Ασφάλεια Συστημάτων και Υπηρεσιών - ΗΡΥ 413

Αστερινός Καράλης – Ζωγραφούλα Ιωάννα Νεαμονιτάκη

Part 4

Ο κανόνας που γράφτηκε παρουσιάζεται παρακάτω:



Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, αριθμός, γραμματοσειρά

Περιγραφή που δημιουργήθηκε αυτόματαTo slammer worm αποτελείται από μόνο ένα πακέτο, το οποίο χρησιμοποιούσε το UDP πρωτόκολλο καθώς είναι πιο ελαφρύ και δεν χρειάζεται handshake όπως το TCP. Το worm έστελνε το πακέτο στο port 1434 του δέκτη με συγκεκριμένα περιεχόμενα όπου περιλαμβάνανε τα strings:

* "h.dllhel32hkernQhounthickChGetTf"
* "hws2"
* "Qhsockf"
* "toQhsend"

Τα οποία ήταν συγκεκριμένα 376 bytes.

Με αυτές τις πληροφορίες για το slammer worm δημιουργήθηκε ο snort κανόνας ο οποίος κοιτάει πακέτο με UDP πρωτόκολλο να στέλνετε συγκεκριμένα στο port 1434 με περιεχόμενα μέρος από ένα από τα 4 strings και μέγεθος μεγαλύτερο από 300 bytes.

Εικόνα που περιέχει κείμενο, στιγμιότυπο οθόνης, γραμματοσειρά

Περιγραφή που δημιουργήθηκε αυτόματαΠαρακάτω φαίνεται το alert που δημιουργεί:

Οι πληροφορίες διαβάστηκαν από το παρακάτω paper:

[MS SQL Slammer/Sapphire Worm](https://www.giac.org/paper/gsec/3091/ms-sql-slammer-sapphire-worm/105136)