УДК 004.78 (043.2)

Скорін К.О.
Національний авіаційний університет

ПРОГРАМНИЙ МОДУЛЬ ПРОТИДІЇ ШКІДЛИВИМ ПРОГРАМАМ ДЛЯ ОПЕРАЦІЙНИХ СИСТЕМ РОДИНИ MICROSOFT WINDOWS

Спеціально створена DDoS атака рівня додатків дозволяє каскадно вивести з ладу системи, використовуючи набагато менший обсяг ресурсів у порівнянні з тими ресурсами, які необхідні для проведення традиційних DDoS атак. Подібний розклад можливий через складні взаємозв'язків, що існують між додатками.

Зловмисник може створити витончені шкідливі запити, що імітують легітимний трафік, який буде проходити через всі захисні системи, в тому числі і WAF (web application firewall).
Згідно зі звітом компанії Akamai, DDoS атаки на рівні додатків займають менше 1% серед всіх DDoS атак. Однак ця метрика не відображає ступінь впливу подібних атак. Коли зловмисник витрачає час на підготовку плану DDoS-атаки, ефективність цього сценарію зростає в рази. З огляду на цей факт, при захисті від подібного типу атак в першу чергу необхідно переконатися, що на всіх комп’ютерах корпоративної мережі не відбудеться вихід з ладу систем лавиноподібним чином. Саме для цього було розроблено програмний модуль виявлення саме даного типу вірусів.

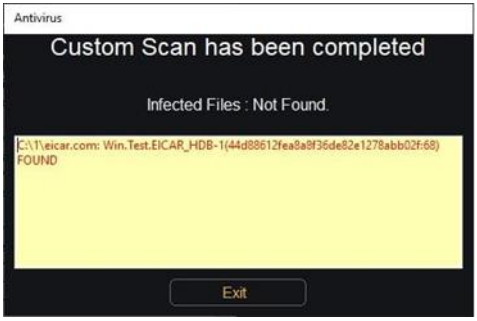

Рис. Вікно з попередженням про виявлення вірусу для DDoS

атаки рівня додатків