УДК 510.635:004.891(045)

І.О. Шиян
Національна академія Служби безпеки України, Київ

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ КОНТРОЛЮ ЗА ДОПОМОГОЮ IP-КАМЕР У БОРОТЬБІ ПРОТИ АГРЕСОРА

У 2022 році практично неможливо обійтися без камер відеоспостереження, особливо набрали популярності IP-камери [1]. Вони призначені для запобігання крадіжкам майна в магазинах, будинках, бізнес-закладах. Але іноді камери служать помічником для стеження або крадіжки. Саме тому важливо дослідити вразливості IP-камер, до яких належать всі проблеми, пов'язані з реалізацією функціональності IP-камер. Головна з них полягає в тому, що вартість апаратної частини камер значно менша, ніж витрати на розробку прошивки. Результатом прагнення компаній заощадити стають найдивніші рішення, наприклад:

1. не оновлювані прошивки або прошивки без автоматичного оновлення;
2. можливість отримати доступ до веб-інтерфейсу камери шляхом багаторазових спроб ввести неправильний пароль або натискання кнопки «Скасувати»;
3. відкритий доступ до всіх камер із сайту виробника;
4. заводський сервісний обліковий запис зі стандартним паролем або без нього, що не відключається (таку вразливість використовувала в 2016 році хакерська група Lizard Squad для створення DDoS-ботнета з потужністю атак до 400 ГБ/с з камер відеоспостереження);
5. можливість несанкціонованої зміни налаштувань навіть при включеній авторизації та забороні анонімного доступу;
6. відсутність шифрування відеопотоку та/або передача облікових даних у відкритому вигляді;
7. використання вразливого веб-сервера GoAhead;
8. тиражування вразливих прошивок (поширене серед китайських виробників пристроїв);
9. вразливості пристроїв для зберігання відео - наприклад, зовсім недавно була опублікована інформація про проникнення на мережні накопичувачі Synology і Lenovo Iomega шкідливих файлів, що видаляють або шифрують і вимагають викуп [2].

CVE - (Common Vulnerabilities and Exposures) - база даних загальновідомих уразливостей інформаційної безпеки. Кожній вразливості надається ідентифікаційний номер виду CVE-рік-номер, опис та ряд загальнодоступних посилань з описом [3].

Навіть якщо виробники камер виправлять усі помилки та випустять ідеальні з точки зору безпеки камери, це не врятує ситуацію, оскільки нікуди не подінуться рукотворні вразливості [4], причина яких у людях, які обслуговують обладнання, наприклад, використання паролів за замовчуванням, якщо є можливість змінити їх; відключення шифрування або VPN, якщо камера дозволяє його використовувати (заради справедливості скажемо, що далеко не всі камери мають достатню продуктивність для такого режиму роботи, перетворюючи цей спосіб захисту на чисту воду декларацію); відключення автоматичного оновлення прошивки камери; забудькуватість або недбалість адміністратора, що не оновлює прошивку пристрою, який не вміє робити це автоматично.

За допомогою зламаних IP-камер відеоспостереження на території країни-агресора або окупованих територіях особливо цінуються камери з виходом на дорогу та підозрілі будівлі. Завдяки цим даним можна стежити за рухом окупантів і коригувати артилерію на техніку і бази навіть не доїхавши до території України. Дані зі зламаних камер передаються в Службу безпеки України для того, щоб зібрати повну картину на окупованих територіях.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Що таке IP-камера: основні відмінності від аналогових та цифрових камер відеоспостереження, URL: https://smartel.ua/articles/chto-takoe-ip-kamera-osnovnye-otlichiya-ot-analogovykh-i-tsifrovykh-kamer-videonablyudeniya/

2. Вразливість безпеки у стандартній реалізації Dahua Open Network Video Interface Forum. URL: https://www.onvif.org/

3. Курс Cisco Networking Academy: IT Essentials.

4. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні інформаційні: Мережі, технології, безпека, економіка, регулювання. – Видання друге (доповнене). – / За загальною ред. Довгого С.О. – К.: «Азимут-Україна». – 2013. – 608 с.