Ασφάλεια Δικτύων και Επικοινωνιών

(Network and Communication Security)

Συστήματα Ανίχνευσης και Πρόληψης Εισβολών (Intrusion Detection and Prevention Systems)

Προηγμένες επιθέσεις ασφάλειας (Advanced Persistent Threats)

Άλλα μέτρα προστασίας δικτύων

Αν. Καθ. Παναγιώτης Κοτζανικολάου

ΠΜΣ Κυβερνοασφάλεια και Επιστήμη Δεδομένων

1. **Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems)**

2. **Συστήματα Πρόληψης Εισβολών (Intrusion Prevention Systems)**

Βασικοί όροι

- **Εισβολή**: Σειρά από δράσεις που στοχεύουν να θέσουν σε κίνδυνο τους πυλώνες της ασφάλειας: της *ακεραιότητας*, της *εμπιστευτικότητας* ή της *διαθεσιμότητας*, στα δίκτυα και τους πόρους.

- **Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems)**: Διαδικασία και εργαλεία εντοπισμού πιθανής δικτυακής εισβολής.

- **Συστήματα Πρόληψης Εισβολής (Intrusion Prevention Systems)**: Επέκταση του IDS με χρήση ενεργού ελέγχου πρόσβασης για την αυτόματη ενεργοποίηση μηχανισμών άμυνας, με στόχο την προστασία των υπολογιστών.

IDS / IPS: Βασικές αρχές λειτουργικότητας

1. **Παρακολούθηση** των χρηστών και της δραστηριότητας του συστήματος.

2. **Ανάλυση συστήματος** και έλεγχος για τρωτά σημεία και λανθασμένες ρυθμίσεις.

3. **Εκτίμηση της ακεραιότητας** των κρίσιμων συστήματος και τα αρχεία δεδομένων.

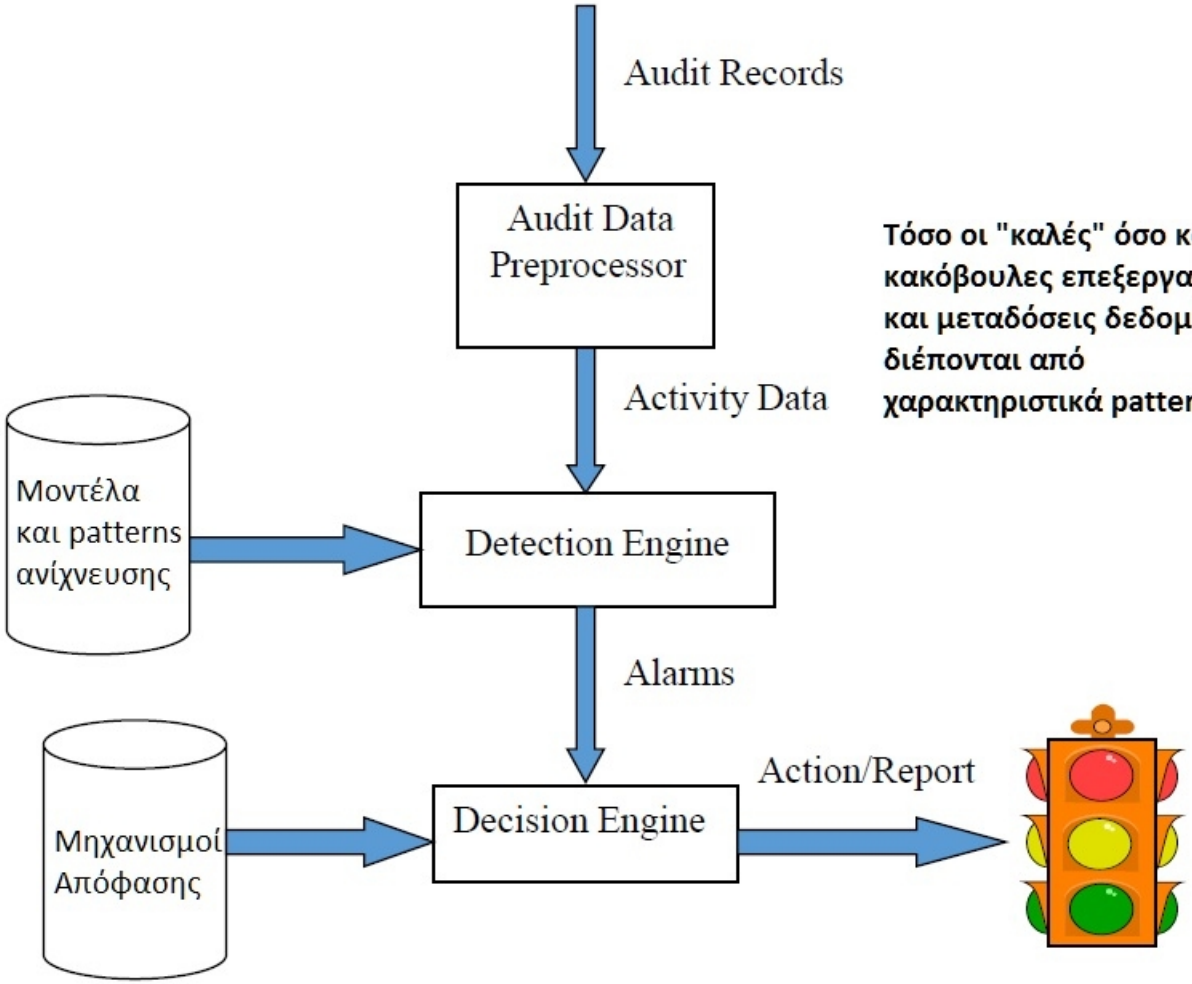
4. **Αναγνώριση** γνωστών μοτίβων επίθεσης στη δραστηριότητα των συστημάτων.

Rule-based vs Behavioral Detection

Η κίνηση θεωρείται **ύποπτη** όταν:

- **(Rule based or signature-based) Ταιριάζει τα πακέτα με γνωστά μοτίβα (pattern) κακόβουλης** δραστηριότητας. Εντοπισμός επιθέσεων όπως:
  - *αντικατάσταση πολλών αρχείων,*
  - *επικοινωνία με όλες τις θύρες σε μια δεδομένη διεύθυνση δικτύου,*
  - *μεταφορά πολλών αρχείων από το τοπικό δίκτυο.*
  - *Δεν μπορεί να εντοπίσει επιθέσεις για τις οποίες δεν γνωρίζει το αντίστοιχο μοτίβο* ***(false negative).***
- **(Behavioral or anomaly detection) Αναζητά αλλαγές στη συμπεριφορά της ελεγχόμενης κίνησης**.
  - *Μπορεί να εντοπίσει ενδείξεις ότι ένας διαφορετικός χρήστης ελέγχει έναν υπολογιστή,*
  - *...ή απλά μια μετατόπιση των αναγκών υπολογιστή* ***(false positive).***

Μοντελοποίηση ID(P)S



Τόσο οι "καλές" όσο και οι κακόβουλες επεξεργασίες και μεταδόσεις δεδομένων διέπονται από χαρακτηριστικά patterns

Αρχιτεκτονικές IDS

- **Network based IDS**

Παρακολουθεί την κίνηση όλου του δικτύου και εξετάζει την κίνηση για πιθανές επιθέσεις, είτε μέσω εφαρμογής κανόνων (rules) για υπογραφές επίθεσης, είτε ελέγχοντας την συμπεριφορά της κίνησης (behavior) .

- **Host based IDS**

IDS που λειτουργεί σε τερματικά (workstations) για την παρακολούθηση και προστασία ενός συστήματος (ΛΣ, σύστημα αρχείων, τοπικές εφαρμογές_.

- **Distributed IDS**

Κατανεμημένο IDS που χρησιμοποιεί αισθητήρες ή πράκτορες (agents) σε διάφορα σημεία του δικτύου, οι οποίοι συλλέγουν εξ αποστάσεως και στέλνουν τις αναφορές τους σε ένα κεντρικό σταθμό διαχείρισης.

- **Gateway IDS**

Κεντρικό IDS που έχει υλοποιηθεί στην πύλη μεταξύ του δικτύου και ενός εξωτερικού δικτύου. Συχνά υλοποιούνται έτσι ώστε να μπορούν να ελέγξουν κίνηση σε όλα τα επίπεδα του OSI.

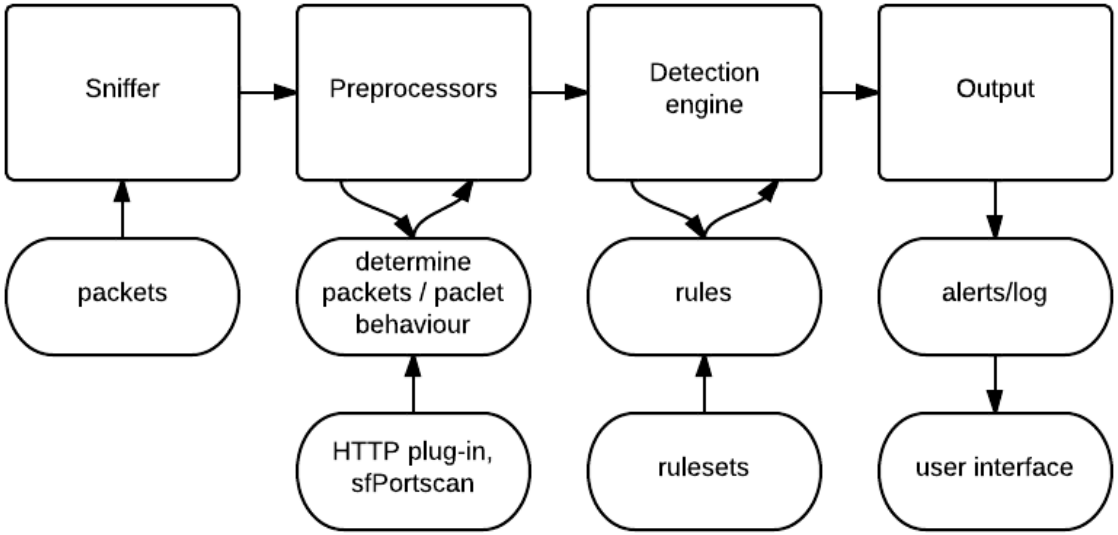
Intrusion Prevention Systems

Πέραν της ανίχνευσης μίας επίθεσης, ένα IPS μπορεί να προκαλέσει την ενεργή αντίδραση για την πρόληψη της επίθεσης, όπως:

- Αποκλεισμός των χρηστών.
- Απόρριψη της κυκλοφορίας από ορισμένες IP διευθύνσεις.
- Διακοπή της πρόσβασης σε ένα αρχείο ή πρόγραμμα.
- Επανακατεύθυνση της κυκλοφορίας σε ένα κεντρικό σημείο ελέγχου ή σε ένα δίκτυο παραπλάνησης εισβολέα (honeypot).
- Απόρριψη της κίνησης ή περάτωση της συνόδου.
- Αυτόματη ανανέωση των κανόνων ενός Firewall και Router
- ...

Παράδειγμα IDS: Snort

- Free open source network-based IDS IPS system www.snort.org
- Created in 1998 by Martin Roesch, owned by CISCO from 2014.
- General architecture:



Snort: Καταστάσεις λειτουργίας

Sniffer mode: Reads packets off of the network and displays them in a continuous stream.

Packet Logger mode: logs the packets to disk.

Network Intrusion Detection System (NIDS) mode: Performs detection and analysis on network traffic.

- To enable NIDS:
- `./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf`

Snort: Παράδειγμα κανόνα

```
log tcp !192.168.0/24 any -> 192.168.0.33 (msg: "mounted access" ; )
```

- Operators <> and -> προσδιορίζουν την κατεύθυνση της δικτυακής κίνησης.
- Keyword *any* προσδιορίζει οποιαδήποτε IP address.

```
alert tcp any any -> 192.168.1.0/24 1524 (flags: S; resp: rst_all; msg: "Root shell backdoor attempt";)
alert udp any any -> 192.168.1.0/24 31 (resp: icmp_port,icmp_host; msg: "Hacker's Paradise access attempt";)
```

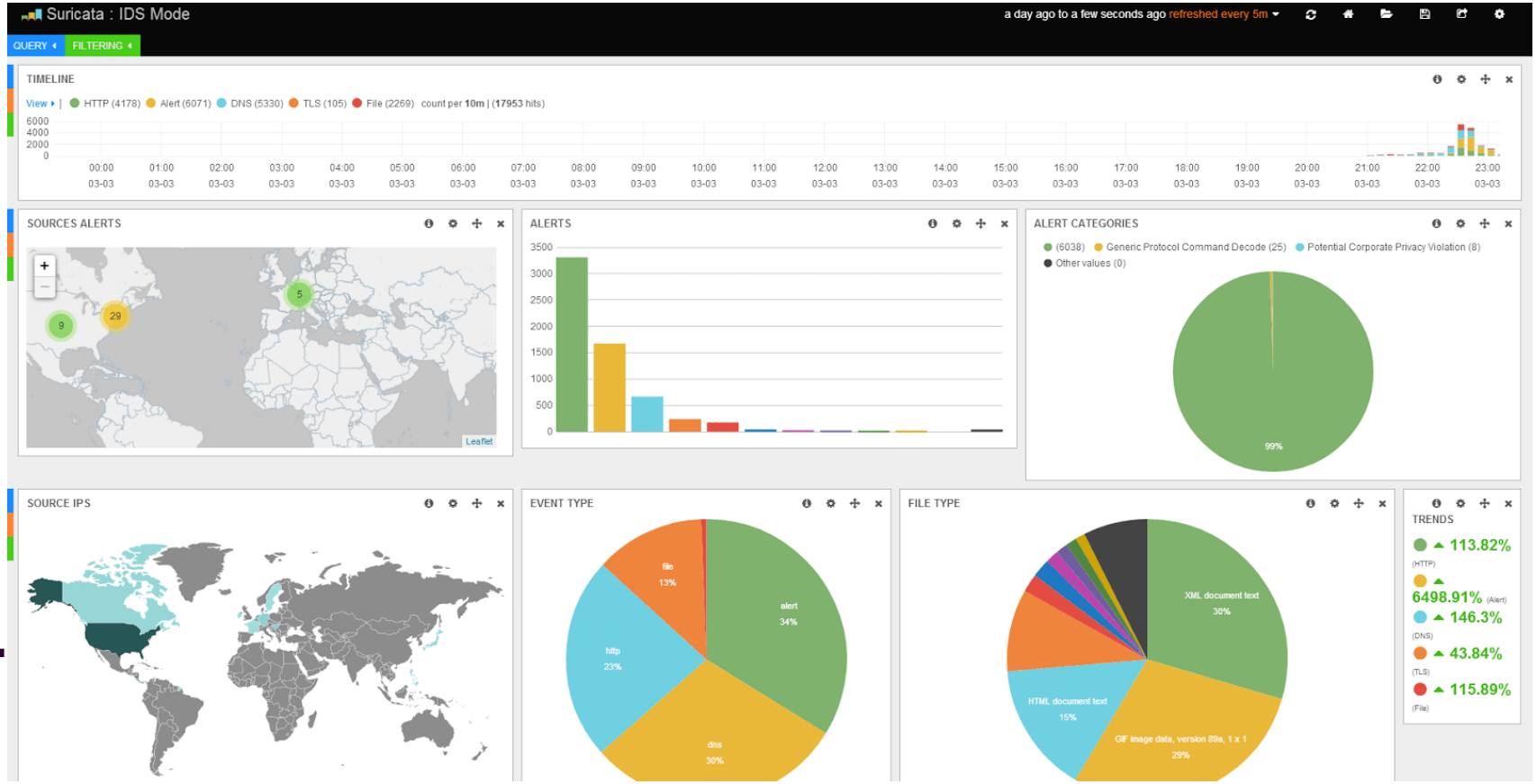
- Flags:S – SYN packet
- Resp: rst_all - TCP_RST packets in both directions
- Resp: icmp_port - send a ICMP_PORT_UNREACH to the sender

Παράδειγμα IDS: Suricata

Free open source network-based IDS with prevention capabilities (https://suricata-ids.org/docs/).

- Compatibe with Snort data structure
- It's possible to implement Snort policies inside Suricata.
- It uses YAML and JSON files as inputs and outputs, to support integration with other solutions.

Παράδειγμα IDS: Suricata



Παράδειγμα IDS: Zeek (formerly, Bro)

- Free open source IDS with monitoring capabilities (https://zeek.org/).
- Unlike Snort, Zeek also also runs on the application layer and can examine services like HTTP, FTP, SNMP, DNS etc.
- It uses both singature -based and anomaly detection.
- Requires more effort to deploy.

IDS/IPS: προβλήματα και ελλείψεις

Συχνή ανακρίβεια των exploit-based υπογραφών (signatures)

Αδυναμία εντοπισμού άγνωστων επιθέσεων και κακόβουλων λογισμικών

Δεν μπορεί να προσφέρει ικανοποιητική ανάλυση σε εξειδικευμένες περιπτώσεις

1. Κάποια detections μπορεί να προέρχονται από αστοχίες υλικού ή λογισμικού
2. Δυσκολία διαχωρισμού της κακόβουλης από την τυχαία λανθασμένη κίνηση (πολλά False Positives)
3. Δεν μπορεί να διαχωρίσει την εκάστοτε περιστασιακή επίθεση ούτε να δώσει χρήσιμες πληροφορίες για αυτή, όπως ο στόχος της επίθεσης, η στρατηγική, το είδος του επιτηθέμενου κτλ.

Προηγμένες επιθέσεις ασφάλειας (Advanced Persistent Threats)

Άλλα μέτρα προστασίας δικτύων: Honeypots, Honey Tokens

Η Συμβατική Άμυνα Δεν Επαρκεί

- Η αποτροπή περίπλοκων επιθέσεων με χρήση μόνο συμβατικών αντιμέτρων είναι μη ρεαλιστική.
- Οι πόροι και οι τεχνογνωσία των επιτιθέμενων υπερτερεί.
- Χρήση 0-day exploits και ανθεκτικού κακόβουλου λογισμικού.
  - "*It's not an arms race, we've already lost*" Haroon Meer, BlackHat 2015.
- Οι αμυνόμενοι πρέπει να εντοπίζουν και να επιδιορθώνουν διαρκώς τις νέες ευπάθειες.
- Παγκόσμια έλλειψη έμπειρων ειδικών IT ασφάλειας (Libicki et al. 2014)

Η Συμβατική Άμυνα Δεν Επαρκεί

- Αφού αποκτήσουν πρόσβαση σε ένα σύστημα, οι επιτιθέμενοι πρέπει να εντοπίσουν και να εξάγουν την πληροφορία για την οποία πραγματοποίησαν την επίθεση.
  - Περίπλοκη και χρονοβόρα διαδικασία (ειδικά σε μεγάλες εταιρείες).
  - Θα πρέπει να μεταπηδούν από το ένα σύστημα/δίκτυο στο άλλο, παραβιάζοντας συνεχώς λογαριασμούς και αποκτώντας πρόσβαση σε πολλαπλά συστήματα.
  - Εταιρικά δίκτυα απαρτίζονται συνήθως από τουλάχιστον 3 υποδίκτυα.
  - Ο σωστός διαχωρισμός των δικτύων αποτρέπει σε μεγάλο βαθμό τη σύνδεση υποδικτύων χωρίς προστασία.

Μηχανισμοί παραπλάνησης εισβολέα

Χρήση τεχνικών εξαπάτησης για τον έγκαιρο εντοπισμό κακόβουλων πράξεων και την αποτροπή παραβίασης των σημαντικών πόρων.

Honeypots: Φυσικά ή λογικά μηχανήματα (VM) που εξομοιώνουν αληθινά παραγωγικά τερματικά.

Honey tokens: Ψεύτικα αρχεία ή καταγραφές που ελκύουν κακόβουλους χρήστες.

Πλεονεκτήματα Και Μειονεκτήματα

Πλεονεκτήματα των honeypots:

- Συλλογή δεδομένων (τα honeypots συνήθως μαζεύουν λίγα δεδομένα αλλά αυτά τα δεδομένα είναι ύψιστης σημασίας)
- Ελάχιστη χρήση πόρων (τα honeypots πιάνουν μόνο την κίνηση που τα αφορά, οπότε δεν επιβαρύνουν πολύ το δίκτυο).

Μειονεκτήματα των honeypots:

- Επικίνδυνα αν χρησιμοποιηθούν λανθασμένα (προσοχή σε τι πόρους προσφέρουν πρόσβαση τα ίδια).
- Είναι χρονοβόρο να σχεδιαστεί, εγκατασταθεί και να παρακολουθείται επαρκώς.

Advanced Persistent Threats (APT)

Πολύ εξελιγμένες επιθέσεις ασφάλειας.

- Ο σχεδιασμός της επίθεσης απαιτεί:
  - Εξειδικευμένη τεχνική γνώση.
  - Υψηλούς διαθέσιμους πόρους (π.χ. υπολογιστική ισχύ, εξειδικευμένο τεχνικό εξοπλισμό κτλ).
  - Χρόνο (ενδεχομένως μήνες ή και χρόνια).

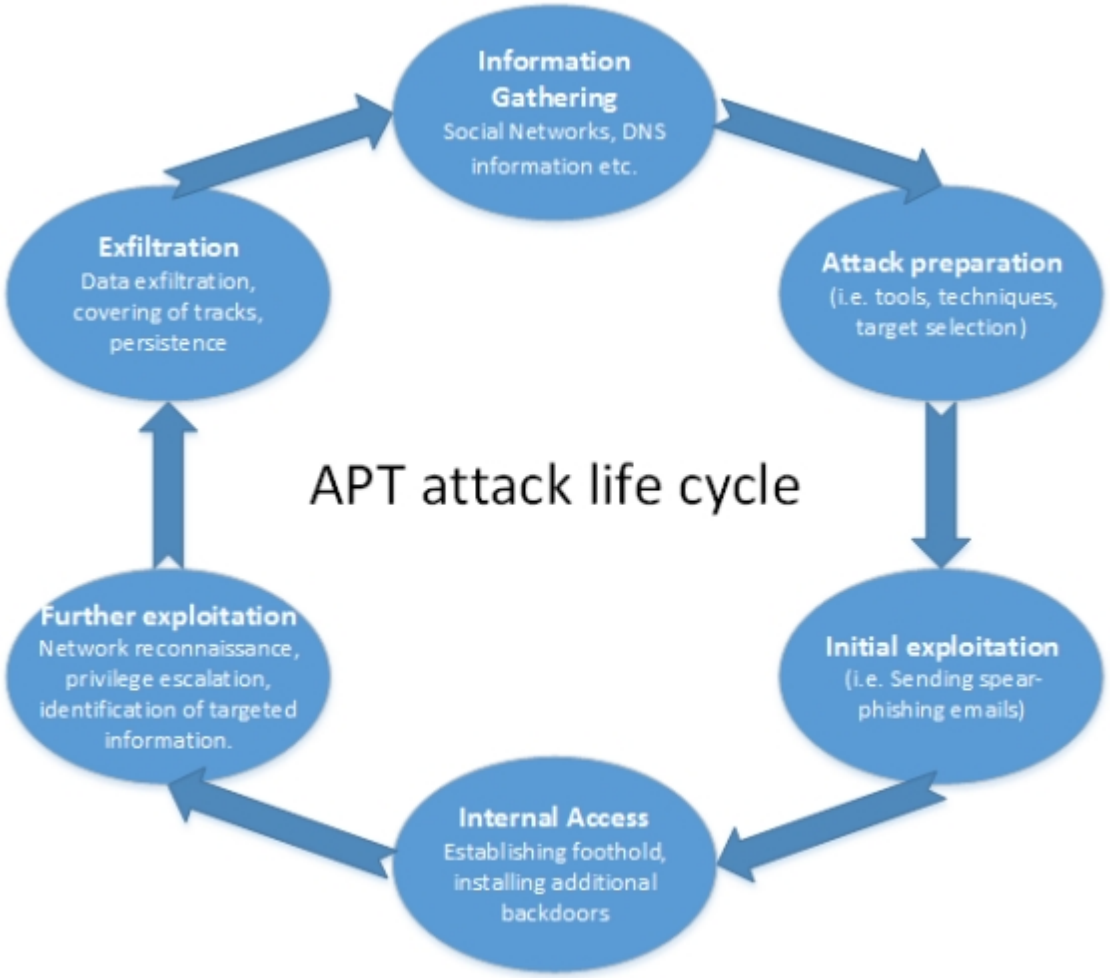
Γνωστά APT: Stuxnet worm (2010)

- Considered at the time to be one of the most sophisticated pieces of Malware ever detected, the Stuxnet Worm was used in operations against Iran in 2010.
- Its complexity indicated that only nation state actors could have been involved in its development and deployment.
- Unlike most viruses, the worm targets systems that are traditionally not connected to the internet for security reasons. It instead infects Windows machines via USB keys and then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC (programmable logic controllers).
- The operations were designed to provide the hackers with sensitive information on Iranian industrial infrastructure.

Γνωστά APT: Deep Panda (2015)

- An APT affecting the US Government's Office of Personnel Management.
- Has been attributed to what’s being described as on-going cyberwar between China and the U.S.
- The attack on OPM in May 2015 was understood to have compromised over 4 million US personnel records.
- Information pertaining to secret service staff may also have been stolen.

Κύκλος ζωής μιας επίθεσης APT



Αντίμετρα κατά την συγκέντρωση πληροφοριών

Συγκέντρωση πληροφοριών

social networks, bulletin boards, search engine queries (e.g. using Google dorks to find email addresses or domains registered to the organization), DNS zone transfers/brute-forcing, server/service fingerprinting, WHOIS lookups etc.

Αντίμετρα εξαπάτησης που μπορούν να χρησιμοποιηθούν σε αυτή την φάση:

- DNS honey tokens
- Web server honey tokens
- Λογαριασμοί Social network

Αντίμετρα: *DNS honey tokens*

Κακή ιδέα η χρήση honeypots κατά μήκος αχρησιμοποίητων δημόσιων IP:

- Παραγωγή μεγάλης κίνησης-θορύβου λόγω μαζικών ελέγχων IP από εξωτερικούς καλόβουλους ή κακόβουλους χρήστες του διαδικτύου (Gebauer 2012).
- Δύσκολος ο διαχωρισμός της κίνησης.

Εισαγωγή **ψεύτικων εγγραφών DNS** (honey token) σε DNS servers.

- Επιτιθέμενοι θα προσπαθήσουν να εκτελέσουν DNS zone transfer (Edge et al. 2010) ή να κάνουν "brute force" στους DNS servers για να μαζέψουν ονόματα στο υποδίκτυο.

Προσφέρει πρόωρη ενημέρωση για προσπάθεια συγκέντρωσης πληροφοριών μέσω DNS επιθέσεων.

Αντίμετρα: *web server tokens*

Οι δημόσιοι web servers αποτελούν πηγή πληροφοριών για hackers.

Τρία είδη honey tokens για εντοπισμό κακόβουλης κίνησης επισκεπτών:

- Προσθήκη **ψεύτικων εγγραφών στο robots.txt** (ανύπαρκτες αλλά ενδιαφέρουσες πηγές όπως *"/admin" ή "/login" στο robots.txt και παρακολούθηση requests*).
- Χρήση **αόρατων συνδέσμων σε ιστοσελίδες** (δεν τις χρησιμοποιούν κανονικοί χρήστες αλλά τις διαβάζουν εργαλεία που σαρώνουν αυτόματα τις ιστοσελίδες).
- Εισαγωγή honey-token(s) στον κώδικα **HTML** (*HTML σχόλιο σε σελίδα login που θα ελκύσει τον επιτιθέμενο να το χρησιμοποιήσει:*

```
<!--test account: admin, pass: passworD123. Remove before production!-->
```

Αντίμετρα: *social network avatars*

Δημιουργία avatars (ψεύτικα άτομα κοινωνικών ιστοσελίδων).

- Πρέπει να είναι όσο το δυνατόν πιο ρεαλιστικά.
- Να έχουν φίλους μέσα και έξω από την εταιρεία.
- Να κάνουν posts σε τακτά χρονικά διαστήματα.

Παρακολούθηση αλληλεπίδρασης με τους avatars (friend requests, ιδιωτικά μηνύματα, emails, etc.)

- Ύπαρξη πιθανότητας λανθασμένης αλληλεπίδρασης κανονικών χρηστών.

Αντίμετρα κατά την Εκτέλεση επίθεσης

Οι επιτιθέμενοι εφόσον αποκτήσουν πρόσβαση σε ένα σύστημα συνήθως:

1. Παραβιάζουν επιπλέον μηχανήματα και τα χρησιμοποιούν ως εναλλακτικές εισόδους.
2. Προσπαθούν να ανεβάσουν τα δικαιώματά τους (root, admin).
3. Εξερευνούν το εσωτερικό δίκτυο για συστήματα που έχουν την πληροφορία ή τον πόρο που στοχεύουν.

Αντίμετρα εξαπάτησης που μπορούν να χρησιμοποιηθούν σε αυτή την φάση:

- Εξαπάτηση σε επίπεδο δικτύου
- Εξαπάτηση σε επίπεδο εφαρμογών

Αντίμετρα κατά την Εκτέλεση επίθεσης: *επίπεδο δικτύου*

Οι επιτιθέμενοι προφανώς θα πρέπει να αποκτήσουν πρόσβαση στο δίκτυο, έτσι θα αφήσουν ίχνη και θα ενεργοποιήσουν συναγερμούς.

- **Darknet**: Διευθύνσεις IP που δρομολογούνται αλλά δεν χρησιμοποιούνται.
  - Κανένας workstation, server ή δικτυακή μηχανή δεν υπάρχει σε αυτό το τμήμα του δικτύου.
  - Πολλαπλές προσπάθειες σύνδεσης στις διευθύνσεις υποδεικνύουν χαρτογράφηση δικτύου.
- **Honeynets** (L. Spitzner 2003) για παρακολούθηση μεγαλύτερων/πιο περίπλοκων δομών και δικτύων.
  - Πολλαπλά ψεύτικα μηχανήματα στο ίδιο IP range που λειτουργούν σας κανονικοί workstations/servers.
  - Επιτιθέμενοι που αποκτούν πρόσβαση στο κομμάτι του δικτύου προφανώς θα προσπαθήσουν να αποκτήσουν πρόσβαση στα συστήματα καθώς δεν αναγνωρίζουν ότι δεν είναι αληθινά. Η αλληλεπίδραση αυτή ενεργοποιεί συναγερμό.

Αντίμετρα κατά την Εκτέλεση επίθεσης: *επίπεδο εφαρμογών*

- Ίδιες τεχνικές που είδαμε και για την εξαπάτηση επιτιθέμενων στους εξωτερικούς web servers.
- Επιπλέον τεχνικές:
  - **Honey tokens βάσης δεδομένων**:
    - ✓ honey tokens (honey records) σε βάσεις δεδομένων (π.χ. ψεύτικη πληροφορία που θα δελεάσει επιτιθέμενο όπως ψεύτικες πιστωτικές κάρτες, passwords κτλ.)
  - **Honey accounts**: Ψεύτικοι αλλά υπαρκτοί λογαριασμοί χρηστών.
    - ✓ Καθαρή ένδειξη επίθεσης.
    - ✓ Πρέπει να κατασκευαστούν έτσι ώστε πιθανή χρήση τους από επιτιθέμενο να μην προσφέρει κάτι στον hacker.

Αντίμετρα κατά την Εκτέλεση επίθεσης: *επίπεδο εφαρμογών*

- **Honey files**: ψεύτικα αρχεία με ενδιαφέροντα ονόματα και πληροφορίες μέσα (e.g. passwords.docx, new_investments.pdf, etc.)
  - ✓ Διανεμημένα σε όλους τους file servers και τερματικά για μέγιστη απόδοση, αλλά ίσως παράξουν και μερικούς λανθασμένους συναγερμούς.
  - ✓ Παρακολούθηση μέσω file system auditing ή χρήση κώδικα (π.χ. Javascript στα αρχεία pdf) που ενημερώνει για προσπέλαση στα αρχεία.

Συμπεράσματα Αντιμέτρων Εξαπάτησης

‘Level of involvement‘ (Symantec, 2010)

Όσο περισσότερο εμπλέκεται ένα honeypot στην κίνηση και την δομή ενός δικτύου, τόσο μεγαλύτερη αξία έχει αλλά ταυτόχρονα, τόσο μεγαλύτερο και η επικινδυνότητα του.

- **Low involvement**: Εύκολη εγκατάσταση και προσομοίωση μερικών services.
  - Περιορισμένο μέγεθος honeypot και υλοποιήσεων.
  - Προσομοιώνουν μόνο τις υπηρεσίες που συχνά ζητούν οι εισβολείς.
  - Δεδομένου ότι καταναλώνουν σχετικά λίγους πόρους, μπορούν να φιλοξενηθούν εύκολα πολλαπλές εικονικές μηχανές.
- **High involvement**: Πραγματικά συστήματα με πληθώρα services και σε σχετικά κεντρικά σημεία των δικτύων.
  - Ένας επιτιθέμενος έχει πρόσβαση σε πολλές υπηρεσίες και προγράμματα.
  - Χρησιμοποιώντας εικονικές μηχανές, μπορούν να φιλοξενούνται πολλαπλά honeypots σε μια ενιαία φυσική μηχανή.

Έμμεσος εντοπισμός κακόβουλου λογισμικού:

Ανάλυση συμπεριφοράς χρηστών

Ανάλυση συμπεριφοράς χρηστών

Εργαλεία monitoring όπως:

- Splunk, Bro, OSSEC για δίκτυα
- ArcSight and QRadar για παρακολούθηση ανθρώπινης δραστηριότητας.

Δυστυχώς τα περισσότερα υπάρχοντα συστήματα βασίζονται σε κανόνες και γνωστά patterns κακόβουλης συμπεριφοράς.

Ανάλυση συμπεριφοράς χρηστών

- Παγκόσμια τάση προς την κατασκευή και χρήση ενοποιημένων αρχιτεκτονικών γνωστών ως: **Security Information and Event Management (SIEM)**
  - User behavioral analysis and pattern development.
  - Log management
  - Anomaly detection
  - Incident forensics

Ανάλυση συμπεριφοράς χρηστών

Προσδιορισμός της διαφοράς ανάμεσα σε ύποπτη συμπεριφορά λογαριασμών και υπηρεσιών και στην κανονική συμπεριφορά υπαλλήλων.

- **Σύγκριση συμπεριφοράς** μέσω μιας δυναμικής ομαδοποίησης της κίνησης.
- **Ταξινόμηση βάσει επικινδυνότητας** για περαιτέρω ανάλυση από τους auditors.
- Χρήση **μαθηματικών αλγορίθμων** (π.χ. αλυσίδες Markov) και big data analytics για τον έγκαιρο εντοπισμό πιθανών απειλών.
- Διαρκής **μηχανική μάθηση** για προσδιορισμό της συμπεριφοράς χρηστών και εφαρμογών για αποτροπή false positives/negatives.
- Χρήση API calls και λεπτομερών συμπεριφορικών στοιχείων για την παραγωγή **high-level profiles συμπεριφοράς εφαρμογών**.

Ανάλυση συμπεριφοράς χρηστών: *Δομή*

- **Ενιαίο framework** για την ανάλυση χρηστών, κίνησης, χρήσης αγαθών και δεδομένων μαζί με πληροφορίες από logs και IDS.
- Σύγκριση και **εντοπισμός «μη-ομαλής» χρήσης** λογαριασμών και υπηρεσιών σε πραγματικό χρόνο.
- Δυνατότητα εντοπισμού γεγονότων υψηλής επικινδυνότητας μεταξύ **δισεκατομμυρίων εγγραφών**.
- **Πλήρης ανάλυση** δικτύων, εφαρμογών και ανθρώπινης συμπεριφοράς.
- Συνδυασμός μεθόδους στατιστικής ανάλυσης, με πολιτικές ασφάλειας και έλεγχο καταγραφής (logs) εφαρμογών και συστημάτων.
- Εκμάθηση δυναμικών και μοναδικών συμπεριφορών χρηστών.
- Παραγωγή συναγερμών όταν παρουσιάζεται απόκλιση συμπεριφοράς από την στατιστική μελέτη.
- Συγκερασμός συμπεριφοράς χρηστών από πολλαπλές πλατφόρμες.

Ανάλυση συμπεριφοράς χρηστών: *Δομή*

Μαθηματικά μοντέλα ανάλυσης συμπεριφοράς (Chari, 2013)(Teodoro, 2009):

1. **Baseline distributions:** Για κάθε χρήστη σε σχέση με μια ομάδα πράξεων, υπολογίζεται η απόκλιση από μια βασική κατανομή. Όταν η απόκλιση γίνεται στατιστικά σημαντική, ενεργοποιείται συναγερμός.
2. **Markov properties.** Οι κινήσεις και οι εντολές χρηστών μοντελοποιούνται με βάση ροές συνηθισμένων πράξεων (workflows).

   Π.χ. Σε μια εφαρμογή source code management, ένας χρήστης (1) ανανεώνει τον κώδικα σε έναν τοπικό brach, (2) βλέπει εκκρεμείς υποχρεώσεις και bugs που του αναλογούν, (3) κάνει αλλαγές κώδικα (4) καταθέτει τις αλλαγές του και αλλάζει τα flags.

Ανάλυση συμπεριφοράς χρηστών: *Δομή*

3. **Στατιστικές αναλύσεις:** Κλασικά μοντέλα βάσει στατιστικών αποκλίσεων. Π.χ. για συγκεκριμένη περίοδο, υπολογίζεται η ιστορική κατανομή κίνησης και υπολογίζεται η πιθανότητας βάσει δείγματος από την κατανομή.

4. **Μέθοδοι Εντροπίας**: Διαφοροποίηση ανθρώπινης χρήσης από batch processes με πολύ μεγάλη ακρίβεια.
5. Π.χ. εντοπισμός χρήσης account από malware αντί της ορθής χρήσης του account.

6. **Γενικές τεχνικές clustering,** όπως Gaussian μοντέλα. Ομαδοποίηση χρηστών σε υποσύνολα για εύκολη σύγκριση και προσδιορισμό αλλαγής συμπεριφοράς.

Συμπεράσματα

- Ο εντοπισμός και η αντιμετώπιση επιθέσεων και εισβολών απαιτεί το συνδυασμό:
  - παραδοσιακών εργαλείων ασφάλειας δικτύων (Firewall, IDS/IPS)
  - και μη συμβατικών εργαλείων ασφάλειας δικτύου (APT countermeasures, honeypots, honeytokens, user behavior analysis, SIEM).

- Συνεχής ανάπτυξη νέων απειλών (0-day exploits, APTs)
- Διαρκής έρευνα για ανάπτυξη μεθόδων για τον έγκαιρο εντοπισμό και αντιμετώπιση εξελιγμένων και άγνωστων απειλών.

Αναφορές

1. N. Virvilis, Facilitating Unconventional Defenses against Advanced Persistent Treats, PhD Thesis, Dept. of Informatics, Athens University of Economics & Business, Greece, October 2015.
2. Libicki, M., Sentry, D. & Pollak, J., 2014. An Examination of the Cybersecurity Labor Market, Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf
3. Gebauer, M., 2012. Warfare with Malware: NATO Faced with Rising Flood of Cyberattacks, Spiegel.
4. Spitzner, L., 2003. Honeypots: Catching the insider threat. In Computer Security Applications Conference, 2003. Proceedings. 19th Annual. pp. 170–179.
5. Sanae Rosen, Zhiyun Qian, and Z. Morely Mao. 2013. AppProfiler: a flexible method of exposing privacy-related behavior in android applications to end users. In Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13). ACM, New York, NY, USA, 221-232.
6. SYMANTEC, Community: Security, The Value of Honeypots, 2010, http://www.symantec.com/connect/articles/value-honeypots-part-two-honeypot-solutions-and-legal-issues
7. Jean-Paul Bergeaux, Insights from Black Hat and DEFCON 2015: Rethinking Honeypots, 2015, http://cyberattackdefenders.com/blog/insights-from-black-hat-and-defcon-2015-rethinking-honeypots-early-warning-can-deliver-real-business-value/
8. Suresh Chari, Ted Habeck, Ian Molloy, Youngja Park, and Wilfried Teiken. 2013. A bigData platform for analytics on access control policies and logs. In Proceedings of the 18th ACM symposium on Access control models and technologies (SACMAT '13). ACM, New York, NY, USA, 185-188.
9. P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez. 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput. Secur. 28, 1-2 (February 2009), 18-28.
10. Phyllis Schneck, Modern Department of Homeland Security Cyber: Our Vision Forward, Hackers & Threats, RSAConference 2015