Н.А. Филатов

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ СЕРВИСА SAMBA С ПОМОЩЬЮ МЕТОДА ЛОВУШЕК

(Самарский университет)

В современном мире стремительно растет уровень угрозы, которому подвергаются пользователи глобальной сети Интернет. Основными целями злоумышленников являются нарушение технической инфраструктуры сети в целом, обнаружение и эксплуатация уязвимостей и т.д. Такие атаки осуществляются, в основном, на различные сетевые сервисы. Одним из таких сетевых сервисов, популярным среди злоумышленников, является сервис Samba. Это сетевая файловая система, реализованная при помощи стандартного набора программ, которые обеспечивают универсальный доступ к сетевым принтерам и хранилищам данных [1].

В настоящей работе рассматриваются результаты анализа данных об информационных вторжениях на сеть серверов-ловушек. Такие специальные сервера-ловушки, размещенные в разных географических зонах, в количестве 4 штук функционируют с 2017 года.

Для проведения эксперимента по анализу вторжений на сетевой ресурс были использованы серверы-ловушки [2]. Сервера-ловушки – это специальные сервера с установленными на них сервисами, записывающие все обращения к ним, а также отвечающими на внешние запросы [3]. В качестве операционной системы для сервера ловушки выбрана GNU Debian/Linux, так как это свободно распространяемая OS с доступными исходными кодами всего применяемого программного обеспечения.

Сервера-ловушки никак не проявляют себя во внешней сети, поэтому осуществление доступа к ним означает, что происходит намеренное сканирование глобальной сети. Слишком часто повторяющиеся запросы с одного и того же IP адреса в данном случае можно однозначно позиционировать как несанкционированные. Любое сетевое обращение к серверу происходит через коммуникационный порт, поэтому важно осуществить контроль над портами. Для этого применяется ряд программных средств, среди которых ПО “Wireshark”, записывающее весь трафик на внешнем порту. Анализ данных с серверов-ловушек позволяет извлечь сведения, необходимые для построения модели вторжения. Такие специальные сервера для репрезентативности данных размещены в разных географических зонах в количестве 4 штук. Они начали функционировать с 2017 года.

В 2019 году был зафиксирован значительный рост запросов на SMB сервис. Проанализировав данные становится видно, что характер атаки напоминает вредоносную программу “SambaCry” [4]. Эта вредоносная программа сканирует в интернете узлы в поисках компьютеров с открытым TCP-портом 445, который отвечает за обслуживание протокола SMB. Обнаружив такой компьютер,

программа предпринимает несколько попыток проэксплуатировать на нём уязвимость EternalBlue и, в случае успеха, устанавливает вредоносное ПО DoublePulsar, через который загружается и запускается исполняемый код программы SambaCry.

После обнаружения машины с открытым портом NetBIOS, SambaCry получает сокет TCP для порта 445, подключится к сокету SMB и получит идентификатор дерева SMB для дальнейшего использования [5]. Затем происходит передача трех пакетов установки сеанса NetBIOS, содержащие либо два IP-адреса (192.168.56.20 и 172.16.99.5) жестко запрограммированных в теле вредоносного ПО, либо случайны адреса. В нашем случае встречается IP-адрес 192.168.56.20 и множество других случайных IP-адресов в равном соотношении (см. рис. 1).

```
SMB        151 Tree Connect AndX Request, Path: \\192.168.9.1\IPC$
SMB        151 Tree Connect AndX Request, Path: \\192.168.0.3\IPC$
SMB        151 Tree Connect AndX Request, Path: \\192.168.1.107\IPC$
SMB        152 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB        152 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB        151 Tree Connect AndX Request, Path: \\169.254.226.5\IPC$
```

Рис. 1. IP-адреса

Затем производится подключение к дереву IPC$ и попытка выполнить транзакцию с FID 0. Если возвращено состояние «STATUS_INSUFF_SERVER_RESOURCES», то это означает, что на машине не было применено исправление CVE-2017-7494 [5]. После чего последовал бы запрос, содержащий вредоносный код. В нашем случае возвращалось другое состояние, так как уязвимость закрыта (см. рис. 2).

```
SMB         144 Negotiate Protocol Request
SMB         219 Negotiate Protocol Response
SMB         159 Session Setup AndX Request, User: .\
SMB         143 Session Setup AndX Response
SMB         151 Tree Connect AndX Request, Path: \\85.14.232.4\IPC$
SMB          95 Tree Connect AndX Response, Error: Bad userid
SMB Pipe    134 PeekNamedPipe Request, FID: 0x0000
SMB          95 Trans Response, Error: STATUS_NETWORK_NAME_DELETED
```

Рис. 2. Запрос FID 0 на сервер и ответ

Целью же запроса SESSION SETUP Trans2 Request было проверить, была ли система уже скомпрометирована Doublepulsar`ом (см. рис. 3).

```
SMB          193 Negotiate Protocol Request
SMB          165 Negotiate Protocol Response
SMB          196 Session Setup AndX Request, User: anonymous
SMB          186 Session Setup AndX Response
SMB          152 Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB          116 Tree Connect AndX Response
SMB          138 Trans2 Request, SESSION_SETUP
SMB           95 Trans2 Response, SESSION_SETUP, Error: STATUS_ACCESS_DENIED
```

Рис. 3. Попытка проверить скомпрометирована ли уже система

Если поле «Multiplex ID» равно 65 (0x41), это означает, что текущая система не является зараженной (см. рис. 4). В противном случае «Multiplex ID», равное 81 (0x51), указывает, что система уже была заражена Doublepulsar`ом.

```
SMB (Server Message Block Protocol)
  SMB Header
      Server Component: SMB
      [Response to: 29]
      [Time from request: 0.000142000 seconds]
      SMB Command: Trans2 (0x32)
      NT Status: STATUS_ACCESS_DENIED (0xc0000022)
    > Flags: 0x88, Request/Response, Case Sensitivity
    > Flags2: 0xc007, Unicode Strings, Error Code Type,
      Process ID High: 0
      Signature: 0000000000000000
      Reserved: 0000
    > Tree ID: 56689 (\\192.168.56.20\IPC$)
      Process ID: 65279
      User ID: 31864
      Multiplex ID: 65
```

Рис. 4. Ответное сообщение, содержащее Multiplex ID равное 65

После первоначального согласования и настройки сеанса, SambaCry отправляет целевой запрос ping, отправив несколько скомпилированных пакетов в скомпрометированную систему. Целью запроса ping было проверить, был ли Doublepulsar успешно установлен. Инструкция «ping» была скрыта в поле «Timeout», которое изначально было временем, которое клиент должен был ждать, пока сервер ответит на невыполненный запрос. Согласно спецификациям, значение по умолчанию для поля Timeout было установлено равным 45 секундам. В сетевом пакете SambaCry поле Timeout было установлено на 4 часа 20 минут 10,881 секунды (0x00ee3401) (см. рис. 5). Это ненормальное значение тайм-аута на самом деле не относится к установленному тайм-ауту, но подразумевает код операции инструкции Doublepulsar. Алгоритм вычисления этого кода операции добавляет каждый байт и удаляет переполнение как результат. Если Doublepulsar успешно установлен в зараженной системе, он отправит обратно созданный пакет с преднамеренно установленным полем «Multiplex ID».

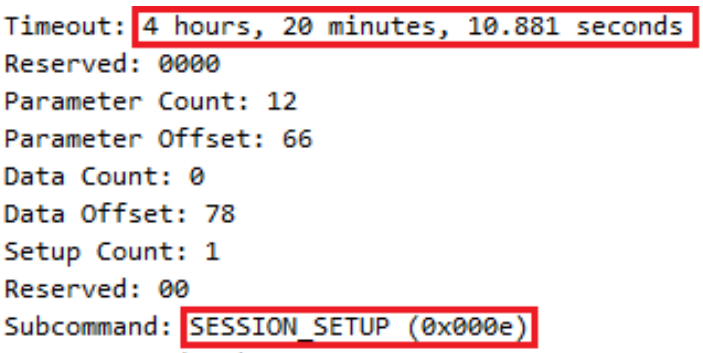

Рис. 5. Команда «Ping» в скрытом поле Timeout

Таким образом, были зафиксированы уникальные данные, анализ которых позволил идентифицировать попытку атаки вредоносной программы под названием «SambaCry». Полученные данные позволяют отслеживать и анализировать действия злоумышленников для выявления актуальных методов и тенденций произведения атак, а также создать модель сетевого вторжения в будущем, на основании которой должно быть разработано соответствующее программное обеспечение, чтобы работать в локальных сетях и производить предварительное тестирование сетевых ресурсов [6].

Литература

1. Котенко И.В., Степашкин М.В., "Обманные системы для защиты информационных ресурсов в компьютерных сетях", Тр. СПИИРАН, 2:1 (2004), 211–230.

2. Shkirdov D. A. et al. Building a Network Intrusion Model Based on Data from Honeypots //2018 26th Telecommunications Forum (TELFOR). – IEEE, 2018. – С. 1-4.

3. Islam A., Oppenheim N., Thomas W. SMB Exploited: WannaCry Use of "EternalBlue" //Retrieved December. – 2017. – Т. 11. – С. 2017.

4. Da-Yu K. A. O., HSIAO S. C., Raylin T. S. O. Analyzing WannaCry Ransomware Considering the Weapons and Exploits //2019 21st International Conference on Advanced Communication Technology (ICACT). – IEEE, 2019. – С. 1098-1107.

5. Lohachab A., Karambir B. Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks //Journal of Communications and Information Networks. – 2018. – Т. 3. – №. 3. – С. 57-78.

6. Зегжда П. Д., Корт С. С. Модель хостовой системы обнаружения вторжений //Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму. – 2007. – С. 102.