УДК 004.492
DOI: 10.33764/2618-981X-2021-6-167-171

ИДЕНТИФИКАЦИЯ IOT-УСТРОЙСТВ ВО ВНУТРЕННЕМ ПЕРИМЕТРЕ ОРГАНИЗАЦИИ

Наталья Дмитриевна Кульбякина
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел. (905)988-86-87, e-mail: n.kulbyakina@yandex.ru

Дмитрий Евгеньевич Пешков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (905)930-46-54, e-mail: peshkowdima@yandex.ru

Глеб Владимирович Попков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент кафедры информационной безопасности, тел. (383)343-91-11

Проблема безопасности IoT устройств присутствует с их появления из-за небезопасной разработки как устройств, так и их компонентов. Вследствие чего в IoT устройствах присутствуют множественные уязвимости. Отмечено, что в новых версиях программного обеспечения используются безопасные протоколы передачи информации, а также уделяется большее внимание безопасности прошивок. Несмотря на это большая часть новых устройств всё ещё не получают патчей безопасности и обновлений.

Ключевые слова: IoT устройства, уязвимость, патч, обновление, мониторинг, трафик, информационная безопасность

IDENTIFYING IOT DEVICES IN THE INTERNAL PERIMETER OF THE ORGANIZATION

Natalia D. Kulbyakina
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, phone: (905)988-86-87, e-mail: natashak-2009@mail.ru

Dmitry E. Peshkow
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (905)930-46-54, e-mail: peshkowdima@yandex.ru

Gleb V. Popkov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security, phone: (383)343-91-11

The security problem of IoT devices has been present since their appearance due to the unsafe development of both devices and their components. As a result, there are multiple vulnerabilities in IoT devices. Now things are a little better, secure data transfer protocols have begun to be used, and

more attention is being paid to the security of firmware. But still, even new devices don't get security patches or banal updates.

Keywords: IoT devices, vulnerability, patch, update, monitoring, traffic, information security

Введение

Проблема безопасности IoT устройств присутствует с их появления из-за небезопасной разработки как устройств, так и их компонентов. Вследствие чего в IoT устройствах присутствуют множественные уязвимости. Однако, стоит отметить, что в новых версиях программного обеспечения стали использоваться безопасные протоколы передачи информации, а также уделяется большее внимание безопасности прошивок. Несмотря на это большая часть новых устройств всё ещё не получают патчей безопасности и обновлений. Именно поэтому специалистам информационной безопасности в организации нужно проверять IoT устройства на наличие в них уязвимостей и патчей безопасности.

Но что делать, если в офисе десятки или сотни IoT устройств, которые имеют разные версии и операционные системы (ОС)? Специалисту нужно достаточно быстро (в разумных пределах) узнать версии этих устройств и в случаях обнаружения уязвимостей принять меры. В итоге мы сможем узнать какие IoT устройства присутствуют в нашей сети, а главное являются ли они уязвимыми.

Методы и методики

Для решения проблемы мониторинга и отслеживания уязвимых версий IoT устройств в локальной сети нужно выполнить следующие задачи:

- написать программу получения информации из трафика локальной сети;
- написать программу обработки результатов;
- написать программу перехвата и обработки трафика для подготовки к анализу.

Для получения информации из трафика локальной сети нужно анализировать DHCP [1] пакеты. DHCP - это сетевой протокол [**Ошибка! Источник ссылки не найден.**], позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Так как ключевой особенностью IoT устройств является выход в интернет или работа в локальной сети, то данные устройства получают IP-адрес и используют протокол DHCP. В протоколе содержится информация, по итогам анализа которой удастся определить версию операционной системы устройства.

Для анализа трафика первым делом нужно этот трафик получить. Есть множество способов это сделать. В данной работе воспользуемся разработанной программой, которая перехватывает трафик в сети организации, реализо-

ванной на базе языка программирования python3. Ниже приведен фрагмент программы, которая отвечает за перехват трафика [**Ошибка! Источник ссылки не найден.**].

```
a = sniff(iface="eth0", count=200)
        wrpcap("temp.pcap",a)
```

Листинг 1. Перехват сетевого трафика

Данный код будет формировать трафик в пакеты фиксированной длины, сохранять их в файл и передавать его на анализ. В зависимости от количества трафика компании размер пакета может быть увеличен.

Следующим шагом необходимо произвести анализ файла с записанным трафиком и получить информацию, при анализе которой будет получена версия IoT устройства. Для того чтобы произвести такой анализ нам нужна следующая информация:

- dhcp fingerprint;
- dhcp vendor;
- mac address;
- ja3 token;
- user-agent.

Ключевым значением является dhcp fingerprint. Зная dhcp fingerprint устройства, его можно будет сравнить с другими значениями в FingerBank (база отпечатков, на их основе будет сделан вывод об устройстве). Для этого была написана программа, позволяющая получить всю необходимую информацию. Для повышения точности распознавания версий и ОС устройства необходимо передавать ja3 token [**Ошибка! Источник ссылки не найден.**] и user-agent. Данная информация встречается только в HTTPS пакетах.

Таким образом для получения максимально точной информации необходимо также прослушивать трафик с 443 порта [**Ошибка! Источник ссылки не найден.**].Ниже приведен фрагмент программы, которая отвечает за анализ DHCP и HTTPS пакетов. Программа анализирует каждый полученный пакет и сопоставляет информацию об устройстве по средствам MAC-адреса, так как он присутствует в обоих протоколах.

```
record = {"source_ip": convert_ip(ip.src),
                    "destination_ip": convert_ip(ip.dst),
                    "source_port": udp.sport,
                    "destination_port": udp.dport,
                    "DHCPFP": dhcpfp,
                    "DHCPFP_hash": md5(dhcpfp.encode()).hexdigest(),
                    "timestamp": ts,
                    "DHCP_vendor":VENDOR,
                    "Mac_src":mac_addr(eth.src),
                    "Mac_dst":mac_addr(eth.dst),
                    "device_name":NAME,
                    "ja3":i['ja3_digest']}
        else:
            record = {"source_ip": convert_ip(ip.src),
                    "destination_ip": convert_ip(ip.dst),
                    "source_port": udp.sport,
                    "destination_port": udp.dport,
                    "DHCPFP": dhcpfp,
                    "DHCPFP_hash": md5(dhcpfp.encode()).hexdigest(),
                    "timestamp": ts,
                    "DHCP_vendor":VENDOR,
                    "Mac_src":mac_addr(eth.src),
                    "Mac_dst":mac_addr(eth.dst),
                    "device_name":NAME,
                    "ja3":'None'}
      results.append(record)
    return results
```

Листинг 2. Получение информации из сетевого трафика

Результатом работы данной программы будет информация, которую необходимо направить в базу данных - FingerBank и получить информацию об IoT устройстве. Ниже представлен вывод ответа базы данных FingerBank. После чего эта информация используется для анализа версий.


```
{
   "operating_system": {
      "can_be_more_precise": true,
      "child_devices_count": 3,
      "child_virtual_devices_count": 0,
      "created_at": "2017-09-18T15:49:16.000Z",
            "name": "Apple OS"
   "request_id": "e7581d68-ddd6-4af9-ab4a-fecf0cb1f515",
   "score": 87,
   "version": "10"
}
```


Листинг 3. Результат работы

Результаты

В результате данной работы была написана программа, которая перехватывает и анализирует трафик в реальном времени и определяет версию устройства, что значительно облегчает поиск уязвимостей и позволяет предотвращать утечки информации или хакерские атаки.

Заключение

Обеспечение безопасности устройств, находящихся в сети организации, важная задача, которую должен обеспечивать дипломированный специалист по информационной безопасности. От скорости и качества выявления новых устройств в сети и уже уязвимых устройств зависит безопасности и целостность данных компании.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. DHCP [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/DHCP (дата обращения: 05.03.2020).

2. DHCP - Dynamic Host Configuration Protocol [Электронный ресурс]. URL: https://www.elektronik-kompendium.de/sites/net/0812221.htm (дата обращения: 05.03.2020).

3. JA3 SSL Fingerprint [Электронный ресурс]. URL: https://ja3er.com (дата обращения: 05.03.2020).

4. TLS Fingerprinting with JA3 and JA3S [Электронный ресурс]. URL: https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967 (дата обращения: 05.03.2020).

5. Перехват данных по сети [Электронный ресурс]. URL: https://www.anti-malware.ru/threats/network-traffic-interception (дата обращения: 10.03.2020).

6. Что такое IoT? [Электронный ресурс]. URL: https://www.oracle.com/at/internet-of-things/what-is-iot/ (дата обращения: 10.03.2020).

7. Более безопасный Интернет вещей [Электронный ресурс]. URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security (дата обращения: 10.03.2020).

8. Что Такое Безопасное Программирование? [Электронный ресурс]. URL: https://www.perforce.com/blog/sca/what-secure-coding (дата обращения: 10.03.2020).

9. Принципы работы протокола DHCP [Электронный ресурс]. URL: https://www.smart-soft.ru/blog/printsipy_raboty_protokola_dhcp (дата обращения: 10.03.2020).

10. Принципы работы протокола DHCP [Электронный ресурс]. URL: https://selectel.ru/blog/dhcp-protocol (дата обращения: 10.03.2020).