ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ SHADOWPAD

РЫБКО Марина Дмитриевна
студент
МИНАЕВ Андрей Николаевич
студент
ФГБОУ ВО «МИРЭА – Российский технологический университет»
г. Москва, Россия

В статье рассматривается один из современных представителей бэкдоров - ShadowPad, а также некоторые атаки с его использованием. В рамках статьи освещена история обнаружения бэкдора, алгоритм действия, примеры применения злоумышленниками.
Ключевые слова: бэкдор; ShadowPad; информационная безопасность; обнаружение атак; кибербезопасность.

Введение. Бэкдор может быть законно установлен разработчиками программного и аппаратного обеспечения, чтобы помочь им легко получить доступ к своим приложениям для решения проблем с программным обеспечением. Но в большинстве случаев бэкдоры устанавливаются киберпреступниками, чтобы получить незаконный доступ к устройству, сети или программному приложению.

Описание. ShadowPad – многомодульный троян-бэкдор, написанный с использованием языков C/C++ и Assembler, предназначенный для работы в 32-х и 64-х разрядных операционных системах семейства Microsoft Windows. ShadowPad чаще всего представляет собой вредоносную DLL-библиотеку. Используется для целевых атак на информационные системы и несанкционированного доступа к данным для их передачи на управляющие серверы. Основная функциональность бэкдора ShadowPad реализована при помощи встроенных в него модулей – плагинов. Модульная структура позволяет масштабировать его возможности, обеспечивая любую функциональность. В чистом виде, без дополнительных вредоносных программ, чаще всего ShadowPad используется злоумышленниками для сбора информации (получения персональных данных, паролей, захвата вводимой с клавиатуры информации и т. п.). Также стоит отметить, что ShadowPad это целое семейство программных версий.

В отличие, например, от схожего публично продаваемого бэкдора PlugX, ShadowPad в частном порядке используется ограниченным кругом пользователей (drweb.ru. Исследование APT-бэкдора ShadowPad и его связи с PlugX [Электронный ресурс]. 2020 – URL: https://news.drweb.ru/show/?i=14048). Плагины также продают отдельно. Из этого можно сделать вывод, что разработчики ShadowPad более тщательно следят за распространением своего продукта. Также редко встречались сборки с более чем 7-10 плагинами одновременно, хотя на сегодняшний момент их известно не менее 23.

По данным исследователей аналитики угроз информационной безопасности ShadowPad регулярно обновляется более продвинутыми методами защиты от обнаружения и сохранения, поэтому информация по бэкдору очень быстро устаревает, что усложняет нахождение решений по защите от потенциальных атак с использованием новых версий ShadowPad. С другой стороны, основные принципы работы бэкдора (не считая появления новых по функционалу модулей) изменяются редко, поэтому если ShadowPad всё-таки будет обнаружен в системе, защититься от его вмешательства будет относительно не трудно.

Обнаружение ShadowPad. В июле 2017 г. к специалистам «Лаборатории Касперского» за помощью обратилась одна из компаний-партнеров в связи с появлением необычных DNS-запросов. Расследование показало [1], что источником подозрительной активности оказалось программное обеспечение, произведенное компанией NetSarang (поставщиком решений управления серверами для крупных корпоративных сетей). Бэкдор-платформа была встроена в одну из библио-

тек кода легитимного программного обеспечения. Дальнейший анализ выявил, что запросы являлись результатом работы вредоносного модуля, спрятанного внутри последней версии программного обеспечения.

Принцип действия базовой версии ShadowPad. После установки зараженного ПО вредоносный модуль начинает отправлять DNS-запросы на командный и контрольный сервер с частотой несколько раз в сутки. Запрос содержит основную информацию о системе жертвы: имя пользователя, доменное имя, имя хоста и пр. Если злоумышленник посчитал систему интересной для дальнейшего взлома, то командный сервер отвечал и активировал полноценную бэкдор-платформу, которая незаметно разворачивалась внутри атакуемой системы. В дальнейшем, бэкдор-платформа могла загружать и выполнять вредоносный код по команде злоумышленника.

Алгоритм работы. На первом этапе происходит дешифрование шелл-кода (shellcode), отвечающего за установку бэкдор-платформы в системе. Дешифрование осуществляется XOR-подобным алгоритмом, характерной особенностью которого является модификация ключа шифрования на каждой итерации при помощи арифметических операций с определенными константами.

После дешифрования управление передается загрузчику, который отличается характерным типом обфускации (приведение исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции). Данный тип заключается во вставке определенных байтов в различные участки кода, которые предварительно обозначены двумя противоположными условными переходами, указывающими на один и тот же адрес. Чтобы избавиться от данной обфускации, необходимо заменить указанные байты (например, на операционный код NOP).

После получения необходимых адресов API-функций и размещения в памяти необходимых участков кода управление передается на этап установки бэкдор-платформы.

Характерной особенностью любого экземпляра ShadowPad является шифрование строк, содержащихся в каждом модуле. Алгоритм шифрования похож на используемый при дешифровании бэкдора, отличаются лишь используемые при модификации ключа константы.

Атаки с использованием ShadowPad. ShadowPad активно используется группой Winnti (APT41, BARIUM, AXIOM), которая активна по меньшей мере с 2012 г. Происходит Winnti предположительно из Китая [2]. Основной арсенал группы состоит из вредоносного программного обеспечения собственной разработки. Первая атака с использованием ShadowPad была зафиксирована в 2017 г.

ShadowPad часто применяется в атаках типа supply-chain. Таким, к примеру, был взлом CCleaner [4]. Последний отчет об активности группы Winnti с использованием ShadowPad был выпущен компанией ESET в январе 2020 г. [3].

От атак с применением ShadowPad пострадали организации в Гонконге, Индии, Пакистане и других странах Центральной Азии.

Заключение. До сих под до конца не известно, кто разработал ShadowPad.

Исследователи отмечали сходство программного кода и принципов действия ShadowPad и бэкдора PlugX, некоторые приемы разработки и технические решения практически копировали друг друга. Можно сделать вывод о связи этих семейств, но при этом возможно, как простое заимствование кода, так и разработка обеих программ одним автором или группой авторов.

По словам исследователей, в области кибербезопасности, использование ShadowPad значительно снижает затраты на разработку и обслуживание вредоносных программ для злоумышленников. Однако, как отмечалось ранее, ShadowPad не распространяется среди злоумышленников так активно, как аналоги, поэтому не смотря на высокое программное качество данного бэкдора, встречается он крайне редко и только у малочисленных групп пользователей.

СПИСОК ЛИТЕРАТУРЫ

1. Global Research & Analysis Team, Kaspersky Lab. ShadowPad in corporate networks. 2017 – URL:https://securelist.com/shadowpad-in-corporate-networks/81432/ (дата обращения: 10.01.2023).
2. Global Research & Analysis Team, Kaspersky Lab. Winnti. More than just a game. 2013 – URL:https://securelist.com/winnti-more-than-just-a-game/37029/ (дата обращения: 10.01.2023).
3. Mathieu Tartare. Winnti Group targeting universities in Hong Kong. 2020. – URL: https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/ (дата обращения: 10.01.2023).
4. ONDREJ VLCEK. Recent findings from CCleaner APT investigation reveal that attackers entered the Piriform network via TeamViewer. 2018. – URL:https://blog.avast. com/update-ccleaner-attackers-entered-via-teamviewer (дата обращения: 10.01.2023).