Темна сторона ForSSHe

Дослідження ESET
Грудень 2018 р.

Вступ

SSH (скорочено від Secure Sheell) — це мережевий протокол для віддаленого підключення до комп'ютерів та пристроїв через зашифроване посилання. Він зазвичай використовується для управління серверами Linux за допомогою текстової консолі. SSH — це найпоширеніший спосіб управління для системних адміністраторів віртуальними, хмарними або орендованими виділеними серверами Linux.

Де-факто реалізація в комплекті майже всіх дистрибутивів Linux — це портативна версія OpenSSH. Створення бекдорів сервера OpenSSH та клієнта на сервері — є популярним способом, який використовують зловмисники для отримання доступу до серверу Linux. Існує кілька причин чому створення зловмисного програмного забезпечення на базі OpenSSH є таким поширеним:

- Це не вимагає відкриття нового TCP-порту на ураженому комп'ютері. SSH має вже бути там та, ймовірно, доступний з мережі Інтернет.
- Демон (daemon) та клієнт OpenSSH бачать паролі в чистому тексті, що дозволяє злодію викрадати облікові дані.
- Вихідний код OpenSSH знаходиться у вільному доступі, а це полегшує створення «індивідуальної» версії бекдора.
- OpenSSH створений таким чином, щоб ускладнити під час атаки man-in-the-middle перегляд активності користувача. Зловмисник може використати це для приховування своєї шкідливої діяльності.

З метою протидії загрозам для ОС Linux, спеціалісти ESET досліджували відомі та невідомі бекдори OpenSSH. Для аналізу даної загрози, спеціалісти використовували одне з попередніх досліджень — операції Windigo. У даному дослідженні спеціалісти ESET детально описали декілька компонентів шкідливих програм та їх взаємодію. Ebury, бекдор OpenSSH та викрадач даних облікових записів, був встановлений на десятки тисяч серверів по всьому світу.

Інформація, яка спочатку не досліджувалась в документі «Операція Windigo», але яку дослідники ESET обговорювали на конференціях, полягає в тому, як зловмисники намагаються виявити інші бекдори OpenSSH перед їх розгортанням (Ebury). Зловмисники використовують Perl-скрипт, який містить більше 40 підписів для різних бекдорів.

```
@sd = gs( 'IN: %s@ \(%s\) ', '-B 2' );
@sc = gc( 'OUT=> %s@%s \(%s\)', '-B 1' );
if ( $sd[1] =~ m|^/| or $sc[0] =~ m|^/| ) {
    print
      "mod_sshd29: '$sd[0]':'$sd[1]':'$sd[2]'\nmod_sshc29: '$sc[0]':'$sc[1]'\
n";
    ssh_ls( $sd[1], $sc[0] );
}
```

Приклад підпису, знайденого в скрипті Windigo Perl для виявлення бекдора OpenSSH

Коли спеціалісти ESET почали шукати кожен підпис, вони зрозуміли, що не можуть знайти зразки для більшості бекдорів, описаних у скрипті. **Оператори зловмисників насправді мали більше знань та огляду бекдорів SSH в реальному середовищі, ніж спеціалісти ESET.** Щоб впоратися з цією ситуацією, спеціалісти почали стежити за зниклими зразками шкідливого програмного забезпечення, використовуючи їх підписи. Це допомогло удосконалити виявлення та повідомити про результати дослідження спеціалістів ESET в даному документі.

Дослідники ESET опублікували документ, присвячений 21 сімейству бекдора OpenSSH, розгорнутим в реальному середовищі. Хоча деякі з цих бекдорів вже були проаналізовані та задокументовані, більшість із них не мали опублікованих аналізів, доступних раніше. Мета цієї статті полягає у наданні огляду поточного стану поширення бекдора OpenSSH. Це результат довготривалого дослідження, що полягає у написанні правил та виявлень, розгортанні різних пасток для зловмисників, класифікації зразків та аналізу різних сімейств шкідливого програмного забезпечення.

Особливості бекдора

Незабаром після дослідження Windigo спеціалісти ESET переклали підписи зі скрипта Perl в правилах YARA (які відтепер доступні в GitHub) та використовували їх для пошуку зразків шкідливого програмного забезпечення з різних каналів. Дослідники зібрали зразки за період більше 3 років та після фільтрації помилкових спрацьовувань отримали кілька сотень троянських OpenSSH-файлів. Аналіз даних зразків показав використання набору загальних ознак у різних бекдорах. Дві з них дійсно виділяються:

- У 18 з 21 сімейств передбачено функцію викрадення даних облікових записів, яка дає можливість викрадати паролі та/або ключі, які використовуються троянізованим OpenSSH-клієнтом та сервером.
- 17 з 21 сімейств мають режим бекдора, який дозволяє зловмисникові зберігати прихований та постійний спосіб підключення до ураженої машини.

Паралельно з аналізом зразків, які спеціалістам ESET вдалося зібрати, вони також створили власну архітектуру ресурсу, який є приманкою для зловмисників (детальна інформація міститься в огляді), щоб розширити результати. Ідея полягала в тому, щоб вилучити в зловмисників облікові дані, використовуючи технології ексфільтрації, зворотну конструкцію зразків. Таким чином, спеціалісти ESET могли спостерігати за поведінкою зловмисників після того, як вони атакували сервер та отримали найновіші зразки.

Поєднання як пасивного спостереження з набором правил YARA, так і взаємодії зі зловмисниками через ресурс, який є приманкою для зловмисників дало спеціалістам ESET уявлення про активність та навички зловмисників.

Сімейство бекдора OpenSSH

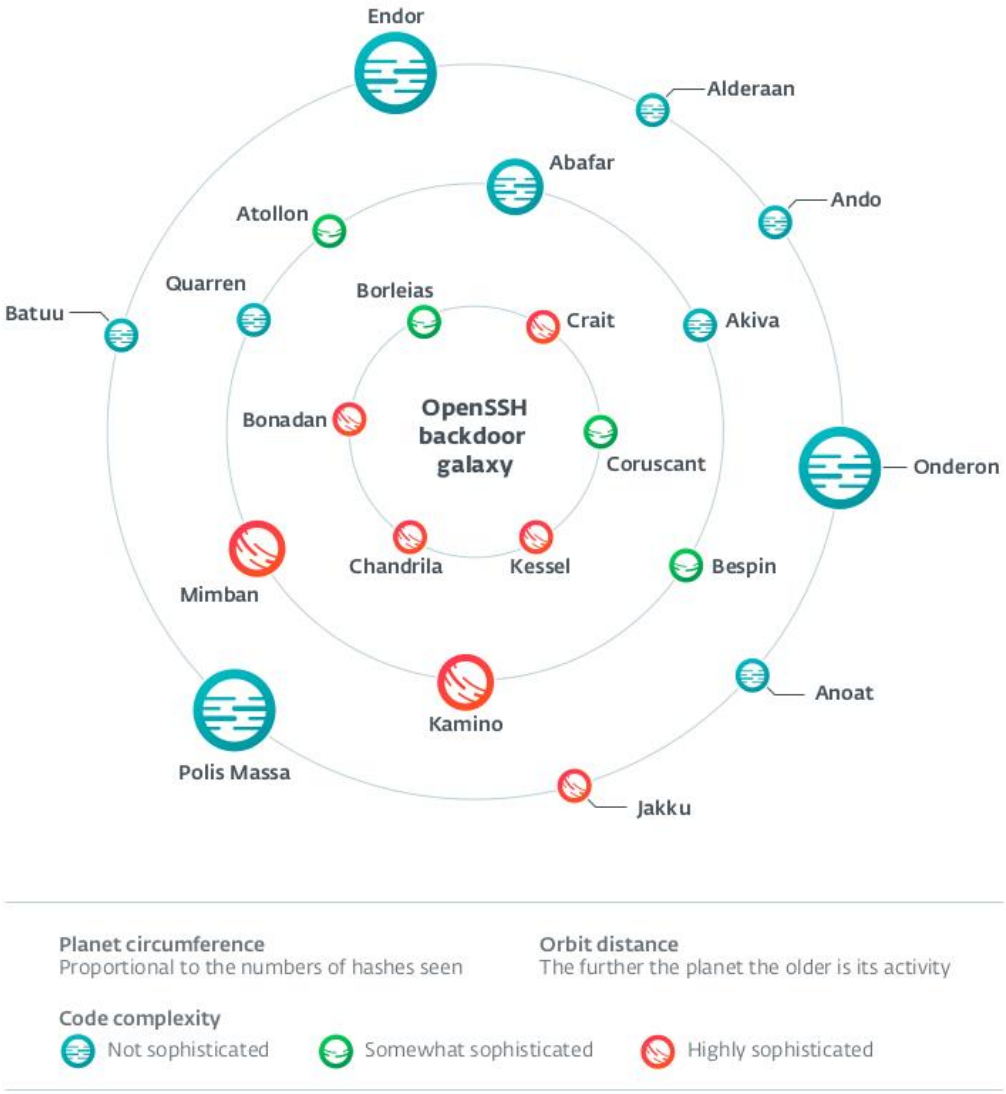

Рис.1. Сімейство бекдора OpenSSH

На малюнку зібрані сімейства OpenSSH, які спеціалісти ESET використовували під час цього дослідження. Деякі з читачів могли помітити, що назви сімейств відповідають назвам планет з саги «Зоряні війни». Зауважте, що вони не відповідають ідентифікаторам ESET; це спосіб їх ідентифікації в дослідженнях спеціалістів ESET. Ідентифікатори їх виявлення наведені в дослідженні та на GitHub.

Оцінка складності сімейств шкідливого програмного забезпечення може бути суб'єктивною. Спеціалісти ESET намагалися бути максимально об'єктивними та створили класифікацію за кількома факторами, зокрема:

- Наявність методики ексфільтрації (наявність командного сервера (C&C), мережевого протоколу, шифрування при переносі або зберіганні тощо);
- Реалізація модулів, які забезпечують додаткові функції для OpenSSH (додаткові команди, майнінг криптовалют тощо);
- Використання шифрування або маскування для ускладнення аналізу.

Кожне сімество загроз має власний опис у повному звіті, але сімейство все ще має деякі винятки:

- Згідно з набором зразків, зібраних спеціалістами ESET, складність коду стає все важливішою для нових сімейств.

- Дослідники ESET зібрали більше зразків старих та простих сімейств. Це можна пояснити тим, що складні зразки важче виявити та вони є менш поширеними.

Виявлені бекдори

Деякі з виявлених бекдорів не є особливо новими або цікавими з технічної точки зору. Однак, існує декілька винятків, які показують, що деякі зловмисники докладають багато зусиль для збереження своїх ботнетів.

Один з них — Kessel, який виділяється багатьма способами комунікації з командним сервером. Він реалізує HTTP, незахищені TCP та DNS. Крім вимагання викрадених облікових даних, командний сервер також має можливість надсилати додаткові команди, такі як завантаження файлів з або на інфікований пристрій. Весь зв'язок з командним сервером також зашифрований. Бекдор Kessel є досить новим: домен командного сервера був зареєстрований в серпні 2018 року.

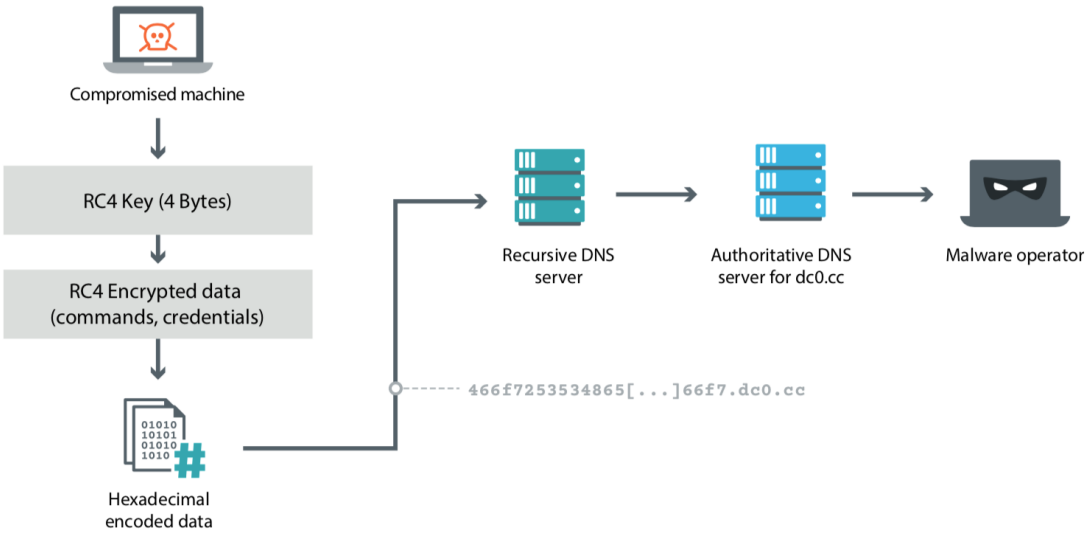

Рис.2. Ексфільтрація DNS Kessel

Інший бекдор має назву Kamino. Після аналізу зразків, виявлених спеціалістами ESET, вдалося з’ясувати, що ця загроза існувала та розвивалася протягом тривалого часу, завдяки методам маскування та використання. Вперше їх було використано зловмисною кампанією, яка, як відомо, використовує шкідливе програмне забезпечення DarkLeech для перенаправлення трафіку, як це було задокументовано дослідниками ESET у 2013 році. Цікаво, що схожий бекдор використовувався для атак на російські банки групою зловмисників Carbanak роками пізніше, як описано групою IB. Перехід від шкідливого програмного забезпечення до більш цілеспрямованих атак є досить цікавим. Можна припустити, що обидві атаки здійснені однією групою, але це також можна пояснити й тим, що існують автори, які продають код декільком групам.

У дослідженні також наведено детальний аналіз бекдорів Chandrila (викрадення паролів) та Bonadan (майнінг криптовалют).

Запобігання ураженню

Оскільки дані, які проаналізували спеціалісти ESET, були шкідливими зразками, взятими поза їх контекстом, важко визначити первинні вектори інфікування. Техніка інфікування може включати в себе: використання облікових даних, викрадених після користування компрометуючим клієнтом SSH, підбором логіна та паролю, розповсюдженням або експлуатацією уразливої сервісної служби. Щоб запобігти небезпеці вашої системи, рекомендується:

- Регулярно оновлювати систему
- Віддавати перевагу аутентифікації на основі ключових слів для SSH
- Вимкнути віддалені входи в систему від імені адміністратора
- Використовувати для SSH багатофакторну аутентифікацію

Рішення ESET виявляють бекдори OpenSSH як варіанти Linux/SSHDoor. Крім того, набір правил YARA, який використовують спеціалісти ESET може допомогти класифікувати потенційні зразки. У дослідженні наведено детальну інформацію про перевірку файлів OpenSSH за допомогою пакетів управління Linux для перевірки цілісності встановлених виконуваних файлів.

Висновок

Завдяки цьому дослідженню, спеціалісти ESET сподіваються розширити інформацію про бекдор OpenSSH та зловмисне програмне забезпечення для операційної системи Linux в цілому. Як зазначалося, через складність коду, деякі зловмисники повторно використовують доступний вихідний код, в той час як інші докладають реальних зусиль для застосування коду . Крім того, спостереження за кіберзлочинцями допомогою ресурсів-приманок показує, що деякі зловмисники все ще активні та дуже обережні при розгортанні своїх бекдорів.

Дане дослідження показує, що кількість шкідливого програмного забезпечення для Linux лише зростає. Така тенденція може бути пов’язана з тим, що через недостаність видимості, загрози залишаються об’єктами спостереження на більш довгий період.

Повна версія дослідження доступна у документі.

Дослідження подано в перекладі. Оригінал доступний за посиланням.