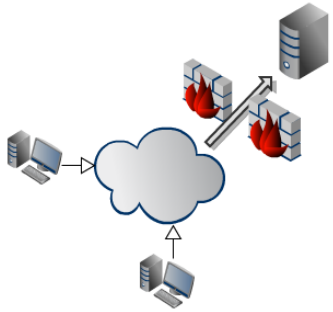
Τείχος Προστασίας Εφαρμογών Διαδικτύου

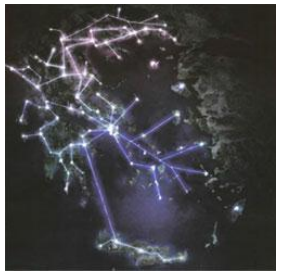
Web Application Firewalls

Ιωάννης Στάης
{istais@census-labs.com}

Γιατί είναι σημαντική η προστασία των εφαρμογών ιστού;

- **Πάνω** από **70%** όλων των επιθέσεων συμβαίνουν στο **επίπεδο εφαρμογών ιστού**
- Αποτελούν μία **καθιερωμένη είσοδο σε ένα σύστημα**. Τα κοινά τείχη προστασίας επιπέδου δικτύου επιτρέπουν την πρόσβαση στις εφαρμογές ιστού.



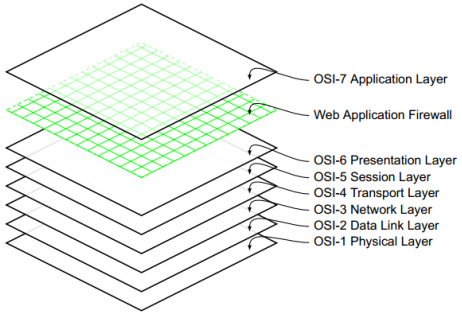


- Το **2010**, υπήρχαν περισσότερες από **400.000** ιστοσελίδες με Ελληνικό domain
- Αυξανόμενος αριθμός κυβερνητικών ιστοσελίδων και γενικότερα σελίδων σημαντικών υποδομών

census®

Τι είναι τα Web Application Firewalls; (WAFs)

- Αποτελούν ένα **εξωτερικό στρώμα ασφάλειας**
- Μπορεί να είναι **είτε λογισμικό, είτε συσκευή**. Συνήθως είναι **εγκατεστημένα μεταξύ** του πελάτη και του εξυπηρετητή, αλλά μπορεί να είναι και **ενσωματωμένα** στον εξυπηρετητή.
- HTTP/HTTPS/SOAP/XML-RPC
- θεωρούνται μέρος της οικογένειας των **Deep Packet Inspection Firewalls**



census®

Πώς λειτουργούν;

Αναζητούν:

- Συγκεκριμένες «**υπογραφές**» - ίχνη επιθέσεων
- **Μοτίβα** που περιγράφουν «οικογένειες» επιθέσεων
- **Μη φυσιολογική συμπεριφορά**, που δεν ταιριάζει με την αναμενόμενη κίνηση της ιστοσελίδας

Negative model – «Μαύρη Λίστα»
Positive model – «Λευκή Λίστα»
Mixed model (mix negative and positive model protection).

- Ελέγχουν κάθε εισερχόμενο αίτημα αλλά και κάθε **εξερχόμενη απάντηση** του εξυπηρετητή

Από ποιες επιθέσεις προστατεύουν;

Αναγνωρίζουν:

- Cross-site scripting (XSS)
- SQL injection
- header injection
- Directory traversal
- Remote File Inclusion
- Local File Inclusion
- Denial of Service (DoS)
- ...

census®

Από ποιες επιθέσεις προστατεύουν;

- **Ιστοσελίδα με ευπάθεια ένεσης sql κώδικα:**

http://www.victim.com/index.php?id=1

- **Επίθεση ένεσης sql κώδικα:**

*http://www.victim.com/index.php?id=1' union select * from users; --*

- **Τείχος προστασίας εφαρμογής ιστού, που αναγνωρίζει το μοτίβο** «union.*select» **ως ίχνος επίθεσης**

*http://www.victim.com/index.php?id=1' union **\ select * from users; --*

census®

Χρήσεις:

- Κατάλληλο εργαλείο για την επίτευξη **βιομηχανικών προτύπων ασφάλειας**, καθώς και την εκπλήρωση **νομικών απαιτήσεων**
- Σημαντικό στην περίπτωση **τρωτών σημείων που δεν έχουν ανακαλυφθεί** μέσω δοκιμών διείσδυσης ή κατά τον έλεγχο του πηγαίου κώδικα
- **Εύκολη παραμετροποίηση**
- Εξασφάλιση προστασίας για εφαρμογές με **πολλαπλές υπό-εφαρμογές**
- **Κεντρική διαχείριση** λαθών, ασφάλειας συνόδου
- **Επιπρόσθετοι μηχανισμοί ασφάλειας**

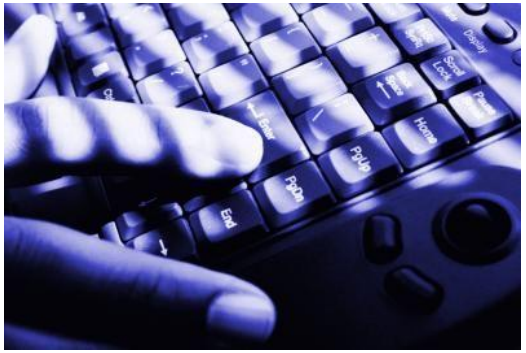
Ρίσκα:

- Αυξάνετε η **πολυπλοκότητα διαχείρισης** της πληροφοριακής υποδομής
- Απαιτούνται **νέα μοντέλα οργάνωσης**
- **Ψευδώς θετική** αναγνώριση επίθεσης
- Πιο **σύνθετη αντιμετώπιση προβλημάτων**
- Οι **καταστάσεις σφάλματος** επηρεάζουν **ολόκληρο το σύστημα**

census®

Open Source WAFs

- ModSecurity
- PHPIDS



census®

ModSecurity

- **Ενσωματώνεται στους εξυπηρετητές**: Apache (Stable), IIS (Beta), Nginx(Beta)
- Ο διαχειριστής της εφαρμογής καλείται να προσδιορίσει το μοντέλο ασφάλειας(black list,white list,…)
- Ελέγχει τόσο την **εισερχόμενη** κίνηση όσο και τυχόν **εξερχόμενες** διαρροές πληροφοριών.
- **5 στάδια επεξεργασίας**: request headers, request body, response headers, response body, και logging
- Υποστηρίζει anomaly scoring και συσχέτιση συμβάντων
- Παρέχεται υπό την άδεια Apache Software License v2

census®

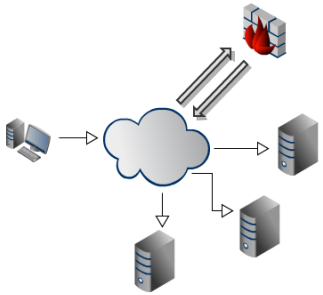
PHPIDS

- **Ενσωματώνεται στον εξυπηρετητή η ακόμα και στις ίδιες τις εφαρμογές ιστού** που είναι υλοποιημένες σε **PHP**
- Εφαρμόζει την προσέγγιση **μαύρη λίστα**, σε συνδυασμό με τις προσπάθειες για τον εντοπισμό άγνωστων επιθέσεων με την εφαρμογή **ευρετικών μεθόδων**.
- Αναλύει τις **μεταβλητές εισόδου** POST, GET, SESSION, COOKIE
- Αυτόματη επιλογή δράσης βάσει **αριθμητικής αξιολόγησης επιθέσεων**.
- Παρέχεται υπό την άδεια LGPL

census®

Cloud Based WAF

- **Software-as-a-Service** (SaaS) μοντέλο λειτουργίας
- **Εύκολη Ενσωμάτωση**
- Παρέχεται σαν υπηρεσία μέσω μίας απλής αλλαγής στις ρυθμίσεις DNS
- **Χαμηλότερο** συνολικό **κόστος** ιδιοκτησίας
- **Συγκεντρωτική Ανάλυση** Απειλών



census®

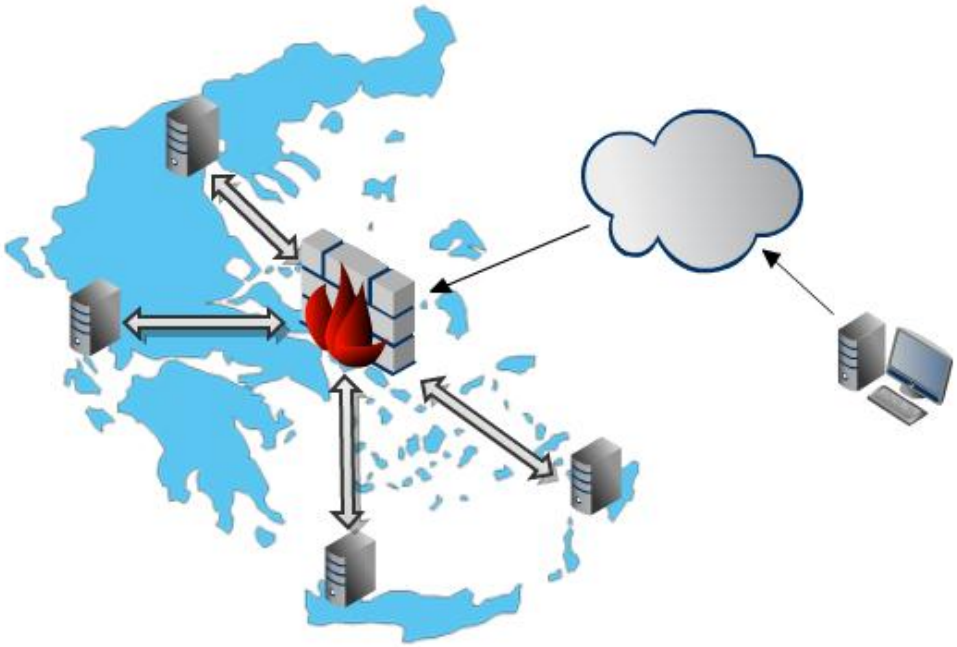
Παρακάμπτοντας ένα WAF

- Καμία λύση WAF **δε μπορεί** να εγγυηθεί την **πλήρη ασφάλεια** ενός ιστοτόπου

- Υπάρχει εκτενής ερεύνα σε ακαδημαϊκό και μη επίπεδο σχετικά με **τεχνικές παράκαμψης**
- Μέθοδος **δοκιμής – αποτελέσματος**
- **Αλλαγή** του **ίχνους-υπογραφής**
- Αξιοποιώντας **ελλείψεις** στο μοτίβο
- Αλλά και στον τρόπο που λειτουργεί η «μηχανή» του τείχους

census®

Κυβερνοάμυνα και Federated WAFs



census®

Ερωτήσεις;