SIP THREAT MANAGER

Προστασία με Deep packet inspection

Η ραγδαία στροφή των επιχειρήσεων στις IP τηλεπικοινωνίες, έχει προσελκύσει το ενδιαφέρον των χάκερς και πλέον οι επιχειρήσεις και οι οργανισμοί αντιμετωπίζουν συνεχείς επιθέσεις αλλά και πρόσβαση από ανεπιθύμητα μέρη.

Οι συχνότερες VOIP επιθέσεις σε IP τηλεφωνικά συστήματα σήμερα είναι οι εξής:

DoS/DDoS επιθέσεις. Είναι σχεδιασμένες για να κατακλύζουν τα IP PBXs με έναν υπερβολικό αριθμό πακέτων. Στόχος τους είναι να καταρρίψουν το σύστημα επικοινωνίας και να το αχρηστεύσουν.

PHREAKERs. Αυτοί οι τύποι εκμεταλλεύονται την απροσεξία των χρηστών και κλέβουν χωρίς στην πραγματικότητα να χακάρουν τίποτα... Απλώς ελέγχουν τα πιο κοινά/προεπιλεγμένα ονόματα χρηστών και τους κωδικούς πρόσβασης, και αν σταθούν τυχεροί, τότε πρόκειται για μια κακή μέρα του θύματός τους.

Buffer overflow. Ένας αριθμός από απάτες σε VoIP συστήματα, στηρίζεται σε μεθόδους που συνήθως χρησιμοποιούνται για απάτες μέσω υπολογιστών. Σε αυτή την περίπτωση, οι απατεώνες χρησιμοποιούν buffer overflow errors για το χειρισμό πακέτων INVITE ή SIP (session initiation protocol). Αυτά θα μπορούσαν να χρησιμοποιηθούν για να συντρίψουν εφαρμογές ή για την εκτέλεση αυθαίρετου κώδικα.

SIP Device Fingerprinting. Σε αυτό τον τύπο επίθεσης, ο χάκερ προσπαθεί να αναγνωρίσει ποιό PBX λογισμικό τρέχει ή ποιό hardware χρησιμοποιείται. Μόλις λάβει αυτή την πληροφορία, αναζητά αδυναμίες και επιτίθεται αναλόγως.

Cross Site Scripting επιθέσεις. Πρόκειται για κάποιες από τις πιο περίπλοκες και δύσκολα επιτεύξιμες επιθέσεις. Μια δέσμη ενεργειών εγχέεται στο PBX από τον χάκερ, που μπορεί να το προγραμματίσει να κάνει κακόβουλες ενέργειες όλων των ειδών, όπως το να ηχούν όλες οι τηλεφωνικές προεκτάσεις ταυτοχρόνως.

Toll Fraud επιθέσεις. Χάκερς εισβάλλουν στο τηλεφωνικό σύστημα εταιριών, ώστε να καλούνται επανειλημμένως υπεραστικοί αριθμοί που χρεώνουν την κλήση ανά λεπτό. Ο ιδιοκτήτης του υπεραστικού αριθμού – συνήθως ο χάκερ ή κάποιος συνεργάτης του – χρεώνει την εταιρεία για την χρήση της τηλεφωνικής γραμμής.

Ο στόχος λοιπόν κάθε ICT είναι να προστατεύει και να ασφαλίζει τα τηλεφωνικά συστήματα των πελατών του. Κατά μέσο όρο, μία τέτοια επίθεση κοστίζει μερικές χιλιάδες ευρώ. Το STM της Allo εγκαθίσταται πριν από οποιοδήποτε SIP based IP PBX ή gateway προσφέροντας πολλαπλά επίπεδα ασφάλειας ενάντια σε πολυάριθμους τύπους επιθέσεων. Θέλετε να αποκλείσετε συγκεκριμένες IPs ή χώρες, θέλετε να προστατεύσετε το PBX από hackers που προσπαθούν να αποκτήσουν πρόσβαση δοκιμάζοντας πολλαπλά usernames και passwords, θέλετε να προστατεύστε το PBX από DDoS επιθέσεις και SIP protocol injections; Κανένα πρόβλημα! Χρησιμοποιώντας την SNORT based Real Time Deep packet inspection μηχανή, το STM της Allo αναλύει κάθε SIP πακέτο που πηγαίνει στο τηλεφωνικό σύστημα, εντοπίζει τα κακόβουλα και τα ανώμαλα sessions μπλοκάροντας δυναμικά την IP από όπου προέρχονται.

Partnernet (www.partnernet.gr), τηλ.: 210-2116501 sm