT/CC είναι:

- Παροχή αξιόπιστου, σε συνεχή λειτουργία, κοινού σημείου επικοινωνίας για επείγοντα περιστατικά
- Γέφυρα μεταξύ των ειδικών που συνεργάζονται για την επίλυση προβλημάτων ασφάλειας
- Λειτουργία ως κεντρικού σημείου για την αναγνώριση και κάλυψη ευπαθειών στα υπολογιστικά συστήματα
- Διεξαγωγή έρευνας για βελτίωση της ασφάλειας των υπαρχόντων συστημάτων
- Εκπαίδευση, ενημέρωση των χρηστών και παροχή πληροφοριών

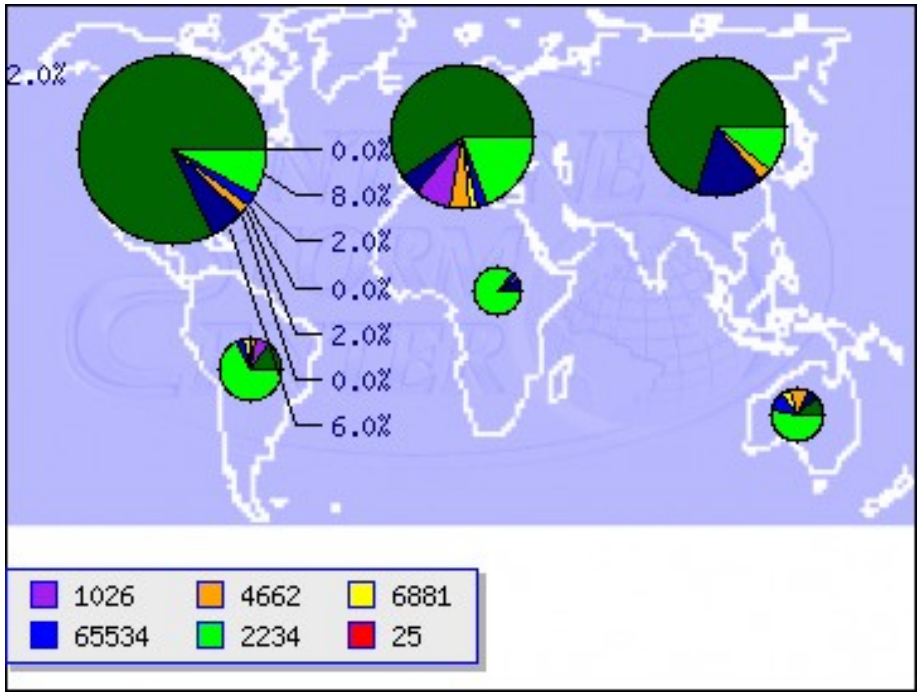
Διεθνής Εμπειρία

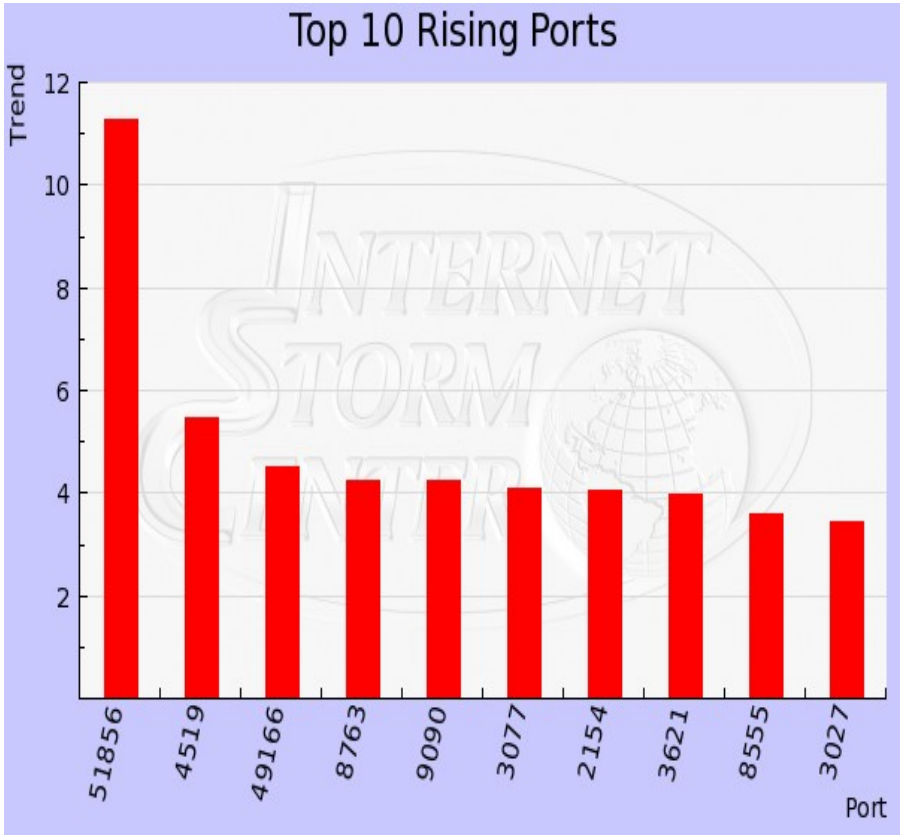


Internet Storm Center

- Το Internet Storm Center δημιουργήθηκε το 2001, μετά την επιτυχή ανίχνευση, ανάλυση και την ευρεία προειδοποίηση για το σκουλήκι Li0n
- Βασίζεται στο κατανεμημένο σύστημα ανίχνευσης απειλών DShield. Αισθητήρες του καλύπτουν περισσότερες από 500.000 IP διευθύνσεις σε περισσότερες από 50 χώρες
- Υποστηρίζεται από το SANS Institute
- Οι εθελοντές χειριστές κρίσεων αναλύουν τα αποτελέσματα ανιχνεύσεων και ανωμαλίες, και καταχωρούν σε ένα καθημερινό ημερολόγιο τις εκτιμήσεις τους στην ιστοσελίδα του Storm Center.
- Προφέρει εποπτική εικόνα της επικινδυνότητας του Internet

Διεθνής Εμπειρία





Διεθνής Εμπειρία

CASEScontact

- Πρωταρχικός στόχος του CASEScontact είναι να εκπαιδεύσει οικιακούς χρήστες και σε μικρές και μεσαίες επιχειρήσεις σχετικά με θέματα που αφορούν κινδύνους του Διαδικτύου

CyTRAP Labs Διεθνής Εμπειρία

Το CASEScontact είναι μια συνεργασία δημόσιου και ιδιωτικού τομέα

- CyTrap - Cyber Threat Reduction and Prevention
- CASES-cc.org
- www.EICAR.org
- Unabhaengiges Landeszentrum fuer Datenschutz Schleswig – Holstein
- International School of New Media (ISNM) του Πανεπιστήμιο του Luebeck

Το CASEScontact είναι μια πολυεθνική πρωτοβουλία

Γερμανία, Δανία, Βέλγιο, Ελβετία

CyTRAP Labs Διεθνής Εμπειρία

Το CASEScontact στοχεύει στην ενημέρωση των οικιακών χρηστών για

- Προστασία των προσωπικών πληροφοριών και δεδομένων, όπως ηλικία ή αριθμός πιστωτικής κάρτας.
- Μείωση των spam αλλάζοντας τις συνήθειες «σερφαρίσματος» και εγκαθιστώντας τα κατάλληλα anti – spam εργαλεία.
- Διασφάλιση της ευρυζωνικής σύνδεσης βοηθώντας να ελεγχθεί εάν έχει γίνει σωστά η εγκατάσταση του firewall.
- Ασφαλής χρήση του τηλεφωνικού καταλόγου του κινητού τηλεφώνου χωρίς το να υπάρχει ο κίνδυνος κλοπής του από κάποιον hacker.
- Προστασία ασύρματων δικτύων στο σπίτι.

Ελληνική Εμπειρία

Το ΕΔΕΤ / GRNET

- Η ΕΔΕΤ Α.Ε. ιδρύθηκε με το Π.Δ. 29/1998 και ανήκει στο Υπουργείο Ανάπτυξης, εποπτευόμενη από την ΓΓΕΤ Διαχειρίζεται τον κόμβο Athens Internet Exchange (AIX), ο οποίος παρέχει τοπική διασύνδεση μεταξύ των μεγαλύτερων εταιρειών παροχής υπηρεσιών Διαδικτύου στην Ελλάδα
- Παρέχει διεθνή διασύνδεση με τα υπόλοιπα ερευνητικά δίκτυα και το Διαδίκτυο μέσω του πανευρωπαϊκού ερευνητικού δικτύου GEANT.
- Διαχειρίζεται / συμμετέχει σε μια σειρά αναπτυξιακών έργων, όπως το e – Business Forum και η Εκπαιδευτική Στήριξη του προγράμματος «Δικτυωθείτε»

Ελληνική Εμπειρία

GRNET – CERT

- Λειτουργεί στα πλαίσια του (ΕΔΕΤ) διασυνδέει τα Ελληνικά ΑΕΙ, τα ΤΕΙ και Ερευνητικά Κέντρα (συνεργάζεται με 82 φορείς - πάνω από 200.000 χρήστες)
- Διαχειρίζεται περιστατικά ασφαλείας που εμπλέκουν το ΕΔΕΤ και φορείς του ΕΔΕΤ
- Παρέχει στους χρήστες του ΕΔΕΤ πληροφόρηση πάνω σε θέματα ασφαλείας και έγκυρες απαντήσεις πάνω σε συγκεκριμένα προβλήματα
- Διατηρεί γραμμή επικοινωνίας με άλλες Ελληνικές, Ευρωπαϊκές και Διεθνείς ομάδες που ασχολούνται με την αντιμετώπιση περιστατικών ασφαλείας (μέλος του TF – CSIRT)
- Βοηθάει με την εκπαίδευση των χρηστών σε θέματα ασφαλείας υπολογιστών και διαφύλαξης του προσωπικού απορρήτου.

Ελληνική Εμπειρία

GSN – CERT

- Βασικός στόχος ήταν η διαχείριση των καταγγελιών / διαμαρτυριών που γίνονταν προς το ΠΣΔ και ονομάστηκε αρχικά Ομάδα Διαχείρισης Περιστατικών Κατάχρησης (Network Abuse Handling Team).
- Επεκτάθηκε σε Ομάδα Διαχείρισης Περιστατικών Ασφαλείας (Computer Emergency Response Team), εξυπηρετώντας το ΠΣΔ για θέματα ασφάλειας.
- Έχει ενταχθεί στο Ε.Π. Κοινωνία της Πληροφορίας και συγχρηματοδοτείται από την Ε.Ε. και το Υπουργείο Παιδείας.
- Η ομάδα χρησιμοποιεί μετά από άδεια του Carnegie Mellon University το ακρωνύμιο CERT.

Ελληνική Εμπειρία

Πλεονεκτήματα:

- Πλήρως ενημερωμένα
- Πλούσιο υλικό
- Όμορφα σχεδιασμένα

..αλλά:

- Απαιτούν εξειδικευμένες γνώσεις

Ελληνική Εμπειρία

Η Microsoft δημοσίευσε 12 πακέτα, τα περισσότερα αυτή τη χρονιά και αρκετά από αυτά θεωρούνται κρίσιμα.*

- MS06-021 Cumulative patch for Internet Explorer - Critical
- MS06-022 ART image library buffer overflow - Critical
- MS06-023 Microsoft JScript memory corruption - Critical
- MS06-024 Windows media player - Critical
- MS06-025 RRAS - Critical
- MS06-026 Graphics rendering engine remote code execution - Critical
- MS06-027 Word remote code execution - Critical
- MS06-028 Powerpoint remote code execution -Critical
- MS06-029 Exchange - Important * MS06-030 SMB privilege escalation - Important * MS06-031 RPC mutual authentication spoofing - Moderate
- MS06-032 IP source routing allows remote code execution - Important

Για λεπτομέρειες δείτε http://www.microsoft.com/technet/security/bulletin/ms06-011.mspx
Ειδικά για το MS06-030 κυκλοφορεί ήδη exploit

Ελληνική Εμπειρία

ΑΠΟΣΠΑΣΜΑ: Το Allaple είναι ένα ισχυρό πολυμορφικό σκουλήκι τοπικού δικτύου και Διαδικτύου. Χρησιμοποιεί έναν αριθμό ευπαθειών για να εξαπλωθεί και κάνει επίθεση προσπάθειας ανεύρεσης κωδικών πρόσβασης χρησιμοποιώντας λεξικά (dictionary attack) σε διαμοιραζόμενους φακέλους. Το σκουλήκι δημιουργεί αρκετά αντίγραφά του στον σκληρό δίσκο και επηρεάζει ακόμα και τα αρχεία HTML. Επιπρόσθετα το σκουλήκι κάνει επίθεση DoS (Denial of Service) σε ορισμένες ιστοσελίδες.Το αρχείο που δημιουργεί το σκουλήκι είναι κρυπτογραφημένο πολυμορφικά. Αυτό σημαίνει ότι κάθε αντίγραφο του είναι διαφορετικό. Το μόνο που μένει σταθερό είναι το μέγεθος του εκτελέσιμου αρχείου που είναι: 57856 bytes. Μόλις το αρχείο του σκουληκιού εκτελεστεί περνάει μέσα από έναν πολυμορφικό αποκρυπτογραφητή και προχωράει στο σταθερό κομμάτι του κώδικα που δεσμεύει μια θέση μνήμης (memory buffer) και εκεί εξαγάγει το κύριο κώδικα του σκουληκιού. Τότε ο έλεγχος περνάει απευθείας στο κώδικα αυτό.Μόλις πάρει τον έλεγχο του μηχανήματος, το σκουλήκι δημιουργεί ορισμένα νήματα (threads) που εκτελούνται παράλληλα. Ένα νήμα σαρώνει ολόκληρα υποδίκτυα σε μια προσπαθεί να ανακαλύψει ευπαθή σταθμούς εργασίας στις πόρτες TCP 139 και 445, μετά στέλνει κατάλληλο κώδικα που εκμεταλλεύεται αυτές στα ευπαθή μηχανήματα με σκοπό να τους μολύνει. Το σκουλήκι προσπαθεί επίσης να "σπάσει" κωδικούς σε κοινόχρηστους φακέλους δικτύου χρησιμοποιώντας επίθεση με χρήση λεξικού (dictionary attack). οι πόρτες TCP του χρησιμοποιούνται για την επίθεση DoS είναι: 22, 80, 97, 443

GR-CERT

Υπό την αιγίδα του ebusinessforum

Πιθανοί Συνεργάτες

- Ελληνικά CERTs (ΕΔΕΤ GRNET, GSN-Cert)
- Διεθνή CERTs (CyTRAP Labs)
- Δημόσιοι οργανισμοί (Υπ. Ανάπτυξης)
- Πανεπιστήμια (ΟΠΑ, Παν. Αιγαίου)
- Ιδιωτικός τομέας (Τραπεζικός Τομέας)

GR-CERT

Στόχοι GR-CERT

- Ενημέρωση για κενά ασφάλειας, απάτες, επείγοντα περιστατικά
- Παροχή συμβουλών – βέλτιστων πρακτικών
- Υπεύθυνη διαχείριση κενών ασφάλειας (εταιρίες –ερευνητές)

GR-CERT

Ενημέρωση

Παράδειγμα

Κενό ασφαλείας σχετικά με την σειριακοποιήση (serialization) στο περιβάλλον εκτέλεσης Java (Java Runtime Enviroment) που μπορεί να οδηγήσει σε κλιμάκωσης δικαιωμάτων σε μη έμπιστο εφαρμογίδιο

ή

Άσχετα με το αν χρησιμοποιείτε Windows, Mac ή Linux, πιθανότατα έχετε εγκατεστημένο κάποιο περιβάλλον Java για να βλέπεται πλούσιο περιεχόμενο στις ιστοσελίδες που επισκέπτεστε. Σε αυτή τη περίπτωση ...

GR-CERT

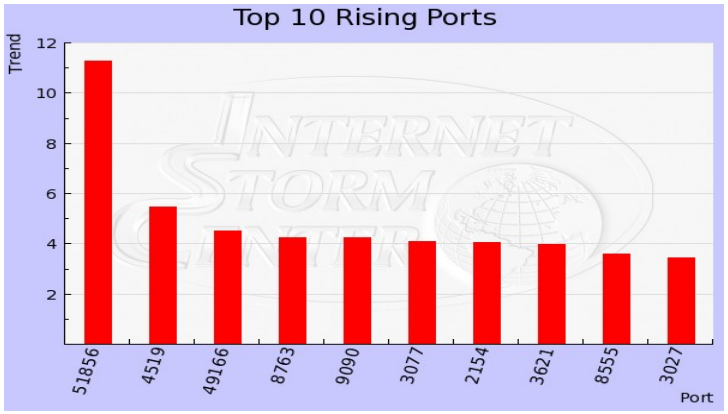
Ενημέρωση

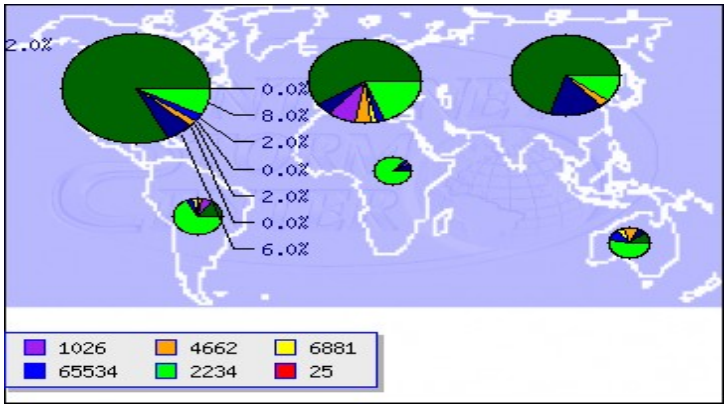
- Επεξεργασία πληροφοριών από Ελληνικά και ξένα CERTs
- Μετατροπή της πληροφορίας σε κατανοητή μορφή για οικιακούς χρήστες και ΜΜΕ

GR-CERT

Επικαιρότητα

- Ημερολόγιο
- Πρόχειρες συμβουλές
- Εθελοντές διαχειριστές



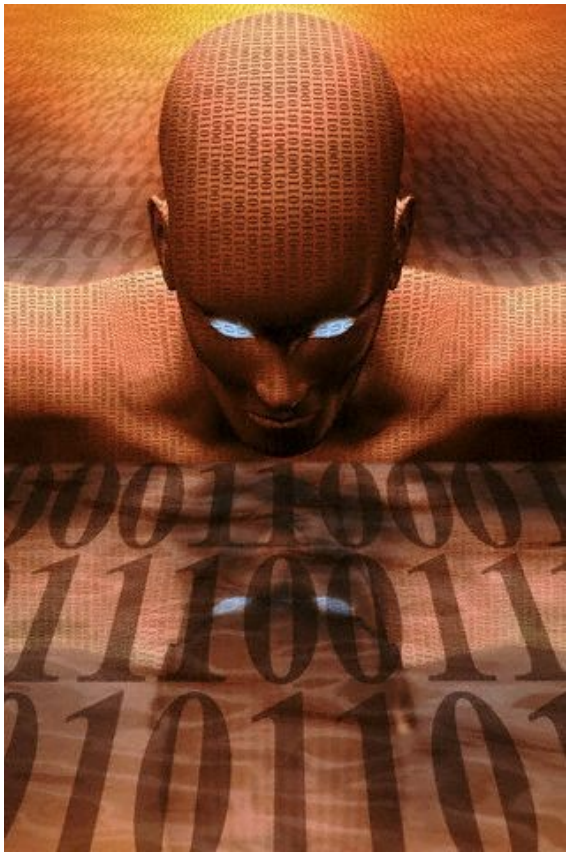


GR-CERT

Διαχείριση κενών ασφαλείας σε

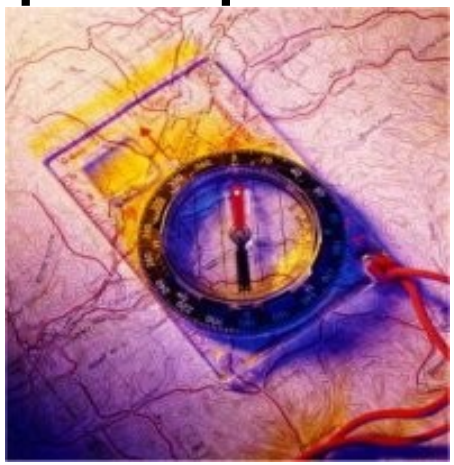
Ελληνικό Λογισμικό

- Λογιστικά προγράμματα
- Δημόσιες Υπηρεσίες
- Τραπεζικός Τομέας



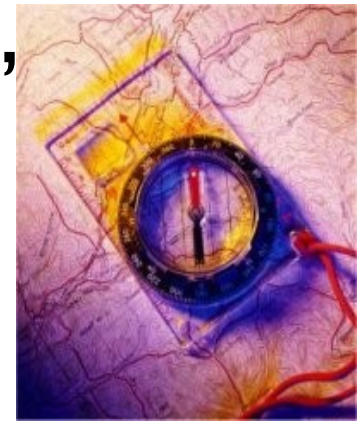
Οδικός Χάρτης

- Σύναψη Συνεργασιών (GRNET-Cert, GSN-Cert, Cases)
- Επεξεργασία προτάσεων με την συμμετοχή ειδικών
- Σύσταση ομάδας ειδικών
  - Διαχειριστές
  - Αναλύτες



Οδικός Χάρτης

1. Δημιουργία μητρώου
   - Σημεία επαφής ΜΕ
   - Ειδικών ασφαλείας
- Αναζήτηση πόρων (υποδομή, προσωπικό)
- Χρηματοδότηση



Συζήτηση

Στοιχεία Επικοινωνίας

Βασίλης Βλάχος vbill@aueb.gr

Πέτρος Μπέλσης pbelsis@aegean.gr