УДК 621.382

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПІДТРИМКОЮ DDoS-АТАК В МЕРЕЖАХ IoT

Аверкієв Є.О., Правило В.В.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: v.v.pravylo@ukr.net, averk1eeev@gmail.com

ANALYZING MALICIOUS SOFTWARE SUPPORTING DDOS ATTACKS ON IOT NETWORKS

The scheme and purpose of DDoS attacks are considered. Three of the most dangerous malware supporting DDoS attacks on IoT networks are presented for review. General recommendations on how to effectively counteract these three malicious software are provided.

DDoS (Distributed Denial of Service) атаки використовуються для переповнення ресурсів обчислювальної техніки, роблячи її недоступною для легітимних користувачів.

Програми, що підтримують такі атаки, стали гострою проблемою через їх здатність збільшувати інтенсивність та масштаб нападів, роблячи їх більш складними для виявлення. До того ж велика кількість цих програм доступна вільно в Інтернеті та має відкритий вихідний код, що робить їх доступними для широкого кола користувачів.

Однією з популярних стратегій є використання ботнетів – мережі компрометованих пристроїв, які віддалено керуються зловмисниками. Вона може включати в себе комп'ютери, ноутбуки чи навіть підключені IoT-пристрої.

Схема DDoS-атаки включає, переважно, одразу декілька пристроїв, що підконтрольні зловмиснику, і генерують шкідливий трафік. Як тільки атака почнеться, чистий трафік відвідувачів певного ресурсу, на який ведеться атака та шкідливий трафік зловмисника збирається в одне ціле, і йде відправка величезної кількості запитів на обчислювальну техніку, яка в результаті при відсутності додаткового захисту, повністю стає ускладненою для доступу, або ж взагалі недоступною (рис. 1).

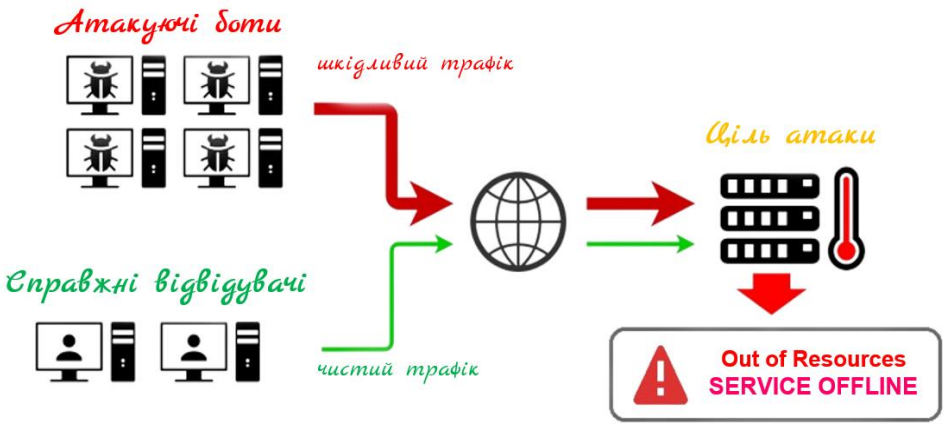

Рис.1. Схема основної роботи DDoS-атаки на ресурси будь-якого типу.

Враховуючи вищенаведену інформацію, стає зрозумілим, що DDoS-атаки становлять серйозну загрозу для цифрового світу. Вони можуть призвести до значних втрат даних, перерв у роботі служб та фінансових збитків. Особливо небезпечними є атаки на Інтернет речей (IoT), оскільки багато IoT-пристроїв не мають достатнього захисту і можуть бути легко скомпрометовані.

Вірусів, що підтримують такі DDoS-атаки існує досить велика кількість. Це пов'язано з тим, що багато з тих вірусів, що були створені на самому початку, мали відкритий вихідний код. Саме цей фактор і дозволяє зловмисникам створювати власні модифікації цих вірусів, тим самим значно збільшуючи їх загальну кількість. В рамках дослідження буде розглянуто 3 найнебезпечніших програмних забезпечення з підтримкою DDoS-атак на мережі IoT, які існують на теперішній час, а також наведено загальні рекомендації щодо їх протидії (Mirai, XOR.DDoS, Linux.Hydra).

1. Mirai:

Це шкідливе програмне забезпечення, яке стало відоме своєю здатністю зламувати та заражати пристрої Інтернету речей (IoT). Його основна мета – створення ботнету для здійснення DDoS-атак на різноманітні цілі.

Головною метою Mirai є використання заражених IoT-пристроїв для проведення DDoS-атак. Це досягається шляхом скоординованого надсилання великої кількості запитів до цільового сервера або мережі, зумовлюючи їх перевантаження та відмову в обслуговуванні. Внаслідок цього, цільовий об'єкт може перестати відповідати на легітимні запити користувачів.

Mirai також вирізняється тим, що він може самостійно розпізнавати та уникати деяких захисних заходів, що може ускладнити виявлення та подолання цього шкідливого ПЗ.

Таким чином, для забезпечення безпеки IoT-пристроїв та захисту від Mirai рекомендації можуть бути наступними:

- Встановіть сильні паролі, які складаються з комбінації великих і малих літер, цифр і спеціальних символів.
- Оновіть вбудоване програмне забезпечення (Firmware) на IoT-пристроях, включаючи оновлення безпеки.
- Налаштуйте фільтри трафіку на мережевих пристроях для виявлення та блокування аномального або потенційно шкідливого трафіку.
- Закрийте порт TCP 23 (бо саме через цей порт працюють основні компоненти ПЗ Mirai) і окремо службу Telnet на маршрутизаторі.

2. XOR.DDoS:

XOR DDoS - це троянський вірус для Linux з можливостями rootkit, який використовувався для запуску масштабних DDoS-атак. Його назва походить від інтенсивного використання XOR-шифрування як у вірусі, так і в мережевому спілкуванні з C&C. Він створений для різних архітектур Linux, таких як ARM, x86 та x64. XOR.DDoS був виявлений у вересні 2014 року групою дослідників MalwareMustDie.

XOR.DDoS використовує механізми уникнення, які дозволяють його операціям залишатися непомітними. Його можливості уникнення включають замаскування дій вірусу, уникнення механізмів виявлення на основі правил та пошуку чужих шкідливих файлів на основі хешу, щоб прибрати «конкуренцію».

Також XOR.DDoS приховує шкідливі дії від спеціального аналізу, перезаписуючи чутливі файли нульовим байтом. Він також включає різні механізми для підтримки різних дистрибутивів Linux.

Таким чином, для забезпечення безпеки IoT-пристроїв від XOR.DDoS наступні рекомендації можуть бути впровадженими:

- Змініть паролі за замовчуванням на сильні.
- Обмежте кількість IP-адрес, з якими ваш пристрій IoT з'єднується.
- Використовуйте мережевий брандмауер та фільтрацію DNS для блокування потенційних SYN-пакетів.
- Встановить оновлення програмного забезпечення.

3. Linux.Hydra:

Linux.Hydra - інструмент для взлому паролів, який підтримує численні протоколи для атаки. Hydra працює, використовуючи різні підходи для виконання атак грубої сили, щоб вгадати правильну комбінацію імені користувача та пароля. Цей інструмент наглядно показує, наскільки легко можна було б отримати несанкціонований доступ до системи віддалено. Hydra може виконувати швидкі атаки перебором за словником проти більш ніж 50 протоколів, включаючи telnet, FTP, HTTP, HTTPS, SMB.

Для забезпечення безпеки IoT-пристроїв від шкідливого ПЗ Linux.Hydra, рекомендації можуть виглядати таким чином:

- Змініть паролі за замовчуванням на сильні.
- Налаштуйте систему, щоб вона блокувала спроби вводу паролів після N-ої невдалої кількості спроб.

Література

1. Навчальний посібник «Технології Інтернету речей» [Електронний ресурс] – Б.Ю. Жураковський, І.О. Зенів – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/42078/1/Zhurakovskyi_B_Zeniv_Tehnologii_internet_rechey.pdf
2. Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, 39(1), Article 3.
3. Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294–1312.
4. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: mirai and other botnets. IEEE Computer, 50(7), 80–84.
5. Houle, K. J., & Weaver, G. M. (2001). Trends in denial of service attack technology. Tech. Rep., CERT Coordination Center, Pittsburgh, Pa, USA.
6. Bertino, E., Choo, K.-K. R., Georgakopolous, D., & Nepal, S. (2016). Internet of things (IoT): smart and secure service delivery. ACM Transactions on Internet Technology (TOIT), 16(4), Article 22.