Το ηλεκτρονικό επιχειρείν στο στόχαστρο των κυβερνοεγκληματιών: **επίκαιρα τεχνάσματα & επιβεβλημένα αντίμετρα** στο ψηφιακό εταιρικό περιβάλλον

Αστυνόμος Α΄ Αναστάσιος Παπαθανασίου, MSc, PhD(c) || **Αστυνόμος Β΄ Γεώργιος Γέρμανος**, MSc
Διεύθυνση **Δ**ίωξης **Η**λεκτρονικού **Ε**γκλήματος / Α.Ε.Α.

Ηλεκτρονικό επιχειρείν

«Οποιαδήποτε μορφή επιχειρηματικής ή διοικητικής συναλλαγής ή ανταλλαγής πληροφοριών, η οποία εκτελείται με τη χρησιμοποίηση οποιασδήποτε τεχνολογίας πληροφορικής και τηλεπικοινωνιών»

Εγκλήματα στον Κυβερνοχώρο

- Δεν περιορίζονται εδαφικά
- Ταχύτητα τέλεσης
- Αριθμός υποψήφιων θυμάτων
- Δυσχέρειες διερεύνησης
  - Νομικές
  - Τεχνικές

Εγκλήματα με οικονομική διάσταση στο ψηφιακό εταιρικό περιβάλλον

- Ransomware & Cryptoware
- Απάτη CEO
- Επιθέσεις Man-in-the-middle
- Εκβίαση με επίθεση DDoS
- Επιθέσεις Phishing

Ransomware & Cryptoware

Το 2012 παρατηρήθηκε η πρώτη ευρεία εξάπλωση ransomware

ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΑΤΤΙΚΗΣ
Διωξης Ηλεκτρονικού Εγκλήματος

Προσοχή!

Αυτό το λειτουργικό σύστημα μπλοκάρεται λόγω παραβίασης των νόμων της Ελλάδας! Σημειώθηκαν οι ακόλουθες παραβιάσεις:

Η IP διεύθυνσή σας είναι " ". Από αυτή την IP διεύθυνση επισκέφτηκαν ιστοσελίδες που περιέχουν πορνογραφία, την παιδική πορνογραφία, κτηνοβασία, και τη βία κατά των παιδιών. Ο υπολογιστής σας επίσης περιείχε βίντεο που περιλαμβάνει πορνογραφία, βία και παιδική πορνογραφία! Επιπλέον, από το ηλεκτρονικό ταχυδρομείο σας αποστελλόταν μηνύματα με τη μορφή spam, που περιείχαν τρομοκρατική πρόθεση.

Αυτό το μπλοκάρισμα του υπολογιστή έγινε για να σταματήσουν οι παράνομες δραστηριότητές σας.

Τα στοιχεία σας: [redacted] Τοποθεσία: Greece, Athens ISP: Tellas S.A.

Για να ξεκλειδώσετε τον υπολογιστή, πρέπει να πληρώσετε πρόστιμο 100 ευρώ.
Μπορείτε να πληρώσετε ποινή με δύο τρόπους:

1) Μέσω του συστήματος Ukash:

Για να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής 19-ψήφιο κωδικό και να πατήσετε OK (αν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο OK).

Εάν στη διαδικασία πληρωμής θα γίνει σφάλμα, θα πρέπει να στείλετε τους κωδικούς στη διεύθυνση economic-crime@hellenicpolice.gr.

2) Πληρωμή μέσω Paysafecard:

Για να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής ένα 16-ψήφιο κωδικό (αν είναι αναγκαίο, με έναν κωδικό πρόσβασης), και στη συνέχεια κάντε κλικ στο OK (εάν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο OK).

Εάν στη διαδικασία πληρωμής θα γίνει σφάλμα, θα πρέπει να στείλετε τους κωδικούς στη διεύθυνση economic-crime@hellenicpolice.gr.

Ukash Πού μπορώ να αγοράσω Ukash?

Μπορείτε να προμηθευτείτε Ukash σε εκατοντάδες σημεία παγκοσμίως, online, από πορτοφόλια, καταστήματα ψιλικών και μηχανήματα αυτόματης ανάληψης.

KKT - KKT Αγοραστέ την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περίπτερα και καταστήματα τροφίμων & ψιλικών

Kapa - Αγοραστέ την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περίπτερα και καταστήματα τροφίμων & ψιλικών

OK

paysafecard Πού μπορώ να αγοράσω Paysafecard?

Payzone Hellas είναι η μεγαλύτερη εταιρεία κινητής τηλεφωνίας top-up δικτύου στην Ελλάδα με εγκατεστημένη πάνω από 11.000 τερματικά POS. Payzone Hellas πρωταγωνιστεί, επίσης, πληρωμή λογαριασμών και υπηρεσιών κοινής ωφελείας για την προκαταβολή και τους παρόχους υπηρεσιών στην Ελλάδα.

OK

Ransomware & Cryptoware

Μετάβαση στην κρυπτογράφηση

Ransomware & Cryptoware

Σήμερα η κατάσταση είναι αρκετά πιο σύνθετη!

Your documents, photos, databases and other important files have been encrypted
with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can
decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker.
Overwise, it's seems that you or your antivirus deleted the locker program.
Now you have the last chance to decrypt your files.

Open http://34r6hq26q2h4jkzj.tor2web.org or http://34r6hq26q2h4jkzj.onion.cab
in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:
1. Download Tor Browser from http://torproject.org
2. In the Tor Browser open the http://34r6hq26q2h4jkzj.onion/
   Note that this server is available via Tor Browser only.
   Retry in 1 hour if site is not reachable.
Copy and paste the following Bitcoin address in the input form on server. Avoid missprints.
1KFgfxz8cUViX16xypNaHkM1eU1Y6wQ3K3
Follow the instructions on the server.

Ransomware & Cryptoware

- Συχνότερες πηγές μόλυνσης
  - Ηλεκτρονικό ταχυδρομείο
  - «Μολυσμένοι» ιστότοποι
  - Λογισμικό άγνωστης προέλευσης
- Μόλυνση εταιρικού δικτύου
- Ανεπανόρθωτη βλάβη
- Η πληρωμή των «λύτρων» δε συνεπάγεται λύση του προβλήματος!

Απάτη CEO

- Ο εγκληματίας επικοινωνεί με τον εργαζόμενο της εταιρείας
- Με email ή τηλεφωνικά
- **Προσποιείται τον CEO ή άλλο υψηλόβαθμο στέλεχος**
- Ζητά επειγόντως:
  - Αποκάλυψη κωδικών πρόσβασης ή
  - Μεταφορά χρημάτων

Στοχευμένες επιθέσεις phishing

- Τάση δημοσιοποίησης στα social media της θέσης που κατέχει κάποιος
  - LinkedIn, Facebook κ.λπ.
- Ο δράστης αναζητά εκείνα τα άτομα που κατέχουν «κρίσιμες» θέσεις
  - διαχειριστής βάσεων δεδομένων
- Ο εργαζόμενος της εταιρείας λαμβάνει phishing email **ειδικά σχεδιασμένο** γι' αυτόν
- Τυχόν **διαρροή δεδομένων** μπορεί να οδηγήσει σε **φαινόμενα εκβίασης**!

Επιθέσεις
Man-in-the-middle

- Ο δράστης «παρεμβαίνει» στην επικοινωνία του «αγοραστή» με τον «πωλητή»
- Ζητά την κατάθεση χρημάτων σε τραπεζικό λογαριασμό διαφορετικό από αυτόν που συμφωνήθηκε αρχικά
- Το θύμα δεν αντιλαμβάνεται την απάτη εγκαίρως
- **Σημαντική αύξηση καταγγελιών τον τελευταίο χρόνο!**

Εκβίαση με επίθεση DDoS

Απειλή πραγματοποίησης επίθεσης DDoS σε περίπτωση μη καταβολής χρημάτων

```
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND
CAN MAKE DECISION!

We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

Your network will be DDoS-ed starting [date] if you don't pay
protection fee - 10 Bitcoins @ [Bitcoin Address].

If you don't pay by [date], attack will start, yours service
going down permanently price to stop will increase to 20 BTC
and will go up 10 BTC for every day of attack.

This is not a joke.
```

Επιβεβλημένα αντίμετρα

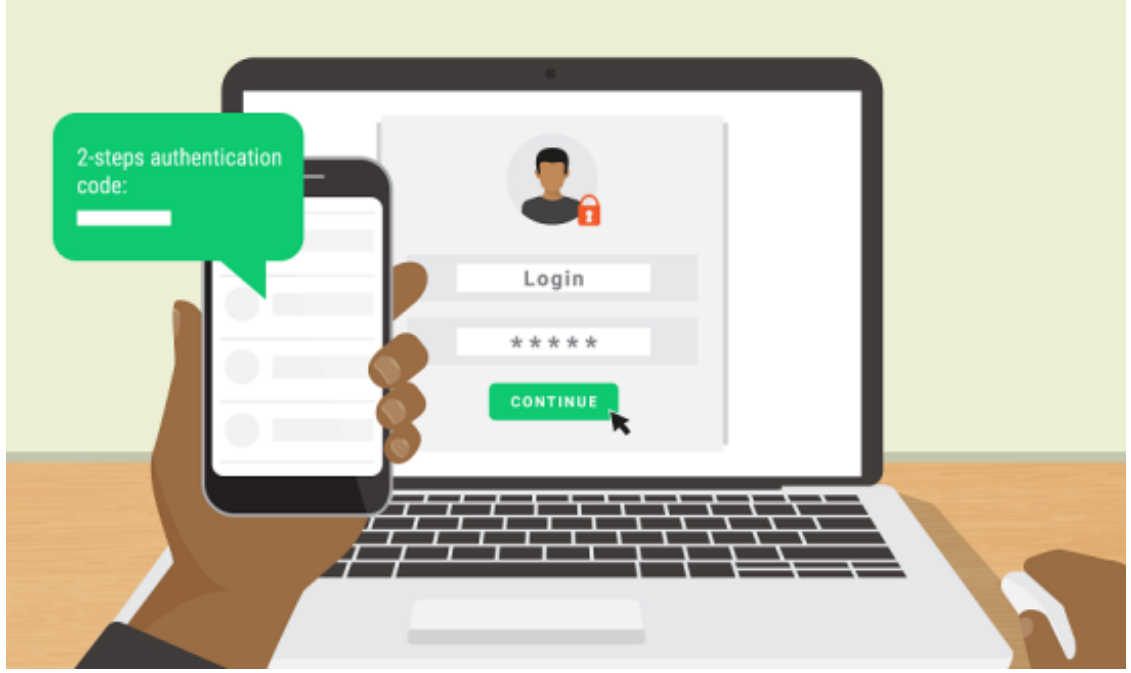
«Ασφάλεια εστί το προνοείν και το προλαμβάνειν, το δε προνοείν και προλαμβάνειν κρείττον εστί του θεραπεύειν»

Ιπποκράτης

Λογισμικό

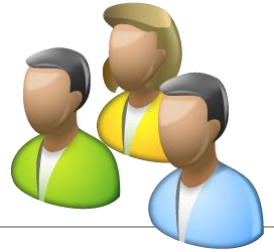
- ✓Χρήση **προγραμμάτων προστασίας** από κακόβουλο λογισμικό, τόσο στον **υπολογιστή**, όσο και στις **φορητές συσκευές** (smartphones, tablets) και **τακτική ενημέρωσή τους**
- ✓Εγκατάσταση διαθέσιμων **αναβαθμίσεων** και **ενημερώσεων / διορθώσεων ασφαλείας** του λειτουργικού συστήματος και των λοιπών προγραμμάτων και εφαρμογών
- ✓Αποφυγή εγκατάστασης προγραμμάτων και εφαρμογών από **μη ασφαλείς πηγές**

Κωδικοί πρόσβασης



- ✓Τακτική αλλαγή **κωδικών πρόσβασης** στο ηλεκτρονικό ταχυδρομείο & τις λοιπές online υπηρεσίες
- ✓Χρήση τεχνικών **αυθεντικοποίησης δύο βημάτων** (2-steps authentication)

Χρήστες



- ✓Δεν ανταποκρινόμαστε σε μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνήματα όπου ζητείται η αποκάλυψη στοιχείων πρόσβασης σε ηλεκτρονικούς λογαριασμούς & υπηρεσίες
- ✓Δεν κλικάρουμε σε συνδέσμους (links) που εμπεριέχονται σε e-mails από αγνώστους, καθώς οι σύνδεσμοι αυτοί ενδέχεται να παραπέμπουν σε κακόβουλες ιστοσελίδες ή/και να προκαλούν την εγκατάσταση κακόβουλου λογισμικού
- ✓Αυτοπρόσωπη ή τηλεφωνική επιβεβαίωση «ύποπτων» αιτημάτων (π.χ. καταβολή χρημάτων σε διαφορετικό τραπεζικό λογαριασμό, αποκάλυψη κωδικών πρόσβασης κ.λπ.)

Ο ρόλος της εταιρείας
& του IT Manager

- ✓ Φυσική ασφάλεια
- ✓ Εφαρμογή αρχής «need to know» & πολιτικής ασφάλειας κατά τη χρήση των ψηφιακών, υπολογιστικών συστημάτων και Διαδικτύου (USB sticks, Cloud κ.λπ.)
  - ➢ Δικαιώματα πρόσβασης
  - ➢ Τήρηση αρχείων καταγραφής
- ✓ Τήρηση αντιγράφων ασφαλείας (back up)

Ο ρόλος της εταιρείας
& του IT Manager

- ✓ Εφαρμογή μεθόδων κρυπτογράφησης
  - ➢ Αποθήκευση
  - ➢ Επικοινωνία
- ✓ Εταιρική πολιτική **Bring-Your-Own-Device (BYOD)**
- ✓ Προσοχή στην πρόσβαση σε εταιρικά δεδομένα από δημόσια WiFi δίκτυα!

Ο ρόλος της εταιρείας
& του IT Manager

✓ **Ενημέρωση / εκπαίδευση του προσωπικού**

Όσα μέτρα ασφαλείας κι αν ληφθούν, σε οποιοδήποτε επίπεδο, αδύναμος κρίκος παραμένει ο άνθρωπος!

Εκστρατεία #MobileMalware

www.cyberalert.gr/feelsafe

- ✓Ενημέρωση για επιχειρηματίες, υπαλλήλους & καταναλωτές

Σας ευχαριστούμε για την προσοχή σας!

Αστυνόμος Α΄ Αναστάσιος Παπαθανασίου, MSc, PhD(c)
a.papathanasiou@cybercrimeunit.gr

Αστυνόμος Β΄ Γεώργιος Γέρμανος, MSc
g.germanos@cybercrimeunit.gr

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος / Α.Ε.Α.
ccu@cybercrimeunit.gov.gr