МЕХАНІЗМ РЕАЛІЗАЦІЇ АТАКИ ТИПУ MAN-IN-THE-MIDDLE НА ПРОЦЕС SLAAC IPv6

Калінєнкова А.Л.
Науковий керівник – к.т.н., доцент Снігуров А. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20), E-mail: anastasiia.kalinienkova@nure.ua

Internet network is a giant network of computers around the world. The billions of devices are constantly connected to each other for the information transmission and reception. The IP address is used for identifying the device on the Internet and route traffic to specific devices. IPv6 network protocol is an improved IPv4 replacement, which will soon end the address space. Now the world is in the conditions where IPv6 becomes an integral part of the network environment, which means attacks will be more frequent.

Актуальність теми дослідження. в кінці лютого 2018 року була зафіксована перша масштабна DDoS-атака по протоколу IPv6. Постраждала UltraDNS - DNS-мережа компанії Neustar, яка обробляє 10% всього інтернет-трафіку. Перехід на протокол IPv6 підтримують світові провайдери та інтернет-компанії, відповідно до цього можна прогнозувати зростання кількості кібератак по даному протоколу.

Мета дослідження. Аналіз існуючої вразливості у протоколі IPv6 – SLAAC, яка дає можливість провести атаки типу MitM на ураження функціональності та розкриття конфіденційної інформації, яка передається.

Для проведення однієї з найефективніших атак зловмиснику потрібно розмістити та приєднати свій IPv6-маршрутизатор до спеціальної мультикаст-групи FF02::2, запустити DHCPv6-сервер (для конфігурації вузлів версії 6 з IP-адресами, префіксами IP), DNSv6 (мережевий протокол для налаштування хостів Інтернет-протоколу версії 6 з IP-адресами, префіксами IP) і NAT64-транслятор.

Як тільки будь-який маршрутизатор приєднається до спеціальної мультикаст-групи FF02::2, він відразу ж починає розсилати RA повідомлення про об'яву маршрутизатора (далі - RA) (рисунок 1). Cisco-маршрутизатори розсилають їх кожні 200 с. за замовчуванням. Нюанс полягає в тому, що клієнтам не потрібно чекати 200 с., вони відправляють RS повідомлення запиту маршрутизатора (далі - RS) на ці мультикаст-адреса і таким чином негайно вимагають всю інформацію.

Якщо маршрутизатору зловмисника вдасться вставити себе в RA повідомлення, він зможе підробити оголошення маршрутизатора ICMPv6 від маршрутизатора клієнта, яке встановлює час життя повідомлення 2 години. Згідно RFC 4862, «якщо час RemainingLifetime менше або дорівнює 2-м годинам, ігноруйте параметр «Інформація про префікс» щодо

дійсного часу роботи, якщо тільки оголошення маршрутизатора, з якого отримано цей параметр, не було аутентифіковано». Це може привести до припинення роботи адреси маршрутизатора клієнта через 2 години, і маршрутизатор зловмисника зможе потім відправити оголошення нового маршрутизатора з новим префіксом (відображається як 2001:DB8:BAD::/64). Побачивши новий префікс, маршрутизатор клієнта вибере нову адресу (показану як 2001: DB8:BAD::A).

Рисунок 1 – Етапи атаки SLAAC IPv6

Перехопивши RS запит маршрутизатора клієнта, зловмисник може підмінити RA відповідь маршрутизатора і вказати у відповіді підроблені налаштування. В якості шлюзу за замовчуванням зловмисник вказує свій пристрій, і весь трафік клієнта, який передається в зовнішні мережі, буде проходити через атакуючого. Згодом, завдяки механізму Stateless Address Autoconfiguration (далі - SLAAC) пристрої отримують свій префікс, довжину префікса і адресу шлюзу від IPv6 маршрутизатора зловмисника.

Пристрій зловмисника виступить в якості проксі сервера між клієнтом і зовнішніми мережами. При цьому весь трафік, який проходитиме через маршрутизатор зловмисника, схильний до атаки MITM, також тому, що зловмисник може призначити помилковий DNS сервер внутрішнім хостам. Невірний DNS-сервер дозволить зловмиснику перенаправити весь внутрішній трафік на будь-яку кількість фішингових сайтів.

Висновки. Результати роботи пропонується використовувати для створення математичної моделі даної атаки, а також розробки механізмів захисту системи маршрутизації від кібератак.

Література:

1. IPv6 First-Hop Security Concerns – [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/about/security-center/ipv6-first-hop.html?fbclid=IwAR0yGa_0cSR4HJjhWh2cdZI4kWf8997rtkHOu6HawsBppPVvT7lXomD3JQ#5a.
2. IPv6 — это весело, часть 2 – [Електронний ресурс]. – Режим доступу до ресурсу: https://habr.com/ru/post/254293/.